Carl Friedrich Gauss

Untersuchungen über höhere Arithmetik

Deutsche Übersetzung

Band I

Dieser Band enthält die historischen Titelblätter, die Widmung, die Vorrede, alle sieben Abschnitte, die Nachträge, Tabellen und den historischen Inhalt, Gauss' handschriftliche Aufzeichnungen sowie die historische Schlussbemerkung des Herausgebers. Die ursprünglich deutschen Passagen des Anhangs und die Schlussbemerkung sind in modernem Deutsch wiedergegeben. Die Seitenangaben im historischen Inhaltsverzeichnis entsprechen denen der Vorlage.

Historische Quelle: Carl Friedrich Gauss, Werke, Band I, Göttingen, 1863. Die Disquisitiones Arithmeticae erschienen erstmals 1801 in Leipzig.
Mit OpenAI GPT-6.1 Sol KI-übersetzt ins Deutsche.

Quellen und Terminologie der Übersetzungen

Historischer Text: Carl Friedrich Gauss, *Werke*, Band I, Göttingen, 1863. Historische Herausgeberbeiträge behalten ihre eigene Urheberschaft und ihre Unterschriften. Ursprünglich deutsche Passagen sind im deutschen Leseband in modernem Deutsch wiedergegeben; ihre historischen Originale werden gesondert mitgeliefert.
Diese englischen und deutschen Ausgaben sind mit OpenAI GPT-6.1 Sol KI-übersetzt; auch der Satz wurde durch KI erstellt. Die folgenden menschlichen Übersetzer und Autoren sind mit ihren Schriften Quellen für die jeweils bezeichnete Terminologie und den Sprachgebrauch. Mathematische Vorlage bleibt Gauss' originalsprachlicher Text.

H. Maser.

Deutscher Übersetzer und Herausgeber, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Entsprechende arithmetische Passagen und deutsche mathematische Terminologie.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead und Adam Miller Hiltebeitel.

Übersetzer von Gauss' *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX-Ausgabe. Verwandte englische geometrische Terminologie und Ausdrucksweise.
`https://www.gutenberg.org/ebooks/36856`

Paul Taylor; Bernard Leak.

Taylors englische Übersetzung von Gauss' zweitem Beweis des Fundamentalsatzes der Algebra, mit Korrekturen von Leak, 1983. Verwandte englische algebraische Terminologie. Die herangezogene Online-Ausgabe nennt Dezember 1983 als Übersetzungsdatum, August 2003 für die LaTeX-Fassung und den 8. Juni 2007 als letztes Änderungsdatum der zugrunde liegenden Quelle. Ihre Danksagung nennt Mark Wainwright für die Rückgabe von Taylors Notizen und Nikita Danilov für die Korrektur von Tippfehlern.
`https://www.paultaylor.eu/misc/gauss.html`

Ulrich Görtz.

Algebra, WS 2021/22, 3.1.1–3.1.3 und Anfang von 3.1.4; *Lineare Algebra II*, SS 2021, 18.4. Zeitgenössischer deutscher arithmetischer und algebraischer Sprachgebrauch.
`https://math.ug/a-ws2122/sect0006.html`
`https://math.ug/la2-ss21/sec-quotient-ring.html`

Nikolay Moshchevitin.

Eine Bemerkung über positiv definite quadratische Formen und rationale Punkte, arXiv:1510.06214v3. Verwandte zeitgenössische deutsche Terminologie quadratischer Formen.
`https://arxiv.org/abs/1510.06214v3`

CARL FRIEDRICH GAUSS WERKE

BAND I.

CARL FRIEDRICH GAUSS

WERKE

ERSTER BAND



HERAUSGEGEBEN

VON DER

KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN

ZU

GÖTTINGEN

1863.

UNTERSUCHUNGEN ÜBER HÖHERE ARITHMETIK

VON

D. CARL FRIEDRICH GAUSS.

LEIPZIG

IN KOMMISSION BEI GERH. FLEISCHER JUN.

1801.

DEM DURCHLAUCHTIGSTEN
FÜRSTEN UND HERRN
KARL WILHELM FERDINAND
HERZOG VON BRAUNSCHWEIG UND LÜNEBURG.

DURCHLAUCHTIGSTER FÜRST

Ich schätze mich sehr glücklich, dass Ihr mir erlaubt, dieses Werk Eurem erhabenen Namen zu widmen; eine heilige Pflicht der Dankbarkeit verbindet mich, es Euch darzubringen. Hätte mir nicht Eure Gunst, durchlauchtigster Fürst, zuerst den Zugang zu den Wissenschaften eröffnet, hätten nicht Eure beständigen Wohltaten meine Studien immer unterstützt, so hätte ich mich nicht ganz der Mathematik widmen können, zu der mich stets eine leidenschaftliche Liebe gezogen hat. Ja, dass ich gerade die Untersuchungen beginnen, über mehrere Jahre fortsetzen und niederschreiben konnte, von denen dieser Band einen Teil enthält, hat allein Eure Güte ermöglicht: Sie befreite mich von anderen Sorgen, sodass ich mich vor allem dieser Arbeit widmen konnte. Als ich sie schließlich veröffentlichen wollte, beseitigte Eure Freigebigkeit alle Hindernisse, die den Druck verzögerten. Diese großen Verdienste, die Ihr Euch um mich und meine Bemühungen erworben habt, kann ich eher mit dankbarem Herzen und stiller Bewunderung bedenken, als sie mit gerechtem und würdigem Lob feiern. Denn ich fühle mich nicht nur einer solchen Aufgabe nicht gewachsen, sondern glaube auch, dass jeder weiß, wie gewohnt Ihr seid, allen, die zur Pflege der besten Wissenschaften beizutragen scheinen, eine so außergewöhnliche Freigebigkeit zu erweisen. Auch die Wissenschaften, die man gewöhnlich für schwerer zugänglich und vom Nutzen des täglichen Lebens weiter entfernt hält, sind von Eurem Schutz nicht ausgeschlossen: Ihr selbst habt mit jenem weisen Geist, der alles so gut kennt, was zum Wohlergehen der menschlichen Gesellschaft beiträgt, den inneren und notwendigen Zusammenhang aller Wissenschaften vollständig erkannt. Wenn Ihr, durchlauchtigster Fürst, dieses Buch, das sowohl von meiner tiefen Dankbarkeit gegen Euch als auch von meiner einer höchst edlen Wissenschaft gewidmeten Arbeit zeugt, jener besonderen Gunst nicht unwürdig findet, mit der Ihr mich so lange begleitet habt, werde ich mich glücklich schätzen, meine Mühe nicht vergebens aufgewandt und die Ehre erlangt zu haben, die ich mir vor allen anderen gewünscht habe

DURCHLAUCHTIGSTER FÜRST

Braunschweig, im Juli 1801.

Eurer Durchlaucht ergebenster Diener
C. F. Gauss.

VORREDE:

Die Untersuchungen in diesem Werk gehören zu dem Teil der Mathematik, der sich mit ganzen Zahlen beschäftigt; Brüche bleiben dabei meist, irrationale Größen immer ausgeschlossen. Die sogenannte unbestimmte oder diophantische Analysis, die lehrt, aus den unendlich vielen Lösungen einer unbestimmten Aufgabe diejenigen auszuwählen, die sich durch ganze oder wenigstens rationale Zahlen ausdrücken lassen (meist mit der zusätzlichen Bedingung, dass sie positiv sind), ist nicht diese Wissenschaft selbst, sondern ein sehr besonderer Teil von ihr. Sie steht zu ihr etwa im selben Verhältnis wie die Kunst, Gleichungen umzuformen und zu lösen (Algebra), zur gesamten Analysis. Wie nämlich alle Untersuchungen über die allgemeinen Eigenschaften von Größen zur *Analysis* gehören, so bilden die ganzen Zahlen (und die Brüche, soweit sie durch ganze Zahlen bestimmt werden) den eigentlichen Gegenstand der Arithmetik. Was man aber gewöhnlich unter dem Namen Arithmetik lehrt, geht kaum über die Kunst, Zahlen darzustellen und zu rechnen, hinaus (also Zahlen durch geeignete Zeichen, etwa im Dezimalsystem, darzustellen und die arithmetischen Operationen auszuführen). Hinzu kommen einige Dinge, die entweder gar nicht zur Arithmetik gehören (wie die Lehre von den Logarithmen), oder wenigstens nicht den ganzen Zahlen eigentümlich sind, sondern für alle Größen gelten. Daher scheint es zweckmäßig, zwei Teile der Arithmetik zu unterscheiden: jene Dinge der elementaren Arithmetik zuzuordnen und alle allgemeinen Untersuchungen über die besonderen Eigenschaften ganzer Zahlen der *höheren Arithmetik* vorzubehalten, von der allein hier die Rede sein wird.

Zur höheren Arithmetik gehört, was Euklid im VII. und den folgenden Büchern der Elemente mit der bei den Alten üblichen Eleganz und Strenge dargestellt hat; allerdings beschränkt es sich auf die ersten Anfänge dieser Wissenschaft. Das berühmte Werk des Diophant, das ganz den unbestimmten Aufgaben gewidmet ist, enthält viele Fragen, deren Schwierigkeit und feine Kunstgriffe große Achtung vor dem Einfallsreichtum und Scharfsinn des Verfassers wecken, besonders wenn man bedenkt, wie gering die Hilfsmittel waren, die ihm zur Verfügung standen. Diese Aufgaben verlangen aber eher Geschick und gewandte Behandlung als tiefere Grundsätze; außerdem sind sie zu speziell und führen selten zu allgemeineren Schlüssen. Daher scheint dieses Buch eher deshalb einen Wendepunkt in der Geschichte der Mathematik zu bilden, weil es die ersten Spuren einer Zeichensprache und der Algebra zeigt, als weil es die höhere Arithmetik um neue Entdeckungen bereichert hätte. Bei weitem das meiste verdanken wir den Neueren. Unter ihnen haben wenige, aber unsterblich ruhmreiche Männer—P. de Fermat, L. Euler, L. La Grange, A. M. Le Gendre (um einige andere zu übergehen)—den Zugang zum innersten Heiligtum dieser göttlichen Wissenschaft geöffnet und gezeigt, welche reichen Schätze es birgt. Welche Entdeckungen von jedem dieser Mathematiker stammen, will ich hier nicht aufzählen. Man kann dies den Vorreden zu den Zusätzen entnehmen, mit denen der ausgezeichnete La Grange Eulers Algebra bereichert hat, und zu dem kürzlich veröffentlichten Werk des ausgezeichneten Le Gendre, das gleich noch zu nennen ist. Die meisten werden außerdem an den entsprechenden Stellen dieser arithmetischen Untersuchungen angeführt.

Der Zweck dieses Werkes, dessen Veröffentlichung ich schon vor fünf Jahren öffentlich zugesagt hatte, war, Untersuchungen aus der höheren Arithmetik bekannt zu machen, die ich zum Teil vor dieser Zeit, zum Teil danach angestellt habe. Damit niemand sich wundert, dass die Wissenschaft hier beinahe von ihren ersten Anfängen an behandelt wird und viele Untersuchungen wieder aufgenommen werden, mit denen sich andere schon beschäftigt haben, hielt ich folgende Bemerkung für nötig: Als ich mich zu Beginn des Jahres 1795 erstmals dieser Art von Untersuchungen zuwandte, wusste ich nichts von dem, was die Neueren auf diesem Gebiet geleistet hatten, und hatte auch keine Hilfsmittel, durch die ich davon hätte erfahren können. Während einer anderen Arbeit stieß ich zufällig auf eine bemerkenswerte arithmetische Wahrheit (wenn ich mich nicht irre, war es der Satz des Artikels 108). Weil ich sie schon für sich genommen sehr schön fand und vermutete, dass sie mit Größerem zusammenhing, bemühte ich mich mit aller Kraft, ihre Grundlagen zu erkennen und einen strengen Beweis zu finden. Als mir das endlich wie gewünscht gelungen war, hatten mich diese Fragen so sehr gefesselt, dass ich sie nicht mehr verlassen konnte. Da eines immer zum anderen führte, war das meiste von dem, was in den ersten vier Abschnitten dieses Werkes steht, bereits ausgearbeitet, bevor ich irgendetwas von den ähnlichen Arbeiten anderer Mathematiker gesehen hatte. Als ich später Gelegenheit bekam, die Schriften dieser großen Geister zu lesen, erkannte ich, dass ich den größten Teil meiner Überlegungen längst erledigten Fragen gewidmet hatte. Doch umso eifriger versuchte ich, ihren Spuren folgend die Arithmetik weiterzuentwickeln; so entstanden verschiedene Untersuchungen, von denen die Abschnitte V, VI und VII einen Teil enthalten. Als ich nach einiger Zeit beschloss, die Früchte meiner nächtlichen Arbeit zu veröffentlichen, ließ ich mich—umso lieber, weil mehrere es wünschten—dazu bewegen, auch von den früheren Untersuchungen nichts zurückzuhalten. Damals gab es kein Buch, aus dem man die Arbeiten anderer Mathematiker über diese Dinge hätte kennenlernen können, die in den Abhandlungen der Akademien verstreut waren; viele meiner Untersuchungen waren ganz neu und die meisten mit neuen Methoden behandelt; schließlich hingen alle sowohl untereinander als auch mit den späteren Untersuchungen so *eng* zusammen, dass auch das Neue ohne eine Wiederaufnahme des Übrigen von Anfang an nicht hinreichend bequem hätte erklärt werden können.

Inzwischen erschien ein ausgezeichnetes Werk eines Mannes, der sich schon zuvor um die höhere Arithmetik sehr verdient gemacht hatte: *Le Gendre, Essai d'une théorie des nombres, Paris, Jahr VI.* Darin hat er nicht nur alles bisher in dieser Wissenschaft Geleistete sorgfältig gesammelt und geordnet, sondern auch sehr vieles Neue aus eigener Arbeit hinzugefügt. Dieses Buch kam erst spät in meine Hände, nachdem der größte Teil meines Werkes schon gedruckt war; daher konnte ich es nicht überall dort erwähnen, wo die Ähnlichkeit der Gegenstände dazu Anlass gegeben hätte. Nur zu wenigen Stellen schien es nötig, in den Zusätzen einige Bemerkungen anzufügen, die dieser überaus höfliche und aufrichtige Mann, wie ich hoffe, freundlich aufnehmen wird.

Während des Drucks dieses Werkes, der mehrfach unterbrochen und durch verschiedene Hindernisse bis in ein viertes Jahr verzögert wurde, habe ich nicht nur schon begonnene Untersuchungen weitergeführt, deren Veröffentlichung ich auf später verschoben hatte, damit das Buch nicht zu umfangreich werde, sondern auch

mehrere neue begonnen. Auch mehrere andere, die ich aus demselben Grund nur kurz berührt hatte, weil eine ausführlichere Behandlung weniger nötig schien (zum Beispiel die in den Artikeln 37, 82 und den folgenden sowie an anderen Stellen), wurden später wieder aufgenommen und führten zu allgemeineren Untersuchungen, die mir einer Veröffentlichung sehr wert erscheinen (man vergleiche auch die Bemerkungen in den Zusätzen zu Artikel 306). Da das Buch schließlich, besonders durch die Länge des Abschnitts V, weit umfangreicher wurde als erwartet, musste ich manches ursprünglich dafür Bestimmte streichen, darunter den ganzen *achten* Abschnitt (der an verschiedenen Stellen dieses Bandes bereits erwähnt wird und eine allgemeine Behandlung algebraischer Kongruenzen beliebigen Grades enthält). All dies wird leicht einen ebenso großen Band füllen wie den vorliegenden und veröffentlicht werden, sobald sich eine Gelegenheit bietet.

Dass ich bei mehreren schwierigen Fragen synthetische Beweise verwendet und die Analysis, durch die sie gefunden wurden, weggelassen habe, liegt vor allem am Streben nach Kürze, auf die ich so weit wie möglich Rücksicht nehmen musste.

Die in Abschnitt VII behandelte Theorie der Kreisteilung oder der regelmäßigen Vielecke gehört zwar *selbst*, *für sich genommen*, nicht zur Arithmetik; ihre *Grundlagen* müssen aber allein aus der höheren Arithmetik gewonnen werden. Das wird den Mathematikern vielleicht ebenso unerwartet sein, wie ihnen, so hoffe ich, die neuen Wahrheiten willkommen sein werden, die sich aus dieser Quelle gewinnen ließen.

Dies wollte ich dem Leser vorweg erklären. Über die Sache selbst zu urteilen, steht mir nicht zu. Nichts wünsche ich mir mehr, als dass das, was bisherige Lücken füllt oder den Zugang zu Neuem öffnet, denen gefällt, denen der Fortschritt der Wissenschaften am Herzen liegt.

UNTERSUCHUNGEN ÜBER HÖHERE ARITHMETIK.

ERSTER ABSCHNITT
ÜBER
DIE KONGRUENZ VON ZAHLEN IM ALLGEMEINEN.

Kongruente Zahlen, Moduln, Reste und Nichtreste.

1.

Wenn die Zahl a die Differenz der Zahlen b, c teilt, heißen b und c *kongruent nach* a, andernfalls *inkongruent*: a selbst nennen wir den *Modul*. Im ersten Fall heißt jede der Zahlen b, c ein *Rest* der anderen, im zweiten Fall ein *Nichtrest*.

Diese Begriffe gelten für alle ganzen Zahlen, sowohl positive als auch negative[*)], sollen aber nicht auf Brüche ausgedehnt werden. *Zum Beispiel* sind -9 und $+16$ nach dem Modul 5 kongruent; -7 ist ein Rest von $+15$ nach dem Modul 11, nach dem Modul 3 dagegen ein Nichtrest. Da außerdem jede Zahl die Null teilt, ist jede Zahl nach jedem Modul als zu sich selbst kongruent anzusehen.

2.

Alle Reste einer gegebenen Zahl a nach dem Modul m sind in der Formel $a + km$ enthalten, wobei k eine unbestimmte ganze Zahl bezeichnet. Die einfacheren Sätze, die wir später angeben werden, lassen sich daraus ohne Mühe beweisen; ihre Richtigkeit kann aber jeder ebenso leicht unmittelbar erkennen.

Von nun an werden wir die Kongruenz von Zahlen durch das Zeichen $\equiv$ bezeichnen und, wo es nötig ist, den Modul in Klammern hinzufügen, $-16 \equiv 9 \pmod 5$. $-7 \equiv 15 \pmod{11}$[*)].

3.

Satz. *Sind m aufeinanderfolgende ganze Zahlen*

$$a,\ a+1,\ a+2\ \ldots.\ a+m-1$$

und eine weitere ganze Zahl A gegeben, so ist genau eine der ersteren nach dem Modul m zu dieser kongruent.

Ist nämlich $\frac{a-A}{m}$ ganzzahlig, so ist $a \equiv A$; ist es ein Bruch, so sei die nächstgrößere ganze Zahl (oder, wenn er negativ ist, die nächst*kleinere*, wenn man vom Vorzeichen absieht) $= k$. Dann liegt $A + km$ zwischen a und $a + m$ und ist also die gesuchte Zahl. Alle Quotienten $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$ usw. liegen offensichtlich zwischen $k-1$ und $k+1$; daher kann nicht mehr als einer von ihnen ganzzahlig sein.

[*)] Der Modul ist immer *absolut*, also ohne Vorzeichen, zu nehmen.

[*)] Wir haben dieses Zeichen wegen der engen Analogie zwischen Gleichheit und Kongruenz gewählt. Aus demselben Grund hat der ausgezeichnete Le Gendre in der Abhandlung, die wir weiter unten öfter anführen werden, für die Kongruenz das Gleichheitszeichen selbst beibehalten; wir haben gezögert, ihm darin zu folgen, um Mehrdeutigkeiten zu vermeiden.

Kleinste Reste.

4.

Jede Zahl hat also sowohl in der Reihe $0, 1, 2, \ldots m-1$ als auch in der Reihe $0, -1, -2, \ldots . -(m-1)$ einen Rest; diese nennen wir *kleinste Reste*. Ist nicht 0 ein Rest, so gibt es offensichtlich immer zwei, einen *positiven* und einen *negativen*. Sind sie dem Betrag nach verschieden, so ist einer $< \frac{m}{2}$; andernfalls sind beide $= \frac{m}{2}$, wenn man vom Vorzeichen absieht. Daher hat jede Zahl einen Rest, der die Hälfte des Moduls nicht übersteigt; dieser heißt *absolut kleinster Rest*.

Zum Beispiel hat -13 nach dem Modul 5 den kleinsten positiven Rest 2, der zugleich der absolut kleinste ist, und den kleinsten negativen Rest -3; $+5$ ist nach dem Modul 7 sein eigener kleinster positiver Rest, während -2 der kleinste negative und zugleich der absolut kleinste Rest ist.

Elementare Sätze über Kongruenzen.

5.

Nachdem diese Begriffe feststehen, wollen wir die Eigenschaften kongruenter Zahlen zusammenstellen, die sich unmittelbar zeigen.

Zahlen, die nach einem zusammengesetzten Modul kongruent sind, sind auch nach jedem seiner Teiler kongruent.

Sind mehrere Zahlen nach demselben Modul zu derselben Zahl kongruent, so sind sie auch untereinander kongruent (nach demselben Modul).

Auch im Folgenden ist stillschweigend vorausgesetzt, dass der Modul derselbe ist.

Kongruente Zahlen haben dieselben kleinsten Reste, inkongruente verschiedene.

6.

Sind beliebig viele ganze Zahlen A, B, C usw. und ebenso viele andere a, b, c usw. gegeben, die ihnen nach irgendeinem Modul kongruent sind,

$$A \equiv a,\ B \equiv b \text{ etc.}, \quad \text{gilt} \quad A + B + C + \text{etc.} \equiv a + b + c + \text{etc.}$$

Ist $A \equiv a, B \equiv b$, so ist $A - B \equiv a - b$.

7.

Ist $A \equiv a$, so ist auch $kA \equiv ka$.

Ist k eine positive Zahl, so ist dies nur ein besonderer Fall des Satzes im vorigen Artikel, wenn man dort $A = B = C$ usw., $a = b = c$ usw. setzt. Ist k negativ, so ist $-k$ positiv, also $-kA \equiv -ka$, und daraus folgt $kA \equiv ka$.

Ist $A \equiv a, B \equiv b$, so ist $AB \equiv ab$. Denn $AB \equiv Ab \equiv ba$.

8.

Sind beliebig viele ganze Zahlen A, B, C usw. und ebenso viele ihnen kongruente Zahlen a, b, c usw. gegeben, $A \equiv a, B \equiv b$ usw., so sind die Produkte beider Gruppen kongruent, ABC etc. $\equiv abc$ etc.

Nach dem vorigen Artikel ist $AB \equiv ab$ und aus demselben Grund $ABC \equiv abc$; auf dieselbe Weise können beliebig viele weitere Faktoren hinzukommen.

Nimmt man alle Zahlen A, B, C usw. als gleich an und ebenso die entsprechenden Zahlen a, b, c usw., so erhält man den Satz: *Ist* $A \equiv a$ *und* k *eine positive ganze Zahl, so ist* $A^k \equiv a^k$.

9.

Sei X *eine algebraische Funktion der Unbestimmten* x *von der Form*

$$Ax^a + Bx^b + Cx^c + \text{etc.}$$

wobei A, B, C *usw. beliebige ganze Zahlen und* a, b, c *usw. nichtnegative ganze Zahlen bezeichnen. Gibt man dann der Unbestimmten* x *nach irgendeinem Modul kongruente Werte, so sind auch die daraus entstehenden Werte der Funktion* X *kongruent.*

Seien f, g kongruente Werte von x. Dann ist nach dem vorigen Artikel $f^a \equiv g^a$ und $Af^a \equiv Ag^a$, ebenso $Bf^b \equiv Bg^b$ usw. Daher

$$Af^a + Bf^b + Cf^c + \text{etc.} \equiv Ag^a + Bg^b + Cg^c + \text{etc.} \quad \textit{Q. E. D.}$$

Es ist außerdem leicht zu sehen, wie sich dieser Satz auf Funktionen mehrerer Unbestimmter ausdehnen lässt.

10.

Setzt man also für x alle aufeinanderfolgenden ganzen Zahlen ein und führt die Werte der Funktion X auf ihre kleinsten Reste zurück, so bilden diese eine Reihe, in der dieselben Glieder nach einem Abstand von m Gliedern wiederkehren (wobei m den Modul bezeichnet); die Reihe besteht also aus einer unendlich oft wiederholten *Periode* von m Gliedern. Sei zum Beispiel $\mathrm{X} = x^3 - 8x + 6$ und $m = 5$; dann ergeben für $x = 0, 1, 2, 3$ usw. die Werte von X die kleinsten positiven Reste $1, 4, 3, 4, 3, 1, 4$ usw., wobei sich die ersten fünf $1, 4, 3, 4, 3$ unbegrenzt wiederholen. Setzt man die Reihe rückwärts fort, gibt man also x negative Werte, so erscheint dieselbe Periode in umgekehrter Reihenfolge ihrer Glieder: daher können in der ganzen Reihe keine anderen Glieder vorkommen als die dieser Periode.

11.

In diesem Beispiel kann also X weder $\equiv 0$ noch $\equiv 2$ (mod. 5) werden, erst recht nicht $= 0$ oder $= 2$. Folglich lassen sich die Gleichungen $x^3 - 8x + 6 = 0$ und $x^3 - 8x + 4 = 0$ nicht durch ganze Zahlen und somit, wie bekannt, auch nicht durch rationale Zahlen lösen. Allgemein ist klar, dass die Gleichung $\mathrm{X} = 0$, wenn X eine Funktion der Unbekannten x von der Form

$$x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$$

mit ganzen Zahlen A, B, C usw. und einer positiven ganzen Zahl n ist (auf diese Form lassen sich bekanntlich alle algebraischen Gleichungen bringen), keine rationale Wurzel hat, wenn sich die Kongruenz $\mathrm{X} \equiv 0$ nach irgendeinem Modul nicht erfüllen lässt. Dieses Kriterium, das sich uns hier von selbst angeboten hat, wird in Abschnitt VIII ausführlicher behandelt. Dieses Beispiel kann gewiss zumindest eine Vorstellung vom Nutzen dieser Untersuchungen geben.

Einige Anwendungen.

12.

Auf den Sätzen dieses Kapitels beruhen mehrere Regeln, die man gewöhnlich in der Arithmetik lehrt, zum Beispiel die Regeln, mit denen man prüft, ob eine gegebene Zahl durch 9, 11 oder andere Zahlen teilbar ist. *Nach dem Modul* 9 sind alle Potenzen der Zahl 10 zu eins kongruent: hat also die gegebene Zahl die Form $a+10b+100c+$etc., so liefert sie nach dem Modul 9 denselben kleinsten Rest wie $a+b+c+$etc. Addiert man also die einzelnen Ziffern einer in Dezimalschreibweise dargestellten Zahl unabhängig von ihrer Stelle, so liefern diese Summe und die gegebene Zahl dieselben kleinsten Reste. Die gegebene Zahl ist daher genau dann durch 9 teilbar, wenn die Summe durch 9 teilbar ist. Dasselbe gilt für den Teiler 3. Da *nach dem Modul* 11 $100 \equiv 1$ ist, gilt allgemein $10^{2k} \equiv 1$. $10^{2k+1} \equiv 10 \equiv -1$, und eine Zahl von der Form $a+10b+100c+$etc. liefert nach dem Modul 11 denselben kleinsten Rest wie $a - b + c$ usw.; daraus folgt sofort die bekannte Regel. Alle ähnlichen Regeln lassen sich aus demselben Grundsatz leicht ableiten.

Die vorigen Ergebnisse erklären ebenso die gewöhnlich empfohlenen Regeln zur Prüfung arithmetischer Rechnungen. Sollen nämlich aus gegebenen Zahlen durch Addition, Subtraktion, Multiplikation oder Potenzieren andere Zahlen abgeleitet werden, so ersetzt man die gegebenen Zahlen durch ihre kleinsten Reste nach einem beliebigen Modul (gewöhnlich 9 oder 11, weil sich die Reste nach diesen Moduln, wie wir eben gezeigt haben, in unserem Dezimalsystem so leicht finden lassen). Die so entstehenden Zahlen müssen zu den aus den gegebenen Zahlen abgeleiteten kongruent sein; trifft dies nicht zu, so hat sich ein Fehler in die Rechnung eingeschlichen.

Da diese und ähnliche Dinge aber hinreichend bekannt sind, wäre es überflüssig, länger dabei zu bleiben.

ZWEITER ABSCHNITT

ÜBER

KONGRUENZEN ERSTEN GRADES.

Vorbereitende Sätze über Primzahlen, Faktoren usw.

13.

Satz. *Das Produkt zweier positiver Zahlen, die kleiner als eine gegebene Primzahl sind, kann nicht durch diese Primzahl geteilt werden.*

Sei p eine Primzahl und a positiv und $< p$: Dann gibt es keine positive Zahl b, die kleiner als p ist, sodass $ab \equiv 0 \pmod{p}$ ist.

Beweis. Wenn jemand dies bestreitet, nehmen wir an, es gebe Zahlen b, c, d usw., alle $< p$, für die $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$ usw. (mod. p) ist. Sei b die kleinste von allen, sodass keine Zahl, die kleiner als b ist, diese Eigenschaft hat. Offensichtlich ist $b > 1$: Wäre nämlich $b = 1$, so wäre $ab = a < p$ (*nach Voraussetzung*) und damit nicht durch p teilbar. Da p eine Primzahl ist, kann es also nicht durch b geteilt werden, sondern liegt zwischen den beiden benachbarten Vielfachen von b, mb und $(m+1)b$. Sei $p - mb = b'$; dann ist b' eine positive Zahl und $< b$. Da wir nun $ab \equiv 0 \pmod{p}$ vorausgesetzt haben, gilt auch $mab \equiv 0$ (Art. 7); zieht man dies von $ap \equiv 0$ ab, so erhält man $a(p - mb) = ab' \equiv 0$. Also muss b' zu den Zahlen b, c, d usw. gehören, obwohl es kleiner als ihre kleinste, b, ist. *Q. E. A.*

14.

Kann weder a noch b durch die Primzahl p geteilt werden, so kann auch das Produkt ab nicht durch p geteilt werden.

Seien die kleinsten positiven Reste der Zahlen a, b nach dem Modul p mit α, β bezeichnet; keiner von ihnen ist 0 (*nach Voraussetzung*). Wäre nun $ab \equiv 0 \pmod{p}$, so wäre wegen $ab \equiv \alpha\beta$ auch $\alpha\beta \equiv 0$, was mit dem vorigen Satz unvereinbar ist.

Einen Beweis dieses Satzes hat bereits Euklid gegeben, *El.* VII. 32. Wir wollten ihn trotzdem nicht weglassen: zum einen, weil mehrere Neuere entweder vage Überlegungen als Beweis ausgegeben oder den Satz ganz übergangen haben; zum anderen, weil sich die Art der hier verwendeten Methode, die wir später zur Klärung viel verborgenerer Dinge benutzen werden, an einem einfacheren Fall leichter verstehen lässt.

15.

Kann keine der Zahlen a, b, c, d usw. durch die Primzahl p geteilt werden, so kann auch das Produkt $abcd$ usw. nicht durch p geteilt werden.

Nach dem vorigen Artikel ist ab nicht durch p teilbar; also auch nicht abc und daher auch nicht $abcd$ usw.

16.

Satz. *Jede zusammengesetzte Zahl lässt sich nur auf eine einzige Weise in Primfaktoren zerlegen.*

Beweis. Dass sich jede zusammengesetzte Zahl in Primfaktoren zerlegen lässt, ist aus den Anfangsgründen bekannt; dass dies aber nicht auf mehrere verschiedene Weisen geschehen kann, wird meist zu Unrecht stillschweigend vorausgesetzt. Nehmen wir an, eine zusammengesetzte Zahl A, die $= a^\alpha b^\beta c^\gamma$ usw. ist, wobei a, b, c usw. verschiedene Primzahlen bezeichnen, ließe sich noch auf eine andere Weise in Primfaktoren zerlegen. Zunächst ist klar, dass in diesem zweiten System von Faktoren keine anderen Primzahlen als a, b, c usw. vorkommen können, weil keine andere Primzahl die aus diesen zusammengesetzte Zahl A teilen kann. Ebenso darf in diesem zweiten System keine der Primzahlen a, b, c usw. fehlen, da sie sonst A nicht teilen würde (voriger Art.). Die beiden Zerlegungen können sich also nur dadurch unterscheiden, dass irgendeine Primzahl in der einen öfter vorkommt als in der anderen. Sei p eine solche Primzahl, die in der einen Zerlegung m-mal und in der anderen n-mal vorkommt, und sei $m > n$: Nun werde der Faktor p aus beiden Systemen n-mal entfernt, sodass er in dem einen noch $m - n$-mal vorkommt, aus dem anderen aber ganz verschwunden ist. Es gibt also zwei Zerlegungen der Zahl $\frac{A}{p^n}$ in Faktoren, von denen die eine den Faktor p gar nicht, die andere aber $m - n$-mal enthält, entgegen dem eben Bewiesenen.

17.

Ist also eine zusammengesetzte Zahl A das Produkt von B, C, D usw., so können unter den Primfaktoren der Zahlen B, C, D usw. offensichtlich keine anderen vorkommen als unter den Faktoren von A; und jeder dieser Faktoren muss in B, C, D usw. zusammengenommen ebenso oft vorkommen wie in A. Daraus ergibt sich ein Kriterium dafür, ob eine Zahl B eine andere Zahl A teilt oder nicht. Sie tut dies, wenn B weder andere Primfaktoren noch einen von ihnen öfter als A enthält; ist eine dieser Bedingungen nicht erfüllt, so teilt B die Zahl A nicht.

Ist $A = a^\alpha b^\beta c^\gamma$ usw., wobei a, b, c usw. wie oben verschiedene Primzahlen bezeichnen, so lässt sich daraus durch Abzählen der Kombinationen leicht ableiten, dass A

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \text{ etc.}$$

verschiedene Teiler besitzt, einschließlich 1 und A.

18.

Ist also $A = a^\alpha b^\beta c^\gamma$ usw., $K = k^\kappa l^\lambda m^\mu$ usw., und sind die Primzahlen a, b, c usw., k, l, m usw. alle verschieden, so haben A und K offensichtlich außer 1 keinen gemeinsamen Teiler, sind also teilerfremd.

Sind mehrere Zahlen A, B, C usw. gegeben, so wird ihr *größter gemeinsamer Teiler* folgendermaßen bestimmt. Man zerlegt sie alle in ihre Primfaktoren und wählt darunter diejenigen aus, die allen Zahlen A, B, C usw. gemeinsam sind (gibt es solche nicht, so gibt es keinen allen gemeinsamen Teiler). Dann notiert man, wie oft jeder dieser Primfaktoren in jeder der Zahlen A, B, C usw. enthalten ist, also *welchen Exponenten* jeder in den einzelnen Zahlen A, B, C usw. hat. Schließlich gibt man jedem Primfaktor den kleinsten seiner Exponenten in A, B, C usw. und bildet daraus das Produkt; dies ist der gesuchte gemeinsame Teiler.

Sucht man dagegen das *kleinste gemeinsame Vielfache* der Zahlen A, B, C usw., so geht man folgendermaßen vor. Man sammelt alle Primzahlen, die wenigstens eine der

Zahlen A, B, C usw. teilen, gibt jeder den größten ihrer Exponenten in den Zahlen A, B, C usw. und bildet so das Produkt aus allen; dies ist das gesuchte Vielfache.

Beispiel. Sei $A = 504 = 2^3 3^2 7$; $B = 2880 = 2^6 3^2 5$; $C = 864 = 2^5 3^3$. Für den größten gemeinsamen Teiler hat man die Primfaktoren $2, 3$, denen die Exponenten $3, 2$ zu geben sind; es ergibt sich $= 2^3 3^2 = 72$; das kleinste gemeinsame Vielfache ist dagegen $2^6 3^3 5.7 = 60480$.

Wegen ihrer Einfachheit lassen wir die Beweise weg. Wie diese Aufgaben zu lösen sind, wenn die Zerlegung der Zahlen A, B, C usw. in Faktoren nicht gegeben ist, ist im Übrigen aus den Anfangsgründen bekannt.

19.

Sind die Zahlen a, b, c usw. zu einer anderen Zahl k teilerfremd, so ist auch ihr Produkt abc usw. zu k teilerfremd.

Da nämlich keine der Zahlen a, b, c usw. einen Primfaktor mit k gemeinsam hat und das Produkt abc usw. keine anderen Primfaktoren haben kann als die Faktoren einer der Zahlen a, b, c usw., hat auch das Produkt abc usw. keinen Primfaktor mit k gemeinsam. Nach dem vorigen Artikel ist also k zu abc usw. teilerfremd.

Sind die Zahlen a, b, c usw. paarweise teilerfremd und teilt jede eine andere Zahl k, so teilt auch ihr Produkt die Zahl k.

Dies folgt ebenso leicht aus den Artikeln 17, 18. Sei nämlich ein beliebiger Primteiler des Produkts abc usw. mit p bezeichnet, der darin π-mal vorkomme; offensichtlich muss eine der Zahlen a, b, c usw. denselben Teiler π-mal enthalten. Daher enthält auch k, das von dieser Zahl geteilt wird, π-mal den Teiler p. Ebenso verhält es sich mit den übrigen Teilern des Produkts abc usw.

Daher gilt: *Sind zwei Zahlen m, n nach mehreren paarweise teilerfremden Moduln a, b, c usw. kongruent, so sind sie auch nach deren Produkt kongruent.* Da nämlich $m-n$ durch jede der Zahlen a, b, c usw. teilbar ist, lässt es sich auch durch ihr Produkt teilen.

Schließlich gilt: *Ist a zu b teilerfremd und ak durch b teilbar, so ist auch ak durch b teilbar.* Denn da ak sowohl durch a als auch durch b teilbar ist, lässt es sich auch durch ab teilen; das heißt, $\frac{ak}{ab} = \frac{k}{b}$ ist ganzzahlig.

20.

Ist $A = a^\alpha b^\beta c^\gamma$ usw., wobei a, b, c usw. verschiedene Primzahlen bezeichnen, irgendeine Potenz, etwa $= k^n$, so sind alle Exponenten α, β, γ usw. durch n teilbar.

Die Zahl k enthält nämlich keine anderen Primfaktoren als a, b, c usw. Enthält sie den Faktor a genau α'-mal, so enthält k^n, also A, diesen Faktor $n\alpha'$-mal; daher ist $n\alpha' = \alpha$ und $\frac{\alpha}{n}$ ganzzahlig. Ebenso zeigt man, dass $\frac{\beta}{n}$ usw. ganzzahlig sind.

21.

Sind a, b, c usw. paarweise teilerfremd und ist ihr Produkt abc usw. eine Potenz, etwa $= k^n$, so sind auch die einzelnen Zahlen a, b, c usw. Potenzen derselben Art.

Sei $a = l^\lambda m^\mu p^\pi$ usw., wobei l, m, p usw. verschiedene Primzahlen bezeichnen. Nach *Voraussetzung* ist keine davon ein Faktor von b, c usw. Das Produkt abc usw. enthält also den Faktor l λ-mal, den Faktor m μ-mal usw. Nach dem *vorigen Artikel* sind daher λ, μ, π usw. durch n teilbar, und somit ist

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}} \text{ usw.}$$

eine ganze Zahl. Dasselbe gilt für die übrigen Zahlen b, c usw.

Diese Tatsachen über Primzahlen mussten vorausgeschickt werden; nun wenden wir uns den Dingen zu, die unmittelbarer mit unserem Ziel zusammenhängen.

22.

Sind die Zahlen a, b, die beide durch eine Zahl k teilbar sind, nach einem Modul m, der zu k teilerfremd ist, kongruent, so sind auch $\frac{a}{k}$ und $\frac{b}{k}$ nach demselben Modul kongruent.

Denn $a - b$ ist offenbar durch k und ebenso durch m teilbar (*nach Voraussetzung*). Nach *Artikel 19* ist also $\frac{a-b}{k}$ durch m teilbar, das heißt $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$.

Haben dagegen m und k bei sonst gleichen Voraussetzungen den größten gemeinsamen Teiler e, so ist $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$. Denn $\frac{k}{e}$ und $\frac{m}{e}$ sind teilerfremd. Nun ist $a - b$ sowohl durch k als auch durch m teilbar, also auch $\frac{a-b}{e}$ sowohl durch $\frac{k}{e}$ als auch durch $\frac{m}{e}$ und damit durch $\frac{km}{ee}$. Das heißt, $\frac{a-b}{k}$ ist durch $\frac{m}{e}$ teilbar, oder $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$.

23.

Ist a zu m teilerfremd und sind e, f nach dem Modul m inkongruent, so sind auch ae, af nach m inkongruent.

Dies ist lediglich die Umkehrung des Satzes im vorigen Artikel.

Daraus folgt: Multipliziert man a mit allen ganzen Zahlen von 0 bis $m - 1$ und führt die Produkte auf ihre kleinsten Reste nach dem Modul m zurück, so sind diese Reste alle verschieden. Keiner dieser Reste ist $> m$, und ihre Anzahl beträgt m; ebenso viele Zahlen gibt es von 0 bis $m - 1$. Daher kann keine dieser Zahlen unter den Resten fehlen.

24.

Der Ausdruck $ax + b$, in dem a, b gegebene Zahlen und x eine unbestimmte oder veränderliche Zahl bezeichnen, kann nach einem Modul m, der zu a teilerfremd ist, jeder gegebenen Zahl kongruent gemacht werden.

Sei c die Zahl, zu der der Ausdruck kongruent sein soll, und sei der kleinste positive Rest von $c - b$ nach dem Modul m gleich e. Nach dem vorigen Artikel gibt es notwendig einen Wert von $x < m$, für den der kleinste Rest des Produkts ax nach dem Modul m gleich e wird. Sei v dieser Wert. Dann ist $av \equiv e \equiv c - b$, also $av + b \equiv c \pmod{m}$. *Q. E. F.*

25.

Einen Ausdruck, der zwei Größen als kongruent angibt, nennen wir in Anlehnung

an Gleichungen eine *Kongruenz*. Enthält er eine Unbekannte, so heißt die Kongruenz *gelöst*, wenn ein Wert der Unbekannten gefunden ist, der die Kongruenz erfüllt (eine *Wurzel*). Damit ist auch klar, was eine *lösbare Kongruenz und eine unlösbare Kongruenz* ist. Schließlich sieht man leicht, dass hier ähnliche Unterscheidungen wie bei Gleichungen möglich sind. Beispiele *transzendenter* Kongruenzen werden später vorkommen. *Algebraische* Kongruenzen werden nach dem höchsten Exponenten der Unbekannten in solche ersten, zweiten und höheren *Grades* eingeteilt. Ebenso können mehrere Kongruenzen mit mehreren Unbekannten vorliegen, deren *Elimination* zu untersuchen ist.

Lösung der Kongruenzen ersten Grades.

26.

Nach Artikel 24 ist also die Kongruenz ersten Grades $ax + b \equiv c$ stets lösbar, wenn der Modul zu a teilerfremd ist. Ist v ein geeigneter Wert von x, also eine Wurzel der Kongruenz, so sind offenbar auch alle Zahlen Wurzeln, die zu v nach dem Modul der gegebenen Kongruenz kongruent sind (Artikel 9). Ebenso leicht sieht man, dass alle Wurzeln zu v kongruent sein müssen: Ist t eine weitere Wurzel, so ist $av + b \equiv at + b$, also $av \equiv at$ und damit $v \equiv t$ (Artikel 22). Folglich gibt die Kongruenz $x \equiv v \pmod{m}$ die vollständige Lösung der Kongruenz $ax + b \equiv c$ an.

Da Lösungen einer Kongruenz durch kongruente Werte von x unmittelbar auf der Hand liegen und kongruente Zahlen in dieser Hinsicht als gleichwertig anzusehen sind, zählen wir solche Lösungen als ein und dieselbe. Da nun unsere Kongruenz $ax + b \equiv c$ keine anderen Lösungen zulässt, sagen wir, sie sei nur auf eine Weise lösbar oder habe nur eine Wurzel. *Zum Beispiel* lässt die Kongruenz $6x + 5 \equiv 13 \pmod{11}$ nur solche Wurzeln zu, die $\equiv 5 \pmod{11}$ sind. Bei Kongruenzen höheren Grades ist dies anders, ebenso bei Kongruenzen ersten Grades, wenn die Unbekannte mit einer Zahl multipliziert wird, zu der der Modul nicht teilerfremd ist.

27.

Es bleibt noch etwas darüber zu sagen, wie man die Lösung einer solchen Kongruenz findet. Zunächst hängt eine Kongruenz der Form $ax + t \equiv u$, deren Modul wir als teilerfremd zu a voraussetzen, von der Kongruenz $ax \equiv \pm 1$ ab: Erfüllt $x \equiv r$ die letztere, so erfüllt $x \equiv \pm(u - t)r$ die erstere. Die Kongruenz $ax \equiv \pm 1$, deren Modul wir mit b bezeichnen, ist gleichwertig mit der unbestimmten Gleichung $ax = by \pm 1$. Wie man diese löst, ist inzwischen gut bekannt; daher genügt es, hier den Rechenalgorithmus anzugeben.

Hängen die Größen A, B, C, D, E usw. von $\alpha, \beta, \gamma, \delta$ usw. durch die Beziehungen

$$A = \alpha, \quad B = \beta A + 1, \quad C = \gamma B + A, \quad D = \delta C + B, \quad E = \varepsilon D + C \text{ usw.}$$

ab, so bezeichnen wir sie der Kürze halber folgendermaßen:

$$A = [\alpha], \quad B = [\alpha, \beta], \quad C = [\alpha, \beta, \gamma], \quad D = [\alpha, \beta, \gamma, \delta] \text{ usw.}^{*)}.$$

Gegeben sei nun die unbestimmte Gleichung $ax = by \pm 1$, in der a, b positiv sind. Wir dürfen annehmen, dass a nicht $< b$ ist. Nach dem bekannten Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen bilden wir durch gewöhnliche Division die Gleichungen

$$a = \alpha b + c, \quad b = \beta c + d, \quad c = \gamma d + e \text{ usw.}$$

Dabei sind α, β, γ usw. sowie c, d, e usw. positive ganze Zahlen, und b, c, d, e nehmen fortlaufend ab, bis wir zu $m = \mu n + 1$ gelangen, was bekanntlich schließlich eintreten muss. Es ist also

$$a = [n, \mu, \ldots . \gamma, \beta, \alpha], \quad b = [n, \mu \ldots . \gamma, \beta]$$

Setzen wir nun

$$x = [\mu, \ldots . \gamma, \beta], \quad y = [\mu, \ldots . \gamma, \beta, \alpha]$$

so ist $ax = by + 1$, wenn die Anzahl der Zahlen $\alpha, \beta, \gamma \ldots . \mu, n$ gerade ist, und $ax = by - 1$, wenn sie ungerade ist. *Q. E. F.*

28.

Der berühmte Euler gab zuerst die allgemeine Lösung solcher unbestimmten Gleichungen an, in *Comment. Petrop. T.* VII, *S.* 46. Seine Methode besteht darin, andere

*)Diese Beziehung lässt sich viel allgemeiner betrachten; vielleicht werden wir dies bei einer anderen Gelegenheit aufgreifen. Hier fügen wir nur zwei Sätze hinzu, die bei der vorliegenden Untersuchung nützlich sind:

$$1^{\text{o}}. \quad [\alpha, \beta, \gamma \ldots . \lambda, \mu].[\beta, \gamma \ldots . \lambda] - [\alpha, \beta, \gamma \ldots \lambda][\beta, \gamma \ldots \lambda, \mu] = \pm 1,$$

Dabei ist das obere Zeichen zu nehmen, wenn die Anzahl der Zahlen $\alpha, \beta, \gamma \ldots \lambda, \mu$ gerade ist, das untere, wenn sie ungerade ist.

2°. Die Reihenfolge der Zahlen α, β, γ usw. kann umgekehrt werden:

$$[\alpha, \beta, \gamma \ldots \lambda, \mu] = [\mu, \lambda \ldots . \gamma, \beta, \alpha].$$

Die Beweise, die nicht schwierig sind, lassen wir hier weg.

Unbekannte an die Stelle von x, y zu setzen, und ist inzwischen gut bekannt. Der berühmte La Grange ging etwas anders vor. Aus der Theorie der Kettenbrüche folgt nämlich: Verwandelt man den Bruch $\frac{b}{a}$ in den Kettenbruch

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{usw.} + \cfrac{1}{\mu + \frac{x}{n}}}}}$$

und wandelt diesen nach Weglassen seines letzten Teils $\frac{x}{n}$ wieder in einen gewöhnlichen Bruch $\frac{x}{y}$ um, so ist $ax = by \pm 1$, sofern a zu b teilerfremd ist. Beide Methoden führen zum selben Algorithmus. La Granges Untersuchungen finden sich in *Hist. de l'Ac. de Berlin Année* 1767, *S.* 175, und zusammen mit weiteren Untersuchungen in den *Zusätzen zur französischen Übersetzung von Eulers Algebra.*

29.

Die Kongruenz $ax + t \equiv u$, deren Modul nicht zu a teilerfremd ist, lässt sich leicht auf den vorigen Fall zurückführen. Sei m der Modul und der größte gemeinsame Teiler von a, m gleich δ. Zunächst erfüllt offenbar jeder Wert von x, der die Kongruenz nach dem Modul m erfüllt, sie auch nach dem Modul δ (Artikel 5). Es ist aber stets $ax \equiv 0 \pmod{\delta}$, da δ ein Teiler von a ist. Die gegebene Kongruenz ist daher unlösbar, wenn nicht $t \equiv u \pmod{\delta}$, das heißt, wenn $t - u$ nicht durch δ teilbar ist.

Setzen wir also $a = \delta e$, $m = \delta f$, $t - u = \delta k$, so ist e zu f teilerfremd. Dann ist die gegebene Kongruenz $\delta ex + \delta k \equiv 0 \pmod{\delta f}$ gleichwertig mit $ex + k \equiv 0 \pmod{f}$. Das heißt, jeder Wert von x, der die letztere erfüllt, erfüllt auch die erstere, und umgekehrt. Denn $ex + k$ ist offenbar durch f teilbar, wenn $\delta ex + \delta k$ durch δf teilbar ist, und umgekehrt. Wie man die Kongruenz $ex + k \equiv 0 \pmod{f}$ löst, haben wir oben gezeigt. Daraus folgt zugleich: Ist v einer der Werte von x, so gibt $x \equiv v \pmod{f}$ die vollständige Lösung der gegebenen Kongruenz an.

30.

Bei einem zusammengesetzten Modul ist manchmal die folgende Methode vorzuziehen.

Der Modul sei $= mn$ und die gegebene Kongruenz $ax \equiv b$. Man löse diese zunächst nach dem Modul m und nehme an, dass sie für $x \equiv v \pmod{\frac{m}{\delta}}$ erfüllt ist, wobei δ den größten gemeinsamen Teiler von m, a bezeichnet. Jeder Wert von x, der die Kongruenz $ax \equiv b$ nach dem Modul mn erfüllt, erfüllt sie offenbar auch nach dem Modul m und hat daher die Form $v + \frac{m}{\delta}x'$, wobei x' eine unbestimmte Zahl bezeichnet. Umgekehrt erfüllen aber nicht alle Zahlen der Form $v + \frac{m}{\delta}x'$ die Kongruenz nach dem Modul mn. Wie x' zu bestimmen ist, damit $v + \frac{m}{\delta}x'$ eine Wurzel der Kongruenz $ax \equiv b \pmod{mn}$ wird, ergibt sich aus der Lösung der Kongruenz $\frac{am}{\delta}x' + av \equiv b \pmod{mn}$, die mit $\frac{a}{\delta}x' \equiv \frac{b-av}{m} \pmod{n}$ gleichwertig ist. Somit lässt sich die Lösung jeder Kongruenz ersten Grades nach dem Modul mn auf die Lösung zweier Kongruenzen nach den Moduln m und n zurückführen. Ist n wiederum ein Produkt zweier Faktoren, so hängt die Lösung der Kongruenz nach dem Modul n ebenso von der Lösung zweier Kongruenzen ab, deren Moduln diese Faktoren sind. Allgemein hängt die Lösung einer Kongruenz nach einem beliebigen zusammengesetzten Modul von der Lösung anderer Kongruenzen ab, deren Moduln Faktoren dieser Zahl sind. Diese können, wenn es zweckmäßig erscheint, stets als Primzahlen gewählt werden.

Beispiel. Gegeben sei die Kongruenz $19x \equiv 1 \pmod{140}$. Man löse sie zunächst nach dem Modul 2 und erhält $x \equiv 1 \pmod{2}$. Setzt man $x = 1 + 2x'$, so wird $38x' \equiv -18 \pmod{140}$, womit $19x' \equiv -9 \pmod{70}$ gleichwertig ist. Löst man diese wiederum nach dem Modul 2, so ergibt sich $x' \equiv 1 \pmod{2}$. Mit $x' = 1 + 2x''$ erhält man $38x'' \equiv -28 \pmod{70}$ oder $19x'' \equiv -14 \pmod{35}$. Die Lösung nach 5 ergibt $x'' \equiv 4 \pmod{5}$, und mit $x'' = 4 + 5x'''$ folgt $95x''' \equiv -90 \pmod{35}$ oder $19x''' \equiv -18 \pmod{7}$. Daraus folgt schließlich $x''' \equiv 2 \pmod{7}$, und setzt man $x''' = 2 + 7x''''$, so ergibt sich $x = 59 + 140x''''$. Daher ist $x \equiv 59 \pmod{140}$ die vollständige Lösung der gegebenen Kongruenz.

31.

So wie die Wurzel der Gleichung $ax = b$ durch $\frac{b}{a}$ ausgedrückt wird, bezeichnen wir auch jede Wurzel der Kongruenz $ax \equiv b$ durch $\frac{b}{a}$ und fügen zur Unterscheidung den Modul der Kongruenz hinzu. Zum Beispiel bezeichnet $\frac{19}{17} \pmod{12}$ jede Zahl, die $\equiv 11 \pmod{12}$ ist[*]. Aus dem Vorhergehenden folgt allgemein, dass $\frac{a}{b} \pmod{c}$ nichts Wirkliches bezeichnet (oder, wenn man will, etwas Imaginäres), wenn a, c einen gemeinsamen Teiler haben, der b nicht teilt. Außer in diesem Fall hat der Ausdruck $\frac{b}{a} \pmod{c}$ stets wirkliche Werte, und zwar unendlich viele. Diese sind alle nach c kongruent, wenn a zu c teilerfremd ist, oder nach $\frac{c}{\delta}$, wenn δ der größte gemeinsame Teiler von c, a ist.

Für diese Ausdrücke gelten fast dieselben Rechenregeln wie für gewöhnliche Brüche. Wir geben hier einige Eigenschaften an, die sich leicht aus dem Vorhergehenden ableiten lassen.

1. Ist nach dem Modul c sowohl $a \equiv \alpha$ als auch $b \equiv \beta$, so sind die Ausdrücke $\frac{a}{b} \pmod{c}$ und $\frac{\alpha}{\beta} \pmod{c}$ gleichwertig.

[*] was entsprechend durch $\frac{11}{1} \pmod{12}$ bezeichnet werden kann.

2. $\frac{a\delta}{b\delta}$ (mod. $c\delta$) und $\frac{a}{b}$ (mod. c) sind gleichwertig.
3. $\frac{ak}{bk}$ (mod. c) und $\frac{a}{b}$ (mod. c) sind gleichwertig, wenn k zu c teilerfremd ist.

Viele weitere ähnliche Sätze ließen sich anführen. Da sie aber keine Schwierigkeiten bereiten und für das Folgende nicht besonders nötig sind, gehen wir zu anderem über.

Bestimmung einer Zahl mit gegebenen Resten nach gegebenen Moduln.

32.

Die Aufgabe, *alle Zahlen zu finden, die nach beliebig vielen gegebenen Moduln gegebene Reste ergeben*, wird im Folgenden sehr nützlich sein und lässt sich aus dem Vorhergehenden leicht lösen. Zunächst seien zwei Moduln A, B gegeben, nach denen die gesuchte Zahl z zu den Zahlen a, b jeweils kongruent sein soll. Alle Werte von z haben also die Form $Ax+a$, wobei x unbestimmt ist, aber $Ax+a \equiv b$ (mod. B) erfüllen muss. Ist nun der größte gemeinsame Teiler von A, B gleich δ, so hat die vollständige Lösung dieser Kongruenz die Form $x \equiv v$ (mod. $\frac{B}{\delta}$) oder, gleichbedeutend, $x = v + \frac{kB}{\delta}$, wobei k eine beliebige ganze Zahl bezeichnet. Die Formel $Av + a + \frac{kAB}{\delta}$ umfasst somit alle Werte von z, das heißt, $z \equiv Av + a$ (mod. $\frac{AB}{\delta}$) ist die vollständige Lösung der Aufgabe. Kommt zu den Moduln A, B ein dritter, C, hinzu, nach dem die gesuchte Zahl $z \equiv c$ sein soll, so geht man offenbar genauso vor, da die ersten beiden Bedingungen bereits zu einer einzigen zusammengefasst sind. Ist nämlich der größte gemeinsame Teiler von $\frac{AB}{\delta}$. und C gleich $= \varepsilon$ und die Lösung der Kongruenz $\frac{AB}{\delta}x + Av + a \equiv c$ (mod. C) durch $x \equiv w$ (mod. $\frac{C}{\varepsilon}$) gegeben, so ist die Aufgabe durch die Kongruenz $z \equiv \frac{ABw}{\delta} + Av + a$ (mod. $\frac{ABC}{\delta\varepsilon}$) vollständig gelöst. Ebenso verfährt man bei beliebig vielen Moduln. Dabei sind $\frac{AB}{\delta}$, $\frac{ABC}{\delta\varepsilon}$ die kleinsten gemeinsamen Vielfachen von A, B beziehungsweise A, B, C. Für beliebig viele Moduln A, B, C usw., deren kleinstes gemeinsames Vielfaches M ist, hat daher die vollständige Lösung die Form $z \equiv r$ (mod. M). Ist eine der Hilfskongruenzen unlösbar, so muss man schließen, dass die Aufgabe unmöglich ist. Das kann offenbar nicht vorkommen, wenn alle Zahlen A, B, C usw. paarweise teilerfremd sind.

Beispiel. Die Zahlen A, B, C und a, b, c seien $504, 35, 16$ beziehungsweise $17, -4, 33$. Dann sind die beiden Bedingungen, dass $z \equiv 17$ (mod. 504) und $\equiv -4$ (mod. 35) sei, mit der einzigen Bedingung gleichwertig, dass es $\equiv 521$ mod. 2520) sei. Zusammen mit $z \equiv 33$ (mod. 16) ergibt dies $z \equiv 3041$ (mod. 5040).

33.

Sind die Zahlen A, B, C usw. paarweise teilerfremd, so ist bekanntlich ihr Produkt das kleinste gemeinsame Vielfache aller dieser Zahlen. In diesem Fall sind alle Kongruenzen $z \equiv a$ (mod. A), $z \equiv b$ (mod. B) usw. offenbar mit der einzigen Kongruenz $z \equiv r$ (mod. R) gleichwertig, wobei R das Produkt von A, B, C usw. bezeichnet. Umgekehrt lässt sich daher die einzige Bedingung $z \equiv r$ (mod. R) in mehrere zerlegen. Wird R auf irgendeine Weise in paarweise teilerfremde Faktoren A, B, C usw. zerlegt, so erfüllen die Bedingungen $z \equiv r$ (mod. A), $z \equiv r$ (mod. B), $z \equiv r$ (mod. C) usw. die Anforderung vollständig. Diese Bemerkung eröffnet uns einen Weg, nicht nur eine etwaige Unmöglichkeit der gegebenen Bedingungen sofort zu erkennen, sondern auch die Rechnung bequemer und übersichtlicher durchzuführen.

34.

Wie oben seien die Bedingungen $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$ gegeben. Man zerlege jeden Modul in paarweise teilerfremde Faktoren, A in $A'A''A'''$ usw., B in $B'B''B'''$ usw., und zwar so, dass die Zahlen A', A'' usw., B', B'' usw. Primzahlen oder Primzahlpotenzen sind. Ist eine der Zahlen A, B, C usw. bereits eine Primzahl oder Primzahlpotenz, so ist für sie keine Zerlegung nötig. Aus dem Vorhergehenden folgt, dass man die gegebenen Bedingungen durch $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$ usw., $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$ usw. ersetzen kann. Sind nun nicht alle Zahlen A, B, C usw. paarweise teilerfremd, ist etwa A zu B nicht teilerfremd, so können offenbar die Primteiler von A, B nicht alle verschieden sein. Unter den Faktoren A', A'', A''' usw. muss mindestens einer unter B', B'', B''' usw. entweder einen gleichen Faktor, ein Vielfaches oder einen Teiler haben. Ist *erstens* $A' = B'$, so müssen die Bedingungen $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$ identisch sein, das heißt, es muss $a \equiv b \pmod{A' \text{ oder } B'}$ gelten. Dann kann eine der beiden wegfallen. Gilt dagegen nicht $a \equiv b \pmod{A'}$, so ist die Aufgabe unmöglich. Ist *zweitens* B' ein Vielfaches von A', so muss die Bedingung $z \equiv a \pmod{A'}$ in $z \equiv b \pmod{B'}$ enthalten sein. Das heißt, die aus der letzteren folgende Bedingung $z \equiv b \pmod{A'}$ muss mit der ersteren identisch sein. Also kann die Bedingung $z \equiv a \pmod{A'}$ wegfallen, sofern sie der anderen nicht widerspricht; andernfalls ist die Aufgabe unmöglich. Sind so alle überflüssigen Bedingungen entfernt, so sind offenbar alle verbleibenden Moduln unter A', A'', A''' usw., B', B'', B''' usw. paarweise teilerfremd. Dann ist die Aufgabe sicher möglich, und wir können nach den zuvor gegebenen Regeln vorgehen.

35.

Beispiel. Soll wie oben $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$ und $\equiv 33 \pmod{16}$ gelten, so lassen sich diese Bedingungen in $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$, $\equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$, $\equiv 33 \pmod{16}$ zerlegen. Davon können die Bedingungen $z \equiv 17 \pmod{8}$, $z \equiv 17 \pmod{7}$ wegfallen, da die erstere in $z \equiv 33 \pmod{16}$ enthalten und die letztere mit $z \equiv -4 \pmod{7}$ identisch ist. Es bleiben also

$$z \equiv \begin{cases} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{cases} \qquad \text{daraus folgt} \quad z \equiv 3041 \pmod{5040}.$$

Meist ist es bequemer, diejenigen verbleibenden Bedingungen, die aus ein und derselben Bedingung hervorgegangen sind, jeweils wieder zusammenzufassen, da dies leicht möglich ist. Sind *zum Beispiel* von den Bedingungen $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$ usw. einige weggefallen, so erhält man aus den übrigen die Bedingung $z \equiv a$ nach dem Modul, der das Produkt aller verbleibenden Moduln unter A', A'', A''' usw. ist. So ergibt sich in unserem Beispiel aus $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$ von selbst wieder die ursprüngliche Bedingung $z \equiv -4 \pmod{35}$. Daraus folgt auch, dass es für die Kürze der Rechnung nicht ganz gleichgültig ist, welche der überflüssigen Bedingungen wegfallen. Diese und andere praktische Verfahren, die man durch Übung

viel leichter als durch Regeln lernt, hier darzustellen, ist aber nicht unsere Absicht.

36.

Sind alle Moduln A, B, C, D usw. paarweise teilerfremd, so ist häufig die folgende Methode vorzuziehen. Man bestimme eine Zahl α, die nach A der Eins, nach dem Produkt der übrigen Moduln aber der Null kongruent ist. Oder es sei α ein beliebiger Wert (meist nimmt man am besten den *kleinsten*) des Ausdrucks $\frac{1}{BCD \text{ usw.}}$ (mod. A), multipliziert mit BCD usw. (siehe Artikel 32). Ebenso sei $\beta \equiv 1$ (mod. B) und $\equiv 0$ (mod. ACD usw.), $\gamma \equiv 1$ (mod. C) und $\equiv 0$ (mod. ABD usw.) usw. Wird dann eine Zahl z gesucht, die nach den Moduln A, B, C, D usw. zu den Zahlen a, b, c, d usw. jeweils kongruent ist, so kann man setzen:

$$z \equiv \alpha a + \beta b + \gamma c + \delta d \text{ usw. (mod. } ABCD \text{ usw.)}.$$

Denn offenbar ist $\alpha a \equiv a$ (mod. A.), während die übrigen Glieder $\beta b, \gamma c$ usw. alle $\equiv 0$ (mod. A) sind; also ist $z \equiv a$ (mod. A). Der Beweis für die übrigen Moduln verläuft ebenso. Diese Lösung ist der früheren vorzuziehen, wenn mehrere solche Aufgaben zu lösen sind, bei denen die Moduln A, B, C usw. ihre Werte behalten. Dann haben nämlich die Zahlen α, β, γ usw. konstante Werte. Dies ist bei der Aufgabe der Zeitrechnung der Fall, das Jahr innerhalb der Julianischen Periode zu finden, dessen Indiktion, Goldene Zahl und Sonnenzirkel gegeben sind. Hier ist $A = 15$, $B = 19$, $C = 28$. Da der Wert des Ausdrucks $\frac{1}{19.28}$ (mod. 15) oder $\frac{1}{532}$ (mod. 15) gleich 13 ist, ist $\alpha = 6916$. Ebenso findet man für β den Wert 4200 und für γ den Wert 4845. Die gesuchte Zahl ist also der kleinste Rest von $6916a + 4200b + 4845c$, wobei a die Indiktion, b die Goldene Zahl und c den Sonnenzirkel bezeichnet.

Lineare Kongruenzen mit mehreren Unbekannten.

37.

Dies möge über Kongruenzen ersten Grades mit einer einzigen Unbekannten genügen. Es bleiben noch die Kongruenzen zu behandeln, in denen mehrere Unbekannte vorkommen. Eine Darstellung aller Einzelheiten mit voller Strenge würde jedoch viel Raum beanspruchen. Wir wollen hier nicht alles erschöpfend behandeln, sondern nur das anführen, was besonders beachtenswert erscheint. Deshalb beschränken wir die Untersuchung auf wenige Bemerkungen und behalten uns eine ausführlichere Darstellung für eine andere Gelegenheit vor.

1) Wie bei Gleichungen erkennt man auch hier, dass es ebenso viele Kongruenzen wie zu bestimmende Unbekannte geben muss.

2) Es seien also die Kongruenzen

$$\begin{aligned} &ax + by + cz \ldots \equiv f \text{ (mod. } m) && \ldots\ldots && (A)\\ &a'x + b'y + c'z \ldots \equiv f' && \ldots\ldots && (A')\\ &a''x + b''y + c''z \ldots \equiv f'' && \ldots\ldots\ldots && (A'')\\ &\text{usw.} \end{aligned}$$

gegeben, ebenso viele, wie es Unbekannte x, y, z usw. gibt.

Man bestimme nun Zahlen ξ, ξ', ξ'' usw. so, dass

$$\begin{aligned} b\xi + b'\xi' + b''\xi'' + \text{usw.} &= 0 \\ c\xi + c'\xi' + c''\xi'' + \text{usw.} &= 0 \\ \text{usw.} & \end{aligned}$$

gilt, und zwar so, dass sie alle ganzzahlig sind und keinen gemeinsamen Faktor haben. Dass dies möglich ist, folgt aus der Theorie der linearen Gleichungen. Ebenso bestimme man v, v', v'' usw., ζ, ζ', ζ'' usw. so, dass

$$\begin{aligned} av + a'v' + a''v'' + \text{usw.} &= 0 \\ cv + c'v' + c''v'' + \text{usw.} &= 0 \\ \text{usw.} & \end{aligned}$$

$$\begin{aligned} a\zeta + a'\zeta' + a''\zeta'' + \text{usw.} &= 0 \\ b\zeta + b'\zeta' + b''\zeta'' + \text{usw.} &= 0 \\ \text{usw.} \quad \text{usw.} & \end{aligned}$$

3) Multipliziert man die Kongruenzen A, A', A'' usw. mit ξ, ξ', ξ'' usw., dann mit v, v', v'', usw., und addiert jeweils die Ergebnisse, so erhält man offenbar die Kongruenzen

$$\begin{aligned} (a\xi + a'\xi' + a''\xi'' + \text{usw.})x &\equiv f\xi + f'\xi' + f''\xi'' + \text{usw.} \\ (bv + b'v' + b''v'' + \text{usw.})y &\equiv fv + f'v' + f''v'' + \text{usw.} \\ (c\zeta + c'\zeta' + c''\zeta'' + \text{usw.})z &\equiv f\zeta + f'\zeta' + f''\zeta'' + \text{usw.} \\ \text{usw.} & \end{aligned}$$

die wir der Kürze halber so schreiben:

$$\Sigma(a\xi)x \equiv \Sigma(f\xi), \quad \Sigma(bv)y \equiv \Sigma(fv), \quad \Sigma(c\zeta)z \equiv \Sigma(f\zeta) \text{ usw.}$$

4) Nun sind mehrere Fälle zu unterscheiden.

Erstens: Sind alle Koeffizienten der Unbekannten, $\Sigma(a\xi), \Sigma(av)$ usw., zum Modul m teilerfremd, so lassen sich diese Kongruenzen nach den zuvor gegebenen Regeln lösen. Die vollständige Lösung der Aufgabe wird durch Kongruenzen der Form $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$ usw. angegeben[*)]. *Zum Beispiel* seien die Kongruenzen

$$x + 3y + z \equiv 1, \quad 4x + y + 5z \equiv 7, \quad 2x + 2y + z \equiv 3 \pmod{8}$$

gegeben. Man findet $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, woraus $-15x \equiv -26$ folgt, also $x \equiv 6 \pmod{8}$. Ebenso erhält man $15y \equiv -4$, $15z \equiv 1$ und damit $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5) *Zweitens*: Sind nicht alle Koeffizienten $\Sigma(a\xi), \Sigma(bv)$ usw. zum Modul teilerfremd, so seien α, β, γ usw. die größten gemeinsamen Teiler von m mit $\Sigma(a\xi), \Sigma(bv), \Sigma(c\zeta)$ usw. in der entsprechenden Reihenfolge. Die Aufgabe ist offenbar unmöglich, wenn sie nicht die Zahlen $\Sigma(f\xi), \Sigma(fv), \Sigma(f\zeta)$ usw. jeweils teilen. Gelten diese Bedingungen,

[*)] Dieser Schluss bedarf eines Beweises, den wir hier jedoch weglassen. Streng genommen folgt aus unserer Untersuchung nur, dass die gegebenen Kongruenzen durch andere Werte der Unbekannten x, y usw. nicht gelöst werden können. Dass diese Werte sie erfüllen, folgt daraus nicht. Es könnte nämlich überhaupt keine Lösung geben. Ein ähnlicher Fehlschluss wird häufig auch bei der Darstellung linearer Gleichungen gemacht.

so werden die Kongruenzen in (3) durch $x \equiv p \pmod{\frac{m}{\alpha}}$, $y \equiv q \pmod{\frac{m}{\beta}}$, $z \equiv r \pmod{\frac{m}{\gamma}}$ usw. vollständig gelöst. Oder man hat α verschiedene Werte von x (das heißt, nach m inkongruente, nämlich $p, p+\frac{m}{\alpha} \ldots p+\frac{(\alpha-1)m}{\alpha}$), β verschiedene Werte von y usw., die diese Kongruenzen erfüllen. Offenbar finden sich alle Lösungen der gegebenen Kongruenzen, falls es überhaupt welche gibt, unter diesen. Diesen Schluss darf man aber nicht umkehren. Im Allgemeinen erfüllen nicht alle Kombinationen sämtlicher α Werte von x mit allen Werten von y und allen Werten von z usw. die Aufgabe, sondern nur einige. Ihr Zusammenhang lässt sich durch eine oder mehrere Kongruenzen als Bedingungen angeben. Da die vollständige Lösung dieser Aufgabe für das Folgende nicht nötig ist, gehen wir hier nicht näher darauf ein. Es genügt uns, durch ein Beispiel eine Vorstellung davon zu geben.

Gegeben seien die Kongruenzen

$$3x+5y+z \equiv 4, \quad 2x+3y+2z \equiv 7, \quad 5x+y+3z \equiv 6 \pmod{12}$$

Hier werden ξ, ξ', ξ'', v, v', v'', ζ, ζ', ζ'' der Reihe nach gleich $= 1, -2, 1,\ 1, 1, -1,\ -13, 22, -1$. Daraus folgen $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. Man erhält vier Werte von x, nämlich $\equiv 2, 5, 8.\ 11$, einen Wert von y, nämlich $\equiv 11$, und vier Werte von z, nämlich $\equiv 0, 3, 6, 9 \pmod{12}$. Um zu erkennen, welche Kombinationen der Werte von x mit den Werten von z zulässig sind, setzen wir in den gegebenen Kongruenzen für x, y, z der Reihe nach $2+3t$, 11, $3u$ ein. Sie gehen über in

$$57+9t+3u \equiv 0, \quad 30+6t+6u \equiv 0, \quad 15+15t+9u \equiv 0 \pmod{12}$$

Damit sind offenbar die folgenden Kongruenzen gleichwertig:

$$19+3t+u \equiv 0, \quad 10+2t+2u \equiv 0, \quad 5+5t+3u \equiv 0 \pmod{4}$$

Die erste verlangt offenbar $u \equiv t+1 \pmod{4}$. Setzt man diesen Wert in die übrigen Kongruenzen ein, so sind auch diese erfüllt. Folglich müssen die Werte von x, nämlich $2, 5, 8, 11$ (die man durch $t \equiv 0.\ 1, 2, 3$ erhält), mit den Werten von z, nämlich $z \equiv 3, 6, 9, 0$, jeweils in dieser Reihenfolge verbunden werden. Insgesamt gibt es also vier Lösungen:

$$\begin{array}{rrrrr} x \equiv & 2, & 5, & 8, & 11 \pmod{12} \\ y \equiv & 11, & 11, & 11, & 11 \\ z \equiv & 3, & 6, & 9, & 0 \end{array}$$

* *
*

Mit diesen Untersuchungen ist das Ziel des Abschnitts erreicht. Wir fügen noch einige Sätze hinzu, die auf ähnlichen Grundsätzen beruhen und im Folgenden oft gebraucht werden.

Verschiedene Sätze.

38.

Aufgabe. *Man bestimme, wie viele positive Zahlen kleiner als eine gegebene positive Zahl A und zugleich zu ihr teilerfremd sind.*

Der Kürze halber bezeichnen wir die Anzahl der positiven Zahlen, die zu einer gegebenen Zahl teilerfremd und kleiner als sie sind, durch das vorangestellte Zeichen ϕ. Gesucht ist also ϕA.

I. Ist A eine Primzahl, so sind offenbar alle Zahlen von 1 bis $A-1$ zu A teilerfremd. In diesem Fall ist daher

$$\phi A = A - 1$$

II. Ist A eine Primzahlpotenz, etwa $= p^m$, so sind alle durch p teilbaren Zahlen nicht zu A teilerfremd, die übrigen dagegen schon. Von den $p^m - 1$ Zahlen müssen also die Zahlen $p, 2p, 3p....(p^{m-1}-1)p$ wegfallen. Es bleiben $p^m - 1 - (p^{m-1}-1)$ oder $p^{m-1}(p-1)$. Somit ist

$$\phi p^m = p^{m-1}(p-1)$$

III. Die übrigen Fälle lassen sich mithilfe des folgenden Satzes leicht auf diese zurückführen: *Ist A in paarweise teilerfremde Faktoren M, N, P usw. zerlegt, so ist*

$$\phi A = \phi M . \phi N . \phi P \text{ usw.}$$

Der Beweis lautet so: Die zu M teilerfremden und unter M liegenden Zahlen seien $m, m'.m''$ usw.; ihre Anzahl ist also $= \phi M$. Ebenso seien die zu N, P usw. jeweils teilerfremden und kleineren Zahlen n, n', n'' usw., p, p', p'' usw.; ihre Anzahlen sind $\phi N, \phi P$ usw. Nun ist jede zum Produkt A teilerfremde Zahl auch zu jedem einzelnen Faktor M, N, P usw. teilerfremd, und umgekehrt (Artikel 19). Ferner ist jede Zahl, die zu einer der Zahlen m, m', m'' usw. nach dem Modul M kongruent ist, zu M teilerfremd, und umgekehrt; ebenso gilt dies für N, P usw. Die Frage ist somit darauf zurückgeführt, wie viele Zahlen unter A es gibt, die nach dem Modul M zu einer der Zahlen m, m', m'' usw., nach N zu einer der Zahlen n, n', n'' usw. kongruent sind. Nach Artikel 32 sind alle Zahlen, die nach den einzelnen Moduln M, N, P usw. bestimmte Reste ergeben, nach deren Produkt A kongruent. Unter A gibt es also nur eine Zahl, die nach den einzelnen Moduln M, N, P usw. zu gegebenen Resten kongruent ist. Die gesuchte Anzahl ist daher gleich der Anzahl der Kombinationen jeder der Zahlen m, m', m'' mit jeder der Zahlen n, n', n'' und jeder der Zahlen p, p', p'' usw. Diese Anzahl ist nach der Kombinationstheorie gleich $= \phi M . \phi N . \phi P$ usw. *Q. E. D.*

IV. Wie dies auf den vorliegenden Fall anzuwenden ist, sieht man nun leicht. Man zerlege A in seine Primfaktoren oder bringe es in die Form $a^\alpha b^\beta c^\gamma$ usw., wobei a, b, c usw. verschiedene Primzahlen bezeichnen. Dann ist

$$\begin{aligned}\phi A &= \phi a^\alpha . \phi b^\beta . \phi c^\gamma \text{ usw.} \\ &= a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1)\, c^{\gamma-1}(c-1) \text{ usw.}\end{aligned}$$

oder übersichtlicher

$$\phi A = A\,\frac{a-1}{a}.\,\frac{b-1}{b}.\,\frac{c-1}{c}\text{ usw.}$$

Beispiel. Sei $A = 60 = 2^2.3.5$, also $\phi A = \frac{1}{2}.\frac{2}{3}.\frac{4}{5}.60 = 16$. Die zu 60 teilerfremden Zahlen sind $1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53.59$.

Die erste Lösung dieser Aufgabe findet sich in der Abhandlung des berühmten Euler *theoremata arithmetica nova methodo demonstrata*, Comm. nov. Ac. Petrop. VIII, S. 74. Der Beweis wurde später in einer anderen Abhandlung wiederholt: *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII, S. 17.

39.

Bestimmt man die Bedeutung des Zeichens ϕ so, dass ϕA die Anzahl der Zahlen angibt, die zu A teilerfremd und *nicht größer* als A sind, so ist offenbar $\phi 1$ nicht mehr $= 0$, sondern $= 1$. In allen übrigen Fällen ändert sich nichts. Mit dieser Definition erhalten wir den folgenden Satz.

Sind a, a', a'' usw. sämtliche Teiler von A, einschließlich der Eins und A selbst, so ist

$$\phi a + \phi a' + \phi a'' + usw. = A$$

Beispiel. Sei $A = 30$, dann ist $\phi 1 + \phi 2 + \phi 3 + \phi 5 + \phi 6 + \phi 10 + \phi 15 + \phi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Beweis. Man multipliziere alle Zahlen, die zu a teilerfremd und nicht größer als a sind, mit $\frac{A}{a}$, ebenso alle zu a' teilerfremden Zahlen mit $\frac{A}{a'}$ usw. Man erhält $\phi a + \phi a' + \phi a''+$ usw. Zahlen, die alle nicht größer als A sind. Nun gilt:

1) Alle diese Zahlen sind verschieden. Für die Zahlen, die aus *demselben* Teiler von A hervorgehen, ist dies unmittelbar klar. Wären aus verschiedenen Teilern M, N und zu ihnen jeweils teilerfremden Zahlen μ, ν gleiche Zahlen hervorgegangen, wäre also $\frac{A}{M}\mu = \frac{A}{N}\nu$, so folgte $\mu N = \nu M$. Wir dürfen $M > N$ annehmen. Da M zu μ teilerfremd ist und μN teilt, müsste es auch N teilen, die größere Zahl also die kleinere. *Q. E. A.*

2) Unter diesen Zahlen finden sich alle Zahlen $1, 2, 3....A$. Sei eine beliebige Zahl, die A nicht übersteigt, gleich t und der größte gemeinsame Teiler von A, t gleich δ. Dann ist $\frac{A}{\delta}$ ein Teiler von A, zu dem $\frac{t}{\delta}$ teilerfremd ist. Die Zahl t findet sich daher offenbar unter denen, die aus dem Teiler $\frac{A}{\delta}$ hervorgehen.

3) Die Anzahl dieser Zahlen ist also A, und somit

$$\phi a + \phi a' + \phi a'' + \text{usw.} = A. \quad Q.\ E.\ D.$$

40.

Ist der größte gemeinsame Teiler von A, B, C, D usw. gleich $= \mu$, so lassen sich Zahlen a, b, c, d usw. so bestimmen, dass

$$aA + bB + cC + usw. = \mu$$

Beweis. Betrachten wir zunächst nur zwei Zahlen A, B, deren größter gemeinsamer Teiler $= \lambda$ sei. Dann ist die Kongruenz $Ax \equiv \lambda \pmod{B}$ lösbar (Artikel 30). Eine Wurzel sei $\equiv \alpha$, und man setze $\frac{\lambda - A\alpha}{B} = \beta$. Dann ist $\alpha A + \beta B = \lambda$, wie verlangt.

Kommt eine dritte Zahl C hinzu, so habe der größte gemeinsame Teiler der Zahlen λ, C den Wert $= \lambda'$. Dieser ist zugleich der größte gemeinsame Teiler von A, B, C[*]. Man bestimme Zahlen k, γ so, dass $k\lambda + \gamma C = \lambda'$ gilt; dann ist $k\alpha A + k\beta B + \gamma C = \lambda'$.

Kommt eine vierte Zahl D hinzu, so setze man den größten gemeinsamen Teiler von λ', D, der offenbar zugleich der größte gemeinsame Teiler von A, B, C, D ist, gleich $= \lambda''$ und bilde $k'\lambda' + \delta D = \lambda''$. Dann ist $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

Ebenso kann man bei beliebig vielen weiteren Zahlen vorgehen.

Haben also die Zahlen A, B, C, D usw. keinen gemeinsamen Teiler, so lässt sich offenbar erreichen, dass

$$aA + bB + cC + \text{usw.} = 1$$

41.

Ist p eine Primzahl und hat man p Gegenstände, von denen beliebig viele gleich sein dürfen, nur nicht alle, so ist die Anzahl ihrer Permutationen durch p teilbar.

Beispiel. Die fünf Gegenstände A, A, A, B, B lassen sich auf zehn verschiedene Arten anordnen.

Dieser Satz lässt sich leicht aus der bekannten Theorie der Permutationen beweisen. Gibt es unter den Gegenständen zunächst a gleiche, nämlich $= A$, dann b gleiche, nämlich $= B$, dann c gleiche, nämlich $= C$ usw., wobei die Zahlen a, b, c usw. auch gleich eins sein dürfen, so ist

$$a + b + c + \text{usw.} = p$$

Die Anzahl der Permutationen ist dann

$$= \frac{1.2.3.....p}{1.2.3...a.1.2..b.1.2..c \text{ usw.}}$$

Offenbar ist der Zähler dieses Bruchs durch den Nenner teilbar, da die Anzahl der Permutationen eine ganze Zahl sein muss. Der Zähler ist durch p teilbar; der Nenner dagegen, der aus Faktoren kleiner als p zusammengesetzt ist, ist nicht durch p teilbar (Artikel 15). Somit ist die Anzahl der Permutationen durch p teilbar (Artikel 19).

Wir hoffen aber, dass manche Leser auch an dem folgenden Beweis Freude haben werden.

Zwei Permutationen heißen *ähnlich*, wenn sich die Reihenfolge ihrer Gegenstände nur darin unterscheidet, dass der Gegenstand, der in der einen an erster Stelle steht, in der anderen einen anderen Platz einnimmt, die übrigen aber in beiden in derselben Reihenfolge aufeinanderfolgen und auf den letzten Gegenstand wieder der erste folgt[*]. So sind in unserem Beispiel die Permutationen $ABAAB$ und $ABABA$ ähnlich, weil die Gegenstände, die in der ersteren an erster, zweiter usw. Stelle stehen, in der letzteren in derselben Reihenfolge an dritter, vierter usw. Stelle stehen.

[*] Denn offenbar teilt λ' alle Zahlen A, B, C. Wäre es nicht der *größte* gemeinsame Teiler, so wäre dieser größer als λ'. Da dieser größte Teiler aber A, B, C teilt, müsste er auch $k\alpha A + k\beta B + \gamma C$, also λ' teilen, die größere Zahl also die kleinere. *Q. E. A.* — Noch leichter folgt dies aus Artikel 18.

[*] Denkt man sich ähnliche Permutationen im Kreis geschrieben, sodass der letzte Gegenstand an den ersten grenzt, so unterscheiden sie sich überhaupt nicht, da keine Stelle als erste oder letzte bezeichnet werden kann.

Da jede Permutation aus p Gegenständen besteht, kann man zu jeder $p-1$ ähnliche finden, indem man den zuvor ersten Gegenstand an die zweite, dritte usw. Stelle verschiebt. Können keine zwei davon identisch sein, so ist offenbar die Gesamtzahl der Permutationen durch p teilbar, denn sie ist p-mal so groß wie die Anzahl aller untereinander unähnlichen Permutationen. Nehmen wir also an, zwei Permutationen

$$PQ \dots TV \dots YZ; \qquad V \dots YZPQ \dots T$$

die durch Verschieben der Glieder auseinander hervorgehen, seien identisch, also $P = V$ usw. Das Glied P, das in der ersteren an erster Stelle steht, stehe in der letzteren an Stelle $n+1$. Dann ist in der letzteren Reihe das Glied an Stelle $n+1$ dem ersten, das an Stelle $n+2$ dem zweiten gleich usw. Somit ist auch das Glied an Stelle $2n+1$ wieder dem ersten gleich, ebenso das an Stelle $3n+1$ usw. Allgemein ist das Glied an Stelle $kn+m$ dem an Stelle m gleich. Übersteigt dabei $kn+m$ die Zahl p, so ist entweder die Reihe $V \dots YZPQ \dots T$ immer wieder von vorn zu beginnen, oder von $kn+m$ ist das nächstkleinere Vielfache von p abzuziehen. Bestimmt man nun k so, dass $kn \equiv 1 \pmod{p}$ gilt, was möglich ist, da p eine Primzahl ist, so ist allgemein das Glied an Stelle m dem an Stelle $m+1$ gleich. Jedes Glied ist also dem folgenden gleich, *das heißt*, alle Glieder sind gleich, entgegen der Voraussetzung.

42.

Sind die Koeffizienten $A, B, C \dots N$, $a, b, c \dots n$ zweier Funktionen der Form

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \dots\dots + N \quad . \quad . \quad . \quad . \quad . \qquad (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \dots\dots + n \quad . \quad . \quad . \quad . \quad . \qquad (Q)$$

sämtlich rational, aber nicht alle ganzzahlig, und ist das Produkt von (P) und (Q) gleich

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \textit{usw.} + \mathfrak{Z}$$

so können nicht alle seine Koeffizienten $\mathfrak{A}, \mathfrak{B} \dots \mathfrak{Z}$ ganzzahlig sein.

Beweis. Man schreibe alle Brüche unter den Koeffizienten A, B usw., a, b usw. vollständig gekürzt und wähle eine beliebige Primzahl p, die einen oder mehrere ihrer Nenner teilt. Wir dürfen annehmen, dass p den Nenner eines gebrochenen Koeffizienten in (P) teilt. Wird (Q) durch p geteilt, so gibt es auch in $\frac{(Q)}{p}$ mindestens einen gebrochenen Koeffizienten, dessen Nenner den Faktor p enthält, nämlich den ersten Koeffizienten $\frac{1}{p}$.

In (P) gibt es offenbar einen gebrochenen Term, dessen Nenner eine *höhere* Potenz von p enthält als die Nenner aller vorhergehenden gebrochenen Terme und eine *nicht niedrigere* als die Nenner aller folgenden. Dieser Term sei $= Gx^g$, und die Anzahl der Faktoren p im Nenner von G sei $= t$. Einen entsprechenden Term gibt es in $\frac{(Q)}{p}$; er sei $= \Gamma x^\gamma$ und die Anzahl der Faktoren p im Nenner von Γ sei $= \tau$. Offenbar ist $t + \tau$ mindestens $= 2$. Nach diesen Vorbereitungen hat der Term $x^{g+\gamma}$ im Produkt von (P) und (Q) einen gebrochenen Koeffizienten, dessen Nenner $t + \tau - 1$ Faktoren p enthält. Dies wird folgendermaßen bewiesen.

Die Terme, die in (P) dem Term Gx^g vorausgehen, seien $'Gx^{g+1}$, $''Gx^{g+2}$ usw., die folgenden dagegen $G'x^{g-1}$, $G''x^{g-2}$ usw. Ebenso seien in $\frac{(Q)}{p}$ die dem Term Γx^γ vorausgehenden Terme $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$ usw., die folgenden $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$ usw. Dann ist im Produkt von (P), $\frac{(Q)}{p}$ der Koeffizient von $x^{g+\gamma}$ gleich

$$\begin{aligned} &= G\Gamma + {}'G\Gamma' + {}''G\Gamma'' + \text{usw.} \\ &\quad + {}'\Gamma G' + {}''\Gamma G'' + \text{usw.} \end{aligned}$$

Das Glied $G\Gamma$ ist ein Bruch, dessen Nenner bei vollständiger Kürzung $t+\tau$ Faktoren p enthält. Die übrigen Glieder enthalten, soweit sie gebrochen sind, weniger Faktoren p im Nenner. Denn sie sind Produkte zweier Faktoren, von denen der eine nicht mehr als t, der andere weniger als τ Faktoren p enthält, oder der eine nicht mehr als τ und der andere weniger als t. Somit hat $G\Gamma$ die Form $\frac{e}{fp^{t+\tau}}$, die Summe der übrigen Glieder dagegen die Form $\frac{e'}{f'p^{t+\tau-\delta}}$, wobei δ positiv ist und e, f, f' frei vom Faktor p sind. Die Summe aller Glieder ist daher $= \frac{ef'+e'fp^\delta}{ff'p^{t+\tau}}$. Ihr Zähler ist nicht durch p teilbar, sodass der Nenner durch keine Kürzung weniger als $t+\tau$ solche Faktoren enthalten kann. Der Koeffizient von $x^{g+\gamma}$ im Produkt von $(P), (Q)$ ist also

$$= \frac{ef' + e'fp^\delta}{ff'p^{t+\tau-1}}.$$

das heißt, ein Bruch, dessen Nenner $t+\tau-1$ Faktoren p enthält.
Q. E. D.

43.

Eine Kongruenz vom Grad m

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \textit{usw.} + Mx + N \equiv 0$$

deren Modul eine Primzahl p ist, die A nicht teilt, lässt sich nicht auf mehr als m verschiedene Arten lösen; sie hat also nicht mehr als m nach p inkongruente Wurzeln (siehe Artikel 25, 26).

Wer dies bestreitet, nehme an, es gebe Kongruenzen verschiedener Grade m, n usw., die mehr als m, n usw. Wurzeln haben. Der kleinste solche Grad sei m, sodass alle entsprechenden Kongruenzen niedrigeren Grades unserem Satz genügen. Da dies für den ersten Grad bereits bewiesen ist (Artikel 26), muss m entweder $= 2$ oder größer sein. Die Kongruenz

$$Ax^m + Bx^{m-1} + \text{usw.} + Mx + N \equiv 0$$

hat also mindestens $m+1$ Wurzeln, etwa $x \equiv \alpha, x \equiv \beta, x \equiv \gamma$ usw. Wir dürfen annehmen, dass alle Zahlen α, β, γ usw. positiv und kleiner als p sind und α die kleinste ist. Setzt man nun in der gegebenen Kongruenz für x den Ausdruck $y+\alpha$ ein, so geht sie über in

$$A'y^m + B'y^{m-1} + C'y^{m-2} .... + M'y + N' \equiv 0$$

Diese Kongruenz ist offenbar erfüllt, wenn man $y \equiv 0$ oder $\equiv \beta - \alpha$ oder $\equiv \gamma - \alpha$ usw. setzt. Diese Wurzeln sind alle verschieden, und ihre Anzahl ist $= m + 1$. Da $y \equiv 0$ eine Wurzel ist, folgt, dass N' durch p teilbar ist. Also gilt auch

$$y(A'y^{m-1} + B'y^{m-2} + \text{usw.} + M') \text{ ist } \equiv 0 \text{ (mod.}p),$$

wenn y einer der m Werte $\beta - \alpha, \gamma - \alpha$ usw. gegeben wird, die alle > 0 und $< p$ sind. In all diesen Fällen gilt daher auch

$$A'y^{m-1} + B'y^{m-2} + \text{usw.} + M' \text{ ist } \equiv 0 \text{ (Artikel 22)}$$

das heißt, die Kongruenz $A'y^{m-1} + B'y^{m-2} + \text{usw.} + M' \equiv 0$
hat den Grad $m - 1$ und m Wurzeln und widerspricht somit unserem Satz. Denn offenbar ist A' gleich $= A$ und daher, wie verlangt, nicht durch p teilbar. Dabei hatten wir angenommen, dass alle Kongruenzen von niedrigerem Grad als m dem Satz genügen. *Q. E. A.*

44.

Obwohl wir hier vorausgesetzt haben, dass der Modul p den Koeffizienten des höchsten Terms nicht teilt, ist der Satz nicht auf diesen Fall beschränkt. Wäre nämlich der erste Koeffizient oder wären auch einige der folgenden durch p teilbar, so könnten diese Terme ohne Weiteres wegfallen. Dadurch würde die Kongruenz schließlich auf einen niedrigeren Grad zurückgeführt, bei dem der erste Koeffizient nicht mehr durch p teilbar wäre. Dies gilt, sofern nicht alle Koeffizienten durch p teilbar sind; dann wäre die Kongruenz eine Identität und die Unbekannte völlig unbestimmt.

Dieser Satz wurde zuerst vom berühmten La Grange aufgestellt und bewiesen (*Mém. de l'Ac. de Berlin, Année* 1768, *S.* 192). Er findet sich auch in der Abhandlung des berühmten Le Gendre *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris* 1785, *S.* 466. Der berühmte Euler bewies in *Nov. Comm. Ac. Petr.* XVIII, *S.* 93, dass die Kongruenz $x^n - 1 \equiv 0$ nicht mehr als n verschiedene Wurzeln haben kann. Obwohl dies ein Sonderfall ist, lässt sich die Methode, die dieser große Mann verwendet hat, leicht auf alle Kongruenzen übertragen. Einen noch eingeschränkteren Fall hatte er schon zuvor behandelt, in *Comm. nov. Ac. Petr.* V, *S.* 6; diese Methode lässt sich aber nicht allgemein anwenden. Weiter unten, in Abschnitt VIII, werden wir den Satz noch auf eine andere Weise beweisen. So verschieden alle diese Methoden auf den ersten Blick erscheinen mögen, werden kundige Leser bei einem Vergleich leicht erkennen, dass sie alle auf demselben Grundsatz beruhen. Da der Satz hier nur als Hilfssatz betrachtet wird und eine vollständige Darstellung nicht hierhergehört, verzichten wir auf eine gesonderte Behandlung zusammengesetzter Moduln.

DRITTER ABSCHNITT

ÜBER

POTENZRESTE.

Die Reste der Glieder einer mit der Eins beginnenden geometrischen Folge bilden eine periodische Folge.

45.

Satz. *In jeder geometrischen Folge* $1, a, aa, a^3$ *usw. gibt es außer dem ersten Glied* 1 *noch ein Glied* a^t*, das nach einem Modul* p*, der zu* a *teilerfremd ist, der Eins kongruent ist und den Exponenten* $t < p$ *hat.*

Beweis. Da der Modul p zu a und damit zu jeder Potenz von a teilerfremd ist, ist kein Glied der Folge $\equiv 0 \pmod{p}$. Jedes ist vielmehr zu einer der Zahlen $1, 2, 3....p-1$ kongruent. Da ihre Anzahl $p-1$ ist, können offenbar nicht alle Glieder verschiedene kleinste Reste haben, wenn man mehr als $p-1$ Glieder der Folge betrachtet. Unter den Gliedern $1, a, aa, a^3....a^{p-1}$ sind also mindestens zwei kongruent. Sei $a^m \equiv a^n$ und $m > n$. Durch Division mit a^n ergibt sich $a^{m-n} \equiv 1$ (Artikel 22), wobei $m - n < p$ und > 0 ist.
Q. E. D.

Beispiel. In der Folge $2, 4, 8$ usw. ist das erste Glied, das nach dem Modul 13 der Eins kongruent ist, $2^{12} = 4096$. Nach dem Modul 23 ergibt sich dagegen in derselben Folge $2^{11} = 2048 \equiv 1$. Ebenso ist die sechste Potenz von 5, nämlich 15625, nach dem Modul 7 der Eins kongruent, die fünfte Potenz, 3125, dagegen nach 11. In manchen Fällen ist also schon eine Potenz mit kleinerem Exponenten als $p-1$ der Eins kongruent; in anderen muss man bis zur Potenz mit dem Exponenten $p-1$ gehen.

46.

Setzt man die Folge über ein der Eins kongruentes Glied hinaus fort, so treten dieselben Reste wie am Anfang erneut auf. Ist nämlich $a^t \equiv 1$, so ist $a^{t+1} \equiv a, a^{t+2} \equiv aa$ usw., bis man zum Glied a^{2t} kommt, dessen kleinster Rest wieder $\equiv 1$ ist und die *Periode* der Reste neu beginnt. Man hat also eine Periode mit t Resten, die nach ihrem Ende stets von vorn wiederholt wird. Andere Reste als die in dieser Periode enthaltenen können in der ganzen Folge nicht vorkommen. Allgemein ist $a^{mt} \equiv 1$ und $a^{mt+n} \equiv a^n$, was sich in unserer Schreibweise so ausdrückt:

$$\textit{Ist } r \equiv \rho \ (\textit{mod.}\, t), \quad \textit{so ist} \quad a^r \equiv a^\rho \ (\textit{mod.}\, p).$$

47.

Dieser Satz ermöglicht es, Reste von Potenzen mit beliebig großen Exponenten rasch zu bestimmen, sobald eine der Eins kongruente Potenz bekannt ist. Sucht man *zum Beispiel* den Rest bei Division von 3^{1000} durch 13, so ist wegen $3^3 \equiv 1$ (mod. 13) auch $t \equiv 3$. Da $1000 \equiv 1$ (mod. 3) ist, folgt $3^{1000} \equiv 3$ (mod. 13).

48.

Ist a^t die *niedrigste* der Eins kongruente Potenz, abgesehen von $a^0 = 1$, was wir hier außer Betracht lassen, so sind jene t Glieder, die die Periode der Reste bilden, alle verschieden, wie man aus dem Beweis von Artikel 45 leicht erkennt. Dann lässt sich der Satz von Artikel 46 umkehren: Ist $a^m \equiv a^n \pmod{p}$, so ist $m \equiv n \pmod{t}$. Wären nämlich m, n nach dem Modul t inkongruent, so wären ihre kleinsten Reste μ, ν verschieden. Es ist aber $a^\mu \equiv a^m, a^\nu \equiv a^n$, also $a^\mu \equiv a^\nu$. *Das heißt*, nicht alle Potenzen unter a^t wären inkongruent, entgegen der Voraussetzung.

Ist also $a^k \equiv 1 \pmod{p}$, so ist $k \equiv 0 \pmod{t}$, *das heißt*, k ist durch t teilbar.

Bisher haben wir beliebige Moduln betrachtet, sofern sie zu a teilerfremd sind. Nun betrachten wir Primzahlmoduln gesondert und bauen später auf dieser Grundlage eine allgemeinere Untersuchung auf.

Zunächst werden Moduln betrachtet, die Primzahlen sind.

49.

Satz. *Ist p eine Primzahl, die a nicht teilt, und ist a^t die niedrigste Potenz von a, die nach dem Modul p der Eins kongruent ist, so ist der Exponent t entweder $= p-1$ oder ein Teiler dieser Zahl.*

Man vergleiche die Beispiele in Artikel 45.

Beweis. Es ist bereits gezeigt, dass t entweder $= p-1$ oder $< p-1$ ist. Es bleibt zu beweisen, dass im letzteren Fall t stets ein Teiler von $p-1$ ist.

I. Man nehme die kleinsten positiven Reste aller Glieder $1, a, aa....a^{t-1}$ und bezeichne sie mit $\alpha, \alpha', \alpha''$ usw., sodass $\alpha = 1, \alpha' \equiv a, \alpha'' \equiv aa$ usw. gilt. Sie sind offenbar alle verschieden. Ergäben nämlich zwei Glieder a^m, a^n denselben Rest, so wäre, wenn man $m > n$ annimmt, $a^{m-n} \equiv 1$ und $m - n < t$, *Q. E. A.*, da keine niedrigere Potenz als a^t der Eins kongruent ist (*nach Voraussetzung*). Ferner gehören alle Zahlen $\alpha, \alpha', \alpha''$ usw. zur Reihe $1, 2, 3...p-1$, schöpfen sie aber nicht aus, da $t < p-1$ ist. Die Gesamtheit aller $\alpha, \alpha', \alpha''$ usw. bezeichnen wir mit (A). Somit enthält (A) genau t Glieder.

II. Man wähle eine beliebige Zahl β aus $1, 2, 3...p-1$, die in (A) fehlt, multipliziere β mit allen $\alpha, \alpha', \alpha''$ usw. und nenne die daraus entstehenden kleinsten Reste β, β', β'' usw. Ihre Anzahl ist ebenfalls t. Diese Reste sind sowohl untereinander als auch von allen $\alpha, \alpha', \alpha''$ usw. verschieden. Wäre die *erste* Behauptung falsch, so wäre $\beta a^m \equiv \beta a^n$ und nach Division durch β auch $a^m \equiv a^n$, entgegen dem eben Bewiesenen. Wäre die *zweite* falsch, so wäre $\beta a^m \equiv a^n$. Für $m < n$ folgte $\beta \equiv a^{n-m}$, *das heißt*, β wäre zu einer der Zahlen $\alpha, \alpha', \alpha''$ usw. kongruent, entgegen der Voraussetzung. Für $m > n$ folgt durch Multiplikation mit a^{t-m} die Kongruenz $\beta a^t \equiv a^{t+n-m}$ oder wegen $a^t \equiv 1$ auch $\beta \equiv a^{t+n-m}$, derselbe Widerspruch. Die Gesamtheit aller β, β', β'' usw., deren Anzahl $= t$ ist, bezeichnen wir mit (B). Damit haben wir bereits $2t$ Zahlen aus $1, 2, 3...p-1$. Umfassen also (A) und (B) alle diese Zahlen, so ist $\frac{p-1}{2} = t$ und der Satz bewiesen.

III. Fehlen noch Zahlen, so sei γ eine davon. Man multipliziere damit alle $\alpha, \alpha', \alpha''$ usw.; die kleinsten Reste der Produkte seien $\gamma, \gamma', \gamma''$ usw. Ihre Gesamtheit werde mit $(C$ bezeichnet. Dann enthält (C) genau t Zahlen aus $1, 2, 3...p-1$, die sowohl

untereinander als auch von den in (A) und (B) enthaltenen Zahlen verschieden sind. Die ersten beiden Behauptungen werden wie in II bewiesen, die dritte folgendermaßen: Wäre $\gamma a^m \equiv \beta a^n$, so folgte $\gamma \equiv \beta a^{n-m}$ oder $\equiv \beta a^{t+n-m}$, je nachdem, ob $m < n$ oder $> n$ ist. In beiden Fällen wäre γ zu einer Zahl aus (B) kongruent, entgegen der Voraussetzung. Man hat also $3t$ Zahlen aus $1, 2, 3...p-1$. Fehlen keine mehr, so ist $t = \frac{p-1}{3}$ und der Satz bewiesen.

IV. Fehlen immer noch Zahlen, so geht man auf dieselbe Weise zu einer vierten Gesamtheit (D) über usw. Da die Anzahl der Zahlen $1, 2, 3....p-1$ endlich ist, müssen sie schließlich alle erfasst sein. Ihre Anzahl ist daher ein Vielfaches von t, also ist t ein Teiler von $p-1$. *Q. E. D.*

Fermats Satz.

50.

Da also $\frac{p-1}{t}$ eine ganze Zahl ist, erhält man durch Erheben beider Seiten der Kongruenz $a^t \equiv 1$ zur Potenz mit dem Exponenten $\frac{p-1}{t}$ die Kongruenz $a^{p-1} \equiv 1$. *Das heißt, $a^{p-1} - 1$ ist stets durch p teilbar, wenn p eine Primzahl ist, die a nicht teilt.*

Dieser Satz verdient wegen seiner Eleganz und seiner außerordentlichen Nützlichkeit volle Aufmerksamkeit. Nach seinem Entdecker wird er gewöhnlich *Fermats Satz* genannt. Siehe *Fermatii Opera Mathem. Tolosae* 1679, *fol. S.* 163. Der Entdecker fügte keinen Beweis hinzu, erklärte aber, einen zu besitzen. Der berühmte Euler veröffentlichte als Erster einen Beweis in der Abhandlung *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T.* VIII[*)]. Dieser Beweis beruht auf der Entwicklung der Potenz $(a+1)^p$. Aus der Form der Koeffizienten folgt leicht, dass $(a+1)^p - a^p - 1$ stets durch p teilbar ist. Daher ist $(a+1)^p - (a+1)$ durch p teilbar, wenn $a^p - a$ durch p teilbar ist. Da nun $1^p - 1$ stets durch p teilbar ist, gilt dies auch für $2^p - 2$, damit auch für $3^p - 3$ usw. und allgemein für $a^p - a$. Teilt also p die Zahl a nicht, so ist auch $a^{p-1} - 1$ durch p teilbar. Dies genügt, um die Art der Methode zu zeigen. Der angesehene Lambert gab einen ähnlichen Beweis in *Actis Erudit.* 1769, *S.* 109. Da aber die Entwicklung einer Binomialpotenz der Zahlentheorie etwas fremd zu sein schien, suchte der berühmte Euler einen anderen Beweis. Er findet sich in *Comment. nov. Petr. T.* VII, *S.* 70, und stimmt völlig mit dem Beweis überein, den wir im vorigen Artikel gegeben haben. Später werden sich uns noch weitere Beweise bieten. Hier dürfen wir noch einen hinzufügen, der auf ähnlichen Grundsätzen wie Eulers erster Beweis beruht. Der folgende Satz, von dem unser Satz nur ein Sonderfall ist, wird auch bei anderen Untersuchungen weiter unten verwendet werden.

[*)] In einer früheren Abhandlung hatte dieser große Mann sein Ziel noch nicht erreicht: *Comm. Petr. T.* VI, *S.* 106. — In dem berühmten Streit zwischen Maupertuis und Konig, der vom Prinzip der kleinsten Wirkung ausging, sich aber bald auf andere Gegenstände ausdehnte, erklärte König, eine eigenhändige Niederschrift von Leibniz zu besitzen, die einen mit Eulers Beweis völlig übereinstimmenden Beweis dieses Satzes enthalte: *Appel au public. S.* 106. Wir wollen diesem Zeugnis zwar nicht die Glaubwürdigkeit absprechen; gewiss ist aber, dass Leibniz seine Entdeckung nie veröffentlichte. Vergleiche *Hist. de l'Ac. de Prusse, A.* 1750, *S.* 530.

51.

Das Polynom $a+b+c+$ usw. ist, zur Potenz mit dem Exponenten p erhoben, nach dem Modul p

$$\equiv a^p + b^p + c^p + \textit{usw.}$$

sofern p eine Primzahl ist.

Beweis. Die Potenz mit dem Exponenten p des Polynoms $a+b+c+$ usw. besteht aus Gliedern der Form $\varkappa a^\alpha b^\beta c^\gamma$ usw., wobei $\alpha+\beta+\gamma$ usw. $= p$ ist. Dabei bezeichnet $\varkappa$ die Anzahl der Permutationen von p Gegenständen, von denen α, β, γ usw. jeweils $= a, b, c$ usw. sind. Nach Artikel 41 ist diese Anzahl stets durch p teilbar, außer wenn alle Gegenstände gleich sind, *das heißt*, wenn eine der Zahlen α, β, γ usw. gleich $= p$ und die übrigen gleich $= 0$ sind. Somit sind alle Glieder von $(a+b+c+\text{usw.})^p$ außer a^p, b^p, c^p usw. durch p teilbar. Bei einer Kongruenz nach dem Modul p dürfen sie also wegfallen, und man erhält

$$(a+b+c+\text{usw.})^p \equiv a^p + b^p + c^p + \text{usw.} \quad \textit{Q. E. D.}$$

Setzt man nun alle Größen a, b, c usw. $= 1$ und ihre Anzahl $= k$, so ergibt sich $k^p \equiv k$, wie im vorigen Artikel.

Wie viele Zahlen zu Perioden gehören, deren Gliederzahl ein gegebener Teiler von $p-1$ ist.

52.

Da nur Teiler von $p-1$ Exponenten der niedrigsten Potenzen sein können, zu denen Zahlen erhoben werden, um der Eins kongruent zu werden, stellt sich die Frage, ob alle Teiler von $p-1$ dafür geeignet sind. Ferner ist zu fragen, wie viele Zahlen zu jedem Exponenten gehören, wenn man alle nicht durch p teilbaren Zahlen nach dem Exponenten ihrer niedrigsten der Eins kongruenten Potenz einteilt. Zunächst genügt es offenbar, die positiven Zahlen von 1 bis $p-1$ zu betrachten. Kongruente Zahlen müssen nämlich zur gleichen niedrigsten Potenz erhoben werden, um der Eins kongruent zu werden. Daher gehört jede Zahl zu demselben Exponenten wie ihr kleinster positiver Rest. Wir müssen also ermitteln, wie die Zahlen $1, 2, 3 \ldots p-1$ in dieser Hinsicht auf die einzelnen Faktoren von $p-1$ verteilt sind. Ist d einer der Teiler von $p-1$, zu denen auch 1 und $p-1$ gehören, so bezeichnen wir der Kürze halber mit ψd die Anzahl der positiven Zahlen unter p, deren niedrigste der Eins kongruente Potenz den Exponenten d hat.

53.

Um die Untersuchung leichter verständlich zu machen, geben wir ein Beispiel. Für $p = 19$ verteilen sich die Zahlen $1, 2, 3 \ldots 18$ auf die Teiler von 18 folgendermaßen:

1	1.
2	18.
3	7, 11.
6	8, 12.
9	4, 5. 6, 9, 16, 17.
18	2, 3, 10, 13. 14, 15.

In diesem Fall ist also $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. Bei einiger Aufmerksamkeit erkennt man, dass zu jedem Exponenten ebenso viele Zahlen gehören, wie es nicht größere und zu ihm teilerfremde Zahlen gibt. Mit der Schreibweise von Artikel 39 ist also zumindest in diesem Fall $\psi d = \phi d$. Dass dies allgemein gilt, beweisen wir so.

I. Es sei eine Zahl a gegeben, die zum Exponenten d *gehört*, *das heißt*, deren Potenz mit dem Exponenten d der Eins kongruent ist, während alle niedrigeren Potenzen dazu inkongruent sind. Dann haben auch alle ihre Potenzen $aa, a^3, a^4 \ldots a^d$ oder deren kleinste Reste die erste Eigenschaft: Ihre Potenzen mit dem Exponenten d sind der Eins kongruent. Anders ausgedrückt sind die kleinsten Reste der Zahlen $a, aa, a^3 \ldots a^d$, die alle verschieden sind, Wurzeln der Kongruenz $x^d \equiv 1$. Da diese nicht mehr als d verschiedene Wurzeln haben kann, gibt es außer den kleinsten Resten der Zahlen $a, aa, a^3 \ldots a^d$ keine weiteren Zahlen zwischen 1 und $p-1$ einschließlich, deren Potenzen mit dem Exponenten d der Eins kongruent sind. Alle zum Exponenten d gehörenden Zahlen finden sich also unter den kleinsten Resten der Zahlen $a, aa, a^3 \ldots a^d$. Welche es sind und wie viele, bestimmt man folgendermaßen. Ist k zu d teilerfremd, so ist keine Potenz von a^k mit einem Exponenten $< d$ der Eins kongruent. Sei nämlich $\frac{1}{k} \,(\mathrm{mod.}\, d) \equiv m$ (siehe Artikel 31); dann ist $a^{km} \equiv a$. Wäre nun die Potenz mit dem Exponenten e von a^k der Eins kongruent und $e < d$, so wäre auch $a^{kme} \equiv 1$ und damit $a^e \equiv 1$, entgegen der Voraussetzung. Also gehört der kleinste Rest von a^k offenbar zum Exponenten d. Hat dagegen k einen gemeinsamen Teiler δ mit d, so gehört der kleinste Rest von a^k nicht zum Exponenten d. Denn schon die Potenz mit dem Exponenten $\frac{d}{\delta}$ ist der Eins kongruent, da $\frac{kd}{\delta}$ durch d teilbar ist, also $\equiv 0 \,(\mathrm{mod.}\, d)$ und damit $a^{\frac{kd}{\delta}} \equiv 1$ gilt. Folglich gehören zum Exponenten d ebenso viele Zahlen, wie unter $1, 2, 3 \ldots d$ zu d teilerfremde Zahlen vorkommen. Dabei ist aber zu beachten, dass wir vorausgesetzt haben, bereits eine Zahl a zu besitzen, die zum Exponenten d gehört. Es bleibt also fraglich, ob zu einem Exponenten vielleicht überhaupt keine Zahl gehört. Der Schluss beschränkt sich daher darauf, dass ψd entweder $= 0$ oder $= \phi d$ ist.

54.

II. Alle Teiler von $p-1$ seien nun d, d', d'' usw. Da alle Zahlen $1, 2, 3 \ldots p-1$ auf diese verteilt sind, ist

$$\psi d + \psi d' + \psi d'' + \text{usw.} = p - 1$$

In Artikel 40 haben wir aber bewiesen, dass

$$\phi d + \phi d' + \phi d'' + \text{usw.} = p - 1$$

Nach dem vorigen Artikel ist ψd entweder gleich oder kleiner als ϕd, kann aber nicht größer sein; ebenso gilt dies für $\psi d'$ und $\phi d'$ usw. Wäre nun eines der Glieder $\psi d, \psi d', \psi d''$ usw. kleiner als das entsprechende Glied unter $\phi d, \phi d', \phi d''$, oder wären es mehrere, so könnten die beiden Summen nicht gleich sein. Wir schließen also schließlich, dass ψd *stets gleich* ϕd *ist* und daher nicht von der Größe von $p-1$ abhängt.

55.

Besondere Aufmerksamkeit verdient der Sonderfall des vorigen Satzes, dass es nämlich *stets Zahlen gibt, deren Potenzen mit kleinerem Exponenten als* $p-1$ *der Eins nicht kongruent sind.* Und zwar gibt es zwischen 1 und $p-1$ ebenso viele davon, wie es unter $p-1$ zu $p-1$ teilerfremde Zahlen gibt. Der Beweis dieses Satzes ist keineswegs so selbstverständlich, wie es auf den ersten Blick scheinen mag. Wegen seiner Bedeutung dürfen wir noch einen etwas anderen Beweis hinzufügen, da verschiedene Methoden oft viel dazu beitragen, schwierigere Dinge verständlich zu machen. Man zerlege $p-1$ in seine Primfaktoren, sodass $p-1 = a^\alpha b^\beta c^\gamma$ usw. ist, wobei a, b, c usw. verschiedene Primzahlen bezeichnen. Zum Beweis zeigen wir nun Folgendes:

I. Es lässt sich stets eine Zahl A, oder auch mehrere, finden, die zum Exponenten a^α gehört; ebenso Zahlen B, C usw., die zu den Exponenten b^β, c^γ usw. jeweils gehören.

II. Das Produkt aller Zahlen A, B, C usw. oder dessen kleinster Rest gehört zum Exponenten $p-1$. Dies beweisen wir folgendermaßen.

I. Sei g eine Zahl aus $1, 2, 3 \ldots p-1$, welche die Kongruenz $x^{\frac{p-1}{a}} \equiv 1 \,(\mathrm{mod.}\, p)$ *nicht* erfüllt. Denn nicht alle diese Zahlen können eine Kongruenz erfüllen, deren Grad $< p-1$ ist. Ich behaupte nun: Ist die Potenz mit dem Exponenten $\frac{p-1}{a^\alpha}$ von $g \equiv h$, so gehört diese Zahl oder ihr kleinster Rest zum Exponenten a^α.

Denn die Potenz mit dem Exponenten a^α von h ist offenbar zur Potenz mit dem Exponenten $p-1$ von g, *also* zur Eins kongruent. Die Potenz mit dem Exponenten $a^{\alpha-1}$ von h ist dagegen zur Potenz mit dem Exponenten $\frac{p-1}{a}$ von g kongruent, *also* zur Eins inkongruent. Noch weniger können die Potenzen mit den Exponenten $a^{\alpha-2}$, $a^{\alpha-3}$ usw. von h der Eins kongruent sein. Der Exponent der niedrigsten der Eins kongruenten Potenz von h, also der Exponent, zu dem h gehört, muss aber ein Teiler von a^α sein (Artikel 48). Da a^α nur durch sich selbst und niedrigere Potenzen von a teilbar ist, muss a^α der Exponent sein, zu dem h gehört. *Q. E. D.* Ebenso zeigt man, dass es Zahlen gibt, die zu den Exponenten b^β, c^γ usw. gehören.

II. Nehmen wir an, das Produkt aller A, B, C usw. gehöre nicht zum Exponenten $p-1$, sondern zu einem kleineren t. Dann teilt t die Zahl $p-1$ (Artikel 48), also ist $\frac{p-1}{t}$ eine ganze Zahl größer als eins. Offenbar ist dieser Quotient entweder eine der Primzahlen a, b, c usw. oder zumindest durch eine davon teilbar (Artikel 17), *zum Beispiel* durch a. Für die übrigen verläuft der Schluss ebenso.

Somit teilt t die Zahl $\frac{p-1}{a}$, und das Produkt ABC usw. ist auch dann der Eins kongruent, wenn es zur Potenz mit dem Exponenten $\frac{p-1}{a}$ erhoben wird (Artikel 46). Aber auch jede einzelne der Zahlen B, C usw., ausgenommen A, ist zur Potenz mit dem Exponenten $\frac{p-1}{a}$ erhoben der Eins kongruent. Denn die Exponenten b^β, c^γ usw.,

zu denen sie gehören, teilen $\frac{p-1}{a}$. Daher ist

$$A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}} \text{ usw.} \equiv A^{\frac{p-1}{a}} \equiv 1.$$

Der Exponent, zu dem A gehört, muss also $\frac{p-1}{a}$ teilen (Artikel 48), *das heißt*, $\frac{p-1}{a^{\alpha+1}}$ muss ganzzahlig sein. Aber $\frac{p-1}{a^{\alpha+1}} = \frac{b^{\beta}c^{\gamma} \text{ usw.}}{a}$ kann keine ganze Zahl sein (Artikel 15). Unsere Annahme kann daher nicht bestehen; *das heißt*, das Produkt ABC usw. gehört tatsächlich zum Exponenten $p-1$. *Q. E. D.*

Der zweite Beweis scheint etwas länger als der erste, der erste dagegen weniger direkt als der zweite zu sein.

56.

Dieser Satz zeigt besonders deutlich, wie viel Vorsicht in der Zahlentheorie oft nötig ist, damit wir nicht als sicher annehmen, was nicht sicher ist. Der angesehene Lambert erwähnt diesen Satz in der bereits angeführten Abhandlung *Acta Erudit.* 1769, *S.* 127, geht aber nicht einmal darauf ein, dass ein Beweis nötig ist. Niemand außer dem großen Euler hat einen Beweis versucht: *Comment. nov. Ac. Petrop. T.* XVIII zum Jahr 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, S. 85 ff. Man vergleiche besonders Artikel 37, in dem er die Notwendigkeit eines Beweises ausführlicher bespricht. Der Beweis dieses scharfsinnigen Mannes hat jedoch zwei Lücken. Erstens setzt er in Artikel 31 ff. stillschweigend voraus, dass die Kongruenz $x^n \equiv 1$, wenn man seine Überlegungen in unsere Zeichen überträgt, tatsächlich n verschiedene Wurzeln hat, obwohl vorher nur gezeigt war, dass sie nicht *mehr* haben kann. Zweitens hat er die Formel in Artikel 34 nur durch Induktion hergeleitet.

Primitive Wurzeln, Basen, Indizes.

57.

Mit dem berühmten Euler nennen wir die zum Exponenten $p-1$ gehörenden Zahlen *primitive Wurzeln.* Ist also a eine primitive Wurzel, so sind die kleinsten Reste der Potenzen $a, aa, a^3 \ldots a^{p-1}$ alle verschieden. Sie müssen daher sämtliche Zahlen $1, 2, 3, \ldots p-1$ enthalten, da diese ebenso zahlreich sind wie jene kleinsten Reste. Das heißt, jede nicht durch p teilbare Zahl ist zu einer Potenz von a kongruent. Diese bemerkenswerte Eigenschaft ist sehr nützlich und kann die Rechenoperationen mit Kongruenzen erheblich erleichtern, ähnlich wie die Einführung der Logarithmen die gewöhnliche Arithmetik erleichtert. Wir wählen eine beliebige primitive Wurzel a als *Basis*, auf die wir alle nicht durch p teilbaren Zahlen beziehen. Ist $a^e \equiv b \,(\text{mod. } p)$, so nennen wir e den *Index* von b. *Zum Beispiel* entsprechen für den Modul 19, wenn die primitive Wurzel 2 als Basis gewählt wird, einander:

Zahlen	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.
Indizes	0.	1.	13.	2.	16.	14.	6.	3.	8.	17.	12.	15.	5.	7.	11.	4.	10.	9.

Bei gleicher Basis gehören zu jeder Zahl offenbar mehrere Indizes, die aber alle nach dem Modul $p-1$ kongruent sind. Sprechen wir von Indizes, so gelten daher diejenigen als gleichwertig, die nach dem Modul $p-1$ kongruent sind, ebenso wie die Zahlen selbst als gleichwertig gelten, wenn sie nach dem Modul p kongruent sind.

Rechnen mit Indizes.

58.

Die Sätze über Indizes entsprechen genau denen über Logarithmen.

Der Index eines Produkts beliebig vieler Faktoren ist nach dem Modul $p-1$ der Summe der Indizes der einzelnen Faktoren kongruent.

Der Index einer Potenz einer Zahl ist nach dem Modul $p-1$ dem Produkt aus dem Index der gegebenen Zahl und dem Exponenten der Potenz kongruent.

Wegen ihrer Einfachheit lassen wir die Beweise weg.

Will man also eine Tabelle erstellen, aus der die Indizes aller Zahlen für verschiedene Moduln entnommen werden können, so darf man sowohl alle Zahlen über dem Modul als auch alle zusammengesetzten Zahlen weglassen. Ein Beispiel einer solchen Tabelle ist am Ende dieses Werkes als *Tabelle* I beigefügt. In ihrer ersten senkrechten Spalte stehen die Primzahlen und Primzahlpotenzen von 3 bis 97, die als Moduln zu betrachten sind; daneben stehen die jeweils als Basis gewählten Zahlen. Es folgen die Indizes der aufeinanderfolgenden Primzahlen, die jeweils zu fünft durch einen kleinen Zwischenraum getrennt sind. Darüber stehen die Primzahlen in derselben Reihenfolge, sodass sich der Index einer gegebenen Primzahl nach einem gegebenen Modul leicht und zuverlässig finden lässt.

So ist *zum Beispiel* für $p = 67$ der Index von 60, wenn 12 als Basis gewählt wird,

$$\equiv 2\,\mathrm{Ind.}\,2 + \mathrm{Ind.}\,3 + \mathrm{Ind.}\,5 \pmod{66} \equiv 58 + 9 + 39 \equiv 40$$

59.

Der Index eines beliebigen Wertes des Ausdrucks $\frac{a}{b}$ (mod.p.), (Artikel 31) ist nach dem Modul $p-1$ der Differenz der Indizes des Zählers a und des Nenners b kongruent, sofern die Zahlen a, b nicht durch p teilbar sind.

Ein beliebiger Wert sei c. Dann ist $bc \equiv a \pmod{p}$, also

$$\mathrm{Ind.}\,b + \mathrm{Ind.}\,c \equiv \mathrm{Ind.}\,a \pmod{p-1}$$

und damit

$$\mathrm{Ind.}\,c \equiv \mathrm{Ind.}\,a - \mathrm{Ind.}\,b$$

Hat man eine Tabelle, die zu jeder Zahl für jeden Primzahlmodul den Index angibt, und eine weitere, die zu einem gegebenen Index die zugehörige Zahl liefert, so lassen sich alle Kongruenzen ersten Grades sehr leicht lösen. Denn alle lassen sich auf solche mit Primzahlmodul zurückführen (Artikel 30).

Zum Beispiel ergebe sich aus der gegebenen Kongruenz

$$29x + 7 \equiv 0 \pmod{47} \quad \text{so ist} \quad x \equiv \frac{-7}{29} \pmod{47}$$

also

$$\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,-7 - \mathrm{Ind.}\,29 \equiv \mathrm{Ind.}\,40 - \mathrm{Ind.}\,29 \equiv 15 - 43 \equiv 18 \pmod{46}$$

Die Zahl mit dem Index 18 ist 3. Daher ist $x \equiv 3 \pmod{47}$. — Die zweite Tabelle haben wir zwar nicht beigefügt; eine andere kann aber an ihre Stelle treten, wie wir in Abschnitt VI zeigen werden.

Wurzeln der Kongruenz $x^n \equiv A$.

60.

Wie wir in Artikel 31 die Wurzeln der Kongruenzen ersten Grades bezeichnet haben, verwenden wir im Folgenden auch ein Zeichen für die Wurzeln reiner Kongruenzen höheren Grades. So wie $\sqrt[n]{A}$ lediglich eine Wurzel der Gleichung $x^n = A$ bezeichnet, steht nach Hinzufügen des Moduls $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ für jede beliebige Wurzel der Kongruenz $x^n \equiv A \,(\mathrm{mod.}\, p)$. Wir sagen, der Ausdruck $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ habe so viele Werte, wie er nach p inkongruente Werte hat. Denn alle nach p kongruenten Werte sind als gleichwertig anzusehen (Artikel 26). Sind A, B nach p kongruent, so sind die Ausdrücke $\sqrt[n]{A}, \sqrt[n]{B} \,(\mathrm{mod.}\, p)$ offenbar gleichwertig.

Setzt man nun $\sqrt[n]{A} \equiv x \,(\mathrm{mod.}\, p)$, so ist $n \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, A \,(\mathrm{mod.}\, p-1)$. Aus dieser Kongruenz erhält man nach den Regeln des vorigen Abschnitts die Werte von $\mathrm{Ind.}\, x$ und aus ihnen die entsprechenden Werte von x. Dabei hat x offenbar ebenso viele Werte, wie die Kongruenz $n \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, A \,(\mathrm{mod.}\, p-1)$ Wurzeln hat. Somit hat $\sqrt[n]{A}$ nur einen Wert, wenn n zu $p-1$ teilerfremd ist. Haben dagegen die Zahlen $n, p-1$ den größten gemeinsamen Teiler δ, so hat $\mathrm{Ind.}\, x$ genau δ nach $p-1$ inkongruente Werte und damit $\sqrt[n]{A}$ ebenso viele nach p inkongruente Werte, sofern $\mathrm{Ind.}\, A$ durch δ teilbar ist. Gilt diese Bedingung nicht, so hat $\sqrt[n]{A}$ keinen wirklichen Wert.

Beispiel. Gesucht sind die Werte des Ausdrucks $\sqrt[15]{11} \,(\mathrm{mod.}\, 19)$. Man muss also die Kongruenz $15 \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, 11 \equiv 6 \,(\mathrm{mod.}\, 18)$ lösen und findet die drei Werte $\mathrm{Ind.}\, x \equiv 4, 10, 16 \,(\mathrm{mod.}\, 18)$. Ihnen entsprechen die Werte von x, nämlich $6, 9, 4$.

61.

So bequem diese Methode bei vorhandenen Tafeln ist, dürfen wir doch nicht vergessen, dass sie indirekt ist. Es lohnt sich also zu untersuchen, was direkte Methoden leisten können. Hier geben wir die Ergebnisse, die sich aus dem Vorhergehenden gewinnen lassen; alles Weitere, das tiefere Überlegungen verlangt, bleibt Abschnitt VIII vorbehalten. Wir beginnen mit dem einfachsten Fall $A = 1$, suchen also die Wurzeln der Kongruenz $x^n \equiv 1 \,(\mathrm{mod.}\, p)$. Nimmt man eine beliebige primitive Wurzel als Basis, so muss $n \operatorname{Ind.} x \equiv 0 \,(\mathrm{mod.}\, p-1)$ sein. Ist n zu $p-1$ teilerfremd, so hat diese Kongruenz nur eine Wurzel, nämlich $\operatorname{Ind.} x \equiv 0 \,(\mathrm{mod.}\, p-1)$. Also hat *in diesem Fall* $\sqrt[n]{1} \,(\mathrm{mod.}\, p)$ einen einzigen Wert, nämlich $\equiv 1$. Haben dagegen die Zahlen $n, p-1$ den größten gemeinsamen Teiler δ, so lautet die vollständige Lösung der Kongruenz $n \operatorname{Ind.} x \equiv 0 \,(\mathrm{mod.}\, p-1)$: $\operatorname{Ind.} x \equiv 0 \,(\mathrm{mod.}\, \frac{p-1}{\delta})$ (siehe Artikel 29). *Das heißt,* $\operatorname{Ind.} x$ muss nach dem Modul $p-1$ einer der Zahlen

$$0, \frac{p-1}{\delta}. \frac{2(p-1)}{\delta}, \frac{3(p-1)}{\delta}, \ldots . \frac{(\delta-1)(p-1)}{\delta}$$

kongruent sein oder δ nach dem Modul $p-1$ inkongruente Werte haben. Somit hat auch x in diesem Fall δ verschiedene Werte (inkongruent nach dem Modul p). Daraus ergibt sich, dass auch der Ausdruck $\sqrt[\delta]{1}$ genau δ verschiedene Werte hat, deren Indizes mit den eben angegebenen vollständig übereinstimmen. Der Ausdruck $\sqrt[\delta]{1} \,(\mathrm{mod.}\, p)$ ist also mit $\sqrt[n]{1} \,(\mathrm{mod.}\, p)$ gleichwertig: Die Kongruenz $x^\delta \equiv 1 \,(\mathrm{mod.}\, p)$ hat dieselben Wurzeln wie $x^n \equiv 1 \,(\mathrm{mod.}\, p)$. Die erste hat aber einen niedrigeren Grad, falls δ und n ungleich sind.

Beispiel. $\sqrt[15]{1} \,(\mathrm{mod.}\, 19)$ hat drei Werte, da 3 der größte gemeinsame Teiler der Zahlen $15, 18$ ist. Diese sind zugleich die Werte von $\sqrt[3]{1} \,(\mathrm{mod.}\, 19)$, nämlich $1, 7, 11$.

62.

Diese Reduktion hat also den Vorteil, dass wir nur noch diejenigen Kongruenzen der Form $x^n \equiv 1$ lösen müssen, bei denen n ein Teiler von $p-1$ ist. Weiter unten zeigen wir, dass sich Kongruenzen dieser Form stets noch weiter im Grad herabsetzen lassen; die bisherigen Ergebnisse reichen dazu allerdings nicht aus. Einen Fall können wir schon hier erledigen, nämlich $n = 2$. Die Werte des Ausdrucks $\sqrt[2]{1}$ sind offenbar $+1$ und -1, denn mehr als zwei kann er nicht haben. Dabei sind $+1$ und -1 stets inkongruent, außer wenn der Modul $= 2$ ist. In diesem Fall kann $\sqrt[2]{1}$ offensichtlich nur einen Wert haben. Daraus folgt, dass $+1$ und -1 auch die Werte von $\sqrt[2m]{1}$ sind, wenn m zu $\frac{p-1}{2}$ teilerfremd ist. Dies gilt immer dann, wenn der Modul so beschaffen ist, dass $\frac{p-1}{2}$ eine Primzahl ist (außer wenn $p-1 = 2m$ gilt; dann sind sämtliche Zahlen $1, 2, 3 \ldots . p-1$ Wurzeln), *zum Beispiel* für $p = 3, 5, 7, 11, 23, 47, 59, 83, 107$ usw. Als Folgerung sei hier festgehalten, dass der Index von -1 stets $\equiv \frac{p-1}{2} \,(\mathrm{mod.}\, p-1)$ ist, ganz gleich, welche primitive Wurzel als Basis gewählt wird. Denn $2 \operatorname{Ind.}(-1) \equiv 0 \,(\mathrm{mod.}\, p-1)$. Also ist $\operatorname{Ind.}(-1)$ entweder $\equiv 0$ oder $\equiv \frac{p-1}{2} \,(\mathrm{mod.}\, p-1)$. Nun ist aber 0 immer der Index von $+1$, und $+1$ und -1 müssen stets verschiedene Indizes haben (abgesehen vom Fall $p = 2$, den wir hier nicht weiter beachten müssen).

63.

In Artikel 60 haben wir gezeigt, dass der Ausdruck $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ genau δ verschiedene Werte oder gar keinen hat, wenn δ der größte gemeinsame Teiler der Zahlen

$n, p-1$ ist. Wie wir eben die Gleichwertigkeit von $\sqrt[n]{A}$ und $\sqrt[\delta]{A}$ für $A \equiv 1$ gezeigt haben, beweisen wir nun allgemeiner, dass sich der Ausdruck $\sqrt[n]{A}$ stets auf einen anderen Ausdruck $\sqrt[\delta]{B}$ zurückführen lässt, mit dem er gleichwertig ist. Bezeichnen wir einen beliebigen Wert des ersten mit x, so ist $x^n \equiv A$. Nun sei t irgendein Wert von $\frac{\delta}{n} \pmod{p-1}$; dass dieser Ausdruck wirkliche Werte hat, ergibt sich aus Artikel 31. Dann ist $x^{tn} \equiv A^t$, aber $x^{tn} \equiv x^\delta$ wegen $tn \equiv \delta \pmod{p-1}$. Also ist $x^\delta \equiv A^t$, und jeder Wert von $\sqrt[n]{A}$ ist somit auch ein Wert von $\sqrt[\delta]{A^t}$. Sobald $\sqrt[n]{A}$ wirkliche Werte hat, ist dieser Ausdruck daher mit $\sqrt[\delta]{A^t}$ vollständig gleichwertig, da er weder andere noch weniger Werte hat. Hat dagegen $\sqrt[n]{A}$ keinen wirklichen Wert, so kann $\sqrt[\delta]{A^t}$ trotzdem wirkliche Werte haben.

Beispiel. Sucht man die Werte des Ausdrucks $\sqrt[21]{2} \pmod{31}$, so ist der größte gemeinsame Teiler von 21 und 30 gleich 3, und ein Wert von $\frac{3}{21} \pmod{30}$ ist 3. Hat also $\sqrt[21]{2}$ wirkliche Werte, so ist dieser Ausdruck mit $\sqrt[3]{2^3}$ oder $\sqrt[3]{8}$ gleichwertig. Tatsächlich findet man, dass die Werte des letzteren Ausdrucks, nämlich $2, 10.19$, auch dem ersten genügen.

64.

Damit wir diese Rechnung nicht womöglich vergeblich ausführen, brauchen wir eine Regel, die sofort entscheidet, ob $\sqrt[n]{A}$ wirkliche Werte hat oder nicht. Mit einer Indextafel ist dies leicht: Nach Artikel 60 gibt es wirkliche Werte, wenn der Index von A bei einer beliebigen primitiven Wurzel als Basis durch δ teilbar ist; andernfalls gibt es keine. Man kann das aber auch ohne eine solche Tafel feststellen. Setzen wir nämlich den Index von A gleich k, so ist, falls dieser durch δ teilbar ist, auch $\frac{k(p-1)}{\delta}$ durch $p-1$ teilbar, und umgekehrt. Nun ist aber der Index der Zahl $A^{\frac{p-1}{\delta}}$ gleich $\frac{k(p-1)}{\delta}$. Hat also $\sqrt[n]{A} \pmod{p}$ wirkliche Werte, so ist $A^{\frac{p-1}{\delta}}$ der Eins kongruent, andernfalls nicht. Im Beispiel des vorigen Artikels gilt etwa $2^{10} = 1024 \equiv 1 \pmod{31}$, woraus folgt, dass $\sqrt[21]{2} \pmod{31}$ wirkliche Werte hat. Ebenso erfahren wir daraus, dass $\sqrt[2]{-1} \pmod{p}$ immer zwei wirkliche Werte hat, wenn p von der Form $4m+1$ ist, dagegen keinen, wenn p von der Form $4m+3$ ist; denn $(-1)^{2m} = 1$ und $(-1)^{2m+1} = -1$. Diesen schönen Satz, den man gewöhnlich so ausspricht: *Ist p eine Primzahl der Form $4m+1$, so lässt sich eine Quadratzahl aa finden, sodass $aa+1$ durch p teilbar ist; ist dagegen p von der Form $4m-1$, so gibt es eine solche Quadratzahl nicht*, hat Euler auf diese Weise bewiesen, *Comm. nov. Acad. Petrop. T.* XVIII, *p.* 112, für das Jahr 1773. Einen anderen Beweis hatte er schon viel früher gegeben, *Comm. nov. T.* V, *p.* 5, erschienen 1760. In einer früheren Abhandlung, *Comm. nov. T.* IV, *p.* 25, hatte er die Sache noch nicht abgeschlossen. Später gab auch La Grange einen Beweis des Satzes, *Nouveaux Mém. de l'Ac. de Berlin A.* 1775, *p.* 342. Einen weiteren Beweis geben wir im nächsten Abschnitt, wo dieser Gegenstand eigens behandelt wird.

65.

Wir haben gezeigt, wie sich alle Ausdrücke $\sqrt[n]{A} \pmod{p}$ auf solche zurückführen lassen, bei denen n ein Teiler von $p-1$ ist, und haben ein Kriterium dafür gefunden, ob wirkliche Werte existieren. Nun betrachten wir solche Ausdrücke $\sqrt[n]{A} \pmod{p}$, bei denen n ein Teiler von $p-1$ ist, genauer. Zuerst zeigen wir, wie die einzelnen Werte eines Ausdrucks miteinander zusammenhängen; dann geben wir einige Verfahren an, mit denen man oft einen Wert finden kann.

Erstens: Ist $A \equiv 1$ und r einer der n Werte von $\sqrt[n]{1} \pmod{p}$, gilt also $r^n \equiv 1 \pmod{p}$, so sind auch alle Potenzen von r Werte dieses Ausdrucks. Dabei gibt es so viele verschiedene Werte, wie der Exponent angibt, zu dem r gehört (Artikel 48). Gehört also der Wert r zum Exponenten n, so umfassen die Potenzen von r, nämlich $r, r^2, r^3 \ldots . r^n$ (wobei man die letzte durch die *Eins* ersetzen kann), alle Werte des Ausdrucks $\sqrt[n]{1} \pmod{p}$. Welche Hilfsmittel es gibt, um solche zum Exponenten n gehörigen Werte zu finden, erläutern wir in Abschnitt VIII ausführlicher.

Zweitens. Ist A der Eins inkongruent und ein Wert von $\sqrt[n]{A} \pmod{p}$, etwa z, bekannt, so erhält man daraus die übrigen wie folgt. Die Werte von $\sqrt[n]{1}$ seien

$$1,\ r,\ r^2 \ldots r^{n-1}$$

wie eben gezeigt. Dann sind sämtliche Werte von $\sqrt[n]{A}$ die folgenden:

$$z,\ zr,\ zr^2 \ldots . zr^{n-1}$$

Sie alle genügen der Kongruenz $x^n \equiv A$. Setzt man nämlich einen beliebigen von ihnen $\equiv zr^k$, so ist seine Potenz mit dem Exponenten n, nämlich $z^n r^{nk}$, wegen $r^n \equiv 1$ und $z^n \equiv A$ der Zahl A kongruent. Dass sie alle verschieden sind, ergibt sich leicht aus Artikel 23. Mehr Werte als diese, deren Anzahl n ist, kann der Ausdruck $\sqrt[n]{A}$ aber nicht haben. Ist also *zum Beispiel* ein Wert von $\sqrt[2]{A}$ gleich z, so ist der andere $-z$. Schließlich müssen wir daraus folgern, dass man nicht alle Werte von $\sqrt[n]{A}$ finden kann, ohne zugleich sämtliche Werte von $\sqrt[n]{1}$ zu kennen.

66.

Als Zweites wollten wir zeigen, in welchem Fall sich ein Wert von $\sqrt[n]{A} \pmod{p}$ direkt finden lässt; dabei setzen wir voraus, dass n ein Teiler von $p-1$ ist. Dies ist möglich, wenn ein Wert einer Potenz von A kongruent ist. Da dieser Fall recht oft vorkommt, lohnt es sich, etwas dabei zu verweilen. Ein solcher Wert, *falls es einen gibt,* sei z; es gelte also $z \equiv A^k$ und $A \equiv z^n \pmod{p}$. Daraus folgt $A \equiv A^{kn}$. Kennt man also eine Zahl k, für die $A \equiv A^{kn}$ gilt, so ist A^k ein gesuchter Wert. Diese Bedingung ist aber gleichbedeutend mit $1 \equiv kn \pmod{t}$, wobei t den Exponenten bezeichnet, zu dem A gehört (Artikel 46, 48). Damit diese Kongruenz lösbar ist, muss n zu t teilerfremd sein. In diesem Fall gilt $k \equiv \frac{1}{n} \pmod{t}$. Haben dagegen t und n einen gemeinsamen Teiler außer der Eins, so kann kein Wert z einer Potenz von A kongruent sein.

67.

Für diese Lösung müssen wir allerdings t kennen. Sehen wir also, wie man vorgehen kann, wenn diese Zahl unbekannt ist. Zunächst ist leicht einzusehen, dass t ein Teiler von $\frac{p-1}{n}$ sein muss, sofern $\sqrt[n]{A} \pmod{p}$ wirkliche Werte hat, wie wir hier stets voraussetzen. Sei nämlich y ein beliebiger Wert. Dann gilt sowohl $y^{p-1} \equiv 1$ als auch $y^n \equiv A \pmod{p}$. Erhebt man beide Seiten der letzteren Kongruenz zur Potenz mit dem Exponenten $\frac{p-1}{n}$, so erhält man $A^{\frac{p-1}{n}} \equiv 1$. Damit ist $\frac{p-1}{n}$ durch t teilbar (Artikel 48). Ist nun $\frac{p-1}{n}$ zu n teilerfremd, so lässt sich die Kongruenz $kn \equiv 1$ des vorigen Artikels auch nach dem Modul $\frac{p-1}{n}$ lösen. Ein Wert von k, der die Kongruenz nach diesem Modul erfüllt, erfüllt sie offenbar auch nach dem Modul t, der ein Teiler

von $\frac{p-1}{n}$ ist (Artikel 5). Damit ist das Gesuchte gefunden. Ist dagegen $\frac{p-1}{n}$ zu n nicht teilerfremd, so entferne man sämtliche Primfaktoren von $\frac{p-1}{n}$, die zugleich n teilen, aus $\frac{p-1}{n}$. So erhalten wir eine Zahl $\frac{p-1}{nq}$, die zu n teilerfremd ist. Dabei bezeichnet q das Produkt aller entfernten Primfaktoren. Gilt nun die Bedingung aus dem vorigen Artikel, dass t zu n teilerfremd ist, so ist auch t zu q teilerfremd und teilt somit ebenfalls $\frac{p-1}{nq}$. Löst man also die Kongruenz $kn \equiv 1 \,(\mathrm{mod.}\, \frac{p-1}{nq})$ (was möglich ist, da n zu $\frac{p-1}{nq}$ teilerfremd ist), so erfüllt der Wert von k die Kongruenz auch nach dem Modul t, wie verlangt. Das ganze Verfahren besteht darin, eine Zahl zu finden, die an die Stelle des unbekannten t treten kann. Wir müssen uns aber gut merken, dass wir, wenn $\frac{p-1}{n}$ zu n nicht teilerfremd ist, die Bedingung des vorigen Artikels vorausgesetzt haben. Gilt sie nicht, so sind alle Schlüsse falsch. Finden wir beim unbedachten Befolgen der angegebenen Regeln für z einen Wert, dessen Potenz mit dem Exponenten n der Zahl A nicht kongruent ist, so zeigt das, dass die Bedingung nicht gilt und dieses Verfahren überhaupt nicht anwendbar ist.

68.

Aber auch in diesem Fall kann die bereits geleistete Arbeit oft nützlich sein. Es lohnt sich zu untersuchen, wie dieser falsche Wert mit den richtigen zusammenhängt. Nehmen wir also an, die Zahlen k, z seien regelgerecht bestimmt, aber z^n sei nicht $\equiv A \,(\mathrm{mod.}\, p)$. Können wir nun die Werte von $\sqrt[n]{\frac{A}{z^n}} \,(\mathrm{mod.}\, p)$ bestimmen, so erhalten wir durch Multiplikation jedes einzelnen mit z die Werte von $\sqrt[n]{A}$. Ist nämlich v ein Wert von $\sqrt[n]{\frac{A}{z^n}}$, so gilt $(vz)^n \equiv A$. Der Ausdruck $\sqrt[n]{\frac{A}{z^n}}$ ist aber insofern einfacher als $\sqrt[n]{A}$, als $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ meistens zu einem kleineren Exponenten gehört als A. Genauer: Ist der größte gemeinsame Teiler der Zahlen t, q gleich d, so gehört $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ zum Exponenten d. Dies beweist man so. Setzt man den Wert von z ein, so erhält man $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \,(\mathrm{mod.}\, p)$. Nun ist $kn-1$ durch $\frac{p-1}{nq}$ teilbar (voriger Artikel), $\frac{p-1}{n}$ aber durch t (ebenda), oder $\frac{p-1}{nd}$ durch $\frac{t}{d}$. Nach Voraussetzung ist jedoch $\frac{t}{d}$ zu $\frac{q}{d}$ teilerfremd. Also ist auch $\frac{p-1}{nd}$ durch $\frac{tq}{dd}$ teilbar, oder $\frac{p-1}{nq}$ durch $\frac{t}{d}$, und damit auch $kn-1'$ durch $\frac{t}{d}$ sowie $(kn-1)d$ durch t. Daher ist $A^{(kn-1)d} \equiv 1 \,(\mathrm{mod.}\, p)$. Daraus ergibt sich leicht, dass $\frac{A}{z^n}$, zur Potenz mit dem Exponenten d erhoben, der Eins kongruent ist. Dass $\frac{A}{z^n}$ nicht zu einem kleineren Exponenten als d gehören kann, lässt sich zwar leicht beweisen; da wir es aber für unseren Zweck nicht brauchen, verweilen wir nicht dabei. Wir können also sicher sein, dass $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ stets zu einem kleineren Exponenten gehört als A, mit einer einzigen Ausnahme: wenn t ein Teiler von q ist, also $d = t$.

Was bringt es uns aber, dass $\frac{A}{z^n}$ zu einem kleineren Exponenten gehört als A? Es gibt mehr Zahlen, die als A auftreten können, als solche, die als $\frac{A}{z^n}$ auftreten können. Wenn mehrere solche Ausdrücke $\sqrt[n]{A}$ nach demselben Modul auszuwerten sind, gewinnen wir dadurch, dass wir mehrere aus derselben Quelle erhalten können. So können wir *zum Beispiel* stets mindestens einen Wert von $\sqrt[2]{A} \,(\mathrm{mod.}\, 29)$ bestimmen, wenn nur die Werte von $\sqrt[2]{-1} \,(\mathrm{mod.}\, 29)$ (nämlich ± 12) bekannt sind. Aus dem vorigen Artikel ergibt sich leicht, dass sich ein Wert solcher Ausdrücke stets direkt bestimmen lässt, wenn t ungerade ist, und dass d dann $= 2$ ist, wenn t gerade ist. Außer -1 gehört aber keine Zahl zum Exponenten 2.

Beispiele. Gesucht ist $\sqrt[3]{31} \,(\mathrm{mod.}\, 37)$. Hier ist $p-1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$, also $q = 3$. Es muss daher $3k \equiv 1 \,(\mathrm{mod.}\, 4)$ gelten, was man mit $k = 3$ erreicht. Damit ist

$z \equiv 31^3 \,(\mathrm{mod.}\, 37) \equiv 6$, und tatsächlich findet man $6^3 \equiv 31 \,(\mathrm{mod.}\, 37)$. Sind die Werte von $\sqrt[3]{1} \,(\mathrm{mod.}\, 37)$ bekannt, so lassen sich auch die übrigen Werte von $\sqrt[3]{6}$ bestimmen. Jene sind $1, 10, 26$. Multipliziert man 6 mit ihnen, so erhält man die übrigen Werte $\equiv 23$ und 8.

Sucht man dagegen einen Wert von $\sqrt[2]{3} \,(\mathrm{mod.}\, 37)$, so ist $n = 2$, $\frac{p-1}{n} = 18$, also $q = 2$. Daher muss $2k \equiv 1 \,(\mathrm{mod.}\, 9)$ gelten, woraus $k \equiv 5 \,(\mathrm{mod.}\, 9)$ folgt. Somit ist $z \equiv 3^5 \equiv 21 \,(\mathrm{mod.}\, 37)$. Doch 21^2 ist nicht $\equiv 3$, sondern $\equiv 34$. Nun ist aber $\frac{3}{34} \,(\mathrm{mod.}\, 37) \equiv -1$ und $\sqrt[2]{-1} \,(\mathrm{mod.}\, 37) \equiv \pm 6$, woraus man die richtigen Werte $\pm 6 \,.\, 21 \equiv \pm 15$ erhält.

Das ist etwa alles, was wir hier über das Auswerten solcher Ausdrücke mitteilen können. Direkte Methoden werden offenbar oft recht langwierig. Dieser Nachteil betrifft aber fast alle direkten Methoden in der Zahlentheorie; deshalb wollten wir es nicht versäumen zu zeigen, was sie hier leisten können. Auch ist anzumerken, dass es nicht zu unserem Vorhaben gehört, die besonderen Kunstgriffe einzeln zu erläutern, die sich Geübten häufig von selbst anbieten.

Zusammenhang der Indizes in verschiedenen Systemen.

69.

Wir kehren nun zu den Wurzeln zurück, die wir primitive genannt haben. Wir haben gezeigt, dass bei jeder primitiven Wurzel als Basis alle Zahlen, deren Indizes zu $p-1$ teilerfremd sind, ebenfalls primitive Wurzeln sind, und keine anderen. Damit ergibt sich zugleich unmittelbar die Anzahl der primitiven Wurzeln; siehe Artikel 53. Welche primitive Wurzel wir als Basis wählen, steht uns im Allgemeinen frei. Also kann es auch hier, wie beim Rechnen mit Logarithmen, gewissermaßen verschiedene Systeme geben[*)]. Sehen wir, wie diese zusammenhängen. Seien a, b zwei primitive Wurzeln und m eine weitere Zahl. Wählt man a als Basis, so sei der Index von $b \equiv \beta$ und der Index von $m \equiv \mu \,(\mathrm{mod.}\, p-1)$. Wählt man dagegen b als Basis, so sei der Index von $a \equiv \alpha$ und der von $m \equiv \nu \,(\mathrm{mod.}\, p-1)$. Dann ist $\alpha\beta \equiv 1 \,(\mathrm{mod.}\, p-1)$. Denn $a^\beta \equiv b$, also nach Voraussetzung $a^{\alpha\beta} \equiv b^\alpha \equiv a \,(\mathrm{mod.}\, p)$, und damit $\alpha\beta \equiv 1 \,(\mathrm{mod.}\, p-1)$. Ebenso findet man $\nu \equiv \alpha\mu$ und $\mu \equiv \beta\nu \,(\mathrm{mod.}\, p-1)$. Hat man also eine Indextafel für die Basis a, so lässt sie sich leicht in eine Tafel zur Basis b umwandeln. Ist nämlich bei der Basis a der Index von $b \equiv \beta$, so ist bei der Basis b der Index von $a \equiv \frac{1}{\beta} \,(\mathrm{mod.}\, p-1)$. Multipliziert man sämtliche Indizes der Tafel mit dieser Zahl, so erhält man alle Indizes zur Basis b.

70.

Eine gegebene Zahl kann zwar verschiedene Indizes erhalten, wenn man verschiedene primitive Wurzeln als Basis nimmt; doch haben sie alle mit $p-1$ denselben größten gemeinsamen Teiler. Ist nämlich bei der Basis a der Index der gegebenen Zahl gleich m und bei der Basis b gleich n, und nimmt man an, die größten gemeinsamen Teiler dieser Indizes mit $p-1$, nämlich μ, ν, seien ungleich, so ist einer größer, etwa $\mu > \nu$. Damit teilt μ die Zahl n nicht. Bezeichnet man aber den Index von a bei der Basis b mit α, so gilt nach dem vorigen Artikel $n \equiv \alpha m \,(\mathrm{mod.}\, p-1)$. Also teilt μ auch n, *entgegen der Annahme.*

[*)] Der Unterschied besteht allerdings darin, dass es bei den Logarithmen unendlich viele Systeme gibt, hier dagegen nur so viele wie primitive Wurzeln. Kongruente Basen erzeugen offenbar dasselbe System.

Dass dieser größte gemeinsame Teiler der Indizes einer gegebenen Zahl und von $p-1$ nicht von der Basis abhängt, ergibt sich auch daraus, dass er gleich $\frac{p-1}{t}$ ist. Dabei bezeichnet t den Exponenten, zu dem die Zahl gehört, um deren Indizes es geht. Ist nämlich der Index für irgendeine Basis gleich k, so ist t die kleinste Zahl, mit der man k multiplizieren muss, um ein Vielfaches von $p-1$ zu erhalten, abgesehen von null (siehe Artikel 48, 58). Sie ist also der kleinste Wert von $\frac{0}{k} \pmod{p-1}$ außer null. Dass dieser dem größten gemeinsamen Teiler der Zahlen k und $p-1$ gleich ist, ergibt sich ohne Schwierigkeit aus Artikel 29.

71.

Ferner lässt sich leicht zeigen, dass man die Basis stets so wählen kann, dass eine zum Exponenten t gehörige Zahl jeden vorgegebenen Index erhält, dessen größter gemeinsamer Teiler mit $p-1$ den Wert $= \frac{p-1}{t}$ hat. Bezeichnen wir diesen Teiler kurz mit d. Der gewünschte Index sei $\equiv dm$, und wenn eine beliebige primitive Wurzel a als Basis genommen wird, sei der Index der gegebenen Zahl $\equiv dn$. Dann sind m, n zu $\frac{p-1}{d}$ oder t teilerfremd. Ist nun ε ein Wert von $\frac{dn}{dm} \pmod{p-1}$ und zugleich zu $p-1$ teilerfremd, so ist a^ε eine primitive Wurzel. Nimmt man sie als Basis, so erhält die gegebene Zahl den Index dm, wie verlangt (denn $a^{\varepsilon dm} \equiv a^{dn} \equiv$ der gegebenen Zahl). Dass aber $\frac{dn}{dm} \pmod{p-1}$ zu $p-1$ teilerfremde Werte hat, beweist man wie folgt. Dieser Ausdruck ist mit $\frac{n}{m} \pmod{\frac{p-1}{d}}$ oder $\frac{n}{m} \pmod{t}$ gleichwertig; siehe Artikel 31, 2. Alle seine Werte sind zu t teilerfremd. Hätte nämlich ein Wert e einen gemeinsamen Teiler mit t, so müsste dieser auch me teilen und damit auch n, dem me nach t kongruent ist. Das widerspricht der Voraussetzung, dass n zu t teilerfremd ist. Teilen also sämtliche Primteiler von $p-1$ auch t, so sind *alle* Werte von $\frac{n}{m} \pmod{t}$ zu $p-1$ teilerfremd, und ihre Anzahl ist $= d$. Enthält dagegen $p-1$ noch andere Primteiler f, g, h usw., die t nicht teilen, so wähle man irgendeinen Wert und schreibe $\frac{n}{m} \pmod{t} \equiv e$. Da nun sämtliche Zahlen t, f, g, h usw. paarweise teilerfremd sind, lässt sich eine Zahl ε finden, die nach t der Zahl e, nach f, g, h usw. dagegen beliebigen zu diesen jeweils teilerfremden Zahlen kongruent ist (Artikel 32). Eine solche Zahl ist durch keinen Primfaktor von $p-1$ teilbar und daher zu $p-1$ teilerfremd, wie verlangt. Schließlich ergibt sich aus der Kombinationslehre ohne Schwierigkeit die Anzahl $= \frac{p-1 \,.\, f-1 \,.\, g-1 \,.\, h-1 \,.\, \text{usw.}}{t \,.\, f \,.\, g \,.\, h \,.\, \text{usw.}}$ dieser Werte. Damit diese Abschweifung nicht zu umfangreich wird, lassen wir den Beweis weg, da er für unseren Zweck nicht besonders nötig ist.

Basen für besondere Zwecke.

72.

Welche primitive Wurzel als Basis gewählt wird, ist im Allgemeinen völlig beliebig. Manchmal bieten aber bestimmte Basen besondere Vorteile gegenüber anderen. In Tafel I haben wir stets die Zahl 10 als Basis gewählt, wenn sie eine primitive Wurzel war. Andernfalls haben wir die Basis immer so bestimmt, dass der Index von 10 möglichst klein wurde, *das heißt* $= \frac{p-1}{t}$. Dabei bezeichnet t den Exponenten, zu dem 10 gehört. Was wir dadurch gewinnen, zeigen wir in Abschnitt VI, wo dieselbe Tafel noch für andere Zwecke verwendet wird. Da aber, wie aus dem vorigen Artikel hervorgeht, auch hier noch eine Wahl bleiben kann, haben wir eine feste Regel getroffen:

Von allen primitiven Wurzeln, die das Verlangte leisten, haben wir stets die *kleinste* als Basis gewählt. So hat für $p = 73$, wobei $t = 8$ und $d = 9$ ist, a^{ε} genau $\frac{72 \cdot 2}{8 \cdot 3}$, *das heißt* 6 Werte, nämlich $5, 14, 20, 28, 39, 40$. Wir haben also den kleinsten, 5, als Basis genommen.

Ein Verfahren zum Finden primitiver Wurzeln.

73.

Die Methoden zum Finden primitiver Wurzeln beruhen größtenteils auf Probieren. Verbindet man das, was wir in Artikel 55 gezeigt haben, mit dem, was wir weiter unten zur Lösung der Kongruenz $x^n \equiv 1$ angeben, so hat man fast alles, was direkte Methoden leisten können. Euler räumt in *Opusc. Analyt. T.* I, *p.* 152 ein, dass es äußerst schwierig scheine, diese Zahlen zu bestimmen, und dass ihre Natur zu den tiefsten Geheimnissen der Zahlen gehöre. Durch Probieren lassen sie sich aber wie folgt recht bequem bestimmen. Geübte werden die langwierige Rechnung mit verschiedenen besonderen Kunstgriffen abkürzen können; diese lernt man durch Übung viel schneller als durch Regeln.

1^0. Man wähle eine beliebige zu p (so bezeichnen wir stets den Modul) teilerfremde Zahl a. Meist verkürzt es die Rechnung, eine möglichst kleine Zahl zu nehmen, *zum Beispiel* 2. Dann bestimme man ihre Periode (Artikel 46), *das heißt* die kleinsten Reste ihrer Potenzen, bis man eine Potenz a^t erreicht, deren kleinster Rest 1 ist[*)]. Ist nun $t = p - 1$, so ist a eine primitive Wurzel.

2^0. Ist dagegen $t < p-1$, so nehme man eine andere Zahl b, die in der Periode von a nicht vorkommt, und bestimme ebenso ihre Periode. Bezeichnet man den Exponenten, zu dem b gehört, mit u, so erkennt man leicht, dass u weder gleich t noch ein echter Teiler davon sein kann. In beiden Fällen wäre nämlich $b^t \equiv 1$, was unmöglich ist, da die Periode von a alle Zahlen umfasst, deren Potenz mit dem Exponenten t der Eins kongruent ist (Artikel 53). Ist $u = p - 1$, so ist b eine primitive Wurzel. Ist u zwar nicht $= p - 1$, aber doch ein Vielfaches von t, so kennen wir nun eine Zahl, die zu einem größeren Exponenten gehört, und sind unserem Ziel näher: eine Zahl zu finden, die zum *größten* Exponenten gehört. Ist u weder $= p - 1$ noch ein Vielfaches von t, so können wir trotzdem eine Zahl finden, deren Exponent größer als t, u ist, nämlich gleich dem kleinsten gemeinsamen Vielfachen von t, u. Dieses sei $= y$. Man zerlege y in zwei teilerfremde Faktoren m, n, von denen einer t, der andere u teilt[†)]. Man bilde nun die Potenz mit dem Exponenten $\frac{t}{m}$ von a, setze sie $\equiv A$, und die Potenz mit dem Exponenten $\frac{u}{n}$ von b, die man $\equiv B \pmod{p}$ setze. Das Produkt AB gehört dann zum Exponenten n. Denn offenbar gehört A zum Exponenten m und B zum Exponenten n. Also gehört das Produkt AB zu mn, weil m, n teilerfremd sind. Das lässt sich genauso beweisen wie in Artikel 55, II.

3^0. Ist nun $y = p - 1$, so ist AB eine primitive Wurzel. Andernfalls muss man wie zuvor eine andere Zahl nehmen, die in der Periode von AB nicht vorkommt. Diese ist entweder eine primitive Wurzel oder gehört zu einem größeren Exponenten als y, oder man kann wenigstens mit ihrer Hilfe wie zuvor eine Zahl finden, die zu einem

[*)] Man sieht unmittelbar, dass die Potenzen selbst nicht bekannt sein müssen. Denn der kleinste Rest jeder Potenz lässt sich leicht aus dem kleinsten Rest der vorigen gewinnen.

[†)] Wie dies möglich ist, ergibt sich leicht aus Artikel 18. Man zerlege y in verschiedene Primzahlen oder Potenzen verschiedener Primzahlen. Jeder dieser Faktoren teilt eine der Zahlen t, u oder auch beide. Man ordne jeden der Zahl t oder der Zahl u zu, je nachdem, welche er teilt. Teilt er beide, so ist die Zuordnung beliebig. Das Produkt der t zugeordneten Faktoren sei $= m$, das Produkt der übrigen $= n$. Dann erkennt man leicht, dass m die Zahl t, n die Zahl u teilt und $mn = y$ gilt.

größeren Exponenten als y gehört. Da die Zahlen, die man durch Wiederholen dieses Verfahrens erhält, zu stetig wachsenden Exponenten gehören, findet man schließlich eine Zahl, die zum *größten* Exponenten gehört, *das heißt* eine primitive Wurzel, *wie verlangt.*

74.

Ein Beispiel macht diese Regeln deutlicher. Sei $p = 73$, und gesucht sei eine primitive Wurzel dafür. Versuchen wir zuerst die Zahl 2, deren Periode lautet:

1. 2. 4. 8. 16. 32. 64. 55. 37. 1 usw.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9 usw.

Da schon die Potenz mit dem Exponenten 9 der Eins kongruent ist, ist 2 keine primitive Wurzel. Man versuche eine andere Zahl, die in der Periode von 2 nicht vorkommt, *zum Beispiel* 3, mit der Periode

1. 3. 9. 27. 8. 24. 72. 70. 64. 46. 65. 49. 1 usw.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12 usw.

Also ist auch 3 keine primitive Wurzel. Das kleinste gemeinsame Vielfache der Exponenten, zu denen $2, 3$ gehören, *also* der Zahlen $9, 12$, ist aber 36. Nach den Regeln des vorigen Artikels zerlegt man es in die Faktoren 9 und 4. Man muss also 2 zur Potenz mit dem Exponenten $\frac{9}{9}$ erheben, *das heißt* die Zahl 2 selbst beibehalten, dagegen 3 zur Potenz mit dem Exponenten 3 erheben. Ihr Produkt ist 54 und gehört somit zum Exponenten 36. Berechnet man schließlich die Periode von 54 und versucht erneut eine darin nicht enthaltene Zahl, *zum Beispiel* 5, so findet man, dass diese eine primitive Wurzel ist.

Verschiedene Sätze über Perioden und primitive Wurzeln.

75.

Bevor wir diesen Gegenstand verlassen, geben wir einige Sätze an, die wegen ihrer Einfachheit Beachtung verdienen dürften.

Das Produkt aller Glieder der Periode einer beliebigen Zahl ist $\equiv 1$*, wenn ihre Anzahl, also der Exponent, zu dem die Zahl gehört, ungerade ist, und* $\equiv -1$*, wenn dieser Exponent gerade ist.*

Beispiel. Für den Modul 13 besteht die Periode der Zahl 5 aus den Gliedern $1, 5, 12, 8$, deren Produkt $480 \equiv -1 \pmod{13}$ ist.

Nach demselben Modul besteht die Periode der Zahl 3 aus den Gliedern $1, 3, 9$, deren Produkt $27 \equiv 1 \pmod{13}$ ist.

Beweis. Der Exponent, zu dem die Zahl gehört, sei t, ihr Index $\frac{p-1}{t}$. Bei geeigneter Wahl der Basis ist dies stets möglich (Artikel 71). Dann ist der Index des Produkts aller Periodenglieder

$$\equiv (1 + 2 + 3 + \text{usw.} + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$$

also $\equiv 0 \,(\mathrm{mod.}\, p-1)$, wenn t ungerade ist, und $\equiv \frac{p-1}{2}$, wenn t gerade ist. Im ersten Fall ist daher das Produkt $\equiv 1 \,(\mathrm{mod.}\, p)$, im zweiten $\equiv -1 \,(\mathrm{mod.}\, p)$ (Artikel 62). *Q. E. D.*

76.

Ist die Zahl im vorigen Satz eine primitive Wurzel, so umfasst ihre Periode sämtliche Zahlen $1, 2, 3. \ldots . p-1$, deren Produkt daher stets $\equiv -1$ ist (denn $p-1$ ist stets gerade, mit der einzigen Ausnahme $p = 2$, in der -1 und $+1$ gleichwertig sind). Diesen schönen Satz, den man gewöhnlich so ausspricht: *Das Produkt aller Zahlen unterhalb einer gegebenen Primzahl, um eins vermehrt, ist durch diese Primzahl teilbar*, hat Waring zuerst angegeben und Wilson, Esq., zugeschrieben, *Meditt. algebr. Ed.* 3, *p.* 380. Doch keiner von beiden konnte ihn beweisen. Waring räumt ein, dass der Beweis umso schwieriger scheine, als sich keine *Bezeichnung* erfinden lasse, die eine Primzahl ausdrücke. — Unserer Ansicht nach sollte man solche Wahrheiten aber eher aus Begriffen als aus Bezeichnungen gewinnen. Später gab La Grange einen Beweis, *Nouv. Mém. de l'Ac. de Berlin,* 1771. Er beruht auf der Betrachtung der Koeffizienten, die beim Ausmultiplizieren des Produkts

$$x + 1.\, x + 2.\, x + 3. \ldots . \, x + p - 1$$

entstehen. Setzt man nämlich dieses Produkt

$$\equiv x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{usw.} + Mx + N$$

so sind die Koeffizienten A, B usw. M durch p teilbar; N ist dagegen $= 1.2.3. \ldots . \, p-1$. Für $x = 1$ ist das Produkt nun durch p teilbar, dann aber $\equiv 1 + N \,(\mathrm{mod.}\, p)$. Also muss $1 + N$ durch p teilbar sein.

Schließlich gab Euler in *Opusc. analyt. T.* I, *p.* 329 einen Beweis, der mit dem hier vorgetragenen übereinstimmt. Wenn solche Männer diesen Satz ihrer Überlegungen wert fanden, hoffen wir, dass man uns einen weiteren Beweis nicht verübeln wird.

77.

Ist nach dem Modul p das Produkt zweier Zahlen a, b der Eins kongruent, so nennen wir die Zahlen a, b mit Euler *Partner*. Nach dem vorigen Abschnitt hat dann jede positive Zahl unter p genau einen positiven Partner unter p. Unter den Zahlen $1, 2, 3. \ldots . \, p-1$ sind, wie man leicht zeigt, nur 1 und $p-1$ ihre eigenen Partner. Denn solche Zahlen sind Wurzeln der Kongruenz $xx \equiv 1$. Da diese zweiten Grades ist, kann sie nicht mehr als zwei Wurzeln haben, *also* keine anderen als 1 und $p-1$. Lässt man diese beiden weg, so sind die übrigen Zahlen $2.3. \ldots . \, p-2$ paarweise Partner. Ihr Produkt ist daher $\equiv 1$, also das Produkt aller Zahlen $1, 2, 3. \ldots p-1 \equiv p-1$ oder $\equiv -1$. *Q. E. D.*

Zum Beispiel bilden für $p = 13$ die Zahlen $2, 3, 4. \ldots . \, 11$ folgende Paare: 2 mit 7; 3 mit 9; 4 mit 10; 5 mit 8; 6 mit 11. Denn $2.7 \equiv 1$; $3.9 \equiv 1$ usw. Damit ist $2.3.4. \ldots . \, 11 \equiv 1$, also $1.2.3. \ldots . \, 12 \equiv -1$.

78.

Man kann den Wilsonschen Satz aber allgemeiner so formulieren: *Das Produkt aller Zahlen, die kleiner als eine beliebige gegebene Zahl A und zu ihr teilerfremd sind, ist nach A der negativ oder positiv genommenen Eins kongruent.* Negativ nimmt man die Eins, wenn A von der Form p^m oder $2p^m$ ist, wobei p eine von 2 verschiedene Primzahl bezeichnet, und außerdem für $A = 4$; in allen übrigen Fällen positiv. Der von Wilson angegebene Satz ist im ersten Fall enthalten. — *Zum Beispiel* ist für $A = 15$ das Produkt der Zahlen $1, 2, 4, 7, 8, 11, 13, 14 \equiv 1 \,(\mathrm{mod.}\, 15)$. Der Kürze wegen fügen wir keinen Beweis hinzu. Wir bemerken nur, dass er wie im vorigen Artikel geführt werden kann, außer dass die Kongruenz $xx \equiv 1$ mehr als zwei Wurzeln haben kann, was besondere Überlegungen erfordert. Auch aus der Betrachtung der Indizes könnte man einen Beweis gewinnen, ähnlich wie in Artikel 75, wenn man das hinzunimmt, was wir gleich über nichtprime Moduln vortragen werden.

79.

Wir kehren zur Aufzählung weiterer Sätze zurück (Artikel 75).

Die Summe aller Glieder der Periode einer beliebigen Zahl ist $\equiv 0$, wie im Beispiel aus Artikel 75: $1 + 5 + 12 + 8 = 26 \equiv 0 \,(\mathrm{mod.}\, 13)$.

Beweis. Die Zahl, deren Periode wir betrachten, sei $= a$, und der Exponent, zu dem sie gehört, $= t$. Dann ist die Summe sämtlicher Periodenglieder

$$\equiv 1 + a + aa + a^3 + \text{usw.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \,(\mathrm{mod.}\, p)$$

Nun ist aber $a^t - 1 \equiv 0$. Daher ist diese Summe stets $\equiv 0$ (Artikel 22), außer wenn $a - 1$ durch p teilbar ist, also $a \equiv 1$. Diesen Fall müssen wir somit ausnehmen, wenn wir auch ein einziges Glied eine *Periode* nennen wollen.

80.

Das Produkt aller primitiven Wurzeln ist $\equiv 1$, mit der einzigen Ausnahme $p = 3$; dann gibt es nur eine primitive Wurzel, nämlich 2.

Beweis. Nimmt man eine beliebige primitive Wurzel als Basis, so sind die Indizes aller primitiven Wurzeln die zu $p - 1$ teilerfremden Zahlen, die kleiner als diese Zahl sind. Deren Summe, *also* der Index des Produkts aller primitiven Wurzeln, ist $\equiv 0 \,(\mathrm{mod.}\, p-1)$, und somit das Produkt $\equiv 1 \,(\mathrm{mod.}\, p)$. Denn ist k zu $p-1$ teilerfremd, so offenbar auch $p - 1 - k$ zu $p - 1$. Also bilden je zwei zu $p - 1$ teilerfremde Zahlen eine durch $p - 1$ teilbare Summe. (Dabei kann k niemals gleich $p - 1 - k$ sein, außer für $p - 1 = 2$, also $p = 3$, welchen Fall wir ausgenommen haben. In allen übrigen Fällen ist $\frac{p-1}{2}$ offenbar zu $p - 1$ nicht teilerfremd.)

81.

Die Summe aller primitiven Wurzeln ist entweder $\equiv 0$ (wenn $p - 1$ durch eine *Quadratzahl* teilbar ist) *oder* $\equiv \pm 1 \,(mod.p)$ (wenn $p - 1$ ein Produkt verschiedener Primzahlen ist; bei gerader Anzahl nimmt man das positive, bei ungerader das negative Vorzeichen).

Beispiele. 1^0 Für $p = 13$ sind die primitiven Wurzeln $2, 6, 7, 11$, deren Summe $26 \equiv 0 \,(\mathrm{mod.}\, 13)$ ist.

2^0 Für $p = 11$ sind die primitiven Wurzeln $2, 6, 7, 8$, deren Summe $23 \equiv +1 \pmod{11}$ ist.

3^0 Für $p = 31$ sind die primitiven Wurzeln $3, 11, 12, 13, 17. 21, 22, 24$, deren Summe $123 \equiv -1 \pmod{31}$ ist.

Beweis. Oben haben wir gezeigt (Artikel 55, II): Ist $p - 1 = a^\alpha b^\beta c^\gamma$ usw. (wobei a, b, c usw. verschiedene Primzahlen bezeichnen), und sind A, B, C usw. beliebige Zahlen, die zu den jeweiligen Exponenten $a^\alpha, b^\beta, c^\gamma$ usw. gehören, so stellen sämtliche Produkte ABC usw. primitive Wurzeln dar. Leicht lässt sich auch zeigen, dass sich jede primitive Wurzel durch ein solches Produkt darstellen lässt, und zwar auf genau eine Weise*).

Diese Produkte können also an die Stelle der primitiven Wurzeln selbst treten. Da in ihnen alle Werte von A mit allen Werten von B usw. zu verbinden sind, ist die Summe aller Produkte gleich dem Produkt aus der Summe aller Werte von A, der Summe aller Werte von B, der Summe aller Werte von C usw., wie aus der Kombinationslehre bekannt ist. Bezeichnen wir alle Werte von A; B usw. mit A, A', A'' usw.; B, B', B'' usw. usw., so ist die Summe aller primitiven Wurzeln

$$\equiv (A + A' + \text{usw.})(B + B' + \text{usw.})\text{usw.}$$

Nun behaupte ich: Ist der Exponent $\alpha = 1$, so ist die Summe $A + A' + A'' + \text{usw.} \equiv -1 \pmod{p}$; ist dagegen $\alpha > 1$, so ist diese Summe $\equiv 0$. Entsprechendes gilt für die übrigen Exponenten β, γ usw. Sobald dies bewiesen ist, liegt die Wahrheit unseres Satzes auf der Hand. Ist nämlich $p-1$ durch eine Quadratzahl teilbar, so ist einer der Exponenten α, β, γ usw. größer als eins. Damit ist einer der Faktoren, deren Produkt der Summe aller primitiven Wurzeln kongruent ist, $\equiv 0$, also auch das Produkt selbst. Ist dagegen $p - 1$ durch keine Quadratzahl teilbar, so sind alle Exponenten α, β, γ usw. $= 1$. Die Summe aller primitiven Wurzeln ist dann einem Produkt aus ebenso vielen Faktoren, jeder $\equiv -1$, kongruent, wie es Zahlen a, b, c usw. gibt. Sie ist also $\equiv \pm 1$, je nachdem, ob deren Anzahl gerade oder ungerade ist. Die Behauptungen beweist man wie folgt.

1^0. Ist $\alpha = 1$ und gehört die Zahl A zum Exponenten a, so sind die übrigen zu diesem Exponenten gehörigen Zahlen $A^2, A^3 \ldots . A^{a-1}$. Nun ist

$$1 + A + A^2 + A^3 \ldots . + A^{a-1}$$

die Summe einer vollständigen Periode, also $\equiv 0$ (Artikel 79). Somit ist

$$A + A^2 + A^3 \ldots . + A^{a-1} \equiv -1$$

2^0. Ist dagegen $\alpha > 1$ und gehört die Zahl A zum Exponenten a^α, so erhält man die übrigen zu diesem Exponenten gehörigen Zahlen, indem man aus

*) Man bestimme die Zahlen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ usw. so, dass $\mathfrak{a} \equiv 1 \pmod{a^\alpha}$ und $\equiv 0 \pmod{b^\beta c^\gamma \text{usw.}}$; $\mathfrak{b} \equiv 1 \pmod{b^\beta}$ und $\equiv 0 \pmod{a^\alpha c^\gamma \text{usw.}}$ usw. gilt (siehe Artikel 32). Dann wird $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \text{usw.} \equiv 1 \pmod{p-1}$ (Artikel 19). Soll nun eine beliebige primitive Wurzel r als Produkt ABC usw. dargestellt werden, so nehme man $A \equiv r^{\mathfrak{a}}, B \equiv r^{\mathfrak{b}}, C \equiv r^{\mathfrak{c}}$ usw. Dabei gehört A zum Exponenten a^α, B zum Exponenten b^β usw. Das Produkt aller A, B, C usw. ist $\equiv r \pmod{p}$. Schließlich erkennt man leicht, dass sich A, B, C usw. nicht anders bestimmen lassen.

$A^2, A^3, A^4 \ldots . A^{a^\alpha - 1}$ die Potenzen A^a, A^{2a}, A^{3a} usw. weglässt; siehe Artikel 53. Ihre Summe ist daher

$$\equiv 1 + A + A^2 \ldots . + A^{a^\alpha - 1} - (1 + A^a + A^{2a} \ldots . + A^{a^\alpha - a})$$

also der Differenz zweier Perioden kongruent und somit $\equiv 0$. *Q. E. D.*

Moduln, die Potenzen von Primzahlen sind.

82.

Alles bisher Vorgetragene beruht auf der Annahme, dass der Modul eine Primzahl ist. Es bleibt der Fall, dass eine zusammengesetzte Zahl als Modul genommen wird. Hier treten aber weder so schöne Eigenschaften wie im vorigen Fall hervor, noch braucht man besondere Kunstgriffe, um sie zu finden. Vielmehr lässt sich fast alles allein durch Anwenden der vorigen Grundsätze gewinnen. Jede Einzelheit auszubreiten wäre daher unnötig und ermüdend. Wir erläutern also kurz, was dieser Fall mit dem vorigen gemeinsam hat und was ihm eigen ist.

83.

Die Sätze der Artikel 45–48 sind bereits allgemein bewiesen. Den Satz aus Artikel 49 muss man jedoch wie folgt ändern:

Bezeichnet f die Anzahl der zu m teilerfremden und unter m liegenden Zahlen, gilt also $f = \phi m$ (Artikel 38), so ist der Exponent t der niedrigsten Potenz einer gegebenen zu m teilerfremden Zahl a, die nach dem Modul m der Eins kongruent ist, entweder $= f$ oder ein echter Teiler dieser Zahl.

Der Beweis aus Artikel 49 gilt auch hier, wenn man überall p durch m, $p - 1$ durch f und die Zahlen $1, 2, 3, \ldots . p - 1$ durch die zu m teilerfremden, unter m liegenden Zahlen ersetzt. Wir verweisen den Leser daher dorthin. Die übrigen dort erwähnten Beweise (Artikel 50, 51) lassen sich dagegen nicht ohne erhebliche Umwege auf diesen Fall anwenden. — Bei den folgenden Sätzen, Artikel 52 und weiter, tritt aber ein großer Unterschied auf zwischen Moduln, die Potenzen von Primzahlen sind, und solchen, die sich durch mehrere Primzahlen teilen lassen. Wir betrachten daher zuerst die Moduln der ersten Art für sich.

84.

Ist der Modul $m = p^n$, wobei p eine Primzahl bezeichnet, so gilt $f = p^{n-1}(p - 1)$ (Artikel 38). Wendet man die Untersuchungen aus Artikel 53, 54 mit den im vorigen Artikel angegebenen Änderungen auf diesen Fall an, so zeigt sich, dass alles dort Bewiesene auch hier gilt, wenn zuvor bewiesen wäre, dass eine Kongruenz der Form $x^t - 1 \equiv 0 \,(\mathrm{mod.}\, p^n)$ nicht mehr als t verschiedene Wurzeln haben kann. Für einen Primzahlmodul haben wir dies aus dem allgemeineren Satz von Artikel 43 abgeleitet. Dieser gilt aber in seinem ganzen Umfang nur für Primzahlmoduln und ist daher hier nicht anwendbar. Trotzdem beweisen wir den Satz für diesen besonderen Fall durch ein eigenes Verfahren. Weiter unten, in Abschnitt VIII, zeigen wir, wie man dasselbe leichter findet.

85.

Wir wollen folgenden Satz beweisen:

Ist der größte gemeinsame Teiler der Zahlen t und $p^{n-1}(p-1)$ gleich e, so hat die Kongruenz $x^t \equiv 1\,(mod.p^n)$ genau e verschiedene Wurzeln.

Sei $e = kp^\nu$, sodass k den Faktor p nicht enthält und somit die Zahl $p-1$ teilt. Dann hat die Kongruenz $x^t \equiv 1$ nach dem Modul p genau k verschiedene Wurzeln. Bezeichnen wir sie mit A, B, C usw., so muss jede Wurzel derselben Kongruenz nach dem Modul p^n nach p einer der Zahlen A, B, C usw. kongruent sein. Nun zeigen wir, dass die Kongruenz $x^t \equiv 1.\,(\mathrm{mod.}\,p^n)$ genau p^ν Wurzeln hat, die A, ebenso viele, die B usw. nach dem Modul p kongruent sind. Damit ist die Anzahl aller Wurzeln kp^ν oder e, wie behauptet. Den Beweis führen wir so: *Zuerst* zeigen wir, dass mit einer Wurzel α, die A nach dem Modul p kongruent ist, auch

$$\alpha + p^{n-\nu},\ \alpha + 2p^{n-\nu},\ \alpha + 3p^{n-\nu}, \ldots . \alpha + (p^\nu - 1)p^{n-\nu}$$

Wurzeln sind. *Zweitens* können unter den Zahlen, die A nach dem Modul p kongruent sind, nur die von der Form $\alpha + hp^{n-\nu}$ Wurzeln sein, wobei h eine beliebige ganze Zahl bezeichnet. Damit gibt es offenbar p^ν verschiedene Wurzeln und nicht mehr. Dasselbe gilt für die Wurzeln, die den einzelnen Zahlen B, C usw. kongruent sind. *Drittens* zeigen wir, wie sich stets eine Wurzel finden lässt, die A nach p kongruent ist.

86.

Satz. *Ist wie im vorigen Artikel t durch p^ν, aber nicht durch $p^{\nu+1}$ teilbar, so gilt*

$$\begin{aligned}(\alpha + hp^\mu)^t - \alpha^t &\equiv 0\,(mod.p^{\mu+\nu}),\\ aber\ &\equiv \alpha^{t-1}hp^\mu t\,(mod.p^{\mu+\nu+1})\end{aligned}$$

Der zweite Teil des Satzes gilt nicht, wenn zugleich $p = 2$ und $\mu = 1$ ist.

Der Satz ließe sich durch Entwickeln der Binompotenz beweisen, wenn man zeigte, dass alle Glieder nach dem zweiten durch $p^{\mu+\nu+1}$ teilbar sind. Da die Betrachtung der Nenner der Koeffizienten aber einige Umwege erfordert, ziehen wir das folgende Verfahren vor.

Nehmen wir *zunächst* $\mu > 1$ und $\nu = 1$ an. Wegen

$$x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{usw.} + y^{t-1})$$

gilt dann

$$\begin{aligned}(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1}&\\ + (\alpha + hp^\mu)^{t-2}\alpha + \text{usw.} + \alpha^{t-1})&\end{aligned}$$

Nun ist $\alpha + hp^\mu \equiv \alpha\,(\mathrm{mod.}\,p^2)$. Daher ist jedes Glied $(\alpha + hp^\mu)^{t-1}$, $(\alpha + hp^\mu)^{t-2}\alpha$ usw. $\equiv \alpha^{t-1}(\mathrm{mod.}\,p^2)$, also die Summe aller Glieder $\equiv t\alpha^{t-1}(\mathrm{mod.}\,p^2)$ oder von der Form $t\alpha^{t-1} + Vp^2$, wobei V irgendeine Zahl bezeichnet. Damit hat $(\alpha + hp^\mu)^t - \alpha^t$ die Form

$$\alpha^{t-1}hp^{\mu}t + Vhp^{\mu+2},$$
$$\textit{das heißt, } \equiv \alpha^{t-1}hp^{\mu}t(\text{mod.}\, p^{\mu+2}) \quad \text{und } \equiv 0\,(\text{mod.}\, p^{\mu+1}).$$

Für diesen Fall ist der Satz also bewiesen.

Wäre der Satz nun für andere Werte von ν bei weiterhin geltendem $\mu > 1$ falsch, so müsste es eine Grenze geben, bis zu der er stets richtig, darüber hinaus aber falsch wäre. Der kleinste Wert von ν, für den er falsch ist, sei $= \varphi$. Dann sieht man leicht: Ist t durch $p^{\varphi-1}$, aber nicht durch p^{φ} teilbar, so gilt der Satz noch; ersetzt man dagegen t durch tp, so gilt er nicht. Wir haben also

$$\begin{aligned}(\alpha + hp^{\mu})^t &\equiv \alpha^t + \alpha^{t-1}hp^{\mu}t(\text{mod.}\, p^{\mu+\varphi}) \\ \text{oder } &= \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi}\end{aligned}$$

wobei u eine ganze Zahl bezeichnet. Da aber der Satz für $\nu = 1$ bereits bewiesen ist, gilt

$$\begin{aligned}(\alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi})^p \equiv \alpha^{tp} &+ \alpha^{tp-1}hp^{\mu+1}t \\ &+ \alpha^{tp-t}up^{\mu+\varphi+1}\,(\text{mod.}\, p^{\mu+\varphi+1})\end{aligned}$$

und somit auch

$$(\alpha + hp^{\mu})^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu}tp\,(\text{mod.}\, p^{\mu+\varphi+1})$$

das heißt, der Satz gilt auch, wenn t durch tp ersetzt wird, *also* auch für $\nu = \varphi$, entgegen der Voraussetzung. Damit gilt der Satz offenbar für sämtliche Werte von ν.

87.

Es bleibt der Fall $\mu = 1$. Mit einem ganz ähnlichen Verfahren wie im vorigen Artikel lässt sich ohne den binomischen Satz zeigen, dass

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \quad (\text{mod.}\, p^2) \\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp \\ \alpha\alpha(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp \\ &\text{usw.}\end{aligned}$$

also die Summe (da die Anzahl der Glieder $= t$)

$$\equiv t\alpha^{t-1} + \tfrac{(t-1)t}{2}\alpha^{t-2}hp(\text{mod.}\, p^2)$$

ist. Da t durch p teilbar ist, ist auch $\dfrac{(t-1)t}{2}$ durch p teilbar, außer wenn $p = 2$ ist; darauf haben wir schon im vorigen Artikel hingewiesen. In den übrigen Fällen gilt $\frac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0\,(\text{mod.}\, p^2)$, und somit ist auch jene Summe $\equiv t\alpha^{t-1}(\text{mod.}\, p^2)$, wie im vorigen Artikel. Im Übrigen verläuft der Beweis hier genauso wie dort.

Wir schließen also allgemein, mit der einzigen Ausnahme $p = 2$, dass

$$(\alpha + hp^{\mu})^t \equiv \alpha^t(\text{mod.}\, p^{\mu+\nu})$$

und $(\alpha + hp^\mu)^t$ *nicht* $\equiv \alpha^t$ für jeden Modul, der eine höhere Potenz von p als $p^{\mu+\nu}$ ist, sofern h nicht durch p teilbar ist und p^ν die höchste Potenz von p ist, die t teilt.

Daraus ergeben sich unmittelbar die erste und zweite Behauptung, die wir in Artikel 85 beweisen wollten:

erstens, ist $\alpha^t \equiv 1$, so auch $(\alpha + hp^{n-\nu})^t \equiv 1 \,(\mathrm{mod.}\, p^n)$;

zweitens, würde eine Zahl α', die A und damit auch α nach dem Modul p kongruent ist, nicht aber nach $p^{n-\nu}$, die Kongruenz $x^t \equiv 1 \,(\mathrm{mod.}\, p^n)$ erfüllen, so setze man $\alpha' = \alpha + lp^\lambda$, wobei l nicht durch p teilbar sei. Dann ist $\lambda < n - \nu$. Damit ist $(\alpha + lp^\lambda)^t$ nach dem Modul $p^{\lambda+\nu}$ der Zahl α^t kongruent, nicht aber nach dem Modul p^n, der eine höhere Potenz ist. Also kann α' keine Wurzel der Kongruenz $x^t \equiv 1$ sein.

88.

Als *Drittes* wollten wir eine Wurzel der Kongruenz $x^t \equiv 1 \,(\mathrm{mod.}\, p^n)$ finden, die A kongruent ist. Wir zeigen hier nur, wie dies geht, wenn schon eine Wurzel derselben Kongruenz nach dem Modul p^{n-1} bekannt ist. Das genügt offenbar, da wir vom Modul p, für den A eine Wurzel ist, zum Modul p^2 und so weiter zu allen aufeinanderfolgenden Potenzen übergehen können.

Sei also α eine Wurzel der Kongruenz $x^t \equiv 1 \,(\mathrm{mod.}\, p^{n-1})$, und gesucht sei eine Wurzel derselben Kongruenz nach dem Modul p^n. Setzen wir diese $= \alpha + hp^{n-\nu-1}$, denn dass sie diese Form haben muss, folgt aus dem vorigen Artikel. (Den Fall $\nu = n - 1$ betrachten wir später gesondert; größer als $n - 1$ kann ν aber nicht sein.) Es muss daher gelten

$$(\alpha + hp^{n-\nu-1})^t \equiv 1 (\mathrm{mod.}\, p^{n-1})$$

Aber $$(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \,(\mathrm{mod.}\, p^n)$$

Bestimmt man also h so, dass $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \,(\mathrm{mod.}\, p^n)$ gilt, oder so, dass (da nach Voraussetzung $1 \equiv \alpha^t (\mathrm{mod.}\, p^{n-1})$ und t durch p^ν teilbar ist) $\dfrac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1} h \dfrac{t}{p^\nu}$ durch p teilbar wird, so ist das Verlangte erreicht. Dass dies immer möglich ist, folgt aus dem vorigen Abschnitt. Denn hier setzen wir voraus, dass t durch keine höhere Potenz von p als p^ν teilbar ist, also $\alpha^{t-1} \dfrac{t}{p^\nu}$ zu p teilerfremd ist.

Ist dagegen $\nu = n - 1$, *das heißt* t durch p^{n-1} oder sogar durch eine höhere Potenz von p teilbar, so erfüllt jeder Wert A, der der Kongruenz $x^t \equiv 1$ nach dem Modul p genügt, diese auch nach dem Modul p^n. Sei nämlich $t = p^{n-1}\tau$. Dann gilt $t \equiv \tau (\mathrm{mod.}\, p - 1)$. Wegen $A^t \equiv 1 \,(\mathrm{mod.}\, p)$ gilt also auch $A^\tau \equiv 1 \,(\mathrm{mod.}\, p)$. Setzen wir daher $A^\tau = 1 + hp$, so ist $A^t = (1 + hp)^{p^{n-1}} \equiv 1 (\mathrm{mod.}\, p^n)$ nach Artikel 87.

89.

Alles, was wir in Artikel 57 und den folgenden mithilfe des Satzes hergeleitet haben, dass die Kongruenz $x^t \equiv 1$ nicht mehr als t verschiedene Wurzeln hat, gilt auch für einen Modul, der eine Potenz einer Primzahl ist. Nennen wir die zum Exponenten $p^{n-1}(p-1)$ gehörigen Zahlen *primitive Wurzeln*, also die Zahlen, deren Perioden alle nicht durch p teilbaren Zahlen enthalten, so gibt es auch hier primitive Wurzeln. Alles oben über Indizes und ihre Verwendung sowie über die Lösung der Kongruenz $x^t \equiv 1$ Gesagte ist auch hier anwendbar. Da dies keine Schwierigkeiten bietet, wäre es

unnötig, alles von Anfang an zu wiederholen. Außerdem haben wir gezeigt, wie sich die Wurzeln der Kongruenz $x^t \equiv 1$ nach dem Modul p^n aus den Wurzeln derselben Kongruenz nach p ableiten lassen. Zum Fall, dass eine Potenz von 2 der Modul ist, müssen wir aber noch einiges hinzufügen, da er oben ausgenommen war.

Moduln, die Potenzen von zwei sind.

90.

Wird eine höhere als die zweite Potenz von 2, etwa 2^n*, als Modul genommen, so ist die Potenz mit dem Exponenten* 2^{n-2} *einer beliebigen ungeraden Zahl der Eins kongruent. Zum Beispiel* $3^8 = 6561 \equiv 1 \,(\mathrm{mod.}\, 32)$.

Jede ungerade Zahl hat nämlich entweder die Form $1 + 4h$ oder $-1 + 4h$. Daraus folgt der Satz unmittelbar (Satz aus Artikel 86).

Da also der Exponent, zu dem eine beliebige ungerade Zahl nach dem Modul 2^n gehört, ein Teiler von 2^{n-2} sein muss, gehört sie zu einer der Zahlen $1, 2, 4, 8 \ldots . 2^{2n-2}$. Zu welcher, lässt sich wie folgt leicht entscheiden. Die gegebene Zahl sei $= 4h \pm 1$, und der Exponent der höchsten Potenz von 2, die h teilt, sei $= m$ (er kann auch $= 0$ sein, nämlich wenn h ungerade ist). Dann ist der Exponent, zu dem die gegebene Zahl gehört, $= 2^{n-m-2}$, sofern $n > m + 2$ ist. Ist dagegen $n =$ oder $< m + 2$, so ist die gegebene Zahl $\equiv \pm 1$ und gehört daher entweder zum Exponenten 1 oder zum Exponenten 2. Dass eine Zahl der Form $\pm 1 + 2^{m+2}k$ (gleichbedeutend mit $4h \pm 1$), zur Potenz mit dem Exponenten 2^{n-m-2} erhoben, der Eins nach dem Modul 2^n kongruent wird, bei einem Exponenten, der eine niedrigere Potenz von 2 ist, dagegen nicht, ergibt sich ohne Schwierigkeit aus Artikel 86. Jede Zahl der Form $8k + 3$ oder $8k + 5$ gehört also zum Exponenten 2^{n-2}.

91.

Hier gibt es somit keine *primitiven Wurzeln* in dem oben verwendeten Sinn: keine Zahlen, deren Periode sämtliche unter dem Modul liegenden und zu ihm teilerfremden Zahlen umfasst. Trotzdem sieht man leicht etwas Entsprechendes. Eine Potenz mit ungeradem Exponenten einer Zahl der Form $8k + 3$ hat stets die Form $8k + 3$, eine mit geradem Exponenten dagegen stets die Form $8k + 1$. Keine Potenz kann also die Form $8k + 5$ oder $8k + 7$ haben. Nun besteht die Periode einer Zahl der Form $8k + 3$ aus 2^{n-2} verschiedenen Gliedern, jedes von der Form $8k + 3$ oder $8k + 1$, und es gibt nicht mehr als 2^{n-2} solche unter dem Modul liegenden Zahlen. Daher ist jede Zahl der Form $8k + 1$ oder $8k + 3$ nach dem Modul 2^n irgendeiner Potenz einer beliebigen Zahl der Form $8k + 3$ kongruent. Ebenso zeigt man, dass die Periode einer Zahl der Form $8k + 5$ alle Zahlen der Formen $8k + 1$ und $8k + 5$ umfasst. Wählt man also eine Zahl der Form $8k + 5$ als Basis, so erhalten alle Zahlen der Formen $8k + 1$ und $8k + 5$, positiv genommen, sowie alle Zahlen der Formen $8k + 3$ und $8k + 7$, negativ genommen, wirkliche Indizes. Dabei sind nach 2^{n-2} kongruente Indizes als gleichwertig anzusehen. So ist unsere Tafel I zu verstehen, in der wir für die Moduln 16, 32 und 64 (für den Modul 8 braucht man keine Tafel) stets die Zahl 5 als Basis gewählt haben. *Zum Beispiel* entspricht der Zahl 19, die von der Form $8n + 3$ und daher *negativ* zu nehmen ist, beim Modul 64 der Index 7. Das bedeutet $5^7 \equiv -19 \,(\mathrm{mod.}\, 64)$.

Den Zahlen der Formen $8n+1$, $8n+5$, negativ genommen, sowie denen der Formen $8n+3$, $8n+7$, positiv genommen, müsste man dagegen gewissermaßen imaginäre Indizes zuordnen. Führt man sie ein, so lässt sich die Rechnung mit Indizes auf einen sehr einfachen Algorithmus zurückführen. Eine völlig strenge Darstellung würde uns jedoch zu weit führen. Wir behalten uns dies daher für eine andere Gelegenheit vor, wenn wir vielleicht die Theorie der imaginären Größen ausführlicher behandeln werden. Unserer Ansicht nach hat sie bisher niemand auf klare Begriffe zurückgeführt. Kundige werden diesen Algorithmus leicht selbst finden; weniger Geübte können die Tafel trotzdem verwenden, so wie auch diejenigen Logarithmen benutzen, die die Erörterungen neuerer Autoren über imaginäre *Logarithmen* nicht kennen, sofern sie nur die oben begründeten Prinzipien gut verstanden haben.

Aus mehreren Primzahlen zusammengesetzte Moduln.

92.

Bei einem aus mehreren Primzahlen zusammengesetzten Modul lässt sich fast alles über die Reste von Potenzen aus der allgemeinen Kongruenztheorie ableiten. Da wir aber weiter unten ausführlicher zeigen, wie man beliebige Kongruenzen nach einem solchen Modul auf Kongruenzen mit Primzahlen oder Primzahlpotenzen als Modul zurückführt, brauchen wir uns hier nicht lange damit aufzuhalten. Wir bemerken nur, dass die sehr schöne Eigenschaft der übrigen Moduln, nämlich dass es stets Zahlen gibt, deren Periode sämtliche zum Modul teilerfremden Zahlen umfasst, hier fehlt. Es gibt nur eine Ausnahme: wenn der Modul das Doppelte einer Primzahl oder einer Primzahlpotenz ist. Bringt man nämlich den Modul m auf die Form $A^aB^bC^c$ usw., wobei A, B, C usw. verschiedene Primzahlen bezeichnen, und bezeichnet man außerdem $A^{a-1}(A-1)$ mit α, $B^{b-1}(B-1)$ mit β usw., und ist schließlich z eine zu m teilerfremde Zahl, so gilt $z^\alpha \equiv 1 \,(\mathrm{mod.}\, A^a)$. $z^\beta \equiv 1 \,(\mathrm{mod.}\, B^b)$ usw. Ist also μ das kleinste gemeinsame Vielfache der Zahlen α, β, γ usw., so gilt $z^\mu \equiv 1$ nach sämtlichen Moduln A^a, B^b usw. und damit auch nach m, das deren Produkt ist. Außer wenn m das Doppelte einer Primzahl oder einer Primzahlpotenz ist, ist aber das kleinste gemeinsame Vielfache der Zahlen α, β, γ usw. kleiner als ihr Produkt. Denn die Zahlen α, β, γ usw. können nicht paarweise teilerfremd sein, sondern haben jedenfalls den gemeinsamen Teiler 2. Also kann die Periode keiner Zahl so viele Glieder umfassen, wie es unter dem Modul liegende, zu ihm teilerfremde Zahlen gibt, da deren Anzahl gleich dem Produkt von α, β, γ usw. ist. So ist *zum Beispiel* für $m = 1001$ jede zu m teilerfremde Zahl, zur Potenz mit dem Exponenten 60 erhoben, der Eins kongruent, da 60 ein gemeinsames Vielfaches der Zahlen $6, 10, 12$ ist. — Der Fall, dass der Modul das Doppelte einer Primzahl oder einer Primzahlpotenz ist, entspricht aber vollständig dem Fall einer Primzahl oder einer Primzahlpotenz als Modul.

93.

Die Schriften, in denen andere Mathematiker den Gegenstand dieses Abschnitts behandelt haben, wurden bereits an verschiedenen Stellen erwähnt. Wer aber manches ausführlicher erläutert sehen möchte, als es uns die Kürze erlaubte, sei besonders auf die folgenden Abhandlungen Eulers verwiesen. Sie sind wegen der Klarheit besonders zu empfehlen, durch die sich dieser große Mann stets vor allen anderen auszeichnete.

Theoremata circa residua ex divisione potestatum relicta Comm. nov. Petr. T. VII, *p.* 49 und folgende.

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.

Ibid. T. XVIII, *p.* 85 und folgende.

Hinzu kommen können *Opusculorum analyt. T.* I, Abhandlungen 5 und 8.

VIERTER ABSCHNITT

ÜBER

KONGRUENZEN ZWEITEN GRADES.

Quadratische Reste und Nichtreste.

94.

Satz. *Nimmt man eine beliebige Zahl m als Modul, so können von den Zahlen $0, 1, 2, 3....m-1$ höchstens $\frac{1}{2}m+1$, wenn m gerade ist, und höchstens $\frac{1}{2}m+\frac{1}{2}$, wenn m ungerade ist, einem Quadrat kongruent sein.*

Beweis. Da die Quadrate kongruenter Zahlen kongruent sind, ist jede Zahl, die einem Quadrat kongruent sein kann, auch einem Quadrat kongruent, dessen Wurzel $< m$ ist. Es genügt also, die kleinsten Reste der Quadrate $0, 1, 4, 9....(m-1)^2$ zu betrachten. Man sieht leicht, dass $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$ usw. gelten. Wenn m gerade ist, haben daher die Quadrate $(\frac{1}{2}m-1)^2$ und $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ und $(\frac{1}{2}m+2)^2$ usw. dieselben kleinsten Reste; wenn m ungerade ist, sind die Quadrate $(\frac{1}{2}m-\frac{1}{2})^2$ und $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ und $(\frac{1}{2}m+\frac{3}{2})^2$ usw. kongruent. Somit können nur Zahlen, die einem der Quadrate $0, 1, 4, 9....(\frac{1}{2}m)^2$ kongruent sind, einem Quadrat kongruent sein, wenn m gerade ist. Ist der Modul ungerade, so muss jede Zahl, die einem Quadrat kongruent ist, einem der Quadrate $0, 1, 4, 9....(\frac{1}{2}m-\frac{1}{2})^2$ kongruent sein. Es gibt also im ersten Fall höchstens $\frac{1}{2}m+1$, im zweiten höchstens $\frac{1}{2}m+\frac{1}{2}$ verschiedene kleinste Reste. *Q. E. D.*

Beispiel. Nach dem Modul 13 findet man für die Quadrate der Zahlen $0, 1, 2, 3...6$ die kleinsten Reste $0, 1, 4, 9, 3, 12, 10$; danach kehren dieselben in umgekehrter Reihenfolge wieder, $10, 12, 3$ usw. Jede Zahl, die keinem dieser Reste kongruent ist, also eine Zahl, die einer der Zahlen $2, 5, 6, 7.\ 8, 11$ kongruent ist, kann daher keinem Quadrat kongruent sein.

Nach dem Modul 15 findet man die Reste $0, 1, 4, 9, 1, 10, 6, 4$, nach denen dieselben in umgekehrter Reihenfolge wiederkehren. Hier ist die Anzahl der Reste, die einem Quadrat kongruent sein können, sogar kleiner als $\frac{1}{2}m+\frac{1}{2}$, denn es sind $0, 1, 4, 6, 9, 10$. Die Zahlen $2, 3, 5, 7, 8, 11, 12, 13, 14$ und die Zahlen, die einer von ihnen kongruent sind, können keinem Quadrat nach dem Modul 15 kongruent sein.

95.

Daraus folgt, dass man für jeden Modul alle Zahlen in zwei Klassen einteilen kann: Die eine enthält die Zahlen, die einem Quadrat kongruent sein können, die andere diejenigen, bei denen dies nicht möglich ist. Die ersteren nennen wir *quadratische Reste der als Modul gewählten Zahl*[*)], die letzteren ihre *quadratischen Nichtreste*,

[*)] Genau genommen verwenden wir hier den Genitiv in einem anderen Sinn als bisher. Wir müssten sagen, r sei ein Rest des Quadrats aa nach dem Modul m, wenn $r \equiv aa \pmod{m}$ gilt. Der Kürze wegen nennen wir in diesem Abschnitt aber stets r einen quadratischen Rest *von m selbst*, ohne dass dadurch eine Mehrdeutigkeit zu befürchten ist. Denn das Wort *Rest* verwenden wir von nun an nicht mehr im Sinn einer kongruenten Zahl, außer wenn wir von *kleinsten* Resten sprechen; dabei kann kein Zweifel entstehen.

oder auch einfach *Reste* und *Nichtreste*, wenn dadurch keine Mehrdeutigkeit entsteht. Es genügt, alle Zahlen $0, 1, 2 \ldots m-1$ einzuordnen, denn kongruente Zahlen gehören zur selben Klasse.

Auch diese Untersuchung beginnen wir mit Primzahlmoduln; das ist auch dann zu verstehen, wenn wir es nicht ausdrücklich erwähnen. Die Primzahl 2 schließen wir jedoch aus, betrachten also nur *ungerade* Primzahlen.

Ist der Modul eine Primzahl, so gibt es unter den kleineren Zahlen ebenso viele Reste wie Nichtreste.

96.

Wählt man die Primzahl p als Modul, so ist die Hälfte der Zahlen $1, 2, 3 \ldots p-1$ quadratischer Rest, die übrigen sind Nichtreste; es gibt also $\frac{1}{2}(p-1)$ Reste und ebenso viele Nichtreste.

Man zeigt leicht, dass alle Quadrate $1, 4, 9 \ldots \frac{1}{4}(p-1)^2$ inkongruent sind. Wäre nämlich $rr \equiv r'r' (\mathrm{mod.}\, p)$ möglich und wären die Zahlen r, r' verschieden und nicht größer als $\frac{1}{2}(p-1)$, so wäre, wenn wir $r > r'$ annehmen, was erlaubt ist, $(r-r')(r+r')$ positiv und durch p teilbar. Aber beide Faktoren $r-r'$ und $r+r'$ sind kleiner als p, sodass diese Annahme unmöglich ist (Artikel 13). Es gibt also $\frac{1}{2}(p-1)$ quadratische Reste unter den Zahlen $1, 2, 3 \ldots p-1$. Mehr kann es nicht geben, denn mit dem Rest 0 erhält man $\frac{1}{2}(p+1)$, und die Anzahl aller Reste kann diesen Wert nicht übersteigen. Die übrigen Zahlen sind daher Nichtreste, und ihre Anzahl ist $= \frac{1}{2}(p-1)$.

Da null stets ein Rest ist, schließen wir diese Zahl und die durch den Modul teilbaren Zahlen aus unseren Untersuchungen aus. Dieser Fall ist für sich klar und würde nur die übersichtliche Form der Sätze stören. Aus demselben Grund haben wir auch den Modul 2 ausgeschlossen.

97.

Mehrere Ergebnisse dieses Abschnitts lassen sich auch aus den Grundsätzen des vorigen Abschnitts herleiten. Da es nützlich ist, dieselbe Wahrheit mit verschiedenen Methoden zu untersuchen, wollen wir diesen Zusammenhang zeigen. Man sieht leicht, dass alle einem Quadrat kongruenten Zahlen *gerade* Indizes haben, dagegen diejenigen, die keinem Quadrat kongruent sein können, ungerade. Da $p-1$ gerade ist, gibt es ebenso viele gerade wie ungerade Indizes, nämlich $\frac{1}{2}(p-1)$, und damit ebenso viele Reste wie Nichtreste.

Beispiele. Für die folgenden Moduln sind die Reste

3	.....	1.
5	.....	1, 4.
7	.....	1, 2, 4.
11	.....	1, 3, 4, 5, 9.
13	.....	1.3.4, 9, 10, 12.
17	....,	1, 2, 4, 8, 9, 13, 15, 16.
		usw.

Die übrigen Zahlen unterhalb dieser Moduln sind Nichtreste.

Ob eine zusammengesetzte Zahl Rest oder Nichtrest einer gegebenen Primzahl ist, hängt von ihren Faktoren ab.

98.

Satz. *Das Produkt zweier quadratischer Reste der Primzahl p ist ein Rest; das Produkt eines Restes und eines Nichtrestes ist ein Nichtrest; das Produkt zweier Nichtreste ist ein Rest.*

Beweis. I. Seien A, B Reste, die aus den Quadraten aa, bb entstehen, also $A \equiv aa$, $B \equiv bb$. Dann ist das Produkt AB dem Quadrat der Zahl ab kongruent, also ein Rest.

II. Ist A ein Rest, etwa $\equiv aa$, und B ein Nichtrest, so ist AB ein Nichtrest. Nehmen wir nämlich, wenn möglich, $AB \equiv kk$ an und setzen $\frac{k}{a} \,(\mathrm{mod.}\, p) \equiv b$. Dann gilt $aaB \equiv aabb$, also $B \equiv bb$; somit wäre B ein Rest, entgegen der Voraussetzung.

Anderer Beweis. Wir multiplizieren alle Reste unter den Zahlen $1, 2, 3 \ldots . p-1$ (ihre Anzahl ist $= \frac{1}{2}(p-1)$) mit A. Alle Produkte sind quadratische Reste und untereinander inkongruent. Multiplizieren wir nun den Nichtrest B mit A, so ist das Produkt keinem der schon erhaltenen Produkte kongruent. Wäre es ein Rest, so hätten wir $\frac{1}{2}(p+1)$ inkongruente Reste, noch ohne den Rest 0, entgegen Artikel 96.

III. Seien A, B Nichtreste. Multiplizieren wir alle Reste unter den Zahlen $1, 2, 3 \ldots . p-1$ mit A, so erhalten wir $\frac{1}{2}(p-1)$ untereinander inkongruente Nichtreste (II). Das Produkt AB kann keinem davon kongruent sein. Wäre es also ein Nichtrest, so hätten wir $\frac{1}{2}(p+1)$ untereinander inkongruente Nichtreste, entgegen Artikel 96. Also ist das Produkt usw. *Q. E. D.*

Noch leichter lassen sich diese Sätze aus den Grundsätzen des vorigen Abschnitts herleiten. Die Indizes der Reste sind stets gerade, die der Nichtreste ungerade. Der Index des Produkts zweier Reste oder zweier Nichtreste ist daher gerade, das Produkt selbst also ein Rest. Dagegen ist der Index des Produkts eines Restes und eines Nichtrestes ungerade und das Produkt selbst ein Nichtrest.

Beide Beweismethoden lassen sich auch auf die folgenden Sätze anwenden: *Der Wert des Ausdrucks* $\frac{a}{b} \,(mod.\, p)$ *ist ein Rest, wenn die Zahlen* a, b *beide Reste oder beide Nichtreste sind; dagegen ist er ein Nichtrest, wenn von den Zahlen* a, b *eine ein Rest und die andere ein Nichtrest ist.* Diese Sätze ergeben sich auch durch Umkehrung der vorigen.

99.

Allgemein ist ein Produkt beliebig vieler Faktoren sowohl dann ein Rest, wenn alle Faktoren Reste sind, als auch dann, wenn unter ihnen eine gerade Anzahl von Nichtresten vorkommt. Ist die Anzahl der Nichtreste unter den Faktoren ungerade, so ist das Produkt ein Nichtrest. Man kann daher leicht entscheiden, ob eine zusammengesetzte Zahl ein Rest ist, wenn man weiß, wie es sich mit jedem ihrer Faktoren verhält. Deshalb haben wir in Tabelle II nur Primzahlen aufgenommen. Die Tabelle ist folgendermaßen angeordnet: Am Rand stehen die Moduln[*)], im Inneren die aufeinanderfolgenden Primzahlen. Ist eine dieser Primzahlen ein Rest eines Moduls, so

[*)] Wie wir auch auf zusammengesetzte Moduln verzichten können, werden wir bald zeigen.

steht im zugehörigen Feld ein kurzer Strich; ist sie ein Nichtrest des Moduls, so bleibt dieses Feld leer.

Zusammengesetzte Moduln.

100.

Bevor wir zu schwierigeren Fragen übergehen, müssen wir noch einiges über nichtprime Moduln ergänzen.

Wählt man für eine Primzahl p eine Potenz p^n als Modul (wobei wir annehmen, dass p nicht 2 ist), so ist von allen Zahlen, die nicht durch p teilbar und kleiner als der Modul sind, die eine Hälfte Rest, die andere Nichtrest. Die Anzahl beider ist also $= \frac{1}{2}(p-1)p^{n-1}$.

Ist nämlich r ein Rest, so ist er einem Quadrat kongruent, dessen Wurzel die Hälfte des Moduls nicht übersteigt; siehe Artikel 94. Man sieht leicht, dass es $\frac{1}{2}(p-1)p^{n-1}$ Zahlen gibt, die nicht durch p teilbar und kleiner als die Hälfte des Moduls sind. Es bleibt also zu zeigen, dass ihre Quadrate alle inkongruent sind, also verschiedene quadratische Reste liefern. Wären die Quadrate zweier Zahlen a, b, die nicht durch p teilbar und kleiner als die Hälfte des Moduls sind, kongruent, so wäre $aa - bb$ oder $(a-b)(a+b)$ durch p^n teilbar (wobei wir $a > b$ annehmen dürfen). Das ist nur möglich, wenn *entweder* eine der Zahlen $a-b$. $a+b$ durch p^n teilbar ist, was nicht sein kann, da beide $< p^n$ sind, *oder* die eine durch p^m, die andere durch p^{n-m}, also beide durch p teilbar sind. Aber auch das ist unmöglich. Denn dann wären ihre Summe und Differenz $2a$ und $2b$ durch p teilbar, also auch a und b, entgegen der Voraussetzung. — Daraus folgt, dass es unter den nicht durch p teilbaren Zahlen unterhalb des Moduls $\frac{1}{2}(p-1)p^{n-1}$ Reste gibt; die übrigen, deren Anzahl ebenso groß ist, sind Nichtreste. *Q. E. D.* — Diesen Satz kann man auch wie in Artikel 97 durch Betrachtung der Indizes herleiten.

101.

Jede nicht durch p teilbare Zahl, die ein Rest von p ist, ist auch ein Rest von p^n; jeder Nichtrest von p ist auch ein Nichtrest von p^n.

Der zweite Teil dieser Aussage ist für sich klar. Wäre der erste falsch, so gäbe es unter den Zahlen, die kleiner als p^n und nicht durch p teilbar sind, mehr Reste von p als von p^n, also mehr als $\frac{1}{2}p^{n-1}(p-1)$. Man sieht aber ohne Schwierigkeit, dass die Anzahl der Reste von p unter diesen Zahlen genau $= \frac{1}{2}p^{n-1}(p-1)$ ist.

Ebenso leicht ist es, ein Quadrat zu finden, das einem gegebenen Rest nach dem Modul p^n kongruent ist, wenn ein ihm nach dem Modul p kongruentes Quadrat bekannt ist.

Hat man nämlich ein Quadrat aa, das dem gegebenen Rest A nach dem Modul p^μ kongruent ist, so erhält man daraus ein Quadrat, das A nach dem Modul p^ν kongruent ist (wobei wir $\nu > \mu$ und $=$ oder $< 2\mu$ voraussetzen), folgendermaßen. Wir setzen die Wurzel des gesuchten Quadrats $= \pm a + xp^\mu$; diese Form muss sie offensichtlich haben. Dann muss $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A \pmod{p^\nu}$ gelten, oder wegen $2\mu \geq \nu$ auch $A - aa \equiv \pm 2axp^\mu \pmod{p^\nu}$. Sei $A - aa = p^\mu d$; dann ist x der Wert des Ausdrucks $\pm\frac{d}{2a} \pmod{p^{\nu-\mu}}$, der dem Ausdruck $\pm\frac{A-aa}{2ap^\mu} \pmod{p^\nu}$ gleichwertig ist.

Ein Quadrat, das A nach dem Modul p kongruent ist, liefert also ein Quadrat, das A nach dem Modul p^2 kongruent ist. Von hier kann man zum Modul p^4, dann zu p^8 usw. aufsteigen.

Beispiel. Ist der Rest 6 gegeben, der nach dem Modul 5 dem Quadrat 1 kongruent ist, so findet man das Quadrat 9^2, dem er nach 25 kongruent ist, ferner 16^2, dem er nach 125 kongruent ist, usw.

102.

Was die durch p teilbaren Zahlen betrifft, so sind ihre Quadrate offensichtlich durch pp teilbar. Daher sind alle Zahlen, die zwar durch p, aber nicht durch pp teilbar sind, Nichtreste von p^n. Ist allgemein eine Zahl $p^k A$ gegeben, wobei A nicht durch p teilbar ist, so sind folgende Fälle zu unterscheiden:

1) Wenn $k =$ oder $> n$, so gilt $p^k A \equiv 0 \,(\mathrm{mod.}\, p^n)$, also handelt es sich um einen Rest.

2) Wenn $k < n$ und der Exponent ungerade ist, so ist $p^k A$ ein Nichtrest.

Wäre nämlich $p^k A = p^{2\kappa+1} A \equiv ss \,(\mathrm{mod.}\, p^n)$, so wäre ss durch $p^{2\kappa+1}$ teilbar. Das ist nur möglich, wenn s durch $p^{\kappa+1}$ teilbar ist. Dann wäre aber ss auch durch $p^{2\kappa+2}$ teilbar und somit (da $2\kappa+2$ sicher nicht größer als n ist) auch $p^k A$, *das heißt* $p^{2\kappa+1} A$. Also wäre A durch p teilbar, entgegen der Voraussetzung.

3) Wenn $k < n$ und der Exponent gerade ist. Dann ist $p^k A$ ein Rest oder Nichtrest von p^n, je nachdem, ob A ein Rest oder Nichtrest von p ist. Ist nämlich A ein Rest von p, so ist es auch ein Rest von p^{n-k}. Setzen wir $A \equiv aa (\mathrm{mod.}\, p^{n-k})$, so gilt $Ap^k \equiv aap^k \,(\mathrm{mod.}\, p^n)$, und aap^k ist ein Quadrat. Ist dagegen A ein Nichtrest von p, so kann $p^k A$ kein Rest von p^n sein. Denn nehmen wir $p^k A \equiv aa \,(\mathrm{mod.}\, p^n)$ an, so muss aa durch p^k teilbar sein. Der Quotient ist ein Quadrat, dem A nach dem Modul p^{n-k} und damit auch nach p kongruent ist. *Das heißt,* A wäre ein Rest von p, entgegen der Voraussetzung.

103.

Da wir den Fall $p = 2$ ausgeschlossen haben, müssen wir darüber noch einiges sagen. Ist 2 der Modul, so ist jede Zahl ein Rest, und es gibt keine Nichtreste. Ist aber 4 der Modul, so sind alle ungeraden Zahlen der Form $4k+1$ Reste, alle Zahlen der Form $4k+3$ Nichtreste. Ist schließlich 8 oder eine höhere Potenz von 2 der Modul, so sind alle ungeraden Zahlen der Form $8k+1$ Reste; die übrigen, also die Zahlen der Formen $8k+3,\ 8k+5,\ 8k+7$, sind Nichtreste. Der zweite Teil dieser Aussage ist klar, denn das Quadrat jeder ungeraden Zahl, ob sie die Form $4k+1$ oder $4k-1$ hat, hat die Form $8k+1$. Den ersten Teil beweisen wir so.

1) Ist die Summe oder die Differenz zweier Zahlen durch 2^{n-1} teilbar, so sind ihre Quadrate nach dem Modul 2^n kongruent. Setzt man nämlich die eine $= a$, so hat die andere die Form $2^{n-1}h \pm a$, deren Quadrat $\equiv aa \,(\mathrm{mod.}\, 2^n)$ ist.

2) Jede ungerade Zahl, die ein quadratischer Rest von 2^n ist, ist einem Quadrat kongruent, dessen Wurzel ungerade und $< 2^{n-2}$ ist. Sei aa ein beliebiges Quadrat, dem jene Zahl kongruent ist, und sei $a \equiv \pm\alpha (\mathrm{mod.}\, 2^{n-1})$, wobei α die Hälfte des Moduls nicht übersteigt (Artikel 4). Dann ist $aa \equiv \alpha\alpha$, also ist auch die gegebene Zahl $\equiv \alpha\alpha$. Offensichtlich sind sowohl a als auch α ungerade, und es gilt $\alpha < 2^{n-2}$.

3) Die Quadrate aller ungeraden Zahlen unterhalb von 2^{n-2} sind nach 2^n inkongruent. Seien nämlich r und s zwei solche Zahlen. Wären ihre Quadrate nach 2^n kongruent, so wäre $(r-s)(r+s)$ durch 2^n teilbar (wobei $r > s$ angenommen ist). Man sieht aber leicht, dass die Zahlen $r-s,\ r+s$ nicht beide durch 4 teilbar sein können. Ist also die eine nur durch 2 teilbar, so müsste, damit das Produkt durch 2^n teilbar wäre, die andere durch 2^{n-1} teilbar sein. *Q. E. A.* Denn beide sind $< 2^{n-2}$.

4) Reduzieren wir schließlich diese Quadrate auf ihre *kleinsten positiven Reste*, so erhalten wir 2^{n-3} verschiedene quadratische Reste unterhalb des Moduls[*)], von denen jeder die Form $8k+1$ hat. Da es aber genau 2^{n-3} Zahlen der Form $8k+1$ unterhalb des Moduls gibt, müssen sie alle unter diesen Resten vorkommen. *Q. E. D.*

Um ein Quadrat zu finden, das einer gegebenen Zahl der Form $8k+1$ nach dem Modul 2^n kongruent ist, kann man ähnlich wie in Artikel 101 vorgehen; siehe auch Artikel 88. — Für gerade Zahlen gilt schließlich dasselbe, was wir in Artikel 102 allgemein dargelegt haben.

104.

Über die Anzahl der verschiedenen Werte (*das heißt,* der nach dem Modul inkongruenten Werte), die ein Ausdruck wie $V = \sqrt{A}\,(\mathrm{mod.}\, p^n)$ zulässt, wenn A ein Rest von p^n ist, ergibt sich aus dem Vorigen leicht Folgendes. (Wir nehmen wie zuvor an, dass p eine Primzahl ist, und schließen der Kürze wegen den Fall $n = 1$ gleich mit ein.) I. Ist A nicht durch p teilbar, so hat V für $p = 2,\ n = 1$ *einen* Wert, nämlich $V \equiv 1$; *zwei*, wenn p ungerade ist, und ebenso für $p = 2,\ n = 2$: Setzt man einen $\equiv v$, so ist der andere $\equiv -v$; *vier* für $p = 2,\ n > 2$: Setzt man einen $\equiv v$, so sind die übrigen $\equiv -v,\ 2^{n-1} + v,\ 2^{n-1} - v$. II. Ist A durch p, aber nicht durch p^n teilbar, so sei die höchste Potenz von p, die A teilt, $p^{2\mu}$ (ihr Exponent muss offensichtlich gerade sein), und es sei $A = ap^{2\mu}$. Dann sind alle Werte von V durch p^μ teilbar, und die entstehenden Quotienten sind Werte des Ausdrucks $V' = \sqrt{a}\,(\mathrm{mod.}\, p^{n-2\mu})$. Alle verschiedenen Werte von V erhält man daher, indem man alle Werte des Ausdrucks V' zwischen 0 und $p^{n-\mu}$ mit p^μ multipliziert. Sie werden also dargestellt durch

$$vp^\mu, \quad vp^\mu + p^{n-\mu}, \quad vp^\mu + 2p^{n-\mu} \ldots vp^\mu + (p^\mu - 1)p^{n-\mu}$$

wobei v nacheinander alle *verschiedenen* Werte des Ausdrucks V' bezeichnet. Ihre Anzahl ist somit $p^\mu,\ 2p^\mu$ oder $4p^\mu$, je nachdem, ob die Anzahl der letzteren (nach Fall I) 1, 2 oder 4 ist. III. Ist A durch p^n teilbar, so setze man $n = 2m$ oder $= 2m-1$, je nachdem, ob der Exponent gerade oder ungerade ist. Man sieht leicht, dass alle durch p^m teilbaren Zahlen und keine anderen Werte von V sind. Alle verschiedenen Werte sind daher $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, und ihre Anzahl ist p^{n-m}.

105.

Es bleibt der Fall, in dem der Modul m aus mehreren Primzahlen zusammengesetzt ist. Sei $m = abc\ldots$, wobei a, b, c usw. verschiedene Primzahlen oder Potenzen verschiedener Primzahlen bezeichnen. Ist n ein Rest von m, so ist n offensichtlich auch ein Rest von jedem der Moduln a, b, c usw.; also ist n sicher ein Nichtrest von m, wenn es ein Nichtrest einer der Zahlen a, b, c usw. ist. Umgekehrt ist n, wenn es ein

[*)] Denn die Anzahl der ungeraden Zahlen unterhalb von 2^{n-2} ist 2^{n-3}.

Rest von jeder der Zahlen a, b, c usw. ist, auch ein Rest ihres Produkts m. Nehmen wir nämlich $n \equiv A^2$, B^2, C^2 usw. nach den Moduln a, b, c usw. an. Bestimmen wir eine Zahl N, die den Zahlen A, B, C usw. nach den Moduln a, b, c usw. jeweils kongruent ist (Artikel 32), so gilt $n \equiv NN$ nach allen diesen Moduln und damit auch nach ihrem Produkt m. — Man sieht leicht, dass auf diese Weise die Verbindung *jedes* Wertes von A, also des Ausdrucks $\sqrt{n} \,(\mathrm{mod.}\, a)$, mit *jedem* Wert von B, mit *jedem* Wert von C usw. einen Wert von N, also des Ausdrucks $\sqrt{n} \,(\mathrm{mod.}\, m)$, liefert; dass verschiedene Verbindungen verschiedene Werte von N ergeben; und dass sämtliche Verbindungen sämtliche Werte liefern. Die Anzahl aller verschiedenen Werte von N ist daher gleich dem Produkt der Anzahlen der Werte von A, B, C usw., deren Bestimmung wir im vorigen Artikel gezeigt haben. — Ist ferner ein Wert des Ausdrucks $\sqrt{n} \,(\mathrm{mod.}\, m)$, also von N, bekannt, so ist dieser auch ein Wert von allen Zahlen A, B, C usw. Da man daraus nach dem vorigen Artikel alle übrigen Werte dieser Größen herleiten kann, lassen sich aus einem Wert von N leicht alle übrigen bestimmen.

Beispiel. Sei der Modul 315 gegeben und gefragt, ob 46 ein Rest oder Nichtrest davon ist. Die Primteiler von 315 sind $3, 5, 7$, und 46 ist ein Rest von jedem von ihnen, also auch ein Rest von 315. Da ferner $46 \equiv 1$ und $\equiv 64 (\mathrm{mod.}\, 9)$; $\equiv 1$ und $\equiv 16 \,(\mathrm{mod.}\, 5)$; $\equiv 4$ und $\equiv 25 \,(\mathrm{mod.}\, 7)$ gelten, findet man die Wurzeln der Quadrate, denen 46 nach dem Modul 315 kongruent ist: $19, 26, 44, 89, 226,\ 271, 289, 296$.

Allgemeines Kriterium dafür, ob eine gegebene Zahl Rest oder Nichtrest einer gegebenen Primzahl ist.

106.

Aus dem Vorigen folgt: Wenn wir stets entscheiden können, ob eine gegebene *Primzahl* Rest oder Nichtrest einer *gegebenen Primzahl* ist, lassen sich alle übrigen Fälle darauf zurückführen. Für diesen Fall müssen wir also mit aller Sorgfalt sichere Kriterien suchen. Bevor wir diese Untersuchung beginnen, geben wir ein Kriterium aus dem vorigen Abschnitt an, das zwar in der Praxis fast keinen Nutzen hat, wegen seiner Einfachheit und Allgemeinheit aber eine Erwähnung verdient.

Jede Zahl A, die nicht durch die Primzahl $2m + 1$ teilbar ist, ist ein Rest oder Nichtrest dieser Primzahl, je nachdem, ob $A^m \equiv +1$ oder $\equiv -1 \,(\mathrm{mod.}\, 2m + 1)$ gilt.

Für den Modul $2m + 1$ sei der Index der Zahl A in einem beliebigen System a. Dann ist a gerade, wenn A ein Rest von $2m + 1$ ist, dagegen ungerade, wenn A ein Nichtrest ist. Der Index der Zahl A^m ist aber ma, *das heißt* $\equiv 0$ oder $\equiv m \,(\mathrm{mod.}\, 2m)$, je nachdem, ob a gerade oder ungerade ist. Also ist A^m im ersten Fall $\equiv +1$, im zweiten $\equiv -1 \,(\mathrm{mod.}\, 2m + 1)$. Siehe Artikel 57 und 62.

Beispiel. 3 ist ein Rest von 13, weil $3^6 \equiv 1 \,(\mathrm{mod.}\, 13)$ gilt; dagegen ist 2 ein Nichtrest von 13, weil $2^6 \equiv -1 \,(\mathrm{mod.}\, 13)$ gilt.

Sobald die zu prüfenden Zahlen aber auch nur mäßig groß sind, ist dieses Kriterium wegen des gewaltigen Rechenaufwands völlig unbrauchbar.

Untersuchungen über die Primzahlen, für die gegebene Zahlen Reste oder Nichtreste sind.

107.

Für einen gegebenen Modul lassen sich alle Zahlen, die seine Reste oder Nichtreste sind, sehr leicht angeben. Setzt man jene Zahl $= m$, so muss man die Quadrate bestimmen, deren Wurzeln die Hälfte von m nicht übersteigen, oder Zahlen, die diesen Quadraten nach m kongruent sind (für die Praxis gibt es noch bequemere Methoden). Dann sind alle Zahlen, die einer von diesen nach m kongruent sind, Reste von m; alle Zahlen, die keiner davon kongruent sind, sind Nichtreste. — Die umgekehrte Frage, *zu einer gegebenen Zahl alle Zahlen anzugeben, von denen sie Rest oder Nichtrest ist*, erfordert jedoch eine viel tiefere Untersuchung. Dieses Problem, von dessen Lösung das im vorigen Artikel gestellte abhängt, werden wir nun untersuchen und dabei mit den einfachsten Fällen beginnen.

Der Rest -1.

108.

Satz. *Für alle Primzahlen der Form* $4n+1$ *ist* -1 *ein quadratischer Rest, für alle Primzahlen der Form* $4n+3$ *dagegen ein Nichtrest.*

Beispiel. -1 ist ein Rest der Zahlen $5, 13, 17, 29, 37, 41, 53, 61.73, 89, 97$ usw., der sich jeweils aus den Quadraten der Zahlen $2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22$ usw. ergibt; dagegen ist es ein Nichtrest der Zahlen $3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83$ usw.

Diesen Satz haben wir schon in Artikel 64 erwähnt. Sein Beweis folgt leicht aus Artikel 106. Für eine Primzahl der Form $4n+1$ gilt nämlich $(-1)^{2n} \equiv 1$, für eine Zahl der Form $4n+3$ dagegen $(-1)^{2n+1} \equiv -1$. Dieser Beweis stimmt mit dem dort gegebenen überein. Wegen der Eleganz und des Nutzens des Satzes wird ein weiterer Beweis auf anderem Weg aber nicht überflüssig sein.

109.

Die Gesamtheit aller Reste der Primzahl p, die kleiner als p sind, mit Ausnahme des Restes 0, bezeichnen wir mit dem Buchstaben C. Da ihre Anzahl stets $= \frac{p-1}{2}$ ist, ist sie gerade, wenn p die Form $4n+1$ hat, und ungerade, wenn p die Form $4n+3$ hat. Wie in Artikel 77, wo es um Zahlen im Allgemeinen ging, nennen wir solche Reste *Partner*, deren Produkt $\equiv 1 \pmod{p}$ ist. Denn ist r ein Rest, so ist offensichtlich auch $\frac{1}{r} \pmod{p}$ ein Rest. Da derselbe Rest unter den Resten C nicht mehrere Partner haben kann, lassen sich alle Reste C in Klassen einteilen, von denen jede zwei als Partner zusammengehörige Reste enthält. Gäbe es keinen Rest, der sein eigener Partner ist, *das heißt,* enthielte jede Klasse zwei *verschiedene* Reste, so wäre die Anzahl aller Reste doppelt so groß wie die Anzahl aller Klassen. Gibt es dagegen Reste, die ihre eigenen Partner sind, *das heißt* Klassen, die nur einen Rest oder, wenn man lieber will, denselben Rest zweimal enthalten, und setzt man die Anzahl dieser Klassen $= a$, die der übrigen $= b$, so ist die Anzahl aller Reste C dann $= a + 2b$. Hat also p die Form $4n+1$, so ist a gerade; hat p die Form $4n+3$, so ist a ungerade. Zahlen kleiner als p können aber nur dann ihre eigenen Partner sein, wenn sie 1 oder

$p-1$ sind (siehe Artikel 77), und die erste Zahl, 1, kommt sicher unter den Resten vor. Daher muss im ersten Fall $p-1$ (oder, was hier dasselbe bedeutet, -1) ein Rest sein, im zweiten dagegen ein Nichtrest; sonst wäre im ersten Fall $a = 1$, im zweiten $= 2$, was unmöglich ist.

110.

Auch dieser Beweis stammt von dem bedeutenden Euler, der auch als Erster den vorigen Beweis gefunden hat. Siehe *Opusc. Anal. Bd. I, S. 135.* — Man erkennt leicht, dass er auf ähnlichen Grundsätzen beruht wie unser zweiter Beweis des Wilsonschen Satzes in Artikel 77. Wenn wir aber diesen Satz voraussetzen, lässt sich der Beweis noch leichter führen. Unter den Zahlen $1, 2, 3 \ldots p-1$ gibt es nämlich $\frac{p-1}{2}$ quadratische Reste von p und ebenso viele Nichtreste. Die Anzahl der Nichtreste ist daher gerade, wenn p die Form $4n+1$ hat, und ungerade, wenn p die Form $4n+3$ hat. Somit ist das Produkt aller Zahlen $1, 2, 3 \ldots p-1$ im ersten Fall ein Rest, im zweiten ein Nichtrest (Artikel 99). Dieses Produkt ist aber stets $\equiv -1 \pmod{p}$; also ist auch -1 im ersten Fall ein Rest, im zweiten ein Nichtrest.

111.

Ist also r ein Rest einer Primzahl der Form $4n+1$, so ist auch $-r$ ein Rest dieser Primzahl. Alle Nichtreste einer solchen Zahl bleiben dagegen auch bei umgekehrtem Vorzeichen Nichtreste[*)]. Bei Primzahlen der Form $4n+3$ ist es umgekehrt: Beim Wechsel des Vorzeichens werden Reste zu Nichtresten und Nichtreste zu Resten. Siehe Artikel 98.

Aus dem Vorigen ergibt sich außerdem leicht die allgemeine Regel: -1 *ist ein Rest aller Zahlen, die weder durch* 4 *noch durch eine Primzahl der Form* $4n+3$ *teilbar sind, und ein Nichtrest aller übrigen Zahlen.* Siehe Artikel 103 und 105.

[*)] Wenn wir also über eine Zahl als Rest oder Nichtrest einer Zahl der Form $4n+1$ sprechen, können wir ihr Vorzeichen ganz außer Acht lassen oder ihr auch das doppelte Vorzeichen $\pm$ geben.

Die Reste +2 und −2.

112.

Wir gehen zu den Resten +2 und −2 über.

Sammeln wir aus Tabelle II alle Primzahlen, für die +2 ein Rest ist, so erhalten wir $7, 17, 23, 31, 41, 47, 71, 73, 79.89, 97$. Man bemerkt leicht, dass keine davon die Form $8n + 3$ oder $8n + 5$ hat.

Sehen wir also nach, ob sich diese Beobachtung zur Gewissheit machen lässt.

Zunächst muss jede zusammengesetzte Zahl der Form $8n + 3$ oder $8n + 5$ einen Primfaktor einer der Formen $8n + 3$ oder $8n + 5$ enthalten. Denn aus Primzahlen der Formen $8n + 1$, $8n + 7$ allein lassen sich nur Zahlen der Form $8n + 1$ oder $8n + 7$ zusammensetzen. Gilt unsere Beobachtung also allgemein, so gibt es überhaupt keine Zahl der Form $8n + 3$, $8n + 5$, für die +2 ein Rest ist. Jedenfalls gibt es unterhalb von 100 keine solche Zahl, für die +2 ein Rest ist. Finden sich aber jenseits dieser Grenze solche Zahlen, so sei die kleinste $= t$. Dann hat t entweder die Form $8n+3$ oder $8n+5$; +2 ist ein Rest davon, aber ein Nichtrest aller kleineren Zahlen dieser Formen. Wir setzen $2 \equiv aa \pmod{t}$. Dabei lässt sich a stets ungerade und $< t$ wählen (denn a hat mindestens zwei positive Werte unterhalb von t, deren Summe $= t$ ist, sodass einer gerade und der andere ungerade ist; siehe Artikel 104 und 105). Dann sei $aa = 2 + tu$ oder $tu = aa - 2$. Somit hat aa die Form $8n + 1$, also tu die Form $8n - 1$, und folglich u die Form $8n + 3$ oder $8n + 5$, je nachdem, ob t die zweite oder die erste Form hat. Aus der Gleichung $aa = 2 + tu$ folgt aber auch $2 \equiv aa \pmod{u}$, *das heißt,* 2 ist auch ein Rest von u. Man sieht leicht, dass $u < t$ gilt. Also ist t nicht die kleinste Zahl, die unserer Beobachtung widerspricht, entgegen der Voraussetzung. Damit gilt das durch Zahlenbeispiele gefundene Muster allgemein.

Verbinden wir dies mit der Aussage von Artikel 111, so erhalten wir folgende Sätze.

I. *Für alle Primzahlen der Form* $8n + 3$ *ist* +2 *ein Nichtrest,* −2 *dagegen ein Rest.*

II. *Für alle Primzahlen der Form* $8n + 5$ *sind sowohl* +2 *als auch* −2 *Nichtreste.*

113.

Ebenso finden wir durch Betrachtung der Tabelle II die folgenden Primzahlen, für die −2 ein Rest ist: $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$[*)]. Keine davon hat die Form $8n + 5$, $8n + 7$. Untersuchen wir also, ob sich auch diese Beobachtung als allgemeiner Satz beweisen lässt. Wie im vorigen Artikel zeigt man, dass jede zusammengesetzte Zahl der Form $8n+5$ oder $8n+7$ einen Primfaktor der Form $8n+5$ oder $8n + 7$ enthält. Gilt unsere Beobachtung allgemein, so kann −2 überhaupt kein Rest einer Zahl der Form $8n + 5$ oder $8n + 7$ sein. Gäbe es solche Zahlen, so sei die kleinste $= t$, und wir setzen $-2 = aa - tu$. Wählen wir wie oben a ungerade und kleiner als t, so hat u die Form $8n + 5$ oder $8n + 7$, je nachdem, ob t die Form $8n + 7$ oder $8n + 5$ hat. Aus $aa + 2 = tu$ und $a < t$ folgt leicht, dass auch u kleiner als t ist. Schließlich ist −2 auch ein Rest von u, *das heißt,* t ist nicht die kleinste Zahl, die unserer Beobachtung widerspricht, entgegen der Voraussetzung. Also muss −2 ein Nichtrest aller Zahlen der Formen $8n + 5$, $8n + 7$ sein.

[*)] Indem wir −2 als Produkt von +2 und −1 betrachten; siehe Artikel 111.

Mit der Aussage von Artikel 111 ergeben sich daraus folgende Sätze:

I. *Für alle Primzahlen der Form* $8n + 5$ *sind sowohl* -2 *als auch* $+2$ *Nichtreste,* wie wir bereits im vorigen Artikel gefunden haben.

II. *Für alle Primzahlen der Form* $8n + 7$ *ist* -2 *ein Nichtrest,* $+2$ *dagegen ein Rest.*

In beiden Beweisen hätten wir für a auch einen geraden Wert wählen können. Dann hätten wir den Fall, dass a die Form $4n + 2$ hat, von dem Fall unterscheiden müssen, dass a die Form $4n$ hat. Der weitere Beweis verläuft wie oben und bereitet keine Schwierigkeit.

114.

Ein Fall bleibt noch übrig: Die Primzahl hat die Form $8n + 1$. Dieser Fall entzieht sich der vorigen Methode und erfordert ganz andere Kunstgriffe.

Für den Primzahlmodul $8n + 1$ sei a eine beliebige primitive Wurzel. Dann gilt (Artikel 62) $a^{4n} \equiv -1 \pmod{8n+1}$. Diese Kongruenz lässt sich auch als $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n + 1}$ oder als $(a^{2n} - 1)^2 \equiv -2a^{2n}$ schreiben. Daher sind sowohl $2a^{2n}$ als auch $-2a^{2n}$ Reste von $8n + 1$. Da aber a^{2n} ein Quadrat ist, das nicht durch den Modul teilbar ist, sind auch $+2$ und -2 Reste (Artikel 98).

115.

Es wird nützlich sein, noch einen anderen Beweis dieses Satzes anzufügen. Er steht zum vorigen in einer ähnlichen Beziehung wie der zweite Beweis (Artikel 109) des Satzes aus Artikel 108 zum ersten (Artikel 108). Mit diesen Fragen vertraute Leser werden dann leichter erkennen, dass weder das eine noch das andere Beweispaar so verschieden ist, wie es auf den ersten Blick scheinen mag.

I. Für einen beliebigen Primzahlmodul der Form $4m + 1$ gibt es unter den kleineren Zahlen $1, 2, 3 \ldots 4m$ genau m, die einer vierten Potenz kongruent sein können; die übrigen $3m$ können es nicht.

Dies folgt leicht aus den Grundsätzen des vorigen Abschnitts, lässt sich aber auch ohne diese Grundsätze leicht beweisen. Wir haben nämlich gezeigt, dass für einen solchen Modul -1 stets ein quadratischer Rest ist. Sei also $ff \equiv -1$. Ist z eine beliebige nicht durch den Modul teilbare Zahl, so sind die vierten Potenzen der vier Zahlen $+z, -z, +fz, -fz$ (die offensichtlich inkongruent sind) untereinander kongruent. Die vierte Potenz einer Zahl, die keiner dieser vier kongruent ist, kann ihren vierten Potenzen nicht kongruent sein. Sonst hätte die Kongruenz $x^4 \equiv z^4$, die vom vierten Grad ist, mehr als 4 Wurzeln, entgegen Artikel 43. Somit liefern alle Zahlen $1, 2, 3, \ldots 4m$ nur m inkongruente vierte Potenzen. Unter denselben Zahlen sind m diesen kongruent; die übrigen können keiner vierten Potenz kongruent sein.

II. Nach einem Primzahlmodul der Form $8n + 1$ kann -1 einer vierten Potenz kongruent sein (-1 ist ein *biquadratischer Rest* dieser Primzahl).

Denn die Anzahl aller biquadratischen Reste unterhalb von $8n+1$ (null ausgeschlossen) ist $= 2n$, *das heißt,* gerade. Ferner zeigt man leicht: Ist r ein biquadratischer Rest von $8n + 1$, so ist auch der Wert des Ausdrucks $\frac{1}{r} \pmod{8n + 1}$ ein solcher Rest. Daher lassen sich alle biquadratischen Reste so in Klassen einteilen, wie wir in Artikel 109 die quadratischen Reste eingeteilt haben. Auch der übrige Teil des Beweises verläuft genau wie dort.

III. Nun sei $g^4 \equiv -1$, und h sei der Wert des Ausdrucks $\frac{1}{g} \pmod{8n+1}$. Dann gilt

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$$

(wegen $gh \equiv 1$). Aber es gilt $g^4 \equiv -1$, also $-h^2 \equiv g^4 h^2 \equiv g^2$, und schließlich $g^2 + h^2 \equiv 0$ sowie $(g \pm h)^2 \equiv \pm 2$; *das heißt,* sowohl $+2$ als auch -2 sind quadratische Reste von $8n+1$. *Q. E. D.*

116.

Aus dem Vorigen ergibt sich außerdem leicht die allgemeine Regel: $+2$ *ist ein Rest jeder Zahl, die weder durch* 4 *noch durch eine Primzahl der Form* $8n+3$ *oder* $8n+5$ *teilbar ist; dagegen ist es ein Nichtrest aller übrigen Zahlen* (*zum Beispiel* aller Zahlen der Formen $8n+3$, $8n+5$, ob sie Primzahlen oder zusammengesetzt sind).

-2 *ist ein Rest jeder Zahl, die weder durch* 4 *noch durch eine Primzahl der Form* $8n+5$ *oder* $8n+7$ *teilbar ist, und ein Nichtrest aller übrigen Zahlen.*

Diese eleganten Sätze waren schon dem scharfsinnigen Fermat bekannt, *Op. Mathem., S.* 168. Einen Beweis, den er nach eigener Aussage besaß, hat er aber nirgends mitgeteilt. Später suchte der bedeutende Euler stets vergeblich danach; der bedeutende Lagrange fand als Erster einen strengen Beweis, *Nouv. Mém. de l'Ac. de Berlin*, 1775, *S.* 349, 351. Dies scheint Euler noch nicht bekannt gewesen zu sein, als er die in *Opusc. Analyt.*, Bd. I, S. 259, enthaltene Abhandlung schrieb.

Die Reste $+3$ *und* -3.

117.

Wir gehen zu den Resten $+3$ und -3 über und beginnen mit dem letzteren.

Aus Tabelle II finden wir folgende Primzahlen, für die -3 ein Rest ist: 3, 7. 13, 19, 31, 37, 43, 61, 67, 73, 79, 97. Keine davon hat die Form $6n+5$. Dass es auch jenseits der Tabelle keine Primzahlen dieser Form gibt, für die -3 ein Rest ist, beweisen wir so: Zunächst enthält jede zusammengesetzte Zahl der Form $6n+5$ einen Primfaktor derselben Form. Solange es also keine Primzahlen der Form $6n+5$ gibt, für die -3 ein Rest ist, gibt es auch keine solchen zusammengesetzten Zahlen. Gäbe es aber jenseits der Tabelle solche Zahlen, so sei die kleinste $= t$, und wir setzen $-3 = aa - tu$. Wählen wir a gerade und kleiner als t, so gilt $u < t$, und -3 ist ein Rest von u. Hat a die Form $6n \pm 2$, so hat tu die Form $6n+1$ und damit u die Form $6n+5$. *Q. E. A.* Denn wir haben angenommen, dass t die kleinste unserer Beobachtung widersprechende Zahl ist. Hat dagegen a die Form $6n$, so hat tu die Form $36n+3$, also $\frac{1}{3}tu$ die Form $12n+1$, und daher $\frac{1}{3}u$ die Form $6n+5$. Aber -3 ist auch ein Rest von $\frac{1}{3}u$, und es gilt $\frac{1}{3}u < t$, *Q. E. A.* Somit kann -3 kein Rest einer Zahl der Form $6n+5$ sein.

Jede Zahl der Form $6n+5$ hat entweder die Form $12n+5$ oder $12n+11$. Die erste Form ist in $4n+1$ enthalten, die zweite in $4n+3$. Daher gelten die folgenden Sätze:

I. *Für jede Primzahl der Form* $12n+5$ *sind sowohl* -3 *als auch* $+3$ *Nichtreste.*

II. *Für jede Primzahl der Form* $12n+11$ *ist* -3 *ein Nichtrest,* $+3$ *dagegen ein Rest.*

118.

Aus Tabelle II finden wir die folgenden Zahlen, für die +3 ein Rest ist: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97. Keine davon hat die Form $12n+5$ oder $12n+7$. Dass es überhaupt keine Zahlen der Formen $12n+5$, $12n+7$ gibt, für die +3 ein Rest ist, lässt sich genau wie in den Artikeln 112, 113 und 117 beweisen; deshalb verzichten wir hier darauf. Mit Artikel 111 erhalten wir die Sätze:

I. *Für jede Primzahl der Form* $12n+5$ *sind sowohl* +3 *als auch* −3 *Nichtreste* (wie schon im vorigen Artikel gefunden).

II. *Für jede Primzahl der Form* $12n+7$ *ist* +3 *ein Nichtrest,* −3 *dagegen ein Rest.*

119.

Für Zahlen der Form $12n+1$ liefert diese Methode aber kein Ergebnis; sie erfordern also besondere Kunstgriffe. Zahlenbeispiele legen nahe, dass +3 und −3 Reste aller Primzahlen dieser Form sind. Man muss nur beweisen, dass −3 ein Rest solcher Zahlen ist, denn dann muss auch +3 ein Rest sein (Artikel 111). Wir zeigen aber allgemeiner, dass −3 ein Rest jeder Primzahl der Form $3n+1$ ist.

Sei p eine solche Primzahl und a eine Zahl, die für den Modul p zum Exponenten 3 gehört (solche Zahlen gibt es nach Artikel 54, da 3 ein Teiler von $p-1$ ist). Dann gilt $a^3 \equiv 1 \pmod{p}$, *das heißt,* a^3-1 oder $(a^2+a+1)(a-1)$ ist durch p teilbar. Aber a kann nicht $\equiv 1 \pmod{p}$ sein, da 1 zum Exponenten 1 gehört. Also ist $a-1$ nicht durch p teilbar, wohl aber a^2+a+1 und daher auch $4aa+4a+4$; *das heißt,* es gilt $(2a+1)^2 \equiv -3 \pmod{p}$, oder −3 ist ein Rest von p. *Q. E. D.*

Dieser Beweis, der von den vorigen unabhängig ist, umfasst auch die Primzahlen der Form $12n+7$, die wir schon im vorigen Artikel behandelt haben.

Man kann noch bemerken, dass sich dieser Gedankengang auch nach dem Vorbild der Methode in den Artikeln 109 und 115 darstellen lässt. Der Kürze wegen gehen wir darauf nicht weiter ein.

120.

Aus dem Vorigen ergeben sich leicht die folgenden Sätze (siehe Artikel 102, 103 und 105).

I. −3 *ist ein Rest aller Zahlen, die weder durch* 8 *noch durch* 9 *noch durch eine Primzahl der Form* $6n+5$ *teilbar sind, und ein Nichtrest aller übrigen Zahlen.*

II. +3 *ist ein Rest aller Zahlen, die weder durch* 4 *noch durch* 9 *noch durch eine Primzahl der Form* $12n+5$ *oder* $12n+7$ *teilbar sind, und ein Nichtrest aller übrigen Zahlen.*

Besonders sollte man sich diesen Spezialfall merken:

−3 ist ein *Rest* aller Primzahlen der Form $3n+1$, oder gleichbedeutend *aller Primzahlen, die Reste von* 3 *sind*; dagegen ein *Nichtrest* aller Primzahlen der Form $6n+5$ oder, wenn man 2 ausschließt, aller Primzahlen der Form $3n+2$, *das heißt aller, die Nichtreste von* 3 *sind.* Alle übrigen Fälle folgen daraus offensichtlich von selbst.

Die Aussagen über die Reste $+3$ und -3 waren schon Fermat bekannt, *Opera Wallisii*, Bd. II, *S.* 857. Doch der bedeutende Euler gab als Erster Beweise, *Comm. nov. Petr.*, Bd. VIII, *S.* 105 ff. Umso überraschender ist es, dass ihm die Beweise der Aussagen über die Reste $+2$ und -2, die auf ganz ähnlichen Kunstgriffen beruhen, trotz seines Scharfsinns stets entgingen. Siehe auch die Abhandlung des bedeutenden Lagrange, *Nouv. Mém. de l'Ac. de Berlin*, 1775, *S.* 352.

Die Reste $+5$ *und* -5.

121.

Zahlenbeispiele legen nahe, dass $+5$ ein Nichtrest jeder ungeraden Zahl der Form $5n+2$ oder $5n+3$ ist, *das heißt* jeder ungeraden Zahl, die ein Nichtrest von 5 ist. Dass diese Regel keine Ausnahme zulässt, beweisen wir so. Die kleinste Ausnahme, falls es eine gibt, sei $= t$. Sie ist also ein Nichtrest von 5, während 5 ein Rest von t ist. Sei $aa = 5 + tu$, wobei a gerade und kleiner als t ist. Dann ist u ungerade und kleiner als t, und $+5$ ist ein Rest von u. Ist nun a nicht durch 5 teilbar, so ist es auch u nicht. Aber tu ist offensichtlich ein Rest von 5, und da t ein Nichtrest von 5 ist, ist auch u ein Nichtrest. *Das heißt,* es gibt einen ungeraden Nichtrest von 5, für den $+5$ ein Rest ist, unterhalb von t, entgegen der Voraussetzung. Ist dagegen a durch 5 teilbar, so setze man $a = 5b$ und $u = 5v$. Daraus folgt $tv \equiv -1 \equiv 4 \pmod 5$, *das heißt, tv* ist ein Rest von 5. Der übrige Beweis verläuft wie im ersten Fall.

122.

Für alle Primzahlen, die Nichtreste von 5 sind und zugleich die Form $4n+1$ haben, *das heißt* für alle Primzahlen der Form $20n+13$ oder $20n+17$, sind also sowohl $+5$ als auch -5 Nichtreste. Für alle Primzahlen der Form $20n+3$ oder $20n+7$ ist dagegen $+5$ ein Nichtrest, -5 ein Rest.

Ganz ähnlich lässt sich zeigen, dass -5 ein Nichtrest aller Primzahlen der Formen $20n+11$, $20n+13$, $20n+17$, $20n+19$ ist. Daraus folgt, dass $+5$ ein Rest aller Primzahlen der Form $20n+11$ oder $20n+19$ und ein Nichtrest aller Primzahlen der Form $20n+13$ oder $20n+17$ ist. Da jede Primzahl außer 2 und 5 (für die ± 5 ein Rest ist) eine der Formen $20n+1, 3, 7, 9, 11, 13, 17, 19$ hat, können wir nun alle Fälle entscheiden, außer denen der Form $20n+1$ oder $20n+9$.

123.

Zahlenbeispiele legen nahe, dass $+5$ und -5 Reste aller Primzahlen der Form $20n+1$ oder $20n+9$ sind. Gilt dies allgemein, so haben wir das elegante Gesetz, dass $+5$ *ein Rest aller Primzahlen ist, die Reste von 5 sind* (denn diese haben eine der Formen $5n+1$ oder $5n+4$, also eine der Formen $20n+1, 9, 11, 19$; für die dritte und vierte dieser Formen ist die Aussage schon bewiesen), *dagegen ein Nichtrest aller ungeraden Zahlen, die Nichtreste von 5 sind*, wie wir bereits oben gezeigt haben. Dieser Satz genügt offensichtlich, um zu entscheiden, ob $+5$ (und damit auch -5, als Produkt von $+5$ und -1 betrachtet) ein Rest oder Nichtrest einer beliebigen gegebenen Zahl ist. Schließlich beachte man die Analogie zu dem Satz über den Rest -3 in Artikel 120.

Diese Beobachtung zu beweisen ist jedoch nicht so leicht. Für eine Primzahl der Form $20n+1$ oder allgemeiner der Form $5n+1$ lässt sich ähnlich wie in den Artikeln 114 und 119 vorgehen. Für den Modul $5n+1$ sei a eine beliebige zum Exponenten 5 gehörige Zahl; solche Zahlen gibt es nach dem vorigen Abschnitt. Dann gilt $a^5 \equiv 1$ oder $(a-1)(a^4+a^3+a^2+a+1) \equiv 0 \pmod{5n+1}$. Da aber $a \equiv 1$ und damit auch $a-1 \equiv 0$ unmöglich ist, muss $a^4+a^3+a^2+a+1 \equiv 0$ sein. Somit ist auch $4(a^4+a^3+a^2+a+1) = (2aa+a+2)^2 - 5a^2 \equiv 0$, *das heißt,* $5a^2$ ist ein Rest von $5n+1$, also auch 5, denn a^2 ist ein nicht durch $5n+1$ teilbarer Rest (denn a ist nicht durch $5n+1$ teilbar, da $a^5 \equiv 1$). *Q. E. D.*

Der Fall einer Primzahl der Form $5n+4$ erfordert dagegen feinere Methoden. Da wir die Sätze, mit denen er sich entscheiden lässt, später allgemeiner behandeln werden, gehen wir hier nur kurz auf sie ein.

I. Ist p eine Primzahl und b ein gegebener quadratischer Nichtrest von p, so ist der Wert des Ausdrucks

$$(A)\ldots \quad \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}}$$

(aus dessen Entwicklung die Irrationalität offensichtlich verschwindet) stets durch p teilbar, welche Zahl man auch für x einsetzt. Betrachtet man die Koeffizienten in der Entwicklung von A, so sieht man, dass alle Glieder vom zweiten bis zum vorletzten einschließlich durch p teilbar sind. Also gilt $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}$. Da aber b ein Nichtrest von p ist, gilt $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (Artikel 106), während x^p stets $\equiv x$ ist (voriger Abschnitt). Daraus folgt $A \equiv 0$. *Q. E. D.*

II. In der Kongruenz $A \equiv 0 \pmod{p}$ hat die Unbestimmte x den Grad p, und alle Zahlen $0, 1, 2....p-1$ sind ihre Wurzeln. Sei nun e ein Teiler von $p+1$. Dann ist der Ausdruck

$$\frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$$

(den wir mit B bezeichnen) nach der Entwicklung frei von Irrationalität; die Unbestimmte x hat darin den Grad $e-1$. Aus den Grundlagen der Analysis ist bekannt, dass A durch B identisch teilbar ist. Ich behaupte nun, dass es $e-1$ Werte von x gibt, die, in B eingesetzt, B durch p teilbar machen. Setzen wir nämlich $A \equiv BC$, so hat x in C den Grad $p-e+1$. Die Kongruenz $C \equiv 0 \pmod{p}$ hat daher höchstens $p-e+1$ Wurzeln. Somit sind alle übrigen Zahlen unter $0, 1, 2, 3....p-1$, deren Anzahl $= e-1$ ist, Wurzeln der Kongruenz $B \equiv 0$.

III. Nun habe p die Form $5n+4$, es sei $e=5$, b ein Nichtrest von p, und die Zahl a sei so bestimmt, dass

$$\frac{(a+\sqrt{b})^5 - (a-\sqrt{b})^5}{\sqrt{b}}$$

durch p teilbar ist. Dieser Ausdruck wird aber zu

$$= 10a^4 + 20aab + 2bb = 2((b+5aa)^2 - 20a^4)$$

Also ist auch $(b + 5aa)^2 - 20a^4$ durch p teilbar, *das heißt,* $20a^4$ ist ein Rest von p. Da aber $4a^4$ ein nicht durch p teilbarer Rest ist (denn a kann offensichtlich nicht durch p teilbar sein), ist auch 5 ein Rest von p. *Q. E. D.*

Damit gilt der am Anfang dieses Artikels angegebene Satz allgemein. —

Wir bemerken noch, dass die Beweise für beide Fälle von dem bedeutenden Lagrange stammen, *Mém. de l'Ac. de Berlin*, 1775, *S.* 352 ff.

Über ± 7.

124.

Durch eine ähnliche Methode beweist man, dass

-7 *ein Nichtrest jeder Zahl ist, die ein Nichtrest von* 7 *ist.*

Zahlenbeispiele legen dagegen nahe, dass

-7 *ein Rest jeder Primzahl ist, die ein Rest von* 7 *ist.*

Doch dies hat bisher niemand streng bewiesen. Für die Reste von 7, die die Form $4n - 1$ haben, ist der Beweis leicht. Mit einer aus dem Vorigen schon vertrauten Methode lässt sich zeigen, dass $+7$ stets ein Nichtrest solcher Primzahlen ist, also -7 ein Rest. Damit ist aber wenig gewonnen, denn die übrigen Fälle lassen sich so nicht behandeln. Einen weiteren Fall können wir ähnlich wie in den Artikeln 119, 123 erledigen. Ist nämlich p eine Primzahl der Form $7n + 1$ und a für den Modul p eine zum Exponenten 7 gehörige Zahl, so ist

$$\frac{4(a^7 - 1)}{a - 1} = (2a^3 + a^2 - a - 2)^2 + 7(a^2 + a)^2$$

offensichtlich durch p teilbar, also $-7(a^2 + a)^2$ ein Rest von p. Aber $(a^2 + a)^2$ ist als Quadrat ein Rest von p und zudem nicht durch p teilbar. Denn da a nach Voraussetzung zum Exponenten 7 gehört, kann es weder $\equiv 0$ noch $\equiv -1 \pmod{p}$ sein. *Das heißt,* weder a noch $a + 1$ ist durch p teilbar und somit auch nicht das Quadrat $(a + 1)^2 a^2$. Also ist auch 7 offensichtlich ein Rest von p. *Q. E. D.* — Die Primzahlen der Form $7n+2$ oder $7n+4$ entziehen sich jedoch allen bisher angegebenen Methoden. Auch diesen Beweis hat der bedeutende Lagrange zuerst an der angegebenen Stelle gefunden. — In Abschnitt VII werden wir allgemein zeigen, dass sich der Ausdruck $\frac{4(x^p-1)}{x-1}$ immer auf die Form $X^2 \mp pY^2$ bringen lässt (wobei das obere Zeichen gilt, wenn p eine Primzahl der Form $4n + 1$ ist, das untere bei der Form $4n + 3$); dabei bezeichnen X, Y rationale Funktionen von x, die keine Brüche enthalten. Über den Fall $p = 7$ hinaus hat Lagrange diese Zerlegung nicht ausgeführt; siehe die angegebene Stelle, S. 352.

Vorbereitung auf die allgemeine Untersuchung.

125.

Da die vorigen Methoden nicht ausreichen, um allgemeine Beweise zu führen, ist es Zeit, eine andere ohne diesen Mangel anzugeben. Wir beginnen mit einem Satz, dessen Beweis unseren Bemühungen ziemlich lange widerstanden hat, obwohl er auf den ersten Blick so offensichtlich erscheint, dass einige nicht einmal die Notwendigkeit eines Beweises erkannt haben. Er lautet: *Jede Zahl außer den positiv genommenen Quadraten ist ein Nichtrest gewisser Primzahlen.* Da wir diesen Satz nur als Hilfsmittel für andere Beweise verwenden, behandeln wir hier nur die dafür nötigen Fälle. Für die übrigen Fälle wird sich dasselbe später von selbst ergeben. Wir zeigen also, dass *jede Primzahl der Form* $4n+1$*, ob positiv oder negativ genommen*[*)]*, ein Nichtrest gewisser Primzahlen ist*, und zwar, falls > 5, solcher Primzahlen, die kleiner als sie selbst sind.

Erstens: Sei die Primzahl p der Form $4n+1$ (> 17; aber $-13\,N3$, $-17\,N5$) *negativ* zu nehmen. Sei $2a$ die gerade Zahl unmittelbar oberhalb von $\sqrt{p}$. Dann ist $4aa$ offensichtlich stets $< 2p$, also $4aa - p < p$. Aber $4aa - p$ hat die Form $4n+3$, und $+p$ ist ein quadratischer Rest von $4aa - p$ (denn $p \equiv 4aa \pmod{4aa-p}$). Ist also $4aa - p$ eine Primzahl, so ist $-p$ ein Nichtrest davon. Andernfalls muss $4aa - p$ einen Faktor der Form $4n+3$ haben. Da $+p$ auch von diesem ein Rest sein muss, ist $-p$ ein Nichtrest davon. *Q. E. D.*

Für *positiv* zu nehmende Primzahlen unterscheiden wir zwei Fälle. *Erstens:* Sei p eine Primzahl der Form $8n+5$. Sei a eine beliebige positive Zahl $< \sqrt{\frac{1}{2}p}$. Dann ist $8n+5-2aa$ eine positive Zahl der Form $8n+5$ oder $8n+3$, je nachdem, ob a gerade oder ungerade ist. Sie ist daher durch eine Primzahl der Form $8n+3$ oder $8n+5$ teilbar; denn ein Produkt beliebig vieler Zahlen der Formen $8n+1$ und $8n+7$ kann weder die Form $8n+3$ noch die Form $8n+5$ haben. Diese Primzahl sei q; dann gilt $8n+5 \equiv 2a^2 \pmod{q}$. Aber 2 ist ein Nichtrest von q (Artikel 112), also auch $2a^2$[*)] und $8n+5$. *Q. E. D.*

126.

Dass jede positiv genommene Primzahl der Form $8n+1$ ein Nichtrest einer kleineren Primzahl ist, lässt sich aber nicht durch so naheliegende Kunstgriffe beweisen. Diese Wahrheit ist von größter Bedeutung; deshalb können wir einen strengen Beweis nicht übergehen, auch wenn er etwas länger ist. Wir stellen folgendes Lemma voran.

[*)] Dass $+1$ ausgeschlossen werden muss, ist für sich klar.

[*)] Artikel 98. Denn a^2 ist ein Rest von q, der nicht durch q teilbar ist; sonst wäre auch die Primzahl p durch q teilbar. *Q. E. A.*

Lemma. *Es seien zwei Zahlenfolgen*

$$A, B, C \text{ usw. } .... \text{ (I)}, \quad A', B', C' \text{ usw. } .... \text{ (II)}$$

(ob sie dieselbe Anzahl von Gliedern haben, spielt keine Rolle) *so beschaffen, dass für jede Primzahl oder Primzahlpotenz p, die ein Glied oder mehrere Glieder der zweiten Folge teilt, mindestens ebenso viele Glieder der ersten Folge durch p teilbar sind wie Glieder der zweiten. Dann behaupte ich, dass das Produkt aller Zahlen* (I) *durch das Produkt aller Zahlen* (II) *teilbar ist.*

Beispiel. (I) bestehe aus den Zahlen $12, 18, 45$, (II) aus $3, 4, 5, 6, 9$. Dann sind durch $2, 4, 3, 9, 5$ in (I) jeweils $2, 1, 3, 2, 1$ Glieder, in (II) jeweils $2, 1, 3, 1, 1$ Glieder teilbar. Das Produkt aller Glieder von (I), $= 9720$, ist durch das Produkt aller Glieder von (II), 3240, teilbar.

Beweis. Das Produkt aller Glieder von (I) sei $= Q$, das aller Glieder von (II) $= Q'$. Jede Primzahl, die Q' teilt, teilt offensichtlich auch Q. Wir zeigen nun, dass jeder Primfaktor von Q' in Q einen mindestens ebenso großen Exponenten hat wie in Q'. Sei p ein solcher Teiler. In der Folge (I) seien a Glieder durch p, b Glieder durch p^2, c Glieder durch p^3 teilbar usw.; die Buchstaben a', b', c' usw. bedeuten Entsprechendes für (II). Dann hat p in Q offensichtlich den Exponenten $a+b+c+$ usw., in Q' dagegen $a'+b'+c'+$ usw. Nach Voraussetzung ist aber a' nicht größer als a, b' nicht größer als b usw. Daher ist $a'+b'+c'$ usw. sicher nicht $> a+b+c$ usw. — Da also keine Primzahl in Q' einen größeren Exponenten haben kann als in Q, ist Q durch Q' teilbar (Artikel 17). *Q. E. D.*

127.

Lemma. *In der Folge* $1, 2, 3, 4, ...n$ *können nicht mehr Glieder durch eine beliebige Zahl h teilbar sein als in der Folge* $a, a+1, a+2.....a+n-1$*, die ebenso viele Glieder hat.*

Ist n ein Vielfaches von h, so sind in beiden Folgen offensichtlich $\frac{n}{h}$ Glieder durch h teilbar. Andernfalls setze man $n = eh+f$, wobei $f < h$ ist. Dann sind in der ersten Folge e Glieder durch h teilbar, in der zweiten entweder ebenso viele oder $e+1$.

Als Folgerung ergibt sich der aus der Theorie der figurierten Zahlen bekannte, aber, wenn wir uns nicht irren, bisher von niemandem direkt bewiesene Satz, dass

$$\frac{a.a+1.a+2....a+n-1}{1\ .\ 2\ .\ 3\ ....\ n}$$

stets eine ganze Zahl ist.

Schließlich hätte man das Lemma allgemeiner so aussprechen können:

In der Folge $a, a+1, a+2, ...a+n-1$ gibt es mindestens ebenso viele Glieder, die nach dem Modul h einer beliebigen gegebenen Zahl r kongruent sind, wie in der Folge $1, 2, 3....n$ Glieder durch h teilbar sind.

128.

Satz. *Sei a eine beliebige Zahl der Form $8n+1$, p eine beliebige zu a teilerfremde Zahl, von der $+a$ ein Rest ist, und schließlich m beliebig. Dann behaupte ich, dass in der Folge*

$$a,\ \tfrac{1}{2}(a-1),\ 2(a-4),\ \tfrac{1}{2}(a-9),\ 2(a-16),$$
$$\ldots.\ 2(a-m^2),\quad \textit{oder}\quad \tfrac{1}{2}(a-m^2)$$

je nachdem, ob m gerade oder ungerade ist, mindestens ebenso viele Glieder durch p teilbar sind wie in der Folge

$$1,\ 2,\ 3,\ \ldots.\ 2m+1$$

Die erste Folge bezeichnen wir mit (I), die zweite mit (II).

Beweis. I. Ist $p = 2$, so sind in (I) alle Glieder außer dem ersten, *das heißt* m Glieder, teilbar; ebenso viele sind es in (II).

II. Sei p eine ungerade Zahl oder das Doppelte oder Vierfache einer ungeraden Zahl, und es gelte $a \equiv rr \pmod{p}$. Dann gibt es in der Folge $-m, -(m-1), -(m-2), \ldots.+m$ (die ebenso viele Glieder wie (II) hat und mit (III) bezeichnet wird) mindestens ebenso viele Glieder, die nach dem Modul p der Zahl r kongruent sind, wie in (II) Glieder durch p teilbar sind (voriger Artikel). Unter diesen können aber keine zwei vorkommen, die sich nur im Vorzeichen, nicht im Betrag unterscheiden[*]. Jedem davon entspricht schließlich ein durch p teilbares Glied von (I). Ist nämlich $\pm b$ ein Glied von (III), das r nach p kongruent ist, so ist $a - bb$ durch p teilbar. Ist also b gerade, so ist das Glied $2(a-bb)$ von (I) durch p teilbar. Ist dagegen b ungerade, so ist das Glied $\frac{1}{2}(a-bb)$ durch p teilbar. Denn $\frac{a-bb}{p}$ ist offensichtlich eine *gerade* ganze Zahl, da $a - bb$ durch 8 teilbar ist, p aber durch keine höhere Zweierpotenz als 4 teilbar ist (denn a hat nach Voraussetzung die Form $8n+1$, und bb als Quadrat einer ungeraden Zahl dieselbe Form; die Differenz hat also die Form $8n$). Somit gibt es in (I) ebenso viele durch p teilbare Glieder wie in (III) Glieder, die r nach p kongruent sind, *das heißt* mindestens ebenso viele, wie in (II) durch p teilbar sind. *Q. E. D.*

III. Sei p von der Form $8n$, und es gelte $a \equiv rr \pmod{2p}$. Denn a ist, da es nach Voraussetzung ein Rest von p ist, offensichtlich auch ein Rest von $2p$. Dann gibt es in (III) mindestens ebenso viele Glieder, die r nach p kongruent sind, wie in (II) durch p teilbar sind; jene haben alle verschiedene Beträge. Jedem davon entspricht aber ein durch p teilbares Glied von (I). Denn wenn $+b$ oder $-b \equiv r \pmod{p}$, so gilt $bb \equiv rr \pmod{2p}$[†], und damit ist das Glied $\frac{1}{2}(a-bb)$ durch p teilbar. Daher gibt es in (I) mindestens ebenso viele durch p teilbare Glieder wie in (II). *Q. E. D.*

[*] Wäre nämlich $r \equiv -f \equiv +f \pmod{p}$, so wäre $2f$ durch p teilbar und damit auch $2a$ (wegen $ff \equiv a \pmod{p}$). Das ist nur möglich, wenn $p = 2$, da a nach Voraussetzung zu p teilerfremd ist. Diesen Fall haben wir aber schon gesondert behandelt.

[†] Denn $bb - rr = (b-r)(b+r)$ ist ein Produkt aus zwei Faktoren, von denen einer durch p teilbar ist (Voraussetzung), der andere durch 2 (da sowohl b als auch r ungerade sind). Also ist $bb - rr$ durch $2p$ teilbar.

129.

Satz. *Ist a eine Primzahl der Form $8n+1$, so gibt es unterhalb von $2\sqrt{a}+1$ notwendig eine Primzahl, von der a ein Nichtrest ist.*

Beweis. Nehmen wir, wenn möglich, an, dass a ein Rest aller Primzahlen unterhalb von $2\sqrt{a}+1$ ist. Dann ist a auch ein Rest aller zusammengesetzten Zahlen unterhalb von $2\sqrt{a}+1$ (siehe die Regeln zur Entscheidung, ob eine Zahl ein Rest einer zusammengesetzten Zahl ist, Artikel 105). Die ganze Zahl unmittelbar unterhalb von $\sqrt{a}$ sei $= m$. Dann gibt es in der Folge

$$\text{(I)}.....a, \tfrac{1}{2}(a-1), 2(a-4), \tfrac{1}{2}(a-9)....2(a-mm)$$
$$\text{oder} \quad \tfrac{1}{2}(a-mm)$$

mindestens ebenso viele Glieder, die durch eine beliebige Zahl unterhalb von $2\sqrt{a}+1$ teilbar sind, wie in der Folge

$$\text{(II)}.....1, 2, 3, 4....2m+1 \quad \text{(voriger Artikel)}$$

Daraus folgt, dass das Produkt aller Glieder von (I) durch das Produkt aller Glieder von (II) teilbar ist (Artikel 126). Das erste Produkt ist entweder $= a(a-1)(a-4)....(a-mm)$ oder die Hälfte davon, je nachdem, ob m gerade oder ungerade ist. Somit ist das Produkt $a(a-1)(a-4)....(a-mm)$ sicher durch das Produkt aller Glieder von (II) teilbar. Da alle diese Glieder zu a teilerfremd sind, gilt dies auch, wenn man den Faktor a weglässt. Das Produkt aller Glieder von (II) lässt sich aber auch schreiben als

$$(m+1).((m+1)^2-1).((m+1)^2-4)....((m+1)^2-m^2)$$

Also ist

$$\frac{1}{m+1}.\frac{a-1}{(m+1)^2-1}.\frac{a-4}{(m+1)^2-4}....\frac{a-m^2}{(m+1)^2-m^2}$$

eine ganze Zahl, obwohl es ein Produkt von Brüchen kleiner als eins ist. Denn $\sqrt{a}$ muss irrational sein. Daher gilt $m+1 > \sqrt{a}$ und damit $(m+1)^2 > a$. Unsere Annahme ist also unmöglich. *Q. E. D.*

Da a sicher > 9 ist, gilt $2\sqrt{a}+1 < a$. Somit gibt es eine Primzahl $< a$, von der a ein Nichtrest ist.

Ein allgemeiner (fundamentaler) Satz wird anhand von Zahlenbeispielen aufgestellt; daraus werden Folgerungen gezogen.

130.

Nachdem wir streng bewiesen haben, dass jede Primzahl der Form $4n+1$, sowohl positiv als auch negativ genommen, ein Nichtrest einer kleineren Primzahl ist, gehen wir nun zu einem genaueren und allgemeineren Vergleich der Primzahlen über, je nachdem, ob eine Rest oder Nichtrest einer anderen ist.

Oben haben wir streng bewiesen, dass -3 und $+5$ Reste oder Nichtreste aller Primzahlen sind, die jeweils Reste oder Nichtreste von $3, 5$ sind.

Die Untersuchung der folgenden Zahlen zeigt, dass -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59 usw. Reste oder Nichtreste aller Primzahlen sind, die, positiv genommen, jeweils Reste oder Nichtreste jener Primzahlen sind. Diese Untersuchung lässt sich mit Tabelle II sehr leicht durchführen.

Bei etwas Aufmerksamkeit wird jeder bemerken, dass unter diesen Primzahlen diejenigen der Form $4n+1$ ein positives Vorzeichen haben, diejenigen der Form $4n+3$ dagegen ein negatives.

131.

Wir werden bald beweisen, dass das, was wir hier anhand von Beispielen gefunden haben, allgemein gilt. Bevor wir diese Aufgabe angehen, müssen wir jedoch alles herleiten, was aus dem Satz folgt, wenn man ihn als wahr voraussetzt. Den Satz selbst sprechen wir so aus.

Ist p eine Primzahl der Form $4n+1$, so ist $+p$, und hat p die Form $4n+3$, so ist $-p$ ein Rest oder Nichtrest jeder Primzahl, die, positiv genommen, ein Rest oder Nichtrest von p ist.

Da fast alles, was sich über quadratische Reste sagen lässt, auf diesem Satz beruht, ist die Bezeichnung *Fundamentalsatz*, die wir von nun an verwenden werden, durchaus passend.

Um unsere Schlüsse möglichst kurz darzustellen, bezeichnen wir mit a, a', a'' usw. Primzahlen der Form $4n+1$, mit b, b', b'' usw. Primzahlen der Form $4n+3$; mit A, A', A'' usw. beliebige Zahlen der Form $4n+1$, mit B, B', B'' usw. dagegen beliebige Zahlen der Form $4n+3$. Schließlich soll der Buchstabe R zwischen zwei Größen bedeuten, dass die erste ein Rest der zweiten ist; der Buchstabe N soll die entgegengesetzte Bedeutung haben. *Zum Beispiel* bedeutet $+5R11$, $\pm 2N5$, dass $+5$ ein Rest von 11 und $+2$ oder -2 ein Nichtrest von 5 ist. Verbindet man nun den Fundamentalsatz mit den Sätzen aus Artikel 111, so erhält man leicht die folgenden Aussagen.

	Wenn		dann
1.	$\pm aRa'$	. . . . .	$\pm a'Ra$
2.	$\pm aNa'$	. . . . .	$\pm a'Na$
3.	$\left\{\begin{array}{l}+aRb\\-aNb\end{array}\right\}$	. . . . .	$\pm bRa$
4.	$\left\{\begin{array}{l}+aNb\\-aRb\end{array}\right\}$	. . . . .	$\pm bNa$
5.	$\pm bRa$	. . . . .	$\left\{\begin{array}{l}+aRb\\-aNb\end{array}\right.$
6.	$\pm bNa$	. . . . .	$\left\{\begin{array}{l}+aNb\\-aRb\end{array}\right.$
7.	$\left\{\begin{array}{l}+bRb'\\-bNb'\end{array}\right\}$	. . . . .	$\left\{\begin{array}{l}+b'Nb\\-b'Rb\end{array}\right.$
8.	$\left\{\begin{array}{l}+bNb'\\-bRb'\end{array}\right\}$	. . . . .	$\left\{\begin{array}{l}+b'Rb\\-b'Nb\end{array}\right.$

132.

Diese enthalten alle Fälle, die beim Vergleich zweier Primzahlen auftreten können. Die folgenden Aussagen beziehen sich auf beliebige Zahlen; ihre Beweise liegen jedoch weniger auf der Hand.

	Wenn		dann
9.	$\pm aRA$	. . . . .	$\pm ARa$
10.	$\pm bRA$	. . . . .	$\left\{\begin{array}{l}+ARb\\-ANb\end{array}\right.$
11.	$+aRB$	. . . . .	$\pm BRa$
12.	$-aRB$	. . . . .	$\pm BNa$
13.	$+bRB$	. . . . .	$\left\{\begin{array}{l}-BRb\\+BNb\end{array}\right.$
14.	$-bRB$	. . . . .	$\left\{\begin{array}{l}+BRb\\-BNb\end{array}\right.$

Da die Beweise all dieser Aussagen aus denselben Prinzipien folgen, müssen wir sie nicht alle ausführen. Der Beweis von Aussage 9, den wir angeben, kann als Beispiel dienen. Zunächst ist zu beachten, dass jede Zahl der Form $4n+1$ entweder keinen Faktor der Form $4n+3$ hat oder zwei oder vier usw.; *das heißt,* die Anzahl solcher Faktoren (unter denen auch gleiche vorkommen können) ist stets gerade. Jede Zahl der Form $4n+3$ enthält dagegen eine ungerade Anzahl von Faktoren der Form $4n+3$ (*das heißt* entweder einen oder drei oder fünf usw.). Die Anzahl der Faktoren der Form $4n+1$ bleibt unbestimmt.

Aussage 9 wird so bewiesen. Sei A das Produkt der Primfaktoren a', a'', a''' usw., b, b', b'' usw. Dann ist die Anzahl der Faktoren b, b', b'' usw. gerade (es können auch keine vorkommen, was auf dasselbe hinausläuft). Ist nun a ein Rest von A, so auch

von allen Faktoren a', a'', a''' usw., b, b', b'' usw. Nach den Aussagen 1, 3 des vorigen Artikels ist daher jeder dieser Faktoren ein Rest von a, also auch ihr Produkt A. Dasselbe muss für $-A$ gelten. — Ist dagegen $-a$ ein Rest von A und damit auch von allen Faktoren a', a'' usw., b, b' usw., so sind die einzelnen a', a'' usw. Reste von a, die einzelnen b, b' usw. dagegen Nichtreste. Da die Anzahl der letzteren gerade ist, ist das Produkt aller Faktoren, *das heißt* A, ein Rest von a und somit auch $-A$.

133.

Stellen wir die Untersuchung noch allgemeiner an. Betrachten wir zwei beliebige teilerfremde ungerade Zahlen mit beliebigen Vorzeichen, P und Q. Man denke sich P ohne Rücksicht auf sein Vorzeichen in seine Primfaktoren zerlegt und bezeichne mit p, wie viele davon Q als Nichtrest haben. Kommt eine Primzahl, von der Q ein Nichtrest ist, mehrmals unter den Faktoren von P vor, so muss sie auch mehrmals gezählt werden. Entsprechend sei q die Anzahl der Primfaktoren von Q, von denen P ein Nichtrest ist. Dann stehen die Zahlen p, q in einer bestimmten Beziehung zueinander, die von der Art der Zahlen P, Q abhängt. Ist nämlich eine der Zahlen p, q gerade oder ungerade, so zeigt die Form der Zahlen P, Q, ob die andere gerade oder ungerade ist. Die folgende Tabelle stellt diese Beziehung dar.

p, q sind beide gerade oder beide ungerade, wenn die Zahlen P, Q die Formen haben:

1.	$+A$,	$+A'$
2.	$+A$,	$-A'$
3.	$+A$,	$+B$
4.	$+A$,	$-B$
5.	$-A$,	$-A'$
6.	$+B$,	$-B'$

Dagegen ist von den Zahlen p, q eine gerade und die andere ungerade, wenn die Zahlen P, Q die Formen haben:

7.	$-A$,	$+B$
8.	$-A$,	$-B$
9.	$+B$,	$+B'$
10.	$-B$,	$-B'$*)

Beispiel. Die gegebenen Zahlen seien -55 und $+1197$, die zum vierten Fall gehören. Dabei ist 1197 ein Nichtrest eines Primfaktors von 55. Dieser Faktor ist die Zahl 5, während -55 ein Nichtrest dreier Primfaktoren von 1197 ist, nämlich der Zahlen $3, 3, 19$.

Bezeichnen P und Q Primzahlen, so gehen diese Aussagen in die aus Artikel 131 über. Hier können p und q nicht größer als 1 sein. Wird also p als gerade angenommen, so muss es $= 0$ sein, *das heißt,* Q ist ein Rest von P; ist dagegen p ungerade, so ist Q ein Nichtrest von P. Und umgekehrt. Schreibt man also a, b anstelle von A, B, so

*) Sei $l = 1$, wenn beide $P, Q \equiv 3 \pmod 4$, sonst $l = 0$
$m = 1$, wenn beide P, Q negativ sind, sonst $m = 0$
Dann hängt die Beziehung von $l + m$ ab.

folgt aus 8: Ist $-a$ ein Rest oder Nichtrest von b, so ist $-b$ ein Nichtrest oder Rest von a. Das stimmt mit 3 und 4 aus Artikel 131 überein.

Allgemein kann Q aber nur dann ein Rest von P sein, wenn $p = 0$. Ist also p ungerade, so ist Q sicher ein Nichtrest von P.

Hieraus lassen sich auch die Aussagen des vorigen Artikels ohne Schwierigkeit herleiten.

Bald wird sich außerdem zeigen, dass diese allgemeine Darstellung mehr als eine unfruchtbare Spekulation ist, da sich ein vollständiger Beweis des Fundamentalsatzes ohne sie kaum führen lässt.

134.

Wir gehen nun zur Herleitung dieser Aussagen über.

I. Man denke sich wie zuvor P ohne Berücksichtigung der Vorzeichen in seine Primfaktoren zerlegt. Auch Q werde auf beliebige Weise in Faktoren zerlegt, wobei aber das Vorzeichen von Q berücksichtigt wird. Man bilde Paare aus jedem der ersten Faktoren und jedem der zweiten. Bezeichnet s die Anzahl aller Paare, in denen der Faktor von Q ein Nichtrest des Faktors von P ist, so sind p und s beide gerade oder beide ungerade. Denn die Primfaktoren von P seien f, f', f'' usw., und unter den Faktoren, in die Q zerlegt ist, seien m Nichtreste von f, m' Nichtreste von f', m'' Nichtreste von f'' usw. Dann sieht man leicht, dass

$$s = m + m' + m'' + \text{usw.}$$

gilt, während p angibt, wie viele der Zahlen m, m', m'' usw. ungerade sind. Daraus folgt unmittelbar, dass s gerade ist, wenn p gerade ist, und ungerade, wenn p ungerade ist.

II. Dies gilt allgemein, auf welche Weise Q auch in Faktoren zerlegt wurde. Gehen wir zu besonderen Fällen über. Betrachten wir zunächst die Fälle, in denen die eine Zahl, P, positiv ist, die andere, Q, dagegen entweder die Form $+A$ oder die Form $-B$ hat. Man zerlege P, Q in ihre Primfaktoren, gebe jedem Faktor von P ein positives Vorzeichen und jedem Faktor von Q ein positives oder negatives, je nachdem, ob er die Form a oder b hat. Dann hat Q offensichtlich entweder die Form $+A$ oder $-B$, wie verlangt. Man bilde Paare aus jedem Faktor von P und jedem Faktor von Q, und bezeichne wie zuvor mit s die Anzahl der Paare, in denen der Faktor von Q ein Nichtrest des Faktors von P ist. Entsprechend sei t die Anzahl der Paare, in denen der Faktor von P ein Nichtrest des Faktors von Q ist. Aus dem Fundamentalsatz folgt, dass diese beiden Mengen von Paaren übereinstimmen, also $s = t$. Aus dem soeben Bewiesenen folgt schließlich $p \equiv s \,(\text{mod. } 2)$, $q \equiv t \,(\text{mod. } 2)$ und damit $p \equiv q \,(\text{mod. } 2)$.

Wir haben damit die Aussagen $1, 3, 4$ und 6 aus Artikel 133.

Die übrigen Aussagen lassen sich auf ähnliche Weise direkt gewinnen, erfordern aber eine neue Überlegung. Leichter lassen sie sich aus dem Vorhergehenden so herleiten.

III. Wieder seien P, Q beliebige teilerfremde ungerade Zahlen, und p, q die Anzahlen der Primfaktoren von P, Q, von denen Q bzw. P Nichtreste sind. Schließlich sei p' die Anzahl der Primfaktoren von P, von denen $-Q$ ein Nichtrest ist (ist Q selbst negativ, so bezeichnet $-Q$ offensichtlich eine positive Zahl). Man teile nun alle Primfaktoren von P in vier Klassen ein:

1) Faktoren der Form a, von denen Q ein Rest ist.

2) Faktoren der Form b, von denen Q ein Rest ist. Ihre Anzahl sei χ.

3) Faktoren der Form a, von denen Q ein Nichtrest ist. Ihre Anzahl sei ψ.

4) Faktoren der Form b, von denen Q ein Nichtrest ist. Ihre Anzahl $= \omega$.

Dann sieht man leicht, dass $p = \psi + \omega$, $p' = \chi + \psi$ gilt.

Hat nun P die Form $\pm A$, so ist $\chi + \omega$ und damit auch $\chi - \omega$ gerade. Also gilt $p' = p + \chi - \omega \equiv p \,(\text{mod. } 2)$. Hat dagegen P die Form $\pm B$, so zeigt ein ähnlicher Schluss, dass die Zahlen p, p' nach dem Modul 2 inkongruent sind.

IV. Wenden wir dies auf die einzelnen Fälle an. Zunächst hätten sowohl P als auch Q die Form $+A$. Dann gilt nach Aussage 1 $p \equiv q \,(\text{mod. } 2)$; es gilt aber auch $p' \equiv p \,(\text{mod. } 2)$, also $p' \equiv q \,(\text{mod. } 2)$. Das stimmt mit Aussage 2 überein. — Entsprechend habe P die Form $-A$. Hat Q die Form $+A$, so gilt $p \equiv q \,(\text{mod. } 2)$ nach der soeben bewiesenen Aussage 2. Da $p' \equiv p$, folgt daraus $p' \equiv q$. Damit ist auch Aussage 5 bewiesen.

Auf dieselbe Weise folgt Aussage 7 aus 3; Aussage 8 aus 4 oder 7; Aussage 9 aus 6 und aus derselben Aussage auch 10.

Strenger Beweis des Fundamentalsatzes.

135.

Im vorigen Artikel wurden die Aussagen aus Artikel 133 zwar nicht bewiesen. Es wurde aber gezeigt, dass ihre Richtigkeit von der des Fundamentalsatzes abhängt, die wir vorläufig vorausgesetzt haben. Aus der Herleitung selbst geht jedoch hervor, dass diese Aussagen für die Zahlen P, Q gelten, sobald der Fundamentalsatz beim Vergleich aller Primfaktoren dieser Zahlen miteinander gilt, selbst wenn er nicht allgemein richtig ist. Wir gehen nun zum Beweis des Fundamentalsatzes selbst über und stellen ihm die folgende Erklärung voran.

Wir sagen, der Fundamentalsatz sei bis zu einer Zahl M richtig, wenn er für zwei beliebige Primzahlen gilt, von denen keine M übersteigt.

Entsprechend ist es zu verstehen, wenn wir sagen, dass die Sätze aus den Artikeln $131, 132, 133$ bis zu einer bestimmten Grenze richtig sind. Ist der Fundamentalsatz bis zu einer Grenze als richtig bekannt, so gelten offensichtlich auch diese Aussagen bis zu derselben Grenze.

136.

Für kleine Zahlen lässt sich der Fundamentalsatz leicht durch Nachprüfen bestätigen. So erhält man eine Grenze, bis zu der er sicher gilt. Wir setzen voraus, dass diese Prüfung durchgeführt wurde; wie weit wir sie fortgesetzt haben, spielt aber keine Rolle. Es würde sogar genügen, wenn wir ihn nur bis zur Zahl 5 bestätigt hätten. Dazu reicht die einzige Beobachtung, dass $+5N3$, $\pm 3N5$ gilt.

Ist nun der Fundamentalsatz nicht allgemein richtig, so gibt es eine Grenze T, bis zu der er gilt, während er bis zur nächstgrößeren Zahl $T+1$ nicht mehr gilt. Das heißt: Es gibt zwei Primzahlen, deren größere $T+1$ ist und deren Vergleich dem Fundamentalsatz widerspricht; je zwei beliebige andere Primzahlen stimmen dagegen mit ihm überein, sofern beide kleiner als $T+1$ sind. Also gelten auch die Aussagen aus den Artikeln $131, 132, 133$ bis zu T. Wir zeigen nun, dass diese Annahme unmöglich ist. Dabei müssen wir die folgenden Fälle unterscheiden, je nachdem, welche Formen $T+1$ und die kleinere Primzahl haben, die kleiner als $T+1$ ist und deren Vergleich mit $T+1$ nach Voraussetzung dem Satz widerspricht. Wir bezeichnen diese Primzahl mit p.

Haben sowohl $T+1$ als auch p die Form $4n+1$, so könnte der Fundamentalsatz auf zwei Arten falsch sein, nämlich wenn gleichzeitig *entweder*

$$\begin{array}{rlll} & \pm pR(T+1) & \text{und} & \pm\,(T+1)Np \\ \textit{oder zugleich} & \pm pN(T+1) & \text{und} & \pm\,(T+1)Rp \end{array}$$

Haben sowohl $T+1$ als auch p die Form $4n+3$, so wäre der Fundamentalsatz falsch, wenn gleichzeitig *entweder*

$$\begin{array}{rlll} & +pR(T+1) & \text{und} & -\,(T+1)Np \\ \text{(gleichbedeutend} & -pN(T+1) & \text{und} & +\,(T+1)Rp) \\ \textit{oder} & +pN(T+1) & \text{und} & -\,(T+1)Rp \\ \text{(oder} & -pR(T+1) & \text{und} & +\,(T+1)Np) \end{array}$$

Hat $T+1$ die Form $4n+1$, p dagegen die Form $4n+3$, so wäre der Fundamentalsatz falsch, wenn *entweder*

$$\begin{array}{ll} & \pm pR(T+1) \text{ und } +(T+1)Np \text{ (oder } -(T+1)Rp) \\ \textit{oder} & \pm pN(T+1) \text{ und } -(T+1)Np \text{ (oder } +(T+1)Rp) \end{array}$$

Hat $T+1$ die Form $4n+3$, p dagegen die Form $4n+1$, so wäre der Fundamentalsatz falsch, wenn *entweder*

$$\begin{array}{ll} & +pR(T+1) \text{ (oder } -pN(T+1)) \text{ und } \pm(T+1)Np \\ \textit{oder} & +pN(T+1) \text{ (oder } -pR(T+1)) \text{ und } \pm(T+1)Rp \end{array}$$

Können wir beweisen, dass keiner dieser acht Fälle eintritt, so steht zugleich fest, dass die Richtigkeit des Fundamentalsatzes durch keine Grenze beschränkt ist. Diese Aufgabe gehen wir nun an. Da aber einige dieser Fälle von anderen abhängen, können wir die Reihenfolge, in der wir sie hier aufgezählt haben, nicht beibehalten.

137.

Erster Fall. Hat $T+1$ die Form $4n+1$ $(=a)$, und p dieselbe Form, und gilt außerdem $\pm pRa$, so kann nicht $\pm aNp$ gelten. Dies war oben der erste Fall.

Sei $+p \equiv e^2 (\text{mod. } a)$, wobei e gerade und $< a$ ist (was sich immer erreichen lässt). Nun sind zwei Fälle zu unterscheiden.

I. Ist e nicht durch p teilbar, so setze man $e^2 = p + af$. Dann ist f positiv, von der Form $4n+3$ (oder der Form B), $< a$ und nicht durch p teilbar. Ferner gilt $e^2 \equiv p (\text{mod. } f)$, *das heißt* pRf, also nach Aussage 11 aus Artikel 132 auch $\pm fRp$ (denn wegen $p, f < a$ gelten diese Aussagen für sie). Es gilt aber auch $afRp$, also ebenfalls $\pm aRp$.

II. Ist e durch p teilbar, so setze man $e = gp$ und $e^2 = p + aph$ oder $pg^2 = 1 + ah$. Dann hat h die Form $4n+3$ (B) und ist zu p und g^2 teilerfremd. Ferner gilt pg^2Rh, also auch pRh; nach Aussage 11 aus Artikel 132 folgt daraus $\pm hRp$. Es gilt aber auch $-ahRp$, da $-ah \equiv 1 (\text{mod. } p)$, also ebenfalls $\mp aRp$.

138.

Zweiter Fall. Hat $T+1$ die Form $4n+1$ $(=a)$, p die Form $4n+3$, und gilt $\pm pR(T+1)$, so kann nicht $+(T+1)Np$ oder $-(T+1)Rp$ gelten. Dies war oben der fünfte Fall.

Wie oben sei $e^2 = p + fa$, wobei e gerade und $< a$ ist.

I. Ist e nicht durch p teilbar, so ist auch f nicht durch p teilbar. Außerdem ist f positiv, von der Form $4n+1$ (oder A) und $< a$. Es gilt $+pRf$, also nach Aussage 10 aus Artikel 132 auch $+fRp$. Es gilt aber auch $+faRp$, also $+aRp$ oder $-aNp$.

II. Ist e durch p teilbar, so sei $e = pg$ und $f = ph$. Somit gilt $g^2p = 1 + ha$. Dann ist h positiv, von der Form $4n+3$ (B) und zu p und g^2 teilerfremd. Ferner gilt $+g^2pRh$, also $+pRh$; daraus folgt nach Aussage 13 aus Artikel 132 $-hRp$. Es gilt aber $-haRp$, woraus $+aRp$ und $-aNp$ folgt.

139.

Dritter Fall. Hat $T+1$ die Form $4n+1$ $(=a)$, p dieselbe Form, und gilt $\pm pNa$, so kann nicht $\pm aRp$ gelten. (Oben der zweite Fall.)

Man nehme eine Primzahl unterhalb von a, von der $+a$ ein Nichtrest ist. Dass es solche Primzahlen gibt, haben wir oben bewiesen (Artikel 125, 129). Hier sind aber zwei Fälle gesondert zu betrachten, je nachdem, ob diese Primzahl die Form $4n+1$ oder $4n+3$ hat. Denn es wurde nicht bewiesen, dass es solche Primzahlen *beider* Formen gibt.

I. Diese Primzahl habe die Form $4n+1$ und sei $= a'$. Dann gilt $\pm a'Na$ (Artikel 131), also $\pm a'pRa$. Sei daher $e^2 \equiv a'p \pmod{a}$, wobei e gerade und $< a$ ist. Nun sind wieder vier Fälle zu unterscheiden.

1) Ist e weder durch p noch durch a' teilbar, so setze man $e^2 = a'p \pm af$ und wähle die Vorzeichen so, dass f positiv ist. Dann gilt $f < a$, und die Zahl ist zu a' und p teilerfremd; beim oberen Zeichen hat sie die Form $4n+3$, beim unteren die Form $4n+1$. Der Kürze wegen bezeichnen wir mit $[x,y]$ die Anzahl der Primfaktoren der Zahl y, von denen x ein Nichtrest ist. Dann gilt $a'pRf$, also $[a'p,f]=0$. Somit ist $[f,a'p]$ gerade (Aussagen 1, 3 aus Artikel 133), *das heißt* entweder $=0$ oder $=2$. Daher ist f entweder ein Rest beider Zahlen a',p oder keiner von beiden. Ersteres ist unmöglich, denn $\pm af$ ist ein Rest von a', und nach Voraussetzung gilt $\pm aNa'$; daraus folgt $\pm fNa'$. Also muss f ein Nichtrest beider Zahlen a',p sein. Wegen $\pm afRp$ gilt dann $\pm aNp$. *Q. E. D.*

2) Ist e durch p, aber nicht durch a' teilbar, so sei $e=gp$ und $g^2p = a' \pm ah$, wobei das Zeichen so gewählt wird, dass h positiv ist. Dann gilt $h<a$, und die Zahl ist zu a', g und p teilerfremd; beim oberen Zeichen hat sie die Form $4n+3$, beim unteren die Form $4n+1$. Aus der Gleichung $g^2p = a' \pm ah$ erhält man durch Multiplikation mit p und a' ohne Schwierigkeit $pa'Rh\ldots.(\alpha)$; $\pm ahpRa'\ldots.(\beta)$; $aa'hRp\ldots.(\gamma)$. Aus (α) folgt $[pa',h]=0$, also ist (nach den Aussagen 1, 3 aus Artikel 133) $[h,pa']$ gerade, *das heißt,* h ist entweder ein Nichtrest beider Zahlen p,a' oder keiner von beiden. *Im ersten Fall* folgt aus (β) $\pm apNa'$. Da nach Voraussetzung $\pm aNa'$ gilt, folgt $\pm pRa'$. Nach dem Fundamentalsatz, der für die Zahlen p,a' unterhalb von $T+1$ gilt, ergibt sich daraus $\pm a'Rp$. Hieraus und aus hNp folgt nach (γ) $\pm aNp$. *Q. E. D. Im zweiten Fall* folgt aus (β) $\pm apRa'$, daraus $\pm pNa'$, $\pm a'Np$ und schließlich zusammen mit hRp nach (γ) $\pm aNp$. *Q. E. D.*

3) Ist e durch a', aber nicht durch p teilbar, so verläuft der Beweis fast genauso wie im vorigen Fall. Er wird niemanden aufhalten, der jenen gründlich verstanden hat.

4) Ist e sowohl durch a' als auch durch p und damit auch durch ihr Produkt $a'p$ teilbar (wir nehmen die Zahlen a',p nämlich als *verschieden* an, da sonst das zu Beweisende, nämlich aNp, schon in der Voraussetzung aNa' enthalten wäre), so sei $e=ga'p$ und $g^2a'p = 1 \pm ah$. Dann gilt $h<a$, und die Zahl ist zu a' und p teilerfremd; beim oberen Zeichen hat sie die Form $4n+3$, beim unteren die Form $4n+1$. Aus dieser Gleichung lassen sich offensichtlich die folgenden Beziehungen herleiten: $a'pRh\ldots.(\alpha)$; $\pm ahRa'\ldots.(\beta)$; $\pm ahRp\ldots.(\gamma)$. Aus (α), das mit (α) in (2) übereinstimmt, folgt wie dort, dass entweder gleichzeitig hRp, hRa' oder hNp, hNa'

gilt. Im ersten Fall würde aber nach (β) aRa' gelten, entgegen der Voraussetzung. Also gilt hNp, nach (γ) somit auch aNp.

II. Hat diese Primzahl die Form $4n+3$, so ist der Beweis dem vorigen so ähnlich, dass wir es für überflüssig hielten, ihn anzugeben. Für diejenigen, die ihn selbst ausarbeiten möchten (was wir sehr empfehlen), bemerken wir nur: Ist man zu einer Gleichung wie $e^2 = bp \pm af$ gelangt (wobei b jene Primzahl bezeichnet), so wird der Beweis übersichtlicher, wenn man beide Vorzeichen gesondert betrachtet.

140.

Vierter Fall. Hat $T+1$ die Form $4n+1$ $(=a)$, p die Form $4n+3$, und gilt $\pm pNa$, so kann nicht $+aRp$ oder $-aNp$ gelten. (Oben der sechste Fall.)

Auch den Beweis dieses Falles lassen wir der Kürze wegen weg, da er genauso verläuft wie der Beweis des dritten Falles.

141.

Fünfter Fall. Hat $T+1$ die Form $4n+3$ $(=b)$, p dieselbe Form, und gilt $+pRb$ oder $-pNb$, so kann nicht $+bRp$ oder $-bNp$ gelten. (Oben der dritte Fall.)

Sei $p \equiv e^2 \pmod{b}$, wobei e gerade und $< b$ ist.

I. Ist e nicht durch p teilbar, so setze man $e^2 = p + bf$. Dann ist f positiv, von der Form $4n+3$, $< b$ und zu p teilerfremd. Ferner gilt pRf, also nach Aussage 13 aus Artikel 132 $-fRp$. Hieraus und aus $+bfRp$ folgt $-bRp$, also $+bNp$. *Q. E. D.*

II. Ist e durch p teilbar, so sei $e = pg$ und $ggp = 1 + bh$. Dann hat h die Form $4n+1$ und ist zu p teilerfremd; es gilt $p \equiv g^2p^2 \pmod{h}$, also pRh. Daraus folgt $+hRp$ (Aussage 10 aus Artikel 132), und hieraus zusammen mit $-bhRp$ ergibt sich $-bRp$ oder $+bNp$. *Q. E. D.*

142.

Sechster Fall. Hat $T+1$ die Form $4n+3$ $(=b)$, p die Form $4n+1$, und gilt pRb, so kann nicht $\pm bNp$ gelten. (Oben der siebente Fall.)

Den Beweis, der genauso wie der vorige verläuft, lassen wir weg.

143.

Siebenter Fall. Hat $T+1$ die Form $4n+3$ $(=b)$, p dieselbe Form, und gilt $+pNb$ oder $-pRb$, so kann nicht $+bNp$ oder $-bRp$ gelten. (Oben der vierte Fall.)

Sei $-p \equiv e^2 \pmod{b}$, wobei e gerade und $< b$ ist.

I. Ist e nicht durch p teilbar, so sei $-p = e^2 - bf$. Dann ist f positiv, von der Form $4n+1$, zu p teilerfremd und kleiner als b (denn e ist sicher nicht größer als $b-1$, und $p < b-1$, also gilt $bf = e^2 + p < b^2 - b$, *das heißt* $f < b-1$). Ferner gilt $-pRf$, nach Aussage 10 aus Artikel 132 somit $+fRp$; hieraus und aus $+bfRp$ folgt $+bRp$ oder $-bNp$.

II. Ist e durch p teilbar, so sei $e = pg$ und $g^2p = -1 + bh$. Dann ist h positiv, von der Form $4n+3$, zu p teilerfremd und $< b$. Ferner gilt $-pRh$, nach Aussage 14 aus Artikel 132 also $+hRp$. Hieraus und aus $bhRp$ folgt $+bRp$ oder $-bNp$. *Q. E. D.*

144.

Achter Fall. Hat $T+1$ *die Form* $4n+3$ $(=b)$*,* p *die Form* $4n+1$*, und gilt* $+pNb$ *oder* $-pRb$*, so kann nicht* $\pm bRp$ *gelten.* (Oben der letzte Fall.)

Der Beweis verläuft wie im vorigen Fall.

Ein ähnliches Verfahren zum Beweis des Satzes aus Artikel 114.

145.

In den vorigen Beweisen haben wir für e stets einen geraden Wert genommen (Artikel 137 .. 144). Man hätte auch einen ungeraden Wert verwenden können, hätte dann aber weitere Unterscheidungen einführen müssen. Wer an diesen Untersuchungen Freude hat, wird seine Kräfte mit Nutzen daran erproben, diese Fälle auszuarbeiten. Außerdem hätten dann die Sätze über die Reste $+2$ und -2 vorausgesetzt werden müssen. Da unser Beweis aber ohne diese Sätze auskommt, gewinnen wir ein neues Verfahren, um sie zu beweisen. Das ist durchaus beachtenswert, denn die oben verwendeten Methoden zum Beweis, dass ± 2 ein Rest jeder Primzahl der Form $8n+1$ ist, mögen weniger direkt erscheinen. Wir setzen voraus, dass die übrigen Fälle (zu den Primzahlen der Formen $8n+3$, $8n+5$, $8n+7$) mit den oben angegebenen Methoden bewiesen sind und jener Satz nur anhand von Beispielen gefunden wurde. Diese Beobachtung werden wir durch die folgenden Überlegungen zur Gewissheit erheben.

Wäre ± 2 nicht ein Rest aller Primzahlen der Form $8n+1$, so sei die kleinste Primzahl dieser Form, von der ± 2 ein Nichtrest ist, $= a$. Für alle Primzahlen unterhalb von a gilt dann der Satz. Man nehme eine Primzahl $< \frac{1}{2}a$, von der a ein Nichtrest ist (dass es eine solche gibt, folgt leicht aus Artikel 129). Diese sei $= p$. Nach dem Fundamentalsatz gilt dann pNa, also $\pm 2pRa$. — Sei daher $e^2 \equiv 2p \pmod{a}$, wobei e ungerade und $< a$ ist. Nun sind zwei Fälle zu unterscheiden.

I. Ist e nicht durch p teilbar, so sei $e^2 = 2p + aq$. Dann ist q positiv, von der Form $8n+7$ oder $8n+3$ (je nachdem, ob p die Form $4n+1$ oder $4n+3$ hat), $< a$ und nicht durch p teilbar. Man teile alle Primfaktoren von q in vier Klassen ein: Es seien e von der Form $8n+1$, f von der Form $8n+3$, g von der Form $8n+5$ und h von der Form $8n+7$. Das Produkt der Faktoren der ersten Klasse sei E, die Produkte der Faktoren der zweiten, dritten und vierten Klasse entsprechend $F, G.H$[*)].

Betrachten wir nun *erstens* den Fall, dass p die Form $4n+1$ oder q die Form $8n+7$ hat. Dann gilt offensichtlich $2RE$, $2RH$, also pRE, pRH und schließlich ERp, HRp. Ferner ist 2 ein Nichtrest jedes Faktors der Form $8n+3$ oder $8n+5$; dasselbe gilt für p. Daher ist jeder solche Faktor ein Nichtrest von p. Es folgt leicht, dass FG ein Rest von p ist, wenn $f+g$ gerade ist, und ein Nichtrest, wenn $f+g$ ungerade ist. Aber $f+g$ kann nicht ungerade sein: Durch Aufzählen aller Fälle sieht man leicht, dass $EFGH$ oder q dann die Form $8n+3$ oder $8n+5$ hätte, wenn $f+g$ ungerade wäre, welche Werte die einzelnen e, f, g, h auch hätten. Das widerspricht der Voraussetzung. Also gilt $FGRp$, $EFGHRp$ oder qRp und schließlich wegen $aqRp$ auch aRp, entgegen der Voraussetzung. Hat *zweitens* p die Form $4n+3$, so kann man ähnlich zeigen, dass pRE, also ERp, und $-pRF$, also FRp, gilt; schließlich ist $g+h$ gerade, also gilt $GHRp$, woraus zuletzt qRp, aRp folgt, entgegen der Voraussetzung.

II. Ist e durch p teilbar, so lässt sich der Beweis auf ähnliche Weise führen und von geübten Lesern (für die allein dieser Artikel geschrieben ist) ohne Schwierigkeit ausarbeiten. Der Kürze wegen lassen wir ihn weg.

[*)] Enthält eine Klasse keine Faktoren, so muss man für deren Produkt 1 schreiben.

Lösung des allgemeinen Problems.

146.

Mit dem Fundamentalsatz und den Aussagen über die Reste -1 und ± 2 lässt sich immer bestimmen, ob eine beliebige gegebene Zahl ein Rest oder Nichtrest einer gegebenen Primzahl ist. Es wird aber nützlich sein, auch die anderen oben angegebenen Ergebnisse hier noch einmal zusammenzustellen, damit alles zur Lösung des folgenden Problems Nötige beisammensteht.

Aufgabe: *Sind zwei beliebige Zahlen P, Q gegeben, so bestimme man, ob die zweite, Q, ein Rest oder Nichtrest der ersten, P, ist.*

Lösung. I. Sei $P = a^\alpha b^\beta c^\gamma$ usw., wobei a, b, c usw. verschiedene positive Primzahlen bezeichnen (denn P ist offensichtlich im Betrag zu nehmen). Der Kürze wegen nennen wir in diesem Artikel einfach die *Beziehung* zweier Zahlen x, y diejenige, nach der die erste, x, ein Rest oder Nichtrest der zweiten, y, ist. Die Beziehung von Q, P hängt also von den Beziehungen von Q, a^α; Q, b^β usw. ab (Artikel 105).

II. Um die Beziehung von Q, a^α zu bestimmen (für die übrigen Q, b^β usw. gilt dasselbe), sind zwei Fälle zu unterscheiden.

1. Ist Q durch a teilbar, so setze man $Q = Q'a^e$, wobei Q' nicht durch a teilbar ist. Ist dann $e = \alpha$ oder $e > \alpha$, so gilt QRa^α; ist dagegen $e < \alpha$ und der Exponent ungerade, so gilt QNa^α; ist schließlich $e < \alpha$ und der Exponent gerade, so hat Q zu a^α dieselbe Beziehung wie Q' zu $a^{\alpha-e}$. Dieser Fall ist damit zurückgeführt auf

2. den Fall, dass Q nicht durch a teilbar ist. Hier unterscheiden wir wiederum zwei Fälle.

(A) Wenn $a = 2$. Dann gilt stets QRa^α, sobald $\alpha = 1$ ist. Ist dagegen $\alpha = 2$, so muss Q die Form $4n + 1$ haben; ist schließlich $\alpha = 3$ oder > 3, so muss Q die Form $8n + 1$ haben. Ist diese Bedingung erfüllt, so gilt QRa^α.

(B) Wenn a eine andere Primzahl ist. Dann hat Q zu a^α dieselbe Beziehung wie zu a (siehe Artikel 101).

III. Die Beziehung einer beliebigen Zahl Q zu einer ungeraden Primzahl a wird so ermittelt. Ist $Q > a$, so ersetze man Q durch seinen kleinsten positiven Rest nach dem Modul a[*)]. Dieser hat zu a dieselbe Beziehung wie Q.

Ferner zerlege man Q oder die dafür genommene Zahl in ihre Primfaktoren p, p', p'' usw.; der Faktor -1 ist hinzuzufügen, wenn Q negativ ist. Bekanntlich hängt dann die Beziehung von Q zu a von den Beziehungen der einzelnen p, p', p'' usw. zu a ab. Sind nämlich unter jenen Faktoren $2m$ Nichtreste von a, so gilt QRa; sind es $2m + 1$, so gilt QNa. Kommen unter den Faktoren p, p', p'' usw. zwei oder vier oder sechs oder allgemein $2k$ gleiche vor, so kann man sie offensichtlich ohne Bedenken weglassen.

IV. Finden sich unter den Faktoren $p.p', p''$ die Zahlen -1 und 2, so lässt sich ihre Beziehung zu a aus den Artikeln 108, 112, 113, 114 bestimmen. Die Beziehung der übrigen zu a hängt von der Beziehung von a zu ihnen ab (Fundamentalsatz und Aussagen aus Artikel 131). Sei p einer dieser Faktoren. Behandelt man die Zahlen a, p genauso wie zuvor Q und a, die entsprechend größer sind, so findet man, dass sich die Beziehung von a zu p entweder nach den Artikeln 108—114 bestimmen

[*)] *Rest* im Sinne von Artikel 4. — Meist ist es besser, den im *Betrag* kleinsten Rest zu nehmen.

lässt (wenn nämlich der kleinste Rest von a (mod. p) keine ungeraden Primfaktoren hat) oder weiter von der Beziehung von p zu gewissen Primzahlen unterhalb von p abhängt. Dasselbe gilt für die übrigen Faktoren p', p'' usw. Nun sieht man leicht, dass die Fortsetzung dieses Verfahrens schließlich zu Zahlen führt, deren Beziehungen nach den Aussagen aus den Artikeln 108—114 bestimmt werden können. Ein Beispiel macht dies deutlicher.

Beispiel. Gesucht ist die Beziehung von $+453$ zu 1236. Es gilt $1236 = 4.3.103$; $+453 R 4$ nach II. 2 (A); $+453 R 3$ nach II. 1. Es bleibt also die Beziehung von $+453$ zu 103 zu untersuchen. Sie ist dieselbe wie die von $+41$ ($\equiv 453$, mod. 103) zu 103, dieselbe wie die von $+103$ zu 41 (nach dem Fundamentalsatz) oder die von -20 zu 41. Es gilt aber $-20 R 41$, denn $-20 = -1.2.2.5$; $-1 R 41$ (Artikel 108) und $+5 R 41$, weil $41 \equiv 1$ und die Zahl somit ein Rest von 5 ist (nach dem Fundamentalsatz). Daraus folgt $+453 R 103$ und schließlich $+453 R 1236$. Tatsächlich gilt $453 \equiv 297^2$ (mod. 1236).

Lineare Formen, die alle Primzahlen enthalten, von denen eine beliebige gegebene Zahl ein Rest oder Nichtrest ist.

147.

Ist eine beliebige Zahl A gegeben, so lassen sich bestimmte *Formeln* angeben, die alle zu A teilerfremden Zahlen enthalten, von denen A ein Rest ist, oder alle Zahlen, die *Teiler* von Zahlen der Form $xx - A$ sein können (wobei xx ein unbestimmtes Quadrat bezeichnet)[*]. Der Kürze wegen betrachten wir aber nur die Teiler, die ungerade und zu A teilerfremd sind, da sich die übrigen Fälle leicht darauf zurückführen lassen.

Zunächst sei A entweder eine positive Primzahl der Form $4n+1$ oder eine negative der Form $4n-1$. Nach dem Fundamentalsatz sind dann alle Primzahlen, die, positiv genommen, Reste von A sind, Teiler von $xx - A$; alle Primzahlen dagegen (außer der Zahl 2, die immer ein Teiler ist), die Nichtreste von A sind, sind Nichtteiler von $xx - A$. Alle Reste von A unterhalb von A (ohne die Null) seien r, r', r'' usw., alle Nichtreste dagegen n, n', n'' usw. Dann ist jede Primzahl in einer der Formen $Ak + r$, $Ak + r'$, $Ak + r''$ usw. ein Teiler von $xx - A$, jede Primzahl in einer der Formen $Ak + n$, $Ak + n'$ usw. dagegen ein Nichtteiler, wobei k eine unbestimmte ganze Zahl bezeichnet. Die ersten Formen nennen wir *Teilerformen von* $xx - A$, die anderen *Nichtteilerformen*. Von beiden Arten gibt es jeweils $\frac{1}{2}(A-1)$. Ist ferner B eine zusammengesetzte ungerade Zahl und gilt ARB, so liegen alle Primfaktoren von B in einer der ersten Formen und damit auch B. Also ist *jede* ungerade Zahl in einer Nichtteilerform ein Nichtteiler der Form $xx - A$. Dieser Satz lässt sich aber nicht umkehren: Ist B ein zusammengesetzter ungerader Nichtteiler der Form $xx - A$, so sind einige Primfaktoren von B Nichtteiler. Ist ihre Anzahl *gerade*, so findet sich B trotzdem in einer Teilerform. Siehe Artikel 99.

Beispiel. So erhält man für $A = -11$ die folgenden Teilerformen von $xx + 11$: $11k + 1, 3, 4, 5, 9$; die Nichtteilerformen sind dagegen $11k + 2, 6, 7, 8, 10$. Also ist -11 ein Nichtrest aller ungeraden Zahlen in einer der letzteren Formen, ein Rest dagegen aller Primzahlen, die zu einer der ersteren gehören.

[*] Solche Zahlen nennen wir einfach *Teiler von* $xx - A$; daraus ist klar, was *Nichtteiler* sind.

Ähnliche Formen gibt es für die Teiler und Nichtteiler von $xx - A$, welche Zahl A auch bezeichnet. Offensichtlich brauchen wir aber nur die Werte von A zu betrachten, die durch kein Quadrat teilbar sind. Ist nämlich $A = a^2A'$, so sind alle Teiler*) von $xx - A$ auch Teiler von $xx - A'$; dasselbe gilt für die Nichtteiler. — Wir unterscheiden drei Fälle: 1) wenn A die Form $+(4n+1)$ oder $-(4n-1)$ hat; 2) wenn A die Form $-(4n+1)$ oder $+(4n-1)$ hat; 3) wenn A gerade ist, also die Form $\pm(4n+2)$ hat.

148.

Erster Fall: wenn A die Form $+(4n+1)$ oder $-(4n-1)$ hat. Man zerlege A in seine Primfaktoren und gebe denjenigen der Form $4n+1$ ein positives, denen der Form $4n-1$ ein negatives Vorzeichen (sodass ihr Produkt $= A$ wird). Diese Faktoren seien a, b, c, d usw. Man teile alle Zahlen unterhalb von A, die zu A teilerfremd sind, in zwei Klassen ein. In die erste kommen alle Zahlen, die von keiner der Zahlen a, b, c, d usw. ein Nichtrest sind oder von zweien oder vieren oder allgemein von einer geraden Anzahl; in die zweite diejenigen, die von einer der Zahlen a, b, c usw. ein Nichtrest sind oder von dreien usw. oder allgemein von einer ungeraden Anzahl. Die ersten bezeichne man mit r, r', r'' usw., die zweiten mit n, n', n'' usw. Dann sind $Ak + r$, $Ak + r'$, $Ak + r''$ usw. Teilerformen von $xx - A$, dagegen $Ak + n$, $Ak + n'$ usw. Nichtteilerformen von $xx - A$ (*das heißt: Jede Primzahl außer* 2 *ist ein Teiler oder Nichtteiler von* $xx - A$, *je nachdem, ob sie in einer der ersten oder zweiten Formen liegt*). Ist nämlich p eine positive Primzahl und ein Rest oder Nichtrest einer der Zahlen a, b, c usw., so ist diese Zahl selbst ein Rest oder Nichtrest von p (nach dem Fundamentalsatz). Gibt es also unter a, b, c usw. m Zahlen, von denen p ein Nichtrest ist, so sind ebenso viele Nichtreste von p. Liegt demnach p in einer der ersten Formen, so ist m gerade und es gilt ARp; liegt sie in einer der zweiten, so ist m ungerade und es gilt ANp.

Beispiel. Sei $A = +105 = -3 \times +5 \times -7$. Dann sind r, r', r'' usw. die folgenden Zahlen: $1, 4, 16, 46, 64, 79$ (die von keiner der Zahlen $3, 5, 7$ Nichtreste sind); $2, 8, 23, 32, 53, 92$ (Nichtreste von $3, 5$); $26, 41, 59, 89, 101, 104$ (Nichtreste von $3, 7$); $13, 52, 73, 82, 97, 103$ (Nichtreste von $5, 7$). — Die Zahlen n, n', n'' usw. sind dagegen $11, 29, 44, 71, 74, 86$; $22, 37, 43, 58, 67, 88$; $19, 31, 34, 61, 76, 94$; $17, 38.47, 62, 68, 83$. Die ersten sechs sind Nichtreste von 3, die nächsten sechs Nichtreste von 5, dann folgen die Nichtreste von 7 und schließlich die Nichtreste aller drei zugleich.

Aus der Kombinationslehre und den Artikeln 32, 96 folgt leicht, dass die Anzahl der Zahlen r, r', r'' usw.

$$= t\left(1 + \frac{l\,.\,l-1}{1\,.\,2} + \frac{l\,.\,l-1\,.\,l-2\,.\,l-3}{1\,.\,2\,.\,3\,.\,4} + \ldots.\right)$$

und die Anzahl der Zahlen n, n', n'' usw.

$$= t\left(l + \frac{l\,.\,l-1\,.\,l-2}{1\,.\,2\,.\,3} + \frac{l\,.\,l-1\,.\ldots.\,l-4}{1\,.\,2\ldots.\,5} + \ldots\right)$$

ist, wobei l die Anzahl der Zahlen a, b, c usw. bezeichnet;

$$t = 2^{-l}(a-1)(b-1)(c-1) \text{ usw.}$$

*) Gemeint sind die zu A teilerfremden.

und jede der beiden Reihen ist fortzusetzen, bis sie abbricht. (Es gibt nämlich t Zahlen, die Reste aller a, b, c usw. sind, $\frac{t\,.\,l\,.\,l-1}{1\,.\,2}$, die Nichtreste von zweien sind, usw.; der Kürze wegen können wir diesen Beweis aber nicht ausführlicher entwickeln.) Die Summe jeder Reihe*) ist $= 2^{l-1}$. Die erste entsteht aus

$$1 + (l-1) + \frac{l-1\,.\,l-2}{1\,.\,2} + \ldots$$

durch Zusammennehmen des zweiten und dritten, des vierten und fünften Gliedes usw.; die zweite aus derselben Reihe durch Zusammennehmen des ersten und zweiten, des dritten und vierten Gliedes usw. Also gibt es ebenso viele Teilerformen von $xx - A$ wie Nichtteilerformen, nämlich $\frac{1}{2}(a-1)(b-1)(c-1)$ usw.

149.

Den *zweiten und dritten Fall* können wir hier gemeinsam betrachten. Man kann hier stets $A = (-1)Q$ oder $= (+2)Q$ oder $= (-2)Q$ setzen, wobei Q eine Zahl der Form $+(4n+1)$ oder $-(4n-1)$ bezeichnet, wie wir sie im vorigen Artikel betrachtet haben. Allgemein sei $A = \alpha Q$, wobei α entweder $= -1$ oder $= \pm 2$ ist. Dann ist A ein Rest aller Zahlen, von denen entweder beide α und Q Reste sind oder keine von beiden, dagegen ein Nichtrest aller Zahlen, von denen genau eine der Zahlen α, Q ein Nichtrest ist. Hieraus ergeben sich die Teiler- und Nichtteilerformen von $xx - A$ leicht. Ist $\alpha = -1$, so teile man alle Zahlen unterhalb von $4A$, die dazu teilerfremd sind, in zwei Klassen. In die erste kommen diejenigen, die in einer Teilerform von $xx - Q$ und zugleich in der Form $4n+1$ liegen, und diejenigen, die in einer Nichtteilerform von $xx - Q$ und zugleich in der Form $4n+3$ liegen; in die zweite die übrigen. Die ersten seien r, r', r'' usw., die zweiten n, n', n'' usw. Dann ist A ein Rest aller Primzahlen in einer der Formen $4Ak + r$, $4Ak + r'$, $4Ak + r''$ usw., ein Nichtrest dagegen aller Primzahlen in einer der Formen $4Ak + n$, $4Ak + n'$ usw. — Ist $\alpha = \pm 2$, so teile man alle Zahlen unterhalb von $8Q$, die dazu teilerfremd sind, in zwei Klassen. In die erste kommen diejenigen, die in einer Teilerform von $xx - Q$ und zugleich in einer der Formen $8n+1$, $8n+7$ beim oberen Zeichen oder $8n+1$, $8n+3$ beim unteren liegen; außerdem diejenigen, die in einer Nichtteilerform von $xx - Q$ und zugleich in einer der Formen $8n+3$, $8n+5$ beim oberen Zeichen oder $8n+5$, $8n+7$ beim unteren liegen. In die zweite kommen die übrigen. Bezeichnet man die Zahlen der ersten Klasse mit r, r', r'' usw. und die der zweiten mit n, n', n'' usw., so ist $\pm 2Q$ ein Rest aller Primzahlen in einer der Formen $8Qk + r$, $8Qk + r'$, $8Qk + r''$ usw., ein Nichtrest dagegen aller Primzahlen in einer der Formen $8Qk + n$, $8Qk + n'$, $8Qk + n''$ usw. Auch hier lässt sich leicht beweisen, dass es ebenso viele Teilerformen von $xx - A$ wie Nichtteilerformen gibt.

Beispiel. So ergibt sich $+10$ als Rest aller Primzahlen in einer der Formen $40k+1, 3, 9, 13, 27, 31, 37, 39$, als Nichtrest dagegen aller Primzahlen in einer der Formen $40k+7, 11, 17, 19, 21, 23, 29, 33$.

*) Ohne den Faktor t.

150.

Diese Formen haben mehrere recht bemerkenswerte Eigenschaften; wir führen aber nur eine an. Ist B eine zusammengesetzte, zu A teilerfremde Zahl, unter deren Primfaktoren $2m$ in einer Nichtteilerform von $xx - A$ liegen, so liegt B in einer Teilerform von $xx - A$. Ist dagegen die Anzahl der Primfaktoren von B, die in einer Nichtteilerform von $xx - A$ liegen, ungerade, so liegt auch B in einer Nichtteilerform. Den Beweis, der nicht schwierig ist, lassen wir weg. Daraus folgt, dass nicht nur jede Primzahl, sondern auch jede zusammengesetzte ungerade, zu A teilerfremde Zahl in einer Nichtteilerform ein Nichtteiler ist: Ein Primfaktor einer solchen Zahl muss notwendig ein Nichtteiler sein.

Über die Arbeiten anderer zu diesen Untersuchungen.

151.

Der Fundamentalsatz, der gewiss zu den elegantesten Ergebnissen auf diesem Gebiet gehört, wurde bisher von niemandem in der einfachen Form ausgesprochen, in der wir ihn oben angegeben haben. Das ist umso erstaunlicher, als dem berühmten Euler bereits gewisse andere darauf beruhende Aussagen bekannt waren, von denen man leicht zu ihm hätte zurückkommen können. Er wusste, dass es bestimmte Formen gibt, die alle Primteiler der Zahlen der Form $xx - A$ enthalten, und andere, die alle primen Nichtteiler von Zahlen derselben Form umfassen und die ersten Formen ausschließen; auch hatte er ein Verfahren gefunden, diese Formen zu bestimmen. Alle seine Versuche, zu einem Beweis zu gelangen, blieben aber erfolglos und machten diese durch Beispiele gefundene Wahrheit nur wahrscheinlicher. In einer Abhandlung, *Novae demonstrationes circa divisores numerorum formae* $xx + nyy$, die am 20. November 1775 in der Petersburger Akademie vorgetragen wurde und nach dem Tod dieses großen Mannes in *Bd.* I der *Nov. Act.* dieser Akademie, S. 47 ff., erhalten ist, scheint er allerdings geglaubt zu haben, sein Ziel erreicht zu haben. Doch hier schlich sich ein Fehler ein: Auf S. 65 nahm er *stillschweigend* an, dass solche Teiler- und Nichtteilerformen existieren*. Daraus war leicht herzuleiten, *welche* Formen es sein müssen; das Verfahren, mit dem er diese Annahme begründete, scheint jedoch nicht geeignet. In einer anderen Schrift, *De criteriis aequationis* $fxx+gyy = hzz$ *utrumque resolutionem admittat necne*, Opusc. Anal., Bd. I (wobei f, g, h gegeben und x, y, z unbestimmt sind), fand er anhand von Beispielen: Ist die Gleichung für einen Wert $h = s$ lösbar, so ist sie auch für jeden anderen Wert lösbar, der s nach dem Modul $4fg$ kongruent ist, sofern er eine Primzahl ist. Aus diesem Satz lässt sich die erwähnte Annahme ohne Schwierigkeit beweisen. Aber auch der Beweis dieses Satzes entzog sich

*Dass es nämlich Zahlen r, r', r'' usw.; n, n', n'' usw. gibt, alle verschieden und $< 4A$, sodass alle Primteiler von $xx - A$ in einer der Formen $4Ak + r$, $4Ak + r'$ usw. und alle primen Nichtteiler in einer der Formen $4Ak + n$, $4Ak + n'$ usw. liegen (wobei k eine unbestimmte Zahl bezeichnet).

allen seinen Bemühungen[*]. Das ist nicht erstaunlich, da man unserer Ansicht nach vom Fundamentalsatz ausgehen musste. Im Übrigen wird sich die Richtigkeit dieses Satzes unmittelbar aus dem ergeben, was wir im nächsten Abschnitt behandeln.

Nach Euler beschäftigte sich der bekannte Le Gendre mit demselben Gegenstand in seiner ausgezeichneten Abhandlung *Recherches d'analyse indéterminée*, Hist. de l'Ac. des Sc., 1785, S. 465 ff. Dort gelangte er zu einem Satz, der inhaltlich mit dem Fundamentalsatz übereinstimmt: Bezeichnen p, q zwei positive Primzahlen, so sind die im Betrag kleinsten Reste der Potenzen $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$ nach den Moduln q, p entweder beide $+1$ oder beide -1, wenn p oder q die Form $4n+1$ hat. Haben dagegen sowohl p als auch q die Form $4n+3$, so ist der eine kleinste Rest $+1$, der andere -1 (S. 516). Daraus folgt nach Artikel 106, dass die *Beziehung* (im Sinne von Artikel 146) von p zu q und von q zu p *dieselbe* ist, wenn p oder q die Form $4n+1$ hat, dagegen *entgegengesetzt*, wenn sowohl p als auch q die Form $4n+3$ haben. Dieser Satz ist unter den Aussagen aus Artikel 131 enthalten; er folgt auch aus 1, 3, 9 des Artikels 133. Umgekehrt lässt sich der Fundamentalsatz aus ihm herleiten. Le Gendre versuchte auch einen Beweis, über den wir, da er äußerst einfallsreich ist, im nächsten Abschnitt ausführlicher sprechen werden. Da er aber darin einiges ohne Beweis voraussetzte (wie er selbst auf S. 520 zugibt: *Wir haben nur angenommen* usw.), was teils bisher von niemandem bewiesen wurde, teils jedenfalls unserer Ansicht nach ohne den Fundamentalsatz selbst nicht bewiesen werden kann, scheint sein eingeschlagener Weg nicht zum Ziel führen zu können; unser Beweis muss daher als der erste gelten. — Weiter unten werden wir noch *zwei andere Beweise* dieses äußerst wichtigen Satzes geben, die vom vorigen und voneinander völlig verschieden sind.

[*]Wie er selbst an der angegebenen Stelle, S. 216, zugibt: „Ein Beweis dieses höchst eleganten Satzes fehlt noch, nachdem viele ihn schon lange vergeblich gesucht haben. … Wer einen Beweis dieses Satzes findet, wird also sehr viel geleistet haben." — Wie sehr dieser unsterbliche Mann einen Beweis dieses Satzes und anderer wünschte, die nur besondere Fälle des Fundamentalsatzes sind, zeigen viele andere Stellen der Opusc. Anall. Vergleiche *Additamentum ad diss.* VIII, Bd. I, und *diss.* XIII, Bd. II, sowie mehrere bereits an verschiedenen Stellen angeführte Abhandlungen in den Comment. Petrop.

Quadratische Kongruenzen mit linearem Glied.

152.

Bisher haben wir die reine Kongruenz $xx \equiv A \pmod{m}$ behandelt und gezeigt, wie sich ihre Lösbarkeit entscheiden lässt. Die Ermittlung *der Wurzeln selbst* wurde in Artikel 105 auf den Fall zurückgeführt, dass m eine Primzahl oder Primzahlpotenz ist; der zweite Fall in Artikel 101 auf den, dass m eine Primzahl ist. Für diesen Fall umfasst das in Artikel 61 ff. Angegebene zusammen mit dem, was wir in den Abschnitten V und VIII behandeln werden, fast alles, was sich durch direkte Methoden gewinnen lässt. Diese sind aber dort, wo sie anwendbar sind, meist unendlich viel umständlicher als die indirekten Methoden, die wir in Abschnitt VI behandeln werden, und daher eher wegen ihrer Schönheit als wegen ihres praktischen Nutzens bemerkenswert. — *Quadratische Kongruenzen mit linearem Glied* lassen sich leicht auf reine zurückführen. Soll die gegebene Kongruenz

$$axx + bx + c \equiv 0$$

nach dem Modul m gelöst werden, so ist dazu die folgende Kongruenz äquivalent:

$$4aaxx + 4abx + 4ac \equiv 0 \pmod{4am}$$

Das heißt, jede Zahl, die einer von beiden genügt, genügt auch der anderen. Diese lässt sich so schreiben:

$$(2ax + b)^2 \equiv bb - 4ac \pmod{4am}$$

Daraus lassen sich alle Werte von $2ax + b$ unterhalb von $4am$ finden, sofern es welche gibt. Bezeichnet man sie mit r, r', r'' usw., so erhält man alle Lösungen der gegebenen Kongruenz aus den Lösungen der Kongruenzen

$$2ax \equiv r - b, \quad 2ax \equiv r' - b \text{ usw. } \pmod{4am}$$

die wir in Abschnitt II finden lehrten. Außerdem lässt sich die Lösung meist durch verschiedene Kunstgriffe verkürzen. *Zum Beispiel* kann man anstelle der gegebenen eine äquivalente Kongruenz

$$a'xx + 2b'x + c' \equiv 0$$

finden, in der a' die Zahl m teilt. Der Kürze wegen können wir dies hier nicht erklären; dazu kann man den letzten Abschnitt heranziehen.

FÜNFTER ABSCHNITT
QUADRATISCHE FORMEN UND UNBESTIMMTE GLEICHUNGEN ZWEITEN GRADES

Ziel der Untersuchung; Definition und Bezeichnung der Formen.

153.

In diesem Abschnitt werden wir vor allem Funktionen zweier Unbestimmter x, y von der Gestalt

$$axx + 2bxy + cyy$$

behandeln, wobei a, b, c gegebene ganze Zahlen sind. Wir nennen sie *Formen zweiten Grades* oder einfach *Formen*. Auf dieser Untersuchung wird die Lösung des berühmten Problems aufbauen, alle Lösungen einer beliebigen unbestimmten Gleichung zweiten Grades mit zwei Unbekannten zu finden, ob diese nun ganzzahlige oder nur rationale Werte annehmen sollen. Der ausgezeichnete Lagrange hat dieses Problem bereits in seiner ganzen Allgemeinheit gelöst. Viele weitere Ergebnisse über die Natur der *Formen* haben teils dieser große Geometer selbst, teils der ausgezeichnete Euler erstmals gefunden; andere, die schon Fermat entdeckt hatte, haben sie mit Beweisen versehen. Als wir die Formen eingehend untersuchten, boten sich uns jedoch so viele neue Ergebnisse, dass wir es der Mühe wert fanden, den ganzen Gegenstand von Anfang an neu aufzugreifen. Dazu hatten wir umso mehr Grund, als wir feststellten, dass die an vielen Stellen verstreuten Entdeckungen jener Männer nur wenigen bekannt waren; ferner, weil die Methode, nach der wir vorgehen werden, größtenteils unsere eigene ist; und schließlich, weil unsere Ergebnisse ohne eine erneute Darstellung der ihren nicht einmal verständlich wären. Wir zweifeln nicht daran, dass auf diesem Gebiet noch viele ausgezeichnete Ergebnisse verborgen liegen, an denen andere ihre Kräfte erproben können. Die Geschichte bedeutender Ergebnisse werden wir stets an der jeweiligen Stelle darstellen.

Die Form $axx + 2bxy + cyy$ werden wir, wenn es auf die Unbestimmten x, y nicht ankommt, mit (a, b, c) bezeichnen. Dieser Ausdruck bezeichnet also, ohne die Unbestimmten festzulegen, die Summe dreier Teile: des Produkts der gegebenen Zahl a mit dem Quadrat einer beliebigen Unbestimmten; des Produkts der doppelten Zahl b mit dieser und einer anderen Unbestimmten; und des Produkts der Zahl c mit dem Quadrat der zweiten Unbestimmten. *Zum Beispiel* bezeichnet $(1, 0, 2)$ die Summe eines Quadrats und eines doppelten Quadrats. Die Formen (a, b, c) und (c, b, a) bezeichnen zwar dasselbe, wenn wir nur auf die *Teile selbst* achten; sie unterscheiden sich aber, wenn wir auch die *Reihenfolge* der Teile berücksichtigen. Wir werden sie deshalb von nun an sorgfältig unterscheiden. Was wir dadurch gewinnen, wird im Folgenden deutlich genug werden.

Darstellung von Zahlen; Determinante.

154.

Wir sagen, dass eine gegebene Zahl durch eine gegebene Form *dargestellt* wird, wenn den Unbestimmten der Form solche ganzzahligen Werte zugewiesen werden, dass der Wert der Form gleich der gegebenen Zahl wird. Hier gilt folgender

Satz. *Kann die Zahl M durch die Form (a, b, c) so dargestellt werden, dass die dabei verwendeten Werte der Unbestimmten teilerfremd sind, so ist $bb - ac$ ein quadratischer Rest der Zahl M.*

Beweis. Die Werte der Unbestimmten seien m, n, also

$$amm + 2bmn + cnn = M$$

und die Zahlen μ, ν seien so gewählt, dass $\mu m + \nu n = 1$ gilt (Artikel 40). Durch Ausmultiplizieren zeigt man leicht, dass

$$\begin{aligned} &amm + 2bmn + cnn)(a\nu\nu - 2b\mu\nu + c\mu\mu \\ &\quad = (\mu(mb + nc) - \nu(ma + nb))^2 - (bb - ac)(m\mu + n\nu)^2 \end{aligned}$$

oder

$$M(a\nu\nu - 2b\mu\nu + c\mu\mu) = (\mu(mb + nc) - \nu(ma + nb))^2 - (bb - ac)$$

Also gilt

$$bb - ac \equiv (\mu(mb + nc) - \nu(ma + nb))^2 \pmod{M}$$

das heißt, $bb - ac$ ist ein quadratischer Rest von M.

Die Zahl $bb - ac$ nennen wir die *Determinante* der Form (a, b, c). Wie wir später zeigen werden, hängen die Eigenschaften einer Form vor allem von der Beschaffenheit dieser Zahl ab.

Werte des Ausdrucks $\sqrt{(bb - ac)}(mod.\, M)$, zu denen eine Darstellung der Zahl M durch die Form (a, b, c) gehört.

155.

Damit ist

$$\mu(mb + nc) - \nu(ma + nb)$$

ein Wert des Ausdrucks

$$\sqrt{(bb - ac)} \pmod{M}$$

Die Zahlen μ, ν lassen sich aber auf unendlich viele Arten so bestimmen, dass $\mu m + \nu n = 1$ gilt. Daraus ergeben sich immer neue Werte jenes Ausdrucks; untersuchen wir ihren Zusammenhang. Es gelte nicht nur $\mu m + \nu n = 1$, sondern auch $\mu' m + \nu' n = 1$, und wir setzen

$$\mu(mb + nc) - \nu(ma + nb) = v, \quad \mu'(mb + nc) - \nu'(ma + nb) = v'$$

Multiplizieren wir die Gleichung $\mu m + \nu n = 1$ mit μ', die andere Gleichung $\mu' m + \nu' n = 1$ mit μ und subtrahieren, so ergibt sich $\mu' - \mu = n(\mu'\nu - \mu\nu')$. Multiplizieren

wir ebenso die erste mit ν' und die zweite mit ν, so ergibt die Subtraktion $\nu' - \nu = m(\mu\nu' - \mu'\nu)$. Daraus folgt sofort

$$v' - v = (\mu'\nu - \mu\nu')(amm + 2bmn + cnn) = (\mu'\nu - \mu\nu')M$$

oder $v' \equiv v \pmod{M}$. Wie auch immer μ, ν bestimmt werden, kann die Formel $\mu(mb + nc) - \nu(ma + nb)$ also keine *verschiedenen*, das heißt inkongruenten, Werte des Ausdrucks $\sqrt{(bb-ac)} \pmod{M}$ liefern. Ist daher v irgendein Wert dieser Formel, so sagen wir, dass die Darstellung der Zahl M durch die Form $axx+2bxy+cyy$, bei der $x = m$, $y = n$ ist, *zum Wert v des Ausdrucks* $\sqrt{(bb-ac)}(mod.\, M)$ *gehört*. Außerdem lässt sich leicht zeigen: Ist ein Wert jener Formel v und gilt $v' \equiv v \pmod{M}$, so kann man anstelle der Zahlen μ, ν, die v liefern, andere Zahlen μ', ν' wählen, die v' liefern. Setzen wir nämlich

$$\mu' = \mu + \frac{n(v' - v)}{M}, \quad \nu' = \nu - \frac{m(v' - v)}{M}$$

so gilt

$$\mu' m + \nu' n = \mu m + \nu n = 1$$

und der aus μ', ν' hervorgehende Wert der Formel übertrifft den aus μ, ν hervorgehenden um die Größe $(\mu'\nu - \mu\nu')M$. Diese wird $= (\mu m + \nu n)(v' - v) = v' - v$; für den erhaltenen Wert gilt also $= v'$.

156.

Haben wir zwei Darstellungen derselben Zahl M durch dieselbe Form (a, b, c), bei denen die Werte der Unbestimmten jeweils teilerfremd sind, so können sie entweder zu demselben Wert des Ausdrucks $\sqrt{(bb-ac)} \pmod{M}$ oder zu verschiedenen Werten gehören. Es sei

$$M = amm + 2bmn + cnn = am'm' + 2bm'n' + cn'n'$$

und

$$\mu m + \nu n = 1, \quad \mu' m' + \nu' n' = 1$$

Gilt

$$\mu(mb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M}$$

so bleibt die Kongruenz offenbar bestehen, welche anderen geeigneten Werte auch für μ, ν und μ', ν' gewählt werden. In diesem Fall sagen wir, dass beide Darstellungen zu *demselben* Wert des Ausdrucks $\sqrt{(bb - ac)} \pmod{M}$ gehören. Gilt die Kongruenz dagegen bei irgendeiner Wahl von μ, ν und μ', ν' nicht, so gilt sie bei keiner, und die Darstellungen gehören zu *verschiedenen* Werten. Ist hingegen

$$\mu(mb + nc) - \nu(ma + nb) \equiv -(\mu'(m'b + n'c) - \nu'(m'a + n'b))$$

so sagen wir, dass die Darstellungen zu *entgegengesetzten* Werten des Ausdrucks $\sqrt{(bb-ac)}$ gehören. Alle diese Bezeichnungen verwenden wir auch dann, wenn mehrere

Darstellungen derselben Zahl durch *verschiedene* Formen mit derselben Determinante betrachtet werden.

Beispiel. Gegeben sei die Form $(3, 7, -8)$ mit der Determinante $= 73$. Sie liefert folgende Darstellungen der Zahl 57:

$$3 \,.\, 13^2 + 14 \,.\, 13 \,.\, 25 - 8 \,.\, 25^2; \quad 3 \,.\, 5^2 + 14 \,.\, 5 \,.\, 9 - 8 \,.\, 9^2$$

Für die erste können wir $\mu = 2$, $\nu = -1$ setzen. Damit ergibt sich der Wert des Ausdrucks $\sqrt{73} \pmod{57}$, zu dem die Darstellung gehört:

$$= 2(13 \,.\, 7 - 25 \,.\, 8) + (13 \,.\, 3 + 25 \,.\, 7) = -4$$

Ebenso findet man durch die Wahl $\mu = 2$, $\nu = -1$, dass die zweite Darstellung zum Wert $+4$ gehört. Beide Darstellungen gehören also zu entgegengesetzten Werten.

Bevor wir weitergehen, bemerken wir, dass Formen mit der Determinante $= 0$ aus den folgenden Untersuchungen vollständig ausgeschlossen sind. Sie würden nur die Geschlossenheit der Sätze stören und verlangen deshalb eine eigene Behandlung.

Eine Form, die eine andere enthält oder in einer anderen enthalten ist; eigentliche und uneigentliche Transformation.

157.

Lässt sich eine Form F mit den Unbestimmten x, y in eine andere Form F' mit den Unbestimmten x', y' durch Substitutionen

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

überführen, bei denen $\alpha, \beta, \gamma, \delta$ ganze Zahlen sind, so sagen wir, dass die erste die zweite *enthält* oder dass die zweite *in der ersten enthalten ist.* Die Form F sei

$$axx + 2bxy + cyy$$

und die Form F' sei

$$a'x'x' + 2b'x'y' + c'y'y'$$

Dann gelten die folgenden drei Gleichungen:

$$\begin{aligned} a' &= a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta\beta + 2b\beta\delta + c\delta\delta \end{aligned}$$

Multipliziert man die zweite Gleichung mit sich selbst und die erste mit der dritten und subtrahiert dann unter Weglassen der sich aufhebenden Glieder, so ergibt sich

$$b'b' - a'c' = (bb - ac)(\alpha\delta - \beta\gamma)^2$$

Daraus folgt, dass die Determinante der Form F' durch die Determinante der Form F teilbar und der Quotient eine Quadratzahl ist. Diese Determinanten haben also

offenbar *dasselbe Vorzeichen*. Lässt sich außerdem die Form F' durch eine ähnliche Substitution in die Form F überführen, ist also sowohl F' in F als auch F in F' enthalten, so sind die Determinanten der Formen gleich[*)] und es gilt $(\alpha\delta - \beta\gamma)^2 = 1$. In diesem Fall nennen wir die Formen *äquivalent*. Die Gleichheit der Determinanten ist also eine notwendige Bedingung für die Äquivalenz von Formen, obwohl diese daraus allein keineswegs folgt. — Die Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ nennen wir eine *eigentliche Transformation*, wenn $\alpha\delta - \beta\gamma$ positiv ist, und eine *uneigentliche*, wenn $\alpha\delta - \beta\gamma$ negativ ist. Wir sagen, dass die Form F' *eigentlich* oder *uneigentlich* in der Form F enthalten ist, wenn F durch eine eigentliche oder uneigentliche Transformation in die Form F' überführt werden kann. Sind also die Formen F, F' äquivalent, so gilt $(\alpha\delta - \beta\gamma)^2 = 1$ und daher bei einer eigentlichen Transformation $\alpha\delta - \beta\gamma = +1$, bei einer uneigentlichen $= -1$. — Sind mehrere Transformationen sämtlich eigentlich oder sämtlich uneigentlich, so nennen wir sie *gleichartig*; eine eigentliche und eine uneigentliche dagegen *ungleichartig*.

Eigentliche und uneigentliche Äquivalenz.

158.

Haben die Formen F, F' gleiche Determinanten und ist F' in F enthalten, so ist auch F in F' enthalten, und zwar eigentlich oder uneigentlich, je nachdem, ob F' eigentlich oder uneigentlich in F enthalten ist. Die Form F gehe in F' über, indem wir setzen:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

Dann geht F' in F über, wenn man

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y$$

setzt. Denn diese Substitution liefert aus F' offenbar dasselbe, was aus F durch die Substitution

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \quad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

oder

$$x = (\alpha\delta - \beta\gamma)x, \quad y = (\alpha\delta - \beta\gamma)y$$

entsteht. Dadurch wird F offenbar in $(\alpha\delta - \beta\gamma)^2 F$, das heißt wieder in F überführt (voriger Artikel). Die zweite Transformation ist offenbar eigentlich oder uneigentlich, je nachdem, ob die erste eigentlich oder uneigentlich ist.

Sind sowohl F' in F als auch F in F' *eigentlich* enthalten, so nennen wir die Formen *eigentlich äquivalent*; sind sie jeweils uneigentlich ineinander enthalten, so nennen wir sie *uneigentlich äquivalent*. — Der Nutzen dieser Unterscheidungen wird sich bald zeigen.

[*)] Aus der vorangehenden Rechnung geht klar hervor, dass diese Aussage auch für Formen mit der Determinante $= 0$ gilt. Die Gleichung $(\alpha\delta - \beta\gamma)^2 = 1$ darf aber nicht auf diesen Fall ausgedehnt werden.

Beispiel. Die Form $2xx - 8xy + 3yy$ geht durch die Substitutionen $x = 2x' + y'$, $y = 3x' + 2y'$ in die Form $-13x'x' - 12x'y' - 2y'y'$ über, diese wiederum in jene durch die Substitutionen $x' = 2x - y$, $y' = -3x + 2y$. Die Formen $(2, -4, 3)$, $(-13, -6, -2)$ sind also *eigentlich äquivalent.*

Die Probleme, denen wir uns nun zuwenden, sind folgende. I. Für zwei beliebige gegebene Formen mit derselben Determinante ist zu untersuchen, ob sie äquivalent sind oder nicht, und ob eigentlich, uneigentlich oder auf beide Arten, denn auch dies ist möglich. Haben sie verschiedene Determinanten, so ist zu untersuchen, ob wenigstens eine die andere enthält, eigentlich, uneigentlich oder auf beide Arten. Schließlich sind alle Transformationen der einen in die andere zu finden, sowohl die eigentlichen als auch die uneigentlichen. II. Für eine beliebige gegebene Form ist zu ermitteln, ob eine gegebene Zahl durch sie dargestellt werden kann, und es sind alle Darstellungen anzugeben. Da Formen mit negativer Determinante hier aber eine andere Methode verlangen als Formen mit positiver Determinante, werden wir zuerst das behandeln, was beiden gemeinsam ist, und danach die Formen jeder Art gesondert betrachten.

Entgegengesetzte Formen.

159.

Enthält die Form F die Form F' und diese wiederum die Form F'', so enthält die Form F auch die Form F''.

Die Unbestimmten der Formen F, F', F'' seien der Reihe nach $x, y,\ x', y',\ x'', y''$, und F gehe in F' über, wenn man

$$x = \alpha x' + \beta y'. \quad y = \gamma x' + \delta y'$$

setzt, und F' in F'', wenn man

$$x' = \alpha' x'' + \beta' y'', \quad y' = \gamma' x'' + \delta' y''$$

setzt. Dann lässt sich F offenbar in F'' überführen durch

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y''), \quad y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

oder

$$x = (\alpha\alpha' + \beta\gamma')x'' + (\alpha\beta' + \beta\delta')y'', \quad y = (\gamma\alpha' + \delta\gamma')x'' + (\gamma\beta' + \delta\delta')y''$$

Also enthält F die Form F''.

Wegen

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

ist dieser Ausdruck positiv, wenn $\alpha\delta - \beta\gamma$ und $\alpha'\delta' - \beta'\gamma'$ beide positiv oder beide negativ sind; er ist dagegen negativ, wenn eine dieser Zahlen positiv und die andere negativ ist. Die Form F enthält also die Form F'' *eigentlich*, wenn F die Form F' auf dieselbe Weise enthält wie F' die Form F'', und *uneigentlich*, wenn dies auf verschiedene Weise geschieht.

Daraus folgt: Haben wir beliebig viele Formen F, F', F'', F''' usw., von denen jede die folgende enthält, so enthält die erste die letzte, und zwar *eigentlich*, wenn die Anzahl der Formen, die ihre folgende uneigentlich enthalten, gerade ist, und *uneigentlich*, wenn diese Anzahl ungerade ist.

Ist die Form F der Form F' und die Form F' der Form F'' äquivalent, so ist die Form F der Form F'' äquivalent, und zwar eigentlich, wenn die Form F der Form F' auf dieselbe Weise äquivalent ist wie die Form F' der Form F'', und uneigentlich, wenn dies auf verschiedene Weise geschieht.

Da nämlich die Formen F, F' der Reihe nach den Formen F', F'' äquivalent sind, enthalten sowohl jene jeweils diese, sodass F die Form F'' enthält, als auch diese jene. Also sind F, F'' äquivalent. Aus dem Vorigen folgt aber, dass F die Form F'' eigentlich oder uneigentlich enthält, je nachdem, ob F der Form F' auf dieselbe oder auf eine andere Weise äquivalent ist wie F' der Form F''. Dasselbe gilt dafür, wie F'' die Form F enthält. Im ersten Fall sind F, F'' also eigentlich, im zweiten uneigentlich äquivalent.

Die Formen $(a, -b, c)$, (c, b, a), $(c, -b, a)$ *sind der Form* (a, b, c) *äquivalent, und zwar die ersten beiden uneigentlich, die letzte eigentlich.*

Denn $axx + 2bxy + cyy$ geht in $ax'x' - 2bx'y' + cy'y'$ über, wenn man $x = x' + 0.y'$, $y = 0.x' - y'$ setzt. Diese Transformation ist wegen $1 \times -1 - 0.0 = -1$ uneigentlich. In die Form $cx'x' + 2bx'y' + ay'y'$ geht sie durch die uneigentliche Transformation $x = 0.x' + y'$, $y = x' + 0.y'$ über und in die Form $cx'x' - 2bx'y' + ay'y'$ durch die eigentliche $x = 0.x' - y'$, $y = x' + 0.y'$.

Daraus ist klar, dass jede der Form (a, b, c) äquivalente Form entweder ihr selbst oder der Form $(a, -b, c)$ *eigentlich* äquivalent ist. Enthält eine Form die Form (a, b, c) oder ist sie in ihr enthalten, so enthält sie ebenso entweder die Form (a, b, c) oder die Form $(a, -b, c)$ *eigentlich*, oder sie ist in einer von beiden *eigentlich* enthalten. Die Formen (a, b, c), $(a, -b, c)$ nennen wir *entgegengesetzt.*

Benachbarte Formen.

160.

Haben die Formen (a, b, c), (a', b', c') dieselbe Determinante und gilt außerdem $c = a'$ und $b \equiv -b' \pmod{c}$, oder $b + b' \equiv 0 \pmod{c}$, so nennen wir diese Formen *benachbart.* Ist eine genauere Bezeichnung nötig, so nennen wir die erste der zweiten *nach links*, die zweite der ersten *nach rechts* benachbart.

So ist *zum Beispiel* die Form $(7, 3, 2)$ der Form $(3, 4, 7)$ nach rechts benachbart, die Form (3.1.3) ihrer entgegengesetzten $(3, -1, 3)$ nach beiden Seiten.

Benachbarte Formen sind stets eigentlich äquivalent. Denn die Form $axx + 2bxy + cyy$ geht in die benachbarte Form $cx'x' + 2b'x'y' + c'y'y'$ durch die Substitution $x = -y'$, $y = x' + \frac{b+b'}{c}y'$ über, die wegen $0 \times \frac{b+b'}{c} - 1 \times -1 = 1$ eigentlich ist. Das lässt sich durch Ausmultiplizieren mit Hilfe der Gleichung $bb - ac = b'b' - cc'$ leicht beweisen; $\frac{b+b'}{c}$ ist nach Voraussetzung eine ganze Zahl. — Diese Definitionen und Folgerungen gelten nicht, wenn $c = a' = 0$ ist. Dieser Fall kann aber nur bei Formen eintreten, deren Determinante eine Quadratzahl ist.

Die Formen (a, b, c), (a', b', c') sind eigentlich äquivalent, wenn $a = a'$. $b \equiv b' \pmod{a}$ gilt. Denn die Form (a, b, c) ist der Form $(c, -b, a)$ eigentlich äquivalent (voriger Artikel), und diese ist der Form (a', b', c') nach links benachbart.

Gemeinsame Teiler der Koeffizienten von Formen.

161.

Enthält die Form (a, b, c) *die Form* (a', b', c')*, so teilt jeder gemeinsame Teiler der Zahlen* a, b, c *auch die Zahlen* a', b', c'*, und jeder gemeinsame Teiler der Zahlen* $a, 2b, c$ *auch die Zahlen* $a', 2b', c'$*.*

Geht nämlich die Form $axx + 2bxy + cyy$ durch die Substitutionen $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ in die Form $a'x'x' + 2b'x'y' + c'y'y'$ über, so gelten die Gleichungen

$$\begin{aligned} a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma &= a' \\ a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta &= b' \\ a\beta\beta + 2b\beta\delta + c\delta\delta &= c' \end{aligned}$$

aus denen die Aussage sofort folgt. Für ihren zweiten Teil verwendet man anstelle der zweiten Gleichung die Gleichung $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$.

Daraus folgt, dass der größte gemeinsame Teiler der Zahlen $a, b(2b), c$ zugleich den größten gemeinsamen Teiler der Zahlen $a', b'(2b'), c'$ teilt. Enthält also außerdem die Form (a', b', c') die Form (a, b, c), sind die Formen also äquivalent, so ist der größte gemeinsame Teiler der Zahlen $a, b(2b), c$ gleich dem größten gemeinsamen Teiler der Zahlen $a', b'(2b'), c'$, weil dann sowohl jener diesen als auch dieser jenen teilen muss. Haben in diesem Fall die Zahlen $a, b(2b), c$ keinen gemeinsamen Teiler, ist also ihr größter gemeinsamer Teiler $= 1$, so haben auch $a', b'(2b'), c'$ keinen gemeinsamen Teiler.

Zusammenhang aller gleichartigen Transformationen einer gegebenen Form in eine gegebene Form.

162.

Aufgabe. *Enthält die Form*

$$AXX + 2BXY + CYY \quad \ldots \quad F$$

die Form

$$axx + 2bxy + cyy \quad \ldots\ldots \quad f$$

und ist irgendeine Transformation der ersten in die zweite gegeben, so sind daraus alle übrigen ihr gleichartigen Transformationen abzuleiten.

Lösung. Die gegebene Transformation sei $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$. Nehmen wir zunächst an, dass eine andere, ihr gleichartige Transformation $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$ gegeben ist, um zu untersuchen, was daraus folgt. Bezeichnen wir die Formen und ihre Determinanten durch $F, f, = D, d$ und setzen $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$, so gilt (Artikel 157) $d = Dee = De'e'$. Da nach Voraussetzung e, e' dasselbe Vorzeichen haben, ist $e = e'$. Es gelten die folgenden sechs Gleichungen:

$$\begin{aligned}
A\alpha\alpha + 2B\alpha\gamma + C\gamma\gamma &= a \quad \ldots\ldots\ldots [1]\\
A\alpha'\alpha' + 2B\alpha'\gamma' + C\gamma'\gamma' &= a \quad \ldots\ldots\ldots [2]\\
A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta &= b \quad \ldots\ldots\ldots [3]\\
A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' &= b \quad \ldots\ldots\ldots [4]\\
A\beta\beta + 2B\beta\delta + C\delta\delta &= c \quad \ldots\ldots\ldots [5]\\
A\beta'\beta' + 2B\beta'\delta' + C\delta'\delta' &= c \quad \ldots\ldots\ldots [6]
\end{aligned}$$

Bezeichnen wir der Kürze halber die Zahlen

$$\begin{gathered}
A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'\\
A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')\\
A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta'
\end{gathered}$$

mit $a', 2b', c'$, so leiten wir aus den vorigen Gleichungen die folgenden neuen ab[*)]:

$$a'a' - D(\alpha\gamma' - \gamma\alpha')^2 = aa \qquad \ldots\ldots\ldots \quad [7]$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab \qquad \ldots \quad [8]$$
$$4b'b' - D\big((\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee'\big) = 2bb + 2ac$$

Addiert man $2Dee' = 2d = 2bb - 2ac$, so ergibt sich

$$4b'b' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4bb \qquad \ldots\ldots \quad [9]$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = bb$$

und durch Subtraktion von $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = bb - ac$ folgt

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac \qquad \ldots\ldots \quad [10]$$
$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc \qquad \ldots \quad [11]$$
$$c'c' - D(\beta\delta' - \delta\beta')^2 = cc \qquad \ldots\ldots\ldots \quad [12]$$

Der größte gemeinsame Teiler der Zahlen $a, 2b, c$ sei nun m, und die Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ seien so bestimmt, dass

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

gilt (Artikel 40). Man multipliziere die Gleichungen $7, 8, 9, 10, 11, 12$ der Reihe nach mit $\mathfrak{AA}, 2\mathfrak{AB}, \mathfrak{BB}, 2\mathfrak{AC}, 2\mathfrak{BC}, \mathfrak{CC}$ und addiere die Produkte. Setzen wir nun der Kürze halber

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T \qquad \ldots\ldots\ldots \quad [13]$$
$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')$$
$$+ \mathfrak{C}(\beta\delta' - \delta\beta') = U \qquad \ldots \quad [14]$$

wobei T, U offenbar ganze Zahlen sind, so ergibt sich

$$TT - DUU = mm$$

Wir gelangen also zu dem eleganten Schluss, dass *aus je zwei beliebigen gleichartigen Transformationen der Form F in f eine ganzzahlige Lösung der unbestimmten Gleichung* $tt - Duu = mm$ *folgt*, nämlich $t = T,\ u = U$. Da wir in unseren Überlegungen nicht vorausgesetzt haben, dass die Transformationen *verschieden* sind, muss sogar *eine* Transformation, zweimal betrachtet, eine Lösung liefern. Dann gilt aber wegen $\alpha' = \alpha,\ \beta' = \beta$ usw. auch $a' = a,\ b' = b,\ c' = c$ und daher $T = m,\ U = 0$, eine Lösung, die sich von selbst versteht.

[*)] Diese Gleichungen entstehen folgendermaßen: 7 aus 1.2, das heißt durch Multiplikation der Gleichung (1) mit der Gleichung (2), oder genauer, indem die linke Seite jener mit der linken Seite dieser und ihre rechte Seite mit der rechten Seite dieser multipliziert und die Produkte gleichgesetzt werden; 8 aus $1.4 + 2.3$; die folgende nicht nummerierte aus $1.6 + 2.5 + 3.4 + 3.4$; die folgende nicht nummerierte aus 3.4; 11 aus $3.6 + 4.5$; 12 aus 5.6. Eine ähnliche Bezeichnung werden wir auch im Folgenden stets verwenden. Das Ausmultiplizieren müssen wir den Lesern überlassen.

Betrachten wir nun die erste Transformation und die Lösung der unbestimmten Gleichung als bekannt und untersuchen, wie daraus die zweite Transformation abgeleitet werden kann oder wie $\alpha', \beta', \gamma', \delta'$ von $\alpha, \beta, \gamma, \delta,\ T, U$ abhängen. Dazu multiplizieren wir zunächst die Gleichung [1] mit $\delta\alpha' - \beta\gamma'$, [2] mit $\alpha\delta' - \gamma\beta'$, [3] mit $\alpha\gamma' - \gamma\alpha'$, [4] mit $\gamma\alpha' - \alpha\gamma'$ und addieren die Produkte. Das ergibt

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a \quad \ldots\ldots \quad [15]$$

Ebenso ergibt sich aus

$$(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] - [6])$$

die Gleichung

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b \quad \ldots\ldots \quad [16]$$

Schließlich folgt aus $(\delta\beta' - \beta\delta')([3] - [4]) + (\alpha\delta' - \gamma\beta')[5] + (\delta\alpha' - \beta\gamma')[6]$:

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c \quad \ldots\ldots \quad [17]$$

Setzt man diese Werte $(15, 16, 17)$ in 13 ein, so ergibt sich

$$(e + e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)$$

oder

$$2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m \quad \ldots\ldots\ldots \quad [18]$$

woraus sich T viel leichter ableiten lässt als aus [13]. — Verbindet man diese Gleichung mit $15, 16, 17$, so erhält man $ma' = Ta,\ 2mb' = 2Tb,\ mc' = Tc$. Setzt man diese Werte von $a', 2b', c'$ in die Gleichungen 7—12 ein und schreibt für TT den Ausdruck $mm + DUU$, so gehen sie nach den nötigen Änderungen über in

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')^2 mm &= aaUU \\
(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')mm &= 2abUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 mm &= 4bbUU \\
(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')mm &= acUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')mm &= 2bcUU \\
(\beta\delta' - \delta\beta')^2 mm &= ccUU
\end{aligned}$$

Mit Hilfe der Gleichung [14] und der Gleichung $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$ leitet man daraus leicht Folgendes ab: Man multipliziert die erste, zweite und vierte; die zweite, dritte und fünfte; die vierte, fünfte und sechste Gleichung jeweils mit $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ und addiert die Produkte.

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')Umm &= maUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')Umm &= 2mbUU \\
(\beta\delta' - \delta\beta')Umm &= mcUU
\end{aligned}$$

Dividiert man dann durch mU*), so ergibt sich

$$\begin{aligned} aU &= (\alpha\gamma' - \gamma\alpha')m \quad \ldots\ldots\ldots [19] \\ 2bU &= (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m \quad \ldots\ldots [20] \\ cU &= (\beta\delta' - \delta\beta')m \quad \ldots\ldots\ldots [21] \end{aligned}$$

Aus jeder dieser Gleichungen lässt sich U viel leichter als aus [14] ableiten. — Zugleich folgt daraus, dass bei jeder Wahl von $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, die auf unendlich viele verschiedene Arten möglich ist, sowohl T als auch U jeweils denselben Wert behalten.

Multipliziert man nun die Gleichung 18 mit α, 19 mit 2β und 20 mit $-\alpha$, so ergibt sich durch Addition

$$2\alpha eT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m$$

Ebenso folgt aus $\beta[18] + \beta[20] - 2\alpha[21]$

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m$$

Ferner folgt aus $\gamma[18] + 2\delta[19] - \gamma[20]$

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m$$

Schließlich ergibt sich aus $\delta[18] + \delta[20] - 2\gamma[21]$

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m$$

Setzt man in diesen Formeln für a, b, c die Werte aus $1, 3, 5$ ein, so folgt

$$\begin{aligned} \alpha' m &= \alpha T - (\alpha B + \gamma C)U \\ \beta' m &= \beta T - (\beta B + \delta C)U \\ \gamma' m &= \gamma T + (\alpha A + \gamma B)U \\ \delta' m &= \delta T + (\beta A + \delta B)U \text{*)} \end{aligned}$$

Aus der vorangehenden Untersuchung folgt, dass es keine Transformation der Form F in f gibt, die der gegebenen gleichartig und nicht in der Formel

$$\begin{aligned} X &= \tfrac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \tfrac{1}{m}(\beta t - (\beta B + \delta C)u)y \\ Y &= \tfrac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \tfrac{1}{m}(\delta t + (\beta A + \delta B)u)y \quad \ldots \quad \text{(I)} \end{aligned}$$

enthalten wäre. Dabei durchlaufen t, u alle ganzen Zahlen, die der Gleichung $tt - Duu = mm$ genügen. Daraus können wir aber noch nicht schließen, dass alle Werte

*) Das wäre nicht erlaubt, wenn $U = 0$ wäre. Dann aber würde die Richtigkeit der Gleichungen 19, 20, 21 sofort aus der ersten, dritten und sechsten der vorangehenden Gleichungen folgen.

*) Daraus ergibt sich leicht

$$\begin{aligned} AeU &= (\delta\gamma' - \gamma\delta')m \\ 2BeU &= (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m \\ CeU &= (\beta\alpha' - \alpha\beta')m \end{aligned}$$

von t, u, die jene Gleichung erfüllen, in die Formel (I) eingesetzt geeignete Transformationen liefern. Es gilt jedoch:

1. Dass die Form F durch eine Substitution aus beliebigen solchen Werten von t, u stets in die Form f übergeht, lässt sich durch Ausmultiplizieren mit Hilfe der Gleichungen $1, 3, 5$ und der Gleichung $tt - Duu = mm$ leicht bestätigen. Die eher lange als schwierige Rechnung lassen wir der Kürze halber weg.

2. Jede aus der Formel abgeleitete Transformation ist der gegebenen gleichartig. Denn

$$\begin{aligned}&\tfrac{1}{m}(\alpha t - (\alpha B + \gamma C)u) \times \tfrac{1}{m}(\delta t + (\beta A + \delta B)u)\\ &\quad - \tfrac{1}{m}(\beta t - (\beta B + \delta C)u) \times \tfrac{1}{m}(\gamma t + (\alpha A + \gamma B)u)\\ &\qquad = \tfrac{1}{mm}(\alpha\delta - \beta\gamma)(tt - Duu) = \alpha\delta - \beta\gamma\end{aligned}$$

3. Haben die Formen F, f verschiedene Determinanten, so kann die Formel (I) für manche Werte von t, u Substitutionen liefern, die *Brüche* enthalten und deshalb verworfen werden müssen. Alle übrigen sind jedoch geeignete Transformationen, und weitere gibt es nicht.

4. Haben dagegen die Formen F, f dieselbe Determinante und sind sie daher *äquivalent*, so liefert die Formel (I) keine Transformationen, die Brüche enthalten, und stellt somit in diesem Fall die vollständige Lösung der Aufgabe dar. Das beweisen wir folgendermaßen.

Aus dem Satz des vorigen Artikels folgt in diesem Fall, dass m zugleich ein gemeinsamer Teiler der Zahlen $A, 2B, C$ ist. Wegen $tt - Duu = mm$ gilt $tt - BBuu = mm - ACuu$, also ist $tt - BBuu$ durch mm teilbar. Damit ist erst recht $4tt - 4BBuu$ dadurch teilbar, und folglich, weil $2B$ durch m teilbar ist, auch $4tt$ durch mm und daher $2t$ durch m. Somit sind $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ ganze Zahlen, und zwar, weil ihre Differenz $\frac{4}{m}Bu$ gerade ist, entweder beide gerade oder beide ungerade. Wären beide ungerade, so wäre auch ihr Produkt ungerade. Dieses ist aber als Vierfaches der Zahl $\frac{1}{mm}(tt - BBuu)$, die wir gerade als ganzzahlig erkannt haben, notwendig gerade. Dieser Fall ist also unmöglich; daher sind $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ stets gerade und somit $\frac{1}{m}(t + Bu)$, $\frac{1}{m}(t - Bu)$ ganze Zahlen. Daraus folgt ohne Mühe, dass alle vier Koeffizienten in (I) stets ganzzahlig sind. *W.z.b.w.*

Aus dem Vorigen folgt: Kennt man alle Lösungen der Gleichung $tt - Duu = mm$, so lassen sich daraus alle der gegebenen Transformation gleichartigen Transformationen der Form (A, B, C) in (a, b, c) ableiten. Wie man jene Lösungen findet, werden wir im Folgenden zeigen. Hier bemerken wir nur, dass ihre Anzahl stets endlich ist, wenn D negativ oder positiv und zugleich eine Quadratzahl ist, dagegen unendlich, wenn D positiv und keine Quadratzahl ist. Gilt dieser letzte Fall und gilt zugleich die Gleichheit $D = d$ nicht (oben Punkt 3^0), so müsste außerdem untersucht werden, wie sich im Voraus diejenigen Werte von t, u, die von Brüchen freie Substitutionen liefern, von denen unterscheiden lassen, die gebrochene ergeben. Für diesen Fall werden wir aber unten eine andere Methode angeben, die diesen Nachteil nicht hat (Artikel 214).

Beispiel. Die Form $xx + 2yy$ geht durch die eigentliche Substitution $x = 2x' + 7y'$, $y = x' + 5y'$ in die Form $(6, 24, 99)$ über. Gesucht sind *alle* eigentlichen Transformationen jener Form in diese. Hier ist $D = -2,\ m = 3$, also lautet die zu lösende Gleichung $tt + 2uu = 9$. Ihr wird auf sechs verschiedene Arten genügt, nämlich durch die Wahl $t = 3, -3, 1, -1, 1, -1;\ u = 0, 0, 2, 2, -2, -2$ der Reihe nach. Die dritte und die sechste Lösung ergeben Substitutionen mit Brüchen und müssen deshalb verworfen werden. Aus den übrigen folgen vier Substitutionen:

$$x = \begin{cases} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{cases} \qquad y = \begin{cases} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y' \end{cases}$$

deren erste die gegebene ist.

Ambige Formen.

163.

Wir haben oben bereits nebenbei erwähnt, dass eine Form F eine andere F' sowohl eigentlich als auch uneigentlich enthalten kann. Das tritt offenbar ein, wenn sich zwischen die Formen F, F' eine andere Form G so einschieben lässt, dass F die Form G und G die Form F' enthält und die Form G sich selbst uneigentlich äquivalent ist. Nehmen wir nämlich an, F enthalte G eigentlich oder uneigentlich. Da G die Form G uneigentlich enthält, enthält F die Form G auch uneigentlich beziehungsweise eigentlich, also in beiden Fällen sowohl eigentlich als auch uneigentlich (Artikel 159). Ebenso folgt daraus: Auf welche Weise auch G die Form F' enthalten mag, F muss die Form F' stets sowohl eigentlich als auch uneigentlich enthalten. — Dass es Formen gibt, die sich selbst uneigentlich äquivalent sind, zeigt der naheliegendste Fall, in dem das mittlere Glied der Form $= 0$ ist. Eine solche Form ist nämlich sich selbst entgegengesetzt (Artikel 159) und daher uneigentlich äquivalent. Allgemeiner besitzt jede Form (a, b, c), in der $2b$ durch a teilbar ist, diese Eigenschaft. Denn ihr ist die Form (c, b, a) nach links benachbart (Artikel 160) und daher eigentlich äquivalent. Nach Artikel 159 ist aber (c, b, a) der Form (a, b, c) uneigentlich äquivalent, also ist (a, b, c) sich selbst uneigentlich äquivalent. Solche Formen (a, b, c), bei denen $2b$ durch a teilbar ist, nennen wir *ambig*. Es gilt also folgender Satz:

Eine Form F enthält eine andere Form F' sowohl eigentlich als auch uneigentlich, wenn sich eine ambige Form finden lässt, die in F enthalten ist und F' enthält. Diese Aussage lässt sich aber auch umkehren, nämlich:

Satz über den Fall, dass eine Form zugleich eigentlich und uneigentlich in einer anderen enthalten ist.

164.

Satz. *Enthält die Form*

$$Axx + 2Bxy + Cyy \quad \ldots\ldots \quad (F)$$

die Form

$$A'x'x' + 2B'x'y' + C'y'y' \quad \ldots\ldots \quad (F')$$

sowohl eigentlich als auch uneigentlich, so lässt sich eine ambige Form finden, die in F enthalten ist und die Form F' enthält.

Wir nehmen an, dass die Form F in die Form F' sowohl durch die Substitution

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

als auch durch die folgende, ihr ungleichartige Substitution übergeht:

$$x = \alpha' x' + \beta' x', \qquad y = \gamma' x' + \delta' y'$$

Bezeichnen wir die Zahlen $\alpha\delta - \beta\gamma$, $\alpha'\delta' - \beta'\gamma'$ mit e, e', so gilt $B'B' - A'C' = ee(BB - AC) = e'e'(BB - AC)$ und daher $ee = e'e'$. Da nach Voraussetzung e, e'

entgegengesetzte Vorzeichen haben, gilt $e = -e'$ oder $e + e' = 0$. Setzt man nun in F' für x' den Ausdruck $\delta' x'' - \beta' y''$ und entsprechend $y', -\gamma' x'' + \alpha' y''$ ein, so entsteht offenbar dieselbe Form, als wenn man in F schreibt:

$$\begin{aligned}
\textit{entweder } 1) \text{ für } x \quad & \alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'') \\
\textit{d. h.} \quad & (\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y'' \\
\text{und für } y \quad & \gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'') \\
\textit{d. h.} \quad & (\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y'' \\
\textit{oder } 2) \text{ für } x \quad & \alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'') \quad \textit{d. h.} \quad e'x'' \\
\text{und für } y \quad & \gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'') \quad \textit{d. h.} \quad e'y''
\end{aligned}$$

Bezeichnen wir also die Zahlen $\alpha\delta' - \beta\gamma',\ \beta\alpha' - \alpha\beta',\ \gamma\delta' - \delta\gamma',\ \delta\alpha' - \gamma\beta'$ mit a, b, c, d, so wird die Form F durch die beiden Substitutionen

$$x = ax'' + by'', \quad y = cx'' + dy''; \qquad x = e'x'', \quad y = e'y''$$

in dieselbe Form überführt. Daraus erhalten wir die folgenden drei Gleichungen:

$$\begin{aligned}
Aaa + 2Bac + Ccc &= Ae'e' \quad \ldots\ldots\ldots [1] \\
Aab + B(ad + bc) + Ccd &= Be'e' \quad \ldots\ldots [2] \\
Abb + 2Bbd + Cdd &= Ce'e' \quad \ldots\ldots\ldots [3]
\end{aligned}$$

Aus den Werten von a, b, c, d findet man aber

$$ad - bc = ee' = -ee = -e'e' \quad \ldots\ldots [4]$$

Damit ergibt sich aus $d[1] - c[2]$

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'e'$$

und daher

$$A(a + d) = 0$$

Ferner ergibt sich aus $(a + d)[2] - b[1] - c[3]$

$$(Ab + B(a + d) + Cc)(ad - bc) = (-Ab + B(a + d) - Cc)e'e'$$

und daher

$$B(a + d) = 0$$

Schließlich folgt aus $a[3] - b[2]$

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)e'e'$$

und daher

$$C(a + d) = 0$$

Da nicht alle A, B, C gleich $= 0$ sein können, gilt notwendig $a+d=0$ oder $a=-d$. Aus $a[2]-b[1]$ folgt

$$(Ba+Cc)(ad-bc)=(Ba-Ab)e'e'$$

und somit

$$Ab-2Ba-Cc=0 \quad \ldots\ldots\ldots \quad [5]$$

Aus den Gleichungen $e+e'=0$, $a+d=0$ oder

$$\alpha\delta-\beta\gamma+\alpha'\delta'-\beta'\gamma'=0, \quad \alpha\delta'-\beta\gamma'-\gamma\beta'+\delta\alpha'=0$$

folgt $(\alpha+\alpha')(\delta+\delta')=(\beta+\beta')(\gamma+\gamma')$ oder

$$(\alpha+\alpha'):(\gamma+\gamma')=(\beta+\beta'):(\delta+\delta')$$

Dieses Verhältnis*) werde in kleinsten Zahlen als $m:n$ geschrieben, sodass m, n teilerfremd sind. Man wähle μ, ν so, dass $\mu m+\nu n=1$ gilt. Ferner sei r der größte gemeinsame Teiler der Zahlen a, b, c. Sein Quadrat teilt daher $aa+bc$ oder $bc-ad$ oder ee, also teilt r auch e. Nehmen wir bei diesen Festlegungen an, dass die Form F durch die Substitution

$$x=mt+\frac{\nu e}{r}u, \qquad y=nt-\frac{\mu e}{r}u$$

in die Form $Mtt+2Ntu+Puu$, (G) übergeht, so ist diese ambig und enthält die Form F'.

Beweis. I. Um zu zeigen, dass die Form G ambig ist, beweisen wir

$$M(b\mu\mu-2a\mu\nu-c\nu\nu)=2Nr$$

Da r die Zahlen a, b, c teilt, ist $\frac{1}{r}(b\mu\mu-2a\mu\nu-c\nu\nu)$ eine ganze Zahl und daher $2N$ ein Vielfaches von M. Es gilt aber

$$M=Amm+2Bmn+Cnn,$$
$$Nr=(Am\nu-B(m\mu-n\nu)-Cn\mu)e \quad .. \quad [6]$$

Ferner bestätigt man durch Ausmultiplizieren leicht, dass

$$\begin{aligned}2e+2a&=e-e'+a-d\\&=(\alpha-\alpha')(\delta+\delta')-(\beta-\beta')(\gamma+\gamma')\end{aligned}$$

$$2b=(\alpha+\alpha')(\beta-\beta')-(\alpha-\alpha')(\beta+\beta')$$

gilt. Wegen $m(\gamma+\gamma')=n(\alpha+\alpha')$, $m(\delta+\delta')=n(\beta+\beta')$ ergibt sich daraus

*) Wären alle $\alpha+\alpha', \gamma+\gamma', \beta+\beta', \delta+\delta'$ gleich $= 0$, so wäre das Verhältnis unbestimmt und die Methode nicht anwendbar. Schon eine kurze Überlegung zeigt aber, dass dies mit unseren Voraussetzungen unvereinbar ist. Denn dann wäre $\alpha\delta-\beta\gamma=\alpha'\delta'-\beta'\gamma'$, das heißt $e=e'$, und daher wegen $e=-e'$ auch $e=e'=0$. Damit würde auch $B'B'-A'C'$, also die Determinante der Form F', gleich $= 0$. Solche Formen haben wir vollständig ausgeschlossen.

$$m(2e+2a) = -2nb \quad \text{oder}$$

$$me + ma + nb = 0 \quad \ldots\ldots\ldots \quad [7]$$

Ebenso gilt

$$\begin{aligned} 2e - 2a &= e - e' - a + d \\ &= (\alpha+\alpha')(\delta-\delta') - (\beta+\beta')(\gamma-\gamma') \end{aligned}$$

$$2c = (\gamma-\gamma')(\delta+\delta') - (\gamma+\gamma')(\delta-\delta')$$

und daher $n(2e-2a) = -2mc$ oder

$$ne - na + mc = 0 \quad \ldots\ldots\ldots \quad [8]$$

Addiert man nun zu $mm(b\mu\mu - 2a\mu\nu - c\nu\nu)$ den Ausdruck

$$\begin{gathered} (1 - m\mu - n\nu)(m\nu(e-a) + (m\mu+1)b) \\ +(me+ma+nb)(m\mu\nu+\nu) + (ne-na+mc)m\nu\nu \end{gathered}$$

der offenbar $= 0$ ist, weil

$$1 - \mu m - \nu u = 0, \quad me + ma + nb = 0, \quad ne - na + mc = 0$$

gilt, so ergibt sich nach Ausmultiplizieren der Produkte und Weglassen der sich aufhebenden Glieder $2m\nu e + b$. Also gilt

$$mm(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2m\nu e + b \quad \ldots\ldots \quad [9]$$

Addiert man ebenso zu $mn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ die Ausdrücke

$$\begin{gathered} (1 - m\mu - n\nu)((n\nu - m\mu)e - (1 + m\mu + n\nu)a) \\ -(me+ma+nb)m\mu\mu + (ne-na+mc)n\nu\nu \end{gathered}$$

so erhält man

$$mn(b\mu\mu - 2a\mu\nu - c\nu\nu) = (n\nu - m\mu)e - a \quad \ldots\ldots [10]$$

Addiert man schließlich zu $nn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ die Ausdrücke

$$\begin{gathered} (m\mu + n\nu - 1)(n\mu(e+a) + (n\nu+1)c) \\ -(me+ma+nb)n\mu\mu - (ne-na+mc)(n\mu\nu+\mu) \end{gathered}$$

so ergibt sich

$$nn(b\mu\mu - 2a\mu\nu - c\nu\nu) = -2n\mu e - c \quad \ldots\ldots [11]$$

Aus 9, 10, 11 leitet man nun ab:

$$(Amm + 2Bmn + Cnn)(b\mu\mu - 2a\mu\nu - c\nu\nu)$$
$$= 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc$$

oder wegen [6],

$$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr. \quad \text{W. z. b. w.}$$

II. Um zu beweisen, dass die Form G die Form F' enthält, zeigen wir *erstens*, dass G in F' übergeht, wenn man

$$t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y',$$
$$u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y' \ \ldots \ (S)$$

setzt, und *zweitens*, dass $\frac{r}{e}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ ganze Zahlen sind.

1. Da F in G übergeht, wenn man

$$x = mt + \frac{\nu e}{r}u, \quad y = nt - \frac{\mu e}{r}u$$

setzt, wird die Form G durch die Substitution (S) in dieselbe Form überführt, in die F übergeht, wenn man

$$x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y')$$
$$+ \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

das heißt $= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y'$ oder $= \alpha x' + \beta y'$,
und

$$y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y')$$
$$- \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

das heißt $= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y'$ oder $= \gamma x' + \delta y'$ setzt.

Durch diese Substitution geht aber F in F' über. Also geht durch die Substitution (S) auch G in F' über.

2. Aus den Werten von e, b, d findet man $\alpha' e + \gamma b - \alpha d = 0$ oder wegen $d = -a$ die Gleichung $n\alpha' e + n\alpha a + n\gamma b = 0$. Daraus folgt nach [7] die Gleichung $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$ oder

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e \quad \ldots\ldots\ldots [12]$$

Ferner gilt $\alpha nb = -\alpha m(e + a)$, $\gamma mb = -m(\alpha' e + \alpha a)$, und daher

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me \quad \ldots\ldots\ldots [13]$$

Schließlich gilt $\gamma' e - \gamma a + \alpha c = 0$. Multipliziert man mit n und setzt für na seinen Wert aus [8] ein, so folgt

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne \quad \ldots\ldots\ldots [14]$$

Ebenso ergibt sich $\beta' e + \delta b - \beta d = 0$ oder $n\beta' e + n\delta b + n\beta a = 0$ und damit nach [7], die Gleichung $n\beta' e + n\beta a = m\delta e + m\delta a$ oder

$$(n\beta - m\delta)a = (m\delta - n\beta')e \quad \ldots\ldots\ldots [15]$$

Ferner gilt $\beta nb = -\beta m(e + a)$, $\delta mb = -m(\beta' e + \beta a)$, und daher

$$(n\beta - m\delta)b = (\beta' - \beta)me \quad \ldots\ldots\ldots [16]$$

Schließlich gilt $\delta e - \delta a + \beta c = 0$. Multipliziert man mit n und setzt für na seinen Wert aus [8] ein, so erhält man

$$(n\beta - m\delta)c = (\delta - \delta')ne \quad \ldots\ldots\ldots [17]$$

Da nun der größte gemeinsame Teiler der Zahlen a, b, c gleich r ist, lassen sich ganze Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ so wählen, dass

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

gilt. Damit folgt aus 12, 13, 14 und 15, 16, 17

$$\begin{aligned} &\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n \\ &\qquad = \frac{r}{e}(n\alpha - m\gamma) \\ &\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n \\ &\qquad = \frac{r}{e}(n\beta - m\delta) \end{aligned}$$

also sind $\frac{r}{e}(n\alpha - n\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ ganze Zahlen. W. z. b. w.

165.

Beispiel. Die Form $3xx + 14xy - 4yy$ wird in die Form $-12x'x' - 18x'y' + 39y'y'$ überführt, sowohl eigentlich durch die Substitution

$$x = 4x' + 11y', \quad y = -x' - 2y'$$

als auch uneigentlich durch die Substitution

$$x = -74x' + 89y', \quad y = 15x' - 18y'$$

Hier sind also $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ der Reihe nach -70, 100, 14, -20, und es gilt $-70 : 14 = 100 : -20 = 5 : -1$. Wir setzen daher $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Die Zahlen a, b, c ergeben sich als -237, -1170, 48, mit dem größten gemeinsamen Teiler $= 3 = r$. Schließlich gilt $e = 3$. Damit lautet die Transformation (S): $x = 5t - u$, $y = -t$. Durch sie geht die Form $(3, 7, -4)$ in die ambige Form $tt - 16tu + 3uu$ über.

Sind die Formen F, F' äquivalent, so ist die Form G, die in F enthalten ist, auch in F' enthalten. Da sie aber dieselbe Form auch enthält, ist sie ihr und damit auch der Form F äquivalent. In diesem Fall lässt sich der Satz also so aussprechen:

Sind F, F' sowohl eigentlich als auch uneigentlich äquivalent, so lässt sich eine beiden äquivalente ambige Form finden. — In diesem Fall ist $e = \pm 1$, und daher ist auch r., das e teilt, gleich $= 1$.

Dies möge über die Transformation der Formen im Allgemeinen genügen. Wir gehen nun zur Betrachtung der *Darstellungen* über.

Allgemeines über Darstellungen von Zahlen durch Formen und ihren Zusammenhang mit Transformationen.

166.

Enthält die Form F die Form F', so lässt sich jede durch F' darstellbare Zahl auch durch F darstellen.

Die Unbestimmten der Formen F, F' seien der Reihe nach $x, y; x', y'$. Nehmen wir an, die Zahl M werde durch F' dargestellt, wenn man $x' = m$, $y' = n$ setzt, und die Form F gehe in F' durch die Substitution

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

über. Dann nimmt offenbar bei der Wahl

$$x = \alpha m + \beta n, \quad y = \gamma m + \delta n$$

die Form F den Wert M an.

Lässt sich M auf mehrere Arten durch die Form F' darstellen, zum Beispiel auch durch die Wahl $x' = m'$, $y' = n'$, so folgen daraus mehrere Darstellungen von M durch F. Gälte nämlich zugleich

$$\alpha m + \beta n = \alpha m' + \beta n' \quad \text{und} \quad \gamma m + \delta n = \gamma m' + \delta n'$$

so wäre entweder $\alpha\delta - \beta\gamma = 0$, also gegen die Voraussetzung auch die Determinante der Form $F = 0$, oder es wäre $m = m'$, $n = n'$. Daraus folgt, dass M sich durch F auf mindestens ebenso viele verschiedene Arten darstellen lässt wie durch F'.

Enthält also sowohl F die Form F' als auch F' die Form F, sind also *mit anderen Worten* F, F' äquivalent, und lässt sich die Zahl M durch eine von beiden darstellen, so lässt sie sich auch durch die andere darstellen, und zwar durch die eine auf ebenso viele verschiedene Arten wie durch die andere.

Schließlich bemerken wir, dass in diesem Fall der größte gemeinsame Teiler der Zahlen m, n gleich dem größten gemeinsamen Teiler von $\alpha m + \beta n$, $\gamma m + \delta n$ ist. Der erste sei $= \Delta$, und die Zahlen μ, ν seien so gewählt, dass $\mu m + \nu n = \Delta$ gilt. Dann ist

$$\begin{aligned}(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n)\\ = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta\end{aligned}$$

Also teilt der größte gemeinsame Teiler von $\alpha m + \beta n$, $\gamma m + \delta n$ die Zahl Δ. Umgekehrt teilt Δ auch diesen Teiler, weil es offenbar $\alpha m + \beta n$, $\gamma m + \delta n$ teilt. Der größte gemeinsame Teiler ist daher notwendig $= \Delta$. — Sind also m, n teilerfremd, so sind auch $\alpha m + \beta n$. $\gamma m + \delta n$ teilerfremd.

167.

Satz. *Die Formen*

$$axx + 2bxy + cyy \quad \ldots\ldots (F)$$

$$a'x'x' + 2b'x'y' + c'y'y' \quad \ldots\ldots (F')$$

seien äquivalent, ihre Determinante = D, und die zweite gehe in die erste über, wenn man

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y$$

setzt. Ferner werde die Zahl M durch F dargestellt, wenn man x = m, y = n setzt, und daher durch F′, wenn man

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n'$$

setzt, und zwar so, dass m zu n und damit auch m′ zu n′ teilerfremd ist. Dann gehören beide Darstellungen entweder zu demselben Wert oder zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, je nachdem, ob die Transformation der Form F′ in F eigentlich oder uneigentlich ist.

Beweis. Man bestimme die Zahlen μ, ν so, dass $\mu m + \nu n = 1$ gilt, und setze

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

Diese Zahlen sind wegen $\alpha\delta - \gamma\beta = \pm 1$ ganzzahlig. Dann gilt

$$\mu' m' + \nu' n' = 1. \quad \text{(Siehe das Ende des vorigen Artikels.)}$$

Ferner sei

$$\mu(bm + cn) - \nu(am + bn) = V,$$
$$\mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$$

Dann sind V, V' die Werte des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, zu denen die erste und die zweite Darstellung gehören. Setzt man in V' für μ', ν', m', n' ihre Werte und in V

$$\begin{array}{lll} \text{für} & a, & a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma \\ \text{für} & b, & a'a\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta \\ \text{für} & c, & a'\beta\beta + 2b'\beta\delta + c'\delta\delta \end{array}$$

ein, so erhält man nach Ausmultiplizieren $V = V'(\alpha\delta - \beta\gamma)$.

Also gilt entweder $V = V'$ oder $V = -V'$, je nachdem, ob $\alpha\delta - \beta\gamma = +1$ oder $= -1$ ist. *Das heißt*, die Darstellungen gehören zu demselben Wert oder zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, je nachdem, ob die Transformation der Form F' in F eigentlich oder uneigentlich ist. W. z. b. w.

Hat man also mehrere Darstellungen der Zahl M durch die Form (a, b, c) mit teilerfremden Werten der Unbestimmten x, y, die zu *verschiedenen* Werten des Ausdrucks

$\sqrt{D}(\mathrm{mod.}\, M)$ gehören, so gehören die entsprechenden Darstellungen durch die Form (a', b', c') jeweils zu denselben Werten. Gibt es keine Darstellung der Zahl M durch eine Form, die zu einem bestimmten Wert gehört, so gibt es auch keine Darstellung zu diesem Wert durch eine dazu äquivalente Form.

168.

Satz. *Wird die Zahl M durch die Form $axx+2bxy+cyy$ dargestellt, indem man x, y die teilerfremden Werte m, n zuweist, und ist der Wert des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, zu dem diese Darstellung gehört, gleich N, so sind die Formen (a, b, c), $(M, N, \frac{NN-D}{M})$ eigentlich äquivalent.*

Beweis. Aus Artikel 155 folgt, dass sich ganze Zahlen μ, ν finden lassen, sodass

$$m\mu + n\nu = 1, \quad \mu(bm + cn) - \nu(am + bn) = N$$

gilt. Damit geht die Form (a, b, c) durch die Substitution $x = mx' - \nu y'$, $y = nx' + \mu y'$, die offenbar eigentlich ist, in eine Form mit der Determinante $= D(m\mu + n\nu)^2$, *das heißt* $= D$, also in eine äquivalente Form über. Schreiben wir diese Form $= (M', N', \frac{N'N'-D}{M'})$, so gilt

$$M' = amm + 2bmn + cnn = M,$$
$$N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N$$

Die Form, in die (a, b, c) durch jene Transformation übergeht, ist also $(M, N, \frac{NN-D}{M})$. W. z. b. w.

Aus den Gleichungen

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

folgt außerdem

$$\mu = \frac{nN + ma + nb}{amm + 2bmn + cnn} = \frac{nN + ma + nb}{M},$$
$$\nu = \frac{mb + nc - mN}{M}$$

Diese Zahlen sind daher ganzzahlig.

Ferner ist zu beachten, dass die Aussage nicht gilt, wenn $M = 0$ ist. Dann wird nämlich der Term $\frac{NN-D}{M}$ unbestimmt[*)].

169.

Gibt es mehrere Darstellungen der Zahl M durch (a, b, c), die zu demselben Wert des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, N gehören, wobei wir die Werte von x, y stets als teilerfremd voraussetzen, so lassen sich daraus auch mehrere eigentliche Transformationen der Form $(a, b, c)..(F)$ in $(M.\ N, \frac{NN-D}{M})..(G)$ ableiten. Entsteht nämlich auch aus den Werten $x = m'$, $y = n'$ eine solche Darstellung, so geht (F) auch durch die Substitution

[*)] Wollen wir unsere Ausdrucksweise auch auf diesen Fall ausdehnen, so bedeutet die Aussage, N sei ein Wert des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$ oder es gelte $NN \equiv D(\mathrm{mod.}\, M)$, dass $NN - D$ ein Vielfaches von M und daher $= 0$ ist.

$$x = m'x' + \frac{m'N - m'b - n'c}{M}y',$$
$$y = n'x' + \frac{n'N + m'a + n'b}{M}y'$$

in (G) über. Umgekehrt ergibt jede eigentliche Transformation der Form (F) in (G) eine Darstellung der Zahl M durch die Form (F), die zum Wert N gehört. Geht nämlich (F) in (G) über, indem man $x = mx' - \nu y'$, $y = nx' + \mu y'$ setzt, so wird M durch (F) dargestellt, wenn man $x = m$, $y = n$ setzt. Da hier $m\mu + n\nu = 1$ gilt, ist der Wert des Ausdrucks $\sqrt{D} (\mathrm{mod.}\, M)$, zu dem die Darstellung gehört, gleich $\mu(bm+cn) - \nu(am+bn)$, *das heißt* N. Aus mehreren verschiedenen eigentlichen Transformationen folgen ebenso viele verschiedene Darstellungen, die zu N gehören[*)]. — Kennt man alle eigentlichen Transformationen der Form (F) in (G), so ergeben sich daraus also leicht alle Darstellungen von M durch (F), die zum Wert N gehören. Damit ist die Aufgabe, die Darstellungen einer gegebenen Zahl durch eine gegebene Form zu finden, bei denen die Unbestimmten teilerfremde Werte erhalten, auf die Aufgabe zurückgeführt, alle eigentlichen Transformationen jener Form in eine gegebene äquivalente Form zu finden.

Wenden wir nun das in Artikel 162 Gezeigte darauf an, so folgt leicht: Ist eine Darstellung der Zahl M durch die Form (F), die zum Wert N gehört, durch $x = \alpha$, $y = \gamma$ gegeben, so lautet die allgemeine Formel, die alle Darstellungen derselben Zahl durch die Form (F), die zum Wert N gehören, umfasst:

$$x = \frac{\alpha t - (\alpha b + \gamma c)u}{m}, \quad y = \frac{\gamma t + (\alpha a + \gamma b)u}{m}$$

Dabei ist m der größte gemeinsame Teiler der Zahlen $a, 2b, c$, und t, u durchlaufen alle Zahlen, die der Gleichung $tt - Duu = mm$ genügen.

[*)] Nimmt man an, dass zwei verschiedene eigentliche Transformationen dieselbe Darstellung liefern, so müssen sie folgende Gestalt haben:

1) $x = mx' - \nu y', \quad y = nx' + \mu y';$
2) $x = mx' - \nu' y', \quad y = nx' + \mu' x'.$

Aus den beiden Gleichungen

$$m\mu + n\nu = m\mu' + n\nu',$$
$$\mu(mb + nc) - \nu(ma + nb) = \mu'(mb + nc) - \nu'(ma + nb),$$

folgt aber leicht, dass entweder $M = 0$ oder $\mu = \mu'$, $\nu = \nu'$ gilt. Den Fall $M = 0$ haben wir bereits ausgeschlossen.

170.

Ist die Form (a, b, c) einer ambigen Form äquivalent und damit der Form $(M, N, \frac{NN-D}{M})$ sowohl eigentlich als auch uneigentlich oder sowohl der Form $(M, N, \frac{NN-D}{M})$ als auch der Form $(M, -N, \frac{NN-D}{M})$ eigentlich äquivalent, so gibt es Darstellungen der Zahl M durch die Form (F), die sowohl zum Wert N als auch zum Wert $-N$ gehören. Gibt es umgekehrt mehrere Darstellungen der Zahl M durch dieselbe Form (F), die zu *entgegengesetzten* Werten des Ausdrucks $\sqrt{D}(\mathrm{mod.}\, M)$, $N, -N$ gehören, so ist die Form (F) der Form (G) sowohl eigentlich als auch uneigentlich äquivalent, und es lässt sich eine ambige Form angeben, der (F) äquivalent ist.

Dies möge hier an allgemeinen Ergebnissen über Darstellungen genügen. Über Darstellungen, bei denen die Unbestimmten keine teilerfremden Werte haben, werden wir weiter unten sprechen. Hinsichtlich der anderen Eigenschaften müssen Formen mit negativer Determinante ganz anders behandelt werden als Formen mit positiver Determinante. Wir werden deshalb nun beide Arten getrennt betrachten und mit den ersten als den leichteren beginnen.

Formen mit negativer Determinante.

171.

Aufgabe. *Zu einer beliebigen Form (a, b, a') mit negativer Determinante $= -D$, wobei D eine positive Zahl bezeichnet, eine eigentlich äquivalente Form (A, B, C) finden, in der A weder größer als $\sqrt{\frac{4}{3}}D$, C noch kleiner als $2B$ ist.*

Lösung. Wir nehmen an, dass die gegebene Form nicht alle drei Bedingungen zugleich erfüllt; sonst müsste man keine andere Form suchen. Sei b' der absolut kleinste Rest der Zahl $-b$ modulo a'[*)], und sei $a'' = \frac{b'b'+D}{a'}$. Dies ist eine ganze Zahl, weil $b'b' \equiv bb$, $b'b' + D \equiv bb + D \equiv aa' \equiv 0 (\mathrm{mod.}\, a')$. Ist nun $a'' < a'$, so sei wieder b'' der absolut kleinste Rest von $-b'$ modulo a'' und $a''' = \frac{b''b''+D}{a''}$. Ist auch hier $a''' < a''$, so sei erneut b''' der absolut kleinste Rest von $-b''$ modulo a''' und $a'''' = \frac{b'''b'''+D}{a'''}$. Man setzt dies fort, bis man in der Folge a', a'', a''', a'''' usw. einen Term a^{m+1} erreicht, der nicht kleiner als sein Vorgänger a^m ist. Das muss schließlich eintreten, da man sonst eine unendliche Folge ganzer Zahlen hätte, die immer weiter abnehmen. Dann erfüllt die Form (a^m, b^m, a^{m+1}) alle Bedingungen.

Beweis. I. In der Folge der Formen (a, b, a'), (a', b', a''), (a'', b'', a''') usw. ist jede ihrer Vorgängerin benachbart; die letzte ist also der ersten eigentlich äquivalent (Artikel 159, 160). II. Da b^m der absolut kleinste Rest von $-b^{m-1}$ modulo a^m ist, ist er nicht größer als $\frac{1}{2}a^m$ (Artikel 4).

III. Da $a^m a^{m+1} = D + b^m b^m$ und a^{m+1} nicht $< a^m$ ist, ist $a^m a^m$ nicht $> D + b^m b^m$. Da b^m nicht $> \frac{1}{2}a^m$ ist, ist $a^m a^m$ nicht $> D + \frac{1}{4}a^m a^m$ und $\frac{3}{4}a^m a^m$ nicht $> D$; schließlich ist a^m *nicht* $> \sqrt{\frac{4}{3}}D$.

Beispiel. Die gegebene Form sei $(304, 217, 155)$, ihre Determinante $= -31$. Hier ergibt sich die Folge der Formen:

$$(304, 217, 155),\ (155, -62, 25),\ (25, 12, 7),\ (7, 2, 5),\ (5, -2, 7).$$

Die letzte ist die gesuchte. — Ebenso findet man zur Form $(121, 49, 20)$ mit Determinante $= -19$ die äquivalenten Formen $(20, -9, 5)$, $(5, -1, 4)$, $(4, 1, 5)$; somit ist $(4, 1, 5)$ die gesuchte Form.

Solche Formen (A, B, C) mit negativer Determinante, bei denen A weder größer als $\sqrt{\frac{4}{3}}D, C$ noch kleiner als $2B$ ist, nennen wir *reduzierte Formen*. Zu jeder Form mit negativer Determinante lässt sich also eine eigentlich äquivalente reduzierte Form finden.

[*)] Man beachte: Ist bei einer Form (a, b, a') der erste oder letzte Term a oder $a' = 0$, so ist ihre Determinante ein positives Quadrat. Das kann also im vorliegenden Fall nicht eintreten. — Aus einem ähnlichen Grund können die äußeren Terme a, a' einer Form mit negativer Determinante keine entgegengesetzten Vorzeichen haben.

172.

Aufgabe. *Die Bedingungen finden, unter denen zwei nicht identische reduzierte Formen mit derselben Determinante $-D$, (a,b,c), (a',b',c'), eigentlich äquivalent sein können.*

Lösung. Wir dürfen annehmen, dass a' nicht $> a$ ist und die Form $axx+2bxy+cyy$ in $a'x'x' + 2b'x'y' + c'y'y'$ übergeht, und zwar durch die eigentliche Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Dann gelten die Gleichungen

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a' \qquad \ldots\ldots\ldots \quad [1]$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b' \qquad \ldots\ldots\ldots \quad [2]$$
$$\alpha\delta - \beta\gamma = 1 \qquad \ldots\ldots\ldots\ldots \quad [3]$$

Aus [1] folgt $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$; somit ist aa' positiv. Da $ac = D + bb$, $a'c' = D+b'b'$, sind auch ac, $a'c'$ positiv; also haben a, a', c, c' alle dasselbe Vorzeichen. Aber sowohl a als auch a' sind nicht $> \sqrt{\frac{4}{3}D}$, also ist aa' nicht $> \sqrt{\frac{4}{3}D}$. Umso weniger kann daher $D\gamma\gamma$ $(= aa' - (a\alpha + b\gamma)^2)$ größer als $\frac{4}{3}D$ sein. Somit ist γ entweder $= 0$ oder $= \pm 1$.

I. Ist $\gamma = 0$, so folgt aus [3] entweder $\alpha = 1.\ \delta = 1$ oder $\alpha = -1$, $\delta = -1$. In beiden Fällen ergibt sich aus [1] $a' = a$ und aus [2] $b' - b = \pm\beta a$. Aber b ist nicht $> \frac{1}{2}a$, und b' ist nicht $> \frac{1}{2}a'$, also auch nicht $> \frac{1}{2}a$. Daher kann die Gleichung $b' - b = \pm\beta a$ nur bestehen, wenn

entweder $b = b'$ gilt; daraus würde $c' = \frac{b'b'+D}{a'} = \frac{bb+D}{a} = c$ folgen, und die Formen (a,b,c), (a',b',c') wären entgegen der Voraussetzung identisch;

oder $b = -b' = \pm\frac{1}{2}a$ gilt. Auch in diesem Fall ist $c' = c$, und die Form (a',b',c') ist $(a,-b,c)$, *das heißt* die zur Form (a,b,c) entgegengesetzte. Zugleich ist klar, dass diese Formen wegen $2b = \pm a$ ambig sind.

II. Ist $\gamma = \pm 1$, so ergibt sich aus [1] $a\alpha\alpha + c - a' = \pm 2b\alpha$. Aber c ist nicht kleiner als a, also auch nicht kleiner als a'. Daher ist $a\alpha\alpha+c-a'$ oder $2b\alpha$ sicher nicht kleiner als $a\alpha\alpha$. Da $2b$ nicht größer als a ist, ist α nicht kleiner als $\alpha\alpha$; somit gilt notwendig entweder $\alpha = 0$ oder $= \pm 1$.

1) Ist $\alpha = 0$, so folgt aus [1] $a' = c$. Da a weder größer als c noch kleiner als a' ist, gilt notwendig $a' = a = c$. Weiter ergibt sich aus [3] $\beta\gamma = -1$ und damit aus [2] $b + b' = \pm\delta c = \pm\delta a$. Hieraus folgt wie in (I), dass

entweder $b = b'$ gilt; dann wären die Formen (a,b,c), (a',b',c') entgegen der Voraussetzung identisch;

oder $b = -b'$ gilt; dann sind die Formen (a,b,c), (a',b',c') entgegengesetzt.

2) Ist $\alpha = \pm 1$, so folgt aus [1] $\pm 2b = a + c - a'$. Da nun a nicht kleiner ist und auch $c < a'$ nicht gilt, ist $2b$ nicht $< a$ und nicht $< c$. Aber $2b$ ist auch nicht $> a$ und nicht $> c$. Daher gilt notwendig $\pm 2b = a = c$ und somit nach der Gleichung $\pm 2b = a + c - a'$ auch $= a'$. Aus [2] ergibt sich also

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

oder wegen $\alpha\delta - \beta\gamma = 1$

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma)$$

also notwendig, wie zuvor,

entweder $b = b'$, sodass die Formen (a, b, c), (a', b', c') entgegen der Voraussetzung identisch wären;

oder $b = -b'$, sodass jene Formen entgegengesetzt sind. Zugleich sind die Formen in diesem Fall wegen $a = \pm 2b$ ambig.

Aus allem zusammen folgt, dass die Formen (a, b, c), (a', b', c') nur dann eigentlich äquivalent sein können, wenn sie entgegengesetzt und zugleich *entweder* ambig sind *oder* $a = c = a' = c'$ gilt. Dass die Formen (a, b, c), (a', b', c') in diesen Fällen eigentlich äquivalent sind, hätte man auch leicht im Voraus sehen können. Denn entgegengesetzte Formen müssen uneigentlich und, wenn sie außerdem ambig sind, auch eigentlich äquivalent sein. Ist dagegen $a = c$, so ist die Form $(\frac{D+(a-b)^2}{a}, a - b, a)$ der Form (a, b, c) benachbart und damit äquivalent. Wegen $D + bb = ac = aa$ gilt aber $\frac{D+(a-b)^2}{a} = 2a - 2b$, und die Form $(2a - 2b, a - b, a)$ ist ambig. Also ist (a, b, c) auch ihrer entgegengesetzten Form eigentlich äquivalent.

Ebenso leicht lässt sich nun entscheiden, wann zwei reduzierte Formen (a, b, c), (a', b', c'), die nicht entgegengesetzt sind, uneigentlich äquivalent sein können. Sie sind nämlich uneigentlich äquivalent, wenn (a, b, c), $(a', -b', c')$, die nicht identisch sind, eigentlich äquivalent sind, und umgekehrt. Damit ist die Bedingung, unter der *jene* uneigentlich äquivalent sind, dass sie identisch und außerdem entweder ambig sind oder $a = c$ gilt. — Reduzierte Formen, die weder identisch noch entgegengesetzt sind, können weder eigentlich noch uneigentlich äquivalent sein.

173.

Aufgabe. *Für zwei gegebene Formen F und F' mit derselben negativen Determinante feststellen, ob sie äquivalent sind.*

Lösung. Man sucht zwei reduzierte Formen f, f', die den Formen F, F' jeweils eigentlich äquivalent sind. Sind die Formen f, f' eigentlich, uneigentlich oder auf beide Arten äquivalent, so gilt das auch für F, F'. Sind dagegen f, f' auf keine Art äquivalent, so auch F, F' nicht.

Nach dem vorigen Artikel gibt es vier mögliche Fälle:

1) Sind f, f' weder identisch noch entgegengesetzt, so sind F, F' auf keine Art äquivalent.

2) Sind f, f' *erstens* entweder identisch oder entgegengesetzt und *zweitens* entweder ambig oder haben gleiche äußere Terme, so sind F, F' sowohl eigentlich als auch uneigentlich äquivalent.

3) Sind f, f' identisch, aber weder ambig noch mit gleichen äußeren Termen, so sind F, F' nur eigentlich äquivalent.

4) Sind f, f' entgegengesetzt, aber weder ambig noch mit gleichen äußeren Termen, so sind F, F' nur uneigentlich äquivalent.

Beispiel. Zu den Formen $(41, 35, 30)$, $(7, 18, 47)$ mit Determinante $= -5$ findet man die äquivalenten reduzierten Formen $(1, 0, 5)$, $(2, 1, 3)$; also sind jene auf keine Art äquivalent. — Zu den Formen $(23, 38, 63)$, $(15, 20, 27)$ ist dagegen dieselbe reduzierte Form $(2, 1, 3)$ äquivalent. Da diese zugleich ambig ist, sind die Formen $(23, 38, 63)$, $(15, 20, 27)$ sowohl eigentlich als auch uneigentlich äquivalent. — Zu den Formen $(37, 53, 78)$, $(53, 73, 102)$ sind die reduzierten Formen $(9, 2, 9)$, $(9, -2, 9)$ äquivalent.

Da diese entgegengesetzt sind und ihre äußeren Terme gleich sind, sind die gegebenen Formen sowohl eigentlich als auch uneigentlich äquivalent.

174.

Die Anzahl aller reduzierten Formen mit einer gegebenen Determinante $-D$ ist immer endlich und im Verhältnis zur Zahl D recht klein. Die Formen selbst lassen sich auf zwei Arten finden. Wir bezeichnen die reduzierten Formen der Determinante $-D$ allgemein mit (a, b, c); es sind also alle Werte von a, b, c zu bestimmen.

Erste Methode. Für a nimmt man alle positiven und negativen Zahlen, die nicht größer als $\sqrt{\frac{4}{3}D}$ sind und für die $-D$ ein quadratischer Rest ist. Für jedes a setzt man b der Reihe nach gleich allen Werten des Ausdrucks $\sqrt{-D}$ (mod. a), die nicht größer als $\frac{1}{2}a$ sind, jeweils positiv und negativ genommen. Für c setzt man bei jedem bestimmten Wertepaar von a, b den Wert $= \frac{D+bb}{a}$. Entstehen dabei Formen, in denen $c < a$ gilt, so verwirft man sie; die übrigen sind offenbar reduziert.

Zweite Methode. Für b nimmt man alle positiven und negativen Zahlen, die nicht größer als $\frac{1}{2}\sqrt{\frac{4}{3}D}$ oder $\sqrt{\frac{1}{3}D}$ sind. Für jedes b zerlegt man $bb + D$ auf alle möglichen Arten in zwei Faktoren (auch unter Berücksichtigung verschiedener Vorzeichen), die beide nicht kleiner als $2b$ sind. Den einen Faktor, und zwar bei ungleichen Faktoren den kleineren, setzt man $= a$, den anderen $= c$. Da a nicht $> \sqrt{\frac{4}{3}D}$ ist, sind alle so entstehenden Formen offenbar reduziert. — Schließlich ist klar, dass jede reduzierte Form mit jeder der beiden Methoden gefunden wird.

Beispiel. Sei $D = 85$. Die Grenze für die Werte von a ist hier $\sqrt{\frac{340}{3}}$, die zwischen 10 und 11 liegt. Die Zahlen zwischen 1 und 10 (einschließlich), für die -85 ein Rest ist, sind $1, 2, 5, 10$. Daraus ergeben sich zwölf Formen:

$$(1, 0, 85),\ (2, 1, 43),\ (2, -1, 43),\ (5, 0, 17),$$
$$(10, 5, 11),\ (10. -5, 11);\ (-1, 0, -85),\ (-2, 1, -43),$$
$$(-2, -1, -43).\ (-5, 0, -17),\ (-10, 5, -11,\ (-10, -5, -11).$$

Bei der anderen Methode ergibt sich als Grenze der Werte von b die Zahl $\sqrt{\frac{85}{3}}$, die zwischen 5 und 6 liegt. Für $b = 0$ entstehen die Formen

$$(1, 0, 85),\ (-1, 0, -85),\ (5, 0, 17),\ (-5, 0, -17),$$

und für $b = \pm 1$ diese: $(2, \pm 1, 43)$, $(-2, \pm 1, -43)$.

Für $b = \pm 2$ gibt es keine, da sich 89 nicht in zwei Faktoren zerlegen lässt, die beide nicht < 4 sind. Dasselbe gilt für ± 3, ± 4. Schließlich ergeben sich für $b = \pm 5$

$$(10, \pm 5, 11),\ (-10, \pm 5. -11).$$

175.

Verwirft man aus allen reduzierten Formen einer gegebenen Determinante von je zwei Formen, die zwar nicht identisch, aber eigentlich äquivalent sind, eine der beiden, so haben die verbleibenden Formen folgende bemerkenswerte Eigenschaft: Jede Form mit derselben Determinante ist einer von ihnen eigentlich äquivalent, und zwar nur einer einzigen (sonst wären einige von ihnen eigentlich äquivalent). Also *lassen sich alle Formen mit derselben Determinante in ebenso viele Klassen einteilen, wie Formen übrig bleiben*, indem man die Formen, die derselben reduzierten Form eigentlich äquivalent sind, derselben Klasse zuordnet. So bleiben für $D = 85$ die Formen

$$(1,0,85),\ (2,1,43),\ (5,0,17),\ (10,5,11),$$
$$(-1,0.\ -84),\ (-2,1,-43).\ (-5,0,-17),\ (-10,5,-11)$$

übrig. Alle Formen mit Determinante -85 lassen sich also in acht Klassen einteilen, je nachdem, ob sie der ersten, der zweiten usw. Form eigentlich äquivalent sind. Offenbar sind Formen derselben Klasse eigentlich äquivalent, während Formen aus verschiedenen Klassen nicht eigentlich äquivalent sein können. Die Klassifikation der Formen werden wir weiter unten viel ausführlicher behandeln. Hier fügen wir nur eine Beobachtung hinzu. Wir haben oben schon gezeigt: Ist die Determinante der Form (a,b,c) negativ $= -D$, so haben a und c dasselbe Vorzeichen (denn es gilt $ac = bb + D$, und dieser Wert ist positiv). Ebenso erkennt man leicht, dass bei äquivalenten Formen (a,b,c), (a',b',c') alle a,c,a',c' dasselbe Vorzeichen haben. Geht nämlich die erste durch die Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ in die zweite über, so gilt $a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a'$ und daher $aa' = (a\alpha + b\beta)^2 + D\gamma\gamma$, was sicher nicht negativ ist. Da aber a nicht null sein kann und $a' = 0$ ausgeschlossen ist, ist aa' positiv, und damit haben a, a' dasselbe Vorzeichen.

Damit ist klar, dass die Formen mit positiven äußeren Termen von denen mit negativen äußeren Termen vollständig getrennt sind. Es reicht aus, von den reduzierten Formen nur die mit positiven äußeren Termen zu betrachten, denn die übrigen sind gleich zahlreich und entstehen aus ihnen, indem man den äußeren Termen die entgegengesetzten Vorzeichen gibt. Dasselbe gilt für die Formen, die aus den reduzierten Formen zu verwerfen oder beizubehalten sind.

176.

Hier steht nun für einige negative Determinanten eine Tabelle von Formen, nach denen sich alle übrigen Formen mit derselben Determinante in Klassen einteilen lassen. Nach der Bemerkung im vorigen Artikel geben wir nur die Hälfte an, nämlich die Formen mit positiven äußeren Termen.

D	
1	$(1,0,1)$.
2	$(1,0,2)$.
3	$(1,0,3),\ (2,1,2)$.
4	$(1,0,4),\ (2,0,2)$.
5	$(1,0,5),\ (2,1,3)$.
6	$(1,0,6),\ (2,0,3)$.
7	$(1,0,7),\ (2,1,4)$.
8	$(1,0,8),\ (2,0,4),\ (3,1,3)$.
9	$(1,0,9),\ (2,1,5),\ (3.0,3)$.
10	$(1,0,10),\ (2,0,5)$.
11	$(1,0,11),\ (2,1,6),\ (3,1,4),\ (3,-1,4)$.
12	$(1,0,12),\ (2,0,6),\ (3,0,4),\ (4,2,4)$.

Es wäre unnötig, diese Tabelle hier weiter fortzusetzen, da wir weiter unten zeigen werden, wie sie sich viel zweckmäßiger anordnen lässt.

Also ist jede Form mit Determinante -1 der Form $xx+yy$ eigentlich äquivalent, wenn ihre äußeren Terme positiv sind, oder der Form $-xx-yy$, wenn sie negativ sind; jede Form mit Determinante -2 und positiven äußeren Termen der Form $xx+2yy$ usw.; jede Form mit Determinante -11 und positiven äußeren Termen einer der Formen $xx+11yy$, $2xx+2xy+6yy$, $3xx+2xy+4yy$, $3xx-2xy+4yy$ usw.

177.

Aufgabe. *Gegeben ist eine Folge von Formen, in der jede ihrer Vorgängerin nach rechts benachbart ist. Gesucht ist eine eigentliche Transformation der ersten Form in eine beliebige Form der Folge.*

Lösung. Die Formen seien $(a, b, a') = F$; $(a', b', a'') = F'$; $(a'', b'', a''') = F''$; $(a''', b''', a'''') = F'''$ usw. Wir bezeichnen $\frac{b+b'}{a'}$, $\frac{b'+b''}{a''}$, $\frac{b''+b'''}{a'''}$ usw. jeweils mit h', h'', h''' usw. Die Unbestimmten der Formen F, F', F'' usw. seien x, y; x', y'; x'', y'' usw. Wir nehmen an, dass F übergeht

$$\begin{array}{lll} \text{in } F' \text{ bei} & x = \alpha' x' + \beta' y', & y = \gamma' x' + \delta' y' \\ F'' \quad \ldots & x = \alpha'' x'' + \beta'' y'', & y = \gamma'' x'' + \delta'' y'' \\ F''' \quad \ldots & x = \alpha''' x''' + \beta''' y''', & y = \gamma''' x''' + \delta''' y''' \\ & \text{usw.} & \end{array}$$

Da nun F in F' übergeht bei $x = -y', \quad y = x' + h'y'$
F' in F'' bei $x' = -y'', \quad y' = x'' + h''y''$
F'' in F''' bei $x'' = -y''', \quad y'' = x''' + h'''y'''$ usw. (Artikel 160)

so ergibt sich leicht folgender Algorithmus (Artikel 159):

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' - \alpha' & \gamma'' = \delta' & \delta'' = h''\delta' - \gamma' \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \alpha'' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \gamma'' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \alpha''' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \gamma''' \\ & \text{usw.} & & \end{array}$$

oder

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta' & \delta'' = h''\delta' - 1 \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' \\ & \text{usw.} & & \end{array}$$

Dass alle diese Transformationen eigentlich sind, folgt ohne Mühe sowohl aus ihrer Konstruktion als auch aus Artikel 159.

Dieser sehr einfache und für die Rechnung praktische Algorithmus ist dem in Artikel 27 beschriebenen Algorithmus analog und lässt sich auch auf ihn zurückführen*). Diese Lösung ist nicht auf Formen mit negativer Determinante beschränkt, sondern gilt in allen Fällen, sofern keine der Zahlen a', a'', a''' usw. $= 0$ ist.

*)In der Bezeichnung von Artikel 27 gilt nämlich $\beta^n = \pm[-h'', h''', -h'''' \ldots \pm h^n]$, wobei für die jeweils zur Wahl stehenden Vorzeichen $--; -+; +-; ++$ zu nehmen sind, je nachdem, ob n die Form $4k+0; 1; 2; 3$ hat, und

$$\delta^n = \pm[h', -h'', h''' \ldots . \pm h^n]$$

wobei die zur Wahl stehenden Vorzeichen $+-; ++; --; -+$ sein müssen, je nachdem, ob n die Form $4k+0; 1; 2; 3$ hat. Um uns kurz zu halten, können wir dies hier nicht ausführlicher entwickeln; jeder kann es aber leicht selbst nachprüfen.

178.

Aufgabe. *Zu zwei gegebenen, eigentlich äquivalenten Formen F, f mit derselben negativen Determinante eine eigentliche Transformation der einen in die andere finden.*

Lösung. Wir nehmen an, dass die Form F gleich (A, B, A') ist und man mit der Methode von Artikel 171 die Folge der Formen (A', B', A''), (A'', B'', A''') usw. bis zu (A^m, B^m, A^{m+1}) gefunden hat, wobei die letzte Form reduziert ist. Ebenso sei f gleich (a, b, a'), und mit derselben Methode sei die Folge (a', b', a''), (a'', b'', a''') bis zu (a^n, b^n, a^{n+1}) gefunden worden, wobei die letzte Form reduziert ist. Dann sind zwei Fälle möglich.

I. Die Formen (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) sind entweder identisch oder entgegengesetzt und zugleich ambig. Dann sind die Formen (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$ benachbart (dabei bezeichnet A^{m-1} den vorletzten Term der Folge $A, A', A'' \dots A^m$, und B^{m-1}, a^{n-1}, b^{n-1} haben entsprechende Bedeutungen). Denn $A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ oder } A^m}$, also $B^{m-1} - b^{n-1} \equiv b^n - B^m$ und damit $\equiv 0$, wenn die Formen (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) identisch sind, und $\equiv 2b^n$, also $\equiv 0$, wenn sie entgegengesetzt und ambig sind. Somit ist in der Folge der Formen

$$(A, B, A'),\ (A', B', A'') \dots (A^{m-1}, B^{m-1}, A^m),$$
$$(a^n, -b^{n-1}, a^{n-1}),\ (a^{n-1}, -b^{n-2}, a^{n-2}) \dots (a', -b, a),\ (a, b, a')$$

jede Form ihrer Vorgängerin benachbart. Nach dem vorigen Artikel lässt sich also eine eigentliche Transformation der ersten Form F in die letzte f finden.

II. Die Formen (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) sind nicht identisch, sondern entgegengesetzt, und zugleich gilt $A^m = A^{m+1} = a^n = a^{n+1}$. Dann besitzt die Folge der Formen

$$(A, B, A'),\ (A', B', A'') \dots (A^m, B^m, A^{m+1}),$$
$$(a^n, -b^{n-1}, a^{n-1}),\ (a^{n-1}, -b^{n-2}, a^{n-2}) \dots (a', -b, a),\ (a, b, a')$$

dieselbe Eigenschaft. Denn $A^{m+1} = a^n$, und $B^m - b^{n-1} = -(b^n + b^{n-1})$ ist durch a^n teilbar. Nach dem vorigen Artikel findet man also eine eigentliche Transformation der ersten Form F in die letzte f.

Beispiel. So ergibt sich für die Formen $(23.\,38, 63)$, $(15, 20, 27)$ die Folge

$$(23, 38, 63).\ (63, 25, 10),\ (10, 5, 3),\ (3, 1.\,2),$$
$$(2.\,-7, 27),\ (27, -20, 15),\ (15, 20, 27)$$

und damit

$$h' = 1, \quad h'' = 3, \quad h''' = 2, \quad h'''' = -3, \quad h''''' = -1, \quad h'''''' = 0.$$

Daraus folgt diese Transformation der Form $23xx + 76xy + 63yy$ in $15tt + 40tu + 27uu$: $x = -13t - 18u$, $y = 8t + 11u$.

Aus dieser Lösung folgt ohne Mühe die Lösung der Aufgabe: *Sind die Formen F, f uneigentlich äquivalent, so soll eine uneigentliche Transformation der Form F in f gefunden werden.* Sei nämlich $f = att + 2btu + a'uu$. Dann ist die entgegengesetzte Form $app - 2bpq + a'qq$ der Form F eigentlich äquivalent. Man sucht eine eigentliche Transformation der Form F in jene, $x = \alpha p + \beta q$, $y = \gamma p + \delta q$. Offenbar geht dann F in f über, wenn man $x = \alpha t - \beta u$, $y = \gamma t - \delta u$ setzt, und diese Transformation ist uneigentlich.

Sind die Formen F, f also sowohl eigentlich als auch uneigentlich äquivalent, so lässt sich sowohl eine eigentliche als auch eine uneigentliche Transformation finden.

179.

Aufgabe. *Sind die Formen F, f äquivalent, so sollen alle Transformationen der Form F in f gefunden werden.*

Lösung. Sind die Formen F, f nur auf eine Art äquivalent, *das heißt* nur eigentlich oder nur uneigentlich, so sucht man nach dem vorigen Artikel eine Transformation der Form F in f. Offenbar kann es nur weitere Transformationen geben, die dieser gleichartig sind. Sind dagegen die Formen F, f sowohl eigentlich als auch uneigentlich äquivalent, so sucht man zwei Transformationen, eine eigentliche und eine uneigentliche. Sei nun die Form $F = (A, B, C)$, ferner $BB - AC = -D$ und der größte gemeinsame Teiler der Zahlen $A, 2B, C = m$. Aus Artikel 162 folgt: Im ersten Fall lassen sich alle Transformationen der Form F in f aus einer Transformation herleiten; im zweiten Fall alle eigentlichen aus der eigentlichen und alle uneigentlichen aus der uneigentlichen, sofern man alle Lösungen der Gleichung $tt + Duu = mm$ kennt. Sind diese gefunden, ist die Aufgabe also gelöst.

Es gilt aber $D = AC - BB$, $4D = 4AC - 4BB$, also ist $\frac{4D}{mm} = 4\frac{AC}{mm} - (\frac{2B}{m})^2$ eine ganze Zahl. Ist nun

1) $\frac{4D}{mm} > 4$, so gilt $D > mm$. Daher muss in $tt + Duu = mm$ notwendig $u = 0$ sein, und t kann nur die Werte $+m$ und $-m$ haben. Somit gilt: Sind F, f nur auf eine Art äquivalent, und ist eine Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

gegeben, so gibt es außer dieser, die aus $t = m$ entsteht (Artikel 162), und der folgenden

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

keine weiteren. Sind dagegen F, f sowohl eigentlich als auch uneigentlich äquivalent, und hat man eine eigentliche Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

und eine uneigentliche

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

so gibt es außer der ersten (aus $t = m$) und dieser

$$x = -\alpha x' - \beta y', \ y = -\gamma x' - \delta y' \text{ (aus } t = -m)$$

keine weitere eigentliche; ebenso gibt es keine weitere uneigentliche außer

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y';$$
$$\text{und } x = -\alpha' x' - \beta' y', \quad y' = -\gamma' x' - \delta' y'$$

2) Ist $\frac{4D}{mm} = 4$ oder $D = mm$, so hat die Gleichung $tt + Duu = mm$ vier Lösungen $t, u; = m, 0;\ -m, 0;\ 0, 1;\ 0, -1$. Sind also F, f nur auf eine Art äquivalent, und ist eine Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

gegeben, so gibt es insgesamt *vier* Transformationen,

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \mp\frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y',$$
$$y = \pm\frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'$$

Sind dagegen F, f auf zwei Arten äquivalent, oder gibt es neben der gegebenen Transformation eine weitere, ihr ungleichartige, so liefert auch diese vier Transformationen, die den ersten vier ungleichartig sind. Damit gibt es *acht* Transformationen. — Übrigens lässt sich leicht beweisen, dass in diesem Fall F, f tatsächlich immer auf beide Arten äquivalent sind. Denn wegen $D = mm = AC - BB$ teilt m auch B. Die Form $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ hat die Determinante $= -1$ und ist daher der Form $(1, 0, 1)$ oder dieser $(-1, 0, -1)$ äquivalent. Man sieht leicht, dass dieselbe Transformation, die $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ in $(\pm 1, 0, \pm 1)$ überführt, die Form (A, B, C) in $(\pm m, 0, \pm m)$ überführt, die ambig ist. Da die Form (A, B, C) einer ambigen Form äquivalent ist, ist sie also jeder Form, der sie äquivalent ist, sowohl eigentlich als auch uneigentlich äquivalent.

3) Ist $\frac{4D}{mm} = 3$ oder $4D = 3mm$, so ist m gerade, und alle Lösungen der Gleichung $tt + Duu = mm$ sind die folgenden sechs:

$$t, u; = m, 0;\ -m, 0;\ \tfrac{1}{2}m, 1;\ -\tfrac{1}{2}m, -1;\ \tfrac{1}{2}m, -1;\ -\tfrac{1}{2}m, 1$$

Hat man also zwei ungleichartige Transformationen der Form F in f,

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$
$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

so erhält man zwölf Transformationen, nämlich sechs, die der ersten gleichartig sind,

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \pm(\tfrac{1}{2}\alpha - \tfrac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta - \tfrac{\beta B + \delta C}{m}) y'$$
$$y = \pm(\tfrac{1}{2}\gamma + \tfrac{\alpha A + \gamma B}{m}) x' \pm (\tfrac{1}{2}\delta + \tfrac{\beta A + \delta B}{m}) y'$$
$$x = \pm(\tfrac{1}{2}\alpha + \tfrac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta + \tfrac{\beta B + \delta C}{m}) y'$$
$$y = \pm(\tfrac{1}{2}\gamma - \tfrac{\alpha A + \gamma B}{m}) x' \pm (\tfrac{1}{2}\delta - \tfrac{\beta A + \delta B}{m}) y'$$

und sechs, die der zweiten gleichartig sind. Diese entstehen aus den vorstehenden, indem man für α, β, γ, δ die Werte α', β', γ', δ' setzt.

Dass in diesem Fall F, f immer auf beide Arten äquivalent sind, beweisen wir so: Die Form $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ hat die Determinante $= -\frac{4D}{mm} = -3$ und ist deshalb (Artikel 176) entweder der Form $(\pm 1, 0, \pm 3)$ oder dieser $(\pm 2, \pm 1, \pm 2)$ äquivalent. Daraus erkennt man leicht, dass die Form (A, B, C) entweder der Form $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ oder dieser $(\pm m, \frac{1}{2}m, \pm m)$[*)] äquivalent ist. Beide sind ambig, also ist sie jeder äquivalenten Form auf beide Arten äquivalent.

4) Nimmt man $\frac{4D}{mm} = 2$ an, so ergibt sich $(\frac{2B}{m})^2 = 4\frac{AC}{mm} - 2$ und damit $\equiv 2 \pmod 4$. Da aber kein Quadrat $\equiv 2 \pmod 4$ sein kann, ist dieser Fall unmöglich.

5) Nimmt man $\frac{4D}{mm} = 1$ an, so ergibt sich $(\frac{2B}{m})^2 = 4\frac{AC}{mm} - 1 \equiv -1 \pmod 4$. Da dies unmöglich ist, kann auch dieser Fall nicht eintreten.

Da außerdem D weder $= 0$ noch negativ ist, gibt es keine anderen als die aufgezählten Fälle.

180.

Aufgabe. *Alle Darstellungen einer gegebenen Zahl M durch die Form $axx + 2bxy + cyy \ldots F$ mit negativer Determinante $-D$ finden, in denen x, y teilerfremde Werte annehmen.*

Lösung. Aus Artikel 154 folgt, dass M nur dann auf die verlangte Art dargestellt werden kann, wenn $-D$ ein quadratischer Rest von M ist. Man bestimmt also zuerst alle verschiedenen (*das heißt* inkongruenten) Werte des Ausdrucks $\sqrt{-D} \pmod M$. Diese seien $N, -N, N', -N', N'', -N''$ usw. Um die Rechnung einfacher zu machen, kann man alle N, N' usw. so wählen, dass sie nicht $> \frac{1}{2}M$ sind. Da jede Darstellung zu einem dieser Werte gehören muss, betrachten wir die Werte einzeln.

Sind die Formen $F, (M, N, \frac{D+NN}{M})$ nicht eigentlich äquivalent, so gibt es keine Darstellung von M, die zum Wert N gehört (Artikel 168). Sind sie es dagegen, so sucht man eine eigentliche Transformation der Form F in

$$Mx'x' + 2Nx'y' + \frac{D+NN}{M}y'y'$$

und zwar sei diese

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

Dann ist $x = \alpha, y = \gamma$ eine Darstellung der Zahl M durch F, die zu N gehört. Sei der größte gemeinsame Teiler der Zahlen $A, 2B, C, = m$; wir unterscheiden drei Fälle (voriger Artikel):

1) Ist $\frac{4D}{mm} > 4$, so gibt es keine anderen Darstellungen, die zu N gehören, als diese *beiden*: $x = \alpha, y = \gamma$; $x = -\alpha, y = -\gamma$ (Artikel 169, 179).

2) Ist $\frac{4D}{mm} = 4$, so gibt es *vier* Darstellungen

$$x = \pm\alpha, \quad y = \pm\gamma; \quad x = \mp\frac{\alpha B + \gamma C}{m}, \quad y = \pm\frac{\alpha A + \gamma B}{m}$$

[*)] Man kann beweisen, dass die Form (A, B, C) notwendig der zweiten äquivalent ist; das ist hier aber nicht nötig.

3) Ist $\frac{4D}{mm} = 3$, so gibt es *sechs* Darstellungen

$$\begin{aligned} x &= \pm\alpha, & y &= \pm\gamma; \\ x &= \pm(\tfrac{1}{2}\alpha - \tfrac{\alpha B+\gamma C}{m}), & y &= \pm(\tfrac{1}{2}\gamma + \tfrac{\alpha A+\gamma B}{m}) \\ x &= \pm(\tfrac{1}{2}\alpha + \tfrac{\alpha B+\gamma C}{m}), & y &= \pm(\tfrac{1}{2}\gamma - \tfrac{\alpha A+\gamma B}{m}) \end{aligned}$$

Ebenso sind die Darstellungen zu bestimmen, die zu den Werten $-N.N', -N'$ usw. gehören.

181.

Die Suche nach den Darstellungen der Zahl M durch die Form F, bei denen x, y keine teilerfremden Werte haben, lässt sich leicht auf den schon betrachteten Fall zurückführen. Eine solche Darstellung entstehe durch $x = \mu e, y = \mu f$, wobei μ der größte gemeinsame Teiler von $\mu e, \mu f$ ist, das heißt e, f teilerfremd sind. Dann gilt $M = \mu\mu(Aee + 2Bef + Cff)$, also ist die Zahl durch $\mu\mu$ teilbar. Die Substitution $x = e, y = f$ stellt dagegen die Zahl $\frac{M}{\mu\mu}$ durch die Form F dar, wobei x, y teilerfremde Werte haben. Ist also M durch kein Quadrat außer 1 teilbar, *zum Beispiel*, wenn es eine Primzahl ist, so gibt es keine solchen Darstellungen von M. Hat dagegen M quadratische Teiler, so seien diese $\mu\mu, \nu\nu, \pi\pi$ usw. Man sucht zuerst alle Darstellungen der Zahl $\frac{M}{\mu\mu}$ durch die Form (A, B, C), bei denen x, y teilerfremde Werte haben. Multipliziert man diese Werte mit μ, so erhält man alle Darstellungen von M, bei denen der größte gemeinsame Teiler der Zahlen x, y gleich μ ist. Ebenso liefern alle Darstellungen von $\frac{M}{\nu\nu}$, bei denen die Werte von x, y teilerfremd sind, alle Darstellungen von M, bei denen der größte gemeinsame Teiler der Werte von x, y gleich ν ist, usw.

Damit ist klar, dass sich mit den vorigen Regeln alle Darstellungen einer gegebenen Zahl durch eine gegebene Form mit negativer Determinante finden lassen.

Besondere Anwendungen auf die Zerlegung von Zahlen in zwei Quadrate, in ein Quadrat und das Doppelte eines Quadrats, in ein Quadrat und das Dreifache eines Quadrats.

182.

Wir wenden uns einigen besonderen Fällen zu, sowohl wegen ihrer bemerkenswerten Eleganz als auch wegen der anhaltenden Arbeit, die der berühmte Euler ihnen gewidmet hat. Dadurch haben sie gewissermaßen klassischen Rang erlangt.

I. Durch die Form $xx + yy$ lässt sich eine Zahl nur dann so darstellen, dass x zu y teilerfremd ist (oder in zwei teilerfremde Quadrate zerlegen), wenn -1 ein quadratischer Rest dieser Zahl ist. Umgekehrt ist dies bei allen solchen Zahlen möglich, wenn man sie positiv nimmt. Sei M eine solche Zahl, und seien alle Werte des Ausdrucks $\sqrt{-1}$ (mod. M) die folgenden: $N, -N, N', -N', N'', -N''$ usw. Dann ist nach Artikel 176 die Form $(M, N, \frac{NN+1}{M})$ der Form $(1, 0, 1)$ eigentlich äquivalent. Eine eigentliche Transformation der zweiten in die erste sei $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Dann sind die Darstellungen der Zahl M durch die Form $xx + yy$, die zu N gehören, diese vier[*]: $x = \pm\alpha, y = \pm\gamma$; $x = \mp\gamma, y = \pm\alpha$.

Da die Form $(1, 0, 1)$ ambig ist, ist offenbar auch die Form $(M, -N, \frac{NN+1}{M})$ ihr eigentlich äquivalent, und die erste geht eigentlich in die zweite über, wenn man $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$ setzt. Daraus ergeben sich vier Darstellungen von M, die zu $-N$ gehören: $x = \pm\alpha, y = \mp\gamma$; $x = \pm\gamma, y = \pm\alpha$. Es gibt also acht Darstellungen von M, von denen die eine Hälfte zu N, die andere zu $-N$ gehört. Sie alle ergeben aber nur *eine* Zerlegung der Zahl M in zwei Quadrate, $M = \alpha\alpha + \gamma\gamma$, wenn wir nur die Quadrate selbst betrachten, ohne ihre Reihenfolge oder die Vorzeichen ihrer Wurzeln zu berücksichtigen.

Gibt es also keine anderen Werte des Ausdrucks $\sqrt{-1}$ (mod. M) als N und $-N$, was *zum Beispiel* eintritt, wenn M eine Primzahl ist, so lässt sich M nur auf eine Art in zwei teilerfremde Quadrate zerlegen. Da nun -1 ein quadratischer Rest jeder Primzahl der Form $4n + 1$ ist (Artikel 108) und sich eine Primzahl offenbar nicht in zwei Quadrate zerlegen lässt, die nicht teilerfremd sind, haben wir den Satz:

Jede Primzahl der Form $4n + 1$ lässt sich in zwei Quadrate zerlegen, und zwar nur auf eine Art.

$$1 = 0 + 1, \quad 5 = 1 + 4, \quad 13 = 4 + 9, \quad 17 = 1 + 16,$$
$$29 = 4 + 25, \quad 37 = 1 + 36, \quad 41 = 16 + 25, \quad 53 = 4 + 49,$$
$$61 = 25 + 36, \quad 73 = 9 + 64, \quad 89 = 25 + 64, \quad 97 = 16 + 81 \quad \text{usw.}$$

Diesen sehr eleganten Satz kannte schon Fermat, doch bewies ihn zuerst der berühmte Euler, *Comm. nov. Petr. Bd.* V, *für die Jahre* 1754, 1755, *S.* 3 ff. In *Bd.* IV steht eine Abhandlung zum selben Thema, *S.* 3 ff.; damals hatte er die Sache aber noch nicht vollständig abgeschlossen. Siehe besonders Artikel 27.

Lässt sich also eine Zahl der Form $4n + 1$ entweder auf mehrere Arten oder gar nicht in zwei Quadrate zerlegen, so ist sie sicher keine Primzahl.

[*] Dieser Fall ist nämlich offenbar unter (2) von Artikel 180 enthalten.

Hat umgekehrt der Ausdruck $\sqrt{-1}$ (mod. M) außer N und $-N$ noch andere Werte, so gibt es weitere Darstellungen von M, die zu diesen gehören. In diesem Fall lässt sich also M auf mehrere Arten in zwei Quadrate zerlegen, *zum Beispiel* $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Die übrigen Darstellungen, bei denen x, y keine teilerfremden Werte haben, lassen sich mit unserer allgemeinen Methode leicht finden. Wir bemerken nur: Enthält eine Zahl Faktoren der Form $4n+3$, die sich durch keine Division durch ein Quadrat entfernen lassen (was eintritt, wenn einer oder mehrere dieser Faktoren mit *ungeradem Exponenten* vorkommen), so lässt sie sich auf keine Art in zwei Quadrate zerlegen[*)].

II. Durch die Form $xx + 2yy$ lässt sich keine Zahl, für die -2 ein Nichtrest ist, so darstellen, dass x zu y teilerfremd ist; bei allen übrigen ist dies möglich. Sei -2 ein Rest der Zahl M und N ein Wert des Ausdrucks $\sqrt{-2}$ (mod. M). Dann sind nach Artikel 176 die Formen $(1, 0, 2)$, $(M, N, \frac{NN+2}{M})$ eigentlich äquivalent. Die erste gehe durch $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ eigentlich in die zweite über. Dann ist $x = \alpha, y = \gamma$ eine Darstellung der Zahl M, die zu N gehört. Außer dieser und $x = -\alpha, y = -\gamma$ gehören keine weiteren zu N (Artikel 180).

Wie oben erkennt man, dass die Darstellungen $x = \pm\alpha, y = \mp\gamma$ zum Wert $-N$ gehören. Alle vier Darstellungen ergeben nur eine Zerlegung von M in ein Quadrat und das Doppelte eines Quadrats. Gibt es außer N und $-N$ keine weiteren Werte des Ausdrucks $\sqrt{-2}$ (mod. M), so gibt es keine weiteren Zerlegungen. Mit den Aussagen von Artikel 116 folgt daraus leicht der Satz:

Jede Primzahl der Form $8n + 1$ *oder* $8n + 3$ *lässt sich in ein Quadrat und das Doppelte eines Quadrats zerlegen, und zwar nur auf eine Art.*

$$1 = 1 + 0, \quad 3 = 1 + 2, \quad 11 = 9 + 2, \quad 17 = 9 + 8,$$
$$19 = 1 + 18, \quad 41 = 9 + 32. \quad 43 = 25 + 18, \quad 59 = 9 + 50,$$
$$67 = 49 + 18, \quad 73 = 1 + 72, \quad 83 = 81 + 2,$$
$$89 = 81 + 8, \quad 97 = 25 + 72 \quad \text{usw.}$$

Auch diesen Satz kannte Fermat, wie mehrere ähnliche; den ersten Beweis gab aber der berühmte La Grange, *Suite des recherches d'Arithmétique*, Nouv. Mém. de l'Ac. de Berlin 1775, S. 323 ff. Vieles zum selben Thema hatte bereits der berühmte Euler geklärt, *Specimen de usu observationum in mathesi pura*, Comm. nov. Petr. Bd. VI, S. 185 ff. Ein vollständiger Beweis des Satzes entzog sich aber immer seinen Bemühungen, S. 220. Vergleiche auch die Abhandlung in Bd. VIII (für die Jahre 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, gegen Ende.

[*)] Ist die Zahl $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$, wobei a, b, c usw. verschiedene Primzahlen der Form $4n+1$ sind und S das Produkt aller Primfaktoren von M der Form $4n+3$ ist (jede positive Zahl lässt sich in diese Form bringen, indem man $\mu = 0$ setzt, wenn M ungerade ist, und $S = 1$, wenn M keine Faktoren der Form $4n+3$ enthält), so lässt sich M auf *keine Art* in zwei Quadrate zerlegen, wenn S kein Quadrat ist. Ist dagegen S ein Quadrat, so gibt es $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ usw. Zerlegungen von M, wenn mindestens eine der Zahlen α, β, γ usw. ungerade ist, oder $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ usw. $+\frac{1}{2}$, wenn alle α, β, γ usw. gerade sind (wobei nur die Quadrate selbst betrachtet werden). Wer mit kombinatorischen Rechnungen etwas vertraut ist, kann den Beweis dieses Satzes ohne große Mühe aus unserer allgemeinen Theorie herleiten. Wir können uns hier bei ihm ebenso wenig wie bei anderen *besonderen Fällen* aufhalten. Vergleiche Artikel 105.

III. Mit einer ähnlichen Methode beweist man, dass sich jede Zahl, für die -3 ein quadratischer Rest ist, entweder durch die Form $xx+3yy$ oder durch diese $2xx+2xy+2yy$ darstellen lässt, und zwar so, dass der Wert von x zum Wert von y teilerfremd ist. Da nun -3 ein Rest aller Primzahlen der Form $3n+1$ ist (Artikel 119) und die Form $2xx+2xy+2yy$ offenbar nur *gerade* Zahlen darstellen kann, ergibt sich wie oben der Satz:

Jede Primzahl der Form $3n+1$ *lässt sich in ein Quadrat und das Dreifache eines Quadrats zerlegen, und zwar nur auf eine Art.*

$$1 = 1+0, \quad 7 = 4+3, \quad 13 = 1+12, \quad 19 = 16+3,$$
$$31 = 4+27, \quad 37 = 25+12, \quad 43 = 16+27, \quad 61 = 49+12,$$
$$67 = 64+3, \quad 73 = 25+48 \quad \text{usw.}$$

Den Beweis dieses Satzes gab zuerst der berühmte Euler in der eben angeführten Abhandlung, *Comm. nov. Petr. Bd.* VIII, *S.* 105 ff.

Ebenso könnten wir weitergehen und *zum Beispiel* zeigen, dass sich jede Primzahl der Form $20n+1$, $20n+3$, $20n+7$ oder $20n+9$ (für die nämlich -5 ein Rest ist) durch eine der Formen $xx+5yy$, $2xx+2xy+3yy$ darstellen lässt: die Primzahlen der Formen $20n+1$ und $20n+9$ durch die erste, die Primzahlen der Formen $20n+3, 20n+7$ durch die zweite. Ebenso lässt sich das Doppelte der Primzahlen der Formen $20n+1, 20n+9$ durch die Form $2xx+2xy+3yy$ und das Doppelte der Primzahlen der Formen $20n+3, 20n+7$ durch die Form $xx+5yy$ darstellen. Doch kann jeder diese Aussage und unendlich viele weitere besondere Aussagen selbst aus den vorigen Ergebnissen und dem herleiten, was wir weiter unten behandeln werden. — Wir gehen also zu den *Formen mit positiver Determinante* über. Da ihre Art ganz verschieden ist, je nachdem, ob die Determinante ein Quadrat ist oder nicht, schließen wir die Formen mit quadratischer Determinante zunächst aus und werden sie später gesondert betrachten.

Formen mit positiver nichtquadratischer Determinante.

183.

Aufgabe. *Zu einer beliebigen Form (a, b, a') mit positiver nichtquadratischer Determinante $= D$ eine eigentlich äquivalente Form (A, B, C) finden, in der B positiv und $< \sqrt{D}$ ist, während A, falls positiv, oder $-A$, falls A negativ ist, zwischen $\sqrt{D}+B$ und $\sqrt{D}-B$ liegt.*

Lösung. Wir nehmen an, dass die gegebene Form noch nicht beide Bedingungen erfüllt; sonst müsste man keine andere Form suchen. Außerdem bemerken wir, dass bei einer Form mit *nichtquadratischer* Determinante der erste oder letzte Term nicht $= 0$ sein kann (Artikel 171, Anmerkung). Sei $b' \equiv -b \pmod{a'}$, und zwar zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp a'$ gelegen (mit dem oberen Vorzeichen, wenn a' positiv ist, und dem unteren, wenn es negativ ist). Dass dies möglich ist, beweist man leicht wie in Artikel 3. Man setzt $\frac{b'b'-D}{a'} = a''$, was eine ganze Zahl ist, weil $b'b' - D \equiv bb - D \equiv aa' \equiv 0 \pmod{a'}$. Ist nun $a'' < a'$, so sei wieder $b'' \equiv -b' \pmod{a''}$, und zwar zwischen $\sqrt{D}$ und $\sqrt{D} \mp a''$ gelegen (je nachdem, ob a'' positiv oder negativ ist), und $\frac{b''b''-D}{a''} = a'''$. Ist erneut $a''' < a''$, so sei wiederum $b''' \equiv -b'' \pmod{a'''}$, zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'''$ gelegen, und $\frac{b'''b'''-D}{a'''} = a''''$. Man setzt dies fort, bis die Folge a', a'', a''', a'''' usw. einen Term a^{m+1} erreicht, der nicht kleiner als sein Vorgänger a^m ist. Das muss schließlich eintreten, da man sonst eine unendliche Folge ganzer Zahlen hätte, die immer weiter abnehmen. Setzt man dann $a^m = A$, $b^m = B$, $a^{m+1} = C$, so erfüllt die Form (A, B, C) alle Bedingungen.

Beweis. I. In der Folge der Formen (a, b, a'), (a', b', a''), (a'', b'', a''') usw. ist jede ihrer Vorgängerin benachbart. Die letzte (A, B, C) ist also der ersten (a, b, a') eigentlich äquivalent.

II. Da B zwischen $\sqrt{D}$ und $\sqrt{D} \mp A$ liegt (stets mit dem oberen Vorzeichen, wenn A positiv ist, und dem unteren, wenn A negativ ist), sind bei der Setzung $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$ die Zahlen p, q offenbar positiv. Man bestätigt leicht $qq + 2pq + 2p\sqrt{D} = D + AA - BB$; also ist $D + AA - BB$ eine positive Zahl, die wir $= r$ setzen. Wegen $D = BB - AC$ ergibt sich $r = AA - AC$, also ist $AA - AC$ positiv. Da aber nach Voraussetzung A nicht größer als C ist, kann dies offenbar nur eintreten, wenn AC negativ ist, also die Vorzeichen von A, C entgegengesetzt sind. Daraus folgt $BB = D + AC < D$ und somit $B < \sqrt{D}$.

III. Da ferner $-AC = D - BB$ gilt, folgt $AC < D$ und daher (weil A nicht $> C$ ist) $A < \sqrt{D}$. Also ist $\sqrt{D} \mp A$ positiv und damit auch B, das zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp A$ liegt.

IV. Umso mehr ist dann $\sqrt{D} + B \mp A$ positiv. Da $\sqrt{D} - B \mp A = -q$ negativ ist, liegt $\pm A$ zwischen $\sqrt{D} + B$ und $\sqrt{D} - B$. *W. z. b. w.*

Beispiel. Die gegebene Form sei $(67, 97, 140)$, ihre Determinante $= 29$. Hier findet man die Folge der Formen $(67, 97, 140)$, $(140, -97, 67)$, $(67, -37, 20)$, $(20, -3, -1)$, $(-1, 5, 4)$. Die letzte ist die gesuchte.

Solche Formen (A, B, C) mit positiver nichtquadratischer Determinante D, bei denen A, positiv genommen, zwischen $\sqrt{D}+B$ und $\sqrt{D}-B$ liegt, während B positiv und $< \sqrt{D}$ ist, nennen wir *reduzierte Formen*. Die reduzierten Formen mit positiver nichtquadratischer Determinante unterscheiden sich also etwas von den reduzierten Formen mit negativer Determinante. Wegen der großen Analogie zwischen beiden wollten wir aber keine verschiedenen Namen einführen.

184.

Könnte man die Äquivalenz zweier *reduzierter* Formen mit positiver Determinante ebenso leicht erkennen wie bei Formen mit negativer Determinante (Artikel 172), so ließe sich ohne Mühe entscheiden, ob zwei *beliebige* Formen mit derselben positiven Determinante äquivalent sind. Hier ist die Lage aber ganz anders: Sehr viele reduzierte Formen können zueinander äquivalent sein. Bevor wir diese Aufgabe angehen, müssen wir die Natur der reduzierten Formen genauer untersuchen (mit positiver nichtquadratischer Determinante, was hier immer mitgemeint ist).

1) Ist (a, b, c) eine reduzierte Form, so haben a und c entgegengesetzte Vorzeichen. Setzt man nämlich die Determinante der Form $= D$, so gilt $ac = bb - D$, was wegen $b < \sqrt{D}$ negativ ist.

2) Die Zahl c liegt ebenso wie a, positiv genommen, zwischen $\sqrt{D}+b$ und $\sqrt{D}-b$. Denn $-c = \frac{D-bb}{a}$; also liegt c, wenn man vom Vorzeichen absieht, zwischen $\frac{D-bb}{\sqrt{D}+b}$ und $\frac{D-bb}{\sqrt{D}-b}$, *das heißt* zwischen $\sqrt{D}-b$ und $\sqrt{D}+b$.

3) Damit ist klar, dass auch (c, b, a) eine reduzierte Form ist.

4) Sowohl a als auch c sind $< 2\sqrt{D}$. Beide sind nämlich $< \sqrt{D}+b$ und damit umso mehr $< 2\sqrt{D}$.

5) Die Zahl b liegt zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$ (mit dem oberen Vorzeichen, wenn a positiv ist, und dem unteren, wenn es negativ ist). Da nämlich $\pm a$ zwischen $\sqrt{D}+b$ und $\sqrt{D}-b$ liegt, ist $\pm a - (\sqrt{D}-b)$ oder $b - (\sqrt{D} \mp a)$ positiv; $b - \sqrt{D}$ dagegen ist negativ. Also liegt b zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$. — Genau auf dieselbe Art beweist man, dass b zwischen $\sqrt{D}$ und $\sqrt{D} \mp c$ liegt (je nachdem, ob c positiv oder negativ ist).

6) *Jede reduzierte Form (a, b, c) hat auf jeder Seite genau eine reduzierte Nachbarform.*

Man setzt $a' = c$, $b' \equiv -b \pmod{a'}$, zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$ gelegen[*)], und $c' = \frac{b'b'-D}{a'}$. Dann ist die Form (a', b', c') der Form (a, b, c) nach rechts benachbart. Zugleich ist klar, dass eine reduzierte Form, die der Form (a, b, c) nach rechts benachbart ist, keine andere als (a', b', c') sein kann. Dass sie tatsächlich reduziert ist, beweisen wir so:

A) Setzt man

$$\sqrt{D} + b \mp a' = p, \quad \pm a' - (\sqrt{D} - b) = q, \quad \sqrt{D} - b = r$$

so sind diese p, q, r nach (2) oben und nach der Definition einer reduzierten Form positiv. Weiter setzt man

$$b' - (\sqrt{D} \mp a) = q', \quad \sqrt{D} - b' = r'$$

[*)] Wo Vorzeichen zur Wahl stehen, gilt stets das obere, wenn a' positiv ist, und das untere, wenn a' negativ ist.

Dann sind q', r' positiv, weil b' zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$ liegt. Schließlich sei $b + b' = \pm ma$; dann ist m eine ganze Zahl. Offenbar gilt $p + q' = b + b'$, also ist $b + b'$ oder $\pm ma'$ positiv und damit auch m. Daraus folgt, dass $m - 1$ sicher nicht negativ ist. Weiter ergibt sich

$$r + q' \pm ma' = 2b' \pm a', \quad \text{oder} \quad 2b' = r + q' \pm (m-1)a'$$

also sind $2b'$ und b' notwendig positiv. Da $b' + r' = \sqrt{D}$, gilt $b' < \sqrt{D}$.

B) Weiter ergibt sich

$$r \pm ma' = \sqrt{D} + b', \quad \text{oder} \quad r \pm (m-1)a' = \sqrt{D} + b' \mp a'$$

also ist $\sqrt{D} + b' \mp a'$ positiv. Daraus und aus $\pm a' - (\sqrt{D} - b') = q'$, was also positiv ist, folgt, dass $\pm a'$ zwischen $\sqrt{D} + b'$ und $\sqrt{D} - b'$ liegt. — Somit ist (a', b', c') eine reduzierte Form.

Ebenso beweist man: Setzt man $'c = a$, $'b \equiv -b \pmod{'c}$, zwischen $\sqrt{D}$ und $\sqrt{D} \pm {}'c$ gelegen, und $'a = \frac{'b'b - D}{'c}$, so ist die Form $('a, 'b, 'c)$ reduziert. Offenbar ist diese Form der Form (a, b, c) nach links benachbart, und keine andere reduzierte Form als $('a, 'b, 'c)$ kann diese Eigenschaft haben.

Beispiel. Die reduzierte Form $(5, 11, -14)$ mit Determinante $= 191$ hat nach rechts die reduzierte Nachbarform $(-14, 3, 13)$ und nach links diese $(-22, 9, 5)$.

7) Ist der reduzierten Form (a, b, c) die reduzierte Form (a', b', c') nach rechts benachbart, so ist der reduzierten Form (c, b, a) die Form (c', b', a') nach links benachbart. Ist der reduzierten Form (a, b, c) die Form $('a, 'b, 'c)$ nach links benachbart, so ist der reduzierten Form (c, b, a) die reduzierte Form $('c, 'b, 'a)$ nach rechts benachbart. Außerdem sind die Formen $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b', -c')$ reduziert, und die zweite ist der ersten, die dritte der zweiten nach rechts benachbart; oder die erste ist der zweiten und die zweite der dritten nach links benachbart. Ebenso verhält es sich mit den drei Formen $(-c', b', -a')$, $(-c, b, -a)$, $(-'c, 'b, -'a)$. Dies ist so klar, dass es keiner weiteren Erläuterung bedarf.

185.

Die Anzahl aller reduzierten Formen mit gegebener Determinante D ist stets endlich; die Formen selbst lassen sich auf zwei Arten finden. Bezeichnen wir alle reduzierten Formen mit Determinante D allgemein durch (a, b, c), sodass sämtliche Werte von a, b, c zu bestimmen sind.

Erste Methode. Für a nehme man alle Zahlen (sowohl positiv als auch negativ), die kleiner als $2\sqrt{D}$ sind und für die D ein quadratischer Rest ist. Für jedes a setze man b gleich allen positiven Werten des Ausdrucks $\sqrt{D}$ (mod. a), die zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$ liegen; c setze man dagegen für jedes bestimmte Wertepaar von a, b $= \frac{bb-D}{a}$. Ergeben sich dabei Formen, in denen $\pm a$ außerhalb des Intervalls zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegt, so sind sie zu verwerfen.

Zweite Methode. Für b nehme man alle positiven Zahlen kleiner als $\sqrt{D}$. Für jedes b zerlege man $bb - D$ auf alle möglichen Arten in zwei Faktoren, die ohne Berücksichtigung ihres Vorzeichens zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegen, und setze den einen $= a$, den anderen $= c$. Jede Zerlegung liefert offenbar zwei Formen, da jeder Faktor sowohl $= a$ als auch $= c$ gesetzt werden muss.

Beispiel. Sei $D = 79$; dann sind die zweiundzwanzig Werte von a: ∓ 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15. Daraus ergeben sich neunzehn Formen:

$$\begin{gathered}(1, 8, -15), \quad (2, 7, -15), \quad (3, 8, -5), \quad (3, 7, -10),\\ (5, 8, -3), \quad (5, 7, -6), \quad (6, 7, -5), \quad (6, 5, -9),\\ (7, 4, -9), \quad (7, 3, -10), \quad (9, 5, -6), \quad (9, 4, -7),\\ (10, 7, -3), \quad (10, 3, -7), \quad (13, 1, -6), \quad (14, 3, -5),\\ (15, 8, -1), \quad (15, 7, -2), \quad (15, 2, -5)\end{gathered}$$

und ebenso viele weitere, die durch Umkehrung der Vorzeichen der äußeren Glieder entstehen, nämlich $(-1, 8, 15)$, $(-2, 7, 15)$ usw., insgesamt also achtunddreißig. Davon sind aber sechs zu verwerfen: $(\pm 13, 1, \mp 6)$, $(\pm 14, 3, \mp 5)$, $(\pm 15, 2, \mp 5)$; die übrigen zweiunddreißig umfassen alle reduzierten Formen. Die zweite Methode liefert dieselben Formen in folgender Reihenfolge[*]:

$$\begin{gathered}(\pm 7, 3, \mp 10), \quad (\pm 10, 3, \mp 7), \quad \pm 7, 4, \mp 9), \quad (\pm 9, 4, \mp 7),\\ (\pm 6, 5, \mp 9), \quad (\pm 9, 5, \mp 6), \quad (\pm 2, 7, \mp 15), \quad (\pm 3, 7, \mp 10),\\ (\pm 5, 7, \mp 6), \quad (\pm 6, 7, \mp 5), \quad (\pm 10, 7, \mp 3), \quad (\pm 15, 7, \mp 2),\\ (\pm 1, 8, \mp 15), \quad (\pm 3, 8, \mp 5), \quad (\pm 5, 8, \mp 3), \quad (\pm 15, 8, \mp 1).\end{gathered}$$

[*] Für $b = 1$ lässt sich -78 nicht in zwei Faktoren zerlegen, die ohne Berücksichtigung ihres Vorzeichens zwischen $\sqrt{79} + 1$ und $\sqrt{79} - 1$ liegen. Daher ist dieser Wert zu überspringen, aus demselben Grund auch die Werte 2 und 6.

186.

Sei F eine reduzierte Form mit Determinante D und F' ihre nach rechts benachbarte reduzierte Form; dieser sei wiederum die reduzierte Form F'' nach rechts benachbart, die reduzierte Form F''' der Form F'' usw. Dann sind alle Formen F', F'', F''' usw. vollständig bestimmt und sowohl untereinander als auch zu F eigentlich äquivalent. Da aber die Anzahl aller reduzierten Formen mit gegebener Determinante endlich ist, können nicht alle Formen der unendlichen Folge F, F', F'' usw. verschieden sein. Nehmen wir an, F^m und F^{m+n} seien identisch. Dann sind F^{m-1}, F^{m+n-1} reduzierte Formen, die derselben reduzierten Form nach links benachbart sind, und daher identisch; ebenso sind F^{m-2} und F^{m+n-2} usw. und schließlich F und F^n identisch. Wird also die Folge F, F', F'' usw. weit genug fortgesetzt, so muss schließlich die erste Form F wiederkehren. Nehmen wir an, F^n sei die erste mit F identische Form, seien also alle $F', F'' \ldots . F^{n-1}$ von F verschieden, so sieht man leicht, dass sämtliche Formen $F, F', F'' \ldots . F^{n-1}$ verschieden sind. Diese Gesamtheit von Formen nennen wir die *Periode der Form* F. Setzt man die Folge über die letzte Form der Periode hinaus fort, so erscheinen dieselben Formen F, F', F'' usw. erneut, und die ganze unendliche Folge F, F', F'' usw. besteht aus dieser unendlich oft wiederholten Periode von F.

Die Folge F, F', F'' usw. lässt sich auch rückwärts fortsetzen, indem man der Form F die ihr nach links benachbarte reduzierte Form $'F$, dieser wiederum die ihr nach links benachbarte reduzierte Form $''F$ usw. voranstellt. So entsteht eine nach *beiden Seiten* unendliche Folge von Formen:

$$\ldots .'''F,\ ''F,\ 'F,\ F,\ F',\ F'',\ F''' \ldots .$$

Man sieht leicht, dass $'F$ mit F^{n-1}, $''F$ mit F^{n-2} usw. identisch ist; damit besteht die Folge auch nach links aus der unendlich oft wiederholten Periode von F.

Ordnet man den Formen F, F', F'' usw., $'F$, $''F$ usw. die Indizes 0, 1, 2 usw., -1, -2 usw. zu, allgemein der Form F^m den Index m und der Form ${}^mF$ den Index $-m$, so sind offenbar *je zwei Formen der Folge identisch oder verschieden, je nachdem ihre Indizes modulo n kongruent oder inkongruent sind.*

Beispiel. Als Periode der Form $(3, 8, -5)$, deren Determinante $= 79$ ist, findet man $3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$. Nach der letzten erscheint erneut $(3, 8, -5)$. Hier ist also $n = 6$.

187.

Hier folgen einige allgemeine Bemerkungen über diese Perioden.

1) Schreibt man die Formen F, F', F'' usw.; $'F, ''F, '''F$ usw. als

$$\begin{array}{c} a, b, -a'), \quad (-a', b', a''), \quad (a'', b'', -a''') \text{ usw.;} \\ (-'a, 'b, a), \quad (''a, ''b, -'a), \quad (-'''a, '''b, ''a) \end{array}$$

so haben alle a, a', a'', a''' usw., $'a, ''a, '''a$ usw. *dasselbe Vorzeichen* (Artikel 184, 1), während alle b, b', b'' usw., $'b, ''b$ usw. positiv sind.

2) Daraus folgt, dass die Zahl n (die Anzahl der Formen, aus denen die Periode von F besteht) stets *gerade* ist. Denn das erste Glied jeder Form F^m dieser Periode hat offenbar dasselbe Vorzeichen wie das erste Glied a von F, wenn m gerade ist, und das entgegengesetzte, wenn m ungerade ist. Da F^n und F identisch sind, muss n gerade sein.

3) Nach Artikel 184, 6 lautet der Algorithmus zur Bestimmung der Zahlen b', b'', b''' usw., a'', a''' usw.:

$$\begin{array}{llll} b' \equiv -b \text{ (mod. } a') & \text{zwischen } \sqrt{D} \text{ und } \sqrt{D} \mp a'; & a'' = \dfrac{D - b'b'}{a'} \\ b'' \equiv -b' \text{ (mod. } a'') & \ldots\ldots\ldots & \sqrt{D} \mp a''; & a''' = \dfrac{D - b''b''}{a''} \\ b''' \equiv -b'' \text{ (mod. } a''') & \ldots\ldots\ldots & \sqrt{D} \mp a'''; & a'''' = \dfrac{D - b'''b'''}{a'''} \end{array}$$

usw.

In der zweiten Spalte sind die oberen oder unteren Vorzeichen zu nehmen, je nachdem a, a', a'' usw. positiv oder negativ sind. Anstelle der Formeln in der dritten Spalte kann man auch die folgenden verwenden, die bequemer sind, wenn D groß ist:

$$\begin{aligned} a'' &= \frac{b + b'}{a'}(b - b') + a \\ a''' &= \frac{b' + b''}{a''}(b' - b'') + a' \\ a'''' &= \frac{b'' + b'''}{a'''}(b'' - b''') + a'' \end{aligned}$$

usw.

4) Jede Form F^m in der Periode von F hat im Wesentlichen dieselbe Periode wie F. Diese lautet nämlich F^m, $F^{m+1} \ldots . F^{n-1}$, $F, F' \ldots . F^{m-1}$; sie enthält dieselben Formen in derselben Reihenfolge wie die Periode von F und unterscheidet sich von ihr nur durch Anfang und Ende.

5) Daher lassen sich alle reduzierten Formen mit derselben Determinante D in Perioden *aufteilen*. Man nehme eine beliebige dieser Formen, F, und bestimme ihre Periode $F, F', F'' \dots F^{n-1}$, die wir mit P bezeichnen. Umfasst sie noch nicht alle reduzierten Formen mit Determinante D, so sei G eine darin nicht enthaltene Form und Q ihre Periode. Dann können P und Q offenbar keine Form gemeinsam haben; andernfalls müsste auch G in P enthalten sein, und die Perioden würden vollständig zusammenfallen. Sind mit P und Q noch nicht alle reduzierten Formen erfasst, so liefert eine der fehlenden Formen, H, eine dritte Periode R, die weder mit P noch mit Q eine Form gemeinsam hat. So können wir fortfahren, bis alle reduzierten Formen erfasst sind. *Zum Beispiel* teilen sich alle reduzierten Formen mit Determinante 79 in sechs Perioden auf:

I.	$(1,8,-15)$,	$(-15,7,2)$,	$(2,7,-15)$,	$(-15,8,1)$.
II.	$(-1,8,15)$,	$(15,7,-2)$,	$(-2,7,15)$,	$(15,8,-1)$.
III.	$(3,8,-5)$,	$(-5,7,6)$,	$(6,5,-9)$,	
	$(-9,4,7)$,	$(7,3,-10)$,	$(-10,7,3)$.	
IV.	$(-3,8,5)$,	$(5,7,-6)$,	$(-6,5,9)$,	
	$(9,4,-7)$,	$(-7,3,10)$,	$(10,7,-3)$.	
V.	$(5,8,-3)$,	$(-3,7,10)$,	$(10,3,-7)$,	
	$(-7,4,9)$,	$(9,5,-6)$,	$(-6,7,5)$.	
VI.	$(-5,8,3)$,	$(3,7,-10)$,	$(-10,3,7)$,	
	$(7,4,-9)$,	$(-9,5,6)$,	$(6,7,-5)$.	

6) Formen, die aus denselben Gliedern in umgekehrter Reihenfolge bestehen, etwa $(a,b,-a')$, $(-a',b,a)$, nennen wir *assoziierte Formen*. Aus Artikel 184, 7 sieht man leicht: Hat die reduzierte Form F die Periode $F, F', F'' \dots F^{n-1}$, ist der Form F die Form f assoziiert und sind den Formen $F^{n-1}, F^{n-2} \dots F'', F'$ jeweils die Formen $f', f'' \dots f^{n-2}, f^{n-1}$ assoziiert, so ist die Periode von f gleich $f, f', f'' \dots f^{n-2}, f^{n-1}$. Sie besteht also aus ebenso vielen Formen wie die Periode von F. Die Perioden assoziierter Formen nennen wir *assoziierte Perioden*. In unserem Beispiel sind die Perioden III und VI sowie IV und V assoziiert.

7) Es kann aber auch die Form f selbst in der Periode der ihr assoziierten Form F vorkommen, wie in unserem Beispiel bei den Perioden I und II. Dann stimmt die Periode von F mit der von f überein, oder *die Periode von F ist sich selbst assoziiert.* In diesem Fall findet man in dieser Periode zwei ambige Formen. Nehmen wir nämlich an, die Periode von F bestehe aus $2n$ Formen, seien also F und F^{2n} identisch; ferner sei $2m+1$ der Index von f in der Periode von F[*)], seien also F^{2m+1} und F assoziiert. Dann sind auch F' und F^{2m}, ferner F'' und F^{2m-1} usw. und damit auch F^m und F^{m+1} assoziiert. Sei $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Dann gilt $b^m + b^{m+1} \equiv 0 \pmod{a^{m+1}}$; nach der Definition assoziierter Formen gilt aber $b^m = b^{m+1}$ und somit $2b^{m+1} \equiv 0 \pmod{a^{m+1}}$, die Form F^{m+1} ist also ambig. — Ebenso sind F^{2m+1} und F^{2n} assoziiert; daher auch F^{2m+2} und F^{2n-1}, F^{2m+3} und F^{2n-2} usw. und schließlich F^{m+n} und F^{m+n+1}. Die letztere ist ambig, wie ein ähnlicher Schluss leicht zeigt. Da aber $m+1$ und $m+n+1$ modulo $2n$ inkongruent sind, sind die Formen F^{m+1} und F^{m+n+1} nicht identisch (Artikel 186, wo n dasselbe bezeichnet wie hier $2n$). So sind in I die Formen $(1, 8, -15)$, $(2, 7, -15)$ und in II die Formen $(-1, 8, 15)$, $(-2, 7, 15)$ ambig.

8) Umgekehrt ist *jede Periode, in der eine ambige Form vorkommt, sich selbst assoziiert.* Denn ist F^m eine reduzierte ambige Form, so sieht man leicht, dass die ihr assoziierte Form (die ebenfalls reduziert ist) zugleich ihre nach links benachbarte Form ist, *das heißt*, F^{m-1} und F^m sind assoziiert. Dann ist aber die ganze Periode sich selbst assoziiert. — Daraus folgt, dass *eine Periode nicht genau eine ambige Form enthalten kann.*

9) Sie kann aber auch *nicht mehr als zwei enthalten.* Nehmen wir an, die Periode von F, die aus $2n$ Formen besteht, enthalte drei ambige Formen F^λ, F^μ, F^ν mit den jeweiligen Indizes λ, μ, ν, sodass λ, μ, ν verschiedene Zahlen zwischen 0 und $2n-1$ einschließlich der Grenzen sind. Dann sind die Formen $F^{\lambda-1}$ und F^λ, ebenso $F^{\lambda-2}$ und $F^{\lambda+1}$ usw. und schließlich F und $F^{2\lambda-1}$ assoziiert. Aus demselben Grund sind F und $F^{2\mu-1}$ sowie F und $F^{2\nu-1}$ assoziiert. Daher sind $F^{2\lambda-1}$, $F^{2\mu-1}$, $F^{2\nu-1}$ identisch und die Indizes $2\lambda-1$, $2\mu-1$, $2\nu-1$ modulo $2n$ kongruent, folglich auch $\lambda \equiv \mu \equiv \nu \pmod{n}$. *Das ist widersinnig*, da zwischen 0 und $2n-1$ offenbar keine drei verschiedenen Zahlen liegen können, die modulo n kongruent sind.

[*)] Dieser Index muss ungerade sein, da die ersten Glieder der Formen F, f offenbar entgegengesetzte Vorzeichen haben (*siehe oben*, 2).

188.

Da alle Formen derselben Periode eigentlich äquivalent sind, stellt sich die Frage, ob auch Formen aus verschiedenen Perioden eigentlich äquivalent sein können. Bevor wir aber zeigen, dass *dies unmöglich ist*, müssen wir einige Punkte über die Transformation reduzierter Formen behandeln.

Da wir im Folgenden sehr oft mit Transformationen von Formen zu tun haben, verwenden wir von jetzt an stets die folgende abgekürzte Schreibweise, um die Schreibweise möglichst kurz zu halten. Wird eine Form $LXX + 2MXY + NYY$ durch die Substitution $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$ in die Form $lxx + 2mxy + nyy$ transformiert, so sagen wir einfach, (L, M, N) werde in (l, m, n) durch die Substitution $\alpha, \beta, \gamma, \delta$ transformiert. So brauchen wir die Unbestimmten der einzelnen betrachteten Formen nicht mit eigenen Zeichen zu bezeichnen. — Dabei muss aber die *erste* Unbestimmte in jeder Form sorgfältig von der *zweiten* unterschieden werden.

Gegeben sei die reduzierte Form $(a, b, -a') \dots f$ mit Determinante D. Wie in Artikel 186 bilde man die nach beiden Seiten unendliche Folge reduzierter Formen $\dots .{}''f, {}'f, f, f', f'' \dots .$, und zwar sei

$$\begin{aligned} f' &= (-a', b', a''), \quad f'' = (a'', b'', -a''') \quad \text{usw.} \\ {}'f &= (-{}'a, {}'b, a), \quad {}''f = ({}''a, {}''b, -{}'a) \quad \text{usw.} \end{aligned}$$

Man setze

$$\begin{aligned} \frac{b + b'}{-a'} &= h', \quad \frac{b' + b''}{a''} = h'', \quad \frac{b'' + b'''}{-a'''} = h''' \quad \text{usw.} \\ \frac{{}'b + b}{a} &= h, \quad \frac{{}''b + {}'b}{-{}'a} = {}'h, \quad \frac{{}'''b + {}''b}{{}''a} = {}''h \quad \text{usw.} \end{aligned}$$

Dann wird offenbar, wenn die Zahlen $\alpha', \alpha'', \alpha'''$ usw., $\beta', \beta'', \beta'''$ usw. und so weiter (wie in Artikel 177) nach dem folgenden Algorithmus gebildet werden,

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta & \delta'' = h''\delta' - 1 \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' \end{array}$$

usw.

f transformiert

in	f'	durch die Substitution	$\alpha',\ \beta',\ \gamma',\ \delta'$
	f''	.....	$\alpha'',\ \beta'',\ \gamma'',\ \delta''$
	f'''	.....	$\alpha''',\ \beta''',\ \gamma''',\ \delta'''$

usw.

und alle diese Transformationen sind eigentlich.

Da $'f$ in f durch die eigentliche Substitution $0, -1, 1, h$ übergeht (Artikel 158), geht f in $'f$ durch die eigentliche Substitution $h, 1, -1, 0$ über. Aus ähnlichem Grund geht $'f$ in $''f$ durch die eigentliche Substitution $'h, 1, -1, 0$ über, $''f$ in $'''f$ durch die eigentliche Substitution $''h, 1, -1, 0$ usw. Daraus folgt nach Artikel 159 auf dieselbe Weise wie in Artikel 177: Werden die Zahlen $'\alpha, ''\alpha, '''\alpha$ usw., $'\beta, ''\beta, '''\beta$ usw. und so weiter nach dem folgenden Algorithmus gebildet,

$$\begin{array}{llll} '\alpha = h & '\beta = 1 & '\gamma = -1 & '\delta = 0 \\ ''\alpha = 'h'\alpha - 1 & ''\beta = '\alpha & ''\gamma = 'h'\gamma & ''\delta = '\gamma \\ '''\alpha = ''h''\alpha - '\alpha & '''\beta = ''\alpha & '''\gamma = ''h''\gamma - '\gamma & '''\delta = ''\gamma \\ ''''\alpha = '''h'''\alpha - ''\alpha & ''''\beta = '''\alpha & ''''\gamma = '''h'''\gamma - ''\gamma & ''''\delta = '''\gamma \end{array}$$

usw.

so wird f transformiert

$$\begin{array}{llll} \text{in} & 'f & \text{durch die Substitution} & '\alpha,\ '\beta,\ '\gamma,\ '\delta \\ & ''f & \ldots\ldots\ldots & ''\alpha,\ ''\beta,\ ''\gamma,\ ''\delta \\ & '''f & \ldots\ldots\ldots & '''\alpha,\ '''\beta,\ '''\gamma,\ '''\delta \end{array}$$

usw.

und alle diese Transformationen sind eigentlich.

Setzt man $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$, so stehen diese Zahlen zur Form f in derselben Beziehung wie $\alpha', \beta', \gamma', \delta'$ zu f', $\alpha'', \beta'', \gamma'', \delta''$ zu f'' usw., $'\alpha, '\beta, '\gamma, '\delta$ zu $'f$ usw. Durch die Substitution $\alpha, \beta, \gamma, \delta$ geht nämlich die Form f in f über. Die unendlichen Folgen $\alpha', \alpha'', \alpha'''$ usw., $'\alpha, ''\alpha, '''\alpha$ usw. lassen sich dann durch Einschieben des Gliedes α so verbinden, dass man sie als eine einzige zusammenhängende, nach beiden Seiten unendliche Folge auffassen kann, die überall demselben Gesetz folgt: $\ldots '''\alpha, ''\alpha, '\alpha, \alpha, \alpha', \alpha'', \alpha''' \ldots$. Dieses Gesetz lautet

$$'''\alpha + '\alpha = ''h''\alpha, \quad ''\alpha + \alpha = 'h'\alpha, \quad '\alpha + \alpha' = h\alpha,$$
$$\alpha + \alpha'' = h'\alpha', \quad \alpha' + \alpha''' = h''\alpha'' \text{ usw.}$$

oder allgemein (wenn ein rechts geschriebener negativer Index dasselbe bedeuten soll wie ein links geschriebener positiver)

$$\alpha^{m-1} + \alpha^{m+1} = h^m \alpha^m$$

Ebenso ist die Folge $\ldots ''\beta, '\beta, \beta, \beta', \beta'' \ldots$ zusammenhängend; ihr Gesetz lautet

$$\beta^{m-1} + \beta^{m+1} = h^{m+1} \beta^m$$

und sie ist im Wesentlichen mit der vorigen identisch, wobei alle Glieder um eine Stelle verschoben sind: $''\beta = '\alpha$, $'\beta = \alpha$, $\beta = \alpha'$ usw. Das Gesetz der zusammenhängenden Folge $\ldots . ''\gamma, '\gamma, \gamma, \gamma', \gamma'' \ldots .$ lautet

$$\gamma^{m-1} + \gamma^{m+1} = h^m \gamma^m$$

und das Gesetz von $\ldots ''\delta, '\delta, \delta, \delta', \delta'' \ldots$ lautet

$$\delta^{m-1} + \delta^{m+1} = h^{m+1} \delta^m$$

außerdem gilt allgemein $\delta^m = \gamma^{m+1}$.

Beispiel. Die gegebene Form f sei $(3, 8, -5)$. Sie wird transformiert

in die Form		durch die Substitution
$''''''f$	$(-10, 7, 3)$	$-805,\ -152,\ +143,\ +27$
$'''''f$	$(3, 8, -5)$	$-152,\ +45,\ +27,\ -8$
$''''f$	$(-5, 7, 6)$	$+45,\ +17,\ -8,\ -3$
$'''f$	$(6, 5, -9)$	$+17,\ -11,\ -3,\ +2$
$''f$	$(-9, 4, 7)$	$-11,\ -6,\ +2,\ +1$
$'f$	$(7, 3, -10)$	$-6,\ +5,\ +1,\ -1$
f	$(-10, 7, 3)$	$+5,\ +1,\ -1,\ 0$
f'	$(3, 8, -5)$	$+1,\ 0,\ 0,\ +1$
f''	$(-5, 7, 6)$	$0,\ -1,\ +1,\ -3$
f'''	$(6, 5, -9)$	$-1,\ -2,\ -3,\ -7$
f''''	$(-9, 4, 7)$	$-2,\ +3,\ -7,\ +10$
f'''''	$(7, 3, -10)$	$+3,\ +5,\ +10,\ +17$
f''''''	$(-10, 7, 3)$	$+5,\ -8,\ +17,\ -27$
f'''''''	$(3, 8, -5)$	$-8,\ -45,\ -27,\ -152$
f''''''''	$(-5, 7, 6)$	$-45,\ +143,\ -152,\ +483$

usw.

189.

Zu diesem Algorithmus ist Folgendes anzumerken.

1) Alle a, a', a'' usw., $'a, ''a$ usw. haben dasselbe Vorzeichen; alle b, b', b'' usw., $'b, ''b$ usw. sind positiv. In der Folge $\ldots ''h, 'h, h, h', h'' \ldots$ wechseln die Vorzeichen ab: Sind alle a, a' usw. positiv, so ist h^m oder ${}^m h$ für gerades m positiv und für ungerades m negativ; sind dagegen a, a' usw. negativ, so ist h^m oder ${}^m h$ für gerades m negativ und für ungerades positiv.

2) Ist a positiv und damit h' negativ, h'' positiv usw., so ist $\alpha'' = -1$ negativ, $\alpha''' = h''\alpha''$ negativ und $> \alpha''$ (oder $= \alpha''$, wenn $h'' = 1$); $\alpha'''' = h'''\alpha''' - \alpha''$ positiv und $> \alpha'''$ (weil $h'''\alpha'''$ positiv und α'' negativ ist); $\alpha''''' = h''''\alpha'''' - \alpha'''$ positiv und $> \alpha''''$ (weil $h''''\alpha''''$ positiv ist) usw. Daraus folgt leicht, dass die Folge $\alpha', \alpha'', \alpha'''$ usw. ins Unendliche wächst und stets zwei positive Vorzeichen auf zwei negative folgen, sodass α^m das Vorzeichen $+, +, -, -$ hat, je nachdem $m \equiv 0, 1, 2, 3 \pmod 4$. Ist a negativ, so erhält man durch einen ähnlichen Schluss α'' negativ, α''' positiv und entweder $>$ oder $= \alpha''$; α'''' positiv und $> \alpha'''$; α''''' negativ und $> \alpha''''$ usw., sodass die Folge $\alpha', \alpha'', \alpha'''$ usw. fortwährend wächst und das Glied α^m das Vorzeichen $+, -, -, +$ hat, je nachdem $m \equiv 0, 1, 2, 3 \pmod 4$.

3) Auf diese Weise findet man, dass alle vier unendlichen Folgen $\alpha', \alpha'', \alpha'''$ usw., $\gamma, \gamma', \gamma''$ usw.; $\alpha', \alpha, {}'\alpha, {}''\alpha$ usw.; $\gamma, {}'\gamma, {}''\gamma$ usw. fortwährend wachsen, also auch die folgenden, mit ihnen identischen Folgen: β, β', β'' usw.; ${}'\delta, \delta, \delta', \delta''$ usw.; $\beta, {}'\beta, {}''\beta$ usw.; ${}'\delta, {}''\delta$ usw. Je nachdem $m \equiv 0, 1, 2, 3 \pmod 4$, lauten die Vorzeichen

$$\begin{array}{llll} \text{von } \alpha^m, & + \pm - \mp; & \text{von } \beta^m, & \pm - \mp + \\ \text{von } \gamma^m, & \pm + \mp -; & \text{von } \delta^m, & + \mp - \pm \\ \text{von } {}^m\alpha, & + \pm - \mp; & \text{von } {}^m\beta, & \mp + \pm - \\ \text{von } {}^m\gamma, & \mp - \pm +; & \text{von } {}^m\delta, & + \mp - \pm \end{array}$$

wobei die oberen Vorzeichen für positives a, die unteren für negatives a gelten. Besonders ist folgende Eigenschaft zu beachten: Bezeichnet m einen beliebigen positiven Index, so haben α^m und γ^m dasselbe Vorzeichen, wenn a positiv ist. Entgegengesetzte, wenn a negativ ist, und ebenso β^m und δ^m; dagegen haben ${}^m\alpha$ und ${}^m\gamma$ oder ${}^m\beta$ und ${}^m\delta$ dasselbe Vorzeichen, wenn a negativ ist, und entgegengesetzte, wenn a positiv ist.

4) In der Bezeichnung von Artikel 27 lässt sich die Größe von α^m usw. bequem so ausdrücken. Man setze

$$\mp h' = k', \quad \pm h'' = k'', \quad \mp h''' = k''' \text{ usw.}$$
$$\pm h = k, \quad \mp' h = {}'k, \quad \pm'' h = {}''k \text{ usw.}$$

sodass alle k', k'' usw., $k, {}'k$ usw. positive Zahlen sind:

$$\alpha^m = \pm[k'', k''', k'''' \ldots k^{m-1}]; \quad \beta^m = \pm[k'', k''', k'''' \ldots k^m]$$
$$\gamma^m = \pm[k', k'', k''' \ldots . k^{m-1}]; \quad \delta^m = \pm[k', k'', k''' \ldots . k^m]$$
$${}^m\alpha = \pm[k, {}'k, {}''k \ldots . . {}^{m-1}k]; \quad {}^m\beta = \pm[k, {}'k, {}''k \ldots . {}^{m-2}k]$$
$${}^m\gamma = \pm[{}'k, {}''k \ldots . . {}^{m-1}k]; \qquad {}^m\delta = \pm[{}'k, {}''k \ldots . {}^{m-2}k]$$

Die *Vorzeichen* müssen aber nach den gerade angegebenen Regeln bestimmt werden. Mit diesen Formeln, deren Beweis wir wegen seiner Einfachheit weglassen, lässt sich die Rechnung stets sehr schnell durchführen.

190.

Hilfssatz. *Bezeichnen m, μ, m', n, ν, n' beliebige ganze Zahlen, von denen aber keine der letzten drei $= 0$ ist, so behaupte ich: Liegt $\frac{\mu}{\nu}$ streng zwischen $\frac{m}{n}$ und $\frac{m'}{n'}$ und gilt $mn' - nm' = \mp 1$, so ist der Nenner ν größer als n und n'.*

Beweis. Offenbar liegt $\mu n n'$ zwischen $\nu m n'$ und $\nu n m'$ und unterscheidet sich daher von jeder Grenze um weniger als die Grenzen voneinander; *das heißt*, es gilt $\nu m n' - \nu n m' > \mu n n' - \nu m n'$ und $> \mu n n' - \nu n m'$, oder $\nu > n'(\mu n - \nu m)$ und $> n(\mu n' - \nu m')$. Da $\mu n - \nu m$ sicher nicht $= 0$ ist (sonst wäre $\frac{\mu}{\nu} = \frac{m}{n}$, im Widerspruch zur Voraussetzung), auch nicht $\mu n' - \nu m' = 0$ (aus ähnlichem Grund), sondern beide mindestens $= 1$ sind, folgt $\nu > n'$ und $> n$. *W. z. b. w.*

Also kann ν offenbar nicht $= 1$ sein; *das heißt*, gilt $mn' - nm' = \pm 1$, so kann zwischen den Brüchen $\frac{m}{n}$, $\frac{m'}{n'}$ keine ganze Zahl liegen. Daher kann auch die Null nicht zwischen ihnen liegen, *das heißt*, diese Brüche können keine entgegengesetzten Vorzeichen haben.

191.

Satz. *Geht eine reduzierte Form* $(a, b, -a')$ *mit Determinante* D *durch die Substitution* $\alpha, \beta, \gamma, \delta$ *in die reduzierte Form* $(A, B, -A')$ *mit derselben Determinante über, so liegt* erstens $\frac{\pm\sqrt{D}-b}{a}$ *zwischen* $\frac{\alpha}{\gamma}$ *und* $\frac{\beta}{\delta}$ *(sofern weder* γ *noch* $\delta = 0$ *ist, also beide Grenzen endlich sind), wobei das obere Vorzeichen zu nehmen ist, wenn keine der beiden Grenzen das zu* a *entgegengesetzte Vorzeichen hat (oder deutlicher: wenn entweder beide das Vorzeichen dieses Koeffizienten haben oder eine dieses Vorzeichen hat und die andere* $= 0$ *ist), das untere, wenn keine dasselbe Vorzeichen hat wie* a*;* zweitens $\frac{\pm\sqrt{D}+b}{a'}$ *zwischen* $\frac{\gamma}{\alpha}$ *und* $\frac{\delta}{\beta}$ *(sofern weder* α *noch* $\beta = 0$ *ist), wobei das obere Vorzeichen zu nehmen ist, wenn keine Grenze das zu* a' *(oder* a*) entgegengesetzte Vorzeichen hat, das untere, wenn keine dasselbe Vorzeichen hat wie* a'[*)]*.*

Beweis. Wir haben die Gleichungen

$$a\alpha\alpha + 2b\alpha\gamma - a'\gamma\gamma = A \quad \ldots\ldots\ldots \quad [1]$$
$$a\beta\beta + 2b\beta\delta - a'\delta\delta = -A' \quad \ldots\ldots\ldots \quad [2]$$

Daraus folgt

$$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{\left(D + \frac{aA}{\gamma\gamma}\right)} - b}{a} \quad \ldots\ldots\ldots \quad [3]$$
$$\frac{\beta}{\delta} = \frac{\pm\sqrt{\left(D - \frac{aA'}{\delta\delta}\right)} - b}{a} \quad \ldots\ldots\ldots \quad [4]$$
$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{\left(D - \frac{a'A}{\alpha\alpha}\right)} + b}{a'} \quad \ldots\ldots\ldots \quad [5]$$
$$\frac{\delta}{\beta} = \frac{\pm\sqrt{\left(D + \frac{a'A'}{\beta\beta}\right)} + b}{a'} \quad \ldots\ldots\ldots \quad [6]$$

Die Gleichung 3, 4. 5, 6 ist jeweils wegzulassen, wenn $\gamma, \delta, \alpha, \beta$ entsprechend $= 0$ ist. — Es bleibt aber offen, welche *Vorzeichen* den Wurzelgrößen zu geben sind. Dies entscheiden wir so.

In [3] und [4] müssen offenbar die oberen Vorzeichen genommen werden, wenn weder $\frac{\alpha}{\gamma}$ noch $\frac{\beta}{\delta}$ das zu a entgegengesetzte Vorzeichen hat; denn beim unteren Vorzeichen würden $\frac{a\alpha}{\gamma}$ und $\frac{a\beta}{\delta}$ negative Größen. Da aber A und A' dasselbe Vorzeichen haben, liegt $\sqrt{D}$ zwischen $\sqrt{\left(D+\frac{aA}{\gamma\gamma}\right)}$ und $\sqrt{\left(D-\frac{aA'}{\delta\delta}\right)}$ und daher in diesem Fall $\frac{\sqrt{D}-b}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$. Damit ist der erste Teil des Satzes für den ersten Fall bewiesen.

Ebenso sieht man, dass in [5] und [6] die unteren Vorzeichen genommen werden müssen, wenn weder $\frac{\gamma}{\alpha}$ noch $\frac{\delta}{\beta}$ dasselbe Vorzeichen hat wie a' oder a, denn beim oberen Vorzeichen würden $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\beta}$ notwendig positive Größen. Daraus folgt sofort, dass $\frac{-\sqrt{D}+b}{a'}$ in diesem Fall zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ liegt. Damit ist auch der zweite Teil des Satzes für den zweiten Fall bewiesen. Ließe sich ebenso leicht zeigen, dass in [3] und [4] die unteren Vorzeichen zu nehmen sind, wenn keine der Größen $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$

[*)] Andere Fälle können offenbar nicht auftreten, da nach dem vorigen Artikel wegen $\alpha\delta - \beta\gamma = \pm 1$ die beiden Grenzen weder entgegengesetzte Vorzeichen haben noch beide zugleich $= 0$ sein können.

dasselbe Vorzeichen hat wie a, und in [5] und [6] die oberen, wenn weder $\frac{\gamma}{\alpha}$ noch $\frac{\delta}{\beta}$ das entgegengesetzte Vorzeichen hat, so würde ebenso folgen, dass im ersteren Fall $\frac{-\sqrt{D-b}}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ liegt, im letzteren $\frac{\sqrt{D+b}}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$. Dann wären der erste Teil auch für den zweiten Fall und der zweite Teil für den ersten Fall bewiesen. Obwohl das nicht schwierig ist, geht es aber nicht ohne einige Umwege. Wir ziehen die folgende Methode vor.

Ist keine der Zahlen $\alpha, \beta.\gamma, \delta = 0$, so haben $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ dieselben Vorzeichen wie $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$. Hat also keine dieser Größen dasselbe Vorzeichen wie a' oder a, sodass $\frac{-\sqrt{D+b}}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ liegt, so hat keine der Größen $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ dasselbe Vorzeichen wie a, und $\frac{a'}{-\sqrt{D+b}} = \frac{-\sqrt{D-b}}{a}$ liegt (wegen $aa' = D - bb$) zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$. Damit ist, sofern weder α noch $\beta = 0$ ist, der erste Teil des Satzes auch für den zweiten Fall bewiesen (denn die Bedingung, dass weder γ noch $\delta = 0$ ist, steht bereits im Satz selbst). Ebenso hat, wenn keine der Zahlen $\alpha, \beta, \gamma, \delta = 0$ ist und weder $\frac{\alpha}{\gamma}$ noch $\frac{\beta}{\delta}$ das zu a oder a' entgegengesetzte Vorzeichen hat, sodass $\frac{\sqrt{D-b}}{a'}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ liegt, auch keine der Größen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ das zu a' entgegengesetzte Vorzeichen, und $\frac{a}{\sqrt{D-b}} = \frac{\sqrt{D+b}}{a'}$ liegt zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$. Damit ist für den Fall, dass weder γ noch $\delta = 0$ ist, der zweite Teil des Satzes auch für den zweiten Fall bewiesen.

Es bliebe also nur zu beweisen, dass der erste Teil des Satzes auch für den zweiten Fall gilt, wenn eine der Zahlen $\alpha, \beta = 0$ ist, und der zweite Teil für den ersten Fall, wenn entweder γ oder $\delta = 0$ ist. Aber *alle diese Fälle sind unmöglich*. Für den *ersten* Teil des Satzes nehmen wir an, weder γ noch $\delta = 0$ sei, $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ hätten nicht dasselbe Vorzeichen wie a, und es sei 1) $\alpha = 0$. Dann folgt aus der Gleichung $\alpha\delta - \beta\gamma = \pm 1$, dass $\beta = \pm 1$, $\gamma = \pm 1$ ist. Aus [1] folgt $A = -a'$, also haben A und a' und damit auch a und A' entgegengesetzte Vorzeichen; daher gilt $\sqrt{\left(D - \frac{aA'}{\delta\delta}\right)} > \sqrt{D} > b$. In [4] ist somit das untere Vorzeichen zu nehmen, denn beim oberen hätte $\frac{\beta}{\delta}$ offenbar dasselbe Vorzeichen wie a. Also gilt $\frac{\beta}{\delta} > \frac{-\sqrt{D-b}}{a} > 1$ (weil nach der Definition einer reduzierten Form $a < \sqrt{D}+b$ ist), *was widersinnig ist*, da $\beta = \pm 1$ und δ nicht $= 0$ ist. — 2) Sei $\beta = 0$. Dann folgt aus der Gleichung $\alpha\delta - \beta\gamma = \pm 1$, dass $\alpha = \pm 1$, $\delta = \pm 1$ ist. Aus [2] folgt $-A' = -a'$, sodass a' und a und A dasselbe Vorzeichen haben; daher gilt $\sqrt{\left(D + \frac{aA}{\alpha\alpha}\right)} > \sqrt{D} > b$. In [3] ist somit das untere Vorzeichen zu nehmen, denn beim oberen hätte $\frac{\alpha}{\gamma}$ dasselbe Vorzeichen wie a. Also gilt $\frac{\alpha}{\gamma} > \frac{-\sqrt{D-b}}{a} > 1$, *was widersinnig ist*, aus demselben Grund wie zuvor. — Für den *zweiten* Teil nehmen wir an, weder α noch $\beta = 0$ sei, $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$ hätten nicht das zu a' entgegengesetzte Vorzeichen, und es sei 1) $\gamma = 0$. Aus der Gleichung $\alpha\delta - \beta\gamma = \pm 1$ folgt $\alpha = \pm 1$, $\delta = \pm 1$. Aus [1] folgt $A = a$, sodass a' und A' dasselbe Vorzeichen haben; daher gilt $\sqrt{\left(D + \frac{a'A'}{\beta\beta}\right)} > \sqrt{D} > b$. In [6] ist also das obere Vorzeichen zu nehmen, denn beim unteren hätte $\frac{\delta}{\beta}$ das zu a' entgegengesetzte Vorzeichen. Somit gilt $\frac{\delta}{\beta} > \frac{\sqrt{D+b}}{a'} > 1$, *was widersinnig ist*, da $\delta = \pm 1$ und β nicht $= 0$ ist. Ist schließlich 2) $\delta = 0$, so folgt aus $\alpha\delta - \beta\gamma = \pm 1$, dass $\beta = \pm 1$, $\gamma = \pm 1$ ist, und damit aus [2], dass $-A' = a$. Daraus folgt $\sqrt{\left(D - \frac{a'A}{\alpha\alpha}\right)} > \sqrt{D} > b$, weshalb in [5] das obere Vorzeichen zu nehmen ist. Also gilt $\frac{\gamma}{\alpha} > \frac{\sqrt{D+b}}{a'} > 1$, *was widersinnig ist*. — Damit ist der Satz in seinem ganzen Umfang bewiesen.

Da die Differenz zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta} = \frac{1}{\gamma\delta}$ ist, ist die Differenz zwischen $\frac{\pm\sqrt{D}-b}{a}$ und $\frac{\alpha}{\gamma}$ oder $\frac{\beta}{\delta} < \frac{1}{\gamma\delta}$; und zwischen $\frac{\pm\sqrt{D}-b}{a}$ und $\frac{\alpha}{\gamma}$ oder zwischen jener Größe und $\frac{\beta}{\delta}$ kann kein Bruch liegen, dessen Nenner nicht größer als γ oder δ ist (*voriger Hilfssatz*). — Ebenso ist die Differenz der Größe $\frac{\pm\sqrt{D}+b}{a}$ zum Bruch $\frac{\gamma}{\alpha}$ oder $\frac{\delta}{\beta}$ kleiner als $\frac{1}{\alpha\beta}$, und zwischen jener Größe und einem dieser Brüche kann kein Bruch liegen, dessen Nenner nicht größer als α und β ist.

192.

Wendet man den vorigen Satz auf den Algorithmus von Artikel 188 an, so folgt, dass die Größe $\frac{\sqrt{D}-b}{a}$, die wir mit L bezeichnen, zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$, zwischen $\frac{\alpha''}{\gamma''}$ und $\frac{\beta''}{\delta''}$, zwischen $\frac{\alpha'''}{\gamma'''}$ und $\frac{\beta'''}{\delta'''}$ usw. liegt (denn aus dem Ende von Artikel 189, 3 folgt leicht, dass keine dieser Grenzen das zu a entgegengesetzte Vorzeichen hat, weshalb der Wurzelgröße $\sqrt{D}$ das positive Vorzeichen zu geben ist), also zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\alpha''}{\gamma''}$, zwischen $\frac{\alpha''}{\gamma''}$ und $\frac{\alpha'''}{\gamma'''}$ usw. Daher liegen alle Brüche $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha'''''}{\gamma'''''}$ usw. auf derselben Seite von L und alle $\frac{\alpha''}{\gamma''}$, $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha''''''}{\gamma''''''}$ usw. auf der anderen. Da aber $\gamma' < \gamma'''$ gilt, liegt $\frac{\alpha'}{\gamma'}$ *außerhalb* des Intervalls zwischen $\frac{\alpha'''}{\gamma'''}$ und L, und aus ähnlichem Grund $\frac{\alpha''}{\gamma''}$ außerhalb von L und $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha'''}{\gamma'''}$ außerhalb von L und $\frac{\alpha'''''}{\gamma'''''}$ usw. Daher liegen diese Größen offenbar in folgender Reihenfolge:

$$\frac{\alpha'}{\gamma'},\ \frac{\alpha'''}{\gamma'''},\ \frac{\alpha'''''}{\gamma'''''} \ldots L \ldots \frac{\alpha''''''}{\gamma''''''},\ \frac{\alpha''''}{\gamma''''},\ \frac{\alpha''}{\gamma''}$$

Die Differenz zwischen $\frac{\alpha'}{\gamma'}$ und L ist aber kleiner als die Differenz zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\alpha''}{\gamma''}$, *das heißt*, $< \frac{1}{\gamma'\gamma''}$, und ebenso ist die Differenz zwischen $\frac{\alpha''}{\gamma''}$ und $L < \frac{1}{\gamma''\gamma'''}$ usw. Daher nähern sich die Brüche $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ usw. der Grenze L immer mehr, und da $\gamma', \gamma'', \gamma'''$ fortwährend ins Unendliche wachsen, kann die Differenz der Brüche zur Grenze kleiner als jede gegebene Größe werden.

Nach Artikel 189 hat keine der Größen $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$ usw. dasselbe Vorzeichen wie a. Durch einen ganz ähnlichen Schluss wie zuvor folgt daraus, dass jene Größen und $\frac{-\sqrt{D}+b}{a'}$, die wir mit L' bezeichnen, in folgender Reihenfolge liegen:

$$\frac{\gamma}{\alpha},\ \frac{''\gamma}{''\alpha},\ \frac{''''\gamma}{''''\alpha} \ldots\ldots L' \ldots\ldots \frac{''''\gamma}{''''\alpha},\ \frac{'''\gamma}{'''\alpha},\ \frac{'\gamma}{'\alpha}$$

Die Differenz zwischen $\frac{\gamma}{\alpha}$ und L' ist kleiner als $\frac{1}{'\alpha\alpha}$, die Differenz zwischen $\frac{'\gamma}{'\alpha}$ und L' kleiner als $\frac{1}{''\alpha'\alpha}$ usw. Daher nähern sich die Brüche $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$ usw. immer mehr L', und die Differenz kann kleiner als jede gegebene Größe werden.

Im *Beispiel* von Artikel 188 gilt $L = \frac{\sqrt{79}-8}{3} = 0{,}2960648$, und die Näherungsbrüche sind $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{5}{17}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$ usw. Dabei ist $\frac{143}{483} = 0{,}2960662$. — Dort gilt auch $L' = \frac{-\sqrt{79}+8}{5} = -0{,}1776388$, und die Näherungsbrüche sind $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$, $-\frac{8}{45}$, $-\frac{27}{152}$, $-\frac{143}{805}$ usw. Es ist aber $\frac{143}{805} = 0{,}1776397$.

193.

Satz. *Sind die reduzierten Formen f, F eigentlich äquivalent, so ist die eine in der Periode der anderen enthalten.*

Sei $f = (a, b, -a')$, $F = (A, B, -A')$, die Determinante dieser Formen sei D, und die erste gehe durch die eigentliche Substitution $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ in die zweite über. Dann behaupte ich: Wenn wir die Periode der Form f suchen und wie in Artikel 188 die nach beiden Seiten unendliche Folge der reduzierten Formen und der Transformationen von f in diese bestimmen, so ist *entweder* $+\mathfrak{A}$ einem Glied der Folge $\ldots {}''\alpha, {}'\alpha, \alpha, \alpha', \alpha'' \ldots$ gleich, und wenn wir dieses $= \alpha^m$ setzen, ist $+\mathfrak{B} = \beta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$; *oder* $-\mathfrak{A}$ ist einem Glied α^m gleich, und $-\mathfrak{B}, -\mathfrak{C}, -\mathfrak{D}$ sind der Reihe nach $= \beta^m, \gamma^m, \delta^m$ (wobei m auch einen negativen Index bezeichnen kann). In beiden Fällen ist F offenbar mit f^m identisch.

Beweis. I. Wir haben die vier Gleichungen

$$a\mathfrak{A}\mathfrak{A} + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}\mathfrak{C} = A \quad \ldots\ldots \qquad [1]$$

$$a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B \quad \ldots\ldots \qquad [2]$$

$$a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D} = -A' \quad \ldots\ldots \qquad [3]$$

$$\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1 \quad \ldots\ldots\ldots \qquad [4]$$

Wir betrachten *zuerst* den Fall, dass eine der Zahlen $\mathfrak{A}\ \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$ ist.

1° Ist $\mathfrak{A} = 0$, so folgt aus [4] $\mathfrak{B}\mathfrak{C} = -1$, also $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Dann ergibt [1] $-a' = A$ und [2] $-b \pm a'\mathfrak{D} = B$ oder $B \equiv -b \pmod{a' \text{ oder } A}$. Daraus folgt, dass die Form $(A, B, -A')$ der Form $(a, b, -a')$ nach rechts benachbart ist. Da die erste reduziert ist, muss sie mit f' identisch sein. Also ist $B = b'$, und aus [2] folgt $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; wegen $\frac{b+b'}{-a'} = h'$ erhalten wir $\mathfrak{D} = \mp h'$. Wir schließen, dass $\mp\mathfrak{A}, \mp\mathfrak{B}, \mp\mathfrak{C}, \mp\mathfrak{D}$ der Reihe nach $= 0, -1, +1, h'$ oder $= \alpha', \beta', \gamma', \delta'$ sind.

2° Ist $\mathfrak{B} = 0$, so ergibt [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; [3] ergibt $a' = A'$; und [2] ergibt $b \mp a'\mathfrak{C} = B$ oder $b \equiv B \pmod{a'}$. Da sowohl f als auch F reduzierte Formen sind, liegen sowohl b als auch B zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$ (je nachdem, ob a' positiv oder negativ ist, Artikel 185, 5). Daher muss $b = B$ und $\mathfrak{C} = 0$ sein. Somit sind die Formen f, F identisch, und es gilt der Reihe nach $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D} = 1, 0, 0, 1 = \alpha, \beta, \gamma\ \delta$.

3° Ist $\mathfrak{C} = 0$, so ergibt [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; [1] ergibt $a = A$; und [2] ergibt $\pm a\mathfrak{B} + b = B$ oder $b \equiv B \pmod{a}$. Da aber sowohl b als auch B zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$ liegen, muss $B = b$ und $\mathfrak{B} = 0$ sein. Dieser Fall unterscheidet sich also nicht vom vorhergehenden.

4° Ist $\mathfrak{D} = 0$, so ergibt [4] $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; [3] ergibt $a = -A'$; und [2] ergibt $\pm a\mathfrak{A} - b = B$ oder $B \equiv -b \pmod{a}$. Daher ist F der Form f nach links benachbart und somit mit der Form ${}'f$ identisch. Wegen $\frac{{}'b+b}{a} = h$ und $B = {}'b$ erhalten wir $\pm\mathfrak{A} = h$. Wir schließen, dass $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D}$ der Reihe nach $= h, 1, -1, 0, = {}'\alpha, {}'\beta, {}'\gamma, {}'\delta$ sind.

Es bleibt der Fall, dass keine der Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$ ist. Nach dem Hilfssatz in Artikel 190 haben dann die Größen $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$, $\frac{\mathfrak{D}}{\mathfrak{B}}$ dasselbe Vorzeichen. Daraus ergeben sich zwei Fälle, denn dieses Vorzeichen kann entweder mit dem von a, a' übereinstimmen oder ihm entgegengesetzt sein.

II. Haben $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ dasselbe Vorzeichen wie a, so liegt die Größe $\frac{\sqrt{D}-b}{a}$ (die wir mit L bezeichnen werden) zwischen diesen Brüchen (Artikel 191). Wir werden nun be-

weisen, dass $\frac{\mathfrak{A}}{\mathfrak{C}}$ einem der Brüche $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha''''}{\gamma''''}$ usw. gleich ist und $\frac{\mathfrak{B}}{\mathfrak{D}}$ dem unmittelbar folgenden; ist also $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$, so ist $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}}$. Im vorhergehenden Artikel haben wir gezeigt, dass die Größen $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ usw. (die wir kurz mit (1), (2), (3) usw. bezeichnen werden) zusammen mit L die folgende Reihenfolge (I) einhalten: $(1), (3), (5) \ldots L \ldots (6), (4), (2)$. Die erste dieser Größen ist $= 0$ (wegen $\alpha' = 0$); alle anderen haben dasselbe Vorzeichen wie L oder a. Nach Voraussetzung haben aber $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ (für die wir $\mathfrak{M}, \mathfrak{N}$ schreiben werden) dasselbe Vorzeichen. Offenbar liegen diese Größen also rechts von (1) (oder, wenn man lieber will, auf derselben Seite wie L); da L zwischen ihnen liegt, liegt die eine rechts von L, die andere links davon. Wir können leicht zeigen, dass $\mathfrak{M}$ nicht rechts von (2) liegen kann. Sonst läge nämlich $\mathfrak{N}$ zwischen (1) und L. Daraus würde *erstens* folgen, dass (2) zwischen $\mathfrak{M}$ und $\mathfrak{N}$ liegt und daher der Nenner des Bruchs (2) größer ist als der von $\mathfrak{N}$ (Artikel 190); *zweitens*, dass $\mathfrak{N}$ zwischen (1) und (2) liegt und daher der Nenner von $\mathfrak{N}$ größer ist als der von (2). *Das ist ein Widerspruch.*

Nehmen wir an, $\mathfrak{M}$ sei keinem der Brüche (2), (3), (4) usw. gleich, und sehen wir, was daraus folgt. Liegt der Bruch $\mathfrak{M}$ links von L, so muss er offenbar entweder zwischen (1) und (3), zwischen (3) und (5), zwischen (5) und (7) usw. liegen (denn L ist irrational, also sicher von $\mathfrak{M}$ verschieden, und die Brüche (1), (3), (5) usw. können L näher kommen als jede gegebene Größe, die von L verschieden ist). Liegt dagegen $\mathfrak{M}$ rechts von L, so liegt es notwendig entweder zwischen (2) und (4), zwischen (4) und (6), zwischen (6) und (8) usw. Nehmen wir also an, $\mathfrak{M}$ liege zwischen (m) und $(m+2)$. Offenbar liegen dann die Größen $\mathfrak{M}, (m), (m+1), (m+2), L$ in der folgenden Reihenfolge:

$$(\text{II})^{*)}: \qquad (m),\ (\mathfrak{M}),\ (m+2),\ L,\ (m+1)$$

Dann muss $\mathfrak{N} = (m+1)$ sein. Denn $\mathfrak{N}$ liegt rechts von L. Läge es aber auch rechts von $(m+1)$, so läge $(m+1)$ zwischen $\mathfrak{M}$ und $\mathfrak{N}$, woraus $\gamma^{m+1} > \mathfrak{C}$ folgt; dagegen läge $\mathfrak{M}$ zwischen (m) und $(m+1)$, woraus $\mathfrak{C} > \gamma^{m+1}$ folgt (Artikel 190), *ein Widerspruch.* Läge dagegen $\mathfrak{N}$ links von $(m+1)$, also zwischen $(m+2)$ und $(m+1)$, so wäre $\mathfrak{D} > \gamma^{m+2}$; und weil $(m+2)$ zwischen $\mathfrak{M}$ und $\mathfrak{N}$ liegt, wäre $\gamma^{m+2} > \mathfrak{D}$, *ein Widerspruch.* Also gilt $\mathfrak{N} = (m+1)$ oder $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}} = \frac{\beta^m}{\delta^m}$.

Da $\mathfrak{AD} - \mathfrak{BC} = 1$, ist $\mathfrak{B}$ zu $\mathfrak{D}$ teilerfremd, und aus demselben Grund ist β^m zu δ^m teilerfremd. Daher kann die Gleichung $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\beta^m}{\delta^m}$ offenbar nur gelten, wenn entweder $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ oder $\mathfrak{B} = -\beta^m$, $\mathfrak{D} = -\delta^m$ ist. Da nun die Form f durch die eigentliche Substitution $\alpha^m, \beta^m, \gamma^m, \delta^m$ in die Form f^m übergeht, die gleich $(\pm a^m, b^m, \mp a^{m+1})$ ist, haben wir die Gleichungen

$$a\alpha^m\alpha^m + 2b\alpha^m\gamma^m - a'\gamma^m\gamma^m = \pm a^m \quad \ldots\ldots \qquad [5]$$

$$a\alpha^m\beta^m + b(\alpha^m\delta^m + \beta^m\gamma^m) - a'\gamma^m\delta^m = b^m \quad \ldots. \qquad [6]$$

$$a\beta^m\beta^m + 2b\beta^m\delta^m - a'\delta^m\delta^m = \mp a^{m+1} \quad \ldots\ldots \qquad [7]$$

$$\alpha^m\delta^m - \beta^m\gamma^m = 1 \quad \ldots\ldots\ldots \qquad [8]$$

*)Es spielt hier keine Rolle, ob die Reihenfolge in (II) dieselbe wie in (I) oder die entgegengesetzte ist, *d.h.*, ob (m) auch in (I) links von L oder rechts davon liegt.

Daraus folgt (aus den Gleichungen 7 und 3) $\mp a^{m+1} = -A'$. Multiplizieren wir ferner Gleichung [2] mit $\alpha^m\delta^m - \beta^m\gamma^m$ und Gleichung [6] mit $\mathfrak{AD} - \mathfrak{BC}$ und subtrahieren, so bestätigt man durch Ausmultiplizieren leicht, dass

$$\begin{aligned} B - b^m = (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)\big(a\mathfrak{B}\beta^m \\ + b(\mathfrak{D}\beta^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m\big) \\ + (\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)\big(a\mathfrak{A}\alpha^m \\ + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m\big) \quad .. \end{aligned} \tag{9}$$

oder, da entweder $\beta^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$ oder $\beta^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$,

$$\begin{aligned} B - b^m &= \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D}) \\ &= \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A' \end{aligned}$$

Also gilt $B \equiv b^m \pmod{A'}$. Da aber sowohl B als auch b^m zwischen $\sqrt{D}$ und $\sqrt{D} \mp A'$ liegen, muss $B = b^m$ und daher $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$ oder $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$, *d.h.*, $\mathfrak{M} = (m)$ sein.

So haben wir aus der Annahme, $\mathfrak{M}$ sei keiner der Größen (2), (3), (4) usw. gleich, hergeleitet, dass es tatsächlich einer von ihnen gleich ist. Nehmen wir dagegen von Anfang an $\mathfrak{M} = (m)$ an, so gilt offenbar entweder $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$ oder $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. In beiden Fällen folgt aus [1] und [5] $A = \pm a^m$ und aus [9] $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)A$ oder $B \equiv b^m \pmod{A}$. Wie oben schließen wir daraus $B = b^m$ und damit $\mathfrak{B}\delta^m = \mathfrak{D}\beta^m$. Weil $\mathfrak{B}$ zu $\mathfrak{D}$ und β^m zu δ^m teilerfremd ist, gilt entweder $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ oder $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$; also folgt aus [7] $-A' = \mp a^{m+1}$. Daher sind die Formen F, f^m identisch. Mithilfe der Gleichung $\mathfrak{AD} - \mathfrak{BC} = \alpha^m\delta^m - \beta^m\gamma^m$ lässt sich aber leicht beweisen, dass wir $+\mathfrak{B} = \beta^m$, $+\mathfrak{D} = \delta^m$ setzen müssen, wenn $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$ ist; dagegen $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = -\delta^m$, wenn $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$ ist. *Damit ist die Behauptung bewiesen.*

III. Ist das Vorzeichen der Größen $\frac{\mathfrak{A}}{\mathfrak{C}}$ usw. dem von a entgegengesetzt, so ist der Beweis dem vorhergehenden so ähnlich, dass es genügt, seine Hauptpunkte anzugeben. Es liegt $\frac{-\sqrt{D}+b}{a'}$ zwischen $\frac{\mathfrak{C}}{\mathfrak{A}}$ und $\frac{\mathfrak{D}}{\mathfrak{B}}$. Der Bruch $\frac{\mathfrak{D}}{\mathfrak{B}}$ ist einem der Brüche

$$\frac{'\delta}{'\beta},\ \frac{''\delta}{''\beta},\ \frac{'''\delta}{'''\beta} \text{ usw. gleich} \quad ..... \tag{I}$$

$$\text{setzen wir diesen } = \frac{{}^m\delta}{{}^m\beta}, \qquad \frac{\mathfrak{C}}{\mathfrak{A}} \text{ ist dann } = \frac{{}^m\gamma}{{}^m\alpha} \quad ..... \tag{II}$$

Wir beweisen (I) wie folgt. Nehmen wir an, $\frac{\mathfrak{D}}{\mathfrak{B}}$ sei keinem jener Brüche gleich, so muss es zwischen zwei solchen Brüchen $\frac{{}^m\delta}{{}^m\beta}$ und $\frac{{}^{m+2}\delta}{{}^{m+2}\beta}$ liegen. Daraus folgt wie oben notwendig

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{m+1}\delta}{{}^{m+1}\beta} = \frac{{}^m\gamma}{{}^m\alpha}$$

und entweder $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$ oder $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. Da aber f durch die eigentliche Substitution ${}^m\alpha, {}^m\beta, {}^m\gamma, {}^m\delta$ in die Form

$${}^m f = (\pm {}^m a, {}^m b, \mp {}^{m-1} a)$$

übergeht, ergeben sich drei Gleichungen. Aus diesen folgt zusammen mit den Gleichungen 1, 2, 3, 4 und mit ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$ wie oben, dass das erste Glied A der Form F gleich dem ersten Glied von ${}^m f$ ist und das mittlere Glied der ersten Form dem der zweiten modulo A kongruent ist. Da beide Formen reduziert sind und somit das mittlere Glied beider zwischen $\sqrt{D}$ und $\sqrt{D} \mp A$ liegt, sind diese mittleren Glieder gleich. Daraus folgt $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$. Wir haben also hier die Richtigkeit der Behauptung (I) aus der Annahme hergeleitet, dass sie falsch sei.

Nehmen wir aber $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$ an, so beweisen wir auf genau dieselbe Weise und mit denselben Gleichungen, dass auch $\frac{{}^m\gamma}{{}^m\beta} = \frac{\mathfrak{C}}{\mathfrak{A}}$ gilt, was (II) besagte. Mithilfe der Gleichungen $\mathfrak{AD} - \mathfrak{BC} = 1$, ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$ folgt daraus, dass entweder

$$\mathfrak{A} = {}^m\alpha,\ \mathfrak{B} = {}^m\beta,\ \mathfrak{C} = {}^m\gamma,\ \mathfrak{D} = {}^m\delta$$

oder

$$-\mathfrak{A} = {}^m\alpha,\ -\mathfrak{B} = {}^m\beta,\ -\mathfrak{C} = {}^m\gamma,\ -\mathfrak{D} = {}^m\delta$$

ist und dass die Formen F, ${}^m f$ identisch sind. *Damit ist die Behauptung bewiesen.*

194.

Da die Formen, die wir oben assoziiert genannt haben (Artikel 187, 6), stets uneigentlich äquivalent sind (Artikel 159), ist klar: Sind die reduzierten Formen F, f uneigentlich äquivalent und ist die zu F assoziierte Form G, so sind f, G eigentlich äquivalent, und daher ist G in der Periode von f enthalten. Sind also die Formen F, f sowohl eigentlich als auch uneigentlich äquivalent, so müssen sowohl F als auch G in der Periode von f vorkommen. Diese Periode ist deshalb zu sich selbst assoziiert und enthält zwei ambige Formen (Artikel 187, 7). Das bestätigt auf schöne Weise den Satz in Artikel 165, aufgrund dessen wir bereits sicher sein konnten, dass es eine ambige Form gibt, die zu F, f äquivalent ist.

195.

Aufgabe. *Für zwei beliebige gegebene Formen Φ, φ mit derselben Determinante entscheiden, ob sie äquivalent sind oder nicht.*

Lösung. Wir suchen zwei reduzierte Formen F, f, die zu den gegebenen Formen Φ, φ der Reihe nach eigentlich äquivalent sind (Artikel 183). Je nachdem, ob diese nur eigentlich, nur uneigentlich, auf beide Arten oder auf keine Art äquivalent sind, sind auch die gegebenen Formen nur eigentlich, nur uneigentlich, auf beide Arten oder gar nicht äquivalent. Wir bestimmen die Periode einer der beiden reduzierten Formen, *z.B.* die von f. Kommt die Form F in dieser Periode vor, aber nicht zugleich die zu F assoziierte Form, so liegt offenbar der *erste* Fall vor; kommt dagegen diese assoziierte Form vor, aber nicht F selbst, der *zweite*; kommen beide vor, der *dritte*; kommt keine vor, der *vierte*.

Beispiel. Gegeben seien die Formen $(129, 92, 65)$, $(42, 59, 81)$ mit der Determinante 79. Als dazu eigentlich äquivalente reduzierte Formen finden wir $(10, 7, -3)$, $(5, 8, -3)$. Die Periode der ersten ist $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 7, -6)$, $(-6, 5, 9)$, $(9, 4. -7)$, $(-7, 3, 10)$. Da darin die Form $(5, 8, -3)$ selbst nicht vorkommt, wohl aber ihre assoziierte Form $(-3, 8, 5)$, schließen wir, dass die gegebenen Formen nur uneigentlich äquivalent sind.

Teilen wir alle reduzierten Formen mit einer gegebenen Determinante wie oben (Artikel 187, 5) in Perioden P, Q, R usw. ein und wählen wir aus jeder Periode eine beliebige Form, aus P die Form F, aus Q die Form G, aus R die Form H usw., so können unter diesen Formen F, G, H usw. keine zwei eigentlich äquivalent sein. Jede andere Form mit derselben Determinante ist aber zu einer von ihnen eigentlich äquivalent, und zwar zu *genau einer*. Offenbar lassen sich also *alle Formen mit dieser Determinante in ebenso viele Klassen einteilen, wie es Perioden gibt*, indem wir die zu F eigentlich äquivalenten Formen in die erste Klasse, die zu G eigentlich äquivalenten in die zweite usw. aufnehmen. So sind alle Formen in derselben Klasse eigentlich äquivalent; Formen aus verschiedenen Klassen können dagegen nicht eigentlich äquivalent sein. Wir halten uns aber hier nicht bei diesem Thema auf, das wir unten ausführlicher behandeln werden.

196.

Aufgabe. *Für zwei gegebene eigentlich äquivalente Formen Φ, φ eine eigentliche Transformation der einen in die andere finden.*

Lösung. Nach der Methode in Artikel 183 können wir zwei Folgen von Formen

$$\Phi, \Phi', \Phi'' \dots \Phi^n \quad \text{und} \quad \varphi, \varphi', \varphi'' \dots \varphi^\nu$$

finden, in denen jede Form zu ihrer Vorgängerin eigentlich äquivalent ist und deren letzte Formen Φ^n, φ^ν reduziert sind. Da Φ, φ nach Voraussetzung eigentlich äquivalent sind, muss Φ^n in der Periode von φ^ν enthalten sein. Sei $\varphi^\nu = f$, und ihre Periode bis zur Form Φ^n sei

$$f,\ f',\ f'' \dots f^{m-1},\ \Phi^n$$

sodass Φ^n in dieser Periode den Index m hat. Wir bezeichnen die Formen, die den assoziierten Formen von

$$\Phi,\ \Phi',\ \Phi'' \dots \Phi^n \quad \text{entgegengesetzt sind, mit } \Psi,\ \Psi',\ \Psi'' \dots \Psi^n \text{ der Reihe nach}^{*)}.$$

Dann ist in der Folge

$$\varphi,\ \varphi',\ \varphi'' \dots f,\ f',\ f'' \dots f^{m-1},\ \Psi^{n-1},\ \Psi^{n-2} \dots \Psi,\ \Phi$$

jede Form ihrer Vorgängerin nach rechts benachbart. Daher können wir nach Artikel 177 eine eigentliche Transformation der ersten Form φ in die letzte Φ finden. Bei den übrigen Formen der Folge ist das leicht zu sehen; für f^{m-1}, Ψ^{n-1} beweisen wir es wie folgt. Sei

$$f^{m-1} = (g, h, i); \quad f^m \text{ oder } \Phi^n = (g', h', i');$$
$$\Phi^{n-1} = (g'', h'', i'')$$

Die Form (g', h', i') ist sowohl der Form (g, h, i) als auch der Form (g'', h'', i'') nach rechts benachbart. Daher gilt $i = g' = i''$ und $-h \equiv h' \equiv -h''$ (mod. i oder g' oder i''). Somit ist die Form $(i'', -h'', g'')$, *d.h.* die Form Ψ^{n-1}, der Form (g, h, i), *d.h.* der Form f^{m-1}, nach rechts benachbart.

Sind die Formen Φ, φ uneigentlich äquivalent, so ist φ zu der Form eigentlich äquivalent, die Φ entgegengesetzt ist. Wir können also eine eigentliche Transformation von φ in die zu Φ entgegengesetzte Form finden. Erfolgt diese durch die Substitution $\alpha, \beta, \gamma, \delta$, so sehen wir leicht, dass φ uneigentlich in Φ selbst transformiert wird, und zwar durch die Substitution $\alpha, -\beta, \gamma, -\delta$.

Damit ist auch klar, dass wir für die Formen Φ, φ, wenn sie sowohl eigentlich als auch uneigentlich äquivalent sind, *zwei* Transformationen finden können, eine eigentliche und eine uneigentliche.

*)Es entsteht also Ψ aus Φ, indem wir das erste und letzte Glied vertauschen und dem mittleren das entgegengesetzte Vorzeichen geben; ebenso bei den anderen.

Beispiel. Gesucht ist eine uneigentliche Transformation der Form $(129, 92, 65)$ in $(42, 59, 81)$, die wir im vorhergehenden Artikel als dazu uneigentlich äquivalent erkannt haben. Wir müssen also zuerst eine eigentliche Transformation von $(129, 92, 65)$ in $(42, -59, 81)$ suchen. Dazu bestimmen wir die folgende Formenfolge: $(129, 92, 65)$, $(65, -27, 10)$, $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 22, 81)$, $(81, 59, 42)$, $(42, -59, 81)$. Daraus leiten wir die eigentliche Transformation $-47, 56, 73, -87$ her, durch die $(129, 92, 65)$ in $(42, -59, 81)$ übergeht; durch die uneigentliche Transformation $-47, -56, 73, 87$ geht sie also in $(42, 59, 81)$ über.

197.

Haben wir eine Transformation einer Form $(a,b,c)\ldots\varphi$ in eine äquivalente Form Φ, so können wir daraus *alle* gleichartigen Transformationen von φ in Φ ableiten, sofern wir alle Lösungen der unbestimmten Gleichung $tt - Duu = mm$ angeben können. Dabei bezeichnet D die Determinante der Formen Φ, φ und m den größten gemeinsamen Teiler von $a, 2b, c$ (Artikel 162). Dieses Problem haben wir oben bereits für einen negativen Wert von D gelöst; nun gehen wir es für einen positiven Wert an. Offenbar erfüllt jeder Wert von t, der der Gleichung genügt, sie auch nach Umkehrung seines Vorzeichens; dasselbe gilt für jeden Wert von u. Daher genügt es, alle *positiven* Werte von t, u anzugeben, und jede Lösung mit positiven Werten vertritt vier Lösungen. Wir werden dazu *zuerst* zeigen, wie man die *kleinsten* Werte von t, u (außer den unmittelbar ersichtlichen $t = m,\ u = 0$) findet, und *dann*, wie man daraus alle übrigen ableitet.

198.

Aufgabe. *Die kleinsten Zahlen t, u finden, die der unbestimmten Gleichung $tt - Duu = mm$ genügen, wenn eine Form (M,N,P) mit der Determinante D gegeben ist und die Zahlen $M, 2N, P$ den größten gemeinsamen Teiler n haben.*

Lösung. Wir wählen eine beliebige reduzierte Form $(a,b,-a')\ldots f$ mit der Determinante D, bei der die Zahlen $a, 2b, a'$ den größten gemeinsamen Teiler m haben. Dass es eine solche gibt, ist schon daraus klar, dass wir eine zu (M,N,P) äquivalente reduzierte Form finden können, die nach Artikel 161 diese Eigenschaft besitzt. Für unseren jetzigen Zweck können wir aber jede reduzierte Form verwenden, die diese Bedingung erfüllt. Wir bestimmen die Periode von f, die aus n Formen bestehen möge. Mit allen Bezeichnungen aus Artikel 188 ist f^n gleich $(+a^n, b^n, -a^{n+1})$, weil n gerade ist; in diese Form geht f durch die eigentliche Substitution $\alpha^n, \beta^n, \gamma^n, \delta^n$ über. Da aber f und f^n identisch sind, geht f auch in f^n über, und zwar durch die eigentliche Substitution $1,0,0,1$. Aus diesen beiden gleichartigen Transformationen von f in f^n können wir nach Artikel 162 eine Lösung der Gleichung $tt - Duu = mm$ *in ganzen Zahlen* ableiten, nämlich $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (Gleichung 18, Artikel 162), $u = \frac{\gamma^n m}{a}$ (Gleichung 19)[*]. Wir bezeichnen diese Werte, positiv genommen, falls sie es noch nicht sind, mit T, U. Dann sind T, U die kleinsten Werte von t, u, außer $t = m,\ u = 0$ (von diesen müssen sie verschieden sein, da γ^n offenbar nicht $= 0$ sein kann).

Nehmen wir nämlich an, es gebe noch kleinere Werte von t, u, etwa $\mathfrak{t}, \mathfrak{u}$, die positiv sind, wobei $\mathfrak{u}$ nicht $= 0$ ist. Dann wird nach Artikel 162 die Form f durch die eigentliche Substitution $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u}),\ \frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$ in eine mit ihr identische Form transformiert. Nach Artikel 193, II muss *entweder* $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ *oder* $-\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ einer der Zahlen $\alpha'', \alpha''', \alpha''''$ usw. gleich sein, etwa $= \alpha^\mu$ (denn wegen $\mathfrak{tt} = D\mathfrak{uu} + mm = bb\mathfrak{uu} + aa'\mathfrak{uu} + mm$ ist $\mathfrak{tt} > bb\mathfrak{uu}$ und daher $\mathfrak{t} - b\mathfrak{u}$ positiv; somit hat der Bruch $\frac{\mathfrak{t}-b\mathfrak{u}}{a\mathfrak{u}}$, der dem Bruch $\frac{\mathfrak{P}}{\mathfrak{C}}$ in Artikel 193 entspricht, dasselbe Vorzeichen wie a

[*] In Artikel 162 hatten wir $\alpha, \beta, \gamma, \delta$; $\alpha', \beta', \gamma', \delta'$;
hier haben wir $1,0,0,1$; $\alpha^n, \beta^n, \gamma^n, \delta^n$;
A, B, C; a, b, c; e,
$a, b, -a'$; $a, b, -a'$; 1.

oder a'). Im ersten Fall sind $\frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t}+b\mathfrak{u})$, im zweiten dieselben Größen mit umgekehrten Vorzeichen der Reihe nach $= \beta^\mu, \gamma^\mu, \delta^\mu$. Da aber $\mathfrak{u} < U$, *d.h.*, $\mathfrak{u} < \frac{\gamma^n m}{a}$ und > 0 ist, gilt $\gamma^\mu < \gamma^n$ und > 0. Weil die Folge $\gamma, \gamma', \gamma''$ usw. ständig wächst, muss μ strikt zwischen 0 und n liegen. Die entsprechende Form f^μ ist aber mit f identisch, *ein Widerspruch*, da alle Formen f, f', f'' usw. bis f^{n-1} als verschieden vorausgesetzt sind. Also sind die kleinsten Werte von t, u (außer $m, 0$) gleich T, U.

Beispiel. Für $D = 79,\ m = 1$ können wir die Form $(3, 8, -5)$ verwenden, für die $n = 6$ und $\alpha^n = -8,\ \gamma^n = -27,\ \delta^n = -152$ gilt (Artikel 188). Daraus folgt $T = 80,\ U = 9$, die kleinsten Werte von t, u, die der Gleichung $tt - 79uu = 1$ genügen.

199.

Für die praktische Rechnung lassen sich noch bequemere Formeln finden. Es gilt nämlich $2b\gamma^n = -a(\alpha^n - \delta^n)$, was sich leicht aus Artikel 162 ergibt, indem wir Gleichung [19] mit $2b$ und [20] mit a multiplizieren und die dortigen Bezeichnungen durch die jetzigen ersetzen. Daraus folgt $\alpha^n + \delta^n = 2\delta^n - \frac{2b}{a}\gamma^n$ und damit

$$\pm T = m\left(\delta^n - \frac{b}{a}\gamma^n\right), \quad \pm U = \frac{\gamma^n m}{a}$$

Auf ähnliche Weise erhalten wir

$$\pm T = m\left(\alpha^n + \frac{b}{a'}\beta^n\right), \quad \pm U = \frac{\beta^n m}{a'}$$

Beide Formelpaare sind sehr bequem, weil $\gamma^n = \delta^{n-1}$, $\alpha^n = \beta^{n-1}$ ist. Verwenden wir das zweite, so brauchen wir nur die Folge $\beta', \beta'', \beta''' \ldots \beta^n$ zu berechnen; bevorzugen wir das erste, nur die Folge $\delta', \delta'', \delta'''$ usw. Außerdem folgt leicht aus Artikel 189, 3, dass, weil n notwendig gerade ist, α^n und $\frac{b}{a'}\beta^n$ dasselbe Vorzeichen haben, ebenso δ^n und $\frac{b}{a}\gamma^n$. Daher müssen wir in der ersten Formel für T die absolute Differenz und in der zweiten die absolute Summe nehmen und brauchen die Vorzeichen überhaupt nicht zu beachten. Mit den Bezeichnungen aus Artikel 189, 4 ergibt die erste Formel

$$T = m[k', k'', k'''. \ldots k^n] - \frac{mb}{a}[k', k'', k'''. \ldots k^{n-1}],$$
$$U = \frac{m}{a}[k', k'', k'''. \ldots k^{n-1}]$$

und die zweite

$$T = m[k'', k'''. \ldots k^{n-1}] + \frac{mb}{a'}[k'', k'''. \ldots k^n],$$
$$U = \frac{m}{a'}[k'', k'''. \ldots k^n]$$

wobei wir für den Wert von T auch $m\left[k'', k'''. \ldots k^n, \frac{b}{a'}\right]$ schreiben können.

Beispiel. Für $D = 61,\ m = 2$ können wir die Form $(2, 7, -6)$ verwenden, für die wir $n = 6$ und $k', k'', k''', k'''', k''''', k'''''' $ der Reihe nach $= 2, 2, 7, 2, 2, 7$ finden. Daraus folgt

$$T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2]$$
$$= 2888 - 1365 = 1523$$

nach der ersten Formel; die zweite ergibt dasselbe:

$$T = 2[2,7,2,2] + \tfrac{7}{3}[2,7,2,2.7]$$

$$U \text{ wird } = [2,2,7,2,2] = \tfrac{1}{3}[2,7,2,2,7] = 195.$$

Es gibt noch weitere Möglichkeiten, die Rechnung zu verkürzen; um uns kurz zu halten, können wir sie hier aber nicht ausführlicher behandeln.

200.

Um aus den kleinsten Werten von t, u *alle* zu erhalten, schreiben wir die Gleichung $TT - DUU = mm$ in der Form

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right) = 1$$

woraus auch folgt

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = 1 \quad \ldots\ldots \qquad [1]$$

wobei e eine beliebige Zahl bezeichnet. Wir bezeichnen nun der Kürze wegen die Werte der Größen

$$\frac{m}{2}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e + \frac{m}{2}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e,$$
$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e - \frac{m}{2\sqrt{D}}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e \text{ *)}$$

allgemein mit t^e, u^e der Reihe nach, *d.h.* ihre Werte für $e = 0$ mit t^0, u^0 (die gleich $m, 0$ sind); für $e = 1$ mit t', u' (die gleich T, U sind); für $e = 2$ mit t'', u''; für $t = 3$ mit t''', u''' usw. — Wir werden beweisen, dass diese Ausdrücke, wenn wir für e alle nichtnegativen ganzen Zahlen nehmen, *d.h.* 0 und alle positiven Zahlen von 1 bis ∞, sämtliche positiven Werte von t, u darstellen: nämlich I) dass alle Werte dieser Ausdrücke tatsächlich Werte von t, u sind; II) dass alle diese Werte ganze Zahlen sind; III) dass es keine positiven Werte von t, u gibt, die nicht in diesen Formeln enthalten sind.

I. Setzen wir für t^e, u^e ihre Werte ein, so bestätigen wir mithilfe von Gleichung [1] leicht, dass

$$(t^e + u^e\sqrt{D})(t^e - u^e\sqrt{D}) = mm, \quad d.h. \quad t^e t^e - Du^e u^e = mm$$

II. Auf dieselbe Weise bestätigen wir leicht, dass allgemein

$$t^{e+1} + t^{e-1} = \frac{2T}{m}t^e, \quad u^{e+1} + u^{e-1} = \frac{2T}{m}u^e$$

*) Nur in diesen vier Ausdrücken und in Gleichung [1] bezeichnet e den *Exponenten* einer Potenz; sonst bezeichnen hochgestellte Buchstaben stets einen *Index*.

Die beiden Folgen t^0, t', t'', t''' usw., u^0, u', u'', u''' usw. erfüllen also Rekursionen, beide mit den Koeffizienten $\frac{2T}{m}, -1$, nämlich

$$t'' = \frac{2T}{m}t' - t^0, \quad t''' = \frac{2T}{m}t'' - t' \text{ usw.}, \quad u'' = \frac{2T}{m}u' \text{ usw.}$$

Nach Voraussetzung gibt es nun eine Form (M, N, P) mit der Determinante D, in der $M, 2N, P$ durch m teilbar sind. Daher gilt

$$TT = (NN - MP)UU + mm$$

und somit ist $4TT$ offenbar durch mm teilbar. Also ist $\frac{2T}{m}$ eine ganze und zwar positive Zahl. Es gilt aber $t^0 = m,\ t' = T,\ u^0 = 0,\ u' = U$; diese Werte sind also ganzzahlig. Damit sind auch alle t'', t''' usw., u'', u''' usw. ganzzahlig. Ferner sind wegen $TT > mm$ offenbar alle t^0, t', t'', t''' usw. positiv und wachsen ständig unbegrenzt an, ebenso alle u^0, u', u'', u''' usw.

III. Nehmen wir an, es gebe noch andere positive Werte von t, u, die nicht in den Folgen t^0, t', t'' usw., u^0, u', u'' usw. enthalten sind, etwa $\mathfrak{T}, \mathfrak{U}$. Da die Folge u^0, u' usw. von 0 aus unbegrenzt wächst, muss $\mathfrak{U}$ offenbar zwischen zwei benachbarten Gliedern u^n und u^{n+1} liegen, sodass $\mathfrak{U} > u^n$ und $\mathfrak{U} < u^{n+1}$ ist. Um zu zeigen, dass diese Annahme zu einem Widerspruch führt, bemerken wir Folgendes.

1° Die Gleichung $tt - Duu = mm$ wird auch erfüllt, wenn wir setzen

$$t = \frac{1}{m}(\mathfrak{T}t^n - D\mathfrak{U}u^n), \quad u = \frac{1}{m}(\mathfrak{U}t^n - \mathfrak{T}u^n).$$

Das lässt sich leicht durch Einsetzen bestätigen. Dass diese Werte, die wir kurz mit $= \tau, \upsilon$ bezeichnen, stets *ganze Zahlen* sind, zeigen wir wie folgt. Ist (M, N, P) eine Form mit der Determinante D und m ein gemeinsamer Teiler von $M, 2N, P$, so sind sowohl $\mathfrak{T} + N\mathfrak{U}$ als auch $t^n + Nu^n$ durch m teilbar und daher auch $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$ oder $\mathfrak{U}t^n - \mathfrak{T}u^n$. Somit ist υ ganzzahlig und daher auch τ, weil $\tau\tau = D\upsilon\upsilon + mm$.

2° Offenbar kann υ nicht $= 0$ sein, denn daraus würde folgen

$$\mathfrak{UU}t^n t^n = \mathfrak{TT}u^n u^n$$

oder

$$\mathfrak{UU}(Du^n u^n + mm) = u^n u^n(D\mathfrak{UU} + mm)$$

oder $\mathfrak{UU} = u^n u^n$, im Widerspruch zur Voraussetzung $\mathfrak{U} > u^n$. Da also außer dem Wert 0 der kleinste Wert von u gleich U ist, ist υ sicher nicht kleiner als U.

3° Aus den Werten von $t^n, t^{n+1}, u^n, u^{n+1}$ lässt sich leicht bestätigen, dass

$$mU = u^{n+1}t^n - t^{n+1}u^n.$$

Daher ist $\mathfrak{U}t^n - \mathfrak{T}u^n$ sicher nicht kleiner als $u^{n+1}t^n - t^{n+1}u^n$.

4° Nun ergibt die Gleichung $\mathfrak{TT} - D\mathfrak{UU} = mm$

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{\left(D + \frac{mm}{\mathfrak{UU}}\right)}$$

und entsprechend

$$\frac{t^{n+1}}{u^{n+1}} = \surd\left(D + \frac{mm}{u^{n+1}u^{n+1}}\right)$$

woraus leicht $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{n+1}}{u^{n+1}}$ folgt. Daraus und aus dem Schluss in 3° folgt

$$\begin{aligned}(\mathfrak{U}t^n - \mathfrak{T}u^n)\left(t^n + u^n\frac{\mathfrak{T}}{\mathfrak{U}}\right)\\ > (u^{n+1}t^n - t^{n+1}u^n)\left(t^n + u^n\frac{t^{n+1}}{u^{n+1}}\right)\end{aligned}$$

oder, wenn wir ausmultiplizieren und für $\mathfrak{T}\mathfrak{T}$, t^nt^n, $t^{n+1}t^{n+1}$ ihre Werte $D\mathfrak{U}\mathfrak{U} + mm$, $Du^nu^n + mm$, $Du^{n+1}u^{n+1} + mm$ einsetzen,

$$\frac{1}{\mathfrak{U}}(\mathfrak{U}\mathfrak{U} - u^nu^n) > \frac{1}{u^{n+1}}(u^{n+1}u^{n+1} - u^nu^n)$$

Da beide Größen offenbar positiv sind, ergibt sich durch Umstellen $\mathfrak{U} + \frac{u^nu^n}{u^{n+1}} > u^{n+1} + \frac{u^nu^n}{\mathfrak{U}}$, *ein Widerspruch*, weil der erste Teil der ersten Größe *kleiner* ist als der erste Teil der zweiten und ebenso ihr zweiter Teil kleiner als der zweite Teil der anderen. Daher kann die Annahme nicht gelten, und die Folgen t^0, t', t'' usw., u^0, u', u'' usw. stellen sämtliche positiven Werte von t, u dar.

Beispiel. Für $D = 61$, $m = 2$ fanden wir als kleinste positive Werte von t, u die Werte $1523, 195$. Daher stellen die folgenden Formeln *alle* positiven Werte dar:

$$\begin{aligned}t &= \left(\frac{1523}{2} + \frac{195}{2}\surd 61\right)^e + \left(\frac{1523}{2} - \frac{195}{2}\surd 61\right)^e\\ u &= \frac{1}{\surd 61}\left(\left(\frac{1523}{2} + \frac{195}{2}\surd 61\right)^e - \left(\frac{1523}{2} - \frac{195}{2}\surd 61\right)^e\right)\end{aligned}$$

Wir finden

$$\begin{aligned}t^0 &= 2, \quad t' = 1523,\\ t'' &= 1523t' - t^0 = 2319527,\\ t''' &= 1523t'' - t' = 3532618098 \text{ usw.}\\ u^0 &= 0, \quad u' = 195,\\ u'' &= 1523u' - u^0 = 296985,\\ u''' &= 1523u'' - u' = 452307960 \text{ usw.}\end{aligned}$$

201.

Zum Problem, das wir in den vorhergehenden Artikeln behandelt haben, fügen wir noch folgende Bemerkungen hinzu.

1) Wir haben gezeigt, wie man die Gleichung $tt - Duu = mm$ in allen Fällen löst, in denen m der größte gemeinsame Teiler dreier Zahlen $M, 2N, P$ mit $NN - MP = D$ ist. Es lohnt sich, alle Zahlen zu bestimmen, die solche Teiler sein können, also alle Werte von m für einen gegebenen Wert von D. Wir setzen $D = nnD'$, sodass D' völlig frei von quadratischen Faktoren ist. Das erreichen wir, indem wir für nn das größte Quadrat nehmen, das D teilt; hat D selbst schon keinen quadratischen Faktor, so müssen wir $n = 1$ setzen. Dann behaupte ich Folgendes.

Erstens: Hat D' die Form $4k + 1$, so ist jeder Teiler von $2n$ ein Wert von m und umgekehrt. Teilt nämlich g die Zahl $2n$, so haben wir die Form $\left(g, n, \frac{nn(1-D')}{g}\right)$ mit der Determinante D, bei der die Zahlen $g, 2n, \frac{nn(D'-1)}{g}$ offenbar den größten gemeinsamen Teiler g haben (denn $\frac{nn(D'-1)}{gg} = \frac{4nn}{gg} \cdot \frac{D'-1}{4}$ ist offenbar ganzzahlig). Nehmen wir umgekehrt an, g sei ein Wert von m, nämlich der größte gemeinsame Teiler von $M, 2N, P$, und es gelte $NN - MP = D$. Dann ist offenbar $4D$ oder $4nnD'$ durch gg teilbar. Daraus folgt, dass $2n$ durch g teilbar sein muss. Würde nämlich g die Zahl $2n$ nicht teilen, so hätten g und $2n$ einen größten gemeinsamen Teiler kleiner als g. Setzen wir diesen $= \delta$ und $2n = \delta n'$, $g = \delta g'$, so wäre $n'n'D'$ durch $g'g'$ teilbar, n' zu g' und daher auch $n'n'$ zu $g'g'$ teilerfremd; somit wäre auch D' durch $g'g'$ teilbar, im Widerspruch zur Voraussetzung, dass D' von jedem quadratischen Faktor frei ist.

Zweitens: Hat D' die Form $4k + 2$ oder $4k + 3$, so ist jeder Teiler von n ein Wert von m, und umgekehrt teilt jeder Wert von m die Zahl n. Teilt nämlich g die Zahl n, so haben wir die Form $\left(g, 0, -\frac{nnD'}{g}\right)$ mit der Determinante $= D$, bei der die Zahlen $g, 0, \frac{nnD'}{g}$ offenbar den größten gemeinsamen Teiler g haben. — Nehmen wir dagegen an, g sei ein Wert von m, nämlich der größte gemeinsame Teiler von $M, 2N, P$, und es gelte $NN - MP = D$, so teilt wie oben g die Zahl $2n$, oder $\frac{2n}{g}$ ist ganzzahlig. Wäre dieser Quotient ungerade, so wäre das Quadrat $\frac{4nn}{gg} \equiv 1 \pmod 4$ und daher $\frac{4nnD'}{gg}$ entweder $\equiv 2$ oder $\equiv 3 \pmod 4$. Nun gilt aber $\frac{4nnD'}{gg} = \frac{4D}{gg} = \frac{4NN}{gg} - \frac{4MP}{gg} \equiv \frac{4NN}{gg} \pmod 4$, also wäre $\frac{4NN}{gg}$ entweder $\equiv 2$ oder $\equiv 3 \pmod 4$, *ein Widerspruch*, da jedes Quadrat modulo 4 entweder zu null oder zu eins kongruent sein muss. Daher ist der Quotient $\frac{2n}{g}$ notwendig gerade und somit $\frac{n}{g}$ ganzzahlig, also g ein Teiler von n.

Also ist 1 stets ein Wert von m, oder die Gleichung $tt - Duu = 1$ lässt sich nach dem Vorhergehenden für jeden positiven nichtquadratischen Wert von D lösen; ferner ist 2 genau dann ein Wert von m, wenn D entweder die Form $4k$ oder $4k + 1$ hat.

2) Ist m größer als 2, aber eine zulässige Zahl, so können wir die Lösung von $tt - Duu = mm$ auf die einer ähnlichen Gleichung zurückführen, in der m entweder 1 oder 2 ist. Setzen wir wie zuvor $D = nnD'$, so teilt, wenn m die Zahl n teilt, auch mm die Zahl D. Sind die kleinsten Werte von p, q in $pp - \frac{D}{mm}qq = 1$ gleich $p = P,\ q = Q$, so sind die kleinsten Werte von t, u in $tt - Duu = mm$ gleich $t = mP,\ u = Q$. — Teilt aber m die Zahl n nicht, so teilt es wenigstens $2n$ und ist sicher gerade; $\frac{4D}{mm}$ ist dann ganzzahlig. Finden wir in diesem Fall als kleinste Werte von p, q in $pp - \frac{4D}{mm}qq = 4$

die Werte $p = P,\ q = Q$, so sind die kleinsten Werte von t, u in $tt - Duu = mm$ gleich $t = \frac{m}{2}P,\ u = Q$. — In beiden Fällen lassen sich nach dieser Methode offenbar nicht nur aus den kleinsten Werten von p, q die kleinsten Werte von t, u, sondern aus *allen* Werten der ersten *alle* Werte der zweiten ableiten.

3) Bezeichnen $t^0, u^0;\ t', u';\ t'', u''$ usw. sämtliche positiven Werte von t, u in $tt - Duu = mm$ (wie im vorhergehenden Artikel), und sind gewisse Werte dieser Folge ihren ersten Werten modulo einer beliebigen gegebenen Zahl r kongruent, etwa $t^\rho \equiv t$ (oder $\equiv m$), $u^\rho \equiv u^0$ oder $\equiv 0$ (mod. r), und zugleich die unmittelbar folgenden Werte den zweiten, etwa

$$t^{\rho+1} \equiv t', \quad u^{\rho+1} \equiv u' \pmod{r}$$

so gilt auch

$$t^{\rho+2} \equiv t'', \quad u^{\rho+2} \equiv u''; \quad t^{\rho+3} \equiv t''', \quad u^{\rho+3} \equiv u''' \text{ usw.}$$

Das folgt leicht daraus, dass beide Folgen t^0, t', t'' usw., u^0, u', u'' usw. Rekursionen erfüllen: Denn wegen

$$t'' = \frac{2T}{m}t' - t^0, \quad t^{\rho+2} = \frac{2T}{m}t^{\rho+1} - t^\rho$$

gilt

$$t'' \equiv t^{\rho+2}$$

und ebenso bei den übrigen. — Daraus folgt allgemein

$$t^{h+\rho} \equiv t^h, \quad u^{h+\rho} \equiv u^h \pmod{r}$$

wobei h eine beliebige Zahl bezeichnet, und noch allgemeiner, wenn

$$\mu \equiv \nu \pmod{\rho}, \quad \text{so gilt } t^\mu \equiv t^\nu, \quad u^\mu \equiv u^\nu \pmod{r}.$$

4) Die Bedingungen der vorhergehenden Bemerkung lassen sich aber immer erfüllen: Wir können stets einen Index ρ finden (für jeden gegebenen Modul r), für den gilt

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u'$$

Um das zu beweisen, bemerken wir Folgendes.

Erstens lässt sich die dritte Bedingung immer erfüllen. Nach den Kriterien in (1) ist offenbar auch die Gleichung $pp - rrDqq = mm$ lösbar. Sind die kleinsten positiven Werte von p, q (außer $m, 0$) gleich P, Q, so gehören zu den Werten von t, u offenbar auch $t = P,\ u = rQ$. Daher kommen P, rQ in den Folgen t^0, t' usw., u^0, u' usw. vor; und wenn $P = t^\lambda,\ rQ = u^\lambda$, so gilt $u^\lambda \equiv 0 \equiv u^0 \pmod{r}$. Außerdem sieht man leicht, dass zwischen u^0 und u^λ kein Glied zu u^0 modulo r kongruent ist.

Zweitens ist klar: Sind außerdem die drei übrigen Bedingungen erfüllt, gilt also auch $u^{\lambda+1} \equiv u',\ t^\lambda \equiv t^0,\ t^{\lambda+1} \equiv t'$, so brauchen wir nur $\rho = \lambda$ zu setzen. Wenn dagegen die eine oder andere dieser Bedingungen nicht gilt, so können wir, behaupte ich, sicher $\rho = 2\lambda$ setzen. Aus Gleichung [1] und den allgemeinen Formeln für t^e, u^e im vorhergehenden Artikel folgt nämlich

$$t^{2\lambda} = \frac{1}{m}(t^\lambda t^\lambda + Du^\lambda u^\lambda) = \frac{1}{m}(mm + 2Du^\lambda u^\lambda)$$

und daher

$$\frac{t^{2\lambda} - t^0}{r} = \frac{2Du^\lambda u^\lambda}{mr}$$

Diese Größe ist ganzzahlig, weil nach Voraussetzung r die Zahl u^λ teilt, ebenso mm die Zahl $4D$ und somit erst recht m die Zahl $2D$. — Ferner gilt $u^{2\lambda} = \frac{2}{m}t^\lambda u^\lambda$, und wegen

$$4t^\lambda t^\lambda = 4Du^\lambda u^\lambda + 4mm$$

und damit der Teilbarkeit durch mm ist $2t^\lambda$ durch m teilbar und somit $u^{2\lambda}$ durch r, also

$$u^{2\lambda} \equiv u^0 \text{ (mod. } r)$$

Drittens finden wir

$$t^{2\lambda+1} = t' + \frac{2Du^\lambda u^{\lambda+1}}{m}$$

und da $\frac{2Du^\lambda}{mr}$ aus demselben Grund ganzzahlig ist, gilt

$$t^{2\lambda+1} \equiv t' \text{ (mod. } r)$$

Schließlich finden wir

$$u^{2\lambda+1} = u' + \frac{2t^{\lambda+1}u^\lambda}{m}$$

und weil $2t^{\lambda+1}$ durch m und u^λ durch r teilbar ist, gilt

$$u^{2\lambda+1} \equiv u' \text{ (mod. } r). \quad \textit{Damit ist die Behauptung bewiesen.}$$

Wozu die letzten beiden Bemerkungen dienen, wird sich im Folgenden zeigen.

202.

Der besondere Fall des Problems, nämlich die Gleichung $tt - Duu = 1$ zu lösen, wurde schon von den Mathematikern des vorhergehenden Jahrhunderts behandelt. Der sehr scharfsinnige Fermat legte dieses Problem den englischen Analysten vor. Wallis nennt Brounker als Urheber der Lösung, die er in *Alg. Cap.* 98, *Opp. T.* II *p.* 418 ff. angibt; Ozanam nennt Fermat; und schließlich der bedeutende Euler, der das Problem in *Comm. Petr.* VI *p.* 175, *Comm. nov.* XI *p.* 28[*)], *Algebra P.* II *p.* 226, *Opusc. An.* I *p.* 310 behandelt, nennt Pell. Daher haben einige Autoren das Problem als *Pellsches Problem* bezeichnet. Alle diese Lösungen stimmen im Wesentlichen mit der überein, die wir erhalten, wenn wir in Artikel 198 die reduzierte Form mit $a = 1$ wählen. Dass aber das von ihnen vorgeschriebene Verfahren notwendig einmal *endet*, also das Problem immer *tatsächlich lösbar* ist, hat vor dem bedeutenden La Grange niemand streng[*)] bewiesen: *Mélanges de la Soc. de Turin T.* IV *p.* 19 und eleganter in *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. Diese Untersuchung steht auch in den schon mehrfach angeführten *Ergänzungen zu Eulers Algebra*. Unsere Methode dagegen (die von völlig anderen Grundsätzen ausgeht und nicht auf $m = 1$ beschränkt ist) bietet meist mehrere Wege zur Lösung, da wir in Artikel 198 von jeder anderen reduzierten Form $(a, b, -a')$ ausgehen können.

[*)] In dieser Abhandlung wird der Algorithmus, den wir in Artikel 27 dargestellt haben, durch ähnliche Zeichen ausgedrückt; wir haben versäumt, das dort zu erwähnen.

[*)] Was Wallis dazu an der genannten Stelle auf S. 427, 428 vorbringt, hat kein Gewicht. Sein Fehlschluss besteht darin, dass er auf S. 428, Zeile 4 voraussetzt, man könne zu einer gegebenen Größe p ganze Zahlen a, z finden, sodass $\frac{z}{a}$ kleiner als p und der Fehlbetrag kleiner als der *vorgegebene* ist. Das ist durchaus richtig, wenn der *vorgegebene* Fehlbetrag eine *gegebene Größe* ist; nicht aber, wenn er von a und z abhängt und somit veränderlich ist, wie im vorliegenden Fall.

203.

Aufgabe. *Sind die Formen Φ, φ äquivalent, so sind alle Transformationen der einen in die andere anzugeben.*

Lösung. Sind diese Formen nur auf eine Art äquivalent (*d.h.*, entweder nur eigentlich oder nur uneigentlich), so suchen wir nach Artikel 196 eine Transformation von φ in Φ, etwa $\alpha, \beta, \gamma, \delta$. Offenbar kann es keine anderen als dazu gleichartige Transformationen geben. Sind aber φ, Φ sowohl eigentlich als auch uneigentlich äquivalent, so suchen wir zwei ungleichartige Transformationen, *d.h.* eine eigentliche und eine uneigentliche, etwa $\alpha, \beta, \gamma, \delta$ und $\alpha', \beta', \gamma', \delta'$. Jede andere Transformation ist mit der einen oder der anderen gleichartig. Sei also die Form φ gleich (a, b, c), ihre Determinante $= D$ und der größte gemeinsame Teiler von $a, 2b, c$ wie stets zuvor m; ferner sollen t, u alle Zahlen durchlaufen, die $tt - Duu = mm$ erfüllen. Dann sind im ersten Fall alle Transformationen von φ in Φ in der ersten der folgenden Formeln, I, enthalten, im zweiten Fall entweder in der ersten, I, oder in der zweiten, II.

$$\begin{array}{lll} \text{I} \ldots\ldots\ldots & \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u), & \frac{1}{m}(\beta t - (\beta b + \delta c)u) \\ & \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u), & \frac{1}{m}(\delta t + (\beta a + \delta b)u) \\ \text{II} \ldots\ldots\ldots & \frac{1}{m}(\alpha' t - (\alpha' b + \gamma' c)u), & \frac{1}{m}(\beta' t - (\beta' b + \delta' c)u) \\ & \frac{1}{m}(\gamma' t + (\alpha' a + \gamma' b)u), & \frac{1}{m}(\delta' t + (\beta' a + \delta' b)u) \end{array}$$

Beispiel. - Gesucht sind alle Transformationen von $(129, 92, 65)$ in $(42, 59, 81)$. In Artikel 195 haben wir gefunden, dass diese nur uneigentlich äquivalent sind, und im nächsten Artikel die uneigentliche Transformation $-47, -56, 73, 87$ der ersten in die zweite ermittelt. Daher werden alle Transformationen von $(129, 92, 65)$ in $(42, 59, 81)$ durch die Formel

$$-(47t + 421u), \quad -(56t + 503u). \quad 73t + 653u, \quad 87t + 780u$$

dargestellt, wobei t, u alle Zahlen durchlaufen, die $tt - 79uu = 1$ erfüllen. Diese werden dargestellt durch

$$\begin{aligned} \pm t &= \tfrac{1}{2}\big((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e\big) \\ \pm u &= \tfrac{1}{2\sqrt{79}}\big((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e\big) \end{aligned}$$

wobei für e alle nichtnegativen ganzen Zahlen zu nehmen sind.

204.

Offenbar wird die allgemeine Formel, die alle Transformationen darstellt, umso *einfacher*, je einfacher die Ausgangstransformation ist, aus der wir sie ableiten. Da wir frei wählen können, von welcher Transformation wir ausgehen, lässt sich die allgemeine Formel oft einfacher machen: Wir leiten aus der zuerst gefundenen Formel eine einfachere Transformation ab, indem wir t, u bestimmte Werte geben, und bilden daraus eine andere Formel. Setzen wir *z.B.* in der Formel aus dem Beispiel des vorhergehenden Artikels $t = 80$, $u = -9$, so erhalten wir eine einfachere Transformation als die, von der wir ausgegangen waren, nämlich $29, 47, -37, -60$. Daraus folgt die

allgemeine Formel $29t - 263u$, $47t - 424u$, $-37t + 337u$, $-60t + 543u$. Haben wir also nach den vorhergehenden Regeln eine allgemeine Formel gefunden, können wir versuchen, ob sich, wenn wir t, u die bestimmten Werte $\pm t', \pm u'$; $\pm t'', \pm u''$ usw. geben, eine einfachere Transformation ergibt als die, aus der die Formel abgeleitet wurde. In diesem Fall lässt sich aus jener Transformation eine einfachere Formel herleiten. — Bei der Beurteilung der Einfachheit bleibt allerdings ein gewisser Spielraum. Wenn es die Mühe lohnte, könnten wir dafür eine feste Regel aufstellen und in der Folge t', u'; t'', u'' usw. auch *Grenzen* angeben, jenseits derer die Transformationen ständig weniger einfach werden. Dann brauchten wir nicht weiterzugehen, sondern nur innerhalb dieser Grenzen zu suchen. Da aber nach unseren Methoden die einfachste Transformation meist entweder sofort oder indem wir t, u die Werte $\pm t', \pm u'$ geben, auftritt, lassen wir diese Untersuchung der Kürze wegen weg.

205.

Aufgabe. *Alle Darstellungen einer gegebenen Zahl M durch eine gegebene Formel $axx + 2bxy + cyy$ mit positiver nichtquadratischer Determinante $= D$ finden.*

Lösung. Zunächst bemerken wir, dass sich die Suche nach Darstellungen durch nicht teilerfremde Werte von x, y genauso wie oben für Formen mit negativer Determinante (Artikel 181) auf den Fall zurückführen lässt, in dem teilerfremde Werte der Unbestimmten gesucht werden. Es wäre daher überflüssig, dies hier zu wiederholen. Damit Darstellungen durch teilerfremde Werte von x, y möglich sind, muss D ein quadratischer Rest von M sein. Sind alle Werte des Ausdrucks $\sqrt{D}$ (mod. M) gleich $N, -N, N', -N', N'', -N''$ usw. (die wir so wählen dürfen, dass keiner $> \frac{1}{2}M$ ist), so gehört jede Darstellung von M durch die gegebene Form zu einem dieser Werte. Wir müssen also zuerst diese Werte ermitteln und dann die zu jedem einzelnen gehörigen Darstellungen untersuchen. Darstellungen zum Wert N gibt es nur, wenn die Formen (a, b, c) und $(M, N, \frac{NN-D}{M})$ eigentlich äquivalent sind. Ist das der Fall, so suchen wir eine beliebige eigentliche Transformation der ersten in die zweite, etwa $\alpha, \beta, \gamma, \delta$. Dann haben wir eine Darstellung der Zahl M durch (a, b, c), die zum Wert N gehört, nämlich $x = \alpha$, $y = \gamma$, und alle zu diesem Wert gehörigen Darstellungen werden durch die Formel

$$x = \tfrac{1}{m}\big(\alpha t - (\alpha b + \gamma c)u\big), \qquad y = \tfrac{1}{m}\big(\gamma t + (\alpha a + \gamma b)u\big)$$

dargestellt. Dabei bezeichnet m den größten gemeinsamen Teiler von $a, 2b, c$, und t, u durchlaufen alle Zahlen, die $tt - Duu = mm$ erfüllen. — Offenbar wird diese allgemeine Formel umso einfacher, je einfacher die Transformation $\alpha, \beta, \gamma, \delta$ ist, aus der sie abgeleitet wurde. Deshalb ist es sinnvoll, vorher nach dem letzten Artikel die einfachste Transformation von (a, b, c) in $(M, N, \frac{NN-D}{M})$ zu ermitteln und daraus die Formel abzuleiten. — Auf genau dieselbe Weise lassen sich die zu den übrigen Werten $-N, N', -N'$ usw. gehörigen Darstellungen, falls es welche gibt, durch allgemeine Formeln angeben.

Beispiel. Gesucht sind alle Darstellungen von 585 durch die Formel $42xx + 62xy + 21yy$. Bei Darstellungen durch nicht teilerfremde Werte von x, y ist sofort klar, dass nur solche möglich sind, bei denen x, y den größten gemeinsamen Teiler 3 haben, denn 585 ist nur durch das eine Quadrat 9 teilbar. Haben wir also alle Darstellungen

von $\frac{585}{9}$, *d.h.* 65, durch die Form $42x'x' + 62x'y' + 21y'y'$ gefunden, in denen x' und y' teilerfremd sind, so erhalten wir daraus alle Darstellungen von 585 durch $42xx+62xy+21yy$, in denen x und y nicht teilerfremd sind, indem wir $x = 3x'$, $y = 3y'$ setzen. Die Werte von $\sqrt{79}$ (mod. 65) sind $\pm 12, \pm 27$. Als Darstellung von 65 zum Wert -12 finden wir $x' = 2$, $y' = -1$. Daher werden alle Darstellungen von 65 zu diesem Wert durch $x' = 2t - 41u$, $y' = -t + 53u$ und alle *daraus* entstehenden Darstellungen von 585 durch $x = 6t - 123u$, $y = -3t + 159u$ gegeben. Ebenso finden wir die allgemeine Formel für alle Darstellungen von 65 zum Wert $+12$, nämlich $x' = 22t - 199u$, $y' = -23t + 211u$, und die Formel für alle daraus entstehenden Darstellungen von 585, nämlich $x = 66t - 597u$, $y' = -69t + 633u$. Zu den Werten $+27$ und -27 gehört aber keine Darstellung von 65. — Um die Darstellungen von 585 durch teilerfremde Werte von x, y zu finden, müssen wir zuerst die Werte von $\sqrt{79}$ (mod. 585) ermitteln; sie sind $\pm 77, \pm 103, \pm 157, \pm 248$. Zu den Werten $\pm 77, \pm 103, \pm 248$ finden wir keine Darstellung. Zum Wert -157 gehört aber die Darstellung $x = 3$, $y = 1$, aus der wir die allgemeine Formel für alle zu diesem Wert gehörigen Darstellungen ableiten: $x = 3t - 114u$, $y = t + 157u$. Ebenso finden wir als Darstellung zum Wert $+157$ die Werte $x = 83$, $y = -87$ und als Formel, die alle gleichartigen enthält, $x = 83t - 746u$, $y = -87t + 789u$. Wir haben also vier allgemeine Formeln, unter denen sämtliche Darstellungen von 585 durch $42xx + 62xy + 21yy$ enthalten sind:

$$\begin{array}{ll} x = 6t - 123u & y = -3t + 159u \\ x = 66t - 597u & y = -69t + 633u \\ x = 3t - 114u & y = t + 157u \\ x = 83t - 746u & y = -87t + 789u \end{array}$$

wobei t, u alle ganzen Zahlen durchlaufen, die $tt - 79uu = 1$ erfüllen.

Bei besonderen Anwendungen der vorhergehenden Untersuchungen über Formen mit positiver nichtquadratischer Determinante halten wir uns der Kürze wegen nicht auf. Jeder kann sie ohne Schwierigkeit selbst durchführen, ähnlich wie in den Artikeln 176, 182. Wir wenden uns gleich den Formen mit positiver quadratischer Determinante zu, die allein noch übrig sind.

Formen mit quadratischer Determinante.

206.

Aufgabe. *Für eine gegebene Form (a, b, c) mit quadratischer Determinante hh, wobei h deren positive Wurzel bezeichnet, eine eigentlich äquivalente Form (A, B, C) finden, in der A zwischen 0 und $2h - 1$ einschließlich liegt und $B = h$ sowie $C = 0$ gilt.*

Lösung. I. Wegen $hh = bb - ac$ ist $(h - b) : a = c : -(h + b)$. Diesem Verhältnis sei $\beta : \delta$ gleich, wobei β und δ teilerfremd sind. Wir bestimmen α, γ so, dass $\alpha\delta - \beta\gamma = 1$ gilt, was möglich ist. Durch die Substitution $\alpha, \beta, \gamma, \delta$ gehe die Form (a, b, c) in (a', b', c') über, die somit zu ihr eigentlich äquivalent ist. Wir erhalten

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ &= (h - b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h + b)\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \\ c' &= a\beta\beta + 2b\beta\delta + c\delta\delta \\ &= (h - b)\beta\delta + 2b\beta\delta - (h + b)\beta\delta = 0 \end{aligned}$$

Liegt also außerdem a' bereits zwischen 0 und $2h - 1$, so erfüllt die Form (a', b', c') alle Bedingungen.

II. Liegt dagegen a' außerhalb der Grenzen 0 und $2h - 1$, so sei A der kleinste positive Rest von a' modulo $2h$, der offenbar zwischen diesen Grenzen liegt; wir setzen $A - a' = 2hk$. Dann geht die Form (a', b', c'), *d.h.* $(a', h, 0)$, durch die Substitution $1, 0, k, 1$ in $(A, h, 0)$ über, die zu (a', b', c'), (a, b, c) eigentlich äquivalent ist und alle Bedingungen erfüllt. — Offenbar geht die Form (a, b, c) in $(A, h, 0)$ über, und zwar durch die Substitution $\alpha + \beta k, \beta, \gamma + \delta k, \delta$.

Beispiel. Gegeben sei die Form $(27, 15, 8)$ mit der Determinante $= 9$. Hier ist $h = 3$; den Verhältnissen $-12 : 27 = 8 : -18$ ist in kleinsten Zahlen das Verhältnis $4 : -9$ gleich. Setzen wir also $\beta = 4$, $\delta = -9$, $\alpha = -1$, $\gamma = 2$, so wird die Form (a', b', c') zu $(-1, 3, 0)$, die in $(5, 3, 0)$ übergeht, und zwar durch die Substitution $1, 0, 1, 1$. Das ist somit die gesuchte Form, und die gegebene geht durch die eigentliche Substitution $3, 4, -7, -9$ in sie über.

Solche Formen (A, B, C), bei denen $C = 0$, $B = h$ ist und A zwischen 0 und $2h - 1$ liegt, nennen wir *reduzierte Formen*. Sie müssen also von den reduzierten Formen mit negativer oder positiver nichtquadratischer Determinante sorgfältig unterschieden werden.

207.

Satz. *Zwei reduzierte Formen* $(a, h, 0)$, $(a', h, 0)$, *die nicht identisch sind, können nicht eigentlich äquivalent sein.*

Beweis. Nehmen wir an, sie seien eigentlich äquivalent, und die erste gehe durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$ in die zweite über. Dann haben wir vier Gleichungen:

$$a\alpha\alpha + 2h\alpha\gamma = a' \quad \ldots\ldots\ldots [1]$$
$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad \ldots\ldots\ldots [2]$$
$$a\beta\beta + 2h\beta\delta = 0 \quad \ldots\ldots\ldots [3]$$
$$\alpha\delta - \beta\gamma = 1 \quad \ldots\ldots\ldots [4]$$

Multiplizieren wir die zweite Gleichung mit β, die dritte mit α und subtrahieren, so folgt $-h(\alpha\delta - \beta\gamma)\beta = \beta h$ oder wegen [4] $-\beta h = \beta h$, also notwendig $\beta = 0$. Daher ergibt [4] $\alpha\delta = 1$ und $\alpha = \pm 1$. Aus [1] folgt dann $a \pm 2\gamma h = a'$. Diese Gleichung kann nur gelten, wenn $\gamma = 0$ ist (da sowohl a als auch a' nach Voraussetzung zwischen 0 und $2h - 1$ liegen), *d.h.*, wenn $a = a'$ ist oder die Formen $(a, h, 0)$, $(a', h, 0)$ identisch sind, entgegen der Voraussetzung.

Damit lassen sich die folgenden Aufgaben, die bei nichtquadratischen Determinanten viel größere Schwierigkeiten bereiteten, leicht lösen.

I. *Für zwei gegebene Formen F, F' mit derselben quadratischen Determinante untersuchen, ob sie eigentlich äquivalent sind.* Wir suchen zwei reduzierte Formen, die zu F, F' der Reihe nach eigentlich äquivalent sind. Sind diese identisch, so sind die gegebenen Formen eigentlich äquivalent; andernfalls nicht.

II. *Unter denselben Voraussetzungen untersuchen, ob sie uneigentlich äquivalent sind.* Die einer der gegebenen Formen, *z.B.* F, entgegengesetzte Form sei G. Ist diese zu F' eigentlich äquivalent, so sind F und F' uneigentlich äquivalent, und umgekehrt.

208.

Aufgabe. *Für zwei gegebene eigentlich äquivalente Formen F, F' mit der Determinante hh eine eigentliche Transformation der einen in die andere finden.*

Lösung. Zur Form F sei die reduzierte Form Φ eigentlich äquivalent, die somit nach Voraussetzung auch zu F' eigentlich äquivalent ist. Wir suchen nach Artikel 206 eine eigentliche Transformation von F in Φ, etwa $\alpha, \beta, \gamma, \delta$, und ebenso eine eigentliche Transformation von F' in Φ, etwa $\alpha', \beta', \gamma', \delta'$. Dann geht Φ in F' über, und zwar durch die eigentliche Substitution $\delta', -\beta', -\gamma', \alpha'$, und somit F in F' durch die eigentliche Substitution

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

Es lohnt sich, für diese Transformation von F in F' eine andere Formel herzuleiten, für die wir nicht einmal die reduzierte Form Φ selbst kennen müssen. Wir nehmen an:

$$F \text{ sei } (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0)$$

Da den Verhältnissen $h - b : a$ oder $c : -(h + b)$ in kleinsten Zahlen das Verhältnis $\beta : \delta$ gleich ist, sehen wir leicht, dass $\frac{h-b}{\beta} = \frac{a}{\delta}$ eine *ganze Zahl* ist; sie sei f. Ebenso ist $\frac{c}{\beta} = \frac{-h-b}{\delta}$ eine ganze Zahl; wir setzen sie $= g$. Wir haben

$$A = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma \quad \text{also}$$
$$\beta A = a\alpha\alpha\beta + 2b\alpha\beta\gamma + c\beta\gamma\gamma$$

oder, wenn wir für $a\beta$ den Wert $\delta(h - b)$ und für c den Wert βg einsetzen,

$$\beta A = \alpha\alpha\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta\beta\gamma\gamma g$$

oder wegen $b = -h - \delta g$

$$\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$$

Ebenso gilt

$$\begin{aligned}\delta A &= a\alpha\alpha\delta + 2b\alpha\gamma\delta + c\gamma\gamma\delta \\ &= \alpha\alpha\delta\delta f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma\gamma h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f\end{aligned}$$

Also

$$\alpha = \tfrac{\beta A - g}{2h}, \qquad \gamma = \tfrac{\delta A - f}{2h}$$

Setzen wir auf genau dieselbe Weise

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \qquad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g'$$

so ergibt sich

$$\alpha' = \tfrac{\beta' A - g'}{2h}, \qquad \gamma' = \tfrac{\delta' A - f'}{2h}$$

Setzen wir diese Werte von $\alpha, \gamma, \alpha', \gamma'$ in die eben angegebene Formel für die Transformation von F in F' ein, so geht sie über in

$$\tfrac{\beta f' - \delta' g}{2h}, \quad \tfrac{\beta' g - \beta g'}{2h}, \quad \tfrac{\delta f' - \delta' f}{2h}, \quad \tfrac{\beta' f - \delta g'}{2h}$$

woraus A ganz verschwunden ist.

Sind zwei uneigentlich äquivalente Formen F, F' gegeben und suchen wir eine uneigentliche Transformation der einen in die andere, so sei G die zu F entgegengesetzte Form und eine eigentliche Transformation von G in F' die folgende: $\alpha, \beta, \gamma.\ \delta$. Dann ist offenbar $\alpha, \beta, -\gamma, -\delta$ eine uneigentliche Transformation von F in F'.

Sind schließlich die gegebenen Formen sowohl eigentlich als auch uneigentlich äquivalent, so können wir auf diese Weise offenbar zwei Transformationen finden, eine eigentliche und eine uneigentliche.

209.

Es bleibt also nur noch zu zeigen, wie sich aus einer Transformation alle übrigen gleichartigen ableiten lassen. Das hängt von der Lösung der unbestimmten Gleichung $tt - hhuu = mm$ ab, wobei m den größten gemeinsamen Teiler von $a, 2b, c$ bezeichnet, wenn (a, b, c) eine der beiden äquivalenten Formen ist. Diese Gleichung lässt sich aber stets nur auf zwei Arten lösen: Wir setzen entweder $t = m$, $u = 0$ oder $t = -m$, $u = 0$. Nehmen wir nämlich an, es gebe noch eine andere Lösung $t = T$, $u = U$, wobei U nicht $= 0$ ist. Da mm sicher $4hh$ teilt, ist $\frac{4TT}{mm} = \frac{4hhUU}{mm} + 4$, und sowohl $\frac{4TT}{mm}$ als auch $\frac{4hhUU}{mm}$ sind ganze Quadratzahlen. Nun sehen wir leicht, dass 4 nur dann die Differenz zweier ganzer Quadratzahlen sein kann, wenn das kleinere Quadrat 0 ist, *d.h.* $U = 0$, entgegen der Voraussetzung. — Geht also die Form F in F' über, und zwar durch die Substitution $\alpha, \beta, \gamma, \delta$, so gibt es außer $-\alpha, -\beta, -\gamma, -\delta$ keine weitere dazu gleichartige Transformation. Sind daher zwei Formen entweder nur eigentlich oder nur uneigentlich äquivalent, so gibt es nur *zwei* Transformationen; sind sie sowohl eigentlich als auch uneigentlich äquivalent, so gibt es *vier*, nämlich zwei eigentliche und zwei uneigentliche.

210.

Satz. *Sind zwei reduzierte Formen* $(a, h, 0)$, $(a', h, 0)$ *uneigentlich äquivalent, so gilt* $aa' \equiv mm\ (mod.\ 2mh)$, *wobei* m *den größten gemeinsamen Teiler von* $a, 2h$ *oder* $a', 2h$ *bezeichnet. Haben umgekehrt* $a, 2h$; $a', 2h$ *denselben größten gemeinsamen Teiler* m *und gilt* $aa' \equiv mm\ (mod.\ 2mh)$, *so sind die Formen* $(a, h, 0)$, $(a', h, 0)$ *uneigentlich äquivalent.*

Beweis. I. Die Form $(a, h, 0)$ gehe in $(a', h, 0)$ über, und zwar durch die uneigentliche Substitution $\alpha, \beta, \gamma, \delta$, sodass wir vier Gleichungen haben:

$$a\alpha\alpha + 2h\alpha\gamma = a' \quad \ldots\ldots\ldots\ldots [1]$$

$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad \ldots\ldots\ldots [2]$$

$$a\beta\beta + 2h\beta\delta = 0 \quad \ldots\ldots\ldots\ldots [3]$$

$$\alpha\delta - \beta\gamma = -1 \quad \ldots\ldots\ldots\ldots [4]$$

Multiplizieren wir [4] mit h und ziehen es von [2] ab, was wir durch $[2] - h[4]$ ausdrücken, so ergibt sich

$$(a\alpha + 2h\gamma)\beta = 2h \quad \ldots\ldots\ldots\ldots [5]$$

Ebenso folgt aus $\gamma\delta[2] - \gamma\gamma[3] - (a + a\beta\gamma + h\gamma\delta)[4]$, nachdem die sich aufhebenden Glieder wegfallen,

$$-a\alpha\delta = a + 2h\gamma\delta, \quad \text{oder} \quad -(a\alpha + 2h\gamma)\delta = a \quad \ldots [6]$$

Schließlich erhalten wir $a[1] \dots a\alpha(a\alpha + 2h\gamma) = aa'$, oder

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

oder

$$(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)} \qquad \dots\dots [7]$$

Aus [5] und [6] folgt nun, dass $a\alpha + 2h\gamma$ sowohl $2h$ als auch a und somit auch m teilt, den größten gemeinsamen Teiler von $a, 2h$. Offenbar teilt aber m auch $a\alpha + 2h\gamma$. Also muss $a\alpha + 2h\gamma$ entweder $= +m$ oder $= -m$ sein. Daraus folgt nach [7] sofort $mm \equiv aa' \pmod{2mh}$. *Damit ist die Behauptung bewiesen.*

II. Haben $a, 2h$; $a', 2h$ denselben größten gemeinsamen Teiler m und ist außerdem $aa' \equiv mm \pmod{2mh}$, so sind $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa'-mm}{2mh}$ ganze Zahlen. Wir können leicht nachprüfen, dass die Form $(a, h, 0)$ in $(a', h, 0)$ übergeht, und zwar durch die Substitution $-\frac{a'}{m}, -\frac{2h}{m}, \frac{aa'-mm}{2mh}, \frac{a}{m}$, und dass diese Transformation uneigentlich ist. Daher sind jene Formen uneigentlich äquivalent. *Damit ist die Behauptung bewiesen.*

Damit lässt sich auch sofort entscheiden, ob eine gegebene reduzierte Form $(a, h, 0)$ zu sich selbst uneigentlich äquivalent ist. Bezeichnen wir den größten gemeinsamen Teiler von $a, 2h$ mit m, so muss $aa \equiv mm \pmod{2mh}$ gelten.

211.

Alle reduzierten Formen mit gegebener Determinante hh erhalten wir, indem wir in der unbestimmten Form $(A, h, 0)$ für A alle Zahlen von 0 bis $2h - 1$ einschließlich einsetzen. Ihre Anzahl ist also $2h$. Offenbar lassen sich alle Formen mit der Determinante hh in ebenso viele *Klassen* einteilen. Diese haben dieselben Eigenschaften, die wir oben (Artikel 175, 195) für die Klassen der Formen mit negativer und mit positiver nichtquadratischer Determinante besprochen haben. So zerfallen alle Formen mit der Determinante 25 in zehn Klassen, die wir anhand der in jeder enthaltenen reduzierten Form unterscheiden können. Diese reduzierten Formen sind $(0, 5, 0)$, $(1, 5, 0)$, $(2, 5, 0)$, $(5, 5, 0)$, $(8, 5, 0)$, $(9, 5, 0)$, die zugleich zu sich selbst uneigentlich äquivalent sind; $(3, 5, 0)$, zu der $(7, 5, 0)$ uneigentlich äquivalent ist; und $(4, 5, 0)$, zu der $(6, 5, 0)$ uneigentlich äquivalent ist.

212.

Aufgabe. *Alle Darstellungen einer gegebenen Zahl M durch eine gegebene Form $axx + 2bxy + cyy$ mit der Determinante hh finden.*

Die Lösung dieser Aufgabe lässt sich aus den Grundsätzen von Artikel 168 genauso ableiten, wie wir es oben (Artikel 180, 181, 205) für Formen mit negativer und mit positiver nichtquadratischer Determinante gezeigt haben. Da dies keine Schwierigkeit macht, wäre es überflüssig, es hier zu wiederholen. Es ist aber sinnvoll, die Lösung aus einem anderen Grundsatz abzuleiten, der dem vorliegenden Fall eigen ist.

Setzen wir wie in den Artikeln 206, 208

$$h - b : a = c : -(h + b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g$$

so lässt sich leicht beweisen, dass die gegebene Form das Produkt der Faktoren $\delta x - \beta y$ und $fx - gy$ ist. Daher liefert jede Darstellung von M durch die gegebene Form eine Zerlegung von M in zwei Faktoren. Sind also alle Teiler von M gleich d, d', d'' usw. (einschließlich 1 und M, wobei jeder *zweimal*, sowohl positiv als auch negativ, zu nehmen ist), so erhalten wir offenbar alle Darstellungen von M, indem wir nacheinander

$$\delta x - \beta y = d, \qquad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \qquad fx - gy = \frac{M}{d'} \quad \text{usw.}$$

setzen, daraus die Werte von x, y ermitteln und diejenigen Darstellungen verwerfen, bei denen x oder y gebrochene Werte annehmen. Aus den beiden ersten Gleichungen folgt offenbar

$$x = \tfrac{\beta M - gdd}{(\beta f - \delta g)d} \quad \text{und} \quad y = \tfrac{\delta M - fdd}{(\beta f - \delta g)d}$$

Diese Werte sind immer *bestimmt*, denn $\beta f - \delta g = 2h$, und daher ist der Zähler sicher nicht $= 0$. — Auch die übrigen Aufgaben hätten sich aus demselben Grundsatz lösen lassen, nämlich dass jede Form mit quadratischer Determinante in zwei Faktoren zerlegt werden kann. Wir haben es aber vorgezogen, auch hier eine Methode zu verwenden, die der oben für Formen mit nichtquadratischer Determinante angegebenen entspricht.

Beispiel. Gesucht sind alle Darstellungen von 12 durch $3xx + 4xy - 7yy$. Diese Form zerfällt in die Faktoren $x - y$ und $3x + 7y$. Alle Teiler von 12 sind $\pm 1, 2, 3, 4, 6, 12$. Setzen wir $x - y = 1$, $3x + 7y = 12$, so ergibt sich $x = \frac{19}{10}$, $y = \frac{9}{10}$; diese Werte müssen wir als gebrochene verwerfen. Ebenso ergeben die Teiler $-1, \pm 3, \pm 4, \pm 6, \pm 12$ unbrauchbare Werte. Der Teiler $+2$ liefert dagegen $x = 2, y = 0$, und -2 liefert $x = -2$, $y = 0$. Außer diesen beiden gibt es also keine weiteren Darstellungen.

Diese Methode lässt sich nicht anwenden, wenn $M = 0$ ist. In diesem Fall müssen offenbar alle Werte von x, y entweder die Gleichung $\delta x - \beta y = 0$ oder $fx - gy = 0$ erfüllen. Alle Lösungen der ersten Gleichung sind in der Formel $x = \beta z$, $y = \delta z$ enthalten, wobei z alle ganzen Zahlen durchläuft (denn β, δ sind wie vorausgesetzt teilerfremd). Setzen wir ebenso den größten gemeinsamen Teiler von $f, g = m$, so

werden alle Lösungen der zweiten Gleichung durch $x = \frac{gz}{m}, y = \frac{hz}{m}$ dargestellt. Diese beiden allgemeinen Formeln umfassen daher alle Darstellungen von M in diesem Fall.

* *
*

Im Vorhergehenden haben wir alles behandelt, was zur Erkennung der Äquivalenz, zur Bestimmung aller Transformationen von Formen und zur Ermittlung aller Darstellungen gegebener Zahlen durch gegebene Formen gehört, sodass nichts mehr zu wünschen übrig zu bleiben scheint. Es bleibt daher nur noch zu zeigen, wie wir bei zwei gegebenen Formen, die wegen der *Ungleichheit ihrer Determinanten* nicht äquivalent sein können, entscheiden, ob die eine unter der anderen enthalten ist, und in diesem Fall alle Transformationen der ersten in die zweite finden.

Formen, die unter anderen enthalten sind, ohne ihnen äquivalent zu sein.

213.

Oben in den Artikeln 157, 158 haben wir gezeigt: Enthält eine Form f mit der Determinante D eine Form F mit der Determinante E und geht sie durch die Substitution $\alpha, \beta, \gamma, \delta$ in diese über, so ist $E = (\alpha\delta - \beta\gamma)^2 D$. Ist $\alpha\delta - \beta\gamma = \pm 1$, so enthält die Form f nicht nur F, sondern ist ihr auch äquivalent. Wenn also f die Form F enthält, ihr aber nicht äquivalent ist, so ist der Quotient $\frac{E}{D}$ eine ganze Zahl größer als 1. Wir müssen daher jetzt *entscheiden, ob eine gegebene Form f mit der Determinante D eine gegebene Form F mit der Determinante Dee enthält*, wobei e als positive Zahl größer als 1 vorausgesetzt wird. Dazu zeigen wir, wie sich endlich viele unter f enthaltene Formen so angeben lassen, dass F, falls sie unter f enthalten ist, notwendig einer von ihnen äquivalent sein muss.

I. Alle positiven Teiler von e (einschließlich 1 und e) seien m, m', m'' usw., und es sei $e = mn = m'n' = m''n''$ usw. Der Kürze wegen bezeichnen wir die Form, in die f durch die eigentliche Substitution $m. 0, 0, n$ übergeht, mit $(m; 0)$, die Form, in die f durch die eigentliche Substitution $m, 1, 0, n$ übergeht, mit $(m; 1)$ usw. Allgemein bezeichnen wir die Form, in die f durch die eigentliche Substitution $m, k, 0, n$ übergeht, mit $(m; k)$. Ebenso gehe f durch die eigentliche Substitution $m', 0, 0, n'$ in $(m'; 0)$, durch $m', 1, 0, n'$ in $(m'; 1)$ usw., durch $m'', 0, 0, n''$ in $(m''; 0)$ usw. über. Alle diese Formen sind unter f eigentlich enthalten, und jede hat die Determinante $= Dee$. Die Gesamtheit aller Formen $(m; 0)$, $(m; 1)$, $(m; 2) \ldots (m; m-1)$, $(m'; 0)$, $(m'; 1) \ldots (m'; m'-1)$; $(m''; 0)$ usw., deren Anzahl $m + m' + m'' +$ usw. ist und die offenbar alle verschieden sind, bezeichnen wir mit Ω.

Ist *z.B.* die Form f gleich $(2, 5, 7)$ und gilt $e = 5$, so enthält Ω die folgenden sechs Formen: $(1; 0)$, $(5; 0)$, $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$. Ausgeschrieben sind dies $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$.

II. Ich behaupte nun: Ist eine Form F mit der Determinante Dee unter f eigentlich enthalten, so muss sie einer der Formen Ω eigentlich äquivalent sein. Nehmen wir an, die Form f gehe in F über, und zwar durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$. Dann ist $\alpha\delta - \beta\gamma = e$. Der größte gemeinsame Teiler der Zahlen γ, δ (die nicht beide 0 sein können), positiv genommen, sei $= n$, und es sei $\frac{e}{n} = m$, was offenbar eine ganze Zahl ist. Wir wählen g, h so, dass $\gamma g + \delta h = n$ ist, und schließlich sei k der kleinste positive Rest von $\alpha g + \beta h$ modulo m. Dann ist $(m; k)$, die offenbar zu den Formen Ω gehört, der Form F eigentlich äquivalent und geht durch die eigentliche Substitution

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

in sie über. Denn *erstens* sind diese vier Zahlen offenbar ganze Zahlen; *zweitens* lässt sich leicht nachprüfen, dass die Substitution eigentlich ist; *drittens* ist die Form, in die $(m; k)$ durch diese Substitution übergeht, offenbar dieselbe wie die, in die f[*)] durch die Substitution

$$m\left(\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h\right) + \frac{k\gamma}{n}, \quad m\left(\frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g\right) + \frac{k\delta}{n}, \quad \gamma, \quad \delta$$

[*)] Sie geht nämlich durch die Substitution $m, k, 0, n$ in $(m; k)$ über. Siehe Artikel 159.

übergeht, oder wegen $mn = e = \alpha\delta - \beta\gamma$ und daher $\beta\gamma + mn = \alpha\delta$, $\alpha\delta - mn = \beta\gamma$ durch

$$\frac{1}{n}(\alpha\gamma g + \alpha\delta h), \quad \frac{1}{n}(\beta\gamma g + \beta\delta h), \quad \gamma, \quad \delta$$

oder schließlich wegen $\gamma g + \delta h = n$ durch $\alpha, \beta, \gamma, \delta$, *d.h.* nach Voraussetzung in F. Also sind $(m; k)$ und F eigentlich äquivalent. *Damit ist die Behauptung bewiesen.*

So lässt sich immer entscheiden, ob eine gegebene Form f mit der Determinante D eine Form F mit der Determinante *Dee* eigentlich enthält. Wollen wir entscheiden, ob f die Form F uneigentlich enthält, brauchen wir nur zu untersuchen, ob die zu F entgegengesetzte Form unter f eigentlich enthalten ist (Artikel 159).

214.

Aufgabe. *Für zwei gegebene Formen, f mit der Determinante D und F mit der Determinante Dee, von denen die erste die zweite eigentlich enthält, alle eigentlichen Transformationen von f in F angeben.*

Lösung. Mit Ω bezeichnen wir dieselbe Gesamtheit von Formen wie im vorhergehenden Artikel. Daraus wählen wir alle Formen aus, denen F eigentlich äquivalent ist; sie seien Φ, Φ', Φ'' usw. Jede dieser Formen liefert auf die folgende Weise eigentliche Transformationen von f in F, wobei verschiedene Formen verschiedene Transformationen liefern (*d.h.* jede Form liefert andere), alle zusammen aber sämtliche (*d.h.* es gibt keine eigentliche Transformation von f in F, die nicht von einer der Formen Φ, Φ' usw. geliefert wird). Da die Methode für alle Formen Φ, Φ' usw. dieselbe ist, sprechen wir nur von einer.

Es sei Φ gleich $(M; K)$ und $e = MN$, sodass f in Φ übergeht, und zwar durch die eigentliche Substitution $M, K, 0, N$. Ferner bezeichnen wir alle eigentlichen Transformationen von Φ in F mit $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$. Dann geht offenbar f in Φ über, und zwar durch die eigentliche Substitution $M\mathfrak{a} + K\mathfrak{c}, M\mathfrak{b} + K\mathfrak{d}, N\mathfrak{c}, N\mathfrak{d}$. Auf diese Weise liefert jede eigentliche Transformation von Φ in F eine eigentliche Transformation von f in F. — Die übrigen Formen Φ', Φ'' usw. behandeln wir genauso: Jede ihrer eigentlichen Transformationen in F liefert eine eigentliche Transformation von f in F.

Um zu sehen, dass diese Lösung in jeder Hinsicht vollständig ist, müssen wir zeigen:

I. *Auf diese Weise erhalten wir alle möglichen eigentlichen Transformationen von f in F.* Eine beliebige eigentliche Transformation von f in F sei $\alpha, \beta, \gamma, \delta$, und wie in II des vorhergehenden Artikels sei n der größte gemeinsame Teiler von γ, δ. Die Zahlen m, g, h, k bestimmen wir wie dort. Dann ist $(m; k)$ unter den Formen Φ, Φ' usw. enthalten, und

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

ist eine ihrer eigentlichen Transformationen in F. Daraus erhalten wir nach der eben angegebenen Regel die Transformation $\alpha, \beta, \gamma, \delta$. Dies alles wurde im vorhergehenden Artikel bewiesen.

II. *Alle auf diese Weise entstehenden Transformationen sind verschieden; keine wird zweimal erhalten.* Wir sehen leicht, dass verschiedene Transformationen derselben Form Φ oder Φ' usw. in F nicht dieselbe Transformation von f in F erzeugen können. Dass aber auch verschiedene Formen, *z.B.* Φ und Φ', nicht dieselbe Transformation liefern können, beweisen wir so. Nehmen wir an, die eigentliche Transformation $\alpha, \beta, \gamma, \delta$ von f in F werde *sowohl* aus der eigentlichen Transformation $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ von Φ in F *als auch* aus der eigentlichen Transformation $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \mathfrak{d}'$ von Φ' in F erhalten. Es sei $\Phi = (M; K)$, $\Phi' = (M'; K')$, $e = MN = M'N'$. Dann haben wir die Gleichungen

$$\begin{aligned}
\alpha &= M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' && \ldots\ldots [1]\\
\beta &= M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}' && \ldots\ldots [2]\\
\gamma &= N\mathfrak{c} = N'\mathfrak{c}' && \ldots\ldots\ldots [3]\\
\delta &= N\mathfrak{d} = N'\mathfrak{d}' && \ldots\ldots\ldots [4]\\
\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} &= \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1 && \ldots\ldots\ldots [5]
\end{aligned}$$

Aus $\mathfrak{a}[4] - \mathfrak{b}[3]$ folgt mithilfe von Gleichung [5] $N = N'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}')$, also teilt N' die Zahl N. Ebenso ergibt $\mathfrak{a}'[4] - \mathfrak{b}'[3]$ die Gleichung $N(\mathfrak{a}'\mathfrak{d} - \mathfrak{b}'\mathfrak{c}) = N'$, also teilt N die Zahl N'. Da sowohl N als auch N' als positiv vorausgesetzt werden, muss $N = N'$ und $M = M'$ sein. Aus [3] und [4] folgt dann $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{d} = \mathfrak{d}'$. Ferner folgt aus $\mathfrak{a}[2] - \mathfrak{b}[1]$

$$K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$$

also $K \equiv K' \pmod{M}$. Das ist nur möglich, wenn $K = K'$ ist, denn sowohl K als auch K' liegen zwischen 0 und $M-1$. Daher sind die Formen Φ, Φ' nicht verschieden, entgegen der Voraussetzung.

Ist D negativ oder positiv quadratisch, so lassen sich mit dieser Methode offenbar alle eigentlichen Transformationen von f in F tatsächlich finden. Ist dagegen D positiv und nichtquadratisch, so können wir allgemeine Formeln angeben, die alle eigentlichen Transformationen enthalten, deren Anzahl unendlich ist.

Ist schließlich die Form F unter der Form f uneigentlich enthalten, so lassen sich nach der angegebenen Methode alle uneigentlichen Transformationen der ersten in die zweite leicht darstellen. Sollen nämlich $\alpha, \beta, \gamma, \delta$ alle eigentlichen Transformationen von f in die zu F entgegengesetzte Form durchlaufen, so werden alle uneigentlichen Transformationen von f in F durch $\alpha, -\beta, \gamma, -\delta$ dargestellt.

Beispiel. Gesucht sind alle Transformationen von $(2, 5, 7)$ in $(275, 0, -1)$, die sowohl eigentlich als auch uneigentlich unter der ersten enthalten ist. Die Gesamtheit Ω für diesen Fall haben wir schon im vorhergehenden Artikel angegeben. Bei der Untersuchung finden wir, dass sowohl $(5; 1)$ als auch $(5; 4)$ der Form $(275, 0, -1)$ eigentlich äquivalent sind. Nach unserer oben entwickelten Theorie sind alle eigentlichen Transformationen von $(5; 1)$, *d.h.* $(50, 35, 19)$, in $(275, 0, -1)$ in der allgemeinen Formel

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u$$

enthalten, wobei t, u alle ganzen Zahlen durchlaufen, die $tt - 275uu = 1$ erfüllen. Daher sind alle daraus entstehenden eigentlichen Transformationen von $(2, 5, 7)$ in

$(275, 0, -1)$ in der allgemeinen Formel

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u$$

enthalten. Ebenso sind alle eigentlichen Transformationen von $(5, 4)$, *d.h.* $(50, 65, 79)$, in $(275, 0, -1)$ in der allgemeinen Formel

$$14t + 275u, \quad t + 14u, \quad -15t - 275u, \quad -t - 15u$$

enthalten und somit alle daraus entstehenden eigentlichen Transformationen von $(2, 5, 7)$ in $(275, 0, -1)$ in

$$10t + 275u, \quad t + 10u, \quad -15t - 275u, \quad -t - 15u$$

enthalten. Diese beiden Formeln umfassen also alle gesuchten eigentlichen Transformationen[*)]. — Auf dieselbe Weise finden wir, dass alle uneigentlichen Transformationen von $(2, 5, 7)$ in $(275, 0, -1)$ in den folgenden beiden Formeln enthalten sind:

$$\text{(I)} \ \ldots \quad 65t - 1100u, \quad 4t - 65u, \quad -15t + 275u, \quad -t + 15u$$

und

$$\text{(II)} \ \ldots \quad 10t + 275u, \quad -t - 10u, \quad -15t - 275u, \quad t + 15u$$

[*)] Eleganter werden alle eigentlichen Transformationen durch die Formel

$$10t + 55u, \quad t + 2u, \quad -15t - 55u, \quad -t - 3u$$

dargestellt, wobei t, u alle ganzen Zahlen durchlaufen, die $tt - 11uu = 1$ erfüllen.

Formen mit der Determinante 0.

215.

Bisher haben wir Formen mit der Determinante 0 aus allen Untersuchungen ausgeschlossen. Damit unsere Theorie in jeder Hinsicht vollständig wird, müssen wir noch einiges über sie hinzufügen. Wir haben allgemein bewiesen: Enthält eine Form mit der Determinante D eine Form mit der Determinante D', so ist D' ein Vielfaches von D. Daher kann eine Form mit der Determinante $= 0$ offenbar nur eine Form enthalten, deren Determinante ebenfalls $= 0$ ist. Es bleiben also nur zwei Aufgaben: 1° *Für zwei gegebene Formen f, F, von denen die zweite die Determinante 0 hat, entscheiden, ob die erste die zweite enthält, und in diesem Fall alle Transformationen der ersten in die zweite angeben.* 2° *Alle Darstellungen einer gegebenen Zahl durch eine gegebene Form mit der Determinante 0 finden.* Die erste Aufgabe erfordert eine andere Methode, wenn die Determinante der ersten Form f ebenfalls 0 ist, als wenn sie nicht 0 ist. Dies alles behandeln wir jetzt.

I. Zunächst bemerken wir, dass sich jede Form $axx + 2bxy + cyy$ mit der Determinante $bb - ac = 0$ als $m(gx + hy)^2$ schreiben lässt, wobei g, h teilerfremd sind und m eine ganze Zahl ist. Sei nämlich m der größte gemeinsame Teiler von a, c, mit demselben Vorzeichen genommen wie diese Zahlen selbst (dass sie keine entgegengesetzten Vorzeichen haben können, sehen wir leicht). Dann sind $\frac{a}{m}, \frac{c}{m}$ teilerfremde nichtnegative ganze Zahlen. Ihr Produkt ist $= \frac{bb}{mm}$, *d.h.* eine Quadratzahl, und daher sind sie selbst Quadratzahlen (Artikel 21). Sei $\frac{a}{m} = gg$, $\frac{c}{m} = hh$. Dann sind auch g, h teilerfremd; außerdem gilt $gghh = \frac{bb}{mm}$ und $gh = \pm\frac{b}{m}$. Daraus folgt offenbar

$$m(gx \pm hy)^2 = axx + 2bxy + cyy$$

Nun seien zwei Formen f, F gegeben, beide mit der Determinante 0, und es sei

$$f = m(gx + hy)^2, \quad F = M(GX + HY)^2$$

wobei g zu h und G zu H teilerfremd ist. Ich behaupte: Enthält f die Form F, so ist m entweder gleich M oder teilt zumindest M, und der Quotient ist eine Quadratzahl. Ist umgekehrt $\frac{M}{m}$ eine ganze Quadratzahl, so ist F unter f enthalten. Nehmen wir nämlich an, f gehe durch die Substitution

$$x = \alpha X + \beta Y, \quad y = \gamma X + \delta Y$$

in F über. Dann ist

$$\frac{M}{m}(GX + HY)^2 = ((\alpha g + \gamma h)X + (\beta g + \delta h)Y)^2$$

woraus leicht folgt, dass $\frac{M}{m}$ eine Quadratzahl ist. Wir setzen sie $= ee$ und erhalten

$$e(GX + HY) = \pm((\alpha g + \gamma h)X + (\beta g + \delta h)Y), \quad d.h.$$

$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h$$

Bestimmen wir also $\mathfrak{G}, \mathfrak{H}$ so, dass $\mathfrak{G}G + \mathfrak{H}H = 1$ ist, so gilt

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h), \quad \text{also } \textit{ganzzahlig.} \quad \textit{Q.E.D.}$$

Nehmen wir umgekehrt an, $\frac{M}{m}$ sei eine ganze Quadratzahl $= ee$, so enthält die Form f die Form F. Wir können nämlich ganze Zahlen $\alpha, \beta, \gamma, \delta$ so bestimmen, dass

$$\alpha g + \gamma h = \pm eG, \quad \beta g + \delta h = \pm eH$$

gilt. Dazu wählen wir ganze Zahlen $\mathfrak{g}, \mathfrak{h}$ so, dass $\mathfrak{g}g + \mathfrak{h}h = 1$ ist. Jene Gleichungen werden erfüllt, wenn wir

$$\begin{aligned} \alpha &= \pm eG\mathfrak{g} + hz, & \gamma &= \pm eG\mathfrak{h} - gz \\ \beta &= \pm eH\mathfrak{g} + hz', & \delta &= \pm eH\mathfrak{h} - gz' \end{aligned}$$

setzen, welche ganzzahligen Werte wir auch z, z' geben. Daher ist F unter f enthalten. *Damit ist die Behauptung bewiesen.* Zugleich sehen wir leicht, dass diese Formeln alle möglichen Werte von $\alpha, \beta, \gamma, \delta$, *d.h.* alle Transformationen von f in F, angeben, wenn z, z' alle ganzen Zahlen durchlaufen.

II. Für zwei gegebene Formen $f = axx + 2bxy + cyy$ mit einer Determinante nicht $= 0$ und $F = M(GX + HY)^2$ mit der Determinante $= 0$ (wobei G, H wie zuvor teilerfremd sind) behaupte ich *erstens*: Enthält f die Form F, so lässt sich die Zahl M durch f darstellen; *zweitens*: Lässt sich M durch f darstellen, so ist F unter f enthalten; *drittens*: Werden in diesem Fall alle Darstellungen von M durch f mit $x = \xi, y = \upsilon$ angegeben, so werden alle Transformationen von f in F durch $G\xi, H\zeta, G\upsilon, H\upsilon$ dargestellt. Dies alles beweisen wir folgendermaßen.

1° Nehmen wir an, f gehe in F über, und zwar durch die Substitution $\alpha, \beta, \gamma, \delta$, und wählen wir $\mathfrak{G}, \mathfrak{H}$ so, dass $\mathfrak{G}G + \mathfrak{H}H = 1$ ist. Setzen wir dann $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, so wird der Wert von f offenbar gleich M, und somit ist M durch f darstellbar.

2° Nehmen wir an, $a\xi\xi + 2b\xi\upsilon + c\upsilon\upsilon = M$ sei erfüllt. Durch die Substitution $G\xi, H\xi, G\upsilon, H\upsilon$ geht die Form f offenbar in F über. Dass aber

3° in diesem Fall die Substitution $G\xi, H\zeta, G\upsilon, H\upsilon$ *alle* Transformationen von f in F angibt, wenn ξ, υ alle Werte von x, y darstellen, für die $f = M$ ist, sehen wir so. Sei $\alpha, \beta, \gamma, \delta$ eine beliebige Transformation von f in F, und wie zuvor gelte $\mathfrak{G}G + \mathfrak{H}H = 1$. Unter den Werten von x, y befinden sich dann auch

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H}, \quad y = \gamma\mathfrak{G} + \delta\mathfrak{H}$$

woraus sich die Substitution

$$G(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad H(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad G(\gamma\mathfrak{G} + \delta\mathfrak{H}), \quad H(\gamma\mathfrak{G} + \delta\mathfrak{H})$$

ergibt, oder

$$\begin{aligned} &\alpha + \mathfrak{H}(\beta G - \alpha H), & &\beta + \mathfrak{G}(\alpha H - \beta G) \\ &\gamma + \mathfrak{H}(\delta G - \gamma H), & &\delta + \mathfrak{G}(\gamma H - \delta G) \end{aligned}$$

Da aber

$$a(\alpha X+\beta Y)^2+2b(\alpha X+\beta Y)(\gamma X+\delta Y) \\ +c(\gamma X+\delta Y)^2=M(GX+HY)^2$$

gilt, ist

$$a(\alpha\delta-\beta\gamma)^2=M(\delta G-\gamma H)^2$$
$$c(\beta\gamma-\alpha\delta)^2=M(\beta G-\alpha H)^2$$

und daher (weil die Determinante von f, mit $(\alpha\delta-\beta\gamma)^2$ multipliziert, gleich der Determinante von F, *d.h.* $=0$, und somit auch $\alpha\delta-\beta\gamma=0$ ist)

$$\delta G-\gamma H=0,\quad \beta G-\alpha H=0$$

Jene Substitution geht damit in $\alpha,\beta,\gamma,\delta$ über. Daher liefert die angegebene Formel *alle* Transformationen von f in F.

III. Es bleibt zu zeigen, wie sich alle Darstellungen einer gegebenen Zahl durch eine gegebene Form mit der Determinante 0 angeben lassen. Sei die Form $m(gx+hy)^2$. Offenbar muss jene Zahl durch m teilbar und der Quotient eine Quadratzahl sein. Setzen wir also die gegebene Zahl $=mee$, so ist für dieselben Werte von x,y, für die $m(gx+hy)^2=mee$ gilt, offenbar $gx+hy$ entweder $=+e$ oder $=-e$. Wir erhalten daher alle Darstellungen, indem wir alle ganzzahligen Lösungen der linearen Gleichungen $gx+hy=e$, $gx+hy=-e$ bestimmen. Dass diese lösbar sind, ist bekannt, denn g,h sind wie vorausgesetzt teilerfremd. Bestimmen wir nämlich $\mathfrak{g},\mathfrak{h}$ so, dass $\mathfrak{g}g+\mathfrak{h}h=1$ ist, so erfüllen wir die erste Gleichung durch $x=\mathfrak{g}e+hz$, $y=\mathfrak{h}e-gz$, die zweite dagegen durch $x=-\mathfrak{g}e+hz$, $y=-\mathfrak{h}e-gz$, wobei z eine beliebige ganze Zahl bezeichnet. Zugleich geben diese Formeln *alle* ganzzahligen Werte von x,y an, wenn z alle ganzen Zahlen durchläuft.

Allgemeine Lösung aller unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten in ganzen Zahlen.

Zum Abschluss dieser Untersuchungen fügen wir hinzu:

216.

Aufgabe. *Alle ganzzahligen Lösungen der allgemeinen*[*)] *unbestimmten Gleichung zweiten Grades mit zwei Unbekannten*

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

finden (wobei a, b, c usw. beliebige gegebene ganze Zahlen sind).

Lösung. Anstelle der Unbekannten x, y führen wir

$$p = (bb - ac)x + be - cd \quad \text{und} \quad q = (bb - ac)y + bd - ae$$

ein. Diese sind offenbar immer ganze Zahlen, wenn x, y ganze Zahlen sind. Damit erhalten wir die Gleichung

$$app + 2bpq + cqq + f(bb - ac)^2 + (bb - ac)(aee - 2bde + cdd) = 0$$

oder, wenn wir der Kürze wegen

$$f(bb - ac)^2 + (bb - ac)(aee - 2bde + cdd) = -M$$

setzen, die Gleichung

$$app + 2bpq + cqq = M$$

Wir haben im Vorhergehenden gezeigt, wie wir alle Lösungen dieser Gleichung, *d.h.* alle Darstellungen von M durch (a, b, c), finden können. Bestimmen wir nun aus den einzelnen Werten von p, q die entsprechenden Werte von x, y mithilfe der Gleichungen

$$x = \frac{p + cd - be}{bb - ac}, \quad y = \frac{q + ae - bd}{bb - ac}$$

so sehen wir leicht, dass alle diese Werte die gegebene Gleichung erfüllen und dass es keine ganzzahligen Werte von x, y gibt, die wir auf diese Weise nicht erhalten. Verwerfen wir also unter allen so entstehenden Werten von x, y die gebrochenen, so bleiben alle gesuchten Lösungen übrig.

Zu dieser Lösung ist Folgendes zu bemerken.

1° Lässt sich entweder M nicht durch (a, b, c) darstellen, oder ergeben sich aus keiner Darstellung *ganzzahlige* Werte von x, y, so hat die Gleichung keine ganzzahlige Lösung.

2° Ist die Determinante von (a, b, c), *d.h.* $bb - ac$, negativ, oder ist sie positiv quadratisch und ist zugleich M nicht $= 0$, so ist die Anzahl der Darstellungen von M durch (a, b, c) endlich. Daher ist auch die Anzahl aller Lösungen der gegebenen Gleichung, wenn es überhaupt welche gibt, endlich.

[*)] Ist eine Gleichung gegeben, deren zweiter, vierter oder fünfter Koeffizient nicht gerade ist, so erhält sie durch Multiplikation mit 2 die hier vorausgesetzte Form.

3º Ist $bb-ac$ positiv und nichtquadratisch oder quadratisch und zugleich $M = 0$, so lässt sich M, wenn überhaupt, auf *unendlich viele verschiedene Arten* durch (a, b, c) darstellen. Da es aber unmöglich ist, alle diese Darstellungen *selbst* zu finden und zu prüfen, ob sie ganzzahlige oder gebrochene Werte von x, y liefern, brauchen wir eine Regel, mit der wir *Gewissheit* erlangen können, falls überhaupt keine Darstellung ganzzahlige Werte von x, y liefert (denn wie viele Darstellungen wir in diesem Fall auch *prüfen*, ohne eine solche Regel würden wir nie Gewissheit erreichen). Liefern dagegen einige Darstellungen ganzzahlige Werte von x, y, andere gebrochene, so müssen wir zeigen, wie wir die letzteren von den ersteren im Voraus allgemein unterscheiden können.

4º Ist $bb-ac = 0$, so lassen sich die Werte von x, y mit den vorhergehenden Formeln überhaupt nicht bestimmen. Daher müssen wir für diesen Fall eine *besondere Methode* finden.

217.

Für den Fall, dass $bb - ac$ eine positive Nichtquadratzahl ist, haben wir oben gezeigt, dass sich alle Darstellungen der Zahl M durch die Form $app + 2bpq + cqq$ (falls es überhaupt welche gibt) durch eine oder mehrere Formeln der folgenden Art angeben lassen:

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

Dabei bezeichnen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ gegebene ganze Zahlen, m den größten gemeinsamen Teiler der Zahlen $a, 2b, c$ und schließlich t, u sämtliche ganzen Zahlen, die der Gleichung $tt - (bb - ac)uu = mm$ genügen. Da alle Werte von t, u sowohl positiv als auch negativ genommen werden können, können wir jede jener Formeln durch *vier* andere ersetzen:

$$\begin{aligned} p &= \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), & q &= \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \\ p &= \tfrac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), & q &= \tfrac{1}{m}(\mathfrak{C}t - \mathfrak{D}u) \\ p &= \tfrac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), & q &= \tfrac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u) \\ p &= -\tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), & q &= -\tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \end{aligned}$$

Die Gesamtzahl der Formeln ist jetzt viermal so groß wie vorher; t und u bezeichnen aber nicht mehr alle Zahlen, die der Gleichung $tt - (bb - ac)uu = mm$ genügen, sondern nur die positiven. Jede dieser Formen muss daher einzeln betrachtet und darauf untersucht werden, welche Werte von t, u ganzzahlige Werte von x, y liefern.

Aus der Formel

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \qquad \ldots . \; [1]$$

folgen diese Werte von x, y:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(bb - ac)}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(bb - ac)}$$

Oben haben wir aber gezeigt, dass alle (positiven) Werte von t eine rekurrente Folge t^0, t', t'' usw. bilden und dass die zugehörigen Werte von u ebenfalls eine rekurrente Folge u^0, u', u'' usw. bilden. Außerdem lässt sich eine Zahl ρ so angeben, dass für jeden gegebenen Modul gilt:

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad t^{\rho+2} \equiv t'' \text{ usw.}, \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u' \text{ usw.}$$

Als diesen Modul nehmen wir die Zahl $m(bb - ac)$. Der Kürze wegen bezeichnen wir die Werte von x, y, die sich durch Setzen von $t = t^0$, $u = u^0$ ergeben und denen wir den Index 0 zuordnen, mit x^0, y^0; ebenso die durch Setzen von $t = t'$, $u = u'$ entstehenden Werte mit x', y', denen wir den Index 1 zuordnen, usw. Man sieht dann ohne Mühe: Sind x^h, y^h ganze Zahlen und ist ρ richtig bestimmt, so sind auch $x^{h+\rho}, y^{h+\rho}$, ebenso $x^{h+2\rho}, y^{h+2\rho}$ und allgemein $x^{h+k\rho}, y^{h+k\rho}$ ganze Zahlen. Ist dagegen x^h oder y^h gebrochen, so ist auch $x^{h+k\rho}$ beziehungsweise $y^{h+k\rho}$ gebrochen. Daraus folgt leicht: Berechnet man die Werte von x, y mit den Indizes $0, 1, 2 \ldots \rho - 1$, und sind für keinen dieser Indizes *sowohl x als auch y* ganzzahlig, so gibt es überhaupt keinen Index, für den sowohl x als auch y ganze Werte annehmen. In diesem Fall

lassen sich aus Formel [1] keine ganzzahligen Werte von x, y ableiten. Gibt es aber unter jenen Indizes einige, etwa μ, μ', μ'' usw., denen ganzzahlige Werte von x, y entsprechen, so sind sämtliche ganzzahligen Werte von x, y, die sich aus Formel [1] gewinnen lassen, diejenigen, deren Indizes in einer der Formeln $\mu+k\rho$, $\mu'+k\rho$, $\mu''+k\rho$ usw. enthalten sind. Dabei durchläuft k alle positiven ganzen Zahlen, einschließlich der Null.

Die übrigen Formeln, in denen die Werte von p, q enthalten sind, müssen genauso behandelt werden. Sollte keine dieser Formeln ganzzahlige Werte von x, y liefern, so wäre die vorgelegte Gleichung überhaupt nicht in ganzen Zahlen lösbar. Ist sie aber tatsächlich lösbar, so lassen sich alle ganzzahligen Lösungen nach den oben angegebenen Regeln darstellen.

218.

Ist $bb - ac$ eine Quadratzahl und $M = 0$, so sind alle Werte von p, q in zwei Formeln der Art $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$ enthalten. Dabei durchläuft z alle ganzen Zahlen, während $\mathfrak{A}, \mathfrak{B}, \mathfrak{A}', \mathfrak{B}'$ gegebene ganze Zahlen sind, von denen die erste und zweite sowie die dritte und vierte jeweils teilerfremd sind (Artikel 212). Alle ganzzahligen Werte von x, y, die aus der ersten Formel entstehen, sind also in Formel [1] enthalten:

$$x = \frac{\mathfrak{A}z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{bb - ac}$$

Alle übrigen, die aus der zweiten Formel entstehen, sind in dieser Formel [2] enthalten:

$$x = \frac{\mathfrak{A}'z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{bb - ac}$$

Da aber beide Formeln auch gebrochene Werte liefern können (außer wenn $bb - ac = 1$), müssen wir in jeder Formel diejenigen Werte von z, die sowohl x als auch y ganzzahlig machen, von den übrigen trennen. Es genügt jedoch, nur die erste Formel zu betrachten, da auf die andere genau dasselbe Verfahren anzuwenden ist.

Da $\mathfrak{A}$, $\mathfrak{B}$ teilerfremd sind, können wir zwei Zahlen $\mathfrak{a}$, $\mathfrak{b}$ so bestimmen, dass $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$ gilt. Dann ist

$$(\mathfrak{a}x + \mathfrak{b}y)(bb - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$$

Hieraus ist sofort klar, dass alle Werte von z, die ganzzahlige Werte von x, y erzeugen können, notwendig zur Zahl $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ modulo $bb - ac$ kongruent sein müssen, also in der Formel $(bb - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ enthalten sind, wobei z' sämtliche ganzen Zahlen durchläuft. Damit erhalten wir leicht anstelle der Formel [1] die folgende:

$$x = \mathfrak{A}z' + \mathfrak{b} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$
$$y = \mathfrak{B}z' - \mathfrak{a} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$

Sie liefert offenbar entweder für alle Werte von z' oder für keinen ganzzahlige Werte von x, y. Der erste Fall tritt immer dann ein, wenn $\mathfrak{A}(bd - ae)$ und $\mathfrak{B}(be - cd)$ modulo

$bb-ac$ kongruent sind, der zweite, wenn sie inkongruent sind. — Formel [2] ist genauso zu behandeln; ihre ganzzahligen Lösungen (falls sie welche liefern kann) sind von den übrigen zu trennen.

219.

Ist $bb-ac=0$, so lässt sich die Form $axx+2bxy+cyy$ als $m(\alpha x+\beta y)^2$ schreiben, wobei m,α,β ganze Zahlen sind (Artikel 215). Setzen wir $\alpha x+\beta y=z$, so geht die vorgelegte Gleichung in diese über:

$$mzz+2dx+2ey+f=0$$

Daraus und aus $z=\alpha x+\beta y$ folgt

$$x=\frac{\beta mzz+2ez+\beta f}{2\alpha e-2\beta d},\quad y=\frac{\alpha mzz+2dz+\alpha f}{2\beta d-2\alpha e}$$

Nun ist klar: Sofern nicht $\alpha e=\beta d$ gilt (diesen Fall betrachten wir gleich gesondert), genügen die Werte von x, y, die aus diesen Formeln durch Einsetzen eines beliebigen Werts für z entstehen, der vorgelegten Gleichung. Es bleibt daher nur zu zeigen, wie sich die Werte von z bestimmen lassen, die ganzzahlige Werte von x, y liefern.

Wegen $\alpha x+\beta y=z$ kommen für z notwendig nur *ganze* Zahlen infrage. Macht außerdem ein Wert von z sowohl x als auch y ganzzahlig, so liefern offenbar auch alle Werte von z, die zu ihm modulo $2\alpha e-2\beta d$ kongruent sind, ganzzahlige Werte. Setzt man also für z alle ganzen Zahlen von 0 bis einschließlich $2\alpha e-2\beta d-1$ (wenn $\alpha e-\beta d$ positiv ist) oder bis einschließlich $2\beta d-2\alpha e-1$ (wenn $\alpha e-\beta d$ negativ ist) ein, und werden für keinen dieser Werte sowohl x als auch y ganzzahlig, so liefert überhaupt kein Wert von z ganzzahlige Werte von x,y, und die vorgelegte Gleichung ist nicht in ganzen Zahlen lösbar. Liefern dagegen einige jener Werte von z ganzzahlige Werte von x,y, etwa ζ,ζ',ζ'' usw. (die sich auch durch Lösen quadratischer Kongruenzen nach den Grundsätzen von Abschnitt IV finden lassen), so erhält man *alle* Lösungen, indem man $z=(2\alpha e-2\beta d)v+\zeta$, $z=(2\alpha e-2\beta d)v+\zeta'$ usw. setzt, wobei v alle ganzen Zahlen durchläuft.

220.

Für den ausgeschlossenen Fall, dass $\alpha e=\beta d$ gilt, müssen wir ein eigenes Verfahren finden. Nehmen wir an, dass α, β teilerfremd sind; nach Artikel 215, I ist das zulässig. Dann ist $\frac{d}{\alpha}=\frac{e}{\beta}$ eine ganze Zahl (Artikel 19), die wir $=h$ setzen. Die vorgelegte Gleichung nimmt dann diese Form an:

$$(m\alpha x+m\beta y+h)^2-hh+mf=0$$

Sie ist also offenbar nur dann rational lösbar, wenn $hh-mf$ eine Quadratzahl ist. Sei $hh-mf=kk$; dann sind die folgenden beiden Gleichungen offenbar der vorgelegten Gleichung äquivalent:

$$m\alpha x+m\beta y+h+k=0,\quad \text{und}\quad m\alpha x+m\beta y+h-k=0$$

d.h., jede Lösung der vorgelegten Gleichung genügt auch einer dieser beiden Gleichungen und umgekehrt. Die erste Gleichung ist offenbar nur dann in ganzen Zahlen

lösbar, wenn $h+k$ durch m teilbar ist; ebenso lässt die zweite nur dann eine ganzzahlige Lösung zu, wenn $h-k$ durch m teilbar ist. Diese Bedingungen reichen aber auch für die Lösbarkeit der jeweiligen Gleichung aus (da α, β als teilerfremd vorausgesetzt sind), und sämtliche Lösungen lassen sich nach den bekannten Regeln angeben.

221.

Den in Artikel 217 betrachteten Fall (da er von allen der schwierigste ist) erläutern wir an einem Beispiel. Gegeben sei die Gleichung $xx + 8xy + yy + 2x - 4y + 1 = 0$. Daraus leiten wir zunächst durch Einführung der anderen Unbekannten $p = 15x - 9$. $q = 15y + 6$ die Gleichung $pp + 8pq + qq = -540$ ab. Man findet, dass sämtliche ganzzahligen Lösungen dieser Gleichung in den folgenden vier Formeln enthalten sind:

$$\begin{aligned} p &= 6t, \quad & q &= -24t - 90u \\ p &= 6t, \quad & q &= -24t + 90u \\ p &= -6t, \quad & q &= 24t - 90u \\ p &= -6t, \quad & q &= 24t + 90u \end{aligned}$$

Dabei durchlaufen t, u alle positiven ganzen Zahlen, die der Gleichung $tt - 15uu = 1$ genügen. Sie sind in der Formel

$$\begin{aligned} t &= \tfrac{1}{2}\big((4+\sqrt{15})^n + (4-\sqrt{15})^n\big) \\ u &= \frac{1}{2\sqrt{15}}\big((4+\sqrt{15})^n - (4-\sqrt{15})^n\big) \end{aligned}$$

enthalten, wenn n alle positiven ganzen Zahlen (einschließlich der Null) durchläuft. Daher sind sämtliche Werte von x, y in den folgenden Formeln enthalten:

$$\begin{aligned} x &= \tfrac{1}{5}(2t+3), \quad & y &= -\tfrac{1}{5}(8t + 30u + 2) \\ x &= \tfrac{1}{5}(2t+3), \quad & y &= -\tfrac{1}{5}(8t - 30u + 2) \\ x &= \tfrac{1}{5}(-2t+3), \quad & y &= \tfrac{1}{5}(8t - 30u - 2) \\ x &= \tfrac{1}{5}(-2t+3), \quad & y &= \tfrac{1}{5}(8t + 30u - 2) \end{aligned}$$

Wendet man unsere Regeln richtig an, so findet man: Damit sich *ganzzahlige* Werte ergeben, muss man in der ersten und zweiten Formel diejenigen Werte von t, u nehmen, die aus einem *geraden* Index n entstehen; in der dritten und vierten dagegen diejenigen, die man aus einem *ungeraden* n erhält. — Die einfachsten Lösungen sind $x = 1, -1, -1$; $y = -2, 0, 12$, jeweils einander entsprechend.

Übrigens lässt sich die Lösung des in den vorhergehenden Artikeln erläuterten Problems meist durch verschiedene Kunstgriffe abkürzen, besonders beim Ausschließen unbrauchbarer Lösungen, *d.h.* solcher, die Brüche enthalten. Doch um nicht zu ausführlich zu werden, haben wir dies hier übergehen müssen.

Historische Bemerkungen.

222.

Da mehrere der bisher behandelten Gegenstände auch von anderen Mathematikern untersucht wurden, können wir deren Verdienste nicht mit Schweigen übergehen. Der angesehene La Grange hat allgemeine Untersuchungen über die *Äquivalenz der Formen* angestellt, *Nouv. Mém. de l'Ac. de Berlin,* 1773 *p.* 263 und 1775 *p.* 323 ff. Insbesondere zeigte er, dass es für jede gegebene Determinante eine endliche Anzahl von Formen gibt, sodass jede Form mit dieser Determinante einer davon äquivalent ist und sich somit alle Formen mit gegebener Determinante in Klassen einteilen lassen. Später entdeckte der berühmte Le Gendre mehrere elegante Eigenschaften dieser Klassifikation, größtenteils durch Induktion aus beobachteten Fällen; wir werden sie unten angeben und mit Beweisen begründen. Die Unterscheidung zwischen eigentlicher und uneigentlicher Äquivalenz, deren Nutzen besonders bei den feineren Untersuchungen sichtbar wird, hatte bisher jedoch niemand getroffen.

Das berühmte, in Artikel 216 ff. erläuterte Problem hat der angesehene La Grange zuerst vollständig gelöst, *Hist. de l'Ac. de Berlin,* 1767 *p.* 165 und 1768 *p.* 181 ff. Eine Lösung (allerdings eine weniger vollständige) steht auch in den schon öfter angeführten *Suppl. ad Euleri Algebram.* Schon vorher hatte der angesehene Euler denselben Gegenstand in Angriff genommen, *Comm. Petr. T.* VI *p.* 175; *Comm. Nov. T.* IX *p.* 3; *Ibid. T.* XVIII *p.* 185 ff. Er beschränkte seine Untersuchung aber stets darauf, aus einer als bekannt vorausgesetzten Lösung andere abzuleiten. Außerdem können seine Methoden nur in wenigen Fällen *alle* Lösungen liefern (siehe La Grange, *Hist. de l'Ac. de Berlin* 1767, *p.* 237). Da die letzte dieser drei Abhandlungen jüngeren Datums ist als La Granges Lösung, die das Problem in seiner ganzen Allgemeinheit erfasst und in dieser Hinsicht nichts zu wünschen übrig lässt, scheint Euler diese Lösung damals noch nicht gekannt zu haben (Band XVIII der Kommentare gehört zum Jahr 1773 und wurde 1774 veröffentlicht). Unsere Lösung beruht dagegen (wie alles andere, was wir bisher in diesem Abschnitt angegeben haben) auf ganz anderen Grundsätzen.

Was andere, etwa Diophant, Fermat usw., zu diesem Gegenstand beigetragen haben, betrifft sehr spezielle Fälle. Da wir das besonders erwähnenswert Erscheinende schon oben genannt haben, verzichten wir darauf, alles einzeln aufzuzählen.

* *
*

Was wir bisher über Formen zweiten Grades dargestellt haben, ist nur als erster Anfang dieser Theorie anzusehen. Als wir diese Untersuchung eingehender verfolgten, eröffnete sich uns ein sehr weites Feld, aus dem wir im Folgenden das besonders beachtenswert Erscheinende auswählen werden. Denn dieser Gegenstand ist so fruchtbar, dass wir der Kürze wegen vieles andere übergehen müssen, das uns bereits zu finden gelungen ist; weit mehr liegt ohne Zweifel noch verborgen und wartet auf neue Anstrengungen. Gleich zu Beginn dieser Untersuchungen ist zu bemerken, dass Formen mit der Determinante 0 ausgeschlossen sind, sofern wir nichts anderes angeben.

WEITERE UNTERSUCHUNGEN ÜBER FORMEN.

Einteilung der Formen mit gegebener Determinante in Klassen.

223.

Schon oben (Artikel 175, 195, 211) haben wir gezeigt: Für jede gegebene ganze Zahl D (positiv oder negativ) lässt sich eine endliche Anzahl von Formen F, F', F'' usw. mit der Determinante D angeben, sodass jede Form mit der Determinante D einer und nur einer davon eigentlich äquivalent ist. Alle Formen mit der Determinante D (deren Anzahl unendlich ist) lassen sich daher nach diesen Formen *klassifizieren*: Die Gesamtheit aller Formen, die F eigentlich äquivalent sind, bildet die erste Klasse; die Formen, die F' eigentlich äquivalent sind, bilden die zweite usw.

Aus jeder Klasse von Formen mit gegebener Determinante D können wir eine Form wählen und als *repräsentierende Form* der ganzen Klasse betrachten. An sich ist völlig beliebig, welche Form wir aus jeder Klasse nehmen. Dennoch sollten wir immer diejenige vorziehen, die die anderen an *Einfachheit* zu übertreffen scheint. Die Einfachheit einer Form (a, b, c) ist offenbar nach der Größe der Zahlen a, b, c zu beurteilen. Mit Recht nennen wir eine Form (a', b', c') weniger einfach als (a, b, c), wenn $a' > a$, $b' > b$, $c' > c$ gelten. Damit ist die Sache aber noch nicht vollständig bestimmt: Es bleibt *zum Beispiel* uns überlassen, welche der Formen $(17, 0, -45)$, $(5, 0, -153)$ wir für einfacher halten wollen. Meist wird es jedoch zweckmäßig sein, diese Regel einzuhalten:

I. Ist die Determinante D negativ, so nehme man die in den einzelnen Klassen enthaltenen reduzierten Formen als repräsentierende Formen. Finden sich in derselben Klasse zwei reduzierte Formen (die dann entgegengesetzt sind, Artikel 172), so nehme man diejenige, deren mittleres Glied positiv ist.

II. Ist die Determinante D positiv und keine Quadratzahl, so entwickle man die Periode einer reduzierten Form der vorgelegten Klasse. Darin werden entweder zwei ambige Formen vorkommen oder keine (Artikel 187).

1) Im ersten Fall seien die ambigen Formen (A, B, C), (A', B', C'); die kleinsten Reste der Zahlen B, B' nach den Moduln A, A' seien jeweils M, M' (sie können positiv genommen werden, sofern sie nicht $= 0$ sind); schließlich sei $\frac{D-MM}{A} = N$, $\frac{D-M'M'}{A'} = N'$. Dann nehme man von den Formen $(A, M, -N)$, $(A', M', -N')$ diejenige als repräsentierende Form, die am einfachsten erscheint. Dabei ist eine Form vorzuziehen, deren mittleres Glied $= 0$ ist. Ist das mittlere Glied in beiden oder in keiner 0, so ziehe man die Form mit dem kleineren ersten Glied vor. Sind die ersten Glieder der Größe nach gleich, aber im Vorzeichen verschieden, so ist das positive Vorzeichen dem negativen vorzuziehen.

2) Gibt es in der ganzen Periode keine ambige Form, so wähle man aus allen Formen der Periode diejenige mit dem kleinsten ersten Glied, ohne Rücksicht auf das Vorzeichen. Kommen in derselben Periode zwei Formen vor, in denen dasselbe erste Glied einmal positiv und einmal negativ ist, so ist die erste der zweiten vorzuziehen. Diese Form sei (A, B, C). Daraus leite man wie im vorigen Fall eine andere Form $(A, M, -N)$ ab (indem man für M den absolut kleinsten Rest von B modulo A nimmt und $N = \frac{D-MM}{A}$ setzt). Diese nehme man schließlich als Repräsentanten.

Sollte dasselbe kleinste erste Glied A mehreren Formen der Periode gemeinsam sein, so behandle man alle diese Formen auf die vorgeschriebene Weise und nehme von den entstehenden Formen diejenige als repräsentierende Form, deren mittleres Glied möglichst klein wird.

So haben wir *zum Beispiel* für $D = 305$ unter anderem diese Periode: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$. Daraus wählen wir zunächst die Form $(7, 16, -7)$ und leiten daraus dann die repräsentierende Form $(7, 2, -43)$ ab.

III. Ist die Determinante eine positive Quadratzahl $= kk$, so ermittle man die in der vorgelegten Klasse enthaltene reduzierte Form $(A, k, 0)$. Ist $A < k$ oder $= k$, so nehme man diese selbst als repräsentierende Form. Ist dagegen $A > k$, so nehme man an ihrer Stelle die Form $(A - 2k, k, 0)$, deren erstes Glied negativ, aber kleiner als k ist.

Beispiel. So werden alle Formen mit der Determinante -235 in sechzehn Klassen eingeteilt. Ihre Repräsentanten sind $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$ und acht weitere, die sich von den vorigen nur durch die Vorzeichen der äußeren Glieder unterscheiden: $(-1, 0, -235)$, $(-2, 1, -118)$ usw.

Alle Formen mit der Determinante 79 zerfallen in sechs Klassen, deren Repräsentanten $(1, 0, -79)$, $(3. 1, -26)$, $(3, -1, -26)$, $(-1, 0. 79)$, $(-3, 1, 26)$, $-3. -1, 26)$ sind.

224.

Durch diese Klassifikation werden also die eigentlich äquivalenten Formen vollständig von den übrigen getrennt. Zwei Formen derselben Determinante D sind eigentlich äquivalent, wenn sie zur selben Klasse gehören. Jede durch die eine darstellbare Zahl lässt sich auch durch die andere darstellen. Lässt sich eine Zahl M durch die erste Form mit teilerfremden Werten der Unbestimmten darstellen, so ist dieselbe Zahl durch die andere Form ebenso darstellbar, und zwar so, dass beide Darstellungen zum selben Wert des Ausdrucks $\sqrt{D}$ (mod. M) gehören. Gehören zwei Formen dagegen zu verschiedenen Klassen, so sind sie nicht eigentlich äquivalent. Von der Darstellbarkeit einer gegebenen Zahl durch die eine kann man nicht auf ihre Darstellbarkeit durch die andere schließen. Lässt sich vielmehr die Zahl M durch die eine mit teilerfremden Werten der Unbestimmten darstellen, so sind wir sofort sicher, dass es keine ähnliche Darstellung derselben Zahl durch die andere Form gibt, die zum selben Wert des Ausdrucks $\sqrt{D}$(mod. M) gehört (siehe Artikel 167, 168).

Andererseits können zwei Formen F, F' aus verschiedenen Klassen K, K' durchaus uneigentlich äquivalent sein. Dann ist *jede* Form der einen Klasse *jeder* Form der anderen uneigentlich äquivalent. Jede Form aus K hat ihre entgegengesetzte Form in K', und die Klassen K, K' selbst heißen *entgegengesetzt*. So ist im ersten Beispiel des vorigen Artikels die dritte Klasse der Formen mit der Determinante -235 der vierten entgegengesetzt und die siebte der achten; im zweiten Beispiel die zweite Klasse der dritten und die fünfte der sechsten. Für beliebige zwei Formen aus entgegengesetzten Klassen gilt also: Jede Zahl M, die durch die eine darstellbar ist, lässt sich auch durch die andere darstellen. Geschieht dies bei der einen mit teilerfremden Werten der Unbestimmten, so ist es bei der anderen ebenso möglich, allerdings so, dass diese beiden

Darstellungen zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}$ (mod. M) gehören. — Die oben angegebenen Regeln zur Wahl der repräsentierenden Formen sind so eingerichtet, dass entgegengesetzte Klassen stets entgegengesetzte repräsentierende Formen erhalten.

Schließlich gibt es auch Klassen, die *sich selbst entgegengesetzt* sind. Gehören nämlich eine Form und ihre entgegengesetzte zur selben Klasse, so sieht man leicht, dass alle Formen dieser Klasse einander sowohl eigentlich als auch uneigentlich äquivalent sind und ihre entgegengesetzten Formen in derselben Klasse haben. Jede Klasse, die eine ambige Form enthält, hat diese Eigenschaft. Umgekehrt enthält jede sich selbst entgegengesetzte Klasse notwendig eine ambige Form (Artikel 163, 165); deshalb heißt sie eine *ambige Klasse*. So gibt es unter den Klassen der Formen mit der Determinante -235 acht ambige, deren Repräsentanten $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$ sind; unter den Klassen der Formen mit der Determinante 79 zwei, mit den Repräsentanten $(1, 0, -79)$, $(-1, 0, 79)$. — Sind die repräsentierenden Formen nach unseren Regeln bestimmt, so lassen sich die ambigen Klassen leicht daran erkennen. Bei einer positiven Nichtquadratzahl als Determinante erhält eine ambige Klasse sicher eine ambige repräsentierende Form (Artikel 194). Bei einer negativen Determinante ist die repräsentierende Form einer ambigen Klasse entweder selbst ambig oder hat gleiche äußere Glieder (Artikel 172). Bei einer positiven Quadratzahl als Determinante lässt sich schließlich nach Artikel 210 leicht entscheiden, ob die repräsentierende Form sich selbst uneigentlich äquivalent und somit die von ihr repräsentierte Klasse ambig ist.

225.

Schon oben (Artikel 175) haben wir gezeigt, dass in einer Form (a, b, c) mit negativer Determinante die äußeren Glieder dasselbe Vorzeichen haben, sowohl untereinander als auch wie die äußeren Glieder jeder äquivalenten Form. Sind a, c positiv, so nennen wir die Form (a, b, c) *positiv*. Ebenso heißt die ganze Klasse, die (a, b, c) enthält und nur aus positiven Formen besteht, eine *positive Klasse*. Dagegen ist (a, b, c) eine *negative Form*, die in einer *negativen Klasse* liegt, wenn a, c negativ sind. Durch eine positive Form lassen sich keine negativen, durch eine negative Form keine positiven Zahlen darstellen. Ist die Form (a, b, c) Repräsentant einer positiven Klasse, so ist die Form $(-a, b, -c)$ Repräsentant einer negativen Klasse. Daher gibt es gleich viele positive und negative Klassen; sobald die ersten angegeben sind, sind auch die zweiten bekannt. Bei Untersuchungen über Formen mit negativer Determinante genügt es deshalb meist, die positiven Klassen zu betrachten, deren Eigenschaften sich leicht auf die negativen Klassen übertragen.

Diese Unterscheidung gilt allerdings nur für Formen mit negativer Determinante. Durch Formen mit positiver Determinante lassen sich ohne Unterschied positive und negative Zahlen darstellen; nicht selten gehören sogar zwei Formen wie (a, b, c), $(-a, b, -c)$ in diesem Fall zur selben Klasse.

Einteilung der Klassen in Ordnungen.

226.

Wir nennen eine Form (a, b, c) *primitiv*, wenn die Zahlen a, b, c keinen gemeinsamen nichttrivialen Teiler haben; andernfalls heißt sie *abgeleitet*. Genauer: Setzen wir den größten gemeinsamen Teiler der Zahlen $a, b, c = m$, so ist die Form (a, b, c) *aus der primitiven Form* $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$ *abgeleitet*. Aus dieser Definition ist sofort klar, dass alle Formen, deren Determinante durch keine Quadratzahl (außer 1) teilbar ist, notwendig primitiv sind. Ferner folgt aus Artikel 161: Enthält eine gegebene Klasse von Formen mit der Determinante D eine primitive Form, so sind alle Formen dieser Klasse primitiv; in diesem Fall heißt die Klasse selbst *primitiv*. Ist außerdem eine Form F mit der Determinante D aus einer primitiven Form f mit der Determinante $\frac{D}{mm}$ abgeleitet, und sind F, f jeweils in den Klassen K, k enthalten, so sind offenbar alle Formen der Klasse K aus der primitiven Klasse k abgeleitet. Daher nennen wir in diesem Fall die Klasse K selbst *aus der primitiven Klasse k abgeleitet*.

Ist (a, b, c) eine primitive Form, sind aber a, c nicht beide gerade (*d.h.*, wenn entweder beide ungerade sind oder wenigstens eine davon ungerade ist), so sieht man leicht, dass nicht nur a, b, c, sondern auch a, $2b$, c keinen gemeinsamen nichttrivialen Teiler haben. Dann heißt die Form (a, b, c) *eigentlich primitiv* oder einfach eine *eigentliche Form*. Ist dagegen (a, b, c) eine primitive Form und sind die Zahlen a, c beide gerade, so haben die Zahlen a, $2b$, c offenbar den gemeinsamen Teiler 2 (der zugleich der größte ist). Dann heißt (a, b, c) eine *uneigentlich primitive Form* oder einfach eine *uneigentliche Form*[*)]. In diesem Fall muss b ungerade sein (sonst wäre (a, b, c) keine primitive Form). Daher gilt $bb \equiv 1 \pmod 4$, und da ac durch 4 teilbar ist, gilt für die Determinante $bb - ac \equiv 1 \pmod 4$. Uneigentliche Formen gibt es also nur für eine Determinante der Form $4n + 1$, wenn sie positiv ist, oder der Form $-(4n + 3)$, wenn sie negativ ist. — Aus Artikel 161 ist außerdem klar: Enthält eine gegebene Klasse eine eigentlich primitive Form, so sind alle Formen dieser Klasse eigentlich primitiv. Dagegen besteht eine Klasse, die eine uneigentlich primitive Form enthält, ausschließlich aus uneigentlich primitiven Formen. Daher heißt die Klasse selbst im ersten Fall *eigentlich primitiv* oder einfach *eigentlich*, im zweiten *uneigentlich primitiv* oder *uneigentlich*. So sind *zum Beispiel* unter den positiven Klassen von Formen mit der Determinante -235 sechs eigentlich, nämlich die mit den Repräsentanten $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$, und ebenso viele unter den negativen Klassen; jeweils zwei sind dagegen uneigentlich. — Die Klassen von Formen mit der Determinante 79 (einer Zahl der Form $4n + 3$) sind sämtlich eigentlich.

Ist eine Form (a, b, c) abgeleitet, und zwar aus der primitiven Form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, so kann diese eigentlich oder uneigentlich primitiv sein. Im ersten Fall ist m auch der größte gemeinsame Teiler der Zahlen a, $2b$, c; im zweiten ist deren größter gemeinsamer Teiler $2m$. Damit wird die Unterscheidung zwischen einer *aus einer eigentlich*

[*)] Wir haben die Ausdrücke *eigentlich* und *uneigentlich* hier gewählt, weil uns keine passenderen einfielen. Wir weisen darauf hin, damit niemand zwischen dieser Bedeutung und der seit Artikel 157 verwendeten einen verborgenen Zusammenhang sucht: Es gibt keinen. Eine Mehrdeutigkeit ist hier jedenfalls nicht zu befürchten.

primitiven Form abgeleiteten Form und einer *aus einer uneigentlich primitiven Form abgeleiteten Form* verständlich; ebenso (da sich nach Artikel 161 alle Formen derselben Klasse in dieser Hinsicht gleich verhalten) die Unterscheidung zwischen einer *aus einer eigentlich primitiven Klasse abgeleiteten Klasse* und einer *aus einer uneigentlich primitiven Klasse abgeleiteten Klasse*.

Mit diesen Unterscheidungen haben wir eine erste Grundlage, auf der wir die Einteilung aller Klassen von Formen mit gegebener Determinante in verschiedene *Ordnungen* aufbauen können. Zwei Klassen mit den repräsentierenden Formen (a, b, c), (a', b', c') rechnen wir zur *selben Ordnung*, wenn *sowohl* die Zahlen a, b, c denselben größten gemeinsamen Teiler haben wie a', b', c' *als auch* a, $2b$, c denselben wie a', $2b'$, c'. Ist eine oder sind beide dieser Bedingungen nicht erfüllt, so gehören die Klassen zu *verschiedenen Ordnungen*. Daraus ist sofort klar, dass alle eigentlich primitiven Klassen eine Ordnung bilden und alle uneigentlich primitiven eine andere. Ist mm eine Quadratzahl, die die Determinante D teilt, so bilden die aus eigentlich primitiven Klassen mit der Determinante $\frac{D}{mm}$ abgeleiteten Klassen eine eigene Ordnung, die aus uneigentlich primitiven Klassen mit der Determinante $\frac{D}{mm}$ abgeleiteten eine andere usw. Ist D durch keine Quadratzahl (außer 1) teilbar, so gibt es keine Ordnungen abgeleiteter Klassen. Es gibt dann entweder nur eine Ordnung (wenn $D \equiv 2$ oder 3 modulo 4), nämlich die Ordnung der eigentlich primitiven Klassen, oder zwei (wenn $D \equiv 1 \pmod 4$), nämlich die Ordnung der eigentlich primitiven und die der uneigentlich primitiven Klassen. Nach den Grundsätzen der Kombinatorik lässt sich leicht folgende allgemeine Regel aufstellen: Es sei $D = D' 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \ldots$, wobei D' keinen quadratischen Faktor enthält und a, b, c usw. verschiedene ungerade Primzahlen sind (auf diese Form lässt sich jede Zahl bringen, indem man $\mu = 0$ setzt, wenn D nicht durch 4 teilbar ist, und α, β, γ usw. sämtlich $= 0$ setzt oder, was dasselbe ergibt, die Faktoren $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$ usw. weglässt, wenn D durch keine ungerade Quadratzahl teilbar ist). Dann gibt es entweder

$$(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$$

Ordnungen, nämlich wenn $D' \equiv 2$ oder $3 \pmod 4$, oder

$$(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$$

Ordnungen, wenn $D' \equiv 1 \pmod 4$. Den Beweis dieser Regel lassen wir jedoch weg, da er weder schwierig noch hier besonders notwendig ist.

Beispiel 1. Für $D = 45 = 5.3^2$ gibt es sechs Klassen mit den Repräsentanten $(1, 0, -45)$, $(-1.0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3.0, -15)$, $(6, 3, -6)$. Sie werden in vier Ordnungen eingeteilt: Ordnung I umfasst die beiden eigentlichen Klassen mit den Repräsentanten $(1, 0, -45)$, $(-1, 0, 45)$; Ordnung II enthält die beiden uneigentlichen Klassen mit den Repräsentanten $(2, 1, -22)$, $(-2, 1, 22)$; Ordnung III enthält eine aus einer eigentlichen Klasse der Determinante 5 abgeleitete Klasse, nämlich die mit dem Repräsentanten $(3, 0, -15)$; Ordnung IV besteht aus einer aus einer uneigentlichen Klasse der Determinante 5 abgeleiteten Klasse, nämlich der mit dem Repräsentanten $(6, 3, -6)$.

Beispiel 2. Die positiven Klassen mit der Determinante $-99 = -11.3^2$ werden in vier Ordnungen eingeteilt. Ordnung I umfasst die folgenden eigentlich primitiven

Klassen[*]: $(1,0,99)$, $(4,1,25)$. $(4,-1,25)$, $(5,1,20)$, $(5,-1,20)$, $(9,0,11)$; Ordnung II enthält die uneigentlichen Klassen $(2,1,50)$, $(10,1,10)$; Ordnung III die aus eigentlichen Klassen der Determinante -11 abgeleiteten Klassen $(3,0,33)$, $(9,3,12)$, $(9,-3,12)$; Ordnung IV die einzige aus einer uneigentlichen Klasse der Determinante -11 abgeleitete Klasse $(6,3,18)$. — Die negativen Klassen dieser Determinante lassen sich genauso in Ordnungen einteilen.

Wir bemerken, dass *entgegengesetzte Klassen stets zur selben Ordnung gehören*; der Grund für diesen Satz ist leicht zu erkennen.

227.

Von diesen verschiedenen Ordnungen verdient besonders die Ordnung der eigentlich primitiven Klassen die größte Aufmerksamkeit. Denn jede abgeleitete Klasse stammt aus einer bestimmten primitiven Klasse (mit kleinerer Determinante); aus deren Betrachtung ergibt sich das auf die erste Klasse Bezügliche meist von selbst. Unten werden wir zeigen, dass jede uneigentlich primitive Klasse ähnlich gewissermaßen entweder einer einzigen eigentlich primitiven Klasse oder dreien (mit derselben Determinante) zugeordnet ist. Bei negativen Determinanten können wir außerdem die negativen Klassen übergehen, da jeder von ihnen stets eine bestimmte positive Klasse entspricht. Um das Wesen der eigentlich primitiven Klassen tiefer zu verstehen, erläutern wir zunächst einen bestimmten wesentlichen Unterschied, nach dem sich die ganze Ordnung der eigentlichen Klassen in mehrere *Geschlechter* einteilen lässt. Da wir diesen sehr wichtigen Gegenstand bisher noch nicht berührt haben, müssen wir ihn von Anfang an aufnehmen.

Einteilung der Ordnungen in Geschlechter.

228.

Satz. *Durch jede eigentlich primitive Form F lassen sich unendlich viele Zahlen darstellen, die durch eine beliebige gegebene Primzahl p nicht teilbar sind.*

Beweis. Ist die Form $F = axx + 2bxy + cyy$, so kann p offenbar nicht alle drei Zahlen a, $2b$, c zugleich teilen. Ist nun a nicht durch p teilbar, so ist klar: Nimmt man für x eine beliebige nicht durch p teilbare Zahl und für y eine durch p teilbare Zahl, so ist der Wert der Form F nicht durch p teilbar. Ist c nicht durch p teilbar, so erreicht man dasselbe, indem man x einen teilbaren und y einen nicht teilbaren Wert gibt. Sind schließlich sowohl a als auch c durch p teilbar, also $2b$ nicht teilbar, so nimmt die Form F einen nicht durch p teilbaren Wert an, wenn man sowohl x als auch y beliebige nicht durch p teilbare Werte gibt. *Q.E.D.*

Der Satz gilt offenbar auch für *uneigentlich primitive* Formen, sofern nur nicht $p = 2$ gilt.

Da mehrere solche Bedingungen gleichzeitig erfüllt sein können, dass dieselbe Zahl durch gewisse gegebene Primzahlen teilbar, durch andere nicht teilbar ist (siehe Artikel 32), sieht man leicht: Die Zahlen x, y lassen sich auf unendlich viele Arten so bestimmen, dass die primitive Form $axx+2bxy+cyy$ einen Wert erhält, der durch beliebig viele gegebene Primzahlen nicht teilbar ist. Von diesen ist nur 2 auszuschließen,

[*]Der Kürze wegen verwenden wir die repräsentierenden Formen anstelle der Klassen, die sie vertreten.

wenn die Form uneigentlich primitiv ist. Daraus folgt diese allgemeinere Fassung des Satzes: *Durch jede primitive Form lassen sich unendlich viele Zahlen darstellen, die zu einer beliebigen gegebenen Zahl teilerfremd sind (die gegebene Zahl muss ungerade sein, wenn die Form uneigentlich primitiv ist).*

229.

Satz. *Sei F eine primitive Form der Determinante D und p eine Primzahl, die D teilt. Dann stimmen die nicht durch p teilbaren Zahlen, die durch die Form F darstellbar sind, darin überein, dass sie entweder alle quadratische Reste von p oder alle Nichtreste sind.*

Beweis. Sei $F = (a, b, c)$; seien m, m' zwei beliebige nicht durch p teilbare Zahlen, die durch die Form F darstellbar sind, nämlich

$$m = agg + 2bgh + chh, \qquad m' = ag'g' + 2bg'h' + ch'h'$$

Dann ist

$$mm' = (agg' + b(gh' + hg') + chh')^2 - D(gh' - hg')^2$$

Also ist mm' einem Quadrat modulo D und damit auch modulo p kongruent, *d.h.*, mm' ist quadratischer Rest von p. Daraus folgt, dass entweder beide Zahlen m, m' quadratische Reste von p oder beide Nichtreste sind. *Q.E.D.*

Ebenso beweist man: Ist die Determinante D durch 4 teilbar, so sind alle durch F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$. oder sämtlich $\equiv 3$ (mod. 4). Denn das Produkt zweier solcher Zahlen ist in diesem Fall stets quadratischer Rest von 4 und daher $\equiv 1$ (mod. 4); somit sind entweder beide $\equiv 1$ oder beide $\equiv 3$.

Ist schließlich D durch 8 teilbar, so ist das Produkt zweier beliebiger ungerader Zahlen, die durch F darstellbar sind, quadratischer Rest von 8 und folglich $\equiv 1$ (mod. 8). Daher sind in diesem Fall alle durch F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$ oder sämtlich $\equiv 3$ oder sämtlich $\equiv 5$ oder sämtlich $\equiv 7$ (mod. 8).

So sind *zum Beispiel*, da die Form $(10, 3, 17)$ die Zahl 10 darstellt, die ein Nichtrest von 7 ist, alle nicht durch 7 teilbaren Zahlen, die jene Form darstellt, Nichtreste von 7. — Da -3 durch die Form $(-3, 1, 49)$ darstellbar und modulo $4 \equiv 1$ ist, verhalten sich alle durch diese Form darstellbaren ungeraden Zahlen ebenso.

Wäre es für unseren gegenwärtigen Zweck nötig, so könnten wir leicht beweisen, dass die durch die Form F darstellbaren Zahlen zu keiner Primzahl, die D nicht teilt, eine solche feste Beziehung haben. Vielmehr lassen sich sowohl Reste als auch Nichtreste jeder Primzahl, die D nicht teilt, durch die Form F darstellen. Bei den Zahlen 4 und 8 gilt dagegen auch in anderen Fällen etwas Ähnliches, das wir nicht übergehen können.

I. *Ist die Determinante D der primitiven Form $F \equiv 3$ (mod. 4), so sind alle durch die Form F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$ oder sämtlich $\equiv 3$ (mod. 4).* Sind nämlich m, m' zwei durch F darstellbare Zahlen, so lässt sich ihr Produkt mm' wie oben auf die Form $pp - Dqq$ bringen. Sind beide Zahlen m, m' ungerade, so muss von den Zahlen p, q eine gerade und die andere ungerade sein; daher ist von den Quadraten pp, qq eines $\equiv 0$ und das andere $\equiv 1$ (mod. 4). Daraus folgt leicht, dass $pp - Dqq$ sicher $\equiv 1$ (mod. 4) ist, also entweder beide Zahlen m,

$m' \equiv 1$ sind oder beide $\equiv 3$ (mod. 4). So lassen sich *zum Beispiel* durch die Form $(10, 3, 17)$ keine anderen ungeraden Zahlen als solche der Form $4n + 1$ darstellen.

II. *Ist die Determinante D der primitiven Form $F \equiv 2$ (mod. 8), so sind alle durch die Form F darstellbaren ungeraden Zahlen entweder teils $\equiv 1$, teils $\equiv 7$, oder teils $\equiv 3$, teils $\equiv 5$ (mod. 8).* Seien nämlich m, m' zwei ungerade Zahlen, die durch F darstellbar sind; ihr Produkt mm' lässt sich also auf die Form $pp - Dqq$ bringen. Sind daher beide Zahlen m, m' ungerade, so muss p ungerade sein (weil D gerade ist), also gilt $pp \equiv 1$ (mod. 8). Dagegen ist qq entweder $\equiv 0$ oder $\equiv 1$ oder $\equiv 4$, und daher Dqq entweder $\equiv 0$ oder $\equiv 2$. Somit ist $mm' = pp - Dqq$ entweder $\equiv 1$ oder $\equiv 7$ (mod. 8). Ist also m entweder $\equiv 1$ oder $\equiv 7$, so ist auch m' entweder $\equiv 1$ oder $\equiv 7$; ist dagegen m entweder $\equiv 3$ oder $\equiv 5$, so ist auch m' entweder $\equiv 3$ oder $\equiv 5$. *Zum Beispiel* sind alle durch die Form $(3, 1, 5)$ darstellbaren ungeraden Zahlen entweder $\equiv 3$ oder $\equiv 5$ (mod. 8), und keine Zahlen der Form $8n + 1$ oder $8n + 7$ sind durch jene Form darstellbar.

III. *Ist die Determinante D der primitiven Form $F \equiv 6$ (mod. 8), so sind durch diese Form entweder nur ungerade Zahlen der beiden Arten $\equiv 1$ und $\equiv 3$ (mod. 8) oder nur solche der beiden Arten $\equiv 5$ und $\equiv 7$ (mod. 8) darstellbar.* Einen Beweis, der dem vorigen (in II) ganz ähnlich ist, kann jeder ohne Mühe ausführen. — So sind *zum Beispiel* durch die Form $(5, 1, 7)$ nur solche ungeraden Zahlen darstellbar, die entweder $\equiv 5$ oder $\equiv 7$ (mod. 8) sind.

230.

Alle Zahlen, die durch eine gegebene primitive Form F der Determinante D darstellbar sind, haben also eine feste Beziehung zu jedem Primteiler von D (durch den sie selbst nicht teilbar sind). Die durch F darstellbaren ungeraden Zahlen haben in gewissen Fällen auch zu den Zahlen 4 und 8 eine feste Beziehung: nämlich zu 4, wenn D entweder $\equiv 0$ oder $\equiv 3$ (mod. 4) ist, und zu 8, wenn D entweder $\equiv 0$ oder $\equiv 2$ oder $\equiv 6$ (mod. 8) ist[*)]. Eine solche Beziehung zu jeder dieser Zahlen nennen wir einen *Charakter* oder *Einzelcharakter* der Form F und drücken sie so aus: Können nur quadratische Reste der Primzahl p durch die Form F dargestellt werden, so geben wir ihr den Charakter Rp, im entgegengesetzten Fall den Charakter Np. Ebenso schreiben wir $1, 4$, wenn die Form F keine anderen ungeraden Zahlen darstellen kann als solche, die $\equiv 1$ (mod. 4) sind. Daraus ist sofort klar, welche Charaktere die Zeichen $3, 4$; $1, 8$; $3, 8$; $5, 8$; $7, 8$ ausdrücken. Schließlich geben wir den Formen, die nur solche ungeraden Zahlen darstellen können, die modulo 8 entweder $\equiv 1$ oder $\equiv 7$ sind, den Charakter 1 *und* $7, 8$. Daraus ergibt sich von selbst die Bedeutung der Charaktere 3 *und* $5, 8$; 1 *und* $3, 8$; 5 *und* $7, 8$.

Die einzelnen Charaktere einer gegebenen primitiven Form (a, b, c) mit der Determinante D lassen sich stets aus wenigstens einer der Zahlen a, c erkennen (die offenbar beide durch jene Form darstellbar sind). Denn ist p ein Primteiler von D, so ist sicher wenigstens eine der Zahlen a, c nicht durch p teilbar. Wären beide durch p teilbar, so würde p auch $bb (= D + ac)$ teilen. und damit auch b; *d.h.*, die Form (a, b, c) wäre nicht primitiv. Ebenso ist in den Fällen, in denen die Form (a, b, c) zur

[*)] Für durch 8 teilbare Determinanten kann die Beziehung zur Zahl 4 weggelassen werden, da sie in diesem Fall schon in der Beziehung zu 8 enthalten ist.

Zahl 4 oder 8 eine feste Beziehung hat, sicher mindestens eine der Zahlen a, c ungerade. Daraus lässt sich also jene Beziehung erkennen. So ergibt sich *zum Beispiel* für die Form $(7, 0, 23)$ der Charakter bezüglich der Zahl 23 aus der Zahl 7 als $N23$; der Charakter derselben Form bezüglich 7 ergibt sich aus der Zahl 23, nämlich $R7$; schließlich lässt sich der Charakter dieser Form bezüglich 4, nämlich $3, 4$, sowohl aus 7 als auch aus 23 erkennen.

Da alle Zahlen, die durch eine Form F der Klasse K darstellbar sind, auch durch jede andere Form dieser Klasse dargestellt werden können, kommen die einzelnen Charaktere der Form F offenbar auch allen übrigen Formen dieser Klasse zu. Wir können sie daher als Charaktere der ganzen Klasse betrachten. Die einzelnen Charaktere einer beliebigen gegebenen primitiven Klasse lassen sich also aus ihrer repräsentierenden Form erkennen. Entgegengesetzte Klassen haben stets sämtliche Charaktere gemeinsam.

231.

Die Gesamtheit *aller* Einzelcharaktere einer gegebenen Form oder Klasse bildet den Gesamtcharakter dieser Form oder Klasse. So ist *zum Beispiel* der Gesamtcharakter der Form $(10, 3, 17)$ oder der ganzen von ihr repräsentierten Klasse $1, 4;\ N7;\ N23$. Ebenso ist der Gesamtcharakter der Form $(7, 1, -17)$ $7, 8;\ R3;\ N5$, denn der Einzelcharakter $3, 4$ wird hier weggelassen, weil er bereits im Charakter $7, 8$ enthalten ist. — Darauf gründen wir die Einteilung der ganzen Ordnung der eigentlich primitiven Klassen (der positiven, wenn die Determinante negativ ist) mit gegebener Determinante in mehrere verschiedene *Geschlechter*: Alle Klassen mit demselben Gesamtcharakter gehören zum selben Geschlecht, Klassen mit verschiedenen Gesamtcharakteren dagegen zu verschiedenen Geschlechtern. Jedem Geschlecht geben wir den Gesamtcharakter der darin enthaltenen Klassen. So gibt es *zum Beispiel* für die Determinante -161 sechzehn positive eigentlich primitive Klassen. Sie verteilen sich auf folgende vier Geschlechter:

Charakter	Repräsentierende Formen der Klassen
$1, 4;\ R7;\ R23$	$(1, 0, 161)$, $(2, 1, 81)$, $(9, 1, 18)$, $(9, -1, 18)$
$1, 4;\ N7;\ N23$	$(5, 2, 33)$, $(5, -2, 33)$, $(10, 3, 17)$, $(10, -3, 17)$
$3, 4;\ R7;\ N23$	$(7, 0, 23)$, $(11, 2, 15)$, $(11, -2, 15)$, $(14, 7, 15)$
$3, 4;\ N7;\ R23$	$(3, 1, 54)$, $(3, -1, 54)$, $(6, 1, 27)$, $(6, -1, 27)$

Für die Anzahl der verschiedenen Gesamtcharaktere, die von vornherein möglich sind, gilt Folgendes.

I. Ist die Determinante D durch 8 teilbar, so sind bezüglich 8 vier verschiedene Einzelcharaktere möglich; die Zahl 4 liefert keinen eigenen Charakter (Anmerkung zum vorigen Artikel). Außerdem gibt es bezüglich jedes ungeraden Primteilers von D zwei Charaktere. Ist deren Anzahl m, so gibt es insgesamt 2^{m+2} verschiedene Gesamtcharaktere (wobei wir $m = 0$ setzen, wenn D eine Zweierpotenz ist).

II. Ist die Determinante D nicht durch 8 teilbar, wohl aber durch 4 und außerdem durch m ungerade Primzahlen, so gibt es insgesamt 2^{m+1} verschiedene Gesamtcharaktere.

III. Ist die Determinante D gerade, aber nicht durch 4 teilbar, so ist sie entweder $\equiv 2 \pmod 8$ oder $\equiv 6$. Im ersten Fall gibt es bezüglich 8 zwei Einzelcharaktere, nämlich 1 *und* $7, 8$ und 3 *und* $5, 8$; im zweiten ebenso viele. Setzen wir also die Anzahl der ungeraden Primteiler von $D = m$, so gibt es insgesamt 2^{m+1} verschiedene Gesamtcharaktere.

IV. Ist D ungerade, so ist sie entweder $\equiv 1$ oder $\equiv 3 \pmod 4$. Im zweiten Fall gibt es bezüglich 4 zwei verschiedene Charaktere; im ersten geht eine solche Beziehung nicht in den Gesamtcharakter ein. Bezeichnet m also dasselbe wie zuvor, so gibt es im ersten Fall 2^m, im zweiten 2^{m+1} verschiedene Gesamtcharaktere.

Es ist aber gut zu beachten, dass daraus keineswegs folgt, dass tatsächlich ebenso viele Geschlechter existieren, wie verschiedene Charaktere von vornherein möglich sind. In unserem Beispiel entsprechen nur der Hälfte von ihnen tatsächlich Klassen oder Geschlechter. Es gibt keine positiven Klassen mit den Charakteren $1, 4;\ R7;\ N23$ oder $1, 4;\ N7;\ R23$; oder $3, 4;\ R7;\ R23$ oder $3, 4;\ N7;\ N23$. Auf diesen sehr wichtigen Gegenstand gehen wir unten ausführlicher ein.

Die Form $(1, 0, -D)$, die zweifellos unter allen Formen mit der Determinante D als die einfachste anzusehen ist, nennen wir von nun an *Hauptform*. Die ganze Klasse, die sie enthält, heißt *Hauptklasse*, und das ganze Geschlecht, das die Hauptklasse enthält, *Hauptgeschlecht*. Wir müssen daher die Hauptform, eine Form aus der Hauptklasse und eine Form aus dem Hauptgeschlecht sorgfältig unterscheiden; ebenso die Hauptklasse und eine Klasse aus dem Hauptgeschlecht. Diese Bezeichnungen verwenden wir stets, auch wenn es für eine Determinante keine anderen Klassen als die Hauptklasse oder keine anderen Geschlechter als das Hauptgeschlecht gibt. Das geschieht *zum Beispiel* häufig, wenn D eine positive Primzahl der Form $4n + 1$ ist.

232.

Zwar haben wir die Charaktere der Formen zunächst erläutert, um darauf die Unterteilung der *positiven eigentlich primitiven* Ordnung zu gründen. Doch können wir dasselbe auch auf negative Formen und Klassen oder auf uneigentlich primitive anwenden. Nach demselben Grundsatz lassen sich sowohl die positive uneigentlich primitive Ordnung als auch die negative eigentlich primitive und die negative uneigentlich primitive Ordnung in Geschlechter einteilen. So kann *zum Beispiel*, nachdem die eigentlich primitive Ordnung der Formen mit der Determinante 145 in die folgenden beiden Geschlechter eingeteilt ist,

$R5,\ R29$	$(1, 0, -145),\ (5, 0, -29)$
$N5,\ N29$	$(3, 1, -48),\ (3, -1, -48)$

auch die uneigentlich primitive Ordnung ebenso in zwei Geschlechter eingeteilt werden:

$R5,\ R29$	$(4, 1, -36),\ (4, -1, -36)$
$N5,\ N29$	$(2, 1, -72),\ (10, 5, -12)$

Oder, wie die positiven Klassen von Formen mit der Determinante -129 in vier Geschlechter zerfallen,

$1, 4;\ R3;\ R43$	$(1, 0, 129),\ (10, 1, 13),\ (10, -1, 13)$
$1, 4;\ N3;\ N43$	$(2, 1, 65),\ (5, 1, 26),\ (5, -1.\ 26)$
$3, 4;\ R3;\ N43$	$(3, 0, 43),\ (7, 2, 19),\ (7, -2, 19)$
$3, 4;\ N3;\ R43$	$(6, 3, 23),\ (11, 5, 14),\ (11, -5, 14)$

so zerfallen auch die negativen Klassen in vier Ordnungen:

$3, 4;\ N3;\ N43$	$(-1, 0, -129),\ (-10, 1, -13),\ (-10, -1, -13)$
$3, 4;\ R3;\ R43$	$(-2, 1, -65),\ (-5, 1, -26),\ (-5, -1, -26)$
$1, 4;\ N3;\ R43$	$(-3, 0, -43),\ (-7, 2, -19),\ (-7, -2, -19)$
$1, 4;\ R3;\ N43$	$(-6, 3, -23),\ (-11, 5, -14),\ (-11, -5, -14)$

Da aber das System der negativen Klassen dem der positiven stets so ähnlich ist, wird es meist überflüssig erscheinen, es gesondert aufzustellen. Wie sich die uneigentlich primitive Ordnung auf die eigentlich primitive zurückführen lässt, werden wir unten zeigen.

Für die Unterteilung der abgeleiteten Ordnungen brauchen wir schließlich keine neuen Regeln. Denn jede abgeleitete Ordnung stammt aus einer primitiven Ordnung

(mit kleinerer Determinante), und ihre einzelnen Klassen entsprechen von selbst den einzelnen Klassen der primitiven Ordnung. Daher lässt sich die Unterteilung der abgeleiteten Ordnung offenbar aus der Unterteilung der primitiven Ordnung gewinnen.

233.

Wenn eine (primitive) Form $F = (a, b, c)$ so beschaffen ist, dass sich zwei Zahlen g, h mit $gg \equiv a$, $gh \equiv b$, $hh \equiv c$ nach einem gegebenen Modul m finden lassen, nennen wir diese Form einen quadratischen Rest der Zahl m und $gx + hy$ einen Wert des Ausdrucks $\sqrt{}(axx + 2bxy + cyy)$(mod. m), oder kürzer (g, h) einen Wert des Ausdrucks $\sqrt{}(a, b, c)$ oder $\sqrt{}F$(mod. m). Allgemeiner: Wenn ein Multiplikator M, der zum Modul m teilerfremd ist, so beschaffen ist, dass

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \quad (\text{mod. } m)$$

gelten kann, nennen wir $M \times (a, b, c)$ oder MF einen quadratischen Rest von m und (g, h) einen Wert des Ausdrucks $\sqrt{}M(a, b, c)$ oder $\sqrt{}MF$(mod. m). So ist *zum Beispiel* die Form $(3, 1, 54)$ ein quadratischer Rest von 23 und $(7, 10)$ ein Wert des Ausdrucks $\sqrt{}(3, 1, 54)$(mod. 23); ebenso ist $(2, -4)$ ein Wert des Ausdrucks $\sqrt{}5(10, 3, 17)$(mod. 23). Wozu diese Definitionen dienen, wird sich später zeigen; hier halten wir die folgenden Sätze fest:

I. Ist $M(a, b, c)$ ein quadratischer Rest der Zahl m, so teilt diese Zahl die Determinante der Form (a, b, c). Denn ist (g, h) ein Wert des Ausdrucks $\sqrt{}M(a, b, c)$ (mod. m), gilt also

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \text{ (mod. } m)$$

so ist $bbMM - acMM \equiv 0$, oder $(bb - ac)MM$ ist durch m teilbar. Da aber M als teilerfremd zu m vorausgesetzt wird, ist auch $bb - ac$ durch m teilbar.

II. Ist $M(a, b, c)$ ein quadratischer Rest von m und m entweder eine Primzahl oder eine Primzahlpotenz, etwa $= p^\mu$, so ist der Einzelcharakter der Form (a, b, c) bezüglich der Zahl p entweder Rp oder Np, je nachdem, ob M Rest oder Nichtrest von p ist. Das folgt sofort daraus, dass sowohl aM als auch cM Rest von m oder von p ist und mindestens eine der Zahlen a, c nicht durch p teilbar ist (Artikel 230).

Ebenso ist, wenn (unter sonst gleichen Bedingungen) $m = 4$ gilt, entweder $1, 4$ oder $3, 4$ der Einzelcharakter der Form (a, b, c), je nachdem, ob $M \equiv 1$ oder $\equiv 3$ ist; Entsprechendes gilt, wenn $m = 8$ oder eine höhere Potenz der Zahl 2 ist. Dann ist $1, 8;\ 3, 8;\ 5, 8;\ 7, 8$ der Einzelcharakter der Form (a, b, c), je nachdem, ob $M \equiv 1;\ 3;\ 5;\ 7$ (mod. 8) gilt.

III. Umgekehrt: Ist m eine Primzahl oder eine Potenz einer ungeraden Primzahl $= p^\mu$, die die Determinante $bb - ac$ teilt, und ist M Rest oder Nichtrest von p, je nachdem, ob der Charakter der Form (a, b, c) bezüglich p gleich Rp oder Np ist, so ist $M(a, b, c)$ ein quadratischer Rest von m. Denn wenn a nicht durch p teilbar ist, ist aM Rest von p und damit auch von m; ist also g ein Wert des Ausdrucks $\sqrt{}aM$ (mod. m) und h ein Wert des Ausdrucks $\frac{bg}{a}$ (mod. m), so ist $gg \equiv aM$; $ah \equiv bg$ und damit

$$agh \equiv bgg \equiv abM \quad \text{und} \quad gh \equiv bM$$

und schließlich

$$ahh \equiv bgh \equiv bbM \equiv bbM - (bb - ac)M \equiv acM$$

und damit $hh \equiv cM$, *d.h.*, (g, h) ist ein Wert des Ausdrucks $\sqrt{}M(a, b, c)$. Ist aber a durch m teilbar, so ist c sicher nicht dadurch teilbar; daraus sieht man leicht, dass

dasselbe folgt, wenn man für h einen Wert des Ausdrucks $\sqrt{cM}$ (mod. m) nimmt. Für g nimmt man einen Wert des Ausdrucks $\frac{bh}{c}$ (mod. m).

Ebenso beweist man: Gilt $m = 4$ und teilt diese Zahl $bb - ac$, und wählt man die Zahl M entweder $\equiv 1$ oder $\equiv 3$, je nachdem, ob $1, 4$ oder $3, 4$ der Einzelcharakter der Form (a, b, c) ist, so ist $M(a, b, c)$ ein quadratischer Rest von m. Ebenso gilt: Gilt $m = 8$ oder ist es eine höhere Potenz von 2, durch die $bb - ac$ teilbar ist, und wählt man M mit $\equiv 1;\ 3;\ 5;\ 7$ (mod. 8), wie es der Einzelcharakter der Form (a, b, c) bezüglich der Zahl 8 verlangt, so ist $M(a, b, c)$ ein quadratischer Rest von m.

IV. Ist die Determinante der Form (a, b, c) durch $= D$ gegeben und $M(a, b, c)$ ein quadratischer Rest von D, so lassen sich alle Einzelcharaktere der Form (a, b, c), sowohl bezüglich der einzelnen ungeraden Primteiler von D als auch bezüglich der Zahl 4 oder der Zahl 8 (wenn sie D teilen), sofort aus der Zahl M ablesen. So sind *zum Beispiel*, weil $3(20, 10, 27)$ ein quadratischer Rest von 440, nämlich $(150, 9)$ ein Wert des Ausdrucks $\sqrt{3(20, 10, 27)}$ nach dem Modul 440 ist und $3N5$, $3R11$ gilt, die Charaktere der Form $(20, 10, 27)$ gleich $3, 8;\ N5;\ R11$. Nur die Einzelcharaktere bezüglich der Zahlen 4 und 8 haben, wenn diese die Determinante nicht teilen, keinen notwendigen Zusammenhang mit der Zahl M

V. Umgekehrt: Enthält die Zahl M, die zu D teilerfremd ist, alle Einzelcharaktere der Form (a, b, c) (mit Ausnahme der Charaktere bezüglich der Zahlen $4, 8$, wenn diese D nicht teilen), so ist $M(a, b, c)$ ein quadratischer Rest von D. Denn aus III folgt: Bringt man D auf die Form $\pm A^\alpha B^\beta D^\gamma \ldots$, wobei A, B, C usw. verschiedene Primzahlen sind, so ist $M(a, b, c)$ ein quadratischer Rest jeder der Zahlen A^α, B^β, C^γ usw. Ist also ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$ nach dem Modul A^α gleich $(\mathfrak{A}, \mathfrak{A}')$; nach dem Modul B^β gleich $(\mathfrak{B}, \mathfrak{B}')$; nach dem Modul C^γ gleich $(\mathfrak{C}, \mathfrak{C}')$ usw., und bestimmt man die Zahlen g, h so, dass $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw.; $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ usw. nach den Moduln A^α, B^β, C^γ usw. gilt (Artikel 32), so sieht man leicht, dass $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ nach allen Moduln A^α, B^β, C^γ usw. gilt und damit auch nach dem Modul D, der ihr Produkt ist.

VI. Aus diesen Gründen nennen wir Zahlen wie M *charakteristische Zahlen* der Form (a, b, c). Nach V lassen sich mehrere solche Zahlen ohne Schwierigkeit finden, sobald alle Einzelcharaktere dieser Form bekannt sind; die einfachsten findet man aber meist am leichtesten durch Probieren. Offenbar sind, wenn M eine charakteristische Zahl einer gegebenen primitiven Form mit der Determinante D ist, alle Zahlen, die M nach dem Modul D kongruent sind, charakteristische Zahlen derselben Form; Formen in derselben Klasse oder auch in verschiedenen Klassen desselben Geschlechts haben dieselben charakteristischen Zahlen, weshalb jede charakteristische Zahl einer gegebenen Form auch der ganzen Klasse und dem ganzen Geschlecht zugeordnet werden kann; schließlich ist 1 stets eine charakteristische Zahl der Hauptform, Hauptklasse und des Hauptgeschlechts, oder jede Form des Hauptgeschlechts ist ein Rest ihrer eigenen Determinante.

VII. Ist (g, h) ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$ (mod. m) und gilt $g' \equiv g$, $h' \equiv h$ (mod. m), so ist auch (g', h') ein Wert desselben Ausdrucks. Solche Werte können als *äquivalent* gelten; sind dagegen (g, h), (g', h') Werte desselben Ausdrucks $\sqrt{M(a, b, c)}$, ohne dass zugleich $g' \equiv g$, $h' \equiv h$ (mod. m) gilt, so sind sie als *verschieden* zu zählen. Offenbar ist, wenn (g, h) ein Wert eines solchen Ausdrucks ist, auch $(-g, -h)$ ein

solcher Wert, und man beweist leicht, dass diese Werte stets verschieden sind, außer wenn $m = 2$ ist. Ebenso leicht beweist man, dass der Ausdruck $\sqrt{M}(a, b, c)$ (mod. m) nicht mehr verschiedene Werte als zwei solche (entgegengesetzte) haben kann, wenn m entweder eine ungerade Primzahl, eine Potenz einer ungeraden Primzahl oder $= 4$ ist; gilt dagegen $m = 8$ oder ist es eine höhere Potenz der Zahl 2, so gibt es genau vier. Daraus folgt mit VI leicht: Ist die Determinante D der Form (a, b, c) durch $= \pm 2^\mu A^\alpha B^\beta \ldots$ gegeben, wobei A, B usw. verschiedene ungerade Primzahlen bezeichnen, deren Anzahl $= n$ ist, und ist M eine charakteristische Zahl dieser Form, so gibt es genau 2^n, 2^{n+1} oder 2^{n+2} verschiedene Werte des Ausdrucks $\sqrt{M}(a, b, c)$ (mod. D), je nachdem, ob $\mu < 2$, $= 2$ oder > 2 ist. So gibt es *zum Beispiel* sechzehn Werte des Ausdrucks $\sqrt{7}(12, 6, -17)$ (mod. 240), nämlich $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Einen ausführlicheren Beweis lassen wir der Kürze wegen weg, da er für das Folgende nicht besonders nötig ist.

VIII. Schließlich bemerken wir: Haben zwei äquivalente Formen (a, b, c), (a', b', c') die Determinante D und die charakteristische Zahl M, und geht die erste durch die Substitution $\alpha, \beta, \gamma, \delta$ in die zweite über, so ergibt sich aus jedem Wert des Ausdrucks $\sqrt{M}(a, b, c)$, etwa (g, h), ein Wert des Ausdrucks $\sqrt{M}(a', b', c')$, nämlich $(\alpha g + \gamma h, \beta g + \delta h)$. Den Beweis kann jeder ohne Schwierigkeit finden.

Komposition der Formen.

234.

Nachdem wir die Einteilung der Formen in Klassen, Geschlechter und Ordnungen besprochen und die allgemeinen Eigenschaften erklärt haben, die sich unmittelbar aus diesen Unterscheidungen ergeben, gehen wir zu einem anderen sehr wichtigen Gegenstand über, den bisher noch niemand behandelt hat: der *Komposition* der Formen. Am Anfang dieser Untersuchung schieben wir gleich das folgende Lemma ein, damit wir später die fortlaufende Folge der Beweise nicht unterbrechen müssen.

Lemma. *Gegeben seien vier Folgen ganzer Zahlen*

$$a, a', a'' \ldots a^n; \qquad b, b', b'' \ldots b^n;$$
$$c, c', c'' \ldots c^n; \qquad d, d', d'' \ldots d^n$$

mit gleich vielen (etwa $n + 1$) Gliedern, so beschaffen, dass

$$cd' - dc', \quad cd'' - dc'' \text{ etc.}, \quad c'd'' - d'c'' \text{ etc. etc.}$$

jeweils gleich

$$= k(ab' - ba'), \quad k(ab'' - ba'') \text{ etc.}, \quad k(a'b'' - b'a'') \text{ etc. etc.}$$

sind, oder allgemein

$$c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$$

gilt; dabei bezeichnet k eine gegebene ganze Zahl; λ, μ sind beliebige verschiedene ganze Zahlen zwischen 0 und n einschließlich, deren größere μ ist[*]*; außerdem haben*

[*] Dabei betrachten wir a als a^0, b als b^0 usw. — Übrigens gilt dieselbe Gleichung offenbar auch, wenn $\lambda = \mu$ oder $\lambda > \mu$ ist.

alle $a^\lambda b^\mu - b^\lambda a^\mu$ *keinen gemeinsamen Teiler. Dann lassen sich vier ganze Zahlen* $\alpha, \beta, \gamma, \delta$ *finden, sodass*

$$\alpha a + \beta b = c, \quad \alpha a' + \beta b' = c', \quad \alpha a'' + \beta b'' = c'' \text{ etc.}$$
$$\gamma a + \delta b = d, \quad \gamma a' + \delta b' = d', \quad \gamma a'' + \delta b'' = d'' \text{ etc.}$$

oder allgemein

$$\alpha a^\nu + \beta b^\nu = c^\nu, \quad \gamma a^\nu + \delta b^\nu = a^\nu$$

gilt; dann ist

$$\alpha\delta - \beta\gamma = k$$

Da nach Voraussetzung die Zahlen $ab' - ba'$, $ab'' - ba''$ usw., $a'b'' - b'a''$ usw. (deren Anzahl $= \frac{1}{2}(n+1)n$ ist) keinen gemeinsamen Teiler haben, lassen sich ebenso viele andere ganze Zahlen finden, sodass die Summe der Produkte $= 1$ ist, wenn man jene jeweils mit diesen multipliziert (Artikel 40). Bezeichnen wir diese Multiplikatoren mit $(0,1)$, $(0,2)$ usw., $(1,2)$ usw., oder allgemein den Multiplikator von $a^\lambda b^\mu - b^\lambda a^\mu$ mit (λ, μ), sodass

$$\Sigma(\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1$$

gilt. (Mit dem Buchstaben Σ bezeichnen wir die Summe aller Werte des Ausdrucks, der auf ihn folgt, die entstehen, wenn man λ, μ alle verschiedenen Werte zwischen 0 und n mit $\mu > \lambda$ gibt.) Setzen wir nun

$$\Sigma(\lambda,\mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha, \quad \Sigma(\lambda,\mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta$$
$$\Sigma(\lambda,\mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma, \quad \Sigma(\lambda,\mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta$$

so haben diese $\alpha, \beta, \gamma.\delta$ die verlangten Eigenschaften.

Beweis. I. Bezeichnet ν eine beliebige ganze Zahl zwischen 0 und n, so ist

$$\begin{aligned}\alpha a^\nu + \beta b^\nu &= \Sigma(\lambda,\mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu)\\ &= \frac{1}{k}\Sigma(\lambda,\mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu)\\ &= \frac{1}{k}c^\nu\Sigma(\lambda,\mu)(c^\lambda d^\mu - d^\lambda c^\mu)\\ &= c^\nu\Sigma(\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu\end{aligned}$$

Eine ähnliche Rechnung ergibt

$$\gamma a^\nu + \delta b^\nu = d^\nu. \qquad Q.\ E.\ P.$$

II. Da also

$$c^\lambda = \alpha a^\lambda + \beta b^\lambda, \quad c^\mu = \alpha a^\mu + \beta b^\mu$$

gilt, ist

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$$

und ebenso

$$a^\lambda c^\mu - c^\lambda a^\mu = \beta(a^\lambda b^\mu - b^\lambda a^\mu)$$
$$d^\lambda b^\mu - b^\lambda d^\mu = \gamma(a^\lambda b^\mu - b^\lambda a^\mu)$$
$$a^\lambda d^\mu - d^\lambda a^\mu = \delta(a^\lambda b^\mu - b^\lambda a^\mu)$$

Aus diesen Formeln lassen sich die Werte von $\alpha, \beta, \gamma, \delta$ viel leichter finden, wenn man nur λ, μ so wählt, dass $a^\lambda b^\mu - b^\lambda a^\mu$ nicht $= 0$ ist. Das ist sicher möglich, weil nach Voraussetzung alle $a^\lambda b^\mu - b^\lambda a^\mu$ keinen gemeinsamen Teiler haben und daher nicht *alle* $= 0$ sein können. — Multipliziert man die erste dieser Gleichungen mit der vierten und die zweite mit der dritten und subtrahiert, so ergibt sich aus denselben Gleichungen

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$$

und damit notwendig

$$\alpha\delta - \beta\gamma = k. \qquad \textit{Q. E. S.}$$

235.

Wenn die Form

$$AXX + 2BXY + CYY \ldots F$$

in das Produkt der beiden Formen

$$axx + 2bxy + cyy \ldots f, \quad \text{und} \quad a'x'x' + 2b'x'y' + c'y'y' \ldots f'$$

durch eine Substitution der Art

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

übergeht (was wir im Folgenden der Kürze wegen stets so ausdrücken: Wenn F in ff' durch die Substitution p, p', p'', p'''; q, q', q'', q''' übergeht[*]), nennen wir die Form F einfach in ff' *transformierbar*; ist diese Transformation außerdem so beschaffen, dass die sechs Zahlen

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''',$$
$$p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

keinen gemeinsamen Teiler haben, so nennen wir die Form F aus den Formen f, f' *zusammengesetzt*.

Wir beginnen diese Untersuchung mit der allgemeinsten Annahme, dass die Form F in ff' durch die Substitution p, p', p'', p'''; q, q', q'', q''' übergeht, und entwickeln ihre Folgen. Dieser Annahme sind offenbar die folgenden neun Gleichungen genau gleichwertig (*d.h.*, sobald diese Gleichungen gelten, geht F durch die genannte Substitution in ff' über, und umgekehrt):

$$App + 2Bpq + Cqq = aa' \quad \ldots \quad [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac' \quad \ldots \quad [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca' \quad \ldots \quad [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc' \quad \ldots \quad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \quad \ldots \quad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \quad \ldots \quad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \quad \ldots \quad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \quad \ldots \quad [8]$$
$$\begin{aligned} A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') \\ + C(qq''' + q'q'') \end{aligned} = 2bb' \quad \ldots \quad [9]$$

[*] Bei dieser Bezeichnung muss man also sowohl die Reihenfolge der Koeffizienten p, p' usw. als auch die der Formen f, f' genau beachten. Man sieht leicht: Wird die Reihenfolge der Formen f, f' umgekehrt, sodass die erste zur zweiten wird, so müssen die Koeffizienten p', q' mit p'', q'' vertauscht werden, während jeder der übrigen an seinem Platz bleibt.

Die Determinanten der Formen F, f, f' seien jeweils D, d, d'; die größten gemeinsamen Teiler der Zahlen $A, 2B, C;\ a, 2b, c;\ a', 2b', c'$ seien jeweils M, m, m' (alle positiv genommen). Weiter bestimmen wir sechs ganze Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ so, dass

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \qquad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$$

gilt. Schließlich bezeichnen wir die Zahlen

$$\begin{gathered} pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''', \\ p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p''' \end{gathered}$$

der Reihe nach mit P, Q, R, S, T, U, und ihr positiv genommener größter gemeinsamer Teiler sei $= k$. — Setzen wir nun

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \quad \ldots . \qquad [10]$$

so folgt aus Gleichung 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \quad \ldots . \qquad [11]$$

Aus diesen elf Gleichungen $1 \ldots 11$ leiten wir die folgenden neuen ab[*)]:

$$\begin{aligned} DPP &= d'aa \quad \ldots\ldots\ldots\ldots && [12] \\ DP(R-S) &= 2d'ab \quad \ldots\ldots\ldots\ldots && [13] \\ DPU &= d'ac - (\Delta\Delta - dd') \quad \ldots\ldots\ldots && [14] \\ D(R-S)^2 &= 4d'bb + 2(\Delta\Delta - dd') \quad \ldots\ldots && [15] \\ D(R-S)U &= 2d'bc \quad \ldots\ldots\ldots\ldots && [16] \\ DUU &= d'cc \quad \ldots\ldots\ldots\ldots && [17] \\ DQQ &= da'a' \quad \ldots\ldots\ldots\ldots && [18] \\ DQ(R+S) &= 2da'b' \quad \ldots\ldots\ldots\ldots && [19] \\ DQT &= da'c' - (\Delta\Delta - dd') \quad \ldots\ldots\ldots && [20] \\ D(R+S)^2 &= 4db'b' + 2(\Delta\Delta - dd') \quad \ldots\ldots && [21] \\ D(R+S)T &= 2db'c' \quad \ldots\ldots\ldots\ldots && [22] \\ DTT &= dc'c' \quad \ldots\ldots\ldots\ldots && [23] \end{aligned}$$

Daraus folgen wiederum diese beiden:

$$\begin{aligned} 0 &= 2d'aa(\Delta\Delta - dd') \\ 0 &= (\Delta\Delta - dd')^2 - 2d'ac(\Delta\Delta - dd') \end{aligned}$$

[*)] Diese Gleichungen entstehen so: 12 aus $5.5 - 1.2$; 13 aus $5.9 - 1.7 - 2.6$; 14 aus $10.11 - 6.7$; 15 aus $5.8 + 5.8 + 10.10 + 11.11 - 1.4 - 2.3 - 6.7 - 6.7$; 16 aus $8.9 - 3.7 - 4.6$; 17 aus $8.8 - 3.4$. Die übrigen sechs leitet man ebenso her, wenn man die Gleichungen $2, 5, 7$ jeweils mit den Gleichungen $3, 6, 8$ vertauscht und die übrigen $1, 4, 9, 10, 11$ weiterhin an derselben Stelle lässt; so entsteht 18 aus $6.6 - 1.3$ usw.

und zwar die erste aus $12.15 - 13.13$, die zweite aus $14.14 - 12.17$; daraus sieht man leicht, dass notwendig $\Delta\Delta - dd' = 0$ ist, ob nun $a = 0$ oder nicht $= 0$ gilt[*]. Wir nehmen also an, dass in den Gleichungen $14, 15, 20, 21$ auf der rechten Seite $\Delta\Delta - dd'$ gestrichen wird.

Setzen wir nun

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n$$

(wobei genau zu beachten ist, dass n, n' auch Brüche sein können, obwohl $mn', m'n$ notwendig ganze Zahlen sind), so folgt leicht aus den Gleichungen $12 \ldots 17$

$$Dmmn'n' = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'mm$$

und ebenso aus den Gleichungen $18 \ldots 23$

$$Dm'm'nn = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'm'$$

Es ist also $d = Dnn$, $d' = Dn'n'$, und wir erhalten den ERSTEN SCHLUSS: *Die Determinanten der Formen F, f, f' stehen notwendig im Verhältnis von Quadraten zueinander;* und den ZWEITEN: *D teilt stets die Zahlen $dm'm', d'mm$.* Offenbar haben also D, d, d' dasselbe Vorzeichen, und es kann keine Form in das Produkt ff' transformierbar sein, deren Determinante größer ist als der größte gemeinsame Teiler der Zahlen $dm'm', d'mm$.

Multiplizieren wir die Gleichungen $12, 13, 14$ jeweils mit $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$; ebenso die Gleichungen $13, 15, 16$ und $14, 16, 17$ mit denselben Zahlen; addieren wir je drei Produkte und teilen die Summe durch Dmn', wobei wir für d' den Wert $Dn'n'$ schreiben. Dann ergibt sich

$$P = an', \quad R - S = 2bn', \quad U = cn'$$

Multipliziert man ebenso die Gleichungen $18, 19, 20$ sowie $19, 21, 22$ und $20, 22, 23$ jeweils mit $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$, so erhält man

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n$$

Daraus folgt der DRITTE SCHLUSS: *Die Zahlen $a, 2b, c$ sind den Zahlen $P, R - S, U$ proportional; setzt man ihr Verhältnis zu diesen gleich 1 zu n', so ist n' eine Quadratwurzel aus $\frac{d'}{D}$; ebenso haben die Zahlen $a', 2b', c'$ zu $Q, R + S, T$ dasselbe Verhältnis, und setzt man dieses gleich 1 zu n, so ist n eine Quadratwurzel aus $\frac{d}{D}$.*

Die Größen n, n' können aber positive oder negative Quadratwurzeln aus $\frac{d}{D}, \frac{d'}{D}$ sein. Daraus gewinnen wir eine Unterscheidung, die auf den ersten Blick unfruchtbar erscheinen mag, deren Nutzen sich aber im Folgenden hinreichend zeigen wird. Wir sagen nämlich, dass bei der Transformation der Form F in ff' die Form f *direkt* genommen wird, wenn n positiv ist, und *invers*, wenn n negativ ist; ebenso wird f' direkt oder invers genommen, je nachdem, ob n' positiv oder negativ ist. Kommt die

[*] Diese Herleitung der Gleichung $\Delta\Delta = dd'$ genügt für unseren gegenwärtigen Zweck; sonst könnten wir eine elegantere, hier aber zu lange Analyse geben, indem wir aus den Gleichungen $1 \ldots 11$ unmittelbar die Gleichung $0 = (\Delta\Delta - dd')^2$ herleiten.

Bedingung hinzu, dass $k = 1$ ist, so heißt die Form F *entweder* aus beiden Formen f, f' direkt zusammengesetzt, *oder* aus beiden invers, *oder* aus f direkt und aus f' invers, *oder* aus f invers und aus f' direkt, je nachdem, ob n, n' beide positiv, beide negativ, die erste positiv und die zweite negativ oder die erste negativ und die zweite positiv sind. Übrigens wird jeder leicht einsehen, dass diese Beziehungen nicht von der Reihenfolge der Formen f, f' abhängen (siehe die erste Anmerkung zu diesem Artikel).

Weiter bemerken wir, dass der größte gemeinsame Teiler der Zahlen P, Q, R, S, T, U, nämlich k, die Zahlen $mn', m'n$ teilt (wie aus den oben festgestellten Werten hervorgeht), also das Quadrat kk die Zahlen $mmn'n', m'm'nn$ und Dkk die Zahlen $d'mm, dm'm'$ teilt. Umgekehrt teilt aber auch jeder gemeinsame Teiler von $mn', m'n$ die Zahl k. Sei nämlich e ein solcher Teiler; er teilt offenbar auch die Zahlen $an', 2bn', cn', a'n, 2b'n, c'n$, *d.h.*, die Zahlen $P, R - S, U, Q, R + S, T$ und damit auch $2R$ und $2S$. Wäre nun $\frac{2R}{e}$ ungerade, so müsste auch $\frac{2S}{e}$ ungerade sein (weil Summe und Differenz gerade sind), also auch ihr Produkt. Dieses Produkt ist aber $= \frac{4}{ee}(b'b'nn - bbn'n') = \frac{4}{ee}(d'nn + a'c'nn - dn'n' - acn'n') = \frac{4}{ee}(a'c'nn - acn'n')$ und damit gerade, weil e die Zahlen $a'n, c'n, an', cn'$ teilt. Also ist $\frac{2R}{e}$ notwendig gerade und damit R sowie S durch e teilbar. Da also e alle sechs Zahlen P, Q, R, S, T, U teilt, teilt es auch deren größten gemeinsamen Teiler k. *Q. E. D.* — Daraus folgt, dass k der größte gemeinsame Teiler der Zahlen $mn', m'n$ ist; daraus sieht man leicht, dass *Dkk der größte gemeinsame Teiler der Zahlen $dm'm', d'mm$ ist.* Das ist der VIERTE SCHLUSS. Offenbar ist also, wenn F aus f und f' zusammengesetzt ist, D der größte gemeinsame Teiler der Zahlen $dm'n', d'mm$, und umgekehrt; diese Eigenschaft hätte man auch als Definition der zusammengesetzten Form nehmen können. Eine aus den Formen f, f' zusammengesetzte Form hat also die größtmögliche Determinante unter allen Formen, die in das Produkt ff' transformierbar sind.

Bevor wir weitergehen können, müssen wir zunächst den Wert von Δ genauer bestimmen. Wir haben zwar gezeigt, dass er $= \sqrt{dd'} = \sqrt{DDnnn'n'}$ ist, doch sein *Vorzeichen* ist dadurch noch nicht bestimmt. Dazu leiten wir aus den Fundamentalgleichungen 1—11 die Gleichung $DPQ = \Delta aa'$ her (sie ergibt sich aus $5.6 - 1.11$), also $Daa'nn' = \Delta aa'$, woraus, wenn nicht eine der Zahlen $a, a' = 0$ ist, $\Delta = Dnn'$ folgt. Ganz ebenso lassen sich aber aus den Fundamentalgleichungen acht weitere herleiten, in denen auf der linken Seite Dnn' und auf der rechten Δ mit $2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc'$ multipliziert sind[*)]. Da weder alle $a, 2b, c$ noch alle $a', 2b', c' = 0$ sein können, folgt leicht, dass in allen Fällen $\Delta = Dnn'$ gilt und damit Δ dasselbe Vorzeichen wie D, d, d' oder das entgegengesetzte hat, je nachdem, ob n, n' gleiche oder verschiedene Vorzeichen haben.

Weiter bemerken wir, dass die Zahlen $aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc', 2bb' + 2\Delta, 2bb' - 2\Delta$ alle durch mm' teilbar sind. Für die ersten neun ist das unmittelbar klar; für die beiden übrigen lässt es sich ebenso beweisen, wie wir oben gezeigt haben, dass R und S durch e teilbar sind. Offenbar sind nämlich $4bb' + 4\Delta$ und $4bb' - 4\Delta$ durch mm' teilbar (weil $4\Delta = \sqrt{16dd'}$ und $4d$ durch mm, $4d'$ durch $m'm'$ teilbar ist, also $16dd'$ durch $mmm'm'$ und 4Δ durch mm'), und die Differenz

[*)] Die Analyse, die die Leser leicht selbst finden können, müssen wir der Kürze wegen weglassen.

der Quotienten ist gerade; ihr Produkt lässt sich leicht als gerade nachweisen, also ist jeder Quotient gerade und $2bb' + 2\Delta, 2bb' - 2\Delta$ sind durch mm' teilbar.

Aus den elf Fundamentalgleichungen folgen nun leicht die sechs folgenden:

$$\begin{aligned}
APP &= aa'q'q' - 2ab'qq' + ac'qq \\
AQQ &= aa'q''q'' - 2ba'qq'' + ca'qq \\
ARR &= aa'q'''q''' - 2(bb' + \Delta)qq''' + cc'qq \\
ASS &= ac'q''q'' - 2(bb' - \Delta)q'q'' + ca'q'q' \\
ATT &= ac'q'''q''' - 2bc'q'q''' + cc'q'q' \\
AUU &= ca'q'''q''' - 2cb'q''q''' + cc'q''q''
\end{aligned}$$

Daraus folgt, dass alle APP, AQQ usw. durch mm' teilbar sind; da kk der größte gemeinsame Teiler der Zahlen PP, QQ, RR usw. ist, folgt daraus leicht, dass auch Akk durch mm' teilbar ist. Setzt man für $a, 2b, c$, $a', 2b', c'$ ihre Werte $\frac{P}{n'}$ usw. oder $\frac{1}{n'}(pq' - qp')$ usw. ein, so gehen sie in sechs andere Gleichungen über, auf deren rechten Seiten die Produkte aus der Größe $\frac{1}{nn'}(q'q'' - qq''')$ mit PP, QQ, RR usw. stehen. Diese sehr leichte Rechnung überlassen wir den Lesern. Daraus folgt (weil nicht alle PP, QQ usw. $= 0$ sein können) $Ann' = q'q'' - qq'''$.

Ebenso leitet man aus den Fundamentalgleichungen sechs weitere Gleichungen her, die sich von den vorigen nur dadurch unterscheiden, dass überall A durch C und q, q', q'', q''' jeweils durch p, p', p'', p''' ersetzt werden. Der Kürze wegen schreiben wir sie nicht hin. Daraus folgt ebenso, dass Ckk durch mm' teilbar ist und $Cnn' = p'p'' - pp'''$ gilt.

Schließlich ergeben sich aus derselben Quelle diese sechs Gleichungen:

$$\begin{aligned}
BPP &= -aa'p'q' + ab'(pq' + qp') - ac'pq \\
BQQ &= -aa'p''q'' + ba'(pq'' + qp'') - ca'pq \\
BRR &= -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq \\
BSS &= -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q' \\
BTT &= -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q' \\
BUU &= -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q''
\end{aligned}$$

woraus wir wie zuvor schließen, dass $2Bkk$ durch mm' teilbar ist und $2Bnn' = pq''' + qp''' - p'q'' - q'p''$ gilt.

Da also $Akk, 2Bkk, Ckk$ durch mm' teilbar sind, sieht man leicht, dass auch Mkk durch mm' teilbar sein muss. Aus den Fundamentalgleichungen folgt aber, dass M die Zahlen $aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc'$ teilt und damit auch $am', 2bm', cm'$ (die größten gemeinsamen Teiler jeweils der ersten, mittleren und letzten drei); schließlich auch mm', ihren größten gemeinsamen Teiler. Daraus sieht man, dass in dem Fall, in dem die Form F aus den Formen f, f' zusammengesetzt ist, also $k = 1$ gilt, notwendig $M = mm'$ ist. Das ist der FÜNFTE SCHLUSS.

Ist der größte gemeinsame Teiler der Zahlen A, B, C gleich $\mathfrak{M}$, so ist dieser entweder $= M$ (wenn die Form F eigentlich primitiv oder aus einer eigentlich primitiven

Form abgeleitet ist) oder $= \frac{1}{2}M$ (wenn F uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet ist); ebenso bezeichnen wir die größten gemeinsamen Teiler der Zahlen a, b, c; a', b', c' jeweils mit $\mathfrak{m}, \mathfrak{m}'$; dann ist $\mathfrak{m}$ entweder $= m$ oder $\frac{1}{2}m$ und $\mathfrak{m}'$ entweder $= m'$ oder $= \frac{1}{2}m'$. Offenbar teilt nun $\mathfrak{mm}$ die Zahl d', $\mathfrak{m}'\mathfrak{m}'$ die Zahl d', also $\mathfrak{mmm}'\mathfrak{m}'$ die Zahl dd' oder $\Delta\Delta$ und $\mathfrak{mm}'$ die Zahl Δ. Aus den letzten sechs Gleichungen für BPP usw. folgt dann, dass $\mathfrak{mm}'$ die Zahl Bkk teilt und damit (weil es auch Akk, Ckk teilt) auch $\mathfrak{M}kk$. Wenn also F aus f, f' zusammengesetzt ist, teilt $\mathfrak{mm}'$ die Zahl $\mathfrak{M}$. Sind daher in diesem Fall beide f, f' eigentlich primitiv oder aus eigentlich primitiven Formen abgeleitet, gilt also $\mathfrak{mm}' = mm' = M$, so ist $\mathfrak{M} = M$, oder F ist eine ebensolche Form. Sind dagegen unter derselben Voraussetzung entweder beide f, f' oder wenigstens eine davon uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet, *zum Beispiel* die Form f, so folgt aus den Fundamentalgleichungen, dass $aa', 2ab', ac', ba', 2bb', bc', ca', 2cb', cc'$ durch $\mathfrak{M}$ teilbar sind, also auch am', bm', cm' und damit auch $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$; daraus folgt in diesem Fall notwendig $\mathfrak{M} = \frac{1}{2}M$, oder die Form F ist ebenfalls uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet. Das ergibt den SECHSTEN SCHLUSS.

Schließlich bemerken wir: Wenn man *annimmt*, dass die neun Gleichungen

$$\begin{gathered} an' = P, \quad 2bn' = R - S, \quad cn' = U \\ a'n = Q, \quad 2b'n = R + S, \quad c'n = T \\ Ann' = q'q'' - qq''', \\ 2Bnn' = pq''' + qp''' - p'q'' - q'p'', \\ Cnn' = p'p'' - pp''' \end{gathered}$$

(die wir mit Ω bezeichnen werden, weil wir im Folgenden öfter darauf zurückkommen müssen) gelten, und dabei sogar n, n' als Unbekannte betrachtet, von denen jedoch keine $= 0$ ist, dann bestätigt man durch Einsetzen leicht, dass auch die Fundamentalgleichungen $1 \ldots 9$ notwendig wahr sind, also die Form (A, B, C) durch die Substitution p, p', p'', p'''; q, q', q'', q''' in das Produkt der Formen $(a, b, c)(a', b', c')$ übergeht; außerdem gilt

$$bb - ac = nn(BB - AC), \quad b'b' - a'c' = n'n'(BB - AC)$$

Die Rechnung, die hier zu lang wäre, überlassen wir dem Fleiß der Leser.

236.

Aufgabe. *Gegeben sind zwei Formen, deren Determinanten entweder gleich sind oder wenigstens im Verhältnis von Quadraten zueinander stehen. Gesucht ist eine aus ihnen zusammengesetzte Form.*

Lösung. Die zusammenzusetzenden Formen seien $(a,b,c)\ldots f$, $(a',b',c')\ldots f'$; ihre Determinanten seien d,d'; die größten gemeinsamen Teiler der Zahlen $a,2b,c$; a', $2b',c'$ seien jeweils m,m'; der größte gemeinsame Teiler der Zahlen $dm'm', d'mm$, mit demselben Vorzeichen wie d,d' versehen, sei D. Dann sind $\frac{dm'm'}{D}, \frac{d'mm}{D}$ positive, zueinander teilerfremde Zahlen, deren Produkt ein Quadrat ist; also sind sie selbst Quadrate (Artikel 21). Damit sind $\sqrt{\frac{d}{D}}, \sqrt{\frac{d'}{D}}$ rationale Größen, die wir $= n, n'$ setzen. Dabei nehmen wir für n den positiven oder negativen Wert, je nachdem, ob die Form f direkt oder invers in die Komposition eingehen soll; ebenso bestimmen wir das Vorzeichen von n' danach, wie f' in die Komposition eingehen soll. Also sind $mn', m'n$ zueinander teilerfremde ganze Zahlen; n und n' können aber auch Brüche sein. Nun bemerken wir, dass $an', cn', a'n, c'n, bn'+b'n, bn'-b'n$ ganze Zahlen sind. Für die ersten vier ist das unmittelbar klar (weil $an' = \frac{a}{m}mn'$ usw.); für die übrigen beiden beweist man es ebenso, wie im vorigen Artikel gezeigt wurde, dass R und S durch e teilbar sind.

Nun wählen wir vier beliebige ganze Zahlen $\mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$, nur unter der Bedingung, dass die vier Größen auf der linken Seite der folgenden Gleichung (I) nicht alle zugleich $= 0$ werden, und setzen

$$\begin{aligned}
\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn'+b'n) &= \mu q \qquad \ldots\ldots \qquad \text{(I)}\\
-\mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}''(bn'-b'n) &= \mu q'\\
\mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn'-b'n) &= \mu q''\\
-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn'+b'n) &= \mu q'''
\end{aligned}$$

so, dass q, q', q'', q''' ganze Zahlen ohne gemeinsamen Teiler werden. Das erreicht man, indem man für μ den größten gemeinsamen Teiler der vier Zahlen auf den linken Seiten dieser Gleichungen nimmt. Dann lassen sich nach Artikel 40 vier ganze Zahlen $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ finden, sodass

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

gilt. Danach bestimmen wir die Zahlen p, p', p'', p''' durch die folgenden Gleichungen:

$$\begin{aligned}
\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn'+b'n) &= p \qquad \ldots\ldots \qquad \text{(II)}\\
-\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn'-b'n) &= p'\\
\mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn'-b'n) &= p''\\
-\mathfrak{P}''cn' - \mathfrak{P}'c'n - \mathfrak{P}(bn'+b'n) &= p'''
\end{aligned}$$

Schließlich setzen wir

$$\begin{gathered}
q'q'' - qq''' = Ann',\\
pq''' + qp''' - p'q'' - q'p'' = 2Bnn',\\
p'p'' - pp''' = Cnn'
\end{gathered}$$

Dann sind A, B, C ganze Zahlen, und die Form $(A, B, C) \dots F$ ist aus den Formen f, f' zusammengesetzt.

Beweis. I. Aus den Gleichungen I bestätigt man ohne Schwierigkeit die folgenden vier Gleichungen:

$$\begin{aligned} 0 &= q'cn' - q''c'n - q'''(bn' - b'n) \qquad \dots\dots \qquad \text{(III)} \\ 0 &= qcn' + q'''a'n - q''(bn' + b'n) \\ 0 &= q'''an' + qc'n - q'(bn' + b'n) \\ 0 &= q''an' - q'a'n - q(bn' - b'n) \end{aligned}$$

II. Nehmen wir nun an, die ganzen Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \mathfrak{N}, \mathfrak{N}'$ seien so bestimmt, dass

$$\begin{aligned} \mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m \\ \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m' \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1 \end{aligned}$$

gilt. Dann ist

$$\begin{aligned} &\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' \\ &\qquad + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1 \end{aligned}$$

Daraus und aus den Gleichungen (III) bestätigt man leicht: Setzt man

$$\begin{aligned} -q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q} \\ q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}' \\ -q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'' \\ q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}''' \end{aligned}$$

so ist

$$\begin{aligned} \mathfrak{q}'an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) &= q \qquad \dots\dots \qquad \text{(IV)} \\ -\mathfrak{q}an' + \mathfrak{q}'''c'n - \mathfrak{q}''(bn' - b'n) &= q' \\ \mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) &= q'' \\ -\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) &= q''' \end{aligned}$$

Wenn $\mu = 1$ gilt, sind diese Gleichungen nicht nötig; an ihrer Stelle kann man die Gleichungen (I) beibehalten, denen sie völlig entsprechen. Entwickelt man nun aus den Gleichungen II, IV die Werte von $Ann', 2Bnn', Cnn'$ (*d.h.*, der Zahlen $q'q'' - qq'''$ usw.) und streicht die Glieder, die einander aufheben, so findet man, dass die Glieder jeder dieser Größen Produkte aus ganzen Zahlen mit nn', mit $dn'n'$ oder mit $d'nn$ sind und außerdem alle Glieder von $2Bnn'$ den Faktor 2 enthalten. Daraus folgt (weil $dn'n' = d'nn$ und daher $\frac{dn'n'}{nn'} = \frac{d'nn}{nn'} = \sqrt{dd'}$ ganze Zahlen sind), dass A, B, C ganze Zahlen sind. *Q. E. P.*

III. Setzt man aus den Gleichungen (II) die Werte von p, p', p'', p''' ein, so bestätigt man mithilfe der Gleichungen (III) und der Gleichung

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

leicht, dass

$$\begin{aligned} pq' - qp' &= an', \\ pq''' - qp''' - p'q'' + q'p'' &= 2bn', \\ p''q''' - q''p''' &= cn' \\ pq'' - qp'' &= a'n, \\ pq''' - qp''' + p'q'' - q'p'' &= 2b'n, \\ p'q''' - q'p''' &= c'n \end{aligned}$$

gilt. Diese Gleichungen sind mit den ersten sechs (Ω) des vorigen Artikels identisch; die übrigen drei gelten bereits nach Voraussetzung. Also geht (*am Ende desselben Artikels*) die Form F in ff' durch die Substitution p, p', p'', p'''; $q, q', q''\, q'''$ über; ihre Determinante ist $= D$, also gleich dem größten gemeinsamen Teiler der Zahlen $dm'm', d'mm$, weshalb nach dem vierten Schluss des vorigen Artikels F aus f, f' zusammengesetzt ist. *Q. E. S.* Schließlich sieht man leicht, dass F aus f, f' *so* zusammengesetzt ist, wie es verlangt war, weil die Vorzeichen der Größen n, n' schon von Anfang an richtig bestimmt wurden.

237.

Satz. *Ist eine Form F in das Produkt zweier Formen f, f' transformierbar und enthält die Form f' die Form f'', so ist F auch in das Produkt der Formen f, f'' transformierbar.*

Beweis. Wir behalten für die Formen F, f, f' alle Bezeichnungen aus Artikel 235 bei; die Form f'' sei $= (a'', b'', c'')$, und f' gehe in f'' durch die Substitution $\alpha. \beta, \gamma, \delta$ über. Dann sieht man ohne Schwierigkeit, dass F in ff'' übergeht, und zwar durch die Substitution

$$\begin{array}{cccc} \alpha p + \gamma p', & \beta p + \delta p', & \alpha p'' + \gamma p''', & \beta p'' + \delta p''' \\ \alpha q + \gamma q', & \beta q + \delta q', & \alpha q'' + \gamma q''', & \beta q'' + \delta q''' \end{array} \qquad \textit{Q. E. D.}$$

Setzen wir der Kürze wegen die Koeffizienten

$$\begin{gathered} \alpha p + \gamma p', \quad \beta p + \delta p' \text{ etc.} \\ = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \quad \mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}''' \end{gathered}$$

und die Zahl $\alpha\delta - \beta\gamma = e$, so bestätigt man aus den Gleichungen Ω des Artikels 235 leicht, dass

$$\begin{aligned} \mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' &= an'e \\ \mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' &= 2bn'e \\ \mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' &= cn'e \\ \mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' &= \alpha\alpha a'n + 2\alpha\gamma b'n + \gamma\gamma c'n = a''n \\ \mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2b''n \\ \mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' &= c''n \\ \mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' &= Ann'e \\ \mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2Bnn'e \\ \mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e \end{aligned}$$

gilt. Bezeichnen wir nun die Determinante der Form f'' mit d'', so ist e eine Quadratwurzel aus $\frac{d''}{d'}$, und zwar positiv oder negativ, je nachdem, ob die Form f' die Form f'' eigentlich oder uneigentlich enthält. Also ist $n'e$ eine Quadratwurzel aus $\frac{d''}{D}$; daraus sieht man, dass die neun vorstehenden Gleichungen den Gleichungen Ω des Artikels 235 völlig entsprechen und die Form f bei der Transformation der Form F in ff'' ebenso genommen wird wie bei der Transformation der Form F in ff'; die Form f'' wird dagegen bei der ersten Transformation entweder ebenso wie f' bei der zweiten oder entgegengesetzt genommen, je nachdem, ob f' die Form f'' eigentlich oder uneigentlich enthält.

238.

Satz. *Ist eine Form F in einer Form F' enthalten und in das Produkt der Formen f, f' transformierbar, so ist auch die Form F' in dasselbe Produkt transformierbar.*

Beweis. Behalten wir für die Formen F, f, f' dieselben Bezeichnungen wie oben bei und nehmen an, die Form F' gehe in F durch die Substitution $\alpha, \beta, \gamma, \delta$ über, so sieht man leicht, dass F' durch die Substitution

$$\begin{array}{cccc} \alpha p + \beta q, & \alpha p' + \beta q', & \alpha p'' + \beta q'', & \alpha p''' + \beta q''' \\ \gamma p + \delta q, & \gamma p' + \delta q', & \gamma p'' + \delta q'', & \gamma p''' + \delta q''' \end{array}$$

dasselbe wird wie F durch die Substitution p, p', p'', p'''; q, q', q'', q''', also F' durch jene Substitution in ff' übergeht. *Q. E. D.*

Weiter bestätigt man durch eine ähnliche Rechnung wie im vorigen Artikel leicht, dass F' in ff' ebenso wie F transformierbar ist, wenn F' die Form F eigentlich enthält; ist dagegen F uneigentlich in F' enthalten, so sind die Transformationen der Form F in ff' und der Form F' in ff' bezüglich jeder der beiden Formen f, f' entgegengesetzt: nämlich wird diejenige dieser Formen, die in eine Transformation direkt eingeht, in der anderen invers genommen.

Verbinden wir diesen Satz mit dem Satz des vorigen Artikels, so erhalten wir den folgenden allgemeineren: *Ist eine Form F in das Produkt ff' transformierbar und enthalten die Formen f, f' jeweils die Formen g, g', während die Form F in der Form G enthalten ist, so ist G in das Produkt gg' transformierbar.* Denn nach dem Satz dieses Artikels ist G in ff' transformierbar, danach nach dem Satz des vorigen Artikels in fg' und nach demselben Satz auch in gg'. Weiter ist klar: Enthalten alle drei Formen f, f', G die Formen g, g', F eigentlich, so ist G in gg' bezüglich der Formen g, g' ebenso transformierbar wie F in ff' bezüglich der Formen f, f'; dasselbe gilt, wenn alle drei Enthaltenseinsbeziehungen uneigentlich sind. Schließlich lässt sich ebenso leicht bestimmen, *wie* G in gg' transformierbar ist, wenn eine dieser Beziehungen von den beiden anderen verschieden ist.

Sind die Formen F, f, f' den Formen G, g, g' jeweils äquivalent, so haben diese dieselben Determinanten wie jene; und für die Formen f, f' sind die Zahlen m, m' dieselben wie für die Formen g, g' (Artikel 161). Daraus folgt nach dem vierten Schluss des Artikels 235 ohne Schwierigkeit, dass in diesem Fall G aus g, g' *zusammengesetzt* ist, wenn F aus f, f' zusammengesetzt ist. Dabei geht die Form g in die erste Komposition ebenso ein wie f in die zweite, wenn F der Form G ebenso äquivalent ist wie f der Form g, und umgekehrt; ebenso wird g' bei der ersten Komposition ebenso oder entgegengesetzt genommen wie f' bei der zweiten, je nachdem, ob die Äquivalenz der Formen f', g' der Äquivalenz der Formen F, G gleichartig oder verschiedenartig ist.

239.

Satz. *Ist eine Form F aus den Formen f, f' zusammengesetzt, so enthält jede andere Form, die in das Produkt ff' ebenso wie F transformierbar ist, die Form F eigentlich.*

Beweis. Behalten wir für F, f, f' alle Bezeichnungen aus Artikel 235 bei, so gelten die Gleichungen Ω auch hier. Nehmen wir an, die Form $F' = (A', B', C')$, deren Determinante $= D'$ ist, gehe in das Produkt ff' durch die Substitution $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''$; $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \mathfrak{q}'''$ über, und bezeichnen wir die Zahlen

$$\begin{gathered}\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', \quad \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', \quad \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}'''. \\ \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', \quad \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', \quad \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''\end{gathered}$$

der Reihe nach mit

$$P', Q', R', S', T', U'$$

Dann haben wir neun den Gleichungen Ω völlig entsprechende Gleichungen, nämlich

$$\begin{gathered}P' = a\mathfrak{n}', \quad R' - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}' \\ Q' = a'\mathfrak{n}, \quad R' + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n} \\ \mathfrak{q}'\mathfrak{q}'' - \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}', \\ \mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \\ \mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}'\end{gathered}$$

die wir mit Ω' bezeichnen. Die Größen $\mathfrak{n}, \mathfrak{n}'$ sind hier Quadratwurzeln aus $\frac{d}{D'}, \frac{d'}{D'}$, und zwar jeweils mit denselben Vorzeichen wie n, n'; setzen wir also die positiv genommene Quadratwurzel aus $\frac{D}{D'}$ (die eine ganze Zahl ist) $= k$, so ist $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. Daraus und aus den ersten sechs Gleichungen in Ω und Ω' folgt offenbar

$$\begin{gathered}P' = kP, \quad Q' = kQ, \quad R' = kR \\ S' = kS, \quad T' = kT, \quad U' = kU\end{gathered}$$

Also lassen sich nach dem Lemma aus Artikel 234 vier ganze Zahlen $\alpha, \beta, \gamma, \delta$ so bestimmen, dass

$$\begin{gathered}\alpha p + \beta q = \mathfrak{p}. \qquad \gamma p + \delta q = \mathfrak{q} \\ \alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}' \text{ etc.}\end{gathered}$$

und

$$\alpha\delta - \beta\gamma = k$$

gilt. Setzen wir diese Werte von $\mathfrak{p}, \mathfrak{q}, \mathfrak{p}', \mathfrak{q}'$ usw. in die letzten drei Gleichungen Ω' ein, so bestätigt man mithilfe der Gleichungen $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ und der letzten drei Gleichungen Ω leicht, dass

$$\begin{aligned}A'\alpha\alpha + 2B'\alpha\gamma + C'\gamma\gamma &= A \\ A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta &= B \\ A'\beta\beta + 2B'\beta\delta + C'\delta\delta &= C\end{aligned}$$

gilt. Daher geht die Form F' durch die Substitution $\alpha, \beta, \gamma, \delta$ (die eigentlich ist, weil $\alpha\delta - \beta\gamma = k$ positiv ist) in F über, *d.h.*, sie enthält die Form F eigentlich. *Q. E. D.*

Ist also F' ebenfalls aus den Formen f, f' zusammengesetzt (ebenso wie F aus ihnen), so haben die Formen F, F' dieselbe Determinante und sind damit eigentlich äquivalent. Allgemeiner: Ist eine Form G aus den Formen g, g' ebenso zusammengesetzt wie F aus f, f', und sind die Formen g, g' den Formen f, f' jeweils eigentlich äquivalent, so sind die Formen F, G eigentlich äquivalent.

Da der Fall, in dem beide zusammenzusetzenden Formen direkt in die Komposition eingehen, der einfachste ist und sich die übrigen leicht darauf zurückführen lassen, betrachten wir im Folgenden nur diesen. Wenn also eine Form einfach aus zwei anderen zusammengesetzt genannt wird, ist stets darunter zu verstehen, dass sie aus jeder der beiden eigentlich zusammengesetzt ist[*)]. Dieselbe Einschränkung gilt, wenn eine Form in das Produkt zweier anderer transformierbar genannt wird.

[*)] Ebenso versteht man bei der Zusammensetzung von Verhältnissen (die eine große Ähnlichkeit mit der Komposition von Formen hat) gewöhnlich, dass die zusammenzusetzenden Verhältnisse direkt zu nehmen sind, wenn nicht das Gegenteil gesagt wird.

240.

Satz. *Aus den Formen f, f' sei die Form F zusammengesetzt; aus F und f'' die Form $\mathfrak{F}$; aus f, f'' die Form F'; aus F' und f' die Form $\mathfrak{F}'$. Dann sind die Formen $\mathfrak{F}, \mathfrak{F}'$ eigentlich äquivalent.*

Beweis. I. Es sei

$$\begin{aligned} f &= axx + 2bxy + cyy \\ f' &= a'x'x' + 2b'x'y' + c'y'y' \\ f'' &= a''x''x'' + 2b''x''y'' + c''y''y'' \\ F &= AXX + 2BXY + CYY \\ F' &= A'X'X' + 2B'X'Y' + C'Y'Y' \\ \mathfrak{F} &= \mathfrak{A}\mathfrak{X}\mathfrak{X} + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}\mathfrak{Y} \\ \mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'\mathfrak{X}' + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'\mathfrak{Y}' \end{aligned}$$

Die Determinanten dieser sieben Formen seien jeweils $d, d', d'', D, D', \mathfrak{D}, \mathfrak{D}'$, die alle dasselbe Vorzeichen haben und im Verhältnis von Quadraten zueinander stehen. Weiter sei m der größte gemeinsame Teiler der Zahlen $a, 2b, c$, und m', m'', M sollen für die Formen $f', f''; F$ eine entsprechende Bedeutung haben. Dann ist nach dem vierten Schluss des Artikels 235 D der größte gemeinsame Teiler der Zahlen $dm'm', d'mm$, also $Dm''m''$ der größte gemeinsame Teiler der Zahlen $dm'm'm''m'', d'mmm''m''$; $M = mm'$; $\mathfrak{D}$ ist der größte gemeinsame Teiler der Zahlen $Dm''m''$, $d''MM$, also der Zahlen $Dm''m'', d''mmm'm'$. Daraus folgt, dass $\mathfrak{D}$ der größte gemeinsame Teiler der drei Zahlen $dm'm'm''m'', d'mmm''m'', d''mmm'm'$ ist; ebenso ist aber $\mathfrak{D}'$ der größte gemeinsame Teiler derselben drei Zahlen. Da $\mathfrak{D}, \mathfrak{D}'$ dasselbe Vorzeichen haben, ist also $\mathfrak{D} = \mathfrak{D}'$, oder die Formen $\mathfrak{F}, \mathfrak{F}'$ haben dieselbe Determinante.

II. Nun gehe F in ff' durch die Substitution

$$\begin{aligned} X &= pxx' + p'xy' + p''yx' + p'''yy' \\ Y &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned}$$

und $\mathfrak{F}$ in Ff'' durch die Substitution

$$\begin{aligned} \mathfrak{X} &= \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy'' \\ \mathfrak{Y} &= \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy'' \end{aligned}$$

über, und wir bezeichnen die positiven Quadratwurzeln aus $\frac{d}{D}, \frac{d'}{D}, \frac{D}{\mathfrak{D}}$. $\frac{d''}{\mathfrak{D}}$ mit $n, n', \mathfrak{N}, \mathfrak{n}''$. Dann erhalten wir nach Artikel 235 achtzehn Gleichungen, von denen die eine Hälfte zur Transformation der Form F in ff' gehört, die andere zur Transformation der Form $\mathfrak{F}$ in Ff''. Die erste ist $pq' - qp' = an'$; nach ihrem Muster lassen sich die übrigen leicht bilden, die wir hier der Kürze wegen weglassen. Die Größen $n, n', \mathfrak{N}, \mathfrak{n}''$ sind zwar rational, aber nicht notwendig ganze Zahlen.

III. Setzt man die Werte von X, Y in die Werte von $\mathfrak{X}, \mathfrak{Y}$ ein, so ergibt sich eine

Substitution der folgenden Art:

$$\begin{aligned}\mathfrak{X} &= (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' \\ &\quad + (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y'' \\ \mathfrak{Y} &= (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' \\ &\quad + (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y''\end{aligned}$$

durch die $\mathfrak{F}$ offenbar in das Produkt $ff'f''$ übergeht. Der Koeffizient (1) ist $= p\mathfrak{p}+q\mathfrak{p}''$; die Werte der übrigen fünfzehn geben wir nicht an, da sie jeder ohne Schwierigkeit entwickeln kann. Bezeichnen wir die Zahl $(1)(10) - (2)(9)$ mit $(1,2)$, die Zahl $(1)(11) - (3)(9)$ mit $(1,3)$ und allgemein $(g)(8+h) - (h)(8+g)$ mit (g,h), wobei g, h verschiedene ganze Zahlen zwischen 1 und 16 sind und die größere h ist[*]; auf diese Weise erhalten wir insgesamt achtundzwanzig Zeichen. Bezeichnen wir nun die positiven Quadratwurzeln aus $\frac{d}{\mathfrak{D}}, \frac{d'}{\mathfrak{D}}$ mit $\mathfrak{n}, \mathfrak{n}'$ (die $= n\mathfrak{N}, n'\mathfrak{N}$ sind), so ergeben sich die folgenden 28 Gleichungen:

$$\begin{aligned}(1,2) &= aa'\mathfrak{n}'' \\ (1,3) &= aa''\mathfrak{n}' \\ (1,4) &= ab'\mathfrak{n}'' + ab''\mathfrak{n}' \\ (1,5) &= a'a''\mathfrak{n} \\ (1,6) &= a'b\mathfrak{n}'' + a'b''\mathfrak{n} \\ (1,7) &= a''b\mathfrak{n}' + a''b'\mathfrak{n} \\ (1,8) &= bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'', \\ (2,3) &= ab''\mathfrak{n}' - ab'\mathfrak{n}'' \\ (2,4) &= ac''\mathfrak{n}' \\ (2,5) &= a'b''\mathfrak{n} - a'b\mathfrak{n}'' \\ (2,6) &= a'c''\mathfrak{n} \\ (2,7) &= bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'', \\ (2,8) &= bc''\mathfrak{n}' + b'c''\mathfrak{n} \\ (3,4) &= ac'\mathfrak{n}''\end{aligned}$$

[*] Die jetzige Bedeutung dieser Zeichen darf nicht mit der verwechselt werden, die sie in Artikel 234 hatten; denn die durch diese Zeichen *hier* ausgedrückten Zahlen entsprechen genau denen, die in Artikel 234 mit den Zahlen multipliziert wurden, die *dort* durch ähnliche Zeichen bezeichnet waren.

$$
\begin{aligned}
(3,5) &= a''b'\mathfrak{n} - a''b\mathfrak{n}' \\
(3,6) &= bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(3,7) &= a''c'\mathfrak{n} \\
(3,8) &= bc'\mathfrak{n}'' + b''c\mathfrak{n} \\
(4,5) &= b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(4,6) &= b'c''\mathfrak{n} - bc''\mathfrak{n}' \\
(4,7) &= b''c'\mathfrak{n} - bc'\mathfrak{n}'' \\
(4,8) &= c'c''\mathfrak{n} \\
(5,6) &= ca'\mathfrak{n}'' \\
(5,7) &= ca''\mathfrak{n}' \\
(5,8) &= b'c\mathfrak{n}'' + b''c\mathfrak{n}' \\
(6,7) &= b''c\mathfrak{n}' - b'c\mathfrak{n}'' \\
(6,8) &= cc''\mathfrak{n}' \\
(7,8) &= cc'\mathfrak{n}''
\end{aligned}
$$

die wir mit Φ bezeichnen werden, und neun weitere:

$$
\begin{aligned}
(10)(11) - (9)(12) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(12) - (2)(11) - (3)(10) + (4)(9) &= 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(2)(3) - (1)(4) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
-(9)(16) + (10)(15) + (11)(14) - (12)(13) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
\begin{matrix}(1)(16) - (2)(15) - (3)(14) + (4)(13)\{ \\ +(5)(12) - (6)(11) - (7)(10) + (8)(9)\}\end{matrix} &= 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
-(1)(8) + (2)(7) + (3)(6) - (4)(5) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
(14)(15) - (13)(16) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(5)(16) - (6)(15) - (7)(14) + (8)(13) &= 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(6)(7) - (5)(8) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}
\end{aligned}
$$

die wir mit Ψ bezeichnen[*)].

IV. Die Entstehung aller dieser 37 Gleichungen herzuleiten, wäre zu lang. Es genügt, einige zu bestätigen, nach deren Muster sich die übrigen ohne große Schwierigkeit beweisen lassen.

1) Es ist

$$
\begin{aligned}
(1,2) &= (1)(10) - (2)(9) \\
&= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp \\
&\quad + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' + \mathfrak{q}'\mathfrak{p}'')pq \\
&\quad + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq \\
&= \mathfrak{n}''(App + 2Bpq + Cqq) = \mathfrak{n}''aa'
\end{aligned}
$$

[*)] Man beachte, dass sich 18 weitere, diesen Ψ ähnliche Gleichungen herleiten lassen, bei denen rechts anstelle der Faktoren a, $2b$, c die Faktoren a', $2b'$, c'; a'', $2b''$, c'' stehen. Da wir sie für unseren Zweck nicht brauchen, lassen wir sie weg.

die erste Gleichung.

2) Es ergibt sich

$$\begin{aligned}(1,3) &= (1)(11) - (3)(9)\\ &= (\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'')(pq' - qp')\\ &= a''\mathfrak{N}an' = aa''\mathfrak{n}'\end{aligned}$$

die zweite Gleichung.

3) Es ist

$$\begin{aligned}(1,8) &= (1)(16) - (8)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp'''\\ &\quad + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''')pq'''\\ &\quad - (\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'')qp'''\\ &\quad + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq'''\\ &= \mathfrak{n}''(App''' + B(pq''' + qp''') + Cqq''')\\ &\quad + b''\mathfrak{N}(pq''' - qp''')\\ &= \mathfrak{n}''(bb' + \sqrt{dd'}) + b''\mathfrak{N}(b'n + bn')^{*)}\\ &= \mathfrak{n}''bb' + \mathfrak{n}'bb'' + \mathfrak{n}b'b'' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''\end{aligned}$$

die achte Gleichung in Φ. Die übrigen Gleichungen überlassen wir den Lesern zur Bestätigung.

V. Aus den Gleichungen Φ folgt auf die folgende Weise, dass die achtundzwanzig Zahlen $(1,2)$, $(1,3)$ usw. keinen gemeinsamen Teiler haben. Zuerst betrachten wir die siebenundzwanzig Produkte aus je drei Faktoren, deren erster entweder $\mathfrak{n}$, deren zweiter eine der Zahlen a', $2b'$, c' und deren dritter eine der Zahlen a'', $2b''$, c'' ist; oder deren erster $\mathfrak{n}'$, deren zweiter eine der Zahlen a, $2b$, c und deren dritter eine der Zahlen a'', $2b''$, c'' ist; oder schließlich deren erster $\mathfrak{n}''$, deren zweiter eine der Zahlen a, $2b$, c und deren dritter eine der Zahlen a', $2b'$, c' ist—jedes dieser siebenundzwanzig Produkte ist nach den Gleichungen Φ entweder einer der achtundzwanzig Zahlen $(1,2)$, $(1,3)$ usw. oder der Summe oder Differenz mehrerer davon gleich (*zum Beispiel* $\mathfrak{n}a'a'' = (1,5)$, $2\mathfrak{n}a'b'' = (1,6)+(2,5)$, $4\mathfrak{n}b'b'' = (1,8)+(2,7)+(3,6)+(4,5)$ und ebenso bei den übrigen). Hätten diese Zahlen also einen gemeinsamen Teiler, so müsste dieser auch alle jene Produkte teilen. Daraus folgt mithilfe des Artikels 40 und nach der schon öfter benutzten Methode leicht, dass derselbe Teiler auch die Zahlen $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$ teilen müsste, also deren Quadrate, nämlich $\frac{dm'm'm''m''}{\mathfrak{D}}$, $\frac{d'mmm''m''}{\mathfrak{D}}$, $\frac{d''mmm'm'}{\mathfrak{D}}$, durch sein Quadrat teilbar wären, *was widersinnig ist*, weil nach I der größte gemeinsame Teiler der drei Zähler $\mathfrak{D}$ ist und somit die Quadrate selbst keinen gemeinsamen Teiler haben können.

VI. Das alles betrifft die Transformation der Form $\mathfrak{F}$ in $ff'f''$ und wurde aus den Transformationen der Form F in ff' und der Form $\mathfrak{F}$ in Ff'' hergeleitet. Ganz ebenso ergibt sich aber aus den Transformationen der Form F' in ff'' und der Form $\mathfrak{F}'$ in

*)Das folgt aus Gleichung 10 des Artikels 235 und dem Folgenden. Die Wurzelgröße $\sqrt{dd'}$ wird $= Dnn' = \mathfrak{D}nn'\mathfrak{M}\mathfrak{M} = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

$F'f'$ eine Transformation der Form $\mathfrak{F}'$ in $ff'f''$ der folgenden Art:

$$\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \text{etc.}$$
$$\mathfrak{Y}' = (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \text{etc.}$$

(wobei wir alle Koeffizienten wie bei der Transformation der Form $\mathfrak{F}$ in $ff'f''$ bezeichnen und zur Unterscheidung jedem einen Strich anfügen). Daraus folgen wie zuvor 28 den Gleichungen Φ entsprechende Gleichungen, die wir mit Φ' bezeichnen, und neun weitere, den Gleichungen Ψ entsprechende, die wir mit Ψ' bezeichnen. Bezeichnen wir nämlich

$$(1)'(10)' - (2)'(9)' \text{ mit } (1,2)', \quad (1)'(11)' - (3)'(9)' \text{ mit } (1,3)'$$

so sind die Gleichungen Φ'

$$(1,2)' = aa'\mathfrak{n}'', \quad (1,3)' = aa''\mathfrak{n}', \quad \text{etc.}$$

und die Gleichungen Ψ'

$$(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}', \quad \text{etc.}$$

(Die ausführlichere Entwicklung überlassen wir der Kürze wegen den Lesern; Kenner werden übrigens finden, dass eine neue Rechnung nicht einmal nötig ist, sondern sich die erste Analyse durch Analogie leicht hierher übertragen lässt.) Danach folgt aus Φ und Φ' sofort

$$(1,2) = (1,2)', \quad (1,3) = (1,3)', \quad (1,4) = (1,4)', \quad (2,3) = (2,3)', \quad \text{etc.}$$

Daraus und weil alle $(1,2)$, $(1,3)$, $(2,3)$ usw. nach V keinen gemeinsamen Teiler haben, folgt mithilfe des Lemmas aus Artikel 234, dass sich vier ganze Zahlen α, β, γ, δ so bestimmen lassen, dass

$$\begin{aligned}
\alpha(1)' + \beta(9)' &= (1),\\
\alpha(2)' + \beta(10)' &= (2),\\
\alpha(3)' + \beta(11)' &= (3), \quad \text{etc.}\\
\gamma(1)' + \delta(9)' &= (9),\\
\gamma(2)' + \delta(10)' &= (10),\\
\gamma(3)' + \delta(11)' &= (11), \quad \text{etc.}
\end{aligned}$$

und $\alpha\delta - \beta\gamma = 1$ gilt.

VII. Daraus bestätigt man leicht, indem man aus den ersten drei Gleichungen Ψ die Werte von $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$ und aus den ersten drei Gleichungen Ψ' die Werte von $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$ einsetzt, dass

$$\begin{aligned}
a(\mathfrak{A}\alpha\alpha + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma\gamma) &= a\mathfrak{A}'\\
a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}'\\
a(\mathfrak{A}\beta\beta + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta\delta) &= a\mathfrak{C}'
\end{aligned}$$

gilt. Wenn nicht $a = 0$ ist, folgt offenbar, dass die Form $\mathfrak{F}$ in $\mathfrak{F}'$ durch die eigentliche Substitution α, β, γ, δ übergeht. — Nimmt man aber anstelle der ersten drei Gleichungen in Ψ und Ψ' die nächsten drei, so bestätigt man leicht drei den eben angegebenen völlig entsprechende Gleichungen, in denen anstelle des Faktors a überall b steht. Daraus sieht man, dass derselbe Schluss weiterhin gilt, sofern nicht $b = 0$ ist. Nimmt man schließlich die letzten drei Gleichungen Ψ, Ψ', so findet man ebenso, dass der Schluss gilt, wenn nicht $c = 0$ ist. Da aber sicher nicht alle a, b, c zugleich $= 0$ sein können, geht notwendig die Form $\mathfrak{F}$ durch die Substitution α, β, γ, δ in $\mathfrak{F}'$ über und ist ihr damit eigentlich äquivalent. *Q. E. D.*

241.

Eine Form wie $\mathfrak{F}$ oder $\mathfrak{F}'$, die entsteht, indem eine von drei gegebenen Formen mit der aus den beiden übrigen zusammengesetzten Form zusammengesetzt wird, nennen wir *aus diesen drei Formen zusammengesetzt*. Nach dem vorigen Artikel kommt es dabei nicht darauf an, in welcher Reihenfolge die drei Formen zusammengesetzt werden. Ebenso: Sind beliebig viele Formen f, f', f'', f''' usw. gegeben (deren Determinanten im Verhältnis von Quadraten zueinander stehen müssen), und setzt man die Form f mit f', die resultierende mit f'', die daraus entstehende mit f''' usw. zusammen, so heißt die am Ende dieser Operation entstehende Form *aus allen Formen* f, f', f'', f''' usw. zusammengesetzt. Man beweist leicht, dass auch hier die Reihenfolge beliebig ist; *d.h.*, in welcher Reihenfolge man die Formen auch zusammensetzt, die daraus entstehenden Formen sind stets eigentlich äquivalent. — Weiter ist offenbar: Sind den Formen f, f', f'' usw. jeweils die Formen g, g', g'' usw. eigentlich äquivalent, so ist die aus diesen zusammengesetzte Form der aus jenen zusammengesetzten Form eigentlich äquivalent.

242.

Die vorigen Sätze erfassen die Komposition der Formen in ihrer vollen Allgemeinheit. Wir gehen nun zu besonderen Anwendungen über, durch die wir ihre Reihenfolge nicht unterbrechen wollten. Zuerst greifen wir das Problem des Artikels 236 wieder auf und schränken es durch die folgenden Bedingungen ein: *erstens*, die zusammenzusetzenden Formen haben dieselbe Determinante, also $d = d'$; *zweitens*, m. m' sind teilerfremd; *drittens*, die gesuchte Form ist aus jeder der beiden Formen f, f' direkt zusammengesetzt. Dann sind auch mm, $m'm'$ teilerfremd; somit wird der größte gemeinsame Teiler von $dm'm'$, $d'mm$, *das heißt,* D, $= d = d'$, und $n = n' = 1$. Die vier Größen $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, die beliebig gewählt werden können, setzen wir jeweils gleich $= -1, 0, 0, 0$. Das ist stets erlaubt, außer in dem einzigen Fall, dass a, a', $b+b'$ zugleich $= 0$ sind, den wir deshalb hier beiseitelassen. Dieser Fall kann offenbar nur bei Formen auftreten, deren Determinante ein positives Quadrat ist. Dann wird μ offenbar zum größten gemeinsamen Teiler von a, a', $b + b'$; die Zahlen $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ müssen so gewählt werden, dass

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$$

während $\mathfrak{P}$ selbst völlig beliebig ist. Setzt man an der angeführten Stelle für p, q, p', q' usw. ihre Werte ein, so ergibt sich

$$A = \frac{aa'}{\mu\mu},$$
$$B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

und C kann durch die Gleichung $AC = BB - D$ bestimmt werden, sofern nicht a null ist und zugleich $a' = 0$ gilt.

Bei dieser Lösung hängt also der Wert von A nicht von den Werten der Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ ab (die auf unendlich viele verschiedene Arten bestimmt werden können). Dagegen nimmt B andere Werte an, wenn man diesen Zahlen andere Werte gibt, und es lohnt sich zu untersuchen, wie alle Werte von B miteinander zusammenhängen. Dazu bemerken wir:

I. Wie auch $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ bestimmt werden, die daraus entstehenden Werte von B sind sämtlich modulo A kongruent. Wir nehmen Folgendes an. Die Festsetzung

$$\mathfrak{P} = \mathfrak{p},$$
$$\mathfrak{P}' = \mathfrak{p}',$$
$$\mathfrak{P}'' = \mathfrak{p}'',$$
$$\mathfrak{P}''' = \mathfrak{p}''',$$
ergibt $B = \mathfrak{B}$

und die Festsetzung

$$\mathfrak{P} = \mathfrak{p} + \mathfrak{d},$$
$$\mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}',$$
$$\mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}''.$$
$$\mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}''',$$
$$\text{ergibt } B = \mathfrak{B} + \mathfrak{D}$$

Dann gilt also

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0,$$
$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \mu\mathfrak{D}$$

Multipliziert man die erste Seite der letzteren Gleichung mit $a\mathfrak{p}' + a'\mathfrak{p}'' + (b+b')\mathfrak{p}'''$, die zweite mit μ, und zieht man vom ersten Produkt die Größe

$$(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (bb' + D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''')$$

ab, die wegen der ersten Gleichung offenbar $= 0$ ist, so erhält man nach dem Ausmultiplizieren und Wegheben der sich aufhebenden Glieder

$$\begin{aligned} aa'(&\mu\mathfrak{d} \\ &+ ((b'-b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' \\ &+ ((b-b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' \\ &- (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}''') = \mu\mu\mathfrak{D} \end{aligned}$$

Damit ist offenbar $\mu\mu\mathfrak{D}$ durch aa', oder $\mathfrak{D}$ durch $\frac{aa'}{\mu\mu}$, *das heißt,* durch A teilbar, und

$$\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D} \text{ (mod. } A)$$

II. Wenn die Werte $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ $\mathfrak{p}'''$ der Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ den Wert $B = \mathfrak{B}$ ergeben, so lassen sich andere Werte dieser Zahlen finden, durch die B jeden vorgegebenen, zu $\mathfrak{B}$ modulo A kongruenten Wert erhält, etwa $\mathfrak{B} + kA$. Zuerst bemerken wir, dass die vier Zahlen μ, c, c', $b - b'$ keinen gemeinsamen Teiler haben können. Denn hätten sie einen, so würde er die sechs Zahlen a, a', $b + b'$, c, c', $b - b'$ teilen, also sowohl a, $2b$, c als auch a', $2b'$, c' und deshalb auch m, m', die nach Voraussetzung teilerfremd sind. Somit lassen sich vier ganze Zahlen h, h', h'', h''' so angeben, dass

$$h\mu + h'c + h''c' + h'''(b - b') = 1$$

Setzt man dann

$$kh = \mathfrak{d},$$
$$k(h''(b+b') - h'''a') = \mu\mathfrak{d}'$$
$$k(h'(b+b') + h'''a) = \mu\mathfrak{d}'',$$
$$-k(h'a' + h''a) = \mu\mathfrak{d}'''$$

so sind $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$, $\mathfrak{d}'''$ offenbar ganzzahlig. Ferner bestätigt man leicht, dass

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0$$

$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}'''$$
$$= \frac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b - b')h''')$$
$$= \mu kA$$

Aus der ersten Gleichung folgt, dass auch $\mathfrak{p} + \mathfrak{d}$, $\mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{p}''' + \mathfrak{d}'''$ Werte der Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ sind; aus der zweiten, dass diese Werte $B = \mathfrak{B} + kA$ ergeben. *Q. E. D.* — Daraus ist klar, dass B stets so bestimmt werden kann, dass es einschließlich der Grenzen zwischen 0 und $A - 1$ liegt, wenn A positiv ist, oder zwischen 0 und $-A - 1$, wenn A negativ ist.

243.

Aus den Gleichungen

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu,$$
$$B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

folgt

$$B = b + \frac{a}{\mu}(\mathfrak{P}a' + \mathfrak{P}'(b' - b) - \mathfrak{P}'''c)$$
$$= b' + \frac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b - b') - \mathfrak{P}'''c')$$

also

$$B \equiv b \text{ (mod. } \tfrac{a}{\mu}) \quad \text{und} \quad B \equiv b' \text{ (mod. } \tfrac{a'}{\mu})$$

Sind $\frac{a}{\mu}$, $\frac{a'}{\mu}$ teilerfremd, so liegt zwischen 0 und $A - 1$ (oder zwischen 0 und $-A - 1$, wenn A negativ ist) nur eine einzige Zahl, die modulo $\frac{a}{\mu} \equiv b$ und $\equiv b'$ modulo $\frac{a'}{\mu}$ ist. Setzt man diese Zahl $= B$ und $\frac{BB-D}{A} = C$, so ist offenbar (A, B, C) aus den Formen (a, b, c), (a', b', c') zusammengesetzt. In diesem Fall braucht man also zur Bestimmung der zusammengesetzten Form die Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ nicht mehr zu berücksichtigen[*]. Sucht man *zum Beispiel* eine aus den Formen $(10, 3, 11)$, $(15, 2, 7)$ zusammengesetzte Form, so sind a, a', $b + b'$ jeweils $= 10, 15, 5$; $\mu = 5$; also $A = 6$; $B \equiv 3$ (mod. 2) und $\equiv 2$ (mod. 3), woraus $B = 5$ und $(6, 5, 21)$ als gesuchte Form folgen. — Die Bedingung, dass $\frac{a}{\mu}$, $\frac{a'}{\mu}$ teilerfremd sind, ist genau dazu gleichwertig, dass die beiden Zahlen a, a' keinen größeren gemeinsamen Teiler haben als die drei a, a', $b + b'$; oder, was auf dasselbe hinausläuft, dass der größte gemeinsame Teiler von a, a' auch die Zahl $b + b'$ teilt. Besonders seien die folgenden Fälle beachtet:

1) Es seien zwei Formen (a, b, c), (a', b', c') derselben Determinante D gegeben, sodass der größte gemeinsame Teiler von a, $2b$, c zum größten gemeinsamen Teiler von a', $2b'$, c' teilerfremd ist und a zu a' teilerfremd ist. Die aus ihnen zusammengesetzte

[*] Das erreicht man stets mithilfe der Kongruenzen

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b + b')B}{\mu} \equiv \frac{bb' + D}{\mu} \text{ (mod. } A)$$

Form (A, B, C) findet man, indem man $A = aa'$, $B \equiv b \pmod{a}$ und $\equiv b' \pmod{a'}$, $C = \frac{BB-D}{A}$ setzt. Dieser Fall liegt stets vor, wenn eine der zusammenzusetzenden Formen die Hauptform ist, etwa $a = 1$, $b = 0$, $c = -D$. Dann gilt $A = a'$, und B kann $= b'$ gesetzt werden, woraus $C = c'$ folgt; also *ist die aus der Hauptform und irgendeiner anderen Form derselben Determinante zusammengesetzte Form diese andere Form selbst.*

2) Sollen zwei *entgegengesetzte*, eigentlich primitive Formen, etwa (a, b, c) und $(a, -b, c)$, zusammengesetzt werden, so ist $\mu = a$. Daraus erkennt man leicht, dass die Hauptform $(1, 0, -D)$ aus ihnen zusammengesetzt ist.

3) Es seien beliebig viele eigentlich primitive Formen (a, b, c), (a', b', c'), (a'', b'', c'') usw. derselben Determinante D gegeben, deren erste Koeffizienten a, a', a'' usw. paarweise teilerfremd sind. Die aus ihnen allen zusammengesetzte Form (A, B, C) wird gefunden. Dazu setzt man A gleich dem Produkt aller a, a', a'' usw.; B kongruent zu b, b', b'' usw. jeweils modulo a, a', a'' usw.; $C = \frac{BB-D}{A}$. Denn man erkennt leicht, dass aus den beiden Formen (a, b, c), (a', b', c') die Form $(aa', B, \frac{BB-D}{aa'})$ zusammengesetzt ist; aus dieser und (a'', b'', c'') die Form $(aa'a'', B, \frac{BB-D}{aa'a''})$ usw. — Umgekehrt:

4) Ist eine eigentlich primitive Form (A, B, C) der Determinante D gegeben, zerlegt man den Koeffizienten A in beliebig viele paarweise teilerfremde Faktoren a, a', a'' usw., wählt Zahlen b, b', b'' usw. gleich B oder wenigstens dazu kongruent jeweils modulo a, a', a'' usw. und setzt $ac = bb - D$, $a'c' = b'b' - D$, $a''c'' = b''b'' - D$ usw., so ist die Form (A, B, C) aus den Formen (a, b, c), $(a'\ b'\ c')$, $(a''\ b''\ c'')$ zusammengesetzt oder *in diese Formen zerlegbar*. Ohne Mühe beweist man, dass derselbe Satz weiterhin gilt, selbst wenn die Form (A, B, C) uneigentlich primitiv oder abgeleitet ist. Auf diese Weise lässt sich also jede Form in andere derselben Determinante zerlegen, deren erste Koeffizienten sämtlich Primzahlen oder Primzahlpotenzen sind. Eine solche Zerlegung kann oft nützlich angewendet werden, wenn aus mehreren gegebenen Formen eine zusammengesetzt werden soll. Sucht man *zum Beispiel* die aus den Formen $(3, 1, 134)$, $(10, 3, 41)$, $(15, 2, 27)$ zusammengesetzte Form, so zerlege man die zweite in $(2, 1, 201)$, $(5, -2, 81)$, die dritte in $(3, -1, 134)$, $(5, 2, 81)$. Offenbar ist die aus den fünf Formen $(3, 1, 134)$, $(2, 1, 201)$, $(5, -2, 81)$, $(3, -1, 134)$, $(5, 2, 81)$ zusammengesetzte Form, in welcher Reihenfolge sie auch genommen werden, auch aus den drei gegebenen Formen zusammengesetzt. Durch Komposition der ersten mit der vierten entsteht aber die Hauptform $(1, 0, 401)$; dieselbe entsteht durch Komposition der dritten mit der fünften; somit ergibt die Komposition aller Formen die Form $(2, 1, 201)$.

5) Wegen des Nutzens dieser Methode lohnt es sich, sie noch weiter zu erläutern. Aus der vorigen Bemerkung ist klar, dass sich das Problem, beliebig viele gegebene eigentlich primitive Formen derselben Determinante zusammenzusetzen, auf die Komposition von Formen zurückführen lässt, deren erste Koeffizienten Primzahlpotenzen sind (denn eine Primzahl kann als die erste Potenz ihrer selbst betrachtet werden). Deshalb ist vor allem der Fall zu betrachten, dass zwei eigentlich primitive Formen (a, b, c), (a', b', c') zusammengesetzt werden sollen, bei denen a und a' Potenzen *derselben* Primzahl sind. Es sei also $a = h^{\varkappa}$, $a' = h^{\lambda}$, wobei h eine Primzahl bezeichnet, und wir nehmen an, was erlaubt ist, dass $\varkappa$ nicht kleiner als λ ist. Dann ist h^{λ} der größte gemeinsame Teiler von a, a'. Teilt dieser außerdem $b + b'$, so

liegt der zu Beginn dieses Artikels betrachtete Fall vor, und (A, B, C) ist aus den gegebenen Formen zusammengesetzt, wenn man $A = h^{\varkappa-\lambda}$, $B \equiv b \pmod{h^{\varkappa-\lambda}}$ und $\equiv b' \pmod 1$ setzt, wobei die letztere Bedingung offenbar weggelassen werden kann; $C = \frac{BB-D}{A}$. Teilt dagegen h^λ die Zahl $b + b'$ nicht, so muss der größte gemeinsame Teiler dieser Zahlen selbst eine Potenz von h sein. Er sei also $= h^\nu$, dann ist $\nu < \lambda$ (man muss $\nu = 0$ setzen. wenn etwa h^λ und $b + b'$ teilerfremd sind). Bestimmt man also $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ so, dass

$$\mathfrak{P}'h^\varkappa + \mathfrak{P}''h^\lambda + \mathfrak{P}'''(b + b') = h^\nu$$

wählt aber $\mathfrak{P}$ beliebig, so ist die Form (A, B, C) aus den gegebenen Formen zusammengesetzt, wenn man

$$A = h^{\varkappa+\lambda-2\nu},$$
$$B = b + h^{\varkappa-\nu}(\mathfrak{P}h^\lambda - \mathfrak{P}'(b - b') - \mathfrak{P}'''c),$$
$$C = \frac{BB - D}{A}$$

setzt. Man erkennt aber leicht, dass in diesem Fall auch $\mathfrak{P}'$ beliebig gewählt werden kann. Setzt man daher $\mathfrak{P} = \mathfrak{P}' = 0$, so wird

$$B = b - \mathfrak{P}'''ch^{\varkappa-\nu}$$

oder allgemein

$$B = kA + b - \mathfrak{P}'''ch^{\varkappa-\nu}$$

wobei k eine beliebige Zahl bezeichnet (voriger Artikel). In diese sehr einfache Formel geht allein $\mathfrak{P}'''$ ein; es ist ein Wert des Ausdrucks $\frac{h^\nu}{b+b'} \pmod{h^\lambda}$[*]. Sucht man *zum Beispiel* die aus $(16, 3, 19)$ und $(8, 1, 37)$ zusammengesetzte Form, so ist $h = 2$, $\varkappa = 4$, $\lambda = 3$, $\nu = 2$. Also ist $A = 8$, und $\mathfrak{P}'''$ ein Wert des Ausdrucks $\frac{4}{4} \pmod 8$, etwa 1, woraus $B = 8k - 73$ folgt. Setzt man also $k = 9$, so ist $B = -1$ und $C = 37$, oder $(8, -1, 37)$ die gesuchte Form.

Sind also beliebig viele Formen gegeben, deren erste Koeffizienten sämtlich Primzahlpotenzen sind, so muss man nachsehen, ob die ersten Koeffizienten einiger Formen Potenzen *derselben* Primzahl sind, und diese jeweils nach der eben gegebenen Regel miteinander zusammensetzen. So entstehen Formen, deren erste Koeffizienten weiterhin Primzahlpotenzen sind, aber Potenzen durchweg verschiedener Primzahlen; die aus ihnen zusammengesetzte Form kann daher nach der dritten Bemerkung bestimmt werden. *Zum Beispiel:* Sind die Formen $(3, 1, 47)$, $(4, 0, 35)$, $(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$, $(16, 6, 11)$ gegeben, so entsteht aus der ersten und fünften die Form $(27, 7, 7)$; aus der zweiten und vierten entsteht $(16, -6, 11)$, aus dieser und der sechsten $(1, 0, 140)$, die weggelassen werden kann. Es bleiben also $(5, 0, 28)$, $(27, 7, 7)$, aus denen $(135, -20, 4)$ entsteht; stattdessen kann man die eigentlich äquivalente Form $(4, 0, 35)$ nehmen. Diese ist also das Ergebnis der Komposition der sechs gegebenen Formen.

[*] oder des Ausdrucks $\frac{1}{\frac{b+b'}{h^\nu}} \pmod{h^{\lambda-\nu}}$, woraus $B \equiv b - \frac{ch^{\varkappa-\nu}}{\frac{b+b'}{h^\nu}} \equiv \frac{(D+bb'):h^\nu}{(b+b'):h^\nu} \pmod A$ folgt

Aus dieser Quelle lassen sich noch andere in der Anwendung nützliche Verfahren schöpfen. Doch um nicht zu weit auszuholen, lassen wir eine ausführlichere Behandlung weg und eilen zu anderen, schwierigeren Dingen.

244.

Wenn durch eine Form f die Zahl a, durch eine Form f' die Zahl a' dargestellt werden kann und die Form F in ff' transformierbar ist, so erkennt man ohne Mühe, dass das Produkt aa' durch die Form F darstellbar ist. Daraus folgt sofort: Sind die Determinanten dieser Formen negativ, so ist die Form F positiv, wenn f, f' entweder beide positiv oder beide negativ sind; dagegen wird F negativ, wenn eine der Formen f, f' positiv und die andere negativ ist. Betrachten wir besonders den Fall des vorigen Artikels, in dem F aus f, f' zusammengesetzt ist. Außerdem haben f, f' und F dieselbe Determinante D. Wir nehmen außerdem an, dass die Zahlen a, a' durch die Formen f, f' mit teilerfremden Werten der Unbestimmten dargestellt werden und die erste Darstellung zum Wert b des Ausdrucks $\sqrt{D}$ (mod. a), die zweite zum Wert b' des Ausdrucks $\sqrt{D}$ (mod. a') gehört, und setzen $bb - D = ac$, $b'b' - D = a'c'$. Dann sind nach Artikel 168 die Formen (a, b, c), (a', b', c') den Formen f, f' eigentlich äquivalent; somit ist F auch aus diesen beiden Formen zusammengesetzt. Aus denselben Formen ist aber die Form (A, B, C) zusammengesetzt, wenn man den größten gemeinsamen Teiler von a, a', $b + b'$ mit $= \mu$ bezeichnet und $A = \frac{aa'}{\mu\mu}$, $B \equiv b$ und b' jeweils modulo $\frac{a}{\mu}$, $\frac{a'}{\mu}$. setzt, $AC = BB - D$; somit ist diese Form der Form F eigentlich äquivalent. Durch die Form $Axx + 2Bxy + Cyy$ wird nun die Zahl aa' dargestellt, indem man $x = \mu$, $y = 0$ setzt; der größte gemeinsame Teiler dieser Werte ist μ. Also kann aa' auch durch die Form F so dargestellt werden, dass die Werte der Unbestimmten den größten gemeinsamen Teiler μ haben (Artikel 166). Gilt also $\mu = 1$, so kann aa' durch die Form F dargestellt werden, indem man den Unbestimmten teilerfremde Werte gibt, und diese Darstellung gehört zu dem Wert B des Ausdrucks $\sqrt{D}$ (modulo aa'), der zu b, b' jeweils modulo a, a' kongruent ist. Die Bedingung $\mu = 1$ gilt stets, wenn a, a' teilerfremd sind; allgemeiner, wenn der größte gemeinsame Teiler von a, a' zu $b + b'$ teilerfremd ist.

Komposition der Ordnungen.

245.

Satz. *Gehört die Form f zu derselben Ordnung wie g und ebenso f' zu derselben Ordnung wie g', so hat die Form F, die aus f, f' zusammengesetzt ist, dieselbe Determinante und gehört zu derselben Ordnung wie die Form G, die aus g, g' zusammengesetzt ist.*

Beweis. Die Formen seien jeweils $f, f', F = (a, b, c)$, (a', b', c'), (A, B, C) und ihre Determinanten $= d, d', D$. Ferner sei der größte gemeinsame Teiler von $a, 2b, c = m$, der größte gemeinsame Teiler von $a, b, c = \mathfrak{m}$; m', $\mathfrak{m}'$ sollen eine entsprechende Bedeutung für die Form f' haben und M, $\mathfrak{M}$ für die Form F. Dann wird die Ordnung der Form f durch die Zahlen $d, m, \mathfrak{m}$ bestimmt; daher gelten dieselben Zahlen auch für die Form g. Ebenso sind die Zahlen $d', m', \mathfrak{m}'$ für die Form g' dieselben wie für die Form f'. Nach Artikel 235 werden nun die Zahlen $D, M, \mathfrak{M}$ durch $d, d', m, m', \mathfrak{m}, \mathfrak{m}'$ bestimmt: D ist nämlich der größte gemeinsame Teiler von $dm'm'$, $d'mm$; $M = mm'$; und $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (wenn zugleich $m = \mathfrak{m}$, $m' = \mathfrak{m}'$) oder $= 2\mathfrak{m}\mathfrak{m}'$ (wenn $m = 2\mathfrak{m}$ oder $m' = 2\mathfrak{m}'$). Diese Eigenschaften von $D, M, \mathfrak{M}$ folgen daraus, dass F aus f, f'

zusammengesetzt ist; daher erkennt man leicht, dass D, M und $\mathfrak{M}$ auch für die Form G gelten und somit G zu derselben Ordnung wie F gehört. *Q. E. D.*

Aus diesem Grund nennen wir die Ordnung, zu der die Form F gehört, zusammengesetzt aus den Ordnungen, zu denen die Formen f, f' gehören. So entsteht *zum Beispiel* aus zwei eigentlich primitiven Ordnungen stets eine ebensolche Ordnung; aus einer eigentlich primitiven und einer uneigentlich primitiven eine uneigentlich primitive. — Ebenso ist es zu verstehen, wenn eine Ordnung aus mehreren anderen Ordnungen zusammengesetzt genannt wird.

Komposition der Geschlechter.

246.

Problem. *Es seien zwei beliebige primitive Formen f, f' gegeben, durch deren Komposition F entsteht. Aus den Geschlechtern, zu denen f, f' gehören, ist das Geschlecht zu bestimmen, zu dem F gehört.*

Lösung. I. Wir betrachten zuerst den Fall, dass mindestens eine der Formen f, f', etwa die erste, eigentlich primitiv ist, und bezeichnen die Determinanten der Formen f, f', F mit d, d', D. Dann ist D der größte gemeinsame Teiler von $dm'm'$, d', wobei m' entweder 1 oder 2 ist, je nachdem, ob die Form f' eigentlich oder uneigentlich primitiv ist; F gehört im ersten Fall zur eigentlich primitiven, im zweiten zur uneigentlich primitiven Ordnung. Das Geschlecht der Form F wird durch ihre Einzelcharaktere bestimmt, und zwar sowohl bezüglich der einzelnen ungeraden Primteiler von D als auch, in bestimmten Fällen, bezüglich der Zahlen 4 oder 8. Diese sind also einzeln zu bestimmen.

1°. Ist p irgendein ungerader Primteiler von D, so teilt diese Zahl notwendig auch d, d'; daher kommen unter den Charakteren der Formen f, f' auch ihre Beziehungen zu p vor. Kann nun f die Zahl a und f' die Zahl a' darstellen, so kann das Produkt aa' durch F dargestellt werden. Können also sowohl f als auch f' quadratische Reste modulo p darstellen (die nicht durch p teilbar sind), so kann auch F quadratische Reste modulo p darstellen; *das heißt,* haben beide f, f' den Charakter Rp, so hat die Form F denselben Charakter. Ebenso hat F den Charakter Rp, wenn beide f, f' den Charakter Np haben; dagegen hat F den Charakter Np, wenn eine der Formen f, f' den Charakter Rp, die andere Np hat.

2°. Geht in den Gesamtcharakter der Form F eine Beziehung zur Zahl 4 ein, so muss eine solche Beziehung auch in die Charaktere der Formen f, f' eingehen. Denn das tritt nur ein, wenn D entweder $\equiv 0$ oder $\equiv 3$ (modulo 4) ist. Ist D durch 4 teilbar, so sind auch $dm'm'$ und d' durch 4 teilbar; daraus folgt sofort, dass f' nicht uneigentlich primitiv sein kann, also $m' = 1$. Somit sind sowohl d als auch d' durch 4 teilbar, und in den Charakter beider geht eine Beziehung zu 4 ein. Gilt $D \equiv 3$ (modulo 4), so teilt D die Zahlen d, d'; die Quotienten sind Quadrate, also sind auch d, d' notwendig entweder $\equiv 0$ oder $\equiv 3$ (modulo 4), und unter den Charakteren von f, f' kommt eine Beziehung zu 4 vor. Wie in (1°) folgt daraus, dass die Form F den Charakter $1, 4$ hat, wenn entweder beide f, f' den Charakter $1, 4$ oder beide $3, 4$ haben; dagegen hat die Form F den Charakter $3, 4$, wenn eine der Formen f, f' den Charakter $1, 4$, die andere $3, 4$ hat.

3°. Ist D durch 8 teilbar, so auch d'; daher ist f' sicher eigentlich primitiv, $m' = 1$, und auch d ist durch 8 teilbar. Somit kann unter den Charakteren der Form F einer der Charaktere $1, 8$; $3, 8$; $5, 8$; $7, 8$ nur dann vorkommen, wenn sowohl im Charakter der Form f als auch in dem der Form f' eine solche Beziehung zu 8 vorhanden ist. Wie zuvor bestätigt man leicht, dass die Form F den Charakter $1, 8$ hat, wenn f und f' bezüglich 8 denselben Charakter haben; die Form F hat den Charakter $3, 8$, wenn eine der Formen f, f' den Charakter $1, 8$, die andere $3, 8$ hat oder eine $5, 8$, die andere $7, 8$; F hat $5, 8$, wenn f, f' die Charaktere $1, 8$ und $5, 8$ oder $3, 8$ und $7, 8$ haben; F hat $.7, 8$, wenn f und f' entweder $1, 8$ und $7, 8$ oder $3, 8$ und $5, 8$ haben.

4°. Gilt $D \equiv 2$ (modulo 8), so ist d' entweder $\equiv 0$ oder $\equiv 2$ (modulo 8), also $m' = 1$ und somit auch d entweder $\equiv 0$ oder $\equiv 2$ (modulo 8). Allerdings können nicht beide d, d' durch 8 teilbar sein, da D ihr *größter* gemeinsamer Teiler ist. Daher kann einer der Charaktere 1 *und* $7, 8$; 3 *und* $5, 8$ der Form F nur dann zukommen, wenn entweder beide Formen f, f' einen davon haben oder eine einen davon und die andere einen der Charaktere $1, 8$; $3, 8$; $5, 8$; $7, 8$. Daraus folgt leicht, dass der Charakter der Form F durch die folgende Tabelle bestimmt wird, wenn der Charakter am Rand zu einer der Formen f, f' gehört, der oben stehende Charakter zur anderen:

	1 *und* $7, 8$ oder $1, 8$ oder $7, 8$	3 *und* $5, 8$ oder $3, 8$ oder $5, 8$
1 *und* $7, 8$	1 *und* $7, 8$	3 *und* $5, 8$
3 *und* $5, 8$	3 *und* $5, 8$	1 *und* 7.8

5°. Ebenso beweist man, dass der Form F keiner der Charaktere 1 *und* $3, 8$; 5 *und* $7, 8$ zukommen kann, wenn nicht auch mindestens eine der Formen f, f' einen davon hat und die andere entweder einen davon oder einen der Charaktere $1, 8$; $3, 8$; $5, 8$; $7, 8$. Dabei wird der Charakter der Form F durch diese Tabelle bestimmt, an deren Rand und oben die Charaktere der Formen f, f' stehen:

	1 *und* $3, 8$ oder $1, 8$ oder $3, 8$	5 *und* $7, 8$ oder $5, 8$ oder $7, 8$
1 *und* $3, 8$	1 *und* $3, 8$	5 *und* $7, 8$
5 *und* $7, 8$	5 *und* $7, 8$	1 *und* 3.8

II. Sind beide Formen f, f' uneigentlich primitiv, so ist D der größte gemeinsame Teiler von $4d$. $4d'$, oder $\frac{1}{4}D$ der größte gemeinsame Teiler von d. d'. Daraus folgt leicht, dass sowohl d als auch d' und $\frac{1}{4}D$ jeweils $\equiv 1$ (modulo 4) sind. Setzt man $F = (A, B, C)$, so ist der größte gemeinsame Teiler von $A, B, C = 2$. und der größte gemeinsame Teiler von $A, 2B, C$ gleich 4. Daher ist F eine von der uneigentlich primitiven Form $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$ abgeleitete Form; deren Determinante ist $\frac{1}{4}D$, und ihr Geschlecht bestimmt das Geschlecht der Form F. Da jene Form uneigentlich primitiv ist, enthält ihr Charakter keine Beziehungen zu 4 oder 8, sondern nur zu den einzelnen ungeraden Primteilern von $\frac{1}{4}D$. Alle diese Teiler teilen nun offenbar auch d, d', und die Hälfte jedes Produkts zweier Faktoren. deren einer durch f, der andere durch f' darstellbar ist, kann durch die Form $(\frac{1}{2}A.\ \frac{1}{2}B, \frac{1}{2}C)$ dargestellt werden. Daher erkennt man leicht, dass der Charakter dieser Form bezüglich jeder ungeraden Primzahl p, die $\frac{1}{4}D$ teilt, gleich Rp ist, *sowohl* wenn $2Rp$ gilt und die Formen f, f' bezüglich p denselben Charakter haben. *als auch* wenn $2Np$ gilt und die Charaktere der Formen f, f' bezüglich p entgegengesetzt sind; dagegen ist der Charakter jener Form Np, *sowohl* wenn f, f' bezüglich p gleiche Charaktere haben und $2Np$ gilt, *als auch* wenn f, f' entgegengesetzte Charaktere haben und $2Rp$ gilt.

247.

Aus der Lösung des vorigen Problems ist klar: Ist g eine primitive Form derselben Ordnung und desselben Geschlechts wie f und ebenso g' eine primitive Form derselben Ordnung und desselben Geschlechts wie f', so gehört die aus g und g' zusammengesetzte Form zu demselben Geschlecht wie die aus f und f' zusammengesetzte. Daraus ergibt sich die Bedeutung eines *Geschlechts*, das aus zwei anderen Geschlechtern (oder auch mehreren) *zusammengesetzt* ist. Ferner folgt daraus: Haben f, f' dieselbe Determinante, ist f eine Form aus dem Hauptgeschlecht und F aus f und f' zusammengesetzt, so gehört F zu demselben Geschlecht wie f'; daher kann das Hauptgeschlecht bei der Komposition mit anderen Geschlechtern derselben Determinante stets weggelassen werden. Gehört dagegen bei sonst gleichen Bedingungen f nicht zum Hauptgeschlecht, während f' eine primitive Form ist, so gehört F sicher zu einem anderen Geschlecht als f'. Sind schließlich f, f' eigentlich primitive Formen desselben Geschlechts, so gehört F zum Hauptgeschlecht; sind dagegen f, f' beide eigentlich primitiv und von derselben Determinante, gehören aber zu verschiedenen Geschlechtern, so kann F nicht zum Hauptgeschlecht gehören. Wird also irgendeine eigentlich primitive Form *mit sich selbst* zusammengesetzt, so gehört die entstehende Form, die ebenfalls eigentlich primitiv und von derselben Determinante ist, notwendig zum Hauptgeschlecht.

248.

Problem. *Es seien zwei beliebige Formen f, f' gegeben, aus denen F zusammengesetzt ist. Aus den Geschlechtern der Formen f, f' ist das Geschlecht der Form F zu bestimmen.*

Lösung. Es sei $f = (a, b, c)$, $f' = (a', b', c')$, $F = (A, B, C)$, ferner $\mathfrak{m}$ der größte gemeinsame Teiler von a, b, c und $\mathfrak{m}'$ der größte gemeinsame Teiler von a', b', c', sodass f, f' von den primitiven Formen $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$, $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$ abgeleitet sind, die wir jeweils mit $\mathfrak{f}$, $\mathfrak{f}'$ bezeichnen. Ist nun mindestens eine der Formen $\mathfrak{f}$, $\mathfrak{f}'$ eigentlich primitiv, so ist der größte gemeinsame Teiler von A, B, C gleich $\mathfrak{m}\mathfrak{m}'$ und daher F von der primitiven Form $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}) \ldots \mathfrak{F}$ abgeleitet; somit hängt das Geschlecht der Form F vom Geschlecht der Form $\mathfrak{F}$ ab. Man erkennt aber leicht, dass $\mathfrak{F}$ durch dieselbe Substitution in $\mathfrak{f}\mathfrak{f}'$ übergeht, durch die F in ff' übergeht. Also ist $\mathfrak{F}$ aus $\mathfrak{f}$, $\mathfrak{f}'$ zusammengesetzt, und ihr Geschlecht kann durch das Problem des Artikels 246 bestimmt werden. — Sind dagegen beide $\mathfrak{f}$, $\mathfrak{f}'$ uneigentlich primitiv, so ist der größte gemeinsame Teiler von A, B, C gleich $2\mathfrak{m}\mathfrak{m}'$; die Form $\mathfrak{F}$ ist weiterhin aus $\mathfrak{f}$, $\mathfrak{f}'$ zusammengesetzt und offenbar von der eigentlich primitiven Form $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$ abgeleitet. Das Geschlecht dieser Form kann daher nach Artikel 246 bestimmt werden; da F von derselben Form abgeleitet ist, ergibt sich daraus sofort auch ihr Geschlecht.

Aus dieser Lösung ist klar, dass der im vorigen Artikel für primitive Formen erläuterte Satz, nämlich *gehören f', g' jeweils zu denselben Geschlechtern wie f, g, so gehört die aus f', g' zusammengesetzte Form zu demselben Geschlecht wie die aus f, g zusammengesetzte*, allgemein für beliebige Formen gilt.

Komposition der Klassen.

249.

Satz. *Gehören die Formen f, f' jeweils zu denselben Ordnungen, Geschlechtern und Klassen wie g, g', so gehört die aus f und f' zusammengesetzte Form zu derselben Klasse wie die aus g und g' zusammengesetzte.*

Aus diesem Satz, dessen Richtigkeit unmittelbar aus Artikel 239 folgt, ergibt sich die Bedeutung einer *aus zwei gegebenen Klassen* oder auch *aus mehreren zusammengesetzten Klasse*.

Wird irgendeine Klasse K mit der Hauptklasse zusammengesetzt, so entsteht die Klasse K selbst; die Hauptklasse kann also bei der Komposition mit anderen Klassen derselben Determinante weggelassen werden. Aus der Komposition zweier entgegengesetzter eigentlich primitiver Klassen entsteht stets die Hauptklasse derselben Determinante (siehe Artikel 243). Da jede ambige Klasse sich selbst entgegengesetzt ist, ergibt die Komposition irgendeiner eigentlich primitiven ambigen Klasse mit sich selbst die Hauptklasse derselben Determinante.

Der letzte Satz gilt auch umgekehrt: *Ergibt die Komposition einer eigentlich primitiven Klasse K mit sich selbst die Hauptklasse H derselben Determinante, so muss K eine ambige Klasse sein.* Ist nämlich K' die zu K entgegengesetzte Klasse, so ist die aus den drei Klassen K, K, K' zusammengesetzte Klasse dieselbe wie die aus H und K' entstehende. Aus jenen entsteht K (denn K und K' ergeben H, diese mit K die Klasse K selbst), aus diesen K'; somit fällt K mit K' zusammen und ist daher eine ambige Klasse.

Ferner ist der folgende Satz zu beachten: *Sind die Klassen K, L den Klassen K', L' jeweils entgegengesetzt, so ist die aus K und L zusammengesetzte Klasse der aus K' und L' zusammengesetzten entgegengesetzt.* Die Formen f, g, f', g' gehören jeweils zu den Klassen K, L, K', L'; die Form F sei aus f, g und F' aus f', g' zusammengesetzt. Da f' der Form f und g' der Form g uneigentlich äquivalent ist, während F aus beiden f, g direkt zusammengesetzt ist, ist F auch aus f', g' zusammengesetzt, aber aus beiden invers. Daher ist jede Form, die F uneigentlich äquivalent ist, aus f', g' direkt zusammengesetzt und somit F' eigentlich äquivalent (Artikel 238, 239). Also sind F, F' uneigentlich äquivalent, und die Klassen, zu denen sie gehören, sind entgegengesetzt.

Daraus folgt: Wird eine ambige Klasse K mit einer ambigen Klasse L zusammengesetzt. so entsteht stets eine ambige Klasse. Denn sie ist der Klasse entgegengesetzt, die aus den zu K, L entgegengesetzten Klassen zusammengesetzt ist, also sich selbst, da diese Klassen sich selbst entgegengesetzt sind.

Schließlich bemerken wir: Sind zwei beliebige Klassen K, L derselben Determinante gegeben, deren erste eigentlich primitiv ist, so lässt sich stets eine Klasse M derselben Determinante finden, aus der zusammen mit K die Klasse L zusammengesetzt ist. Das erreicht man offenbar, indem man für M die Klasse nimmt, die aus L und der zu K entgegengesetzten Klasse zusammengesetzt ist. Zugleich erkennt man sehr leicht, dass diese Klasse die einzige mit dieser Eigenschaft ist; verschiedene Klassen derselben Determinante ergeben also bei Komposition mit derselben eigentlich primitiven Klasse verschiedene Klassen.

Die Komposition der Klassen kann zweckmäßig mit dem Additionszeichen + bezeichnet werden, ebenso wie die Gleichheit der Klassen mit dem Gleichheitszeichen. Mit diesen Zeichen lässt sich der eben gegebene Satz so darstellen: Ist K' die zu K entgegengesetzte Klasse, so ist $K + K'$ die Hauptklasse derselben Determinante, also $K + K' + L = L$; setzt man daher $K' + L = M$, so gilt $K + M = L$, wie verlangt. Gäbe es aber neben M noch eine andere M mit derselben Eigenschaft, also $K + M' = L$, so wäre $K + K' + M' = L + K' = M$ und damit $M' = M$. — Werden mehrere identische Klassen zusammengesetzt, so kann man dies wie bei der Multiplikation durch Voranstellen ihrer Anzahl bezeichnen, sodass $2K$ dasselbe wie $K + K$, $3K$ dasselbe wie $K + K + K$ bedeutet usw. Dieselben Zeichen könnten auch auf Formen übertragen werden, sodass $(a, b, c) + (a', b', c')$ die aus (a, b, c), (a', b', c') zusammengesetzte Form bezeichnete. Um aber auch nur den Anschein einer Mehrdeutigkeit zu vermeiden, verzichten wir lieber auf diese Abkürzung, zumal wir einem solchen Zeichen $\sqrt{M}(a, b, c)$ bereits eine besondere Bedeutung gegeben haben. — Wir sagen, die Klasse $2K$ entstehe durch *Verdopplung* der Klasse K, die Klasse $3K$ durch *Verdreifachung* usw.

250.

Ist D eine durch mm teilbare Zahl, wobei wir m als positiv voraussetzen, so gibt es eine Ordnung von Formen der Determinante D, die von der eigentlich primitiven Ordnung der Determinante $\frac{D}{mm}$ abgeleitet ist (oder *zwei*, wenn D negativ ist, nämlich eine positive und eine negative). Offenbar gehört die Form $(m, 0, -\frac{D}{m})$ zu dieser Ordnung, und zwar zur positiven, und kann darin mit Recht als *einfachste Form* betrachtet werden (ebenso ist $(-m, 0, \frac{D}{m})$ die einfachste in der negativen Ordnung, wenn D negativ ist). Gilt außerdem $\frac{D}{mm} \equiv 1$ (modulo 4), so gibt es auch eine Ordnung von Formen der Determinante D, die von der uneigentlich primitiven Ordnung der Determinante $\frac{D}{mm}$ abgeleitet ist; zu ihr gehört offenbar die Form $(2m, m, \frac{mm-D}{2m})$, die als einfachste in ihr gilt. (Ist D negativ, so gibt es wiederum zwei Ordnungen, und in der negativen gilt die Form $(-2m, -m, \frac{D-mm}{2m})$ als einfachste.) So sind *zum Beispiel*, wenn wir auch den Fall $m = 1$ hier einbeziehen, in den vier Ordnungen von Formen der Determinante 45 die folgenden die einfachsten: $(1, 0, -45)$, $(2, 1, -22)$. $(3, 0, -15)$, $(6, 3, -6)$. Damit ergibt sich das folgende

Problem. *Es sei irgendeine Form F aus der Ordnung O gegeben. Gesucht ist eine eigentlich primitive (positive) Form derselben Determinante, aus deren Komposition mit der einfachsten Form in O die Form F entsteht.*

Lösung. Die Form $F = (ma, mb, mc)$ sei von der primitiven Form $f = (a, b, c)$ mit der Determinante $= d$ abgeleitet, und wir nehmen *zuerst* an, dass f eigentlich primitiv ist. Zunächst bemerken wir: Ist etwa a nicht zu $2dm$ teilerfremd, so gibt es sicher andere, zu (a, b, c) eigentlich äquivalente Formen, deren erste Koeffizienten diese Eigenschaft haben. Denn nach Artikel 228 gibt es zu $2dm$ teilerfremde Zahlen, die durch jene Form darstellbar sind. Es sei $a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$ eine solche Zahl, und wir nehmen an, was erlaubt ist, dass α, γ teilerfremd sind. Wählt man dann β, δ so, dass $\alpha\delta - \beta\gamma = 1$, so gehe f durch die Substitution $\alpha, \beta, \gamma, \delta$ in die Form (a', b', c') über; diese ist ihr eigentlich äquivalent und hat die verlangte Eigenschaft. Da auch F und $(a'm, b'm, c'm)$ eigentlich äquivalent sind, erkennt man leicht, dass es

genügt, den Fall zu betrachten, dass a zu $2dm$ teilerfremd ist. Dann ist (a, bm, cmm) eine eigentlich primitive Form (denn hätten $a, 2bm, cmm$ einen gemeinsamen Teiler, so würde er auch $2dm = 2bbm - 2acm$ teilen) derselben Determinante wie F. Man bestätigt leicht, dass F in das Produkt der Form $(m, 0, -dm)$, die außer bei negativem F die einfachste der Ordnung O ist, mit (a, bm, cmm) durch die Substitution $1, 0, -b, -cm;\ 0, m, a, bm$ übergeht; daraus folgt nach dem Kriterium in Bemerkung 4 des Artikels 235, dass F aus $(m, 0, -dm)$ und (a, bm, cmm) zusammengesetzt ist. Ist dagegen F eine negative Form, so geht sie in das Produkt der einfachsten Form derselben Ordnung $(-m, 0, dm)$ mit der positiven Form $(-a, bm, -cmm)$ durch die Substitution $1, 0, b, -cm;\ 0, -m, -a, bm$ über und ist somit aus ihnen zusammengesetzt.

Zweitens: Ist f eine uneigentlich primitive Form, so darf man annehmen, dass $\frac{1}{2}a$ zu $2dm$ teilerfremd ist. Denn gilt diese Eigenschaft bei der Form f noch nicht, so kann eine der Form f eigentlich äquivalente Form mit dieser Eigenschaft gefunden werden. Daraus folgt leicht, dass $(\frac{1}{2}a, bm, 2cmm)$ eine eigentlich primitive Form derselben Determinante wie F ist. Ebenso leicht bestätigt man, dass F in das Produkt der Formen

$$(\pm 2m, \pm m, \pm\tfrac{1}{2}(m - dm)), \quad (\pm\tfrac{1}{2}a, bm, \pm 2cmm)$$

durch die Substitution

$$1, 0, \tfrac{1}{2}(1 \mp b), -cm; \quad 0, \pm 2m, \pm\tfrac{1}{2}a, (b \pm 1)m$$

übergeht. Dabei sind die unteren Zeichen zu nehmen, wenn F eine negative Form ist, in den übrigen Fällen die oberen. Sie ist also aus diesen beiden Formen zusammengesetzt, deren erste die einfachste der Ordnung O, deren zweite eine eigentlich primitive (positive) Form ist.

251.

Problem. *Es seien zwei Formen F, f derselben Determinante D gegeben, die zu derselben Ordnung O gehören. Gesucht ist eine eigentlich primitive Form der Determinante D, die mit f zusammengesetzt F ergibt.*

Lösung. Es sei φ die einfachste Form der Ordnung O; $\mathfrak{F}$, $\mathfrak{f}$ seien eigentlich primitive Formen der Determinante D, die mit φ zusammengesetzt jeweils F. f ergeben; schließlich sei f' eine eigentlich primitive Form, die mit $\mathfrak{f}$ zusammengesetzt $\mathfrak{F}$ ergibt. Dann ist die Form F aus den drei Formen $\varphi, \mathfrak{f}, f'$ oder aus den beiden f, f' zusammengesetzt. *Q. E. I.*

Jede Klasse einer gegebenen Ordnung kann also als zusammengesetzt aus irgendeiner gegebenen Klasse derselben Ordnung und einer eigentlich primitiven Klasse derselben Determinante betrachtet werden.

Bei gegebener Determinante enthalten die einzelnen Geschlechter derselben Ordnung gleich viele Klassen.

252.

Satz. *Bei gegebener Determinante enthalten die einzelnen Geschlechter derselben Ordnung gleich viele Klassen.*

Beweis. Die Geschlechter G und H sollen zu derselben Ordnung gehören; G bestehe aus n Klassen $K, K', K'' \dots K^{n-1}$, und L sei irgendeine Klasse des Geschlechts H. Nach dem vorigen Artikel suche man eine eigentlich primitive Klasse M derselben Determinante, aus deren Komposition mit K die Klasse L entsteht, und bezeichne die Klassen, die aus der Komposition von M mit $K', K'' \dots K^{n-1}$ entstehen, jeweils mit $L', L'' \dots L^{n-1}$. Dann folgt aus der letzten Bemerkung des Artikels 249, dass alle Klassen $L, L', L'' \dots L^{n-1}$ verschieden sind; nach Artikel 248 gehören sie alle zu demselben Geschlecht, *das heißt,* zum Geschlecht H. Schließlich erkennt man leicht, dass H keine weiteren Klassen enthalten kann, da jede Klasse des Geschlechts H als zusammengesetzt aus M und einer anderen Klasse derselben Determinante betrachtet werden kann, die notwendig stets zum Geschlecht G gehört. Somit enthält H ebenso wie G n verschiedene Klassen. *Q. E. D.*

Vergleich der Klassenzahlen in den einzelnen Geschlechtern verschiedener Ordnungen.

253.

Der vorige Satz setzt dieselbe Ordnung voraus und darf nicht auf verschiedene Ordnungen ausgedehnt werden. So gibt es *zum Beispiel* bei der Determinante -171 20 positive Klassen, die auf vier Ordnungen verteilt sind: Die eigentlich primitive Ordnung enthält zwei Geschlechter mit jeweils sechs Klassen; in der uneigentlich primitiven Ordnung besitzen zwei Geschlechter vier Klassen, jedes zwei; in der von der eigentlich primitiven Ordnung der Determinante -19 abgeleiteten Ordnung gibt es ein einziges Geschlecht mit drei Klassen; schließlich hat die von der uneigentlich primitiven Ordnung der Determinante -19 abgeleitete Ordnung ein einziges Geschlecht, das aus einer Klasse besteht. Ebenso verhält es sich mit den negativen Klassen. Es lohnt sich also, nach einem allgemeinen Prinzip zu suchen, von dem der Zusammenhang zwischen den Klassenzahlen verschiedener Ordnungen abhängt. Wir nehmen an, K, L seien zwei Klassen derselben (positiven) Ordnung O der Determinante D und M eine eigentlich primitive Klasse derselben Determinante, aus deren Komposition mit K die Klasse L entsteht; eine solche lässt sich nach Artikel 251 stets angeben. In manchen Fällen kann M die *einzige* eigentlich primitive Klasse sein, die mit K zusammengesetzt L ergibt; in anderen können mehrere verschiedene eigentlich primitive Klassen diese Eigenschaft haben. Wir nehmen allgemein an, es gebe r solche eigentlich primitiven Klassen $M, M', M'' \dots M^{r-1}$, die jeweils mit K zusammengesetzt dieselbe Klasse L ergeben, und bezeichnen ihre Menge mit W. Ferner sei L' eine andere Klasse der Ordnung O (verschieden von der Klasse L) und N' eine eigentlich primitive Klasse der Determinante D, die mit L zusammengesetzt L' ergibt. Die Menge der Klassen $N'+M, N'+M', N'+M'' \dots N'+M^{r-1}$, die sämtlich eigentlich primitiv und voneinander verschieden sind, werde mit W' bezeichnet. Dann erkennt man leicht, dass K mit irgendeiner Klasse aus W' zusammengesetzt L' ergibt; daraus folgt, dass W und W' keine Klasse gemeinsam haben. Außerdem bestätigt man ohne Mühe, dass es keine eigentlich primitive Klasse außerhalb der Menge W' gibt, die mit K zusammengesetzt L' ergibt. Ebenso ist klar: Ist L'' eine weitere Klasse der Ordnung O, verschieden von den Klassen L, L', so gibt es r eigentlich primitive Formen, die sowohl untereinander als auch von den Formen W, W' verschieden sind und jeweils mit K zusammengesetzt L'' ergeben; ebenso verhält es sich bei allen übrigen Klassen der Ordnung O. Da aber jede eigentlich primitive (positive) Klasse der Determinante D mit K zusammengesetzt eine Klasse der Ordnung O ergibt, folgt leicht: Ist die Gesamtzahl der Klassen der Ordnung O gleich n, so ist die Gesamtzahl aller eigentlich primitiven (positiven) Klassen derselben Determinante gleich rn.

Wir erhalten also die allgemeine Regel: Bezeichnen K, L beliebige Klassen der Ordnung O und r die Anzahl verschiedener eigentlich primitiver Klassen derselben Determinante, die jeweils mit K zusammengesetzt L ergeben, so ist die Gesamtzahl aller Klassen in der eigentlich primitiven (positiven) Ordnung r-mal so groß wie die Anzahl der Klassen der Ordnung O.

Da die Klassen K, L in der Ordnung O völlig beliebig gewählt werden können, dürfen wir auch identische Klassen nehmen. Dabei ist es zweckmäßig, diejenige Klasse

zu verwenden. in der die einfachste Form dieser Ordnung liegt. Nehmen wir sie also für K und L, so ist die Aufgabe darauf zurückgeführt, alle eigentlich primitiven Klassen anzugeben, die mit K zusammengesetzt K selbst wieder ergeben. Den Weg dazu bereitet der folgende Satz.

254.

Satz. *Ist $F = (A, B, C)$ die einfachste Form der Ordnung O der Determinante D und $f = (a, b, c)$ eine eigentlich primitive Form derselben Determinante, so lässt sich durch diese Form f die Zahl AA darstellen, wenn F durch Komposition der Formen f, F entsteht; und umgekehrt ist F aus sich selbst und f zusammengesetzt, wenn AA durch f dargestellt werden kann.*

Beweis. I. Geht F in das Produkt fF durch die Substitution p, p', p'', p'''; q, q', q'', q''' über, so ergibt Artikel 235

$$A(aq''q'' - 2bqq'' + cqq) = A^3, \quad \text{also}$$
$$AA = aq''q'' - 2bqq'' + cqq. \quad \textit{Erster Teil bewiesen.}$$

II. Es werde *angenommen*, dass AA durch f darstellbar ist. Die Werte der Unbestimmten, durch die dies geschieht, bezeichnen wir mit $q''. -q$, also sei $AA = aq''q'' - 2bqq'' + cqq$, und setzen

$$\begin{aligned} q''a - q(b + B) &= Ap, \\ -qC &= Ap', \\ q''(b - B) - qc &= Ap'' \\ -q''C &= Ap''', \\ q''a - q(b - B) &= Aq', \\ q''(b + B) - qc &= Aq''' \end{aligned}$$

Dann bestätigt man leicht, dass F in das Produkt fF durch die Substitution p, p', p'', p'''; q, q', q'', q''' übergeht. und somit aus f und F zusammengesetzt ist, sofern alle Zahlen p, p' usw. ganzzahlig sind. Nach der Beschreibung der einfachsten Form ist nun B entweder 0 oder $\frac{1}{2}A$, also $\frac{2B}{A}$ ganzzahlig; daraus ist auch klar, dass $\frac{C}{A}$ stets ganzzahlig ist. Somit sind $q' - p$, p', $q''' - p''$, p''' ganzzahlig, und es bleibt nur noch zu beweisen, dass p und p'' ganzzahlig sind. Es gilt aber

$$pp + \frac{2pqB}{A} = a - \frac{qqC}{A}, \quad p''p'' + \frac{2p''q''B}{A} = c - \frac{q''q''C}{A}$$

also gilt im Fall $B = 0$

$$pp = a - \frac{qqC}{A}, \quad p''p'' = c - \frac{q''q''C}{A}$$

und daher sind p, p'' ganzzahlig; gilt dagegen $B = \frac{1}{2}A$, so ist

$$pp + pq = a - \frac{qqC}{A}, \quad p''p'' + p''q'' = c - \frac{q''q''C}{A}$$

woraus ebenso leicht folgt, dass p und p'' auch in diesem Fall ganzzahlig sind. Daraus schließen wir, dass F aus f und F zusammengesetzt ist. *Zweiter Teil bewiesen.*

255.

Die Aufgabe ist also darauf zurückgeführt, alle eigentlich primitiven Klassen der Determinante D anzugeben, durch deren Formen AA darstellbar ist. Offenbar kann AA durch jede Form dargestellt werden, deren erster Koeffizient entweder AA oder das Quadrat eines Teilers von A ist. Kann umgekehrt AA durch eine Form f dargestellt werden, indem man ihren Unbestimmten die Werte αe, γe mit dem größten gemeinsamen Teiler e gibt, so geht die Form f durch die Substitution $\alpha, \beta, \gamma, \delta$ in eine Form über, deren erster Koeffizient $\frac{AA}{ee}$ ist; diese Form ist der Form f eigentlich äquivalent, wenn β, δ so gewählt werden, dass $\alpha\delta - \beta\gamma = 1$. Daher gibt es in jeder Klasse, durch deren Formen AA darstellbar ist, Formen, deren erster Koeffizient AA oder das Quadrat eines Teilers von A ist. Es kommt also darauf an, alle eigentlich primitiven Klassen der Determinante D zu finden, in denen solche Formen vorkommen. Das geschieht folgendermaßen: Es seien a, a', a'' usw. alle (positiven) Teiler von A; man suche alle Werte des Ausdrucks $\sqrt{D} \pmod{aa}$, die einschließlich der Grenzen zwischen 0 und $aa - 1$ liegen, bezeichne sie mit b, b', b'' usw. und setze

$$bb - D = aac, \quad b'b' - D = aac', \quad b''b'' - D = aac'' \text{ etc.}$$

Die Menge der Formen (aa, b, c), (aa, b', c') usw. werde mit V bezeichnet. Dann erkennt man leicht, dass jede Klasse der Determinante D, in der eine Form mit dem ersten Koeffizienten aa vorkommt, auch eine Form aus V enthalten muss. Ebenso suche man alle Formen der Determinante D, deren erster Koeffizient $a'a'$ ist und deren mittlerer Koeffizient einschließlich der Grenzen zwischen 0 und $a'a' - 1$ liegt, und bezeichne ihre Menge mit V'; entsprechend sei V'' die Menge solcher Formen mit dem ersten Koeffizienten $a''a''$ usw. Aus V, V', V'' usw. entferne man alle Formen, die nicht eigentlich primitiv sind, ordne die übrigen in Klassen ein und behalte, falls mehrere zu derselben Klasse gehören, in jeder Klasse nur eine. So erhält man alle gesuchten Klassen; ihre Anzahl verhält sich zur Einheit wie die Anzahl aller eigentlich primitiven (positiven) Klassen zur Anzahl der Klassen in der Ordnung O.

Beispiel. Es sei $D = -531$ und O die positive Ordnung, die von der uneigentlich primitiven Ordnung der Determinante -59 abgeleitet ist; ihre einfachste Form ist $(6, 3, 90)$, also $A = 6$. Hier sind a, a', a'', a''' gleich $1, 2, 3, 6$; V enthält die Form $(1, 0, 531)$; V' die Formen $(4, 1, 133)$, $(4, 3, 135)$; V'' die Formen $(9, 0, 59)$, $(9, 3, 60)$, $(9, 6, 63)$; schließlich V''' die Formen $(36, 3, 15)$, $(36, 9, 17)$, $(36, 15, 21)$, $(36, 21, 27)$, $(36, 27, 35)$, $(36, 33, 45)$. Von diesen zwölf Formen müssen aber sechs entfernt werden, nämlich aus V'' die zweite und dritte, aus V''' die erste, dritte, vierte und sechste; diese sind sämtlich abgeleitete Formen. Die sechs übrigen gehören, wie man findet, alle zu verschiedenen Klassen. Tatsächlich ist die Anzahl der eigentlich primitiven (positiven) Klassen der Determinante -531 gleich 18, und die Anzahl der uneigentlich primitiven (positiven) Klassen der Determinante -59 (oder die Anzahl der Klassen der Determinante -531, die von diesen abgeleitet sind) gleich 3; somit verhält sich die erste Anzahl zur zweiten wie 6 zu 1.

256.

Die folgenden allgemeinen Bemerkungen werden diese Lösung noch deutlicher machen.

I. Ist die Ordnung O von einer eigentlich primitiven Ordnung abgeleitet, so teilt AA die Zahl D; ist dagegen O uneigentlich primitiv oder von einer uneigentlich primitiven Ordnung abgeleitet, so ist A gerade, D durch $\frac{1}{4}AA$ teilbar und der Quotient $\equiv 1 \pmod 4$. Somit teilt das Quadrat jedes Teilers von A entweder D selbst oder wenigstens $4D$, und im letzteren Fall ist der Quotient stets $\equiv 1 \pmod 4$.

II. Teilt aa die Zahl D, so sind alle Werte des Ausdrucks $\sqrt{D} \pmod{aa}$, die zwischen 0 und $aa-1$ liegen, gleich $0, a, 2a \ldots aa-a$, und a ist daher die Anzahl der Formen in V; eigentlich primitiv sind darunter aber nur so viele, wie es unter den Zahlen

$$\frac{D}{aa}, \quad \frac{D}{aa}-1, \quad \frac{D}{aa}-4 \ldots \frac{D}{aa}-(a-1)^2$$

solche gibt, die mit a keinen gemeinsamen Teiler haben. Ist $a=1$, so besteht V aus einer einzigen Form, $(1,0,-D)$, die stets eigentlich primitiv ist. Ist a gleich 2 oder irgendeiner Potenz von 2, so ist die Hälfte jener a Zahlen gerade, die andere ungerade; daher gibt es in V $\frac{1}{2}a$ eigentlich primitive Formen. Ist a eine andere Primzahl p oder eine Potenz der Primzahl p, so sind drei Fälle zu unterscheiden: Alle jene a Zahlen sind zu a teilerfremd und somit alle Formen in V eigentlich primitiv, wenn $\frac{D}{aa}$ nicht durch p teilbar und zugleich quadratischer Nichtrest modulo p ist; teilt dagegen p die Zahl $\frac{D}{aa}$, so gibt es in V $\frac{(p-1)a}{p}$ eigentlich primitive Formen; ist schließlich $\frac{D}{aa}$ quadratischer Rest modulo p und nicht durch p teilbar, so gibt es in V $\frac{(p-2)a}{p}$ eigentlich primitive Formen. Das alles lässt sich ohne Mühe beweisen. Setzt man allgemein $a = 2^\nu p^\pi q^\chi r^\rho \ldots$, wobei p, q, r usw. verschiedene ungerade Primzahlen bezeichnen, so ist die Anzahl der eigentlich primitiven Formen in V gleich $NPQR \ldots$, wobei man setzen muss

$$\begin{aligned}
&N = 1 \quad (\text{wenn } \nu = 0) \text{ oder } N = 2^{\nu-1} \ (\text{wenn } \nu > 0)\\
&P = p^\pi \quad (\text{wenn } \tfrac{D}{aa} \text{ quadratischer Nichtrest modulo } p \text{ ist}) \text{ oder}\\
&P = (p-1)p^{\pi-1} \quad (\text{wenn } \tfrac{D}{aa} \text{ durch } p \text{ teilbar ist}) \text{ oder}\\
&P = (p-2)p^{\pi-1} \quad (\text{wenn } \tfrac{D}{aa} \text{ quadratischer Rest modulo } p\\
&\qquad\qquad \text{und nicht durch } p \text{ teilbar ist})
\end{aligned}$$

und Q, R usw. aus q, r usw. ebenso bestimmen muss wie P aus p.

III. Teilt aa die Zahl D nicht, so ist $\frac{4D}{aa}$ ganzzahlig und $\equiv 1 \pmod 4$, und die Werte des Ausdrucks $\sqrt{D} \pmod{aa}$ sind $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a \ldots aa-\frac{1}{2}a$. Somit ist die Anzahl der Formen in V gleich a; eigentlich primitiv sind darunter aber nur so viele, wie es unter den Zahlen

$$\frac{D}{aa}-\tfrac{1}{4}, \quad \frac{D}{aa}-\tfrac{9}{4}, \quad \frac{D}{aa}-\tfrac{25}{4} \quad \ldots \quad \frac{D}{aa}-(a-\tfrac{1}{2})^2$$

solche gibt, die zu a teilerfremd sind. Gilt $\frac{4D}{aa} \equiv 1 \pmod 8$, so sind alle diese Zahlen gerade, und es gibt daher in V keine eigentlich primitive Form; gilt dagegen $\frac{4D}{aa} \equiv 5 \pmod 8$. so sind alle jene Zahlen ungerade und somit alle Formen in V eigentlich

primitiv, wenn a gleich 2 oder einer Potenz von 2 ist. Allgemein gibt es in diesem Fall in V so viele eigentlich primitive Formen, wie unter jenen Zahlen durch keinen ungeraden Primteiler von a teilbar sind. Diese Anzahl ist $NPQR\ldots$, wenn $a = 2^\nu p^\pi q^\chi r^\rho \ldots$, wobei man $N = 2^\nu$ setzen und P, Q, R usw. aus p, q, r usw. ebenso ableiten muss wie im vorigen Fall.

IV. Auf diese Weise lassen sich also die Anzahlen der eigentlich primitiven Formen in V, V', V'' usw. bestimmen. Für die Summe all dieser Anzahlen findet man ohne große Mühe die folgende allgemeine Regel: Ist $A = 2^\nu \mathfrak{A}^\alpha \mathfrak{B}^\beta \mathfrak{C}^\gamma \ldots$, wobei $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. verschiedene ungerade Primzahlen bezeichnen, so ist die Gesamtzahl aller eigentlich primitiven Formen in V, V', V'' usw. $= \frac{Anabc\ldots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots}$, wobei man setzen muss

$\mathfrak{n} = 1$ (wenn $\frac{4D}{AA} \equiv 1, \mod 8$), oder
$\mathfrak{n} = 2$ (wenn $\frac{D}{AA}$ ganzzahlig ist), oder
$\mathfrak{n} = 3$ (wenn $\frac{4D}{AA} \equiv 5, \mod 8$); ferner
$\mathfrak{a} = \mathfrak{A}$ (wenn $\mathfrak{A}$ ein Teiler von $\frac{4D}{AA}$ ist), oder
$\mathfrak{a} = \mathfrak{A} \pm 1$ (wenn $\mathfrak{A}$ kein Teiler von $\frac{4D}{AA}$ ist,
mit dem oberen Vorzeichen
oder dem unteren, je nachdem, ob $\frac{4D}{AA}$ quadratischer Nichtrest
oder quadratischer Rest modulo $\mathfrak{A}$ ist)

und schließlich $\mathfrak{b}, \mathfrak{c}$ usw. aus $\mathfrak{B}, \mathfrak{C}$ ebenso ableiten muss wie $\mathfrak{a}$ aus $\mathfrak{A}$. Den Beweis hier ausführlicher darzustellen. erlaubt die Kürze nicht.

V. Was nun die Anzahl der Klassen betrifft, die durch die eigentlich primitiven Formen in V, V', V'' usw. gegeben werden, so sind die folgenden drei Fälle zu unterscheiden.

Erstens: Ist D eine negative Zahl, so bildet jede eigentlich primitive Form in V, V' usw. eine eigene Klasse; die Anzahl der gesuchten Klassen wird also durch die Formel der vorigen Bemerkung ausgedrückt, mit zwei Ausnahmen, nämlich wenn $\frac{4D}{AA}$ entweder $= -4$ oder $= -3$ ist, also wenn D entweder $= -AA$ oder $= -\frac{3}{4}AA$ ist. Zum Beweis dieses Satzes muss offenbar nur gezeigt werden, dass zwei verschiedene Formen aus V, V', V'' usw. nicht eigentlich äquivalent sein können. Wir nehmen also an, (hh, i, k), $(h'h', i', k')$ seien zwei verschiedene eigentlich primitive Formen aus V, V', V'' usw., die derselben Klasse angehören, und die erste gehe durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$ in die zweite über. Dann haben wir die Gleichungen

$$\alpha\delta - \beta\gamma = 1,$$
$$hh\alpha\alpha + 2i\alpha\gamma + k\gamma\gamma = h'h',$$
$$hh\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i'$$

Daraus folgt leicht, *erstens*, dass γ gewiss nicht $= 0$ ist (woraus $\alpha = \pm 1$, $hh = h'h'$, $i' \equiv i \pmod{hh}$ folgen würden und damit die Identität der vorgelegten Formen, entgegen der Annahme); *zweitens*, dass γ durch den größten gemeinsamen Teiler der Zahlen h, h' teilbar ist; (setzt man nämlich diesen Teiler $= r$, so teilt er offenbar auch $2i, 2i'$, ist aber zu k teilerfremd; ferner teilt rr die Zahl $hhk - h'h'k' = ii - i'i'$,

woraus leicht folgt, dass r auch $i - i'$ teilt. Nun gilt aber $\alpha i' - \beta h'h' = \alpha i + \gamma k$, also ist γk und somit auch γ durch r teilbar); *drittens*, dass $(\alpha hh + \gamma i)^2 - D\gamma\gamma = hhh'h'$. Setzt man also $\alpha hh + \gamma i = rp$, $\gamma = rq$, so sind p und q ganze Zahlen, von denen die zweite nicht $= 0$ ist, und es gilt $pp - Dqq = \frac{hhh'h'}{rr}$. Nun ist $\frac{hhh'h'}{rr}$ die kleinste durch hh und $h'h'$ zugleich teilbare Zahl und teilt somit AA und daher auch $4D$. Also ist $\frac{4Drr}{hhh'h'}$ eine (negative) ganze Zahl; setzt man sie $= -e$, so gilt $pp - Dqq = -\frac{4D}{e}$ oder $4 = (\frac{2rp}{hh'})^2 + eqq$. In dieser Gleichung muss der Term $(\frac{2rp}{hh'})^2$, als Quadrat kleiner als 4, entweder 0 oder 1 sein. Im ersten Fall gilt $eqq = 4$ und $D = -(\frac{hh'}{rq})^2$; daraus folgt, dass $\frac{4D}{AA}$ ein mit negativem Vorzeichen versehenes Quadrat ist und somit gewiss nicht $\equiv 1 \pmod 4$, also O weder eine uneigentlich primitive noch eine von einer uneigentlich primitiven Ordnung abgeleitete Ordnung ist. Daher ist $\frac{D}{AA}$ ganzzahlig, woraus leicht folgt, dass e durch 4 teilbar ist, dass $qq = 1$, $D = -(\frac{hh'}{r})^2$ gilt und auch $\frac{AA}{D}$ ganzzahlig ist. Somit muss $D = -AA$ oder $\frac{D}{AA} = -1$ gelten; dies ist die erste Ausnahme. Im zweiten Fall ist $eqq = 3$, also $e = 3$ und $4D = -3(\frac{hh'}{r})^2$; daher ist $3(\frac{hh'}{rA})^2$ eine ganze Zahl, die, da sie mit dem ganzzahligen Quadrat $(\frac{rA}{hh'})^2$ multipliziert 3 ergibt, nur 3 sein kann. Somit gilt $4D = -3AA$ oder $D = -\frac{3}{4}AA$; dies ist die zweite Ausnahme. In allen übrigen Fällen gehören also sämtliche eigentlich primitiven Formen in V, V', V'' usw. zu verschiedenen Klassen. — Für die Ausnahmefälle genügt es, die Ergebnisse einer nicht schwierigen Untersuchung anzugeben, die wir hier der Kürze wegen weglassen müssen. Im ersten Fall gehören von den eigentlich primitiven Formen in V, V', V'' usw. stets je zwei, im zweiten je drei zu derselben Klasse; somit ist die Gesamtzahl aller gesuchten Klassen im ersten Fall die Hälfte, im zweiten ein Drittel des Wertes des in der vorigen Bemerkung angegebenen Ausdrucks.

Zweitens: Ist D eine positive Quadratzahl, so bildet jede eigentlich primitive Form in V, V', V'' usw. ausnahmslos eine eigene Klasse. Nehmen wir nämlich an, (hh, i, k), $(h'h', i', k')$ seien zwei solche verschiedenen eigentlich äquivalenten Formen, und die erste gehe durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$ in die zweite über. Dann gelten offenbar auch hier alle Überlegungen des vorigen Falls, in denen nicht vorausgesetzt wird, dass D negativ ist. Bezeichnen also p, q, r dasselbe wie dort, so ist auch hier $\frac{4Drr}{hhh'h'}$ ganzzahlig, nun aber positiv statt negativ und außerdem ein Quadrat. Setzt man es $= gg$, so ist $(\frac{2rp}{hh'})^2 - ggqq = 4$, *was widersinnig ist,* da die Differenz zweier Quadrate nicht 4 sein kann, wenn das kleinere Quadrat nicht 0 ist. Die Annahme kann daher nicht bestehen.

Für den *dritten* Fall dagegen, in dem D eine positive Nichtquadratzahl ist, haben wir bisher keine allgemeine Regel, um die Anzahl der eigentlich primitiven Formen in V, V', V'' usw. mit der Anzahl der daraus entstehenden verschiedenen Klassen zu vergleichen. Wir können allerdings sagen, dass die zweite Anzahl der ersten entweder gleich oder ein Teiler von ihr ist. Wir haben sogar einen besonderen Zusammenhang zwischen dem Quotienten dieser Zahlen und den kleinsten Werten von t, u, die der Gleichung $tt - Duu = AA$ genügen, entdeckt; ihn hier darzustellen würde aber zu weit führen. Ob sich jener Quotient in allen Fällen allein durch Betrachtung der Zahlen D, A erkennen lässt (wie in den vorigen Fällen), darüber können wir nichts Sicheres sagen. Hier sind einige Beispiele, deren Anzahl jeder leicht vermehren kann. Für $D = 13$, $A = 2$ ist die Anzahl der eigentlich primitiven Formen in V usw. gleich 3; alle

sind äquivalent, bilden also nur eine Klasse. Für $D = 37$, $A = 2$ gibt es ebenfalls drei eigentlich primitive Formen in V usw., die zu drei verschiedenen Klassen gehören; für $D = 588$, $A = 7$ gibt es acht eigentlich primitive Formen in V usw., die vier Klassen bilden; für $D = 867$, $A = 17$ gibt es in V usw. 18 eigentlich primitive Formen, ebenso viele für $D = 1445$, $A = 17$, die aber bei der ersten Determinante in zwei, bei der zweiten in sechs Klassen zerfallen.

VI. Wendet man diese allgemeine Theorie auf den Fall an. in dem O eine uneigentlich primitive Ordnung ist, so folgt: Die Anzahl der Klassen in dieser Ordnung verhält sich zur Gesamtzahl aller Klassen in der eigentlich primitiven Ordnung wie 1 zur Anzahl der verschiedenen eigentlich primitiven Klassen, die durch die drei Formen $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ gebildet werden. Dabei entsteht eine einzige Klasse, wenn $D \equiv 1 \pmod 8$, weil in diesem Fall die zweite und dritte Form uneigentlich primitiv sind; gilt dagegen $D \equiv 5 \pmod 8$, so sind alle drei Formen eigentlich primitiv und ergeben ebenso viele verschiedene Klassen, wenn D negativ ist, mit der einzigen Ausnahme $D = -3$, bei der sie eine einzige Klasse bilden. Schließlich gehört der Fall, dass D positiv ist (von der Form $8n + 5$), zu denen, für die bisher eine allgemeine Regel fehlt. Wir können aber sagen, dass jene drei Formen in diesem Fall entweder zu drei verschiedenen Klassen oder zu einer einzigen gehören, niemals zu zweien. Denn gehören die Formen $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ jeweils zu den Klassen K, K', K'', so gilt offenbar $K + K' = K'$, $K' + K' = K''$; nimmt man also an, dass K und K' identisch sind, so sind auch K' und K'' identisch. Nimmt man ebenso K und K'' als identisch an, so sind es auch K' und K''; da schließlich $K' + K'' = K$ gilt, folgt aus der Annahme, K' und K'' seien identisch, dass auch K und K'' zusammenfallen. Somit sind entweder alle drei Klassen K, K', K'' verschieden oder alle drei identisch. *Zum Beispiel* gibt es unterhalb von 600 75 Zahlen der Form $8n + 5$, darunter 16 Determinanten, für die der erste Fall gilt, bei denen also die Anzahl der Klassen in der eigentlich primitiven Ordnung dreimal so groß ist wie in der uneigentlich primitiven, nämlich $37, 101, 141, 189, 197, 269.\ 325, 333, 349, 373, 381, 389, 405, 485, 557, 573$; für die übrigen 59 gilt der zweite Fall, die Klassenzahl ist also in beiden Ordnungen gleich.

VII. Es ist kaum nötig zu bemerken, dass man durch die vorige Untersuchung nicht nur die Klassenzahlen verschiedener Ordnungen derselben Determinante vergleichen kann, sondern dass sie auch auf beliebige verschiedene Determinanten anwendbar ist, deren Verhältnis ein Verhältnis von Quadraten ist. Bezeichnet nämlich O irgendeine Ordnung der Determinante dmm und O' eine Ordnung der Determinante $dm'm'$, so lässt sich O mit der eigentlich primitiven Ordnung der Determinante dmm vergleichen und diese mit der von der eigentlich primitiven Ordnung der Determinante d abgeleiteten Ordnung, oder, was hinsichtlich der Klassenzahl auf dasselbe hinausläuft, mit dieser Ordnung selbst; mit derselben lässt sich auf genau ähnliche Weise die Ordnung O' vergleichen.

Die Anzahl der ambigen Klassen.

257.

Unter allen Klassen in einer gegebenen Ordnung einer gegebenen Determinante verlangen besonders die ambigen Klassen eine ausführlichere Untersuchung; die Bestimmung ihrer Anzahl wird uns den Weg zu vielem anderen öffnen. Es genügt aber, diese Anzahl nur in der eigentlich primitiven Ordnung zu bestimmen, da sich die übrigen Fälle leicht auf diesen zurückführen lassen. Wir werden dazu zuerst zeigen, wie man alle eigentlich primitiven ambigen Formen (A, B, C) der vorgelegten Determinante D findet, in denen entweder $B = 0$ oder $B = \frac{1}{2}A$ gilt, und dann, wie man aus ihrer Anzahl die Anzahl aller eigentlich primitiven ambigen Klassen der Determinante D gewinnt.

I. Alle eigentlich primitiven Formen $(A, 0, C)$ der Determinante D findet man offenbar, indem man für A die einzelnen Teiler von D (sowohl positiv als auch negativ) nimmt, für die $C = -\frac{D}{A}$ zu A teilerfremd ist. Ist also $D = 1$, so gibt es zwei solche Formen, $(1, 0, -1)$, $(-1, 0, 1)$; ebenso viele, wenn $D = -1$, nämlich $(1, 0, 1)$, $(-1, 0, -1)$; ist D eine Primzahl oder eine Primzahlpotenz (mit positivem oder negativem Vorzeichen), so gibt es vier: $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. Ist allgemein D durch n verschiedene Primzahlen teilbar (zu denen hier auch 2 gerechnet werden muss), so gibt es insgesamt 2^{n+1} solche Formen. Setzt man nämlich $D = \pm PQR\ldots$, wobei P, Q, R usw. verschiedene Primzahlen oder Potenzen verschiedener Primzahlen bezeichnen, deren Anzahl $= n$ ist, so sind die Werte von A gleich $1, P, Q, R$ usw. und den Produkten aus beliebig vielen dieser Zahlen. Nach der Kombinationslehre ist die Anzahl dieser Werte 2^n; sie muss aber verdoppelt werden, da man jedem Wert sowohl ein positives als auch. ein negatives Vorzeichen geben muss.

II. Ebenso erhält man alle eigentlich primitiven Formen $(2B, B, C)$ der Determinante D, indem man für B alle Teiler von D (positiv und negativ) nimmt, für die $C = \frac{1}{2}(B - \frac{D}{B})$ ganzzahlig und zu $2B$ teilerfremd ist. Da C notwendig ungerade sein muss und daher $CC \equiv 1 \pmod 8$ gilt, folgt aus $D = BB - 2BC = (B - C)^2 - CC$, dass D entweder $\equiv 3 \pmod 4$ ist, wenn B ungerade ist, oder $\equiv 0 \pmod 8$, wenn B gerade ist; ist also D einer der Zahlen $1, 2, 4, 5, 6$ modulo 8 kongruent, so gibt es keine solchen Formen. Gilt $D \equiv 3 \pmod 4$, so ist C ganzzahlig und ungerade, welchen Teiler von D man auch für B nimmt; damit aber C mit $2B$ keinen gemeinsamen Teiler hat, muss B so gewählt werden, dass $\frac{D}{B}$ zu B teilerfremd ist. Daher gibt es für $D = -1$ zwei Formen, $(2, 1, 1)$, $(-2.\ -1, -1)$, und allgemein erkennt man leicht: Ist die Anzahl aller Primzahlen, die D teilen, gleich n, so entstehen insgesamt 2^{n+1} Formen. — Ist D durch 8 teilbar, so wird C ganzzahlig, wenn man für B irgendeinen geraden Teiler von $\frac{1}{2}D$ nimmt; die andere Bedingung, dass $C = \frac{1}{2}B - \frac{D}{2B}$ zu $2B$ teilerfremd sein soll, erfüllt man *erstens*, indem man für B alle Teiler von D nimmt, die das Doppelte einer ungeraden Zahl sind und für die $\frac{D}{B}$ mit B keinen gemeinsamen Teiler hat. Ihre Anzahl (unter Berücksichtigung der verschiedenen Vorzeichen) ist 2^{n+1}, wenn D durch n verschiedene ungerade Primzahlen teilbar angenommen wird; *zweitens*, indem man für B alle durch vier teilbaren Teiler von $\frac{1}{2}D$ nimmt, für die $\frac{D}{2B}$ zu B teilerfremd ist. Ihre Anzahl ist ebenfalls 2^{n+1}, sodass es in diesem Fall insgesamt 2^{n+2} solche Formen gibt. Setzt man nämlich $D = \pm 2^\mu PQR\ldots$, wobei μ

einen Exponenten größer als 2 bezeichnet und P, Q, R verschiedene ungerade Primzahlen oder Potenzen solcher Primzahlen bezeichnen, deren Anzahl n ist, so kann man *sowohl* für $\frac{1}{2}B$ *als auch* für $\frac{D}{2B}$ die Werte $1, P, Q, R$ usw. und die Produkte aus beliebig vielen dieser Zahlen mit positivem und negativem Vorzeichen nehmen.

Aus allem folgt: Wird D durch n verschiedene ungerade Primzahlen teilbar angenommen (mit $n = 0$, wenn $D = \pm 1$ oder ± 2 oder eine Zweierpotenz vorliegt), so ist die Anzahl aller eigentlich primitiven Formen (A, B, C), in denen B entweder 0 oder $\frac{1}{2}A$ ist, gleich 2^{n+1}, wenn D entweder $\equiv 1$ oder $\equiv 5 \pmod 8$ ist; gleich 2^{n+2}, wenn $D \equiv 2, 3, 4, 6$ oder $7 \pmod 8$; und schließlich gleich 2^{n+3}, wenn $D \equiv 0 \pmod 8$. Vergleichen wir diese Anzahl mit dem, was wir in Artikel 231 für die Anzahl aller möglichen Charaktere primitiver Formen der Determinante D angegeben haben, so sehen wir, dass jene in allen Fällen genau doppelt so groß ist wie diese. Ist D negativ, so gibt es unter jenen Formen offenbar ebenso viele positive wie negative.

258.

Alle im vorigen Artikel gefundenen Formen gehören offenbar zu ambigen Klassen, und umgekehrt muss jede eigentlich primitive ambige Klasse der Determinante D mindestens eine jener Formen enthalten. Denn in einer solchen Klasse gibt es gewiss ambige Formen, und jeder eigentlich primitiven ambigen Form (a, b, c) der Determinante D ist eine der Formen des vorigen Artikels äquivalent, nämlich entweder

$$(a, 0, -\tfrac{D}{a}) \text{ oder } (a, \tfrac{1}{2}a, \tfrac{1}{4}a - \tfrac{D}{a})$$

je nachdem, ob b entweder $\equiv 0$ oder $\equiv \frac{1}{2}a \pmod{a}$ ist. Die Aufgabe ist also darauf zurückgeführt, zu untersuchen, wie viele verschiedene Klassen jene Formen bilden.

Ist die Form $(a, 0, c)$ unter den Formen des vorigen Artikels, so kommt auch die Form $(c, 0, a)$ darunter vor und ist stets von ihr verschieden, mit der einzigen Ausnahme $a = c = \pm 1$, also $D = -1$, die wir vorerst beiseitelassen. Da diese Formen offenbar derselben Klasse angehören, genügt es, eine zu behalten; wir entfernen diejenige, deren erster Koeffizient größer als der dritte ist. Auch den Fall $a = -c = \pm 1$ oder $D = 1$ lassen wir beiseite. So können wir alle Formen $(A, 0, C)$ auf die Hälfte ihrer Anzahl reduzieren, indem wir von je zweien stets eine behalten; in allen übrigen gilt $A < \sqrt{\pm D}$.

Kommt ebenso unter den Formen des vorigen Artikels die Form $(2b, b, c)$ vor, so findet sich darunter auch

$$(4c - 2b,\ 2c - b,\ c) = \left(-\frac{2D}{b},\ -\frac{D}{b},\ c\right)$$

die ihr eigentlich äquivalent und von ihr verschieden ist, mit der einzigen Ausnahme $c = b = \pm 1$ oder $D = -1$, die wir beiseitelassen. Von diesen beiden Formen genügt es, diejenige zu behalten, deren erster Koeffizient kleiner als der erste Koeffizient der anderen ist (dem Betrag nach gleich und im Vorzeichen verschieden können sie in diesem Fall nicht sein). Somit lassen sich auch alle Formen $(2B, B, C)$ auf die Hälfte ihrer Anzahl reduzieren, indem man von je zweien stets eine entfernt; in den übrigen gilt $B < \frac{D}{B}$ oder $B < \sqrt{\pm D}$. So bleibt von allen Formen des vorigen Artikels nur die Hälfte übrig. Ihre Menge bezeichnen wir mit W, und es bleibt nur zu zeigen, wie viele verschiedene Klassen aus diesen Formen entstehen. Ist D negativ, so gibt es offenbar in W ebenso viele positive wie negative Formen.

I. Ist D negativ, so gehören die einzelnen Formen in W zu verschiedenen Klassen. Denn alle Formen $(A, 0, C)$ sind reduziert; ebenso sind alle Formen $(2B, B, C)$ reduziert, außer denen, in denen $C < 2B$ gilt. In einer solchen Form ist $2C < 2B + C$; daher gilt (weil $B < \frac{D}{B}$, *das heißt* $B < 2C - B$, also $2B < 2C$ oder $B < C$) $2C - 2B < C$ und $C - B < \frac{1}{2}C$, und somit ist $(C, C - B, C)$, die jener offenbar äquivalent ist, eine reduzierte Form. So erhält man ebenso viele reduzierte Formen, wie es Formen in W gibt. Da darunter offenbar weder identische noch entgegengesetzte Formen vorkommen können (mit der einzigen Ausnahme $C - B = 0$, bei der $B = C = \pm 1$, also $D = -1$ gilt und die wir bereits beiseitegelassen haben), gehören alle zu verschiedenen Klassen. Daraus folgt: Die Anzahl aller eigentlich primitiven ambigen Klassen der Determinante D ist gleich der Anzahl der Formen in W oder

der Hälfte der Anzahl der Formen des vorigen Artikels. Im Ausnahmefall $D = -1$ ergibt sich durch Ausgleich dasselbe: Es gibt zwei Klassen; zur einen gehören die Formen $(1, 0, 1)$, $(2, 1, 1)$, zur anderen $(-1, 0, -1)$, $(-2, -1, -1)$. Allgemein ist also bei negativer Determinante die Anzahl aller eigentlich primitiven ambigen Klassen gleich der Anzahl aller zuweisbaren Charaktere primitiver Formen dieser Determinante; die Anzahl der positiven eigentlich primitiven ambigen Klassen ist dagegen halb so groß.

II. Ist D eine positive Quadratzahl $= hh$, so lässt sich ohne große Mühe beweisen, dass die einzelnen Formen in W zu verschiedenen Klassen gehören. In diesem Fall können wir aber auf folgende Weise noch kürzer zur Lösung gelangen. Nach Artikel 210 enthält jede eigentlich primitive ambige Klasse der Determinante hh und keine andere Klasse genau eine reduzierte Form $(a, h, 0)$, in der a ein Wert des Ausdrucks $\sqrt{1}$ (mod. $2h$) ist, der zwischen 0 und $2h - 1$ einschließlich der Grenzen liegt. Es gibt also so viele eigentlich primitive ambige Klassen der Determinante hh, wie dieser Ausdruck Werte hat. Aus Artikel 105 folgt ohne Mühe, dass die Anzahl dieser Werte 2^n oder 2^{n+1} oder 2^{n+2} ist, je nachdem, ob h ungerade, das Doppelte einer ungeraden Zahl oder durch vier teilbar ist, also je nachdem, ob $D \equiv 1$ oder $\equiv 4$ oder $\equiv 0$ (mod. 8) gilt; dabei bezeichnet n die Anzahl der verschiedenen ungeraden Primteiler von h oder von D. Somit ist die Anzahl der eigentlich primitiven ambigen Klassen stets die Hälfte der Gesamtzahl aller im vorigen Artikel gefundenen Formen oder gleich der Anzahl der Formen in W oder aller möglichen Charaktere.

III. Ist D eine positive Nichtquadratzahl, so leiten wir aus jeder Form (A, B, C) in W eine andere Form (A, B', C') ab, indem wir $B' \equiv B$ (mod. A) zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp A$ nehmen (mit dem oberen oder unteren Vorzeichen, je nachdem, ob A. positiv oder negativ ist) und $C' = \frac{B'B' - D}{A}$ setzen; die Menge dieser Formen bezeichnen wir mit W'. Offenbar sind sie eigentlich primitive ambige Formen der Determinante D und sämtlich voneinander verschieden; außerdem sind sie alle reduziert. Gilt nämlich $A < \sqrt{D}$, so ist B' offenbar $< \sqrt{D}$ und positiv; ferner gilt $B' > \sqrt{D} \mp A$, also $A > \sqrt{D} - B'$, und somit liegt A, positiv genommen, gewiss zwischen $\sqrt{D} + B'$ und $\sqrt{D} - B'$. Gilt dagegen $A > \sqrt{D}$, so kann nicht $B = 0$ sein (solche Formen haben wir ja entfernt), sondern es muss $B = \frac{1}{2}A$ gelten; daher ist B' dem Betrag nach gleich $\frac{1}{2}A$ und dem Vorzeichen nach positiv (denn wegen $A < 2\sqrt{D}$ liegt $\pm\frac{1}{2}A$ zwischen den für B' festgelegten Grenzen und ist B modulo A kongruent, also $B' = \pm\frac{1}{2}A$). Somit gilt $B' < \sqrt{D}$, woraus $2B' < \sqrt{D} + B'$ oder $A < \sqrt{D} + B'$ folgt; daher liegt $\pm A$ notwendig zwischen den Grenzen $\sqrt{D} + B'$ und $\sqrt{D} - B'$. Schließlich enthält W' alle reduzierten eigentlich primitiven ambigen Formen der Determinante D. Ist nämlich (a, b, c) eine solche Form, so gilt entweder $b \equiv 0$ oder $b \equiv \frac{1}{2}a$ (mod. a). Im ersten Fall kann offenbar nicht $b < a$ und somit auch nicht $a > \sqrt{D}$ gelten, weshalb die Form $\left(a, 0, -\frac{D}{a}\right)$ gewiss in W und die entsprechende Form (a, b, c) in W' enthalten ist; im zweiten Fall gilt gewiss $a < 2\sqrt{D}$, also liegt $\left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a}\right)$ in W und die entsprechende Form (a, b, c) in W'. Daraus folgt, dass die Anzahl der Formen in W gleich der Anzahl aller reduzierten eigentlich primitiven ambigen Formen der Determinante D ist. Da aber jede ambige Klasse *zwei* reduzierte ambige Formen enthält (Artikel 187, 194), ist die Anzahl aller eigentlich primitiven ambigen Klassen der Determinante D halb so groß wie die Anzahl der Formen in W oder wie die

Anzahl aller zuweisbaren Charaktere.

259.

Die Anzahl der uneigentlich primitiven ambigen Klassen einer gegebenen Determinante D ist stets gleich der Anzahl der eigentlich primitiven ambigen Klassen derselben Determinante. Es sei K die Hauptklasse, und K', K'' usw. seien die übrigen eigentlich primitiven ambigen Klassen dieser Determinante; L sei irgendeine uneigentlich primitive ambige Klasse derselben Determinante, *zum Beispiel* diejenige, in der die Form $(2, 1, \frac{1}{2} - \frac{1}{2}D)$ liegt. Durch Komposition der Klasse L mit K entsteht also die Klasse L selbst. Aus der Komposition der Klasse L mit K', K'' usw. mögen jeweils die Klassen L', L'' usw. entstehen, die offenbar alle zur selben Determinante D gehören und uneigentlich primitiv und ambig sind. Der Satz ist also bewiesen, sobald gezeigt ist, dass alle Klassen L, L', L'' usw. verschieden sind und es außer ihnen keine uneigentlich primitiven ambigen Klassen der Determinante D gibt. Dazu unterscheiden wir die folgenden Fälle.

I. Ist die Anzahl der uneigentlich primitiven Klassen gleich der Anzahl der eigentlich primitiven, so entsteht jede der ersten durch Komposition der Klasse L mit einer bestimmten eigentlich primitiven Klasse; daher sind notwendig alle L, L', L'' usw. verschieden. Bezeichnet nun $\mathfrak{L}$ irgendeine uneigentlich primitive ambige Klasse der Determinante D, so gibt es eine eigentlich primitive Klasse $\mathfrak{K}$ mit $\mathfrak{K} + L = \mathfrak{L}$. Ist der Klasse $\mathfrak{K}$ die Klasse $\mathfrak{K}'$ entgegengesetzt, so gilt auch (weil die Klassen L, $\mathfrak{L}$ sich selbst entgegengesetzt sind) $\mathfrak{K}' + L = \mathfrak{L}$; daher ist notwendig $\mathfrak{K}$ mit $\mathfrak{K}'$ identisch und somit ambig. Also findet sich $\mathfrak{K}$ unter den Klassen K, K', K'' usw. und $\mathfrak{L}$ unter L, L', L'' usw.

II. Ist die Anzahl der uneigentlich primitiven Klassen ein Drittel der Anzahl der eigentlich primitiven, so sei H die Klasse, in der die Form $\left(4, 1, \frac{1-D}{4}\right)$ liegt, und H' diejenige, in der $\left(4, 3, \frac{9-D}{4}\right)$ liegt; dann sind H, H' eigentlich primitiv und sowohl voneinander als auch von der Hauptklasse K verschieden, und es gilt $H + H' = K$; $2H = H'$, $2H' = H$. Ist $\mathfrak{L}$ irgendeine uneigentlich primitive Klasse der Determinante D, die durch Komposition der Klasse L mit der eigentlich primitiven Klasse $\mathfrak{K}$ entsteht, so gilt auch $\mathfrak{L} = L + \mathfrak{K} + H$ und $\mathfrak{L} = L + \mathfrak{K} + H'$. Außer den drei (eigentlich primitiven und verschiedenen) Klassen $\mathfrak{K}$, $\mathfrak{K}+H$, $\mathfrak{K}+H'$ gibt es keine anderen, die mit L zusammengesetzt $\mathfrak{L}$ ergeben. Ist also $\mathfrak{L}$ ambig und $\mathfrak{K}'$ der Klasse $\mathfrak{K}$ entgegengesetzt, so gilt auch $L + \mathfrak{K}' = \mathfrak{L}$; daher muss $\mathfrak{K}'$ mit einer jener drei Klassen identisch sein. Gilt $\mathfrak{K}' = \mathfrak{K}$, so ist $\mathfrak{K}$ ambig; gilt $\mathfrak{K}' = \mathfrak{K}+H$, so gilt $K = \mathfrak{K}+\mathfrak{K}' = 2\mathfrak{K}+H = 2(\mathfrak{K}+H')$, und somit ist $\mathfrak{K}+H'$ ambig; gilt ebenso $\mathfrak{K}' = \mathfrak{K}+H'$, so ist $\mathfrak{K}+H$ ambig. Daher muss $\mathfrak{L}$ unter den Klassen L, L', L'' usw. vorkommen. Unter den drei Klassen $\mathfrak{K}$, $\mathfrak{K}+H$, $\mathfrak{K}+H'$ kann aber offenbar nicht mehr als eine ambig sein. Wären nämlich sowohl $\mathfrak{K}$ als auch $\mathfrak{K}+H$ ambig, also ihren jeweiligen entgegengesetzten Klassen $\mathfrak{K}'$, $\mathfrak{K}'+H'$ gleich, so wäre $\mathfrak{K}+H = \mathfrak{K}+H'$. Dasselbe folgt aus der Annahme, $\mathfrak{K}$ und $\mathfrak{K}+H'$ seien ambig; wären schließlich $\mathfrak{K}+H$, $\mathfrak{K}+H'$ ambig, also ihren entgegengesetzten Klassen $\mathfrak{K}'+H'$, $\mathfrak{K}'+H$ gleich, so wäre $\mathfrak{K}+H+\mathfrak{K}'+H = \mathfrak{K}'+H'+\mathfrak{K}+H'$, woraus $2H = 2H'$ oder $H' = H$ folgt. Daher gibt es nur eine eigentlich primitive ambige Klasse, die mit L zusammengesetzt $\mathfrak{L}$ ergibt; somit sind alle L, L', L'' usw. verschieden.

Die Anzahl der ambigen Klassen in einer *abgeleiteten* Ordnung ist offenbar gleich

der Anzahl der ambigen Klassen in der primitiven Ordnung, von der sie abgeleitet ist; sie lässt sich also nach dem Vorigen stets bestimmen.

260.

Aufgabe. *Eine eigentlich primitive Klasse K der Determinante D entsteht durch Verdopplung einer eigentlich primitiven Klasse k derselben Determinante. Gesucht sind a l l e solchen Klassen, deren Verdopplung die Klasse K ergibt.*

Lösung. Es sei H die Hauptklasse der Determinante D, und H', H'', H''' usw. seien die übrigen eigentlich primitiven ambigen Klassen derselben Determinante. Die Klassen, die aus ihrer Komposition mit k entstehen, nämlich $k + H'$, $k + H''$, $k + H'''$, seien mit k', k'', k''' usw. bezeichnet. Dann sind alle Klassen k, k', k'' usw. eigentlich primitiv von der Determinante D und voneinander verschieden; ebenso leicht sieht man, dass aus der Verdopplung jeder die Klasse K entsteht. Bezeichnet nun $\mathfrak{K}$ irgendeine eigentlich primitive Klasse der Determinante D, deren Verdopplung die Klasse K ergibt, so muss sie unter den Klassen k, k', k'' usw. enthalten sein. Setzen wir nämlich $\mathfrak{K} = k + \mathfrak{H}$, wobei $\mathfrak{H}$ eine eigentlich primitive Klasse der Determinante D ist (Artikel 249). so gilt $2k + 2\mathfrak{H} = 2\mathfrak{K} = K = 2k$; daraus folgt leicht, dass $2\mathfrak{H}$ mit der Hauptklasse zusammenfällt, $\mathfrak{H}$ ambig ist, also unter H, H', H'' usw. vorkommt, und $\mathfrak{K}$ unter k, k', k'' usw. Diese Klassen geben daher die vollständige Lösung der Aufgabe.

Ist D negativ, so ist offenbar von den Klassen k, k', k'' usw. die Hälfte positiv, die andere negativ.

Jede eigentlich primitive Klasse der Determinante D, die durch Verdopplung irgendeiner solchen Klasse entstehen kann, entsteht also durch Verdopplung genau so vieler solcher Klassen, wie es eigentlich primitive ambige Klassen der Determinante D gibt. Ist daher die Anzahl aller eigentlich primitiven Klassen der Determinante D gleich r und die Anzahl aller eigentlich primitiven ambigen Klassen dieser Determinante gleich n, so ist die Anzahl aller eigentlich primitiven Klassen derselben Determinante, die durch Verdopplung einer solchen Klasse entstehen können, gleich $\frac{r}{n}$. Dieselbe Formel ergibt sich bei negativer Determinante, wenn die Zeichen r, n die Anzahlen *positiver* Klassen bezeichnen, das erste *aller* eigentlich primitiven, das zweite nur der ambigen. So ist *zum Beispiel* für $D = -161$ die Anzahl aller positiven eigentlich primitiven Klassen gleich 16, die Anzahl der ambigen gleich 4; daher muss die Anzahl aller Klassen, die durch Verdopplung irgendeiner Klasse entstehen können, gleich 4 sein. Tatsächlich haben alle im Hauptgeschlecht enthaltenen Klassen diese Eigenschaft: Die Hauptklasse $(1, 0, 161)$ entsteht durch Verdopplung der vier ambigen Klassen; $(2, 1, 81)$ durch Verdopplung der Klassen $(9, 1, 18)$, $(9, -1, 18)$, $(11, 2, 15)$, $(11, -2, 15)$; $(9, 1, 18)$ durch Verdopplung der Klassen $(3, 1, 54)$, $(6, 1, 27)$, $(5, -2, 33)$, $(10, 3, 17)$; schließlich $(9, -1, 18)$ durch Verdopplung der Klassen $(3, -1, 54)$, $(6, -1, 27)$, $(5, 2, 33)$, $(10, -3, 17)$.

Mindestens der Hälfte aller für eine gegebene Determinante zuweisbaren Charaktere können keine eigentlich primitiven Geschlechter entsprechen (bei negativer Determinante keine positiven).

261.

Satz. *Bei einer positiven Nichtquadratzahl als Determinante können mindestens der Hälfte aller zuweisbaren Charaktere keine eigentlich primitiven Geschlechter entsprechen; bei negativer Determinante keine positiven eigentlich primitiven Geschlechter.*

Beweis. Es sei m die Anzahl aller eigentlich primitiven (positiven) Geschlechter der Determinante D und k die Anzahl der Klassen in jedem Geschlecht, sodass km die Anzahl aller eigentlich primitiven (positiven) Klassen ist; n sei die Anzahl aller verschiedenen für diese Determinante zuweisbaren Charaktere. Dann ist nach Artikel 258 die Anzahl aller eigentlich primitiven (positiven) ambigen Klassen gleich $\frac{1}{2}n$. Somit ist nach dem vorigen Artikel die Anzahl aller eigentlich primitiven Klassen, die durch Verdopplung einer solchen Klasse entstehen können, gleich $\frac{2km}{n}$. Nach Artikel 247 gehören aber alle diese Klassen zum Hauptgeschlecht, das k Klassen enthält. Können also alle Klassen des Hauptgeschlechts durch Verdopplung irgendeiner Klasse entstehen (was, wie wir im Folgenden beweisen werden, tatsächlich immer gilt), so ist $\frac{2km}{n} = k$ oder $m = \frac{1}{2}n$; gewiss kann aber weder $\frac{2km}{n} > k$ noch daher $m > \frac{1}{2}n$ sein. Da somit die Anzahl aller eigentlich primitiven (positiven) Geschlechter gewiss nicht größer als die Hälfte aller zuweisbaren Charaktere ist, können mindestens der Hälfte dieser Charaktere keine solchen Geschlechter entsprechen. *Damit ist der Satz bewiesen.* — Dabei muss man beachten, dass daraus noch nicht folgt, dass der Hälfte aller zuweisbaren Charaktere tatsächlich eigentlich primitive (positive) Geschlechter entsprechen. Die Wahrheit dieser sehr wichtigen Aussage lässt sich erst weiter unten aus den tiefsten Geheimnissen der Zahlen erschließen.

Da es bei negativer Determinante stets ebenso viele negative wie positive Geschlechter gibt, können offenbar von allen zuweisbaren Charakteren nicht mehr als die Hälfte zu negativen eigentlich primitiven Geschlechtern gehören. Darüber und über uneigentlich primitive Geschlechter werden wir weiter unten sprechen. Schließlich gilt der Satz nicht für positive Quadratzahlen als Determinanten; bei diesen sieht man ohne Mühe, dass jedem zuweisbaren Charakter tatsächlich Geschlechter entsprechen.

Ein zweiter Beweis des Fundamentalsatzes und der übrigen Sätze über die Reste -1, $+2$, -2.

262.

Lassen sich also für eine gegebene Nichtquadratzahl D als Determinante nur zwei verschiedene Charaktere zuweisen, so entspricht nur einem ein eigentlich primitives (positives) Geschlecht (das nur das Hauptgeschlecht sein kann); der andere gehört zu keiner eigentlich primitiven (positiven) Form dieser Determinante. Das geschieht bei den Determinanten -1, 2, -2, -4. den positiv genommenen Primzahlen der Form $4n+1$ und den negativ genommenen der Form $4n+3$, schließlich bei allen positiv genommenen Potenzen ungeraden Exponenten von Primzahlen der Form $4n+1$ und bei den Potenzen von Primzahlen der Form $4n+3$, die je nach geradem oder ungeradem Exponenten positiv oder negativ genommen werden. Aus diesem Prinzip können wir eine neue Methode gewinnen, nicht nur den Fundamentalsatz, sondern auch die übrigen Sätze des vorigen Abschnitts über die Reste -1, $+2$, -2 zu beweisen. Sie ist von den im vorigen Abschnitt benutzten Methoden völlig verschieden und scheint ihnen an Eleganz keineswegs nachzustehen. Die Determinante -4 und diejenigen, die Primzahlpotenzen sind, lassen wir jedoch aus, da sie nichts Neues lehren.

Für die Determinante -1 gibt es also keine positive Form mit dem Charakter $3, 4$; für die Determinante $+2$ überhaupt keine Form mit dem Charakter 3 *und* $5, 8$; bei der Determinante -2 hat keine positive Form den Charakter 5 *und* $7, 8$; bei der Determinante $+p$, wenn p eine Primzahl der Form $4n+1$ ist, oder bei der Determinante $-p$, wenn p eine Primzahl der Form $4n+3$ ist, hat keine eigentlich primitive Form (im zweiten Fall keine positive) den Charakter Np. Damit beweisen wir die Sätze des vorigen Abschnitts folgendermaßen.

I. -1 ist Nichtrest jeder (positiven) Zahl der Form $4n+3$. Wäre nämlich -1 Rest einer solchen Zahl A, so wäre bei $-1 = BB - AC$ die Form (A, B, C) eine positive Form der Determinante -1 mit dem Charakter $3, 4$.

II. -1 ist Rest jeder Primzahl p der Form $4n+1$. Denn der Charakter der Form $(-1, 0, p)$ ist, wie bei allen eigentlich primitiven Formen der Determinante p. gleich Rp, also $-1Rp$.

III. Sowohl $+2$ als auch -2 ist Rest jeder Primzahl p der Form $8n+1$. Denn entweder sind die Formen $\left(8, 1, \frac{1-p}{8}\right)$, $\left(-8, 1, \frac{p-1}{8}\right)$ oder die Formen $\left(8, 3, \frac{9-p}{8}\right)$, $\left(-8, 3, \frac{p-9}{8}\right)$ eigentlich primitiv (je nachdem, ob n ungerade oder gerade ist); ihr Charakter ist also Rp. Daher gilt $+8Rp$ und $-8Rp$, woraus auch $2Rp$, $-2Rp$ folgt.

IV. $+2$ ist Nichtrest jeder Zahl der Form $8n+3$ oder $8n+5$. Wäre es nämlich Rest einer solchen Zahl A, so gäbe es eine Form (A, B, C) der Determinante $+2$ mit dem Charakter 3 *und* $5, 8$.

V. Ebenso ist -2 Nichtrest jeder Zahl der Form $8n+5$ oder $8n+7$; sonst gäbe es eine Form (A, B, C) der Determinante -2 mit dem Charakter 5 *und* $7, 8$.

VI. -2 ist Rest jeder Primzahl p der Form $8n+3$. Diese Aussage lässt sich auf zwei Arten beweisen. *Erstens*: Da nach IV $+2Np$ und nach I $-1Np$ gilt, muss $-2Rp$ gelten. Der *zweite* Beweis ergibt sich aus der Betrachtung der Determinante $+2p$, für die vier

Charaktere zuweisbar sind, nämlich Rp, 1 *und* $3, 8$; Rp, 5 *und* $7, 8$; Np, 1 *und* $3, 8$; Np, 5 *und* $7, 8$. Mindestens zweien davon entsprechen also keine Geschlechter. Nun hat die Form $(1, 0, -2p)$ den ersten Charakter, die Form $(-1, 0, 2p)$ den vierten; somit müssen der zweite und dritte ausgeschlossen werden. Da also der Charakter der Form $(p, 0, -2)$ in Bezug auf die Zahl 8 gleich 1 *und* $3, 8$ ist, kann ihr Charakter in Bezug auf p nur Rp sein, also $-2Rp$.

VII. $+2$ ist Rest jeder Primzahl p der Form $8n+7$, was sich auf zwei Arten beweisen lässt. *Erstens*: Da aus I und V $-1Np$, $-2Np$ folgt, gilt $+2Rp$. *Zweitens*: Da entweder $\left(8, 1, \frac{1+p}{8}\right)$ oder $\left(8, 3, \frac{9+p}{8}\right)$ eine eigentlich primitive Form der Determinante $-p$ ist (je nachdem, ob n gerade oder ungerade ist), ist ihr Charakter Rp, also $8Rp$ und $2Rp$.

VIII. Jede Primzahl p der Form $4n + 1$ ist Nichtrest jeder ungeraden Zahl q, die Nichtrest von p ist. Wäre nämlich p Rest von q, so gäbe es offenbar eine eigentlich primitive Form der Determinante p mit dem Charakter Np.

IX. Ist ebenso irgendeine ungerade Zahl q Nichtrest einer Primzahl p der Form $4n+3$, so ist $-p$ Nichtrest von q; sonst gäbe es eine positive eigentlich primitive Form der Determinante $-p$ mit dem Charakter Np.

X. Jede Primzahl p der Form $4n + 1$ ist Rest jeder anderen Primzahl q, die Rest von p ist. Ist auch q von der Form $4n + 1$, so folgt dies sofort aus VIII; ist dagegen q von der Form $4n + 3$, so ist auch $-q$ Rest von p (nach II), also pRq (nach IX).

XI. Ist irgendeine Primzahl q Rest einer anderen Primzahl p der Form $4n + 3$, so ist $-p$ Rest von q. Ist nämlich q von der Form $4n + 1$; so folgt aus VIII pRq, also nach II $-pRq$; der Fall aber, dass auch q von der Form $4n + 3$ ist, entzieht sich dieser Methode, lässt sich jedoch durch Betrachtung der Determinante $+pq$ leicht erledigen. Von den vier für diese Determinante zuweisbaren Charakteren Rp. Rq; Rp, Nq; Np, Rq; Np, Nq können nämlich zweien keine Geschlechter entsprechen. Da die Charaktere der Formen $(1, 0, -pq)$, $(-1, 0, pq)$ jeweils der erste und vierte sind, können der zweite und dritte zu keiner eigentlich primitiven Form der Determinante pq gehören. Da somit der Charakter der Form $(q, 0, -p)$ in Bezug auf die Zahl p nach Voraussetzung Rp ist, muss der Charakter derselben Form in Bezug auf die Zahl q gleich Rq sein, also $-pRq$. *Damit ist der Satz bewiesen.*

Nimmt man in den Aussagen VIII und IX an, dass q eine Primzahl bezeichnet, so ergeben diese zusammen mit X und XI den Fundamentalsatz des vorigen Abschnitts.

Die Hälfte der Charaktere, denen keine Geschlechter entsprechen können, wird genauer bestimmt.

263.

Nachdem wir den Fundamentalsatz mit einem neuen Beweis bestätigt haben, werden wir zeigen, wie man für jede gegebene Nichtquadratzahl als Determinante jene Hälfte der Charaktere erkennt, denen keine eigentlich primitiven (positiven) Formen entsprechen können. Dies lässt sich umso kürzer erledigen, als die Grundlage bereits in der Untersuchung der Artikel 147–150 enthalten ist. Es sei ee das größte Quadrat, das die vorgelegte Determinante D teilt, und $D = D'ee$, sodass D' keinen quadratischen Faktor enthält. Ferner seien a, b, c usw. alle ungeraden Primteiler von D'; dann ist D' ohne Rücksicht auf das Vorzeichen entweder ihr Produkt oder das Doppelte dieses Produkts. Mit Ω werde die Menge der Einzelcharaktere Na, Nb, Nc usw. allein bezeichnet, wenn $D' \equiv 1 \pmod 4$; unter Hinzunahme des Charakters $3, 4$, wenn $D' \equiv 3$ und e ungerade oder das Doppelte einer ungeraden Zahl ist; unter Hinzunahme von $3, 8$ und $7, 8$, wenn $D' \equiv 3$ und e durch vier teilbar ist; unter Hinzunahme entweder des Charakters 3 *und* $5, 8$ oder der beiden $3, 8$ und $5, 8$, wenn $D' \equiv 2 \pmod 8$, je nachdem, ob e ungerade oder gerade ist; schließlich unter Hinzunahme entweder des Charakters 5 *und* $7, 8$ oder der beiden $5, 8$ und $7, 8$, wenn $D' \equiv 6 \pmod 8$, je nachdem, ob e ungerade oder gerade ist. Dann können allen Gesamtcharakteren, die eine ungerade Anzahl von Einzelcharakteren aus Ω enthalten, keine eigentlich primitiven (positiven) Geschlechter der Determinante D entsprechen. In allen Fällen tragen die Einzelcharaktere, die die Beziehung zu solchen Primteilern von D ausdrücken, die D' nicht teilen, nichts zur Möglichkeit oder Unmöglichkeit von Geschlechtern bei. — Nach der Kombinationslehre erkennt man sehr leicht, dass so tatsächlich die Hälfte aller zuweisbaren Gesamtcharaktere ausgeschlossen wird.

Diese Regeln werden folgendermaßen bewiesen. Aus den Prinzipien des vorigen Abschnitts oder den im vorigen Artikel erneut bewiesenen Sätzen folgt ohne Mühe: Ist p eine Primzahl (ungerade und positiv), die D nicht teilt und einen der ausgeschlossenen Charaktere hat, so enthält D' eine ungerade Anzahl von Faktoren, die Nichtreste von p sind; somit ist D' und daher auch D Nichtrest von p. Ferner kann offenbar ein Produkt aus beliebig vielen zu D teilerfremden ungeraden Zahlen, von denen keine einen ausgeschlossenen Charakter hat, ebenfalls nicht mit einem solchen Charakter übereinstimmen. Umgekehrt enthält daher jede zu D teilerfremde positive ungerade Zahl, die einen der ausgeschlossenen Charaktere hat, gewiss einen Primfaktor derselben Art, sodass D Nichtrest dieser Zahl ist. Gäbe es also eine eigentlich primitive (positive) Form der Determinante D, die einem ausgeschlossenen Charakter entspricht, so wäre D Nichtrest jeder durch eine solche Form darstellbaren positiven ungeraden und zu ihm teilerfremden Zahl; dies ist offenbar mit dem Satz von Artikel 154 nicht vereinbar.

Als Beispiele vergleiche man die Klassifikationen in den Artikeln 231, 232, deren Anzahl jeder nach Belieben vermehren kann.

264.

Auf diese Weise werden also für jede gegebene Nichtquadratzahl als Determinante alle zuweisbaren Charaktere gleichmäßig in zwei Arten P, Q verteilt: Keinem der Charaktere Q kann eine eigentlich primitive (positive) Form entsprechen, während bei den übrigen P, soweit wir bisher wissen, nichts verhindert, dass sie zu solchen Formen gehören. Bei diesen beiden Arten beachte man besonders die folgende Aussage, die leicht aus ihrem Kriterium folgt: Setzt man einen Charakter aus P mit einem Charakter aus Q zusammen (nach der Regel von Artikel 246, so als entspräche auch diesem ein Geschlecht), so entsteht ein Charakter aus Q; setzt man dagegen zwei Charaktere aus P. oder zwei aus Q zusammen, so gehört der entstehende Charakter zu P. Mithilfe dieses Satzes lässt sich auch bei negativen und uneigentlich primitiven Geschlechtern die Hälfte aller zuweisbaren Charaktere folgendermaßen ausschließen.

I. Bei negativer Determinante D sind die negativen Geschlechter in dieser Hinsicht den positiven völlig entgegengesetzt: Keiner der Charaktere P gehört zu einem negativen eigentlich primitiven Geschlecht, sondern alle diese Geschlechter haben Charaktere aus Q. Gilt nämlich $D' \equiv 1 \pmod 4$, so ist $-D'$ eine positive Zahl der Form $4n+3$; somit gibt es unter a, b, c usw. eine ungerade Anzahl von Zahlen der Form $4n+3$, von denen jede -1 als Nichtrest hat. Daher enthält der Gesamtcharakter der Form $(-1, 0, D)$ in diesem Fall eine ungerade Anzahl von Einzelcharakteren aus Ω, gehört also zu Q. Gilt $D' \equiv 3 \pmod 4$, so findet sich aus demselben Grund unter a, b, c usw. entweder keine Zahl der Form $4n+3$ oder zwei oder vier usw. Da aber in diesem Fall entweder $3, 4$ oder $3, 8$ oder $7, 8$ unter den Einzelcharakteren der Form $(-1, 0, D)$ vorkommt, gehört der Gesamtcharakter dieser Form auch hier $\cdot$ zu Q. Dasselbe folgt ebenso leicht in den übrigen Fällen sodass die negative Form $(-1, 0, D)$ stets einen Charakter aus Q hat. Da diese Form mit jeder anderen negativen eigentlich primitiven Form derselben Determinante zusammengesetzt eine solche positive Form ergibt, kann offenbar keine negative eigentlich primitive Form einen Charakter aus P haben.

II. Für uneigentlich primitive (positive) Geschlechter beweist man ebenso, dass es sich entweder genauso verhält wie bei den eigentlich primitiven oder entgegengesetzt, je nachdem, ob $D \equiv 1$ oder $\equiv 5 \pmod 8$ gilt. Im ersten Fall gilt nämlich auch $D' \equiv 1 \pmod 8$; daher gibt es unter den Zahlen a, b, c usw. entweder keine Zahl der Formen $8n+3$ und $8n+5$ oder zwei oder vier usw. (denn ein Produkt aus beliebig vielen ungeraden Zahlen, unter denen die Zahlen der Formen $8n+3$ und $8n+5$ zusammen in ungerader Anzahl vorkommen, wird stets entweder $\equiv 3$ oder $\equiv 5 \pmod 8$, während das Produkt aller a, b, c usw. entweder D' oder $-D'$ gleich sein muss). Daher enthält der Gesamtcharakter der Form $(2, 1, \frac{1-D}{2})$ entweder keinen Einzelcharakter aus Ω oder zwei oder vier usw., gehört also zu P. Da nun jede uneigentlich primitive (positive) Form der Determinante D als zusammengesetzt aus $(2, 1, \frac{1-D}{2})$ und einer eigentlich primitiven (positiven) Form derselben Determinante angesehen werden kann, hat in diesem Fall offenbar keine uneigentlich primitive (positive) Form einen Charakter aus Q. Im anderen Fall. $D \equiv 5 \pmod 8$ ist alles entgegengesetzt: D', das ebenfalls $\equiv 5$ ist, enthält gewiss eine ungerade Anzahl von Faktoren der Formen $8n+3$ und $8n+5$. Daher gehört der Charakter der Form $(2, 1, \frac{1-D}{2})$ und somit auch der Charakter jeder uneigentlich primitiven (positiven) Form der Determinante

D zu Q; also kann keinem der Charaktere P ein uneigentlich primitives positives Geschlecht entsprechen.

III. Bei negativer Determinante sind schließlich die negativen uneigentlich primitiven Geschlechter wiederum den positiven uneigentlich primitiven entgegengesetzt: Die ersten können keinen Charakter aus P oder aus Q haben, je nachdem, ob $D \equiv 1$ oder $\equiv 5 \pmod 8$ gilt, also je nachdem, ob $-D$ von der Form $8n+7$ oder $8n+3$ ist. Denn die Komposition der Form $(-1, 0, D)$, deren Charakter aus Q ist, mit negativen uneigentlich primitiven Formen derselben Determinante ergibt positive uneigentlich primitive Formen. Sind also bei diesen die Charaktere Q ausgeschlossen, so müssen bei jenen die Charaktere P ausgeschlossen sein und umgekehrt.

Eine besondere Methode, Primzahlen in zwei Quadrate zu zerlegen.

265.

Aus den Untersuchungen der Artikel 257, 258 über die Anzahl der ambigen Klassen, auf denen alles Vorige beruht, lassen sich viele weitere sehr beachtenswerte Folgerungen ziehen, die wir der Kürze wegen weglassen müssen. Die folgende ist jedoch so elegant, dass wir sie nicht übergehen können. Für eine positive Determinante p, die eine Primzahl der Form $4n+1$ ist, haben wir gezeigt, dass es nur eine eigentlich primitive ambige Klasse gibt; daher sind alle eigentlich primitiven ambigen Formen einer solchen Determinante eigentlich äquivalent. Ist also b die unmittelbar unter $\sqrt{p}$ liegende positive ganze Zahl und $p - bb = a'$, so sind die Formen $(1, b, -a')$, $(-1, b, a')$ eigentlich äquivalent; da beide offenbar reduziert sind, liegt die eine in der Periode der anderen. Geben wir der ersten Form in ihrer Periode den Index 0, so muss der Index der zweiten ungerade sein (da die ersten Koeffizienten beider Formen entgegengesetzte Vorzeichen haben); er sei also $= 2m+1$. Sind ferner die Formen mit den Indizes $1, 2, 3$ usw. jeweils

$$(-a', b', a''), \quad (a'', b'', -a'''), \quad (-a''', b''', a'''') \text{ usw.}$$

so entsprechen offenbar den Indizes $2m$, $2m-1$, $2m-2$, $2m-3$ usw. die Formen

$$(a', b, -1), \quad (-a'', b', a'), \quad (a''', b'', -a''), \quad (-a'''', b''', a''') \text{ usw.}$$

Ist also die Form mit dem Index m gleich (A, B, C), so ist sie auch $(-C, B, -A)$; daher gilt $C = -A$ und $p = BB + AA$. Somit lässt sich jede Primzahl der Form $4n+1$ in zwei Quadrate zerlegen (eine Aussage, die wir oben in Artikel 182 aus völlig anderen Prinzipien hergeleitet haben). Zu einer solchen Zerlegung gelangt man durch eine sehr einfache und ganz einheitliche Methode: Man entwickelt die Periode der reduzierten Form, deren Determinante jene Primzahl und deren erster Koeffizient 1 ist, bis zu einer Form, deren äußere Koeffizienten dem Betrag nach gleich und im Vorzeichen entgegengesetzt sind. So erhält man *zum Beispiel* für $p = 233$ $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$ und $233 = 64 + 169$. Ferner muss A offenbar ungerade sein (da $(A, B, -A)$ eigentlich primitiv sein muss), also B gerade. — Da bei einer positiven Determinante p, die eine Primzahl der Form $4n+1$ ist, auch die uneigentlich primitive Ordnung nur eine ambige Klasse enthält, sind offenbar, wenn g

die unmittelbar unter $\sqrt{p}$ liegende ungerade Zahl und $p - gg = 4h$ ist, die reduzierten uneigentlich primitiven Formen $(2, g, -2h)$, $(-2, g, 2h)$ eigentlich äquivalent; somit liegt die eine in der Periode der anderen. Durch ganz ähnliche Überlegungen wie zuvor folgt, dass die Periode der Form $(2, g, -2h)$ eine Form enthält, deren äußere Koeffizienten dem Betrag nach gleich und im Vorzeichen entgegengesetzt sind, sodass sich auch daraus die Zerlegung der Zahl p in zwei Quadrate gewinnen lässt. Die äußeren Koeffizienten dieser Form sind offenbar gerade, der mittlere also ungerade. Da eine Primzahl nur auf eine Weise in zwei Quadrate zerlegt werden kann, ist die nach dieser zweiten Methode gefundene Form entweder $(B, \pm A, -B)$ oder $(-B, \pm A, B)$. So erhält man in unserem Beispiel für $p = 233$ $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$ und $233 = 169 + 64$ wie oben.

EXKURS MIT EINER BEHANDLUNG DER TERNÄREN FORMEN.

266.

Bisher haben wir unsere Untersuchung auf solche Funktionen zweiten Grades beschränkt, die *zwei* Unbestimmte enthalten, und mussten ihnen keine besondere Bezeichnung geben. Doch lässt sich dieser Gegenstand offenbar als ein sehr spezieller Teil der allgemeinsten Untersuchung *über ganzrationale algebraische homogene Funktionen mehrerer Unbestimmter und verschiedener Grade* auffassen. Diese Funktionen können wir zweckmäßig nach ihrem Grad als *Formen zweiten, dritten, vierten Grades usw.*, nach der Anzahl ihrer Unbestimmten dagegen als *binäre, ternäre, quaternäre Formen* usw. unterscheiden. Die Formen, die wir bisher einfach so genannt haben, werden also *binäre Formen zweiten Grades* heißen; Funktionen wie

$$Axx + 2Bxy + Cyy + 2Dxz + 2Eyz + Fzz$$

wobei A, B, C, D, E, F gegebene ganze Zahlen bezeichnen) werden dagegen *ternäre Formen zweiten Grades* heißen, und so weiter. Dieser Abschnitt ist zunächst allein den binären Formen zweiten Grades gewidmet. Doch sind noch mehrere Wahrheiten über sie übrig, und zwar besonders schöne, deren eigentliche Quelle in der Theorie der ternären Formen zweiten Grades zu suchen ist. Deshalb schieben wir hier einen kurzen Exkurs zu dieser Theorie ein und werden aus ihren ersten Grundlagen das behandeln, was zur Vervollständigung der Theorie der binären Formen nötig ist. Wir hoffen, dass dies den Mathematikern willkommener sein wird, als wenn wir jene Wahrheiten entweder unterdrückten oder durch weniger natürliche Methoden gewännen. Eine eingehendere Untersuchung dieses sehr wichtigen Gegenstands müssen wir uns für eine andere Gelegenheit vorbehalten: zum einen, weil seine Fülle schon jetzt die Grenzen dieses Werks weit überschreiten würde, zum anderen, weil wir hoffen dürfen, dass er künftig noch durch bedeutende Fortschritte bereichert wird. Sowohl die quaternären, quinären usw. Formen zweiten Grades als auch alle Formen höherer Grade schließen wir hier gänzlich aus unserem Vorhaben aus[*)]. Es mag genügen, die Mathematiker auf dieses weite Feld aufmerksam zu machen, in dem sie überreiches Material finden werden, um ihre Kräfte zu erproben und die höhere Arithmetik durch hervorragende Fortschritte zu bereichern.

267.

Es wird sehr zur Klarheit beitragen, unter den drei Unbestimmten einer ternären Form ebenso wie bei den binären Formen eine feste Reihenfolge einzuführen, sodass die *erste, zweite* und *dritte Unbestimmte* voneinander unterschieden werden. Bei der Anordnung der einzelnen Glieder der Form werden wir stets folgende Reihenfolge einhalten: An erster Stelle steht das Glied mit dem Quadrat der ersten Unbestimmten; danach folgen nacheinander die Glieder mit dem Quadrat der zweiten, dem Quadrat der dritten, dem doppelten Produkt der zweiten und dritten, dem doppelten Produkt der ersten und dritten sowie dem doppelten Produkt der ersten und zweiten. Schließlich werden wir die bestimmten ganzen Zahlen, mit denen diese Quadrate und

[*)] Deshalb sind im Folgenden immer binäre oder ternäre Formen *zweiten Grades* gemeint, wenn wir einfach von solchen Formen sprechen.

doppelten Produkte multipliziert sind, in derselben Reihenfolge den *ersten, zweiten, dritten, vierten, fünften, sechsten Koeffizienten* nennen. So ist

$$axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

eine richtig angeordnete ternäre Form, deren erste Unbestimmte x, zweite x', dritte x'', erster Koeffizient a usw., vierter b usw. ist. Es wird aber die Schreibweise sehr verkürzen, wenn wir die Unbestimmten einer ternären Form nicht immer durch besondere Buchstaben bezeichnen müssen. Deshalb werden wir dieselbe Form, wenn wir von den Unbestimmten absehen, auch so

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

bezeichnen.

Setzt man

$$\begin{array}{lll} bb - a'a'' = A, & b'b' - aa'' = A', & b''b'' - aa' = A'' \\ ab - b'b'' = B, & a'b' - bb'' = B', & a''b'' - bb' = B'' \end{array}$$

so entsteht eine andere Form

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \dots F$$

die wir die *der Form*

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \dots f$$

adjungierte nennen werden. Bezeichnet man der Kürze halber die Zahl

$$abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b'' \quad \text{mit} \quad D$$

so findet man wiederum

$$\begin{array}{lll} BB - A'A'' = aD, & B'B' - AA'' = a'D, & B''B'' - AA' = a''D \\ AB - B'B'' = bD, & A'B' - BB'' = b'D, & A''B'' - BB' = b''D \end{array}$$

Daraus folgt, dass die der Form F adjungierte Form die Form

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}$$

ist. Die Zahl D, von deren Beschaffenheit die Eigenschaften der ternären Form f vor allem abhängen, werden wir die *Determinante* dieser Form nennen. Auf diese Weise wird die Determinante der Form $F = DD$, also gleich dem Quadrat der Determinante der Form f, der sie adjungiert ist.

So ist *zum Beispiel* der ternären Form $\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix}$ die Form $\begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{pmatrix}$ adjungiert; die Determinante beider $= 1$.

Ternäre Formen mit der Determinante 0 werden aus der folgenden Untersuchung vollständig ausgeschlossen. Denn wie in der bei anderer Gelegenheit ausführlicher zu behandelnden Theorie der ternären Formen gezeigt werden wird, sind sie nur *dem Anschein nach* ternär und in Wirklichkeit binären Formen gleichwertig.

268.

Wird eine ternäre Form f mit der Determinante D und den Unbestimmten x, x', x'' (die erste $= x$ usw.) in eine ternäre Form g mit der Determinante E und den Unbestimmten y, y', y'' durch eine Substitution der Art

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'' \\ x' &= \alpha' y + \beta' y' + \gamma' y'' \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \end{aligned}$$

verwandelt, wobei alle neun Koeffizienten α, β usw. als ganze Zahlen vorausgesetzt werden, so werden wir der Kürze halber die Unbestimmten weglassen und einfach sagen, f gehe in g durch die Substitution (S)

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

über, und f *enthalte* g, oder g *sei in* f *enthalten*. Aus dieser Voraussetzung folgen unmittelbar sechs Gleichungen für die sechs Koeffizienten in g, die wir nicht aufschreiben müssen. Eine leichte Rechnung liefert daraus die folgenden Schlüsse:

I. Bezeichnet man der Kürze halber die Zahl

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'' \quad \text{mit } k$$

so findet man nach den nötigen Umformungen $E = kkD$. Also teilt D die Zahl E, und der Quotient ist ein Quadrat. Die Zahl k spielt somit bei den Transformationen ternärer Formen eine ähnliche Rolle wie die Zahl $\alpha\delta - \beta\gamma$ in Artikel 157 bei den Transformationen binärer Formen: Sie ist eine Quadratwurzel aus dem Quotienten der Determinanten. Daher könnten wir vermuten, dass der Unterschied im Vorzeichen von k auch hier einen wesentlichen Unterschied zwischen eigentlichen und uneigentlichen Transformationen und Enthaltungen begründet. Bei näherer Betrachtung ist aber klar. f geht in g auch durch die Substitution

$$\begin{matrix} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma'' \end{matrix}$$

über; setzt man im Wert von k für α den Wert $-\alpha$, für β den Wert $-\beta$ usw., so erhält man $-k$. Diese Substitution wäre also der Substitution S unähnlich, und jede ternäre Form, die eine andere auf die eine Art enthält, würde sie auch auf die andere Art enthalten. Eine solche Unterscheidung wird deshalb hier ganz ausgeschlossen, da sie bei ternären Formen keinen Nutzen hat.

II. Bezeichnet man mit F, G die den Formen f, g jeweils adjungierten Formen, so werden die Koeffizienten in F durch die Koeffizienten in f bestimmt, und die Koeffizienten in G durch die Werte der Koeffizienten der Form g, die aus den Gleichungen der Substitution S bekannt sind. Drückt man die Koeffizienten der Form f durch Buchstaben aus und vergleicht die Werte der Koeffizienten der Formen F, G,

so bestätigt sich ohne Mühe, dass F die Form G enthält und durch die Substitution (S')

$$\begin{array}{ccc} \beta'\gamma'' - \beta''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\beta'' - \alpha''\beta' \\ \beta''\gamma - \beta\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\beta - \alpha\beta'' \\ \beta\gamma' - \beta'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\beta' - \alpha'\beta \end{array}$$

in sie verwandelt wird. Die Rechnung selbst, die keinerlei Schwierigkeiten bietet, lassen wir weg.

III. Die Form g wird durch die Substitution (S'')

$$\begin{array}{ccc} \beta'\gamma'' - \beta''\gamma', & \beta''\gamma - \beta\gamma'', & \beta\gamma' - \beta'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\beta'' - \alpha''\beta', & \alpha''\beta - \alpha\beta'', & \alpha\beta' - \alpha'\beta \end{array}$$

offenbar in dieselbe Form verwandelt, in die f durch

$$\begin{array}{ccc} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{array}$$

übergeht, also in die Form, die man erhält, indem man jeden Koeffizienten der Form f mit kk multipliziert. Diese Form werden wir mit f' bezeichnen.

IV. Auf genau dieselbe Weise beweist man, dass die Form G durch die Substitution (S''')

$$\begin{array}{ccc} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{array}$$

in die Form übergeht, die aus F entsteht, indem man jeden Koeffizienten mit kk multipliziert. Diese Form werden wir mit F' bezeichnen.

Wir werden sagen, die Substitution S''' entstehe *durch Transposition* der Substitution S. Dann entsteht offenbar auch S wieder durch Transposition der Substitution S''', und S', S'' entstehen jeweils durch Transposition der anderen. — Die Substitution S' kann zweckmäßig als die der Substitution S *adjungierte* bezeichnet werden; somit ist der Substitution S''' die Substitution S'' adjungiert.

269.

Wenn nicht nur die Form f die Form g enthält, sondern auch diese jene, werden die Formen f, g *äquivalent* genannt. In diesem Fall teilt also nicht nur D die Zahl E, sondern auch E die Zahl D, woraus sich leicht ergibt, dass $D = E$ gelten muss. Enthält umgekehrt eine Form f eine Form g mit derselben Determinante, so sind diese beiden Formen äquivalent. Denn mit denselben Bezeichnungen wie im vorigen Artikel und unter Ausschluss des Falls $D = 0$ gilt $k = \pm 1$; somit ist die Form f'. in die g durch die Substitution S'' übergeht, mit f identisch, oder f ist in g enthalten. Ferner sind in diesem Fall offenbar auch die Formen F, G, die den Formen f, g adjungiert sind, einander äquivalent, und die letztere geht durch die Substitution S''' in die erstere über. Werden schließlich umgekehrt die Formen F, G als äquivalent *vorausgesetzt* und geht die erstere durch die Substitution T in die letztere über, so sind

auch die Formen f, g äquivalent: f geht in g durch die der Substitution T adjungierte Substitution über, und g in f durch die Substitution, die durch Transposition der Substitution T entsteht. Denn durch diese beiden Substitutionen geht jeweils die der Form F adjungierte Form in die der Form G adjungierte Form und diese in jene über. Diese beiden Formen entstehen aber aus f, g, indem man jeden Koeffizienten mit D multipliziert; daraus folgt ohne Mühe, dass durch dieselben Substitutionen jeweils f in g. und g in f übergeht.

270.

Wenn eine ternäre Form f eine ternäre Form f' enthält und diese eine Form f'': dann enthält auch f die Form f''. Denn es ist sehr leicht zu sehen, dass, wenn die folgenden Übergänge stattfinden:

f in f' durch Substitution	f' in f'' durch Substitution
$\alpha, \quad \beta, \quad \gamma$	$\delta, \quad \varepsilon, \quad \zeta$
$\alpha', \quad \beta', \quad \gamma'$	$\delta', \quad \varepsilon', \quad \zeta'$
$\alpha'', \quad \beta'', \quad \gamma''$	$\delta'', \quad \varepsilon'', \quad \zeta''$

f durch die Substitution

$$\begin{array}{lll} \alpha\delta+\beta\delta'+\gamma\delta'', & \alpha\varepsilon+\beta\varepsilon'+\gamma\varepsilon'', & \alpha\zeta+\beta\zeta'+\gamma\zeta'' \\ \alpha'\delta+\beta'\delta'+\gamma'\delta'', & \alpha'\varepsilon+\beta'\varepsilon'+\gamma'\varepsilon'', & \alpha'\zeta+\beta'\zeta'+\gamma'\zeta'' \\ \alpha''\delta+\beta''\delta'+\gamma''\delta'', & \alpha''\varepsilon+\beta''\varepsilon'+\gamma''\varepsilon'', & \alpha''\zeta+\beta''\zeta'+\gamma''\zeta'' \end{array}$$

verwandelt wird.

In dem Fall also, dass f zu f' und f' zu f'' äquivalent ist, ist auch die Form f zur Form f'' äquivalent. — Wie diese Sätze auf mehrere Formen anzuwenden sind, ist im Übrigen unmittelbar klar.

271.

Nun ist klar, dass alle ternären Formen ebenso wie die binären in *Klassen* eingeteilt werden können, indem man äquivalente Formen derselben Klasse und nicht äquivalente Formen verschiedenen Klassen zuordnet. Formen mit verschiedenen Determinanten gehören also gewiss zu verschiedenen Klassen, und damit gibt es unendlich viele Klassen ternärer Formen. Ternäre Formen mit derselben Determinante bilden dagegen einmal weniger, einmal mehr Klassen. Als herausragende Eigenschaft dieser Formen ist aber anzusehen, dass *alle Formen mit derselben gegebenen Determinante stets eine endliche Anzahl von Klassen bilden.* Bevor wir diesen sehr wichtigen Satz ausführlicher entwickeln, müssen wir den folgenden wesentlichen Unterschied zwischen ternären Formen erläutern.

Einige ternäre Formen sind so beschaffen, dass durch sie ohne Unterschied positive und negative Zahlen dargestellt werden können, *zum Beispiel* die Form $xx + yy - zz$. Sie werden daher *indefinite Formen* heißen. Durch andere dagegen können keine negativen Zahlen, sondern nur positive dargestellt werden (außer der Null, die man erhält, indem man jede Unbestimmte $= 0$ setzt), wie durch $xx + yy + zz$; deshalb werden sie *positive Formen* heißen. Schließlich können durch andere keine positiven Zahlen dargestellt werden, wie durch $-xx - yy - zz$, weshalb sie *negative Formen* genannt werden. Die positiven und negativen Formen werden zusammen *definite Formen* heißen. Hier folgen nun allgemeine Kriterien, mit denen sich diese Eigenschaften der Formen unterscheiden lassen.

Multipliziert man die ternäre Form

$$f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

mit der Determinante D mit a und bezeichnet die Koeffizienten der zu f adjungierten Form wie in Artikel 267 mit A, A', A'', B, B', B'', so erhält man

$$(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = g$$

Multipliziert man nochmals mit A', ergibt sich

$$A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'x' = h$$

Daraus folgt sofort: Sind sowohl A' als auch aD negative Zahlen, so sind alle Werte von h negativ. Durch die Form f können dann offenbar nur solche Zahlen dargestellt werden, deren Vorzeichen dem von aA' entgegengesetzt ist, *also* mit dem von a übereinstimmt oder dem von D entgegengesetzt ist. In diesem Fall ist f also eine definite Form, und zwar positiv oder negativ, je nachdem, ob a positiv oder negativ ist oder ob D negativ oder positiv ist.

Sind dagegen entweder beide Zahlen aD, A' positiv oder die eine positiv und die andere negativ (keine $= 0$), so sieht man leicht, dass h durch geeignete Wahl der Größen x, x', x'' sowohl positive als auch negative Werte annehmen kann. In diesem Fall kann also f sowohl Werte mit demselben Vorzeichen wie aA' als auch solche mit entgegengesetztem Vorzeichen annehmen und ist daher eine indefinite Form.

Für den Fall, dass $A' = 0$, aber nicht $a = 0$, gilt

$$g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2Bx'')$$

Gibt man x' einen beliebigen Wert (der aber nicht $= 0$ ist) und wählt x'' so, dass $\frac{A''x'}{2B} - x''$ dasselbe Vorzeichen wie Bx' hat (was offenbar möglich ist, da B nicht $= 0$ sein kann; denn daraus würde $BB - A'A'' = aD = 0$ und somit auch $D = 0$ folgen, welchen Fall wir ausschließen), so ist $x'(A''x' - 2Bx'')$ eine positive Größe. Daraus ist leicht zu sehen, dass x so gewählt werden kann, dass g einen negativen Wert erhält. Offenbar lassen sich diese Werte auch so wählen, dass sie, wenn gewünscht, alle ganzzahlig sind. Schließlich kann man bei beliebigen Werten von x', x'' offenbar x so groß wählen, dass g positiv wird. Daraus folgt, dass die Form f in diesem Fall indefinit ist. Ist schließlich $a = 0$, so gilt

$$f = a'x'x' + 2bx'x'' + a''x''x'' + 2x(b''x' + b'x'')$$

Wählt man also x', x'' beliebig, jedoch so, dass $b''x' + b'x''$ nicht $= 0$ ist (was offenbar möglich ist, sofern nicht b' und b'' zugleich $= 0$ sind; dann wäre aber $D = 0$), so sieht man ohne Mühe, dass x so gewählt werden kann, dass f sowohl positive als auch negative Werte annimmt. Also ist f auch in diesem Fall eine indefinite Form.

Ebenso, wie wir hier aus den Zahlen aD, A' die Beschaffenheit der Form f beurteilt haben, können wir auch aD und A'' verwenden: f ist definit, wenn sowohl aD als auch A'' negativ sind, und in allen übrigen Fällen indefinit. Auf genau dieselbe Weise kann man zu diesem Zweck auch die Zahlen $a'D$ und A, oder $a'D$ und A'', oder $a''D$ und A, oder schließlich $a''D$ und A' betrachten.

Aus allem folgt, dass bei einer definiten Form die sechs Zahlen A, A', A'', aD, $a'D$, $a''D$ negativ sind. Bei einer positiven Form sind dabei a, a', a'' positiv und D negativ; bei einer negativen dagegen a, a', a'' negativ und D positiv. Also zerfallen alle ternären Formen mit einer gegebenen positiven Determinante in negative und indefinite, alle mit einer negativen Determinante dagegen in positive und indefinite. Positive Formen mit positiver Determinante oder negative Formen mit negativer Determinante gibt es überhaupt nicht. — Aus denselben Überlegungen sieht man leicht, dass einer definiten Form stets eine definite, und zwar *negative*, einer indefiniten dagegen eine indefinite Form adjungiert ist.

Da alle durch eine gegebene ternäre Form darstellbaren Zahlen offenbar auch durch jede zu ihr äquivalente Form dargestellt werden können, sind die ternären Formen derselben Klasse entweder alle indefinit oder alle positiv oder alle negativ. Deshalb dürfen wir diese Bezeichnungen der Formen auch auf ganze Klassen übertragen.

272.

Den im vorigen Artikel aufgestellten Satz, dass alle ternären Formen mit gegebener Determinante in eine *endliche* Anzahl von Klassen zerfallen, werden wir mit einer ähnlichen Methode wie bei den binären Formen behandeln. Wir zeigen zunächst, wie jede ternäre Form auf eine einfachere Form reduziert werden kann, und dann, dass die Anzahl der einfachsten Formen (zu denen solche Reduktionen führen) bei jeder gegebenen Determinante endlich ist. Nehmen wir allgemein an, es sei eine ternäre Form $f = \left(\begin{smallmatrix} a,\ a',\ a'' \\ b,\ b',\ b'' \end{smallmatrix}\right)$ mit der Determinante D (verschieden von Null) gegeben, die durch die Substitution (S)

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

in eine äquivalente Form $g = \left(\begin{smallmatrix} m,\ m',\ m'' \\ n,\ n',\ n'' \end{smallmatrix}\right)$ übergeht. Unsere Aufgabe besteht darin, α, β, γ usw. so zu bestimmen, dass die Form g einfacher als f wird. Die den Formen f, g adjungierten Formen seien jeweils $\left(\begin{smallmatrix} A,\ A',\ A'' \\ B,\ B',\ B'' \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} M,\ M',\ M'' \\ N,\ N',\ N'' \end{smallmatrix}\right)$. und werden mit F, G bezeichnet. Nach Artikel 269 geht dann F in G durch die der Substitution S adjungierte Substitution über, G dagegen in F durch die Substitution, die durch Transposition von S entsteht. Die Zahl

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma''$$

die entweder $= +1$ oder $= -1$ sein muss, werden wir mit k bezeichnen. Unter diesen Voraussetzungen bemerken wir:

I. Setzt man $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, so gilt

$$\begin{aligned} m &= a\alpha\alpha + 2b''\alpha\alpha' + a'\alpha'\alpha', \\ m' &= a\beta\beta + 2b''\beta\beta' + a'\beta'\beta', \\ m'' &= a'' \\ n &= b\beta' + b'\beta, \\ n' &= b\alpha' + b'\alpha, \\ n'' &= a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta' \end{aligned}$$

Außerdem muss $\alpha\beta' - \beta\alpha'$ entweder $= +1$ oder $= -1$ sein. Daraus ist klar, dass die binäre Form (a, b'', a') mit der Determinante A'' durch die Substitution α, β, α', β' in die binäre Form (m, n'', m') mit der Determinante M'' verwandelt wird und ihr daher wegen $\alpha\beta' - \beta\alpha' = \pm 1$ äquivalent ist. Also gilt $M'' = A''$, was sich auch unmittelbar leicht bestätigen lässt. Wenn also (a, b'', a') nicht schon eine einfachste Form ihrer Klasse ist, dürfen wir α, β, α', β' so bestimmen, dass (m, n'', m') eine einfachere Form ist. Aus der Theorie der Äquivalenz binärer Formen folgt dabei leicht, dass dies so geschehen kann, dass m nicht größer als $\sqrt{-\frac{4}{3}A''}$ ist, wenn A'' negativ ist, oder nicht größer als $\sqrt{A''}$, wenn A'' positiv ist, oder $m = 0$, wenn $A'' = 0$. Somit lässt sich in allen Fällen der (absolute) Wert von m gewiss unter oder wenigstens

bis auf $\sqrt{\pm\frac{4}{3}A''}$ herabsetzen. Auf diese Weise wird also die Form f auf eine andere reduziert, deren erster Koeffizient, wenn möglich, kleiner ist und deren adjungierte Form denselben dritten Koeffizienten hat wie die Form F, die f adjungiert ist. Darin besteht die *erste Reduktion.*

II. Setzt man dagegen $\alpha = 1, \beta = 0, \gamma = 0, \alpha' = 0, \alpha'' = 0$, so gilt $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$. Die der Substitution S adjungierte Substitution ist also

$$\begin{array}{rrr} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta' \end{array}$$

durch die F in G übergeht. Somit gilt

$$\begin{aligned} m &= a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\beta'' + b''\beta' \\ m' &= a'\beta'\beta' + 2b\beta'\beta'' + a''\beta''\beta'' \\ m'' &= a'\gamma'\gamma' + 2b\gamma'\gamma'' + a''\gamma''\gamma'' \\ n &= a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'' \\ M' &= A'\gamma''\gamma'' - 2B\gamma'\gamma'' + A''\gamma'\gamma' \\ N &= -A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma' \\ M'' &= A'\beta''\beta'' - 2B\beta'\beta'' + A''\beta'\beta' \end{aligned}$$

Daraus folgt, dass die binäre Form (A'', B, A') mit der Determinante Da durch die Substitution β', $-\gamma'$, $-\beta''$, γ'' in die Form (M'', N, M') mit der Determinante Dm übergeht und ihr daher (wegen $\beta'\gamma'' - \gamma'\beta'' = \pm 1$ oder wegen $Da = Dm$) äquivalent ist. Wenn also (A'', B, A') nicht schon eine einfachste Form ihrer Klasse ist, lassen sich die Koeffizienten β', γ', β'', γ'' so bestimmen, dass $(M''. N, M')$ einfacher ist. Dies ist stets so möglich, dass M'' ohne Rücksicht auf das Vorzeichen nicht größer als $\sqrt{\pm\frac{4}{3}Da}$ ist. Auf diese Weise wird die Form f also auf eine andere mit demselben ersten Koeffizienten reduziert, deren adjungierte Form aber, wenn möglich, einen kleineren dritten Koeffizienten hat als die Form F, die f adjungiert ist. Darin besteht die *zweite Reduktion.*

III. Ist also f eine ternäre Form, auf die weder die erste noch die zweite Reduktion anwendbar ist, *das heißt*, die durch keine von beiden in eine einfachere Form verwandelt werden kann: so gilt notwendig sowohl $aa <$ oder $= \frac{4}{3}A''$ als auch $A''A'' <$ oder $= \frac{4}{3}aD$, ohne Rücksicht auf das Vorzeichen. Also ist $a^4 <$ oder $= \frac{16}{9}A''A''$, somit $a^4 <$ oder $= \frac{64}{27}aD$, $a^3 <$ oder $= \frac{64}{27}D$, und $a <$ oder $= \frac{4}{3}\sqrt[3]{D}$; daraus wiederum $A''A'' <$ oder $= \frac{16}{9}\sqrt[3]{D^4}$ und $A'' <$ oder $= \frac{4}{3}\sqrt[3]{D^2}$. Solange also a oder A'' diese Grenzen noch überschreitet, muss die eine oder die andere der vorigen Reduktionen auf die Form f anwendbar sein. — Dieser Schluss darf jedoch nicht umgekehrt werden, da es durchaus häufig vorkommt, dass eine ternäre Form, deren erster Koeffizient sowie der dritte Koeffizient ihrer adjungierten Form schon unter jenen Grenzen liegen, dennoch durch die eine oder die andere Reduktion weiter vereinfacht werden kann.

IV. Wendet man aber auf eine beliebige gegebene ternäre Form mit der Determinante D abwechselnd die erste und die zweite Reduktion an, *das heißt*, auf sie selbst

die erste oder zweite, auf die daraus entstandene Form die zweite oder erste, auf die nächste daraus entstandene Form wieder die erste oder zweite usw., so muss man offenbar schließlich zu einer Form gelangen, auf die keine der beiden mehr anwendbar ist. Denn sowohl die absoluten Beträge der ersten Koeffizienten der so entstehenden Formen als auch die der dritten Koeffizienten ihrer adjungierten Formen bleiben fortwährend abwechselnd gleich und nehmen ab. Dieser Vorgang muss deshalb schließlich irgendwo enden, da man sonst zwei unendliche Folgen fortwährend abnehmender Zahlen hätte. Damit haben wir einen bemerkenswerten Satz gewonnen: *Jede ternäre Form mit der Determinante D kann auf eine andere äquivalente Form reduziert werden, deren erster Koeffizient nicht größer als* $\frac{4}{3}\sqrt[3]{D}$ *und der dritte Koeffizient ihrer adjungierten Form nicht größer als* $\frac{4}{3}\sqrt[3]{D^2}$ *ist, ohne Rücksicht auf das Vorzeichen, sofern die gegebene Form diese Eigenschaften nicht schon selbst besitzt.* — Statt des ersten Koeffizienten der Form f und des dritten der zu f adjungierten Form hätten wir auf genau dieselbe Weise entweder den ersten Koeffizienten der Form selbst und den zweiten ihrer adjungierten Form behandeln können; oder den zweiten der Form selbst und den ersten oder dritten ihrer adjungierten Form; oder den dritten der Form selbst und den ersten oder zweiten ihrer adjungierten Form. Auf allen diesen Wegen wären wir ebenso zum vorgesehenen Ziel gelangt. Es ist aber zweckmäßig, beständig bei einer Methode zu bleiben, damit die zugehörigen Operationen leichter in einen festen Algorithmus gefasst werden können. Schließlich bemerken wir, dass sich für die beiden Koeffizienten, die wir unter feste Grenzen herabzusetzen gelehrt haben. noch kleinere Grenzen bestimmen lassen, wenn man die definiten von den indefiniten Formen trennt; für unser gegenwärtiges Vorhaben ist dies jedoch nicht nötig.

273.

Hier folgen einige Beispiele, die die vorigen Regeln näher erläutern.

Beispiel 1. Es sei $f = \left(\begin{smallmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{smallmatrix}\right)$; dann gilt $F = \left(\begin{smallmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{smallmatrix}\right)$, $D = -1$. Da $(19, 1, 21)$ eine reduzierte binäre Form ist, zu der keine andere mit einem ersten Koeffizienten kleiner als 19 äquivalent ist, lässt sich die erste Reduktion hier nicht anwenden. Die Theorie der Äquivalenz binärer Formen zeigt aber, dass die binäre Form $(A'', B, A') = (-398, 257, -166)$ in die einfachere äquivalente Form $(-2, 1, -10)$ verwandelt werden kann, in die sie durch die Substitution $2, 7, 3, 11$ übergeht. Setzt man also $\beta' = 2$, $\gamma' = -7$, $\beta'' = -3$, $\gamma'' = 11$, so muss auf die Form f die Substitution $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11 \end{smallmatrix}\right\}$ angewendet werden, durch die sie in $\left(\begin{smallmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{smallmatrix}\right) \ldots f'$ übergeht. Der dritte Koeffizient der dieser Form adjungierten Form ist -2; in dieser Hinsicht ist also f' als einfacher als f anzusehen.

Auf die Form f' lässt sich die erste Reduktion anwenden. Da nämlich die binäre Form $(19, -82, 354)$ in $(1, 0, 2)$ durch die Substitution $13, 4, 3, 1$ verwandelt wird: muss auf die Form f' die Substitution $\left\{\begin{smallmatrix} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$ angewendet werden, durch die sie in $\left(\begin{smallmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{smallmatrix}\right) \ldots f''$ übergeht.

Auf die Form f'', der die Form $\left(\begin{smallmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{smallmatrix}\right)$ adjungiert ist, lässt sich wieder die zweite Reduktion anwenden. Denn $(-2, -95, -4513)$ geht durch die Substitution $47, 1, -1, 0$ in $(-1, 1, -2)$ über: deshalb muss auf f'' die Substitution $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0 \end{smallmatrix}\right\}$ angewendet werden, durch die sie in $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right) \ldots f'''$ übergeht. Deren erster Koeffizient kann durch die erste Reduktion nicht weiter verkleinert werden, ebenso wenig der dritte Koeffizient der ihr adjungierten Form durch die zweite.

Beispiel 2. Es sei die Form $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right) \ldots f$ gegeben, der die Form $\left(\begin{smallmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{smallmatrix}\right)$ adjungiert ist und deren Determinante $= 2$. Wendet man abwechselnd die zweite und die erste Reduktion an, so erhält man nacheinander

Substitutionen	überführen	in
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{smallmatrix}\right\}$	f	$\left(\begin{smallmatrix} 10, & 2, & 2 \\ -1, & 0, & -4 \end{smallmatrix}\right) = f'$
$\left\{\begin{smallmatrix} 0, & -1, & 0 \\ 1, & -2, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$	f'	$\left(\begin{smallmatrix} 2, & 2, & 2 \\ 2, & -1, & 0 \end{smallmatrix}\right) = f''$
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 2, & -1 \end{smallmatrix}\right\}$	f''	$\left(\begin{smallmatrix} 2, & 2, & 2 \\ -2, & 1, & -2 \end{smallmatrix}\right) = f'''$
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$	f'''	$\left(\begin{smallmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{smallmatrix}\right) = f''''$

Die Form f'''' lässt sich durch die erste oder zweite Reduktion nicht weiter herabsetzen.

274.

Hat man eine ternäre Form, deren erster Koeffizient sowie der dritte Koeffizient ihrer adjungierten Form durch die vorigen Methoden so weit wie möglich herabgesetzt worden sind: so liefert die folgende Methode eine weitere Reduktion.

Verwendet man dieselben Bezeichnungen wie in Artikel 272 und setzt $\alpha = 1$, $\alpha' = 0$, $\beta' = 1$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, *das heißt*, verwendet man die Substitution

$$\begin{matrix} 1, & \beta, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1 \end{matrix}$$

so gilt

$$\begin{aligned} m &= a, \quad m' = a' + 2b''\beta + a\beta\beta, \\ m'' &= a'' + 2b\gamma' + 2b'\gamma + a\gamma\gamma + 2b''\gamma\gamma' + a'\gamma'\gamma' \\ n &= b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma, \\ n' &= b' + a\gamma + b''\gamma', \quad n'' = b'' + a\beta \end{aligned}$$

und außerdem

$$M'' = A'', \quad N = B - A''\gamma', \quad N' = B' - N\beta - A''\gamma$$

Durch eine solche Substitution werden also die Koeffizienten a, A'', die durch die vorigen Reduktionen verkleinert worden sind, nicht verändert. Die Aufgabe besteht daher darin, durch geeignete Wahl von β, γ, γ' die übrigen Koeffizienten zu verkleinern. Dazu bemerken wir zunächst: Ist $A'' = 0$, so darf man annehmen, dass auch $a = 0$ gilt. Denn wäre a nicht $= 0$, so ließe sich die erste Reduktion noch einmal anwenden, da jede binäre Form mit der Determinante 0 zu einer Form der Art $(0, 0, h)$ äquivalent ist, also zu einer Form, deren erster Koeffizient $= 0$ ist (siehe Artikel 215). Auf genau dieselbe Weise darf man annehmen, dass auch $A'' = 0$ gilt, wenn $a = 0$, sodass entweder keine der Zahlen a, A'' gleich 0 ist oder beide.

Im ersten Fall ist klar, dass β, γ, γ' so gewählt werden können, dass ohne Rücksicht auf das Vorzeichen n'', N, N' jeweils nicht größer als $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$ sind. So geht im ersten Beispiel des vorigen Artikels die letzte Form $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right)$, der die Form $\left(\begin{smallmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{smallmatrix}\right)$ adjungiert ist, durch die Substitution $\left\{\begin{smallmatrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$ in $\left(\begin{smallmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right) \ldots f''''$ über, der die Form $\left(\begin{smallmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ adjungiert ist.

Im zweiten Fall, in dem $a = A'' = 0$ und damit auch $b'' = 0$ gilt, erhält man

$$\begin{aligned} m &= 0, \quad m' = a', \quad m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'\gamma' \\ n &= b + a'\gamma' + b'\beta, \quad n' = b', \quad n'' = 0 \end{aligned}$$

Also gilt

$$D = a'b'b' = m'n'n'$$

und man sieht leicht, dass β und γ' so bestimmt werden können, dass n gleich dem absolut kleinsten Rest von b nach dem Modul wird, der der größte gemeinsame Teiler

von a', b' ist; das heißt, dass n ohne Rücksicht auf das Vorzeichen nicht größer als die Hälfte dieses Teilers wird, also $n = 0$, sobald a', b' teilerfremd sind. Sind β, γ' auf diese Weise bestimmt, so lässt sich der Wert von γ so wählen, dass m'' ohne Rücksicht auf das Vorzeichen nicht größer als b' ist. Dies wäre zwar unmöglich, wenn $b' = 0$; dann wäre aber $D = 0$, welchen Fall wir ausgeschlossen haben. So erhält man für die letzte Form in *Beispiel* 2 des vorigen Artikels $n = -2 - \beta + 2\gamma'$, woraus man durch $\beta = -2$, $\gamma' = 0$ den Wert $n = 0$ erhält. Ferner gilt $m'' = 2 - 2\gamma$, und mit $\gamma = 1$ erhält man $m'' = 0$. Wir haben also die Substitution $\left\{\begin{smallmatrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$, durch die jene Form in $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right) \ldots f''''''$ übergeht.

275.

Hat man eine Folge äquivalenter ternärer Formen f, f', f'', f''' usw. und Transformationen jeder dieser Formen in die folgende: so lässt sich aus den Transformationen der Form f in f' und der Form f' in f'' nach Artikel 270 eine Transformation der Form f in f'' herleiten. Aus dieser und der Transformation der Form f'' in f''' folgt eine Transformation der Form f in f''' usw. Offenbar lässt sich so eine Transformation der Form f in jede andere Form der Folge finden. Da sich außerdem aus einer Transformation der Form f in eine beliebige andere äquivalente Form g eine Transformation der Form g in f herleiten lässt (S'' aus S, Artikel 268, 269), kann man auf diese Weise eine Transformation jeder Form der Folge f', f'' usw. in die erste, f, bestimmen. — So findet man für die Formen des ersten Beispiels im vorigen Artikel die Substitutionen

$$\begin{array}{rrr|rrr|rrr} 13, & 4, & 0 & 13, & 188, & -4 & 13, & -20, & 16 \\ 6, & 2, & -7 & 6, & 87, & -2 & 6, & -9, & 7 \\ -9, & -3, & 11 & -9, & -130, & 3 & -9, & 14, & -11 \end{array}$$

durch die f jeweils in f'', f''', f'''' übergeht, und aus der letzten Substitution diese $\left\{\begin{smallmatrix} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3 \end{smallmatrix}\right\}$, durch die f'''' in f übergeht. Ebenso erhält man für *Beispiel* 2 des vorigen Artikels die Substitutionen

$$\begin{array}{rrr|rrr} 1, & -1, & 1 & 2, & -3, & -1 \\ -3, & 4, & -3 & 3, & 1, & 0 \\ 10, & -14, & 11 & 2, & 4, & 1 \end{array}$$

durch die jeweils die Form $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right)$ in $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right)$ und diese in jene übergeht.

276.

Satz. *Die Anzahl der Klassen, in die alle ternären Formen mit gegebener Determinante zerfallen, ist stets endlich.*

Beweis. I. Die Anzahl aller Formen $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ mit gegebener Determinante D, bei denen $a = 0$, $b'' = 0$ gelten, b nicht größer als die Hälfte des größten gemeinsamen Teilers der Zahlen a', b' ist und a'' nicht größer als b' ist, ist offenbar endlich. Da nämlich $a'b'b' = D$ gelten muss, kann b' nur die Werte $+1$, -1 und die mit positivem und negativem Vorzeichen versehenen Wurzeln der Quadrate annehmen, die D teilen (falls es außer 1 noch andere gibt). Die Anzahl dieser Werte ist endlich. Für jeden Wert von b' ist aber der Wert von a' bestimmt, und die Werte von b, a'' sind offenbar auf eine endliche Anzahl beschränkt.

II. Ebenso ist die Anzahl aller Formen $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ mit der Determinante D endlich, bei denen a nicht $= 0$ und nicht größer als $\frac{4}{3}\sqrt[3]{\pm D}$ ist; $b''b'' - aa' = A''$ nicht $= 0$ und nicht größer als $\frac{4}{3}\sqrt[3]{D^2}$ ist; b'' nicht größer als $\frac{1}{2}a$ ist; und $ab - b'b'' = B$ und $a'b' - bb'' = B'$ nicht größer als $\frac{1}{2}A''$ sind. Denn die Anzahl aller Kombinationen der Werte von a, b'', A'', B, B' ist endlich. Sind diese einzeln bestimmt, so sind auch die übrigen Koeffizienten der Form, a', b, b', a'', sowie die Koeffizienten der adjungierten Form

$$bb - a'a'' = A, \quad b'b' - aa'' = A', \quad a''b'' - bb' = B''$$

durch folgende Gleichungen bestimmt:

$$\begin{aligned}
a' &= \frac{b''b'' - A''}{a}, \quad A' = \frac{BB - aD}{A''}, \\
A &= \frac{B'B' - a'D}{A''}, \quad B'' = \frac{BB' + b''D}{A''} \\
b &= \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, \\
b' &= \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''} \\
a'' &= \frac{b'b' - A'}{a} = \frac{bb - A}{a'} = \frac{bb' + B''}{b''}
\end{aligned}$$

Nun erhält man alle jene Formen, indem man aus sämtlichen Kombinationen der Werte von a, b'', A'', B, B' diejenigen wählt, für die auch a', a'', b, b' ganzzahlige Werte annehmen; ihre Anzahl ist daher offenbar endlich.

III. Alle Formen in I und II bilden somit eine endliche Anzahl von Klassen. Diese kann sogar kleiner sein als die Anzahl der Formen selbst, wenn einige von ihnen einander äquivalent sind. Da nun nach den vorigen Untersuchungen jede ternäre Form mit der Determinante D einer jener Formen äquivalent sein muss, *das heißt*, zu einer der von ihnen gebildeten Klassen gehören muss: umfassen diese Klassen alle Formen mit der Determinante D, *das heißt*, alle ternären Formen mit der Determinante D zerfallen in eine endliche Anzahl von Klassen. *W.z.b.w.*

277.

Die Regeln, mit denen alle Formen in I und II des vorigen Artikels bestimmt werden können, folgen unmittelbar aus ihrer Beschreibung; einige Beispiele werden daher genügen. Für $D = 1$ ergeben sich durch die verschiedenen Vorzeichen diese sechs Formen I.

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$$

Bei den Formen II können a und A'' keine anderen Werte als $+1$ und -1 haben. Für jede der vier daraus entstehenden Kombinationen müssen b'', B und $B' = 0$ gesetzt werden; daraus entstehen vier Formen

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

Ebenso erhält man für $D = -1$ sechs Formen I und vier Formen II,

$$\begin{pmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & -1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}; \quad \begin{pmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} -1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$$

Für $D = 2$ entstehen sechs Formen I

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$$

und acht Formen II

$$\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

Die Anzahl der Klassen, die sich in diesen drei Fällen aus diesen Formen ergeben, ist jedoch viel kleiner als die Anzahl der Formen. Es lässt sich nämlich leicht bestätigen:

I. Die Form $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ geht in

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

jeweils durch die Substitutionen

$$\begin{array}{rrr|rrr|rrr|rrr} 1, & 0, & 0 & 0, & 0, & 1 & 0, & 0, & 1 & 1, & 0, & -1 \\ 0, & 1, & 0 & 0, & 1, & -1 & 0, & 1, & 1 & 1, & 1, & -1 \\ 0, & 0, & -1 & \pm 1, & 1, & 0 & \pm 1, & -1, & -1 & 0, & -1, & 1 \end{array}$$

über, die Form $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ dagegen in $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ allein durch Vertauschung der Unbestimmten. Jene zehn ternären Formen mit der Determinante 1 reduzieren sich also auf diese beiden $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$; für die erste kann man, wenn man möchte, auch $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ nehmen. Da die erstere Form indefinit und die letztere definit

ist, ist klar, dass jede indefinite ternäre Form mit der Determinante 1 zur Form $xx + 2yz$ und jede definite zu $-xx - yy - zz$ äquivalent ist.

II. Auf genau dieselbe Weise findet man, dass jede indefinite ternäre Form mit der Determinante -1 zur Form $-xx + 2yz$ und jede definite zu $xx + yy + zz$ äquivalent ist.

III. Für die Determinante 2 können von den acht Formen (II) sofort die zweite, sechste und siebte verworfen werden, da sie aus der ersten allein durch Vertauschung der Unbestimmten entstehen. Aus demselben Grund können auch die fünfte, die ebenso aus der dritten, und die achte, die aus der vierten entsteht, verworfen werden. Die drei übrigen bilden mit den sechs Formen I drei Klassen. Denn $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{smallmatrix}\right)$ geht in $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right)$ durch die Substitution $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1 \end{smallmatrix}\right\}$ über, und die Form $\left(\begin{smallmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ in

$$\left(\begin{smallmatrix} 0, & 2, & 1 \\ 0, & 1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 2, & 1 \\ 0, & -1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 0, & 2, & -1 \\ 0, & 1, & 0 \end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix} 0, & 2, & -1 \\ 0, & -1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

jeweils durch die Substitutionen

$$\begin{array}{ccc|ccc|ccc|ccc|ccc} 1, & 0, & 1 & 1, & 0, & -1 & 1, & 0, & 0 & 1, & 0, & 0 & 1, & 0, & 0 \\ 1, & 2, & 0 & 1, & 2, & 0 & 1, & 2, & -1 & 1, & 2, & 1 & 0, & 1, & 2 \\ 1, & 1, & 0 & 1, & 1, & 0 & 1, & 1, & -1 & 1, & 1, & 1 & 0, & 1, & 1 \end{array}$$

über. Jede ternäre Form mit der Determinante 2 lässt sich also auf eine dieser drei reduzieren

$$\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{smallmatrix}\right)$$

Anstelle der ersten kann man, wenn man möchte, auch $\left(\begin{smallmatrix} 2, & 0, & 0 \\ 1, & 0, & 0 \end{smallmatrix}\right)$ nehmen. Offenbar muss jede definite ternäre Form zur dritten, $-xx - yy - 2zz$, äquivalent sein, da die beiden ersten indefinit sind. Jede indefinite ist zur ersten oder zweiten äquivalent: zur ersten, $2xx + 2yz$, wenn ihr erster, zweiter und dritter Koeffizient alle gerade sind (denn man sieht leicht, dass eine solche Form durch jede Substitution wieder in eine Form derselben Art übergeht und daher nicht zur zweiten Form äquivalent sein kann); zur zweiten, $xx + yy - 2zz$, dagegen, wenn ihr erster, zweiter und dritter Koeffizient nicht alle gerade, sondern einer, zwei oder alle ungerade sind (in eine solche Form kann nämlich aus demselben Grund die erste Form $2xx + 2yz$ durch keine Substitution verwandelt werden). Was also in den Beispielen der Artikel 273, 274 geschah, dass die definite Form $\left(\begin{smallmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{smallmatrix}\right)$ mit der Determinante -1 auf $xx + yy + zz$ und die indefinite Form $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right)$ mit der Determinante 2 auf $2xx - 2yz$ oder, was auf dasselbe hinausläuft, auf $2xx + 2yz$ reduziert wurde, hätte man aus den vorigen Untersuchungen im Voraus erkennen können.

278.

Durch eine ternäre Form mit den Unbestimmten x, x', x'' werden sowohl Zahlen *dargestellt*, indem man x, x', x'' bestimmte Werte gibt, als auch binäre Formen durch Substitutionen der Art

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u$$

wobei m, n, m' usw. bestimmte Zahlen und t, u die Unbestimmten der dargestellten Form bezeichnen. Eine vollständige Theorie der ternären Formen würde daher die Lösung folgender Probleme erfordern: I. Alle Darstellungen einer gegebenen Zahl durch eine gegebene ternäre Form finden. II. Alle Darstellungen einer gegebenen binären Form durch eine gegebene ternäre Form finden. III. Entscheiden, ob zwei gegebene ternäre Formen mit derselben Determinante äquivalent sind, und wenn ja, alle Transformationen der einen in die andere finden. IV. Entscheiden, ob eine gegebene ternäre Form eine andere gegebene Form mit größerer Determinante enthält, und wenn ja, alle Transformationen jener in diese angeben. Diese Probleme, die viel schwieriger sind als die entsprechenden bei den binären Formen, werden wir an anderer Stelle ausführlicher behandeln. Hier beschränken wir unsere Untersuchung darauf zu zeigen, wie sich das erste Problem auf das zweite und das zweite auf das dritte zurückführen lässt. Für einige sehr einfache Fälle, die besonders die Theorie der binären Formen erhellen, werden wir die Lösung des dritten zeigen. Das vierte schließen wir hier ganz aus.

279.

Lemma. *Zu drei beliebigen gegebenen ganzen Zahlen a, a', a'' (die aber nicht alle $= 0$ sind): sechs andere B, B', B'', C, C', C'' finden, sodass gilt*

$$B'C'' - B''C' = a, \qquad B''C - BC'' = a', \qquad BC' - B'C = a''$$

Lösung. Es sei α der größte gemeinsame Teiler von a, a', a''. und man wähle ganze Zahlen A, A', A'' so, dass

$$Aa + A'a' + A''a'' = \alpha$$

Ferner wähle man drei ganze Zahlen $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ beliebig mit der einzigen Bedingung, dass die drei Zahlen $\mathfrak{C}'A'' - \mathfrak{C}''A'$, $\mathfrak{C}''A - \mathfrak{C}A''$, $\mathfrak{C}A' - \mathfrak{C}'A$, die wir jeweils mit b, b', b'' und deren größten gemeinsamen Teiler wir mit β bezeichnen werden, nicht alle $= 0$ sind. Dann setze man

$$a'b'' - a''b' = \alpha\beta C, \qquad a''b - ab'' = \alpha\beta C', \qquad ab' - a'b = \alpha\beta C''$$

Offenbar sind C, C', C'' ganze Zahlen. Wählt man schließlich ganze Zahlen $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ so, dass

$$\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta$$

setzt

$$\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = h$$

und bestimmt

$$B = \alpha\mathfrak{B} - hA, \qquad B' = \alpha\mathfrak{B}' - hA', \qquad B'' = \alpha\mathfrak{B}'' - hA''$$

so erfüllen diese Werte von B, B', B'', C, C', C'' die geforderten Gleichungen.

Denn man findet

$$aB + a'B' + a''B'' = 0$$
$$bA + b'A' + b''A'' = 0 \quad \text{also} \quad bB + b'B' + b''B'' = \alpha\beta$$

Aus den Werten von C', C'' ergibt sich nun

$$\begin{aligned}\alpha\beta(B'C'' - B''C') &= ab'B' - a'bB' - a''bB'' + ab''B'' \\ &= a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\beta a\end{aligned}$$

also $B'C'' - B''C' = a$; ebenso findet man $B''C - BC'' = a'$, $BC' - B'C = a''$. *Q.E.F.* — Die Analyse, durch die diese Lösung gefunden wurde, sowie die Methode, aus einer Lösung alle zu finden, müssen wir hier weglassen.

280.

Nehmen wir an, die binäre Form

$$att + 2btu + cuu \ldots \varphi$$

mit der Determinante $= D$ werde durch die ternäre Form f mit den Unbestimmten x, x', x'' dargestellt, indem man

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u$$

setzt, und der Form f sei die Form F mit den Unbestimmten X, X', X'' adjungiert. Dann bestätigt eine Rechnung leicht (wenn man die Koeffizienten der Formen f, F durch eigene Buchstaben bezeichnet), oder es folgt auch unmittelbar aus Art. 268. II., dass die Zahl D durch F dargestellt wird, indem man

$$X = m'n'' - m''n', \qquad X' = m''n - mn'', \qquad X'' = mn' - m'n$$

setzt. Diese Darstellung der Zahl D kann man zweckmäßig der Darstellung der Form φ durch f *adjungiert* nennen. Haben die Werte von X, X', X'' keinen gemeinsamen Teiler, so nennen wir diese Darstellung von D der Kürze halber *eigentlich*, andernfalls *uneigentlich*. Dieselben Bezeichnungen geben wir auch der Darstellung der Form φ durch f, der jene Darstellung von D adjungiert ist. Das Auffinden aller eigentlichen Darstellungen der Zahl D durch die Form F beruht nun auf folgenden Punkten:

I. Jede Darstellung von D durch F lässt sich aus einer Darstellung irgendeiner Form mit der Determinante D durch die Form f ableiten, *d.h.*, sie ist einer solchen Darstellung adjungiert.

Sei nämlich irgendeine Darstellung von D durch F durch $X = L$, $X' = L'$, $X'' = L''$ gegeben. Nach dem Lemma des vorigen Artikels wähle man m, m', m'', n, n', n'' so, dass

$$m'n'' - m''n' = L, \qquad m''n - mn'' = L', \qquad mn' - m'n = L''$$

gilt, und die Form f gehe durch die Substitution

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u$$

in die binäre Form $\varphi = att + 2btu + cuu$ über. Dann sieht man leicht, dass D die Determinante der Form φ ist und dass ihrer Darstellung durch f die vorgelegte Darstellung von D durch F adjungiert ist.

Beispiel. Sei $f = xx + x'x' + x''x''$, also $F = -XX - X'X' - X''X''$; ferner $D = -209$, und ihre Darstellung durch F sei durch $X = 1$, $X' = 8$, $X'' = 12$ gegeben. Daraus ergeben sich für m, m', m'', n, n', n'' die Werte $-20, 1, 1, -12, 0, 1$, in dieser Reihenfolge, und $\varphi = 402tt + 482tu + 145uu$.

II. Sind φ, χ eigentlich äquivalente binäre Formen, so ist jede Darstellung von D durch F, die einer Darstellung der Form φ durch f adjungiert ist, auch einer Darstellung der Form χ durch f adjungiert.

Seien p, q die Unbestimmten der Form χ; die Form φ gehe in χ durch die eigentliche Substitution $t = \alpha p + \beta q$, $u = \gamma p + \delta q$ über, und irgendeine Darstellung der Form φ durch f sei

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u \ldots (R)$$

Dann sieht man ohne Schwierigkeit: Setzt man

$$\begin{array}{lll} \alpha m + \gamma n = g, & \alpha m' + \gamma n' = g', & \alpha m'' + \gamma n'' = g'' \\ \beta m + \delta n = h, & \beta m' + \delta n' = h', & \beta m'' + \delta n'' = h'' \end{array}$$

so wird die Form χ durch f dargestellt, indem man

$$x = gp + hq, \qquad x' = g'p + h'q, \qquad x'' = g''p + h''q \ldots (R')$$

setzt. Durch Rechnung findet man (wegen $\alpha\delta - \beta\gamma = 1$)

$$g'h'' - g''h' = m'n'' - m''n', \quad g''h - gh'' = m''n - mn'', \quad gh' - g'h = mn' - m'n$$

d.h., den Darstellungen R, R' ist dieselbe Darstellung von D durch F adjungiert.

So ist im vorigen Beispiel die Form φ äquivalent zu $\chi = 13pp - 10pq + 18qq$, in die sie durch die eigentliche Substitution $t = -3p + q$, $u = 5p - 2q$ übergeht. Daraus ergibt sich die Darstellung der Form χ durch f als $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$, aus der wieder dieselbe Darstellung der Zahl -209 folgt, von der wir ausgegangen waren.

III. Können schließlich zwei binäre Formen φ, χ mit der Determinante D und den Unbestimmten t, u; p, q durch f dargestellt werden, und ist einer Darstellung der einen dieselbe eigentliche Darstellung von D durch F adjungiert wie einer Darstellung der anderen, so sind diese Formen notwendig eigentlich äquivalent. Nehmen wir an, φ werde durch f dargestellt, indem man

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u$$

setzt, χ dagegen, indem man

$$x = gp + hq. \qquad x' = g'p + h'q, \qquad x'' = g''p + h''q$$

setzt, und es gelte

$$\begin{array}{c} m'n'' - m''n' = g'h'' - g''h' = L \\ m''n - mn'' = g''h - gh'' = L' \\ mn' - m'n = gh' - g'h = L'' \end{array}$$

Man wähle ganze Zahlen l, l', l'' so, dass $Ll + L'l' + L''l'' = 1$ gilt, und setze

$$\begin{array}{lll} n'l'' - n''l' = M, & n''l - nl'' = M', & nl' - n'l = M'' \\ l'm'' - l''m' = N, & l''m - lm'' = N', & lm' - l'm = N'' \end{array}$$

Schließlich setze man

$$\begin{array}{ll} gM + g'M' + g''M'' = \alpha, & hM + h'M' + h''M'' = \beta \\ gN + g'N' + g''N'' = \gamma, & hN + h'N' + h''N'' = \delta \end{array}$$

Daraus folgt leicht

$$\alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g$$
$$\beta m + \delta n = h - l(hL + h'L' + h''L'') = h$$

und ebenso

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''$$

Daraus folgt. $mt + nu$, $m't + n'u$, $m''t + n''u$ gehen durch die Substitution

$$t = \alpha p + \beta q, \quad u = \gamma p + \delta q \ldots (S)$$

in $gp + hq$, $g'p + h'q$, $g''p + h''q$ über. Also geht φ offenbar durch die Substitution S in dieselbe Form über wie f, wenn man

$$x = gp + hq, \qquad x' = g'p + h'q, \qquad x'' = g''p + h''q$$

setzt, also in die Form χ, der sie somit äquivalent ist. Schließlich erhält man durch die nötigen Einsetzungen leicht

$$\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1$$

Die Substitution S ist also eigentlich, und die Formen φ, χ sind eigentlich äquivalent.

Aus diesen Bemerkungen folgen die folgenden Regeln, um alle eigentlichen Darstellungen von D durch F zu finden: Man bestimme alle Klassen binärer Formen mit der Determinante D und wähle aus jeder eine beliebige Form. Man suche alle eigentlichen Darstellungen jeder dieser Formen durch f (wobei man diejenigen verwirft, die nicht durch f dargestellt werden können) und leite aus jeder dieser Darstellungen die Darstellungen der Zahl D durch F ab. Aus I und II ist offenbar, dass man so alle möglichen eigentlichen Darstellungen erhält, die Lösung also vollständig ist; aus III, dass Transformationen von Formen aus verschiedenen Klassen sicher verschiedene Darstellungen liefern.

281.

Das Auffinden der *uneigentlichen* Darstellungen einer gegebenen Zahl D durch die Form F lässt sich leicht auf den vorigen Fall zurückführen. Ist nämlich D durch kein Quadrat (außer 1) teilbar, so gibt es offenbar überhaupt keine solchen Darstellungen. Andernfalls, wenn D durch die Quadrate $\lambda\lambda, \mu\mu, \nu\nu$ usw. teilbar ist, findet man alle uneigentlichen Darstellungen von D durch F, indem man alle eigentlichen Darstellungen der Zahlen $\frac{D}{\lambda\lambda}$, $\frac{D}{\mu\mu}$, $\frac{D}{\nu\nu}$ usw. durch dieselbe Form bestimmt und die Werte der Unbestimmten jeweils mit λ, μ, ν usw. multipliziert.

So hängt das Auffinden aller Darstellungen einer gegebenen Zahl durch eine gegebene ternäre Form, *die einer ternären Form adjungiert ist*, vom zweiten Problem ab. Auf diesen Fall, der auf den ersten Blick weniger weit zu reichen scheint, lassen sich die übrigen folgendermaßen zurückführen. Sei D die Zahl, die durch die Form $\left(\begin{smallmatrix} g,g',g'' \\ h,h',h'' \end{smallmatrix}\right)$

mit der Determinante Δ dargestellt werden soll; dieser sei die Form $\left(\begin{smallmatrix} G,G',G'' \\ H,H',H'' \end{smallmatrix}\right) = f$ adjungiert. Dieser wiederum ist die Form $\left(\begin{smallmatrix} \Delta g,\Delta g',\Delta g'' \\ \Delta h,\Delta h',\Delta h'' \end{smallmatrix}\right) = F$ adjungiert, und offenbar sind die Darstellungen der Zahl ΔD durch F (deren Bestimmung vom Vorangegangenen abhängt) genau dieselben wie die Darstellungen der Zahl D durch die vorgelegte Form. — Haben ferner alle Koeffizienten der Form f einen gemeinsamen Teiler μ, so sind offenbar alle Koeffizienten der Form F durch $\mu\mu$ teilbar. Also muss auch ΔD durch $\mu\mu$ teilbar sein (andernfalls gäbe es keine Darstellungen); und die Darstellungen der Zahl D durch die vorgelegte Form stimmen mit den Darstellungen der Zahl $\frac{\Delta D}{\mu\mu}$ durch die Form überein, die aus F entsteht, indem man jeden Koeffizienten durch $\mu\mu$ teilt. Diese Form ist derjenigen adjungiert, die aus f entsteht, indem man jeden Koeffizienten durch μ teilt.

Schließlich bemerken wir, dass diese Lösung des ersten Problems in dem einzigen Fall, wo $D = 0$ ist, nicht anwendbar ist; denn hier verteilen sich nicht alle binären Formen mit der Determinante D auf eine endliche Anzahl von Klassen. Diesen Fall werden wir unten nach anderen Grundsätzen lösen.

282.

Das Auffinden der Darstellungen einer gegebenen binären Form, deren Determinante nicht $= 0$ ist[*)], durch eine gegebene ternäre Form beruht auf den folgenden Bemerkungen:

I. Aus jeder eigentlichen Darstellung der binären Form $(p, q, r) = \varphi$ mit der Determinante D durch die ternäre Form f mit der Determinante Δ lassen sich ganze Zahlen B, B' ableiten, für die

$$BB \equiv \Delta p, \qquad BB' \equiv -\Delta q, \qquad B'B' \equiv \Delta r \text{ (mod. } D)$$

gilt, *d.h.*, ein Wert des Ausdrucks $\sqrt{\Delta(p, -q, r)}$(mod. D). Eine eigentliche Darstellung der Form φ durch f sei

$$x = \alpha t + \beta u, \qquad x' = \alpha' t + \beta' u, \qquad x'' = \alpha'' t + \beta'' u$$

(wobei $x, x', x''; t, u$ die Unbestimmten der Formen f, φ bezeichnen). Man wähle ganze Zahlen $\gamma, \gamma', \gamma''$ so, dass

$$(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma''$$

$= k$ entweder $= +1$ oder $= -1$ ist, und die Form f gehe durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

in die Form $\left(\begin{smallmatrix} a,a',a'' \\ b,b',b'' \end{smallmatrix}\right) = g$ über, der die Form $\left(\begin{smallmatrix} A,A',A'' \\ B,B',B'' \end{smallmatrix}\right) = G$ adjungiert sei. Dann sind offenbar $a = p$, $b'' = q$, $a' = r$, $A'' = D$, und Δ ist die Determinante der Form g; also gilt

$$BB = \Delta p + A'D, \qquad BB' = -\Delta q + B''D, \qquad B'B' = \Delta r + AD$$

So wird *z.B.* die Form $19tt + 6tu + 41uu$ durch $xx + x'x' + x''x''$ dargestellt, indem man $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$ setzt. Setzt man dann $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$, so erhält man $B = -171$, $B' = 27$, also den Wert $(-171, 27)$ des Ausdrucks $\sqrt{-1(19, -3, 41)}$(mod. 770).

Daraus folgt nun, dass, wenn $\Delta(p, -q, r)$ kein quadratischer Rest von D ist, φ durch keine ternäre Form mit der Determinante Δ eigentlich dargestellt werden kann. Sind also Δ, D teilerfremd, so muss Δ eine charakteristische Zahl der Form φ sein.

II. Da man $\gamma, \gamma', \gamma''$ auf unendlich viele verschiedene Arten bestimmen kann, ergeben sich daraus auch immer wieder andere Werte von B, B'. Sehen wir uns ihren Zusammenhang an. Nehmen wir an, auch $\delta, \delta', \delta''$ seien so beschaffen, dass

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$$

[*)] Diesen Fall, der eine etwas andere Methode erfordert, übergehen wir hier der Kürze halber.

entweder $= +1$ oder $= -1$ ist, und die Form f gehe durch die Substitution

$$\begin{array}{lll} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

in $\left(\begin{smallmatrix} \mathfrak{a},\mathfrak{a}',\mathfrak{a}'' \\ \mathfrak{b},\mathfrak{b}',\mathfrak{b}'' \end{smallmatrix}\right) = \mathfrak{g}$ über, der die Form $\left(\begin{smallmatrix} \mathfrak{A},\mathfrak{A}',\mathfrak{A}'' \\ \mathfrak{B},\mathfrak{B}',\mathfrak{B}'' \end{smallmatrix}\right) = \mathfrak{G}$ adjungiert sei. Dann sind $g, \mathfrak{g}$ äquivalent, also auch G und $\mathfrak{G}$. Wendet man die Regeln aus Art. 269, 270 an[*)], so findet man, wenn man

$$\begin{aligned} (\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' &= \zeta \\ (\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' &= \eta \end{aligned}$$

setzt, dass die Form $\mathfrak{G}$ in G übergeht, und zwar durch die Substitution

$$\begin{array}{lll} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k} \end{array}$$

Daraus folgt

$$B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}, \qquad B' = \zeta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}'$$

und also wegen $\mathfrak{k}k = \pm 1$ entweder $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$ oder $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). Im ersten Fall nennen wir die Werte (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ äquivalent, im zweiten entgegengesetzt. Von der Darstellung der Form φ sagen wir, dass sie zu jedem Wert des Ausdrucks $\sqrt{\Delta}(p, -q, r)(\text{mod. } D)$ *gehört*, der sich aus ihr nach der Methode in I ableiten lässt. Alle Werte, zu denen dieselbe Darstellung gehört, sind also entweder äquivalent oder entgegengesetzt.

III. Wenn umgekehrt, wie oben in I, die Darstellung der Form φ durch f mittels $x = \alpha t + \beta u$ usw. zu dem Wert (B, B') gehört, der aus ihr mithilfe der Transformation

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

abgeleitet wird, so gehört dieselbe auch zu jedem anderen Wert $(\mathfrak{B}, \mathfrak{B}')$, der dem ersten äquivalent oder entgegengesetzt ist; *d.h.*, anstelle von $\gamma, \gamma', \gamma''$ kann man andere ganze Zahlen $\delta, \delta', \delta''$ wählen, für die die Gleichung (Ω), nämlich

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1$$

gilt und die so beschaffen sind, dass die Koeffizienten mit den Nummern 4 und 5 in der Form, die derjenigen adjungiert ist, in die f durch die Substitution (S)

$$\begin{array}{lll} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

[*)] Man leite aus der Transformation der Form f in g die Transformation der Form g in f ab; aus dieser und der Transformation der Form f in $\mathfrak{g}$ die Transformation der Form g in $\mathfrak{g}$; schließlich aus dieser durch Transposition die Transformation der Form $\mathfrak{G}$ in G.

übergeht, jeweils $= \mathfrak{B}, \mathfrak{B}'$ werden. Man setze nämlich

$$\pm B = \mathfrak{B} + \eta D, \qquad \pm B' = \mathfrak{B}' + \zeta D$$

(wobei hier und im Folgenden die oberen oder unteren Vorzeichen zu nehmen sind, je nachdem die Werte $(B.\ B')$, $(\mathfrak{B}, \mathfrak{B}')$ äquivalent oder entgegengesetzt sind). Dann sind ζ, η ganze Zahlen. Die Form g gehe durch die Substitution

$$\begin{array}{lll} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{array}$$

in die Form $\mathfrak{g}$ über. Man sieht leicht, dass ihre Determinante Δ ist und dass in der adjungierten Form die Koeffizienten mit den Nummern 4 und 5 jeweils $= \mathfrak{B}, \mathfrak{B}'$ werden. Setzt man aber

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta''$$

so sieht man ohne Schwierigkeit, dass f durch die Substitution (S) in $\mathfrak{g}$ übergeht und dass die Gleichung (Ω) erfüllt ist. *Q. E. D.*

283.

Aus diesen Grundsätzen ergibt sich die folgende Methode, um alle eigentlichen Darstellungen der binären Form

$$\varphi = ptt + 2qtu + ruu$$

mit der Determinante D durch die ternäre Form f mit der Determinante Δ zu finden.

I. Man bestimme alle verschiedenen (*d.h.*, nicht äquivalenten) Werte des Ausdrucks $\sqrt{\Delta}(p, -q, r)(\text{mod. } D)$. Für den Fall, dass φ eine primitive Form und Δ zu D teilerfremd ist, wurde dieses Problem oben (Art. 233) gelöst. Die übrigen Fälle lassen sich sehr leicht darauf zurückführen; der Kürze halber können wir dies hier aber nicht ausführlich erklären. Wir bemerken nur, dass, wenn Δ zu D teilerfremd ist, der Ausdruck $\Delta(p, -q, r)$ nur dann ein quadratischer Rest von D sein kann, wenn φ eine primitive Form ist. Setzt man nämlich

$$\Delta p = BB - DA', \qquad -\Delta q = BB' - DB'', \qquad \Delta r = B'B' - DA$$

so erhält man

$$(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$$

Durch Ausmultiplizieren und Einsetzen von $qq - pr$ für D folgt daraus

$$(qq - pr)(B''B'' - AA') - \Delta(Ap + 2B''q + A'r) + \Delta\Delta = 0$$

Man schließt daraus leicht, dass, wenn p, q, r einen gemeinsamen Teiler hätten, dieser auch $\Delta\Delta$ teilen würde; dann könnte aber Δ nicht zu D teilerfremd sein. Also können p, q, r keinen gemeinsamen Teiler haben; mit anderen Worten, φ ist eine primitive Form.

II. Bezeichnen wir die Anzahl dieser Werte mit m, und nehmen wir an, unter ihnen seien n Werte, die sich selbst entgegengesetzt sind (wobei wir $n = 0$ setzen, wenn es keine solchen gibt). Dann bilden die übrigen $m - n$ Werte offenbar Paare entgegengesetzter Werte (da wir voraussetzen, dass alle Werte vollständig vorliegen). Man verwerfe aus jedem Paar entgegengesetzter Werte einen beliebigen; insgesamt bleiben dann $\frac{1}{2}(m+n)$ Werte übrig. So sind *z.B.* von den acht Werten des Ausdrucks $\sqrt{-1}(19, -3, 41) \text{ (mod. } 770)$, nämlich $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$, $(-39, -237)$, $(-171, 27)$, $(-269, 83)$, $(-291, 127)$, die letzten vier als den ersten vier entgegengesetzt zu verwerfen. Ist ferner (B, B') ein sich selbst entgegengesetzter Wert, so sind offenbar $2B$, $2B'$ und daher auch $2\Delta p$, $2\Delta q$, $2\Delta r$ durch D teilbar. Sind also Δ, D teilerfremd, so sind auch $2p$, $2q$, $2r$ durch D teilbar. Da nach I in diesem Fall auch p, q, r keinen gemeinsamen Teiler haben können, muss auch 2 durch D teilbar sein. Dies ist nur möglich, wenn D entweder $= \pm 1$ oder $= \pm 2$ ist. Für alle Werte von D, die größer als 2 sind, ist daher stets $n = 0$, wenn Δ zu D teilerfremd ist.

III. Ist dies geschehen, so muss offenbar jede eigentliche Darstellung der Form φ durch f zu einem der übrig gebliebenen Werte gehören, und zwar zu genau einem. Man muss diese Werte also der Reihe nach durchgehen und die zu jedem gehörenden Darstellungen bestimmen. Um die Darstellungen zu finden, die zu einem *gegebenen* Wert (B, B') gehören, bestimme man zuerst die ternäre Form $g = \left(\begin{smallmatrix} a, a', a'' \\ b, b', b'' \end{smallmatrix}\right)$ mit der

Determinante $= \Delta$, in der $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$ gilt. Die Werte von a'', b, b' erhält man daraus mithilfe der Gleichungen in II von Art. 276. Aus diesen sieht man leicht, dass in dem Fall, wo Δ, D teilerfremd sind, $b, b'\, a''$ notwendig ganze Zahlen sind (denn diese drei Zahlen ergeben sowohl mit D als auch mit Δ multipliziert ganze Zahlen). Ist nun entweder einer der Koeffizienten b, b', b'' gebrochen, oder sind die Formen f, g nicht äquivalent, so kann es keine Darstellungen der Form φ durch f geben, die zu (B, B') gehören. Sind dagegen b, b', a'' ganze Zahlen und die Formen f, g äquivalent, so liefert jede Transformation der ersten in die zweite, etwa

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

eine solche Darstellung, nämlich

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

Offenbar kann es keine Darstellung dieser Art geben, die sich nicht aus einer Transformation ableiten ließe. So ist nun der Teil des zweiten Problems, der die *eigentlichen* Darstellungen sucht, auf das dritte Problem zurückgeführt.

IV. Verschiedene Transformationen der Form f in g liefern stets verschiedene Darstellungen, außer in dem einzigen Fall, wo der Wert (B, B') sich selbst entgegengesetzt ist. In diesem Fall liefern immer zwei Transformationen eine einzige Darstellung. Nehmen wir nämlich an, f gehe auch in g über durch die Substitution

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

(die dieselbe Darstellung wie die vorige Transformation liefert). Bezeichnen wir mit k, $\mathfrak{k}$, ζ, η dieselben Zahlen wie in II des vorigen Artikels, so gilt

$$B = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$$

Nimmt man also an, dass k, $\mathfrak{k}$ entweder beide $= +1$ oder beide $= -1$ sind, so ist (da wir den Fall $D = 0$ ausgeschlossen haben) $\zeta = 0$, $\eta = 0$. Daraus folgt leicht $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$. Die beiden Transformationen können also nur dann verschieden sein, wenn von den Zahlen k, $\mathfrak{k}$ die eine $+1$, die andere -1 ist. Dann gilt $B \equiv -B$, $B' \equiv -B'$, (mod. D), oder der Wert (B, B') ist sich selbst entgegengesetzt.

V. Aus den oben (Art. 271) angegebenen Kriterien für definite und indefinite Formen folgt leicht: Ist Δ positiv, D negativ und φ eine negative Form, so ist g eine negative definite Form. Ist dagegen Δ positiv und entweder D positiv oder D negativ und φ eine positive Form, so ist g eine indefinite Form. Da nun f, g sicher nur dann äquivalent sein können, wenn sie in dieser Eigenschaft übereinstimmen, können offenbar binäre Formen mit positiver Determinante sowie positive binäre Formen nicht durch eine negative ternäre Form eigentlich dargestellt werden; ebenso wenig negative binäre Formen durch eine indefinite ternäre Form mit positiver Determinante. Eine ternäre Form der ersten bzw. zweiten Art stellt also nur binäre Formen

der zweiten bzw. ersten Art dar. Ebenso folgt, dass eine definite ternäre Form mit negativer Determinante (*d.h.*, eine positive Form) nur positive binäre Formen darstellt, eine indefinite dagegen nur negative binäre Formen und Formen mit positiver Determinante.

284.

Da die *uneigentlichen* Darstellungen der binären Form φ mit der Determinante D durch die ternäre Form f, der die Form F adjungiert ist, diejenigen sind, aus denen uneigentliche Darstellungen der Zahl D durch die Form F folgen, kann φ offenbar nur dann durch f uneigentlich dargestellt werden, wenn D Quadratfaktoren enthält. Nehmen wir an, alle Quadrate, die D teilen (außer 1), seien ee, $e'e'$, $e''e''$ usw. (ihre Anzahl ist endlich, da wir voraussetzen, dass nicht $D = 0$ ist). Dann liefert jede uneigentliche Darstellung der Form φ durch f eine Darstellung der Zahl D durch F, in der die Werte der Unbestimmten eine der Zahlen e, e', e'' usw. als größten gemeinsamen Teiler haben. In diesem Sinn sagen wir der Kürze halber, dass jede uneigentliche Darstellung der Form φ zum Quadratteiler ee oder $e'e'$ oder $e''e''$ usw. *gehört*. Alle Darstellungen der Form φ, die zu demselben *gegebenen* Quadratteiler ee gehören (dessen Wurzel e wir positiv nehmen), findet man nun nach den folgenden Regeln. Aus ihrem synthetischen Beweis, den wir hier der Kürze halber vorziehen, lässt sich leicht die Analysis wiederherstellen, durch die sie gefunden wurden.

Erstens bestimme man alle binären Formen mit der Determinante $\frac{D}{ee}$, die in die Form φ übergehen, und zwar durch eine eigentliche Substitution der Form $T = \kappa t + \lambda u$, $U = \mu u$. Dabei bezeichnen T, U die Unbestimmten einer solchen Form; t, u die Unbestimmten der Form φ; κ, μ positive ganze Zahlen (deren Produkt also $= e$ ist); λ eine positive ganze Zahl kleiner als μ (oder auch null). Diese Formen findet man mit den zugehörigen Transformationen folgendermaßen:

Man setze κ der Reihe nach jedem positiven Teiler von e gleich (einschließlich 1 und e) und $\mu = \frac{e}{\kappa}$. Für jedes Paar bestimmter Werte von κ, μ gebe man λ alle ganzzahligen Werte von 0 bis $\mu - 1$. So erhält man sicher alle Transformationen. Die Form, die durch eine beliebige Substitution $T = \kappa t + \lambda u$, $U = \mu u$ in φ übergeht, findet man nun, indem man die Form bestimmt, in die φ durch $t = \frac{1}{\kappa}T - \frac{\lambda}{e}U$, $u = \frac{1}{\mu}U$ übergeht. So erhält man die zu den einzelnen Transformationen gehörenden Formen; von allen diesen behalte man aber nur diejenigen, in denen alle drei Koeffizienten ganze Zahlen sind[*)].

Zweitens sei Φ eine dieser Formen, die in φ durch die Substitution $T = \kappa t + \lambda u$, $U = \mu u$ übergeht. Man suche alle *eigentlichen* Darstellungen der Form Φ durch f (falls es solche gibt) und bezeichne sie allgemein durch

$$x = \mathfrak{A}T + \mathfrak{B}U, \quad x' = \mathfrak{A}'T + \mathfrak{B}'U, \quad x'' = \mathfrak{A}''T + \mathfrak{B}''U \quad \dots \quad (\mathfrak{R})$$

Schließlich leite man aus jeder $(\mathfrak{R})$ die Darstellung

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u \quad \dots \quad (\rho)$$

[*)] Dürften wir dieses Problem hier ausführlicher behandeln, so könnten wir die Lösung erheblich verkürzen. Es ist sofort klar, dass man für κ nur solche Teiler von e nehmen muss, deren Quadrat den ersten Koeffizienten der Form φ teilt. Dieses Problem, aus dem sich auch einfachere Lösungen der Probleme in Art. 213, 214 ableiten lassen, behalten wir uns für eine andere geeignete Gelegenheit vor.

mithilfe der Gleichungen

$$\begin{array}{llll} \alpha = \kappa\mathfrak{A}, & \alpha' = \kappa\mathfrak{A}', & \alpha'' = \kappa\mathfrak{A}'' & \dots \quad (R) \\ \beta = \lambda\mathfrak{A} + \mu\mathfrak{B}, & \beta' = \lambda\mathfrak{A}' + \mu\mathfrak{B}', & \beta'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}'' & \end{array}$$

ab. Man behandle die übrigen nach der ersten Regel gefundenen Formen (falls es weitere gibt) genauso wie die Form Φ, sodass aus jeder ihrer eigentlichen Darstellungen weitere Darstellungen abgeleitet werden. Ich behaupte, dass man so sämtliche Darstellungen der Form φ erhält, die zum Teiler ee gehören, und zwar jede genau einmal.

Beweis. I. Dass die ternäre Form f durch jede Substitution (ρ) tatsächlich in φ übergeht, ist so offensichtlich, dass keine weitere Erklärung nötig ist. Dass aber jede Darstellung (ρ) uneigentlich ist und zum Teiler ee gehört, folgt daraus, dass die Zahlen $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$, $\alpha\beta' - \alpha'\beta$ jeweils $= e(\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B})$ werden. Ihr größter gemeinsamer Teiler ist also offenbar e (weil $(\mathfrak{R})$ eine eigentliche Darstellung ist).

II. Wir werden zeigen, dass sich aus jeder gegebenen Darstellung (ρ) der Form φ eine eigentliche Darstellung einer Form mit der Determinante $\frac{D}{ee}$ finden lässt, die unter den nach der ersten Regel gefundenen Formen enthalten ist. Mit anderen Worten: Aus den gegebenen Werten von $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ lassen sich ganzzahlige Werte von κ, λ, μ, die den vorgeschriebenen Bedingungen genügen, und Werte von $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$, die den Gleichungen (R) genügen, ableiten, und zwar auf genau eine Art. Zunächst folgt sofort aus den ersten drei Gleichungen in (R), dass man für κ den positiv genommenen größten gemeinsamen Teiler von α, α', α'' nehmen muss (denn da $\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B}$ keinen gemeinsamen Teiler haben dürfen, können auch $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ keinen haben). Damit sind auch $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ bestimmt, ebenso $\mu = \frac{e}{\kappa}$ (das notwendig ganzzahlig ist, wie man leicht sieht). Nehmen wir an, drei ganze Zahlen $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$ seien so gewählt, dass $\mathfrak{a}\mathfrak{A} + \mathfrak{a}'\mathfrak{A}' + \mathfrak{a}''\mathfrak{A}'' = 1$ gilt; und schreiben wir der Kürze halber k für $\mathfrak{a}\mathfrak{B} + \mathfrak{a}'\mathfrak{B}' + \mathfrak{a}''\mathfrak{B}''$. Dann folgt aus den letzten drei Gleichungen (R), dass $\mathfrak{a}\beta + \mathfrak{a}'\beta' + \mathfrak{a}''\beta'' = \lambda + \mu k$ gelten muss. Daraus sieht man sofort, dass es für λ genau einen Wert zwischen den Grenzen 0 und $\mu - 1$ gibt. Da damit auch $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ bestimmte Werte erhalten, bleibt nur zu zeigen, dass diese stets ganze Zahlen sind. Es gilt aber

$$\begin{aligned} \mathfrak{B} = \frac{1}{\mu}(\beta - \lambda\mathfrak{A}) &= \frac{1}{\mu}(\beta(1 - \mathfrak{a}\mathfrak{A}) - \mathfrak{A}(\mathfrak{a}'\beta' + \mathfrak{a}''\beta'')) + \mathfrak{A}k \\ &= \frac{1}{\mu}(\mathfrak{a}''(\mathfrak{A}''\beta - \mathfrak{A}\beta'') - \mathfrak{a}'(\mathfrak{A}\beta' - \mathfrak{A}'\beta)) + \mathfrak{A}k \\ &= \frac{1}{e}(\mathfrak{a}''(\alpha''\beta - \alpha\beta'') - \mathfrak{a}'(\alpha\beta' - \alpha'\beta)) + \mathfrak{A}k \end{aligned}$$

Dieser Wert ist daher offenbar ganzzahlig. Ebenso bestätigt man leicht, dass auch $\mathfrak{B}'$, $\mathfrak{B}''$ ganzzahlige Werte erhalten. — Aus diesen Überlegungen folgt, dass keine uneigentliche Darstellung der Form φ durch f, die zum Teiler ee gehört, existieren kann, die man mit der angegebenen Methode entweder gar nicht oder mehrmals erhält.

Behandelt man nun die übrigen Quadratteiler von D genauso und bestimmt die zu jedem gehörenden Darstellungen, so erhält man sämtliche uneigentlichen Darstellungen der Form φ durch f.

Aus dieser Lösung folgt ferner leicht, dass der am Ende des vorigen Artikels für eigentliche Darstellungen angegebene Satz auch für uneigentliche gilt: Allgemein lässt sich keine positive binäre Form mit negativer Determinante durch eine negative ternäre Form darstellen usw. Ist nämlich φ eine solche binäre Form, die wegen jenes Satzes nicht durch f eigentlich dargestellt werden kann, so können auch alle Formen mit den Determinanten $\frac{D}{ee}$, $\frac{D}{e'e'}$ usw., die φ enthalten, nicht durch f eigentlich dargestellt werden. Denn alle diese Formen haben eine Determinante mit demselben Vorzeichen wie φ. Sind diese Determinanten negativ, so sind sie alle positive oder alle negative Formen, je nachdem φ zur ersten oder zur zweiten Art gehört.

285.

Zu den Fragen, die unser drittes Problem bilden (auf das die beiden ersten oben zurückgeführt wurden), können wir hier nur wenig sagen: Bei zwei gegebenen ternären Formen derselben Determinante ist zu entscheiden, ob sie äquivalent sind, und im ersten Fall sind alle Transformationen der einen in die andere zu finden. Eine vollständige Lösung, wie wir sie für die entsprechenden Probleme bei binären Formen gegeben haben, stößt hier auf noch größere Schwierigkeiten. Wir beschränken unsere Untersuchung daher auf einige besondere Fälle, derentwegen dieser Exkurs hauptsächlich unternommen wurde.

I Für die Determinante +1 haben wir oben gezeigt, dass alle ternären Formen in zwei Klassen zerfallen, von denen die eine alle indefiniten, die andere alle definiten (negativen) Formen enthält. Daraus folgt sofort, dass zwei beliebige ternäre Formen mit der Determinante 1 äquivalent sind, wenn entweder beide definit oder beide indefinit sind; ist dagegen die eine definit, die andere indefinit, so sind sie nicht äquivalent (der letzte Teil gilt offenbar allgemein für Formen jeder Determinante). — Ebenso sind zwei beliebige Formen mit der Determinante −1 sicher äquivalent, wenn entweder beide definit oder beide indefinit sind. — Zwei definite Formen mit der Determinante 2 sind stets äquivalent. Zwei indefinite sind nicht äquivalent, wenn in der einen die ersten drei Koeffizienten alle gerade, in der anderen aber nicht alle gerade sind; in den übrigen Fällen (wenn in beiden die ersten drei Koeffizienten alle gerade sind oder in keiner) sind sie äquivalent. — Auf diese Weise könnten wir noch viel mehr besondere Sätze angeben, wenn oben (Art. 277) mehr Beispiele ausgearbeitet worden wären.

II. Bezeichnen f, f' äquivalente ternäre Formen, so lässt sich in allen diesen Fällen auch eine Transformation der einen in die andere finden. Denn in allen Fällen haben wir oben in jeder Klasse ternärer Formen eine recht kleine Anzahl von Formen angegeben, auf deren eine sich jede Form derselben Klasse nach einheitlichen Methoden zurückführen lässt; dort haben wir auch gezeigt, wie sich alle diese auf eine einzige zurückführen lassen. Sei F diese Form in der Klasse, in der f, f' liegen. Dann kann man nach den oben gegebenen Regeln Transformationen der Formen f, f' in F und auch der Form F in f, f' finden. Daraus lassen sich nach Art. 270 Transformationen der Form f in f' und der Form f' in f ableiten.

III. Es bliebe also nur zu zeigen, wie man aus einer Transformation der ternären Form f in eine andere f' alle möglichen Transformationen ableiten kann. Dieses Problem hängt von einem einfacheren ab, nämlich alle Transformationen der ternären Form f in sich selbst zu finden. Geht nämlich f durch mehrere Substitutionen (τ), (τ'), (τ'') usw. in sich selbst und durch die Substitution (t) in f' über, so erhält man offenbar durch Verbindung der Transformation (t) mit (τ), (τ'), (τ'') usw. nach Art. 270 Transformationen, durch die f jeweils in f' übergeht. Ferner beweist man durch Rechnung leicht, dass jede Transformation der Form f in f' auf diese Weise aus der Verbindung der gegebenen Transformation (t) der Form f in f' mit irgendeiner (und zwar *genau einer*) Transformation der Form f in sich selbst abgeleitet werden kann. Verbindet man also die gegebene Transformation der Form f in f' mit *allen* Transformationen der Form f in sich selbst, so erhält man *alle* Transformationen der Form f in f', und zwar jede genau einmal.

Die Untersuchung aller Transformationen der Form f in sich selbst beschränken wir hier auf den Fall, dass f eine definite Form ist, deren Koeffizienten mit den Nummern $4, 5, 6$ alle $= 0$ sind*). Sei also $f = \left(\begin{smallmatrix} a, a', a'' \\ 0, 0, 0 \end{smallmatrix}\right)$, und bezeichnen wir alle Substitutionen, durch die f in sich selbst übergeht, allgemein durch

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

sodass die Gleichungen

$$\begin{aligned} a\alpha\alpha + a'\alpha'\alpha' + a''\alpha''\alpha'' &= a \qquad \ldots \quad (\Omega) \\ a\beta\beta + a'\beta'\beta' + a''\beta''\beta'' &= a' \\ a\gamma\gamma + a'\gamma'\gamma' + a''\gamma''\gamma'' &= a'' \\ a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' &= 0 \\ a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' &= 0 \\ a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' &= 0 \end{aligned}$$

erfüllt sein müssen. Nun sind drei Fälle zu unterscheiden:

I. Sind a, a', a'' (die dasselbe Vorzeichen haben) alle verschieden, so nehmen wir $a < a'$, $a' < a''$ an (bei einer anderen Größenfolge erhält man dieselben Schlüsse auf genau dieselbe Weise). Dann verlangt die erste Gleichung in (Ω) offenbar $\alpha' = \alpha'' = 0$, also $\alpha = \pm 1$. Aus den Gleichungen $4, 5$ folgt dann $\beta = 0$, $\gamma = 0$. Ebenso folgt aus Gleichung 2, dass $\beta'' = 0$, also $\beta' = \pm 1$ ist; aus Gleichung 6 folgt $\gamma' = 0$, und aus 3, dass $\gamma'' = \pm 1$ ist. Da die Vorzeichen unabhängig voneinander gewählt werden können, gibt es insgesamt 8 verschiedene Transformationen.

II. Sind von den Zahlen a, a', a'' zwei gleich, *z.B.* $a' = a''$, die dritte aber verschieden, so nehmen wir an,

erstens, dass $a < a'$ ist. Dann gilt wie im vorigen Fall $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$. Aus den Gleichungen $2, 3, 6$ folgt aber leicht, dass entweder $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$ oder $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$ sein muss.

Ist dagegen *zweitens* $a > a'$, so erhält man dieselben Schlüsse folgendermaßen: Aus den Gleichungen $2, 3$ folgt notwendig $\beta = 0$, $\gamma = 0$, und entweder $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$ oder $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$. Unter beiden Voraussetzungen folgt aus den Gleichungen $4, 5$, dass $\alpha' = 0$, $\alpha'' = 0$ ist, und aus 1, dass $\alpha = \pm 1$ ist. Für beide Fälle gibt es also 16 verschiedene Transformationen. — Die übrigen beiden Fälle, in denen entweder $a = a''$ oder $a = a'$ ist, erledigt man genauso, indem man die Zeichen α, α', α'' im ersten Fall jeweils mit β, β', β'', im zweiten mit γ, γ', γ'' vertauscht.

III. Sind alle a, a', a'' gleich, so verlangen die Gleichungen $1, 2, 3$, dass von den drei Zahlen α, α', α'' sowie von β, β', β'' und auch von γ, γ', γ'' jeweils zwei $= 0$, die dritte $= \pm 1$ sind. Aus den Gleichungen $4, 5, 6$ sieht man aber leicht, dass von den

*) Die übrigen Fälle, in denen f eine definite Form ist, lassen sich auf diesen zurückführen. Ist dagegen f eine indefinite Form, so muss man eine ganz andere Methode anwenden, und die Anzahl der Transformationen ist unendlich.

drei Zahlen α, β, γ nur eine $= \pm 1$ sein kann; ebenso von α', β', γ' und von α'', β'', γ''. Es gibt daher nur sechs Kombinationen:

$$\begin{array}{|c|c|c|c|c|c|l|} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array} \quad \text{Die übrigen sechs Koeffizienten } = 0$$

Wegen der Wahl der Vorzeichen erhält man insgesamt 48 Transformationen. — Dasselbe Schema umfasst auch die vorigen Fälle: Von den ersten sechs Spalten darf man aber nur die erste nehmen, wenn a, a', a'' alle verschieden sind; die erste und zweite, wenn $a' = a''$; die erste und dritte, wenn $a = a'$; die erste und sechste, wenn $a = a''$ ist.

Daraus folgt: Geht die Form $f = axx + a'x'x' + a''x''x''$ in eine andere äquivalente Form f' über, und zwar durch die Substitution

$$x = \delta y + \varepsilon y' + \zeta y'', \quad x' = \delta' y + \varepsilon' y' + \zeta' y'', \quad x'' = \delta'' y + \varepsilon'' y' + \zeta'' y''$$

so sind alle Transformationen der Form f in f' in folgendem Schema enthalten:

$$\begin{array}{|c|c|c|c|c|c|l|} x & x & x' & x' & x'' & x'' & = \pm(\delta y + \varepsilon y' + \zeta y'') \\ x' & x'' & x & x'' & x & x' & = \pm(\delta' y + \varepsilon' y' + \zeta' y'') \\ x'' & x' & x'' & x & x' & x & = \pm(\delta'' y + \varepsilon'' y' + \zeta'' y'') \end{array}$$

Dabei müssen alle ersten sechs Spalten verwendet werden, wenn $a = a' = a''$; die Spalten 1 und 2, wenn a', a'' gleich und a verschieden sind; 1 und 3, wenn $a = a'$; 1 und 6, wenn $a = a''$; schließlich nur die erste Spalte, wenn a, a', a'' alle verschieden sind. Im ersten Fall ist die Anzahl der Transformationen 48, im zweiten, dritten und vierten 16, im fünften 8.

* *
*

EINIGE ANWENDUNGEN AUF DIE THEORIE DER BINÄREN FORMEN.

Eine Form finden, durch deren Verdopplung eine gegebene binäre Form des Hauptgeschlechts entsteht.

Von dieser kurzen Darstellung der ersten Grundlagen der Theorie ternärer Formen gehen wir zu einigen besonderen Anwendungen über, unter denen die folgende den ersten Platz verdient.

286.

Aufgabe. *Gegeben ist eine binäre Form $F = (A, B, C)$ mit der Determinante D aus dem Hauptgeschlecht. Gesucht ist eine binäre Form f, durch deren Verdopplung sie entsteht.*

Lösung. I. Man suche eine eigentliche Darstellung der zu F entgegengesetzten Form $F' = ATT - 2BTU + CUU$ durch die ternäre Form $xx - 2yz$, etwa

$$x = \alpha T + \beta U, \quad y = \alpha' T + \beta' U, \quad z = \alpha'' T + \beta'' U$$

Dass dies möglich ist, folgt leicht aus der vorigen Theorie der ternären Formen. Da nämlich F nach Voraussetzung zum Hauptgeschlecht gehört, gibt es einen Wert des Ausdrucks $\sqrt{(A, B, C)}(\mathrm{mod.}\, D)$. Daraus kann man eine ternäre Form φ mit der Determinante 1 finden, die $(A, -B, C)$ als Teil enthält. Dass alle Koeffizienten dieser Form ganze Zahlen sind, sieht man ohne Schwierigkeit. Ebenso leicht sieht man, dass φ eine indefinite Form ist (denn nach Voraussetzung ist F sicher keine negative Form); sie ist daher notwendig zur Form $xx - 2yz$ äquivalent. Man kann also eine Transformation der letzten in die erste angeben, die eine eigentliche Darstellung der Form F' durch $xx - 2yz$ liefert. — Dann gilt also

$$A = \alpha\alpha - 2\alpha'\alpha'', \quad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \quad C = \beta\beta - 2\beta'\beta''$$

Bezeichnet man ferner die Zahlen $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ mit a, b, c, so haben sie keinen gemeinsamen Teiler, und es gilt $D = bb - 2ac$.

II. Mithilfe der letzten Bemerkung aus Art. 235 folgt daraus leicht, dass F durch die Substitution $2\beta', \beta, \beta, \beta''$; $2\alpha', \alpha, \alpha, \alpha''$ in das Produkt der Form $(2a, -b, c)$ mit sich selbst und durch die Substitution $\beta', \beta, \beta, 2\beta''$; $\alpha', \alpha, \alpha, 2\alpha''$ in das Produkt der Form $(a, -b, 2c)$ mit sich selbst übergeht. Nun ist der größte gemeinsame Teiler der Zahlen $2a, 2b, 2c$ gleich 2. Ist also c ungerade, so haben $2a, 2b, c$ keinen gemeinsamen Teiler; mit anderen Worten, $(2a, -b, c)$ ist eine eigentlich primitive Form. Ebenso ist, wenn a ungerade ist, $(a, -b, 2c)$ eine eigentlich primitive Form. Im ersten Fall entsteht F durch Verdopplung der Form $(2a, -b, c)$, im zweiten durch Verdopplung der Form $(a, -b, 2c)$ (vgl. Schluss 4, Art. 235); einer dieser Fälle muss aber sicher stets eintreten. Wären nämlich beide a, c gerade, so müsste b ungerade sein. Nun bestätigt man leicht, dass $\beta''a + \beta b + \beta' c = 0$, $\alpha''a + \alpha b + \alpha' c = 0$ gilt; daraus würde folgen, dass βb, αb, also auch α und β gerade sind. Dann wären aber A und C gerade, entgegen der Voraussetzung, dass F eine Form des Hauptgeschlechts und daher von eigentlich primitiver Ordnung ist. — Es kann übrigens auch sein, dass sowohl a als auch c ungerade sind. In diesem Fall hat man sofort zwei Formen, durch deren Verdopplung F entsteht.

Beispiel. Gegeben sei die Form $F = (5.2, 31)$ mit der Determinante -151. Als Wert des Ausdrucks $\sqrt{(5, 2, 31)}$ findet man hier $(55, 22)$; daraus folgt die ternäre Form $\varphi = \begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix}$. Nach den Regeln aus Art. 272 findet man dazu die äquivalente Form $\begin{pmatrix} 1, & 1. & -1 \\ 0, & 0, & 0 \end{pmatrix}$, die in φ durch die Substitution $\begin{Bmatrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{Bmatrix}$ übergeht. Mithilfe der Transformationen aus Art. 277 findet man dann, dass $\begin{pmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{pmatrix}$ in φ durch die

Substitution $\left\{\begin{smallmatrix} 3.\ -7,\ -2 \\ 2,\ -1,\ \ 0 \\ 1,\ -9,\ -3 \end{smallmatrix}\right\}$ übergeht. Es ist also $a = 11$, $b = -17$, $c = 20$. Da a ungerade ist, entsteht F durch Verdopplung der Form $(11, 17, 40)$ und geht durch die Substitution $-1, -7, -7, -18;\ \ 2, 3, 3, 2$ in das Produkt dieser Form mit sich selbst über.

Allen Charakteren, außer den in Art. 263, 264 *als unmöglich erkannten, entsprechen tatsächlich Geschlechter.*

287.

Zum Problem des vorigen Artikels fügen wir noch die folgenden Bemerkungen hinzu.

I. Geht die Form F durch die Substitution p, p', p'', p'''; q, q', q'', q''' in das Produkt der beiden Formen (h, i, k), (h', i', k') über (beide, wie wir stets voraussetzen, im eigentlichen Sinn genommen), so erhält man die folgenden Gleichungen, die sich leicht aus Schluss 3 in Art. 235 ableiten lassen:

$$p''hn' - p'h'n - p(in' - i'n) = 0$$
$$(p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0$$
$$p'kn' - p''k'n - p'''(in' - i'n) = 0$$

sowie drei weitere, die daraus durch Vertauschen der Zahlen p, p', p'', p''' mit q, q', q'', q''' entstehen. Dabei sind n, n' die positiven Quadratwurzeln der Quotienten, die man erhält, wenn man die Determinanten der Formen (h, i, k), (h', i', k') durch die Determinante der Form F teilt. Sind also diese Formen identisch, oder gilt $n = n'$, $h = h'$, $i = i'$, $k = k'$, so gehen jene Gleichungen in die folgenden über:

$$(p'' - p')hn = 0, \quad (p'' - p')in = 0, \quad (p'' - p')kn = 0$$

Daraus folgt *notwendig* $p' = p''$, und auf genau dieselbe Weise $q' = q''$. — Gibt man also den Formen (h, i, k), (h', i', k') *dieselben* Unbestimmten t, u und bezeichnet die Unbestimmten der Form F mit T, U, so geht F durch die folgende Substitution über:

$$T = ptt + 2p'tu + p'''uu, \quad U = qtt + 2q'tu + q'''uu \quad \text{in} \quad (htt + 2itu + kuu)^2$$

II. Entsteht die Form F durch Verdopplung der Form f, so entsteht sie auch durch Verdopplung jeder anderen Form, die mit f in derselben Klasse liegt; mit anderen Worten, die Klasse der Form F entsteht durch Verdopplung der Klasse der Form f (vgl. Art. 238). So entsteht im Beispiel des vorigen Artikels $(5, 2, 31)$ auch durch Verdopplung der Form $(11, -5, 16)$, die zu $(11, 17, 40)$ eigentlich äquivalent ist. Aus einer Klasse, durch deren Verdopplung die Klasse der Form F entsteht, findet man mithilfe von Problem 260 *alle* solchen Klassen (falls es mehrere gibt). In unserem Beispiel gibt es keine andere positive Klasse dieser Art, weil nur eine positive eigentlich primitive ambige Klasse mit der Determinante -151 existiert (nämlich die Hauptklasse). Aus der Komposition der einzigen negativen ambigen Klasse $(-1, 0, -151)$ mit der Klasse $(11, -5, 16)$ entsteht die Klasse $(-11, -5. \ -16)$. Diese ist also die einzige negative Klasse, durch deren Verdopplung die Klasse $(5, 2, 31)$ entsteht.

III. Schon die Lösung des Problems im vorigen Artikel zeigt, dass jede eigentlich primitive (positive) Klasse binärer Formen, die zum Hauptgeschlecht gehört, durch Verdopplung einer eigentlich primitiven Klasse derselben Determinante entstehen kann. Der Satz aus Art. 261, der uns die Gewissheit gab, dass *mindestens* der Hälfte aller für eine gegebene nichtquadratische Determinante D zuweisbaren Charaktere

keine eigentlich primitiven (positiven) Geschlechter entsprechen können, lässt sich nun so erweitern: *Genau* der Hälfte aller dieser Charaktere entsprechen tatsächlich solche Geschlechter; der anderen Hälfte können also keine entsprechen (vgl. den Beweis jenes Satzes). In Art. 264 wurden alle diese zuweisbaren Charaktere gleichmäßig in zwei Arten P, Q aufgeteilt. Von den letzteren Q wurde bewiesen, dass sie keinen eigentlich primitiven (positiven) Formen entsprechen können; bei den übrigen P blieb dagegen ungewiss, ob jedem tatsächlich stets ein Geschlecht entspricht. Dieser Zweifel ist nun ganz beseitigt, und wir sind sicher, dass es in der gesamten Menge der Charaktere P keinen gibt, dem kein Geschlecht entspricht. — Daraus folgt auch leicht, dass bei negativer Determinante in der *negativen* eigentlich primitiven Ordnung, in der nach Art. 264, I alle P unmöglich und *nur* die Q möglich sind, tatsächlich *alle* Q möglich sind. Bezeichne nämlich K einen beliebigen Charakter aus Q, f eine beliebige Form aus der negativen eigentlich primitiven Ordnung der Formen mit der Determinante D und K' ihren Charakter, so liegt dieser in Q. Daraus sieht man leicht, dass der aus K, K' nach Art. 246 zusammengesetzte Charakter zu P gehört. Es gibt also positive eigentlich primitive Formen mit der Determinante D, die ihm entsprechen. Aus der Komposition einer solchen Form mit f entsteht offenbar eine negative eigentlich primitive Form mit der Determinante D, deren Charakter K ist. — Auf genau dieselbe Weise zeigt man, dass in der uneigentlich primitiven Ordnung diejenigen Charaktere, die nach den Regeln aus Art. 264 II, III als *einzig* mögliche gefunden werden, *alle* möglich sind, ob sie nun P oder Q sind. — Diese Sätze gehören, wenn wir uns nicht sehr irren, zu den schönsten in der Theorie der binären Formen, umso mehr, als sie bei größter Einfachheit doch so tief verborgen liegen, dass man ohne die Hilfe so vieler anderer Untersuchungen keinen strengen Beweis für sie geben kann.

Theorie der Zerlegung von Zahlen und binären Formen in drei Quadrate.

Wir gehen nun zu einer anderen Anwendung des vorigen Exkurses über: der Zerlegung von Zahlen und binären Formen in drei Quadrate. Wir stellen ihr das folgende Problem voran.

288.

Aufgabe. *Sei M eine positive Zahl. Gesucht sind die Bedingungen, unter denen primitive negative binäre Formen mit der Determinante $-M$ existieren können, die quadratische Reste von M sind, das heißt, für die* 1 *eine charakteristische Zahl ist.*

Lösung. Bezeichnen wir mit Ω die Gesamtheit aller besonderen Charaktere, die sich aus den Beziehungen der Zahl 1 sowohl zu den einzelnen (ungeraden) Primteilern von M als auch zur Zahl 8 oder 4 ergeben, wenn diese M teilt. Diese Charaktere sind offenbar Rp, Rp', Rp'' usw., wobei p, p', p'' usw. jene Primteiler bezeichnen; ferner $1, 4$ bei Teilbarkeit durch 4 und $1, 8$, wenn 8 die Zahl M teilt. Außerdem verwenden wir die Buchstaben P, Q im selben Sinn wie im vorigen Artikel oder in Art. 264. Nun unterscheiden wir die folgenden Fälle.

I. Ist M durch 4 teilbar, so ist Ω ein vollständiger Charakter. Nach Art. 233 V kann 1 nur für solche Formen eine charakteristische Zahl sein, deren Charakter Ω ist. Nun ist Ω offenbar der Charakter der Hauptform $(1, 0, M)$, gehört also zu P und

kann daher keiner eigentlich primitiven negativen Form zukommen. Da es für eine solche Determinante keine uneigentlich primitiven Formen gibt, gibt es in diesem Fall überhaupt keine primitiven negativen Formen, die Reste von M sind.

II. Ist $M \equiv 3 \pmod 4$, so gelten genau dieselben Überlegungen, mit der einzigen Ausnahme, dass in diesem Fall die *uneigentlich* primitive negative Ordnung existiert. In ihr sind die Charaktere P möglich oder unmöglich, je nachdem $M \equiv 3$ oder $\equiv 7 \pmod 8$ ist; vgl. Art. 264, III. Im ersten Fall gibt es also in dieser Ordnung ein Geschlecht mit dem Charakter Ω, sodass 1 eine charakteristische Zahl aller darin enthaltenen Formen ist. Im zweiten Fall kann es überhaupt keine negativen Formen mit dieser Eigenschaft geben.

III. Ist $M \equiv 1 \pmod 4$, so ist Ω noch kein vollständiger Charakter; die Beziehung zur Zahl 4 muss hinzukommen. Offenbar muss aber Ω im Charakter einer Form enthalten sein, deren charakteristische Zahl 1 ist; umgekehrt hat jede Form, deren Charakter entweder $\Omega;\ 1, 4$ oder $\Omega;\ 3, 4$ ist, die charakteristische Zahl 1. Nun ist $\Omega;\ 1, 4$ offenbar der Charakter des Hauptgeschlechts, der zu P gehört und somit in der negativen eigentlich primitiven Ordnung unmöglich ist. Aus demselben Grund gehört $\Omega;\ 3, 4$ zu Q (Art. 263), sodass ihm in der negativen eigentlich primitiven Ordnung ein Geschlecht entspricht, dessen Formen alle die charakteristische Zahl 1 haben. Die uneigentlich primitive Ordnung gibt es in diesem Fall ebenso wenig wie im folgenden.

IV. Ist $M \equiv 2 \pmod 4$, so muss zu Ω die Beziehung zu 8 hinzukommen, damit der Charakter vollständig wird, nämlich entweder 1 *und* $3, 8$ oder 5 *und* $7, 8$, wenn $M \equiv 2 \pmod 8$, und entweder 1 *und* $7, 8$ oder 3 *und* $5, 8$, wenn $M \equiv 6 \pmod 8$ ist. Im ersten Fall gehört der Charakter $\Omega;\ 1$ *und* $3, 8$ offenbar zu P, also $\Omega;\ 5$ *und* $7, 8$ zu Q, sodass ihm ein negatives eigentlich primitives Geschlecht entspricht. Ebenso gibt es im zweiten Fall ein Geschlecht in der negativen eigentlich primitiven Ordnung, dessen Formen die vorgeschriebene Eigenschaft haben, nämlich mit dem Charakter $\Omega;\ 3$ *und* $5, 8$.

Daraus folgt, dass primitive negative Formen mit der Determinante $-M$, deren charakteristische Zahl 1 ist, existieren, wenn M einer der Zahlen 1, 2, 3, 5, 6 modulo 8 kongruent ist, und zwar stets in einem einzigen Geschlecht, das uneigentlich ist, wenn $M \equiv 3$. Solche Formen gibt es überhaupt nicht, wenn $M \equiv 0,\ 4$ oder $7 \pmod 8$. Ist ferner $(-a, -b, -c)$ eine primitive negative Form mit der charakteristischen Zahl $+1$, so ist (a, b, c) offenbar eine primitive positive Form mit der charakteristischen Zahl -1. In den ersten fünf Fällen (wenn $M \equiv 1, 2, 3, 5, 6$) gibt es also ein primitives positives Geschlecht, dessen Formen die charakteristische Zahl -1 haben, und zwar für $M \equiv 3$ ein *uneigentliches*. In den übrigen drei Fällen (wenn $M \equiv 0, 4, 7$) kann es überhaupt keine solchen positiven Formen geben.

289.

Aus der allgemeinen Theorie in Art. 282 folgt für die eigentlichen Darstellungen binärer Formen durch die ternäre Form $xx + yy + zz = f$ Folgendes.

I. Eine binäre Form φ kann nur dann durch f eigentlich dargestellt werden, wenn sie eine primitive positive Form ist und -1 (also die Determinante der Form f) ihre charakteristische Zahl ist. Daher gibt es bei positiver Determinante und ebenso bei negativer Determinante $-M$, wenn M entweder durch 4 teilbar oder von der Form $8n + 7$ ist, keine durch f eigentlich darstellbaren binären Formen.

II. Ist dagegen $\varphi = (p, q, r)$ eine primitive positive Form mit der Determinante $-M$ und -1 eine charakteristische Zahl der Form φ, also auch der entgegengesetzten Form $(p, -q, r)$, so gibt es eigentliche Darstellungen der Form φ durch f, die zu jedem gegebenen Wert des Ausdrucks $\sqrt{-}(p, -q, r)$ gehören. Denn alle Koeffizienten der ternären Form g mit der Determinante -1 (Art. 283) sind notwendig ganzzahlig, und g ist eine definite Form, also sicher zu f äquivalent (Art. 285, I).

III. Nach Art. 283, III ist die Anzahl aller Darstellungen, die zu demselben Wert des Ausdrucks $\sqrt{-}(p, -q, r)$ gehören, in allen Fällen außer $M = 1$ und $M = 2$ ebenso groß wie die Anzahl der Transformationen der Form f in g, also nach Art. 285 $= 48$. Daraus erkennt man auch: Hat man eine zu einem gegebenen Wert gehörende Darstellung, so erhält man die übrigen 47, indem man die Werte von x, y, z auf alle möglichen Arten miteinander vertauscht und ihre Vorzeichen umkehrt. Alle 48 Darstellungen ergeben daher *eine einzige* Zerlegung der Form φ in drei Quadrate, wenn man nur die Quadrate selbst betrachtet, ohne ihre Reihenfolge oder die Vorzeichen ihrer Wurzeln zu berücksichtigen.

IV. Die Anzahl aller verschiedenen ungeraden Primzahlen, die M teilen, sei $= \mu$. Aus Art. 233 folgt leicht, dass die Anzahl aller verschiedenen Werte des Ausdrucks $\sqrt{-}(p, -q, r) (\text{mod. } M) = 2^\mu$ ist. Nach Art. 283 braucht man davon nur die Hälfte zu betrachten (wenn $M > 2$). Die Anzahl aller eigentlichen Darstellungen der Form φ durch f ist daher $= 48 \,.\, 2^{\mu-1} = 3 \,.\, 2^{\mu+3}$, die Anzahl der verschiedenen Zerlegungen in drei Quadrate aber $= 2^{\mu-1}$.

Beispiel. Sei $\varphi = 19tt + 6tu + 41uu$, also $M = 770$. Hier muss man die folgenden vier Werte des Ausdrucks $\sqrt{-}(19, -3, 41) (\text{mod. } 770)$ betrachten (Art. 283): $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$. Um die zum Wert $(39, 237)$ gehörenden Darstellungen zu finden, bestimmt man zuerst die ternäre Form $\left(\begin{smallmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{smallmatrix}\right) = g$. Nach den Regeln aus Art. 272, 275 geht f durch die Substitution $\left\{\begin{smallmatrix} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{smallmatrix}\right\}$ in sie über. Daraus erhält man die folgende Darstellung der Form φ durch f:

$$x = t - 6u, \quad y = -3t - 2u. \quad z = -3t - u$$

Die übrigen 47 zum selben Wert gehörenden Darstellungen, die durch Vertauschen dieser Werte und Umkehren ihrer Vorzeichen entstehen, schreiben wir der Kürze wegen nicht auf. Alle 48 Darstellungen ergeben dieselbe Zerlegung der Form φ in die drei Quadrate

$$tt - 12tu + 36uu, \quad 9tt + 12tu + 4uu, \quad 9tt + 6tu + uu$$

Auf genau dieselbe Weise liefert der Wert $(171, -27)$ die Zerlegung in die Quadrate $(3t+5u)^2$, $(3t-4u)^2$, tt; der Wert $(269, -83)$ liefert $(t+6u)^2+(3t+u)^2+(3t-2u)^2$ und schließlich der Wert $(291, -127)$ die Zerlegung $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$. Jede dieser Zerlegungen entspricht 48 Darstellungen. — Außer diesen 192 Darstellungen oder vier Zerlegungen gibt es keine weiteren, da 770 durch kein Quadrat teilbar ist und somit keine uneigentlichen Darstellungen existieren können.

290.

Die Formen mit den Determinanten -1 und -2, für die gewisse Ausnahmen galten, besprechen wir kurz gesondert. Zunächst die allgemeine Bemerkung: Sind φ, φ' beliebige äquivalente binäre Formen und (Θ) eine gegebene Transformation der ersten in die zweite, so ergibt die Verbindung einer beliebigen Darstellung der Form φ durch eine ternäre Form f mit der Substitution (Θ) eine Darstellung der Form φ' durch f. Dabei entstehen aus eigentlichen Darstellungen von φ eigentliche Darstellungen von φ', aus verschiedenen verschiedene und schließlich aus allen sämtliche. All dies lässt sich sehr leicht durch Rechnung bestätigen. Die eine der Formen φ, φ' lässt sich also auf genauso viele Arten durch f darstellen wie die andere.

I. Sei zuerst $\varphi = tt + uu$ und φ' eine beliebige andere positive binäre Form mit der Determinante -1, zu der φ daher äquivalent ist. Es gehe φ in φ' durch die Substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ über. Die Form φ wird durch die ternäre Form $f = zz + yy + zz$ dargestellt, wenn man $x = t$, $y = u$, $z = 0$ setzt. Durch Vertauschen von x, y, z entstehen daraus *sechs* Darstellungen und aus jeder durch Ändern der Vorzeichen von t, u wiederum vier. So erhält man insgesamt 24 verschiedene Darstellungen, denen eine einzige Zerlegung in drei Quadrate entspricht; dass es keine weiteren Darstellungen geben kann, sieht man leicht. Daher lässt sich auch die Form φ' nur auf eine einzige Weise in drei Quadrate zerlegen, nämlich in $(\alpha t' + \beta u')^2$, $(\gamma t' + \delta u')^2$ und 0. Diese Zerlegung entspricht 24 Darstellungen.

II. Sei $\varphi = tt + 2uu$ und φ' eine beliebige andere positive binäre Form mit der Determinante -2, in die φ durch die Substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ übergeht. Dann folgt wie im vorigen Fall, dass sich φ und somit auch φ' nur auf eine einzige Weise in drei Quadrate zerlegen lässt: φ in $tt + uu + uu$ und φ' in $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$. Dass eine solche Zerlegung 24 Darstellungen entspricht, sieht man leicht.

Daraus folgt, dass die binären Formen mit den Determinanten -1 und -2 hinsichtlich der Anzahl ihrer Darstellungen durch die ternäre Form $xx + yy + zz$ mit den anderen binären Formen völlig übereinstimmen. Denn in beiden Fällen ist $\mu = 0$, und die Formel aus IV des vorigen Artikels ergibt tatsächlich 24 Darstellungen. Der Grund dafür ist, dass sich die beiden Ausnahmen, denen solche Formen unterlagen, gegenseitig ausgleichen.

Die Anwendung der in Art. 284 entwickelten allgemeinen Theorie der uneigentlichen Darstellungen auf die Form $xx + yy + zz$ lassen wir der Kürze wegen weg.

291.

Die Aufgabe, alle eigentlichen Darstellungen einer gegebenen positiven *Zahl* M durch die Form $xx + yy + zz$ zu finden, wird nach Art. 281 zunächst auf die Suche nach den eigentlichen Darstellungen der Zahl $-M$ durch die Form $-xx-yy-zz = f$ zurückgeführt. Diese erhält man nach den Regeln aus Art. 280 wie folgt.

I. Man bestimme alle Klassen binärer Formen mit der Determinante $-M$, deren Formen sich durch $XX + YY + ZZ = F$ (die ternäre Form, deren Adjunkte f ist) eigentlich darstellen lassen. Ist $M \equiv 0,\ 4$ oder $7 \pmod 8$, so gibt es nach Art. 288 keine solchen Klassen, und M lässt sich daher nicht in drei Quadrate ohne gemeinsamen Teiler zerlegen*). Ist dagegen $M \equiv 1,\ 2,\ 5$ oder 6, so gibt es ein positives eigentlich primitives Geschlecht, und bei $M \equiv 3$ ein uneigentlich primitives, das alle diese Klassen umfasst. Ihre Anzahl bezeichnen wir mit k.

II. Nun wähle man aus diesen Klassen beliebig k Formen, aus jeder eine, und bezeichne sie mit φ, φ', φ'' usw. Man bestimme sämtliche eigentlichen Darstellungen aller dieser Formen durch F. Ihre Anzahl ist daher $3\,.\,2^{\mu+3}k = K$, wobei μ die Anzahl der (ungeraden) Primfaktoren von M bezeichnet. Schließlich leite man aus jeder solchen Darstellung, etwa

$$X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u$$

die folgende Darstellung von M durch $xx + yy + zz$ ab:

$$x = m'n'' - m''n', \quad y = m''n - mn'', \quad z = mn' - m'n$$

Die Gesamtheit dieser K Darstellungen, die wir mit Ω bezeichnen, enthält notwendig sämtliche Darstellungen von M.

III. Es bleibt also nur zu untersuchen, ob in Ω *identische* Darstellungen auftreten können. Nach Art. 280, III sind die Darstellungen in Ω, die aus verschiedenen Formen, *zum Beispiel* aus φ und φ', hergeleitet wurden, notwendig verschieden. Es bleibt daher nur die Frage, ob verschiedene Darstellungen derselben Form, *zum Beispiel* von φ, durch F identische Darstellungen der Zahl M durch $xx + yy + zz$ ergeben können. Nun ist sofort klar: Kommt unter den Darstellungen von φ die folgende vor,

$$X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u \quad \ldots\ (r)$$

so auch diese:

$$X = -mt - nu, \quad Y = -m't - n'u, \quad Z = -m''t - n''u \quad \ldots\ (r')$$

Aus beiden folgt dieselbe Darstellung von M, die wir mit (R) bezeichnen. Wir untersuchen also, ob sich dieselbe (R) noch aus anderen Darstellungen der Form φ ergeben

*) Diese Unmöglichkeit folgt auch daraus, dass die Summe dreier ungerader Quadrate notwendig $\equiv 3 \pmod 8$ ist; die Summe zweier ungerader und eines geraden Quadrats ist entweder $\equiv 2$ oder $\equiv 6$; die Summe eines ungeraden und zweier gerader Quadrate entweder $\equiv 1$ oder $\equiv 5$; schließlich die Summe dreier gerader Quadrate entweder $\equiv 0$ oder $\equiv 4$. Im letzten Fall ist die Darstellung aber offenbar uneigentlich.

kann. Setzt man in Art. 280, III $\chi = \varphi$, so folgt leicht: Werden alle eigentlichen Transformationen der Form φ in sich selbst durch

$$t = \alpha t + \beta u, \quad u = \gamma t + \delta u$$

gegeben, so werden alle Darstellungen der Form φ, aus denen R folgt, durch

$$\begin{aligned} x &= (\alpha m + \gamma n)t + (\beta m + \delta n)u \\ y &= (\alpha m' + \gamma n')t + (\beta m' + \delta n')u \\ z &= (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u \end{aligned}$$

ausgedrückt. Aus der in Art. 179 entwickelten Theorie der Transformationen binärer Formen mit negativer Determinante folgt aber, dass es in allen Fällen außer $M = 1$ und $M = 3$ nur zwei eigentliche Transformationen der Form φ in sich selbst gibt, nämlich $\alpha, \beta, \gamma, \delta = 1, 0, 0, 1$ und $= -1, 0, 0, -1$. (Da φ eine primitive Form ist, ist das in Art. 179 mit m Bezeichnete entweder 1 oder 2. Abgesehen von den Ausnahmefällen gilt dort also sicher (1).) Somit kann (R) nur aus r, r' entstehen. Jede eigentliche Darstellung der Zahl M kommt daher in Ω zweimal und nicht öfter vor, und die Anzahl aller verschiedenen eigentlichen Darstellungen von M ist $\frac{1}{2}K = 3\,.\,2^{\mu+2}k$.

Für die Ausnahmefälle ist die Anzahl der eigentlichen Transformationen der Form φ in sich selbst nach Art. 179 gleich 4 für $M = 1$ und 6 für $M = 3$. Tatsächlich bestätigt man leicht, dass die Anzahlen der eigentlichen Darstellungen der Zahlen 1, 3 gleich $\frac{1}{4}K$ bzw. $\frac{1}{6}K$ sind. Jede dieser Zahlen lässt sich nämlich nur auf eine einzige Weise in drei Quadrate zerlegen: 1 in $1+0+0$ und 3 in $1+1+1$. Die Zerlegung von 1 liefert sechs, die von 3 acht verschiedene Darstellungen. Dabei ist $K = 24$ für $M = 1$ (wobei $\mu = 0$, $k = 1$) und $= 48$ für $M = 3$ (wobei $\mu = 1$, $k = 1$).

Außerdem bemerken wir: Bezeichnet h die Anzahl der Klassen im Hauptgeschlecht, der nach Art. 252 die Anzahl der Klassen in jedem anderen eigentlich primitiven Geschlecht gleich ist, so ist $k = h$ für $M \equiv 1,\ 2,\ 5$ oder 6 (mod. 8), aber $k = \frac{1}{3}h$ für $M \equiv 3$ (mod. 8), mit der einzigen Ausnahme $M = 3$, wo $k = h = 1$ ist. Für Zahlen der Form $8n + 3$ ist die Anzahl der Darstellungen also *allgemein* $= 2^{\mu+2}h$, da sich bei der Zahl 3 die beiden Ausnahmen gegenseitig ausgleichen.

292.

Die Zerlegungen von Zahlen in drei Quadrate unterscheiden wir (wie oben bei den binären Formen) von den Darstellungen durch die Form $xx + yy + zz$ so, dass wir bei jenen nur die Größe der Quadrate, bei diesen aber auch ihre Reihenfolge und die Vorzeichen ihrer Wurzeln betrachten. Wir halten also die Darstellungen $x = a$, $y = b$, $z = c$ und $x = a'$, $y = b'$, $z = c'$ für verschieden, sofern nicht zugleich $a = a'$, $b = b'$, $c = c'$ gilt. Die Zerlegungen in $aa + bb + cc$ und in $a'a' + b'b' + c'c'$ gelten dagegen als eine, wenn diese Quadrate jenen ohne Rücksicht auf die Reihenfolge gleich sind. Daraus folgt:

I. Eine Zerlegung der Zahl M in die Quadrate $aa+bb+cc$ entspricht 48 Darstellungen, wenn keines $= 0$ und alle ungleich sind; aber 24, wenn *entweder* eines $= 0$ und die übrigen ungleich sind, *oder* keines $= 0$ ist und zwei gleich sind. Sind dagegen in einer Zerlegung der gegebenen Zahl in drei Quadrate zwei davon $= 0$, *oder* eines $= 0$ und die übrigen gleich, *oder* alle gleich, so entspricht sie 6, *oder* 12, *oder* 8 Darstellungen. Dies kann aber nur in den besonderen Fällen $M = 1$, 2 bzw. 3 vorkommen, sofern die Darstellungen eigentlich sein sollen. Diese Fälle seien ausgeschlossen. Die Anzahl aller Zerlegungen der Zahl M in drei Quadrate (ohne gemeinsamen Teiler) sei E, und darunter seien e, in denen ein Quadrat 0 ist, sowie e', in denen zwei Quadrate gleich sind. Jene kann man auch als Zerlegungen in zwei Quadrate, diese als Zerlegungen in ein Quadrat und das Doppelte eines Quadrats ansehen. Dann ist die Anzahl aller eigentlichen Darstellungen der Zahl M durch $xx + yy + zz$

$$= 24(e + e') + 48(E - e - e') = 48E - 24(e + e')$$

Aus der Theorie der binären Formen folgt aber leicht, dass e entweder $= 0$ oder $= 2^{\mu-1}$ ist, je nachdem -1 quadratischer Nichtrest oder Rest von M ist; ebenso $e' = 0$ oder $= 2^{\mu-1}$, je nachdem -2 Nichtrest oder Rest von M ist. Dabei bezeichnet μ die Anzahl der (ungeraden) Primfaktoren von M (vgl. Art. 182; eine ausführlichere Darstellung lassen wir hier weg). Daraus folgt leicht:

$E = 2^{\mu-2}k$, wenn -1 und -2 beide *N.R.* von M sind;
$E = 2^{\mu-2}(k+2)$, wenn beide Zahlen Reste sind; schließlich
$E = 2^{\mu-2}(k+1)$, wenn eine Zahl Rest, die andere Nichtrest ist.

In den ausgeschlossenen Fällen $M = 1$ und $M = 2$ würde diese Formel $E = \frac{3}{4}$ ergeben, während $E = 1$ sein muss; für $M = 3$ ergibt sich dagegen richtig $E = 1$, da sich die Ausnahmen gegenseitig ausgleichen.

Ist also M eine Primzahl, so ist $\mu = 1$, also $E = \frac{1}{2}(k + 2)$, wenn $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k + 1)$, wenn $M \equiv 3$ oder $\equiv 5$. Diese besonderen Sätze hat der berühmte Le Gendre durch Induktion gefunden und in seiner schon öfter angeführten ausgezeichneten Abhandlung *Hist. de l'Ac. de Paris* 1785, S. 530 ff. mitgeteilt, wenn auch in etwas anderer Form. Der Grund liegt vor allem darin, dass er die eigentliche von der uneigentlichen Äquivalenz nicht unterschieden und daher entgegengesetzte Klassen zusammengefasst hat.

II. Um alle Zerlegungen der Zahl M in drei Quadrate (ohne gemeinsamen Teiler) zu finden, braucht man nicht sämtliche eigentlichen Darstellungen aller Formen φ,

φ', φ'' zu bestimmen. Zunächst bestätigt man leicht, dass alle (48) Darstellungen der Form φ, die zu demselben Wert des Ausdrucks $\sqrt{-}(p,-q,r)$ gehören (wobei $\varphi = (p,q,r)$ gesetzt wird), dieselbe Zerlegung der Zahl M ergeben. Daher genügt es, eine davon zu haben, oder, was auf dasselbe hinausläuft, nur alle verschiedenen Zerlegungen*) der Form φ in drei Quadrate aufzuschreiben; ebenso bei den übrigen φ', φ'' usw. Gehört ferner φ zu einer nichtambigen Klasse, so darf man die aus der entgegengesetzten Klasse gewählte Form ganz übergehen; von zwei entgegengesetzten Klassen genügt es also, eine einzige zu betrachten. Da die Wahl der Form aus jeder Klasse ganz beliebig ist, nehmen wir an, aus der zur Klasse von φ entgegengesetzten Klasse werde die zu φ entgegengesetzte Form gewählt, und diese sei $= \varphi'$. Dann sieht man ohne Mühe: Werden die eigentlichen Zerlegungen der Form φ allgemein durch

$$(gt+hu)^2 + (g't+h'u)^2 + (g''t+h''u)^2$$

gegeben, so werden alle Zerlegungen der Form φ' durch

$$(gt-hu)^2 + (g't-h'u)^2 + (g''t-h''u)^2$$

ausgedrückt, und aus diesen folgen dieselben Zerlegungen der Zahl M wie aus jenen. Ist schließlich φ eine Form aus einer ambigen Klasse, die aber weder der Hauptklasse angehört noch zu der Form $(2,0,\frac{1}{2}M)$ oder $(2,1,\frac{1}{2}(M+1))$ äquivalent ist (je nachdem M gerade oder ungerade ist), so darf man von den Werten des Ausdrucks $\sqrt{-}(p,-q,r)$ die Hälfte weglassen. Der Kürze wegen erklären wir diese Abkürzung hier aber nicht näher. — Dieselben Abkürzungen lassen sich auch verwenden, wenn sämtliche eigentlichen Darstellungen von M durch $xx+yy+zz$ gesucht sind, da sich diese sehr leicht aus den Zerlegungen ergeben.

Als Beispiel suchen wir alle Zerlegungen der Zahl 770 in drei Quadrate. Hier ist $\mu = 3$, $e = e' = 0$, also $E = 2k$. Aus der Klassifikation der positiven binären Formen mit der Determinante -770, die wir der Kürze wegen weglassen, da sie jeder nach Art. 231 leicht aufstellen kann, ergibt sich die Anzahl der positiven Klassen $= 32$. Alle sind eigentlich primitiv und auf 8 Geschlechter verteilt, sodass $k = 4$ und daher $E = 8$ ist. Das Geschlecht mit der charakteristischen Zahl -1 muss bezüglich der Zahlen $5, 7, 11$ offenbar die besonderen Charaktere $R5$; $N7$; $N11$ haben. Daraus folgt nach Art. 263 leicht, dass sein Charakter bezüglich der Zahl 8 gleich 1 und 3, 8 sein muss. Nun finden sich in dem Geschlecht mit dem Charakter 1 und 3, 8; $R5$; $N7$; $N11$ vier Klassen, als deren Vertreter wir die Formen $(6,2,129)$, $(6,-2,129)$, $(19,3,41)$, $19,-3,41)$ wählen. Die zweite und vierte Klasse lassen wir aber als entgegengesetzte der ersten und dritten weg. Vier Zerlegungen der Form $(19,3,41)$ haben wir schon in Art. 289 angegeben; daraus folgen die Zerlegungen der Zahl 770 in $9+361+400$, $16+25+729$, $81+400+289$, $576+169+25$. Ebenso findet man vier Zerlegungen

*) Dabei ist stets *eigentliche* mitzudenken, wenn man diesen Ausdruck von den Darstellungen auf die Zerlegungen übertragen will.

der Form $6tt + 4tu + 129uu$ in

$$(t - 8u)^2 + (2t + u)^2 + (t + 8u)^2,$$
$$(t - 10u)^2 + (2t + 5u)^2 + (t + 2u)^2$$
$$(2t - 5u)^2 + (t + 10u)^2 + (t + 2u)^2,$$
$$(2t + 7u)^2 + (t - 8u)^2 + (t - 4u)^2$$

die der Reihe nach aus den folgenden Werten des Ausdrucks $\sqrt{-(6, -2, 129)}$ entstehen: $(48, 369)$, $(62, -149)$, $(92, -159)$, $(202, 61)$. Daraus folgen die Zerlegungen der Zahl 770 in $225 + 256 + 289$, $1 + 144 + 625$, $64 + 81 + 625$, $16 + 225 + 529$. Außer diesen acht Zerlegungen gibt es keine weiteren.

Was die Zerlegungen von Zahlen in drei Quadrate mit gemeinsamen Teilern betrifft, so folgt dies so leicht aus der allgemeinen Theorie in Art. 281, dass wir uns dabei nicht aufzuhalten brauchen.

Beweis der Sätze von Fermat, dass sich jede ganze Zahl in drei Dreieckszahlen oder vier Quadrate zerlegen lässt.

293.

Die vorigen Untersuchungen liefern auch einen Beweis des berühmten Satzes, dass sich *jede positive ganze Zahl in drei Dreieckszahlen zerlegen lässt*, den Fermat schon vor langer Zeit gefunden hat, für den aber bisher ein strenger Beweis fehlte. Offenbar ergibt jede Zerlegung der Zahl M in Dreieckszahlen

$$\tfrac{1}{2}x(x + 1) + \tfrac{1}{2}y(y + 1) + \tfrac{1}{2}z(z + 1)$$

eine Zerlegung der Zahl $8M + 3$ in drei ungerade Quadrate

$$(2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2$$

und umgekehrt. Nach der vorigen Theorie lässt sich aber jede positive ganze Zahl $8M + 3$ in drei Quadrate zerlegen, die notwendig ungerade sind (vgl. die Anmerkung zu Art. 291). Die Anzahl der Zerlegungen hängt sowohl von der Anzahl der Primfaktoren von $8M + 3$ als auch von der Anzahl der Klassen ab, in die sich die binären Formen mit der Determinante $-(8M + 3)$ verteilen. Ebenso viele Zerlegungen der Zahl M in drei Dreieckszahlen gibt es. Wir setzen dabei voraus, dass $\frac{1}{2}x(x + 1)$ für jeden ganzzahligen Wert von x als Dreieckszahl angesehen wird. Wollte man die Null lieber ausschließen, müsste man den Satz so ändern: Jede positive ganze Zahl ist entweder selbst eine Dreieckszahl oder lässt sich in zwei oder drei Dreieckszahlen zerlegen. Eine ähnliche Änderung wäre beim folgenden Satz nötig, wenn man die Null von den Quadraten ausschließen wollte.

Aus denselben Grundsätzen folgt ein anderer Satz von Fermat: *Jede positive ganze Zahl lässt sich in vier Quadrate zerlegen.* Zieht man von einer Zahl der Form $4n + 2$ ein beliebiges Quadrat (das kleiner als diese Zahl ist), von einer Zahl der Form $4n + 1$ ein gerades Quadrat und von einer Zahl der Form $4n + 3$ ein ungerades Quadrat ab, so lässt sich der Rest in allen diesen Fällen in drei Quadrate zerlegen,

die gegebene Zahl also in vier. Schließlich kann man eine Zahl der Form $4n$ als $4^\mu N$ darstellen, wobei N zu einer der drei vorigen Formen gehört. Mit der Zerlegung von N in vier Quadrate ist auch $4^\mu N$ zerlegt. Von einer Zahl der Form $8n + 3$ kann man auch ein Quadrat mit durch vier teilbarer Wurzel abziehen, von einer Zahl der Form $8n + 7$ ein Quadrat, dessen Wurzel das Doppelte einer ungeraden Zahl ist, und von einer Zahl der Form $8n + 4$ ein ungerades Quadrat; der Rest lässt sich dann in drei Quadrate zerlegen. Übrigens hatte der berühmte La Grange diesen Satz schon bewiesen, *Nouv. Mém. de l'Ac. de Berlin* 1770, S. 123. Diesen von unserem ganz verschiedenen Beweis hat der berühmte Euler in *Actis Ac. Petr. Vol.* II, S. 48 ausführlicher erklärt. — Andere Sätze Fermats, die gewissermaßen die Fortsetzung dieser Sätze bilden, nämlich dass sich jede ganze Zahl in fünf Fünfeckszahlen, sechs Sechseckszahlen, sieben Siebeneckszahlen *usw.* zerlegen lässt, sind bisher unbewiesen und scheinen tiefer liegende Grundsätze zu erfordern.

Lösung der Gleichung $axx + byy + czz = 0$.

294.

Satz. *Seien* a, b, c *paarweise teilerfremde Zahlen, von denen keine* $= 0$ *oder durch ein Quadrat teilbar ist. Die Gleichung*

$$axx + byy + czz = 0 \ldots (\Omega)$$

besitzt keine ganzzahlige Lösung (außer $x = y = z = 0$*, die wir nicht berücksichtigen), sofern nicht* $-bc, -ac, -ab$ *quadratische Reste von* a, b, c *der Reihe nach sind und diese Zahlen nicht alle dasselbe Vorzeichen haben. Sind diese vier Bedingungen aber erfüllt, so ist* (Ω) *in ganzen Zahlen lösbar.*

Beweis. Ist (Ω) überhaupt in ganzen Zahlen lösbar, so auch durch Werte von x, y, z, die keinen gemeinsamen Teiler haben. Denn beliebige Werte, die der Gleichung Ω genügen, genügen ihr auch nach Division durch ihren größten gemeinsamen Teiler. Nehmen wir nun $app + bqq + crr = 0$ an und seien p, q, r ohne gemeinsamen Teiler, so sind sie auch paarweise teilerfremd. Hätten nämlich q, r einen gemeinsamen Teiler μ, so wäre dieser zu p teilerfremd, aber $\mu\mu$ würde app und somit auch a teilen, entgegen der Voraussetzung. Ebenso sind p, r; p, q paarweise teilerfremd. Daher wird $-app$ durch die binäre Form $byy + czz$ dargestellt, indem man y, z die teilerfremden Werte q, r gibt. Ihre Determinante $-bc$ ist somit quadratischer Rest von app und daher auch von a (Art. 154). Ebenso ist $-acRb$, $-abRc$. Dass aber (Ω) keine Lösung haben kann, wenn a, b, c dasselbe Vorzeichen haben, ist so offensichtlich, dass es keiner Erklärung bedarf.

Den Beweis der Umkehrung, die den zweiten Teil des Satzes bildet, richten wir so ein: *Zuerst* zeigen wir, wie man eine zu $\left(\begin{smallmatrix} a,b,c \\ 0,0,0 \end{smallmatrix}\right) \ldots f$ äquivalente ternäre Form findet, deren Koeffizienten $2, 3, 4$ durch abc teilbar sind. Daraus leiten wir *zweitens* eine Lösung der Gleichung (Ω) ab.

I. Man bestimme drei ganze Zahlen A, B, C ohne gemeinsamen Teiler so, dass A zu b und c, B zu a und c, C zu a und b teilerfremd ist, während $aAA + bBB + cCC$ durch abc teilbar ist. Dies erreicht man wie folgt. Seien $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ Werte der Ausdrücke $\sqrt{-bc} \pmod a$, $\sqrt{-ac} \pmod b$, $\sqrt{-ab} \pmod c$, die notwendig zu a, b, c der Reihe nach teilerfremd sind. Man wähle drei ganze Zahlen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ganz beliebig, nur so, dass sie der Reihe nach zu a, b, c teilerfremd sind (*zum Beispiel* alle $= 1$), und bestimme A, B, C so, dass

$$\begin{aligned} A &\equiv \mathfrak{b}c \pmod b \quad \text{und} \quad \equiv \mathfrak{c}\mathfrak{C} \pmod c \\ B &\equiv \mathfrak{c}a \pmod c \quad \text{und} \quad \equiv \mathfrak{a}\mathfrak{A} \pmod a \\ C &\equiv \mathfrak{a}b \pmod a \quad \text{und} \quad \equiv \mathfrak{b}\mathfrak{B} \pmod b \end{aligned}$$

Dann ist

$$\begin{aligned} aAA + bBB + cCC &\equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} + cbb) \\ &\equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} - \mathfrak{A}\mathfrak{A}b) \equiv 0 \pmod a \end{aligned}$$

also durch a teilbar, ebenso durch b, c und somit auch durch abc. Außerdem ist offenbar A notwendig zu b und c, B zu a und c, C zu a und b teilerfremd. Haben diese Werte von A, B, C aber einen (größten) gemeinsamen Teiler μ, so ist dieser

offenbar zu a, b, c und somit zu abc teilerfremd. Durch Division jener Werte durch μ erhalten wir daher neue ohne gemeinsamen Teiler, die für $aAA+bBB+cCC$ weiterhin einen durch abc teilbaren Wert ergeben und somit alle Bedingungen erfüllen.

II. Sind die Zahlen A, B, C so bestimmt, so haben auch Aa, Bb, Cc keinen gemeinsamen Teiler. Hätten sie nämlich einen gemeinsamen Teiler μ, so wäre dieser notwendig zu a teilerfremd (da dieses sowohl zu Bb als auch zu Cc teilerfremd ist) und ebenso zu b und c. Daher müsste μ auch A, B, C teilen, entgegen der Voraussetzung. Man kann also ganze Zahlen α, β, γ finden, sodass $\alpha Aa + \beta Bb + \gamma Cc = 1$ ist. Ferner bestimme man sechs ganze Zahlen $\alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ so, dass

$$\beta'\gamma'' - \gamma'\beta'' = Aa, \quad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \quad \alpha'\beta'' - \beta'\alpha'' = Cc$$

Nun gehe f durch die Substitution

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

in $\left(\begin{smallmatrix} m,m',m'' \\ n,n',n'' \end{smallmatrix}\right) = g$ über (die zu f äquivalent ist). Ich behaupte, dass m', m'', n durch abc teilbar sind. Setzt man nämlich

$$\begin{gathered} \beta''\gamma - \gamma''\beta = A', \quad \gamma''\alpha - \alpha''\gamma = B', \quad \alpha''\beta - \beta''\alpha = C' \\ \beta\gamma' - \gamma\beta' = A'', \quad \gamma\alpha' - \alpha\gamma' = B'', \quad \alpha\beta' - \beta\alpha' = C'' \end{gathered}$$

so ist

$$\begin{gathered} \alpha' = B''Cc - C''Bb, \quad \beta' = C''Aa - A''Cc, \quad \gamma' = A''Bb - B''Aa \\ \alpha'' = C'Bb - B'Cc, \quad \beta'' = A'Cc - C'Aa, \quad \gamma'' = B'Aa - A'Bb \end{gathered}$$

Durch Einsetzen dieser Werte in die Gleichungen

$$\begin{aligned} m' &= a\alpha'\alpha' + b\beta'\beta' + c\gamma'\gamma' \\ m'' &= a\alpha''\alpha'' + b\beta''\beta'' + c\gamma''\gamma'' \\ n &= a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma'' \end{aligned}$$

erhält man modulo a

$$\begin{aligned} m' &\equiv bcA''A''(BBb + CCc) \equiv 0 \\ m'' &\equiv bcA'A'(BBb + CCc) \equiv 0 \\ n &\equiv bcA'A''(BBb + CCc) \equiv 0 \end{aligned}$$

also sind m', m'', n durch a teilbar. Ebenso findet man, dass dieselben Zahlen durch b, c und somit auch durch abc teilbar sind, wie behauptet.

III. Für die Determinante der Formen f, g schreiben wir der Übersicht wegen $-abc = d$ und setzen

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N''$$

Offenbar geht f durch die Substitution (S)

$$\begin{array}{lll} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{array}$$

in die ternäre Form $\left(\begin{smallmatrix} Md,M'd,M''d \\ Nd,N'd,N''d \end{smallmatrix}\right) = g'$ mit der Determinante d^3 über, die daher unter f enthalten ist. Nun behaupte ich, dass diese Form g' notwendig zu $\left(\begin{smallmatrix} d,0,0 \\ d,0,0 \end{smallmatrix}\right) = g''$ äquivalent ist. Denn $\left(\begin{smallmatrix} M,M',M'' \\ N,N',N'' \end{smallmatrix}\right) = g'''$ ist offenbar eine ternäre Form mit der Determinante 1. Da außerdem nach Voraussetzung a, b, c nicht alle dasselbe Vorzeichen haben, ist f eine indefinite Form. Daraus folgt leicht, dass auch g' und g''' indefinit sein müssen. Daher ist g''' zur Form $\left(\begin{smallmatrix} 1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$ äquivalent (Art. 277), und man kann eine Transformation (S') der ersten in die zweite finden. Offenbar geht aber durch (S') die Form g' in g'' über. Somit ist auch g'' unter f enthalten, und aus der Verbindung der Substitutionen $(S), (S')$ folgt eine Transformation der Form f in g''. Ist diese

$$\begin{array}{lll} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{array}$$

so erhält man offenbar zwei Lösungen der Gleichung (Ω), nämlich $x = \delta', y = \varepsilon', z = \zeta'$ und $x = \delta'', y = \varepsilon'', z = \zeta''$. Zugleich ist klar, dass in keiner der beiden Wertgruppen alle Werte $= 0$ werden können, da notwendig

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d. \quad \text{Wie verlangt.}$$

Beispiel. Die gegebene Gleichung sei $7xx - 15yy + 23zz = 0$. Sie ist lösbar, weil $345\,R\,7, -161\,R\,15, 105\,R\,23$. Hier sind die Werte von $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ gleich $3, 7, 6$; setzt man $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$, so findet man $A = 98, B = -39, C = -8$. Daraus erhält man die Substitution

$$\left\{\begin{array}{rrr} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{array}\right\}$$

durch die f in $\left(\begin{smallmatrix} 1520,14490,-7245 \\ -2415,-1246,4735 \end{smallmatrix}\right) = g$ übergeht. Daher ist

$$(S) = \left\{\begin{array}{rrr} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{array}\right\}, \quad g''' = \left(\begin{smallmatrix} 3670800,6,-3 \\ -1,-1246,4735 \end{smallmatrix}\right).$$

Man findet, dass die Form g''' in $\left(\begin{smallmatrix} 1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$ durch die Substitution

$$\left\{\begin{array}{rrr} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{array}\right\} \ldots (S')$$

übergeht. Verbindet man diese mit (S), so ergibt sich $\left\{\begin{smallmatrix}9,11.12\\-1,9,-9\\-9,4,3\end{smallmatrix}\right\}$, durch die f in g'' übergeht. Wir haben also zwei Lösungen der gegebenen Gleichung, $x = 11, y = 9, z = 4$ und $x = 12, y = -9, z = 3$. Die zweite wird einfacher, wenn man die Werte durch den gemeinsamen Teiler 3 dividiert; daraus folgt $x = 4, y = -3, z = 1$.

295.

Den zweiten Teil des Satzes im vorigen Artikel kann man auch wie folgt beweisen. Man suche eine ganze Zahl h so, dass $ah \equiv \mathfrak{C} \pmod{c}$ ist (die Zeichen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ verwenden wir im selben Sinn wie im vorigen Artikel), und setze $ahh + b = ci$. Dann sieht man leicht, dass i ganzzahlig und die Zahl $-ab$ die Determinante der binären Form $(ac, ah, i) \ldots \varphi$ ist. Diese Form ist sicher nicht positiv (denn da nach Voraussetzung a, b, c nicht alle dasselbe Vorzeichen haben, können ab und ac nicht zugleich positiv sein). Ferner hat sie die charakteristische Zahl -1, was wir wie folgt synthetisch beweisen: Man bestimme ganze Zahlen e, e' so, dass

$$\begin{aligned} e &\equiv 0 \pmod{a} \text{ und } \equiv \mathfrak{B} \pmod{b};\\ ce' &\equiv \mathfrak{A} \pmod{a} \text{ und } \equiv h\mathfrak{B} \pmod{b} \end{aligned}$$

Dann ist (e, e') ein Wert des Ausdrucks $\sqrt{} - (ac, ah, i) \pmod{-ab}$. Denn modulo a ist

$$\begin{aligned} ee \equiv 0 \equiv -ac, \quad ee' \equiv 0 \equiv -ah\\ cce'e' \equiv \mathfrak{A}\mathfrak{A} \equiv -bc \equiv -cci \quad \text{also } e'e' \equiv -i \end{aligned}$$

modulo b dagegen

$$\begin{aligned} ee \equiv \mathfrak{B}\mathfrak{B} \equiv -ac, \quad cee' \equiv h\mathfrak{B}\mathfrak{B} \equiv -ach \quad \text{also } ee' \equiv -ah\\ cce'e' \equiv hh\mathfrak{B}\mathfrak{B} \equiv -achh \equiv -cci \quad \text{also } e'e' \equiv -i \end{aligned}$$

Dieselben drei Kongruenzen, die für beide Moduln a, b gelten, gelten aber auch modulo ab. Aus der Theorie der ternären Formen folgt leicht, dass φ durch die Form $\left(\begin{smallmatrix}-1,0,0\\1,0,0\end{smallmatrix}\right)$ darstellbar ist. Es sei also

$$actt + 2ahtu + iuu = -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Durch Multiplikation mit c erhält man

$$a(ct + hu)^2 + buu = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Gibt man nun t, u bestimmte Werte, sodass entweder $\gamma t + \delta u$ oder $\varepsilon t + \zeta u = 0$ wird, so hat man eine Lösung der Gleichung Ω. Dieser genügen daher sowohl

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha\delta - \beta\gamma$$

als auch

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha\zeta - \beta\varepsilon$$

Dabei ist klar, dass weder die ersten noch die zweiten Werte sämtlich $= 0$ werden können. Denn wäre $\delta c - \gamma h = 0, \gamma = 0$, so wäre auch $\delta = 0$ und $\varphi = -(\alpha t +$

$\beta u)^2$, woraus $ab = 0$ folgte, entgegen der Voraussetzung; ebenso bei den anderen Werten. — In unserem Beispiel finden wir als Form φ die Form $(161, -63, 24)$, als Wert des Ausdrucks $\sqrt{} - \varphi \pmod{105} = (7, -51)$ und als Darstellung der Form φ durch $\left(\begin{smallmatrix} -1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$ die folgende:

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$$

Daraus folgen die Lösungen $x = 7, y = 11, z = -8$; $x = 20, y = 15, z = -5$, oder nach Division durch 5 und Vernachlässigung des Vorzeichens von z die Lösung $x = 4, y = 3, z = 1$.

Von diesen beiden Methoden zur Lösung der Gleichung Ω hat die zweite den Vorteil, dass man meist mit kleineren Zahlen auskommt. Die erste, die sich auch durch verschiedene hier übergangene Kunstgriffe verkürzen lässt, erscheint aber eleganter, besonders weil die Zahlen a, b, c ganz gleich behandelt werden und sich die Rechnung durch keine Vertauschung dieser Zahlen ändert. Anders bei der zweiten Methode: Hier ergibt sich meist die bequemste Rechnung, wenn man für a die kleinste und für c die größte der drei gegebenen Zahlen nimmt, wie wir es in unserem Beispiel getan haben.

Über die Methode, mit der der berühmte Le Gendre den Fundamentalsatz behandelte.

296.

Den eleganten Satz der vorigen Artikel hat zuerst der berühmte Le Gendre gefunden, *Hist. de l'Ac. de Paris* 1784, S. 507, und mit einem schönen, von unseren beiden ganz verschiedenen Beweis versehen. Zugleich versuchte dieser ausgezeichnete Geometer dort, daraus einen Beweis von Sätzen abzuleiten, die mit dem Fundamentalsatz des vorigen Abschnitts übereinstimmen. Dass uns dieser Beweis für diesen Zweck ungeeignet erscheint, haben wir schon oben in Art. 151 erklärt. Hier ist daher der Ort, diesen an sich sehr eleganten Beweis kurz darzustellen und die Gründe für unser Urteil hinzuzufügen. Wir schicken die folgende Bemerkung voraus: *Sind die Zahlen* a, b, c *sämtlich* $\equiv 1 \pmod 4$*, so kann die Gleichung* $axx + byy + czz = 0 \ldots (\Omega)$ *nicht lösbar sein.* Denn man sieht sehr leicht, dass der Wert von $axx + byy + czz$ in diesem Fall notwendig entweder $\equiv 1$, $\equiv 2$ oder $\equiv 3 \pmod 4$ ist, sofern nicht alle x, y, z zugleich gerade gewählt werden. Wäre also Ω lösbar, so nur durch gerade Werte von x, y, z, *was ein Widerspruch ist*, da beliebige Werte, die der Gleichung Ω genügen, ihr auch nach Division durch ihren größten gemeinsamen Teiler genügen, wobei notwendig mindestens ein ungerader Wert herauskommen muss. Die verschiedenen Fälle des zu beweisenden Satzes lassen sich nun auf die folgenden Punkte zurückführen.

I. Seien p, q Primzahlen der Form $4n + 3$ (positiv und ungleich). Dann kann nicht zugleich $p\,R\,q, q\,R\,p$ sein. Wäre dies nämlich möglich, so wären mit $1 = a, -p = b, -q = c$ offenbar alle Bedingungen für die Lösbarkeit der Gleichung $axx+byy+czz = 0$ erfüllt (Art. 294). Nach der vorigen Bemerkung hat sie aber keine Lösung; die Annahme kann also nicht bestehen. Daraus folgt sofort Satz 7 in Art. 131.

II. Ist p eine Primzahl der Form $4n + 1$ und q eine Primzahl der Form $4n + 3$, so kann nicht zugleich $q\,R\,p, p\,N\,q$ sein. Sonst wäre nämlich $-p\,R\,q$ und die Gleichung

$xx + pyy - qzz = 0$ lösbar, die nach der vorigen Bemerkung keine Lösung zulässt. Daraus folgen die Fälle 4 und 5 in Art. 131.

III. Sind p, q Primzahlen der Form $4n + 1$, so kann nicht zugleich $p\,R\,q, q\,N\,p$ sein. Man nehme eine andere Primzahl r der Form $4n + 3$, die Rest von q ist und von der p Nichtrest ist. Nach den gerade bewiesenen Fällen (II) ist dann $q\,R\,r, r\,N\,p$. Wäre also $p\,R\,q, q\,N\,p$, so wäre $qr\,R\,p, pr\,R\,q, pq\,N\,r$ und daher $-pq\,R\,r$. Somit wäre die Gleichung $pxx + qyy - rzz = 0$ lösbar, entgegen der vorigen Bemerkung; die Annahme kann also nicht bestehen. Daraus folgen die Fälle 1 und 2 in Art. 131.

Dieser Fall lässt sich auf folgende Weise übersichtlicher behandeln. Sei r eine Primzahl der Form $4n + 3$, von der p Nichtrest ist. Dann ist auch $r\,N\,p$, also (unter der Annahme $p\,R\,q, q\,N\,p$) $qr\,R\,p$. Ferner ist $-p\,R\,q, -p\,R\,r$ und somit auch $-p\,R\,qr$; daher wäre die Gleichung $xx + pyy - qrzz = 0$ lösbar, entgegen der vorigen Bemerkung. Daraus usw.

IV. Ist p eine Primzahl der Form $4n + 1$ und q eine Primzahl der Form $4n + 3$, so kann nicht zugleich $p\,R\,q, q\,N\,p$ sein. Man nehme eine Hilfsprimzahl r der Form $4n + 1$, die Nichtrest von beiden p, q ist. Dann ist (nach II) $q\,N\,r$ und (nach III) $p\,N\,r$, also $pq\,R\,r$. Wäre daher $p\,R\,q, q\,N\,p$, so wäre auch $pr\,N\,q, -pr\,R\,q, qr\,R\,p$ und die Gleichung $pxx - qyy + rzz = 0$ lösbar, *was ein Widerspruch ist.* — Daraus folgen die Fälle 3 und 6 in Art. 131.

V. Seien p, q Primzahlen der Form $4n + 3$. Dann kann nicht zugleich $p\,N\,q, q\,N\,p$ sein. Angenommen, dies wäre möglich, und man nehme eine Hilfsprimzahl r der Form $4n + 1$, die Nichtrest von beiden p, q ist. Dann wäre $qr\,R\,p, pr\,R\,q$, ferner (nach II) $p\,N\,r, q\,N\,r$, also $pq\,R\,r$ und $-pq\,R\,r$. Somit wäre die Gleichung $-pxx - qyy + rzz = 0$ möglich, entgegen der vorigen Bemerkung. Daraus folgt Fall 8 in Art. 131.

297.

Wer den vorigen Beweis genauer betrachtet, erkennt leicht, dass die Fälle I und II ohne Einwand erledigt sind. Die Beweise der übrigen Fälle stützen sich aber auf die Existenz von Hilfszahlen. Solange diese nicht bewiesen ist, verliert die Methode offenbar jede Beweiskraft. Diese Annahmen mögen so einleuchtend sein, dass sie einem weniger aufmerksamen Leser gar keines Beweises zu bedürfen scheinen, und sie heben den zu beweisenden Satz gewiss auf den höchsten Grad der *Wahrscheinlichkeit*; verlangt man aber geometrische Strenge, so darf man sie keinesfalls ohne Beweis zulassen. Was die Annahme in IV und V betrifft, es gebe eine Primzahl r der Form $4n+1$, die Nichtrest zweier anderer gegebener Primzahlen p, q ist, so folgt aus Abschnitt IV leicht, dass alle Zahlen unter $4pq$, die dazu teilerfremd sind (ihre Anzahl ist $2(p-1)(q-1)$), gleichmäßig auf vier Klassen verteilt sind. Eine enthält Nichtreste von beiden p, q, die übrigen drei Reste von p und Nichtreste von q, Nichtreste von p und Reste von q sowie Reste von beiden p, q. In jeder Klasse ist die Hälfte der Zahlen von der Form $4n+1$, die andere von der Form $4n+3$. Es gibt darunter also $\frac{1}{4}(p-1)(q-1)$ Nichtreste von beiden p, q der Form $4n+1$; diese seien $g.g', g''$ usw. Die übrigen $\frac{7}{4}(p-1)(q-1)$ Zahlen seien h, h', h'' usw. Offenbar sind alle in den Formen $4pqt+g, 4pqt+g', 4pqt+g''$ usw. (G) enthaltenen Zahlen ebenfalls Nichtreste von p, q der Form $4n+1$. Um die Annahme zu begründen, braucht man daher nur zu beweisen, dass unter den Formen (G) sicher *Primzahlen* vorkommen. Das erscheint schon an sich sehr plausibel, da diese Formen zusammen mit $4pqt+h, 4pqt+h'$ usw. (H) alle zu $4pq$ teilerfremden Zahlen und somit auch alle Primzahlen (außer $2, p, q$) umfassen. Es scheint kein Grund vorzuliegen, weshalb die Reihe der Primzahlen nicht gleichmäßig auf jene Formen verteilt sein sollte, sodass ein Achtel auf (G), die übrigen auf (H) entfallen. Eine solche Überlegung ist aber offenbar weit von geometrischer Strenge entfernt. Der berühmte Le Gendre selbst räumt ein, dass der Beweis des Satzes, unter einer solchen Form $kt+l$ mit gegebenen teilerfremden Zahlen k, l und veränderlichem t kämen sicher Primzahlen vor, ziemlich schwierig erscheine. Er deutet beiläufig eine Methode an, die vielleicht dorthin führen könnte. Uns scheinen aber viele Voruntersuchungen nötig, bevor man wenigstens auf diesem Weg zu einem strengen Beweis gelangen kann. — — Zur anderen Annahme (III, zweite Methode), es gebe eine Primzahl r der Form $3n+3$, von der eine andere gegebene Primzahl p der Form $4n+1$ Nichtrest ist, hat der berühmte Le Gendre überhaupt nichts hinzugefügt. Wir haben oben in Art. 129 bewiesen, dass es sicher Primzahlen gibt, von denen p Nichtrest ist. Unsere Methode scheint aber kaum geeignet, die Existenz solcher Primzahlen nachzuweisen, *die zugleich von der Form* $4n+3$ sind, wie es hier, aber nicht in unserem ersten Beweis nötig ist. Die Wahrheit dieser Annahme können wir allerdings so leicht beweisen: Nach Art. 287 gibt es ein positives Geschlecht binärer Formen mit der Determinante $-p$ und dem Charakter $3, 4$; Np. Sei (a, b, c) eine solche Form und a ungerade, was wir voraussetzen dürfen. Dann ist a von der Form $4n+3$ und entweder selbst eine Primzahl oder hat wenigstens einen Primfaktor r der Form $4n+3$. Es ist aber $-pRa$, also auch $-pRr$, woraus pNr folgt. Dabei muss man sorgfältig beachten, dass sich die Sätze aus Art. 263, 287 auf den Fundamentalsatz stützen. Es wäre also ein Zirkelschluss, einen Teil dieses Satzes darauf zu gründen. — — Schließlich ist die Annahme in III der ersten Methode noch viel weniger begründet, sodass wir hier

nichts weiter darüber hinzuzufügen brauchen.

Wir fügen noch eine Bemerkung zu Fall V hinzu, der durch die vorige Methode zwar nicht ausreichend bewiesen, durch die folgende aber bequem erledigt wird. Wäre dort zugleich pNq, qNp, so wäre $-pRq, -qRp$. Daraus folgt leicht, dass -1 eine charakteristische Zahl der Form $(p, 0, q)$ ist, die daher nach der Theorie der ternären Formen durch $xx + yy + zz$ dargestellt werden kann. Es sei

$$ptt + quu = (\alpha t + \beta u)^2 + (\alpha' t + \beta' u)^2 + (\alpha'' t + \beta'' u)^2$$

oder

$$\begin{aligned} \alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' &= p, \\ \beta\beta + \beta'\beta' + \beta''\beta'' &= q, \\ \alpha\beta + \alpha'\beta' + \alpha''\beta'' &= 0 \end{aligned}$$

Dann sind nach den Gleichungen 1 und 2 alle $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ ungerade; die dritte Gleichung kann aber dann offenbar nicht bestehen. — Auf ganz ähnliche Weise lässt sich auch Fall II erledigen.

298.

Aufgabe. *Es seien a, b, c beliebige Zahlen, von denen keine $= 0$ ist. Gesucht sind die Bedingungen für die Lösbarkeit der Gleichung*

$$axx + byy + czz = 0 \ldots (\omega).$$

Lösung. Es seien $\alpha\alpha, \beta\beta, \gamma\gamma$ die größten Quadrate, die der Reihe nach bc, ac, ab teilen, und es sei $\alpha a = \beta\gamma A,\ \beta b = \alpha\gamma B,\ \gamma c = \alpha\beta C$. Dann sind A, B, C paarweise teilerfremde ganze Zahlen. Die Gleichung (ω) ist genau dann lösbar, wenn

$$AXX + BYY + CZZ = 0 \ldots (\Omega)$$

lösbar ist. Das lässt sich nach Art. 294 entscheiden.

Beweis. Man setze $bc = \mathfrak{A}\alpha\alpha,\ ac = \mathfrak{B}\beta\beta,\ ab = \mathfrak{C}\gamma\gamma$. Dann sind $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ganze Zahlen ohne quadratische Faktoren, und es gilt $\mathfrak{A} = BC,\ \mathfrak{B} = AC,\ \mathfrak{C} = AB$. Daraus folgt $\mathfrak{A}\mathfrak{B}\mathfrak{C} = (ABC)^2$, also ist $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ notwendig eine ganze Zahl. Der größte gemeinsame Teiler der Zahlen $\mathfrak{A}, A\mathfrak{A}$ sei m, und es sei $\mathfrak{A} = gm,\ A\mathfrak{A} = hm$. Dann ist g teilerfremd zu h und, da $\mathfrak{A}$ keine quadratischen Faktoren hat, auch zu m. Nun gilt $hhm = gAA\mathfrak{A} = g\mathfrak{B}\mathfrak{C}$, also teilt g die Zahl hhm. Das ist offenbar nur möglich, wenn $g = \pm 1$. Somit gilt $\mathfrak{A} = \pm m,\ A = \pm h$, also ist diese Zahl ganz; ebenso sind B, C ganz. *Damit ist die erste Behauptung bewiesen.* — Da $\mathfrak{A} = BC$ keine quadratischen Faktoren enthält, müssen B, C teilerfremd sein. Ebenso ist A teilerfremd zu C und zu B. *Damit ist die zweite Behauptung bewiesen.* — Wird schließlich (Ω) durch $X = P, Y = Q,\ Z = R$ erfüllt, so wird offenbar (ω) durch $x = \alpha P, y = \beta Q, z = \gamma R$ gelöst. Wird umgekehrt diese durch $x = p, y = q, z = r$ erfüllt, so wird jene durch $X = \beta\gamma p,\ Y = \alpha\gamma q, Z = \alpha\beta r$ erfüllt. Also sind entweder beide lösbar oder keine. *Damit ist die dritte Behauptung bewiesen.*

Darstellung der Null durch beliebige ternäre Formen.

299.

Aufgabe. *Für eine gegebene ternäre Form*

$$f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

ist zu entscheiden, ob sie die Null darstellen kann, wobei die Werte der Unbestimmten nicht alle $= 0$ sein dürfen.

Lösung. I. Ist $a = 0$, so können die Werte von x', x'' beliebig gewählt werden. Aus der Gleichung

$$a'x'x' + 2bx'x'' + a''x''x'' = -2x(b'x'' + b''x')$$

ergibt sich offenbar ein bestimmter rationaler Wert für x. Ergibt sich auf diese Weise für x ein Bruch, so braucht man die Werte von x, x', x'' nur mit dessen Nenner zu multiplizieren, um ganze Zahlen zu erhalten. Auszuschließen sind nur die Werte von x', x'', die $b'x'' + b''x' = 0$ ergeben, sofern sie nicht zugleich $a'x'x' + 2bx'x'' + a''x''x'' = 0$ ergeben; in diesem Fall kann x beliebig gewählt werden. Offenbar erhält man so alle möglichen Lösungen. Der Fall, dass b' null ist und $b'' = 0$ gilt, gehört allerdings nicht

hierher: Dann kommt x in f nicht vor, also ist f eine binäre Form. Ob die Null durch f darstellbar ist, muss dann nach der Theorie dieser Formen entschieden werden.

II. Gilt dagegen nicht $a = 0$, so ist die Gleichung $f = 0$ gleichbedeutend mit

$$(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = 0$$

wobei man

$$b''b'' - aa' = A'',$$
$$ab - b'b'' = B,$$
$$b'b' - aa'' = A'$$

setzt. Ist hier $A' = 0$, aber nicht $B = 0$, so ergeben sich bei beliebiger Wahl von $ax + b''x' + b'x''$ und x'' offenbar rationale Werte für x und x'. Sind sie nicht ganz, so werden sie wenigstens durch einen geeigneten Multiplikator ganz. Für den einen Wert von x'', nämlich $x'' = 0$, ist der Wert von $ax + b''x' + b'x''$ nicht beliebig, sondern muss ebenfalls $= 0$ gesetzt werden. Dann kann aber x' beliebig gewählt werden und liefert einen rationalen Wert für x. — Ist dagegen zugleich A'' null und gilt $B = 0$, und ist A' ein Quadrat $= kk$, so zerfällt $f = 0$ offenbar in die beiden linearen Gleichungen

$$ax + b''x' + (b' + k)x'' = 0,$$
$$ax + b''x' + (b' - k)x'' = 0$$

von denen *entweder* die eine *oder* die andere gelten muss. Ist hingegen unter derselben Voraussetzung A' kein Quadrat, so hängt die Lösung der vorgelegten Gleichung offenbar von $x'' = 0$ und $ax + b''x' = 0$ ab, die *zugleich* gelten müssen.

Es braucht kaum erwähnt zu werden, dass die Methode in I auch anwendbar ist, wenn a' null ist oder $a'' = 0$ gilt, und die Methode in II, wenn $A' = 0$.

III. Ist dagegen weder a null, noch gilt $A'' = 0$, so ist $f = 0$ gleichbedeutend mit

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''x'' = 0$$

wobei D die Determinante der Form f bezeichnet oder Da die Zahl $BB - A'A''$. Ist $D = 0$, so verhält sich die Lösung ähnlich wie am Ende des vorigen Falls. Ist nämlich A'' ein Quadrat $= kk$, so zerfällt die vorgelegte Gleichung in

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0,$$
$$kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$$

ist dagegen A'' kein Quadrat, so muss

$$ax + b''x' + b'x'' = 0,$$
$$A''x' - Bx'' = 0$$

gelten. Ist aber D nicht $= 0$, so sind wir auf die Gleichung

$$A''tt - uu + Davv = 0$$

geführt, deren Lösbarkeit sich nach dem vorigen Artikel entscheiden lässt. Hat diese nur die Lösung $t = 0,\ u = 0,\ v = 0$, so hat offenbar auch die vorgelegte keine andere

Lösung als $x = 0,\ x' = 0,\ x'' = 0$. Ist jene aber anders lösbar, so ergeben sich aus beliebigen solchen ganzzahligen Werten von t, u, v durch die Gleichungen

$$ax + b''x' + b'x'' = t,$$
$$A''x' - Bx'' = u,$$
$$x'' = v$$

wenigstens rationale Werte von x, x', x''. Enthalten diese Brüche, so erhält man durch einen geeigneten Multiplikator ganze Zahlen.

Sobald aber *eine* ganzzahlige Lösung von $f = 0$ gefunden ist, kann man die Aufgabe auf Fall I zurückführen und wie dort sämtliche Lösungen auf folgende Weise angeben. Die Gleichung $f = 0$ werde durch die Werte von x, x', x'' erfüllt, nämlich $\alpha, \alpha', \alpha''$, die wir ohne gemeinsamen Faktor voraussetzen. Nach Art. 40, 279 wähle man ganze Zahlen $\beta, \beta', \beta'',\ \gamma, \gamma', \gamma''$ so, dass

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1$$

und es gehe f durch die Substitution

$$x = \alpha y + \beta y' + \gamma y''.$$
$$x' = \alpha' y + \beta' y' + \gamma' y'',$$
$$x'' = \alpha'' y + \beta'' y' + \gamma'' y'' \ldots (S)$$

in

$$g = cyy + c'y'y' + c''y''y'' + 2dy'y'' + 2d'yy'' + 2d''yy'$$

über. Dann ist offenbar $c = 0$, und g ist zu f äquivalent. Daher ergeben sich aus allen Lösungen von $g = 0$ durch S sämtliche ganzzahligen Lösungen von $f = 0$. Nach I sind nun alle Lösungen von $g = 0$ in den Formeln

$$y = -z(c'pp + 2dpq + c''qq),$$
$$y' = 2z(d''pp + d'pq),$$
$$y'' = 2z(d''pq + d'qq)$$

enthalten. Dabei bezeichnen p, q beliebige ganze Zahlen und z eine beliebige Zahl, für die auch Brüche zugelassen sind, sofern y, y', y'' ganz bleiben. Setzt man diese Werte von y, y', y'' in (S) ein, so erhält man alle ganzzahligen Lösungen von $f = 0$. — Ist zum Beispiel

$$f = xx + x'x' + x''x'' - 4x'x'' + 2xx'' + 8xx'$$

und hat man eine Lösung von $f = 0$, nämlich $x = 1,\ x' = -2,\ x'' = 1$, so ergibt sich für $\beta, \beta', \beta'',\ \gamma, \gamma', \gamma'' = 0, 1, 0, 0, 0, 1$

$$g = y'y' + y''y'' - 4y'y'' + 12yy''$$

Damit sind sämtliche ganzzahligen Lösungen von $g = 0$ in der Formel

$$y = -z(pp - 4pq + qq),$$
$$y' = 12zpq,$$
$$y'' = 12zqq$$

enthalten und somit alle Lösungen von $f = 0$ in

$$x = -z(pp - 4pq + qq)$$
$$x' = 2z(pp + 2pq + qq)$$
$$x'' = -z(pp - 4pq - 11qq)$$

Allgemeine Lösung unbestimmter Gleichungen zweiten Grades mit zwei Unbekannten durch rationale Zahlen.

300.

Aus der Aufgabe des vorigen Artikels ergibt sich unmittelbar die Lösung der unbestimmten Gleichung

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

wenn nur rationale Werte verlangt werden. Für ganzzahlige Werte haben wir sie schon oben in Art. 216 und den folgenden Artikeln gelöst. Denn sämtliche rationalen Werte von x, y lassen sich als $\frac{t}{v}, \frac{u}{v}$ schreiben, wobei t, u, v ganz sind. Die Lösung jener Gleichung durch rationale Zahlen ist also offenbar gleichbedeutend mit der ganzzahligen Lösung von

$$att + 2btu + cuu + 2dtv + 2euv + fvv = 0$$

und diese stimmt mit der im vorigen Artikel behandelten Gleichung überein. Auszuschließen sind nur die Lösungen mit $v = 0$; solche können aber nicht auftreten, wenn $bb - ac$ kein Quadrat ist. So sind zum Beispiel alle rationalen Lösungen der Gleichung

$$xx + 8xy + yy + 2x - 4y + 1 = 0$$

die in Art. 221 allgemein durch ganze Zahlen gelöst wurde, in der Formel

$$x = \frac{pp - 4pq + qq}{pp - 4pq - 11qq},$$
$$y = -\frac{2pp + 4pq + 2qq}{pp - 4pq - 11qq}$$

enthalten, wobei p, q beliebige ganze Zahlen sind. — Wir haben diese beiden eng verbundenen Aufgaben hier nur kurz behandelt und viele zugehörige Bemerkungen weggelassen, teils um nicht zu ausführlich zu werden, teils weil wir eine andere Lösung der Aufgabe des vorigen Artikels haben, die auf allgemeineren Grundsätzen beruht. Da ihre Darstellung eine tiefere Untersuchung der ternären Formen verlangt, müssen wir sie einer anderen Gelegenheit vorbehalten.

Über die durchschnittliche Anzahl der Geschlechter.

301.

Wir kehren zu den binären Formen zurück, von denen noch mehrere bemerkenswerte Eigenschaften zu besprechen sind. Zunächst fügen wir einige Bemerkungen zur Anzahl der Geschlechter und Klassen in der eigentlich primitiven Ordnung hinzu, bei negativer Determinante in der positiven. Auf diese Ordnung beschränken wir der Kürze wegen die Untersuchung.

Die *Anzahl der Geschlechter*, in die sich alle eigentlich primitiven Formen, bei negativer Determinante die positiven, einer gegebenen positiven oder negativen Determinante $\pm D$ verteilen, ist immer $1, 2, 4$ oder eine höhere Potenz von 2. Ihr Exponent hängt von den Faktoren von D ab und lässt sich aus den vorigen Untersuchungen vollständig im Voraus bestimmen. Da in der natürlichen Zahlenreihe Primzahlen mit mehr oder weniger zusammengesetzten Zahlen vermischt sind, nimmt die Anzahl der Geschlechter bei mehreren aufeinanderfolgenden Determinanten $\pm D, \pm(D+1), \pm(D+2)$ usw. bald zu, bald ab, und diese unregelmäßige Reihe scheint keine Ordnung zu haben. Addiert man aber die Anzahlen der Geschlechter für viele aufeinanderfolgende Determinanten

$$\pm D, \quad \pm(D+1) \ \ldots \ \pm(D+m)$$

und teilt die Summe durch die Anzahl der Determinanten, so erhält man die *durchschnittliche Anzahl der Geschlechter*. Diese kann man etwa der mittleren Determinante $\pm(D + \frac{1}{2}m)$ zuordnen; sie bildet eine sehr regelmäßige Folge. Dabei setzen wir nicht nur voraus, dass m hinreichend groß ist, sondern auch, dass D noch viel größer ist, sodass das Verhältnis der äußersten Determinanten $D, D+m$ nicht zu stark von der Gleichheit abweicht. Die Regelmäßigkeit dieser Folge ist so zu verstehen: Ist D' viel größer als D, so ist die durchschnittliche Anzahl der Geschlechter um die Determinante $\pm D'$ merklich größer als um D. Unterscheiden sich dagegen D, D' nicht zu stark, so sind auch die durchschnittlichen Anzahlen der Geschlechter um D und D' nahezu gleich. Ferner findet man die durchschnittliche Anzahl der Geschlechter um die positive Determinante $+D$ stets nahezu gleich der durchschnittlichen Anzahl um die negative, und zwar umso genauer, je größer D ist. Für einen kleinen Wert ist die erste etwas größer als die zweite. Das verdeutlichen die folgenden Beispiele aus einer Klassifikationstafel der binären Formen für mehr als 4000 Determinanten. Unter den hundert Determinanten von 801 bis 900 gibt es 7, denen nur ein Geschlecht entspricht, sowie $32, 52, 8, 1$, denen der Reihe nach $2, 4, 8$. 16 Geschlechter entsprechen. Insgesamt ergeben sich also 359 Geschlechter und damit die durchschnittliche Anzahl = 3,59. Die hundert negativen Determinanten von -801 bis 900 ergeben 360 Geschlechter. Alle folgenden Beispiele stammen von negativen Determinanten. Im 16. Hunderter, von -1501 bis -1600, findet man die durchschnittliche Anzahl 3,89; im 25. Hunderter 4,03; im 51. Hunderter 4,24; aus den sechshundert Determinanten $-9401 \ \ldots - 10000$ ergibt sich 4,59. Diese Beispiele zeigen, dass die durchschnittliche Anzahl der Geschlechter viel langsamer wächst als die Determinanten selbst. Nach welchem Gesetz verläuft aber diese Folge? — Eine ziemlich schwierige theoretische Untersuchung, deren Darstellung hier zu ausführlich wäre, hat ergeben, dass die

durchschnittliche Anzahl der Geschlechter um die Determinante $+D$ oder $-D$ sehr nahe durch die Formel

$$\alpha \log D + \beta$$

gegeben wird. Dabei sind α, β Konstanten, und zwar

$$\alpha = \frac{4}{\pi\pi} = 0{,}4052847346$$

wobei π den halben Umfang eines Kreises mit dem Radius 1 bezeichnet, und

$$\beta = 2\alpha g + 3\alpha\alpha h - \frac{1}{6}\alpha \log 2 = 0{,}8830460462$$

wobei g die Summe der Reihe

$$1 - \log(1+1) + \frac{1}{2} - \log(1+\frac{1}{2}) + \frac{1}{3} - \log(1+\frac{1}{3}) + \text{etc.} = 0{,}5772156649$$

ist (siehe Euler, *Inst. Calc. Diff.*, S. 444), während h die Summe der Reihe

$$\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 + \text{etc.}$$

ist, die durch Näherung = 0,9375482543 gefunden wurde. Aus dieser Formel folgt, dass die durchschnittliche Anzahl der Geschlechter in einer arithmetischen Folge wächst, wenn die Determinanten in einer geometrischen Folge wachsen. Für $D = 850\frac{1}{2}, 1550\frac{1}{2}, 2450\frac{1}{2}, 5050\frac{1}{2}, 9700\frac{1}{2}$ ergeben sich die Werte $3{,}617; 3{,}86; 4{,}046; 4{,}339; 4{,}604$, die von den oben angegebenen Durchschnittswerten wenig abweichen. Je größer die mittlere Determinante ist und je mehr Determinanten zur Berechnung des Durchschnitts dienen, desto weniger weicht er vom Wert der Formel ab. Mit dieser Formel lässt sich auch die Summe der Anzahlen der Geschlechter für aufeinanderfolgende Determinanten $\pm D, \pm(D+1) \ldots \pm (D+m)$ sehr nahe bestimmen, wie verschieden die äußersten $D, D+m$ auch sein mögen: Man berechnet die jeweils zugehörigen Durchschnittswerte und addiert sie. Diese Summe ist

$$= \alpha(\log D + \log(D+1) + \text{etc.} + \log(D+m)) + \beta(m+1)$$

oder hinreichend genau

$$= \alpha((D+m)\log(D+m) - (D-1)\log(D-1)) + (\beta - \alpha)(m+1)$$

So ergibt sich für die Summe der Geschlechterzahlen der Determinanten -1 bis -100 der Wert = 234,4, während sie tatsächlich 233 beträgt; ebenso von -1 bis -2000 der Wert = 7116,6, während sie 7112 beträgt; von -9001 bis -10000, wo sie 4595 beträgt, gibt die Formel 4594,9. Eine solche Übereinstimmung hätte man kaum erwarten können.

Über die durchschnittliche Anzahl der Klassen.

302.

Hinsichtlich der *Anzahl der Klassen*, wobei stets eigentlich primitive Klassen gemeint sind, bei negativer Determinante die positiven, verhalten sich positive Determinanten ganz anders als negative. Deshalb betrachten wir beide getrennt. Sie stimmen darin überein, dass bei gegebener Determinante alle Geschlechter gleich viele Klassen enthalten. Somit ist die Gesamtzahl der Klassen gleich dem Produkt aus der Anzahl der Geschlechter und der Anzahl der Klassen in jedem Geschlecht.

Zunächst zu den negativen Determinanten: Die Anzahl der Klassen für mehrere aufeinanderfolgende Determinanten $-D, -(D+1), -(D+2)$ usw. bildet eine ebenso unregelmäßige Folge wie die Anzahl der Geschlechter. Die durchschnittliche Anzahl der Klassen, die keiner Definition bedarf, wächst dagegen sehr regelmäßig, wie die folgenden Beispiele zeigen. Die hundert Determinanten von -500 bis -600 ergeben 1729 Klassen, also die durchschnittliche Anzahl = 17,29. Ebenso findet man im 15. Hunderter die durchschnittliche Anzahl 28,26; aus den beiden Hundertern 24 und 25 ergibt sich 36,28; aus den drei 61, 62 und 63 erhält man 58,50; aus den fünf $91 \ldots 95$ ergibt sich 71,56; schließlich aus den fünf $96 \ldots 100$ der Wert 73,54. Diese Beispiele zeigen, dass die durchschnittliche Anzahl der Klassen zwar langsamer wächst als die Determinanten, aber viel schneller als die durchschnittliche Anzahl der Geschlechter. Bei einiger Aufmerksamkeit erkennt man, dass sie ziemlich genau im Verhältnis der Quadratwurzeln der mittleren Determinanten wächst. Tatsächlich haben wir durch eine theoretische Untersuchung gefunden, dass die durchschnittliche Anzahl der Klassen um die Determinante $-D$ näherungsweise durch

$$\gamma\sqrt{D} - \delta$$

ausgedrückt wird. Dabei ist

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$$

wobei e die Summe der Reihe

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} \text{ etc.}$$

bezeichnet.

Außerdem ist

$$\delta = 0{,}2026423673 = \frac{2}{\pi\pi}$$

Die nach dieser Formel berechneten Durchschnittswerte unterscheiden sich wenig von denen, die wir oben aus der Klassifikationstafel entnommen haben. Mit dieser Formel lässt sich auch die Summe der Anzahlen sämtlicher eigentlich primitiven Klassen, bei negativer Determinante der positiven, für aufeinanderfolgende Determinanten $-D, -(D+1), -(D+2) \ldots -(D+m-1)$ sehr nahe angeben, wie verschieden die

äußersten auch sein mögen. Man addiert die ihnen nach der Formel zugehörigen Durchschnittswerte und erhält

$$= \gamma(\sqrt{D} + \sqrt{(D+1)} + \text{etc.} + \sqrt{(D+m-1)}) - \delta m$$

oder sehr nahe

$$= \frac{2}{3}\gamma((D+m-\frac{1}{2})^{\frac{3}{2}} - (D-\frac{1}{2})^{\frac{3}{2}}) - \delta m$$

So berechnet sich zum Beispiel diese Summe für die hundert Determinanten $-1 \ldots -100$ nach der Formel = 481,1, während sie tatsächlich 477 beträgt. Die tausend Determinanten $-1 \ldots -1000$ liefern nach der Tafel 15533 Klassen, die Formel gibt 15551,4. Der zweite Tausender enthält nach der Tafel 28595 Klassen, die Formel gibt 28585,7; ebenso liefert der dritte Tausender tatsächlich 37092 Klassen, die Formel 37074,3; der zehnte Tausender gibt nach der Tafel 72549, nach der Formel 72572.

303.

Die nach ihren verschiedenen Klassifikationen geordnete Tafel der negativen Determinanten bietet viele weitere bemerkenswerte Beobachtungen. Bei Determinanten der Form $-(8n+3)$ ist die Anzahl der Klassen, sowohl in allen eigentlich primitiven Geschlechtern zusammen als auch in jedem einzelnen, stets durch 3 teilbar, mit der einzigen Ausnahme der Determinante -3. Der Grund folgt unmittelbar aus Art. 256, VI. Bei Determinanten, deren Formen nur ein Geschlecht bilden, ist die Anzahl der Klassen stets ungerade. Für eine solche Determinante gibt es nämlich nur eine ambige Klasse, die Hauptklasse. Die übrigen Klassen treten paarweise entgegengesetzt auf; ihre Anzahl muss also gerade und damit die Gesamtzahl ungerade sein. Diese letzte Eigenschaft gilt auch für positive Determinanten. — Ferner scheint die Reihe der Determinanten, denen dieselbe gegebene Klassifikation entspricht, also eine gegebene Anzahl sowohl der Geschlechter als auch der Klassen, stets abzubrechen. Diese ziemlich überraschende Beobachtung erläutern wir an einigen Beispielen. Die erste, römische Zahl bezeichnet die Anzahl der eigentlich primitiven Geschlechter, bei negativer Determinante der positiven; die folgende die Anzahl der Klassen in jedem Geschlecht. Danach folgt die Reihe der Determinanten mit dieser Klassifikation; ihr negatives Vorzeichen ist der Kürze wegen weggelassen.

I. 1 ...	1, 2, 3, 4, 7
I. 3 ...	11, 19, 23, 27, 31, 43, 67, 163
I. 5 ...	47, 79, 103. 127
I. 7 ...	71, 151, 223, 343, 463, 487
II. 1 ...	5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
II. 2 ...	14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193
IV. 1 ...	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
VIII. 1 ...	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345. 357, 385, 408, 462, 520, 760
XVI. 1 ...	840, 1320, 1365, 1848

Ebenso findet man 20 Determinanten, die größte $= -1423$, mit der Klassifikation I. 9; 4, die größte $= -1303$, mit der Klassifikation I. 11 usw. Den Klassifikationen II. 3; II. 4; II. 5; IV. 2 entsprechen der Reihe nach nicht mehr als $48, 31, 44, 69$ Determinanten, deren größte $-652, -862, -1318, -1012$ sind. Die Tafel, der wir diese Beispiele entnommen haben, ist weit über die größten hier vorkommenden Determinanten hinaus fortgesetzt worden*), ohne dass weitere zu diesen Klassifikationen gehörige Determinanten aufgetreten wären. Daher scheint kein Zweifel, dass die angegebenen Reihen wirklich abgebrochen sind, und nach Analogie darf man denselben Schluss auf jede andere Klassifikation ausdehnen. Da sich zum Beispiel im ganzen zehnten

*) Während des Drucks ist sie *ohne Unterbrechung* bis -3000 fortgesetzt, außerdem durch den ganzen zehnten Tausender und mehrere andere verstreute Hunderter, dazu sehr viele sorgfältig ausgewählte einzelne Determinanten.

Tausender der Determinanten keine mit weniger als 24 Klassen gezeigt hat, ist es höchst wahrscheinlich, dass die Klassifikationen I. 23; I. 21 usw.; II. 11; II. 10 usw.; IV. 5; IV. 4; IV. 3; VIII. 2 schon vor -9000 aufgehört haben oder wenigstens nur sehr wenigen Determinanten jenseits von -10000 zukommen. *Strenge* Beweise dieser Beobachtungen scheinen aber sehr schwierig. — Nicht weniger bemerkenswert ist, dass alle Determinanten, deren Formen sich auf 32 oder mehr Geschlechter verteilen, mindestens zwei Klassen in jedem Geschlecht haben. Die Klassifikationen XXXII. 1, LXIV. 1 usw. fallen also ganz weg; der kleinsten solchen Determinante, -9240, entspricht XXXII. 2. Es erscheint ziemlich wahrscheinlich, dass mit wachsender Anzahl der Geschlechter immer mehr Klassifikationen wegfallen. In dieser Hinsicht sind die oben angegebenen 65 Determinanten, denen die Klassifikationen I. 1; II. 1; IV. 1; VIII. 1; XVI. 1 entsprechen, sehr bemerkenswert. Man sieht leicht, dass sie alle und nur sie die beiden besonderen Eigenschaften haben, dass sämtliche zugehörigen Formenklassen ambig sind und beliebige Formen desselben Geschlechts notwendig sowohl eigentlich als auch uneigentlich äquivalent sind. Dieselben 65 Zahlen hat übrigens schon der berühmte Euler unter einem etwas anderen, unten zu erwähnenden Gesichtspunkt und mit einem leicht zu beweisenden Kriterium angegeben: *Nouv. Mém. de l'Ac. de Berlin*, 1776, S. 338.

304.

Die Anzahl der eigentlich primitiven Klassen binärer Formen mit einer positiven Determinante, die eine *Quadratzahl* kk ist, lässt sich vollständig im Voraus angeben. Sie ist gleich der Anzahl der zu $2k$ teilerfremden und darunterliegenden Zahlen. Daraus folgt durch nicht schwierige, hier aber zu übergehende Überlegungen, dass sich die durchschnittliche Anzahl der Klassen für solche Determinanten um kk näherungsweise durch $\frac{8k}{\pi\pi}$ ausdrückt. — Positive nichtquadratische Determinanten zeigen in dieser Hinsicht aber ganz besondere Erscheinungen. Eine kleine Klassenanzahl, zum Beispiel die Klassifikation I. 1 oder I. 3 oder II. 1 usw., tritt bei negativen und quadratischen Determinanten nur für kleine Werte auf und hört bald ganz auf. Dagegen liefert der weitaus größte Teil der positiven nichtquadratischen Determinanten, wenigstens der nicht sehr großen, Klassifikationen mit nur einer Klasse in jedem Geschlecht, sodass I. 3; I. 5; II. 2; II. 3; IV. 2 usw. sehr selten sind. So findet man zum Beispiel unter den 90 nichtquadratischen Determinanten unter 100 deren $11, 48, 27$ mit den Klassifikationen I. 1, II. 1, IV. 1 der Reihe nach. Nur eine, (37), hat I. 3; zwei, (34 und 82), haben II. 2; eine, (79), hat II. 3. Mit wachsenden Determinanten werden größere Klassenanzahlen aber allmählich häufiger. Unter den 96 nichtquadratischen Determinanten von 101 bis 200 haben zwei, $(101, 197)$, I. 3; vier, $(145, 146, 178, 194)$, II. 2; drei, $(141, 148, 189)$, II. 3. Von den 197 Determinanten von 801 bis 1000 haben drei I. 3; vier II. 2; vierzehn II. 3; zwei II. 5; zwei II. 6; fünfzehn IV. 2; sechs IV. 3; zwei IV. 4; vier VIII. 2; die übrigen 145 haben eine Klasse in jedem Geschlecht. — Es wäre eine interessante, des Scharfsinns der Mathematiker würdige Frage, nach welchem Gesetz die Determinanten mit einer Klasse in jedem Geschlecht immer seltener werden. Bisher können wir weder theoretisch entscheiden noch aus Beobachtungen mit hinreichender Sicherheit vermuten, ob sie schließlich ganz abbrechen, was allerdings wenig wahrscheinlich erscheint, oder wenigstens *unendlich selten* werden oder

ob ihre Häufigkeit sich immer mehr einer festen Grenze nähert. Die durchschnittliche Anzahl der Klassen wächst nur wenig schneller als die Anzahl der Geschlechter und weit langsamer als die Quadratwurzeln der Determinanten. Zwischen 800 und 1000 findet man sie $= 5,01$. Diesen Beobachtungen sei eine weitere hinzugefügt, die die Analogie zwischen positiven und negativen Determinanten gewissermaßen wiederherstellt. Wir haben nämlich gefunden, dass bei positiver Determinante D weniger die Klassenanzahl selbst als vielmehr ihr Produkt mit dem Logarithmus von $t + u\sqrt{D}$, wobei t, u die kleinsten, von $1, 0$ verschiedenen Lösungen der Gleichung $tt - Duu = 1$ sind, der Klassenanzahl bei negativer Determinante in mehreren, hier nicht näher auszuführenden Beziehungen entspricht. Der Durchschnittswert dieses Produkts wird ebenso genau durch eine Formel der Gestalt $m\sqrt{D} - n$ ausgedrückt. Die Werte der Konstanten m, n konnten wir bisher aber nicht theoretisch bestimmen. Soweit man aus dem Vergleich einiger Hunderter von Determinanten schließen darf, scheint m wenig von $2\frac{1}{3}$ abzuweichen. — Über die Grundsätze der vorigen Untersuchungen zu Durchschnittswerten von Größen, die keinem analytischen Gesetz folgen, sich einem solchen aber asymptotisch immer mehr nähern, behalten wir uns eine ausführlichere Behandlung bei anderer Gelegenheit vor. Wir gehen nun zu einer anderen Untersuchung über, die verschiedene eigentlich primitive Klassen derselben Determinante miteinander vergleicht und diesen langen Abschnitt abschließt.

Ein besonderer Algorithmus für eigentlich primitive Klassen: reguläre und irreguläre Determinanten usw.

305.

Satz. *Es bezeichne K die Hauptklasse der Formen einer gegebenen Determinante D und C eine beliebige andere Klasse im Hauptgeschlecht der Formen derselben Determinante. Ferner seien $2C, 3C, 4C$ usw. die Klassen, die durch Verdopplung, Verdreifachung, Vervierfachung usw. der Klasse C entstehen, wie in Art. 249. Setzt man die Folge $C, 2C, 3C$ usw. weit genug fort, so erreicht man schließlich eine mit K identische Klasse. Ist mC die erste mit K identische Klasse und die Gesamtzahl der Klassen im Hauptgeschlecht $= n$, so gilt entweder $m = n$, oder m ist ein echter Teiler von n.*

Beweis. I. Alle Klassen $K, C, 2C, 3C$ usw. gehören notwendig zum Hauptgeschlecht, nach Art. 247. Daher können die ersten $n + 1$ Klassen dieser Reihe, $K, C, 2C \ldots nC$, offenbar nicht alle verschieden sein. Also ist entweder K mit einer der Klassen $C, 2C, 3C \ldots nC$ identisch, oder wenigstens zwei dieser Klassen sind miteinander identisch. Es sei $rC = sC$ und $r > s$. Dann gilt auch

$$(r-1)C = (s-1)C, \quad (r-2)C = (s-2)C$$
$$\text{usw. und } (r+1-s)C = C$$

also $(r - s)C = K$. *Damit ist die erste Behauptung bewiesen.*

II. Daraus folgt auch unmittelbar entweder $m = n$ oder $m < n$. Es bleibt nur zu zeigen, dass im zweiten Fall m ein echter Teiler von n ist. Da die Klassen

$$K, C, 2C \ldots (m-1)C, \text{ deren Gesamtheit wir mit } \mathfrak{C}$$

bezeichnen, in diesem Fall das Hauptgeschlecht noch nicht ausschöpfen, sei C' eine Klasse dieses Geschlechts, die nicht in $\mathfrak{C}$ enthalten ist. Wir betrachten die Gesamtheit der Klassen, die durch Zusammensetzung von C' mit den einzelnen Klassen in $\mathfrak{C}$ entstehen, nämlich

$$C', C'+C, C'+2C \ldots C'+(m-1)C, \text{ mit der Bezeichnung } \mathfrak{C}'$$

Offenbar sind alle Klassen in $\mathfrak{C}'$ sowohl voneinander als auch von allen in $\mathfrak{C}$ verschieden und gehören zum Hauptgeschlecht. Schöpfen also $\mathfrak{C}$ und $\mathfrak{C}'$ dieses Geschlecht aus, so gilt $n = 2m$, andernfalls $2m < n$. Im zweiten Fall sei C'' eine Klasse des Hauptgeschlechts, die weder in $\mathfrak{C}$ noch in $\mathfrak{C}'$ enthalten ist. Man betrachte die Gesamtheit der Klassen, die durch Zusammensetzung von C'' mit den einzelnen Klassen in $\mathfrak{C}$ entstehen, also

$$C'', C''+C, C''+2C \ldots C''+(m-1)C, \text{ mit der Bezeichnung } \mathfrak{C}''$$

Diese sind offenbar alle voneinander und von allen in $\mathfrak{C}$ und $\mathfrak{C}'$ verschieden und gehören zum Hauptgeschlecht. Wenn daher $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ dieses Geschlecht ausschöpfen, ist $n = 3m$, andernfalls $n > 3m$. Dann zeigt eine ebenso behandelte weitere Klasse C''' des Hauptgeschlechts, die weder in $\mathfrak{C}, \mathfrak{C}'$ noch in $\mathfrak{C}''$ enthalten ist, dass entweder $n = 4m$ oder $n > 4m$ gilt, und so weiter. Da n und m endliche Zahlen sind, wird das Hauptgeschlecht schließlich notwendig ausgeschöpft. Dann ist n ein Vielfaches von m, oder m ein echter Teiler von n. *Damit ist die zweite Behauptung bewiesen.*

Beispiel. Es sei $D = -356$, $C = (5, 2, 72)$[*)]. Dann findet man $2C = (20, 8, 21), 3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Hier ist also $m = 6$, während n bei dieser Determinante 12 ist. Wählt man für C' die Klasse $(8, 2, 45)$, so sind die übrigen fünf Klassen in $\mathfrak{C}'$ gleich $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

[*)] Klassen werden hier stets durch die in ihnen enthaltenen einfachsten *Formen* bezeichnet.

306.

Der Beweis des vorigen Satzes ist den Beweisen in Art. 45, 49 ganz analog. Tatsächlich hat die Theorie der Multiplikation von Klassen in jeder Hinsicht große Ähnlichkeit mit dem in Abschnitt III behandelten Gegenstand. Die Grenzen dieses Werks erlauben aber nicht, diese Theorie hier so ausführlich zu verfolgen, wie sie es verdient. Deshalb fügen wir nur wenige Bemerkungen hinzu, übergehen auch die Beweise, die längere Vorbereitungen erfordern würden, und behalten uns eine umfassendere Untersuchung für eine andere Gelegenheit vor.

I. Setzt man die Reihe $K, C, 2C, 3C$ usw. über $(m-1)C$ hinaus fort, so treten dieselben Klassen wieder auf:

$$mC = K, \quad (m+1)C = C, \quad (m+2)C = 2C \text{ usw.}$$

Allgemein sind, wenn man der Übersicht wegen K als $0C$ betrachtet, die Klassen $gC, g'C$ identisch oder verschieden, je nachdem g und g' nach dem Modul m kongruent oder inkongruent sind. Die Klasse nC ist also stets mit der Hauptklasse K identisch.

II. Die Gesamtheit der Klassen $K, C, 2C \ldots (m-1)C$, die wir oben mit $\mathfrak{C}$ bezeichnet haben, nennen wir die *Periode* der Klasse C. Diesen Ausdruck darf man nicht mit den *Perioden reduzierter Formen* positiver nichtquadratischer Determinante verwechseln, die in Art. 186 und den folgenden Artikeln behandelt wurden. Offenbar entsteht durch Zusammensetzung beliebig vieler Klassen derselben Periode wieder eine Klasse dieser Periode:

$$gC + g'C + g''C \text{ usw.} = (g + g' + g'' + \text{usw.})C$$

III. Da $C + (m-1)C = K$, sind die Klassen C und $(m-1)C$ entgegengesetzt, ebenso $2C$ und $(m-2)C$, $3C$ und $(m-3)C$ usw. Ist also m gerade, so ist die Klasse $\frac{1}{2}mC$ sich selbst entgegengesetzt und damit *ambig*. Kommt umgekehrt in $\mathfrak{C}$ außer K eine weitere ambige Klasse vor, etwa gC, so gilt $gC = (m-g)C$, also $g = m-g = \frac{1}{2}m$. Daraus folgt: Ist m gerade, so kann es außer K und $\frac{1}{2}mC$ keine weitere ambige Klasse geben; ist dagegen m ungerade, so kann außer K keine weitere in $\mathfrak{C}$ enthalten sein.

IV. Die Periode einer Klasse hC, die in $\mathfrak{C}$ enthalten ist, sei

$$K, hC, 2hC, 3hC \ldots (m'-1)hC$$

Dann ist offenbar $m'h$ das kleinste Vielfache von h, das durch m teilbar ist. Sind also m und h teilerfremd, so ist $m' = m$, und die beiden Perioden enthalten dieselben Klassen in verschiedener Reihenfolge. Bezeichnet allgemein μ den größten gemeinsamen Teiler von m, h, so ist $m' = \frac{m}{\mu}$. Die Anzahl der Klassen in der Periode einer beliebigen Klasse aus $\mathfrak{C}$ ist daher entweder m oder ein echter Teiler von m. Und zwar haben so viele Klassen in $\mathfrak{C}$ Perioden mit m Gliedern, wie unter den Zahlen $0, 1, 2 \ldots m-1$ zu m teilerfremd sind, also φm mit dem Zeichen aus Art. 39. Allgemein haben so viele Klassen in $\mathfrak{C}$ Perioden mit $\frac{m}{\mu}$ Gliedern, wie unter den Zahlen $0, 1, 2 \ldots m-1$ den größten gemeinsamen Teiler μ mit m haben. Ihre Anzahl ist offenbar $\varphi\frac{m}{\mu}$. Gilt also $m = n$, das heißt, ist das *ganze* Hauptgeschlecht in $\mathfrak{C}$ enthalten, so gibt es in diesem Geschlecht genau φn Klassen, deren Perioden dasselbe ganze Geschlecht umfassen, und φe Klassen, deren Perioden aus e Gliedern bestehen, wobei e einen beliebigen

Teiler von n bezeichnet. Dieser Schluss gilt allgemein, wenn im Hauptgeschlecht eine Klasse vorkommt, deren Periode aus n Gliedern besteht.

V. Unter derselben Voraussetzung lässt sich das System der Klassen des Hauptgeschlechts am zweckmäßigsten ordnen, indem man eine Klasse mit einer Periode von n Gliedern gewissermaßen als *Basis* wählt und die Klassen des Hauptgeschlechts in der Reihenfolge ihrer Periode anordnet. Gibt man dann der Hauptklasse den *Index* 0, der als Basis gewählten Klasse den Index 1 usw., so lässt sich allein durch Addition der Indizes feststellen, welche Klasse aus der Zusammensetzung beliebiger Klassen des Hauptgeschlechts entsteht. Hier ein Beispiel für die Determinante -356, bei dem wir die Klasse $(9, 2, 40)$ als Basis gewählt haben:

0	$(1, 0, 356)$	4	$(20, 8, 21)$	8	$(20, -8, 21)$
1	$(9, 2, 40)$	5	$(17, 1, 21)$	9	$(8, 2, 45)$
2	$(5, 2, 72)$	6	$(4, 0, 89)$	10	$(5, -2, 72)$
3	$(8, -2, 45)$	7	$(17, -1, 21)$	11	$(9, -2, 40)$

VI. Sowohl die Analogie mit Abschnitt III als auch die Untersuchung von mehr als 200 negativen und noch weit mehr positiven nichtquadratischen Determinanten mögen es höchst wahrscheinlich erscheinen lassen, dass jene Voraussetzung für *alle* Determinanten gilt. Ein solcher Schluss wäre trotzdem falsch und würde durch Fortsetzung der Klassifikationstafel widerlegt. Der Kürze wegen nennen wir die Determinanten, bei denen das ganze Hauptgeschlecht in einer einzigen Periode enthalten sein kann, *regulär*, die übrigen, bei denen das nicht möglich ist, *irregulär*. Dieser Gegenstand scheint zu den tiefsten Geheimnissen der höheren Arithmetik zu gehören und Raum für äußerst schwierige Untersuchungen zu lassen. Hier können wir ihn nur durch wenige Bemerkungen erläutern, denen wir die folgende allgemeine voranstellen.

VII. Gibt es im Hauptgeschlecht Klassen C, C', deren Perioden aus m, m' Klassen bestehen, und ist M die kleinste durch m und m' teilbare Zahl, so gibt es in demselben Geschlecht auch Klassen, deren Perioden M Glieder enthalten. Man zerlege M in zwei teilerfremde Faktoren r, r', deren erster (r) die Zahl m, deren zweiter (r') die Zahl m' teilt, wie in Art. 73. Dann hat die Klasse $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ die verlangte Eigenschaft. Bestehe nämlich die Periode der Klasse C'' aus g Gliedern, so gilt

$$\begin{aligned} K = grC'' &= gmC + \frac{grm'}{r'}C' \\ &= K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C' \end{aligned}$$

also muss $\frac{grm'}{r'}$ durch m' teilbar sein oder gr durch r' und damit auch g durch r'. Ganz ebenso findet man g durch r teilbar und daher auch durch $rr' = M$. Da aber offenbar $MC'' = K$, ist auch M durch g teilbar. Also gilt notwendig $M = g$. Daraus folgt leicht, dass die *größte* Anzahl von Klassen in einer Periode bei gegebener Determinante durch die Klassenanzahl jeder anderen Periode einer Klasse desselben Hauptgeschlechts teilbar ist. Zugleich lässt sich daraus eine Methode gewinnen, eine Klasse mit möglichst großer Periode zu finden, die also bei regulärer Determinante das ganze Hauptgeschlecht umfasst. Sie ist der Methode der Art. 73, 74 ganz analog,

obwohl sich die Arbeit in der Praxis durch verschiedene Kunstgriffe verkürzen lässt. Der Quotient aus n und der Klassenanzahl der größten Periode ist für reguläre Determinanten 1, für irreguläre aber stets eine ganze Zahl größer als 1. Bei diesen eignet er sich besonders gut, die verschiedenen Arten der Irregularität auszudrücken, und kann deshalb *Irregularitätsexponent* heißen.

VIII. Bisher gibt es keine allgemeine Regel, mit der sich reguläre von irregulären Determinanten im Voraus unterscheiden lassen, zumal unter den letzten sowohl Primzahlen als auch zusammengesetzte Zahlen vorkommen. Einige besondere Beobachtungen müssen hier also genügen. Enthält das Hauptgeschlecht mehr als zwei ambige Klassen, so ist die Determinante sicher irregulär und der Irregularitätsexponent gerade. Gibt es in diesem Geschlecht dagegen nur eine oder zwei, so ist die Determinante entweder regulär oder wenigstens ihr Irregularitätsexponent ungerade. Alle negativen Determinanten der Form $-(216k + 27)$, mit der einzigen Ausnahme -27, sind irregulär, und ihr Irregularitätsexponent ist durch 3 teilbar. Dasselbe gilt für negative Determinanten der Formen $-(1000k + 75)$ und $-(1000k + 675)$, mit der einzigen Ausnahme -75, und für unendlich viele andere. Ist der Irregularitätsexponent eine Primzahl p oder wenigstens durch p teilbar, so ist n durch pp teilbar. Hat also n keinen quadratischen Teiler, so ist die Determinante sicher regulär. Nur bei positiven Determinanten, die *Quadratzahlen* ee sind, lässt sich stets im Voraus erkennen, ob sie regulär oder irregulär sind. Regulär sind sie, wenn e gleich 1 oder 2, eine ungerade Primzahl oder eine Potenz einer ungeraden Primzahl ist; in allen übrigen Fällen sind sie irregulär. Bei negativen Determinanten werden die irregulären mit wachsender Determinante immer häufiger. *Zum Beispiel* findet man im ganzen ersten Tausender dreizehn irreguläre: ohne negatives Vorzeichen $576, 580, 820, 884, 900$ mit dem Irregularitätsexponenten 2 sowie $243, 307, 339, 459, 675, 755, 891, 974$ mit dem Irregularitätsexponenten 3. Im zweiten Tausender wurden 13 mit dem Exponenten 2 und 15 mit dem Exponenten 3 gefunden; im zehnten Tausender 31 mit dem Exponenten 2 und 32 mit dem Exponenten 3. Ob Determinanten mit einem Irregularitätsexponenten größer als 3 unter -10000 vorkommen, lässt sich noch nicht entscheiden. Jenseits dieser Grenze können beliebige gegebene Exponenten vorkommen. Es ist sehr wahrscheinlich, dass mit wachsenden Determinanten das Verhältnis der Häufigkeit irregulärer negativer Determinanten zu der regulärer sich immer mehr einer festen Zahl nähert. Diese zu bestimmen wäre des Scharfsinns der Mathematiker sehr würdig. — Bei positiven nichtquadratischen Determinanten sind irreguläre viel seltener. Mit geradem Irregularitätsexponenten gibt es sicher unendlich viele, *zum Beispiel* 3026, bei der er 2 ist. Es scheint auch kein Zweifel, dass solche mit ungeradem Irregularitätsexponenten vorkommen, obwohl wir zugeben müssen, dass uns bisher keine begegnet ist.

IX. Die zweckmäßigste Anordnung des Systems der Klassen im Hauptgeschlecht einer irregulären Determinante können wir hier der Kürze wegen nicht behandeln. Wir bemerken nur: Da eine einzige Basis hier nicht genügt, muss man zwei oder sogar noch mehr Klassen wählen, aus deren Multiplikation und Zusammensetzung alle Klassen entstehen. Daraus ergeben sich *doppelte oder mehrfache Indizes*, die ungefähr denselben Zweck erfüllen wie die einfachen bei regulären Determinanten. Dies behandeln wir ein anderes Mal ausführlicher.

X. Schließlich bemerken wir, dass alle in diesem und dem vorigen Artikel betrachteten Eigenschaften vor allem von der Zahl n abhängen, die eine ähnliche Rolle spielt wie $p-1$ in Abschnitt III. Daher verdient diese Zahl die größte Aufmerksamkeit, und eine allgemeine Beziehung zwischen ihr und der zugehörigen Determinante zu entdecken wäre höchst wünschenswert. Bei dieser sehr wichtigen Frage halten wir es umso weniger für angebracht, die Hoffnung aufzugeben, als es bereits gelungen ist, den Durchschnittswert des Produkts aus n und der im Voraus bestimmbaren Geschlechteranzahl wenigstens bei negativen Determinanten durch eine analytische Formel auszudrücken, in Art. 302.

307.

Die Untersuchungen der vorigen Artikel umfassen nur die Klassen des Hauptgeschlechts. Sie genügen daher sowohl für positive Determinanten mit nur einem Geschlecht überhaupt als auch für negative mit nur einem positiven Geschlecht, wenn wir das negative nicht berücksichtigen wollen. Es bleibt, auch über die übrigen eigentlich primitiven Geschlechter einige Bemerkungen hinzuzufügen.

I. Gibt es in einem Geschlecht G', das vom Hauptgeschlecht G derselben Determinante verschieden ist, eine ambige Klasse, so gibt es darin ebenso viele wie in G. Die ambigen Klassen in G seien L, M, N usw., darunter auch die Hauptklasse K, in G' dagegen L', M', N' usw. Ihre Gesamtheiten seien der Reihe nach A und A'. Da offenbar alle Klassen $L+L',\ M+L',\ N+L'$ usw. ambig und verschieden sind, zu G' gehören und somit in A' enthalten sein müssen, kann die Klassenanzahl in A' sicher nicht kleiner sein als in A. Ebenso sind die Klassen $L'+L',\ M'+L',\ N'+L'$ usw. verschieden und ambig, gehören zu G und sind also in A enthalten. Daher kann die Klassenanzahl in A nicht kleiner sein als in A'. Die Klassenanzahlen in A und A' sind somit notwendig gleich.

II. Da die Gesamtzahl der ambigen Klassen gleich der Anzahl der Geschlechter ist, nach Art. 261, 287 III, muss offenbar, wenn es in G nur eine ambige Klasse gibt, *jedes* Geschlecht eine ambige Klasse enthalten. Gibt es in G zwei, so enthält die Hälfte aller Geschlechter je zwei, die übrigen keine. Sind schließlich in G mehr enthalten, etwa a*), so enthält der a-te Teil aller Geschlechter je a ambige Klassen, die übrigen keine.

III. Für den Fall, dass G zwei ambige Klassen enthält, seien G, G', G'' usw. die Geschlechter mit je zwei und H, H', H'' usw. die ohne ambige Klassen. Die Gesamtheit der ersten sei $\mathfrak{G}$, die der letzten $\mathfrak{H}$. Da durch Zusammensetzung zweier ambiger Klassen stets eine ambige Klasse entsteht, nach Art. 249, ergibt sich durch Zusammensetzung zweier Geschlechter aus $\mathfrak{G}$ offenbar stets ein Geschlecht aus $\mathfrak{G}$. Daraus folgt weiter, dass die Zusammensetzung eines Geschlechts aus $\mathfrak{G}$ mit einem aus $\mathfrak{H}$ ein Geschlecht aus $\mathfrak{H}$ ergibt. Denn gehörte *zum Beispiel* $G'+H$ nicht zu $\mathfrak{H}$, sondern zu $\mathfrak{G}$, so müsste auch $G'+H+G'$ zu $\mathfrak{G}$ gehören. *Das ist ein Widerspruch*, da $G'+G'=G$ und somit $G'+H+G'=H$. Schließlich sieht man leicht, dass die Geschlechter $G+H$, $G'+H,\ G''+H$ usw. zusammen mit $H+H,\ H'+H,\ H''+H$ usw. alle verschieden und daher mit $\mathfrak{G}$ und $\mathfrak{H}$ zusammengenommen identisch sind. Nach dem gerade Bewiesenen gehören aber die Geschlechter $G+H,\ G'+H,\ G''+H$ usw. alle zu $\mathfrak{H}$ und

*) Dies kann nur bei irregulären Determinanten geschehen, und a ist dann stets eine Zweierpotenz.

schöpfen diese Gesamtheit also aus. Daher müssen die übrigen $H+H$, $H'+H$, $H''+H$ usw. sämtlich zu $\mathfrak{G}$ gehören. *Das heißt*, die Zusammensetzung zweier Geschlechter aus $\mathfrak{H}$ ergibt also stets ein Geschlecht aus $\mathfrak{G}$.

IV. Ist E eine Klasse des Geschlechts V, das vom Hauptgeschlecht G verschieden ist, so gehören offenbar $2E, 4E$, $6E$ usw. alle zu G, dagegen $3E, 5E, 7E$ usw. zu V. Besteht die Periode der Klasse $2E$ aus m Gliedern, so ist in der Reihe $E, 2E, 3E$ usw. offenbar die Klasse $2mE$ und keine frühere mit K identisch. Die Periode der Klasse E besteht also aus $2m$ Gliedern. Daher ist die Gliederzahl der Periode einer beliebigen Klasse außerhalb des Hauptgeschlechts entweder $2n$ oder ein echter Teiler von $2n$, wobei n die Anzahl der Klassen in jedem Geschlecht bezeichnet.

V. Es sei C eine gegebene Klasse des Hauptgeschlechts G und E eine Klasse eines Geschlechts V, aus deren Verdopplung C entsteht; eine solche gibt es stets nach Art. 286. Ferner seien sämtliche ambigen Klassen, eigentlich primitiv und von derselben Determinante, K, K', K'' usw. Dann sind *alle* Klassen, aus deren Verdopplung C entsteht, die folgenden: $E\ (= E+K)$, $E+K'$, $E+K''$ usw. Ihre Gesamtheit sei $\mathfrak{Q}$. Die Anzahl dieser Klassen ist gleich der Anzahl der ambigen Klassen, also der Anzahl der Geschlechter. Offenbar gehören von den Klassen in $\mathfrak{Q}$ so viele zum Geschlecht V, wie es ambige Klassen in G gibt. Ihre Anzahl sei a. Dann enthält jedes Geschlecht entweder a Klassen aus $\mathfrak{Q}$ oder keine. Daraus folgt leicht: Ist $a = 1$, so enthält jedes Geschlecht eine Klasse aus $\mathfrak{Q}$; ist $a = 2$, so enthält die Hälfte aller Geschlechter je zwei Klassen aus $\mathfrak{Q}$, die übrigen keine. Dabei stimmt die erste Hälfte entweder ganz mit $\mathfrak{G}$ überein, im selben Sinn wie oben in III, und die zweite mit $\mathfrak{H}$, oder diese mit $\mathfrak{G}$ und jene mit $\mathfrak{H}$. — Ist a noch größer, so enthält stets der a-te Teil aller Geschlechter Klassen aus $\mathfrak{Q}$, und zwar jedes dieser Geschlechter a Klassen.

VI. Nun sei C eine Klasse, deren Periode aus n Gliedern besteht. Für den Fall $a = 2$, in dem also n gerade ist, sieht man leicht, dass keine Klasse aus $\mathfrak{Q}$ zu G gehören kann. Dann wäre nämlich eine solche Klasse in der Periode der Klasse C enthalten. Wäre sie also $= rC$, oder $2rC = C$, so wäre $2r \equiv 1 \pmod{n}$, *was ein Widerspruch ist.* Da G zu $\mathfrak{G}$ gehört, müssen also sämtliche Klassen $\mathfrak{Q}$ auf die Geschlechter $\mathfrak{H}$ verteilt sein. Weil es bei regulärer Determinante in G genau φn Klassen mit Perioden von n Gliedern gibt, folgt: Für den Fall $a = 2$ enthält jedes Geschlecht $\mathfrak{H}$ genau $2\varphi n$ Klassen, deren Perioden $2n$ Glieder und somit sowohl ihr eigenes als auch das Hauptgeschlecht umfassen. Ist dagegen $a = 1$, so gibt es in jedem vom Hauptgeschlecht verschiedenen Geschlecht φn solche Klassen.

VII. Auf diese Beobachtungen gründen wir die folgende Methode, das System *aller* eigentlich primitiven Klassen für jede gegebene reguläre Determinante möglichst zweckmäßig aufzubauen; irreguläre lassen wir ganz beiseite. Man wähle beliebig eine Klasse E, deren Periode $2n$ Glieder und damit sowohl ihr eigenes Geschlecht, etwa V, als auch das Hauptgeschlecht G umfasst. Die Klassen dieser beiden Geschlechter ordne man in der Reihenfolge dieser Periode. Damit ist die Aufgabe schon erledigt, wenn es überhaupt nicht mehr als diese beiden Geschlechter gibt oder wenn es nicht nötig erscheint, die übrigen hinzuzufügen, *zum Beispiel* bei einer negativen Determinante mit nur zwei positiven Geschlechtern. Sollen aber vier oder mehr Geschlechter aufgebaut werden, so behandle man die übrigen auf folgende Weise. Es sei V' eines der übrigen und $V + V' = V''$. Dann gibt es in V' und V'' zusammen zwei ambige

Klassen, entweder in jedem eine oder in einem zwei und im anderen keine. Daraus wähle man eine beliebige A. Setzt man A mit den einzelnen Klassen in G und V zusammen, so entstehen offenbar $2n$ verschiedene Klassen, die zu V' und V'' gehören und diese Geschlechter somit ausschöpfen. So lassen sich auch diese Geschlechter ordnen. — Sind außer diesen vier weitere Geschlechter übrig, sei V''' eines davon, und es seien V'''', V''''', V''''''' die Geschlechter, die durch Zusammensetzung von V''' mit V, V' und V'' entstehen. Diese vier Geschlechter $V''' \dots V'''''''$ enthalten vier ambige Klassen. Wählt man daraus eine A' und setzt sie mit den einzelnen Klassen in G, V, V', V'' zusammen, so entstehen offenbar alle Klassen in $V''' \dots V'''''''$. — Sind noch weitere Geschlechter übrig, so fahre man ebenso fort, bis alle ausgeschöpft sind. Ist die Anzahl aller aufzubauenden Geschlechter 2^μ, so braucht man offenbar insgesamt $\mu - 1$ ambige Klassen. Jede Klasse dieser Geschlechter entsteht entweder durch Multiplikation der Klasse E oder durch Zusammensetzung einer so entstandenen Klasse mit einer oder mehreren ambigen Klassen. Zwei Beispiele erläutern diese Regeln. Mehr über den Nutzen einer solchen Anordnung oder über Kunstgriffe zur Erleichterung der Arbeit können wir hier nicht hinzufügen.

I. Determinante -161.

Vier positive Geschlechter; je vier Klassen.

G

$1, 4;\ R7;\ R23$

$(1, 0, 161) = K$
$(9, 1, 18) = 2E$
$(2, 1, 81) = 4E$
$(9, -1, 18) = 6E$

V

$3, 4;\ N7;\ R23$

$(3, 1, 54) = E$
$(6, -1, 27) = 3E$
$(6, 1, 27) = 5E$
$(3, -1, 54) = 7E$

V'

$3, 4;\ R7;\ N23$

$(7, 0, 23) = A$
$(11, -2, 15) = A + 2E$
$(14, 7, 15) = A + 4E$
$(11, 2, 15) = A + 6E$

V''

$1, 4;\ N7;\ N23$

$(10, 3, 17) = A + E$
$(5, 2, 33) = A + 3E$
$(5, -2, 33) = A + 5E$
$(10, -3, 17) = A + 7E$

II. Determinante -546.

Acht positive Geschlechter; je drei Klassen.

G

1 und $3, 8; R3; R7; R13$

$(1, 0, 546) = K$
$(22, -2, 25) = 2E$
$(22, 2, 25) = 4E$

V

5 und $7, 8; N3; N7; N13$

$(5, 2, 110) = E$
$(21, 0, 26) = 3E$
$(5, -2, 110) = 5E$

V'

1 und $3, 8; N3; R7; N13$

$(2, 0, 273) = A$
$(11, -2, 50) = A + 2E$
$(11, 2, 50) = A + 4E$

V''

5 und $7, 8; R3; N7; R13$

$(10, 2, 55) = A + E$
$(13, 0, 42) = A + 3E$
$(10, -2, 55) = A + 5E$

V'''

1 und $3, 8; N3; N7; R13$

$(3, 0, 182) = A'$
$(17, 7, 35) = A' + 2E$
$(17, -7, 35) = A' + 4E$

V''''

5 und $7, 8; R3; R7; N13$

$(15, -3, 37) = A' + E$
$(7, 0, 78) = A' + 3E$
$(15, 3, 37) = A' + 5E$

V'''''

1 und $3, 8; R3; N7; N13$

$(6, 0, 91) = A + A'$
$(19, 9, 33) = A + A' + 2E$
$(19, -9, 33) = A + A' + 4E$

V''''''

5 und $7, 8; N3; R7; R13$

$(23, 11, 29) = A + A' + E$
$(14, 0, 39) = A + A' + 3E$
$(23, -11, 29) = A + A' + 5E$

SECHSTER ABSCHNITT.

VERSCHIEDENE ANWENDUNGEN DER VORANGEGANGENEN UNTERSUCHUNGEN.

308.

Wie reich die höhere Arithmetik an Wahrheiten ist, die auch in anderen Teilen der Mathematik nützlich sind, haben wir bereits an mehreren Stellen angedeutet. Einige Anwendungen, die eine ausführlichere Darstellung verdienen, gesondert zu behandeln, schien uns nicht unnütz. Dabei wollen wir diesen Gegenstand, der leicht mehrere Bände füllen könnte, weniger erschöpfen als vielmehr durch einige Beispiele erläutern. In diesem Abschnitt behandeln wir zuerst die Zerlegung von Brüchen in einfachere, dann die Umwandlung gewöhnlicher Brüche in Dezimalbrüche. Danach erklären wir ein neues Ausschlussverfahren zur Lösung unbestimmter Gleichungen zweiten Grades. Schließlich geben wir neue, bequeme Methoden an, Primzahlen von zusammengesetzten Zahlen zu unterscheiden und die Faktoren der letzten zu ermitteln. Im folgenden Abschnitt begründen wir die allgemeine Theorie einer besonderen Art von Funktionen, die sich durch die ganze Analysis sehr weit erstreckt, soweit sie mit der höheren Arithmetik sehr eng zusammenhängt. Insbesondere wollen wir die Theorie der Kreisteilung, von der bisher nur die ersten Grundlagen bekannt geworden sind, durch neue Ergebnisse erweitern.

Zerlegung von Brüchen in einfachere.

309.

Aufgabe. *Einen Bruch $\frac{m}{n}$, dessen Nenner n das Produkt zweier teilerfremder Zahlen a, b ist, in zwei andere mit den Nennern a, b zerlegen.*

Lösung. Die gesuchten Brüche seien $\frac{x}{a}, \frac{y}{b}$. Dann muss $bx + ay = m$ gelten. Also ist x eine Wurzel der Kongruenz $bx \equiv m \pmod{a}$, die sich nach Abschnitt II finden lässt, während dann $y = \frac{m-bx}{a}$ gilt.

Bekanntlich hat die Kongruenz $bx \equiv m$ unendlich viele Wurzeln, die aber nach a kongruent sind, und nur eine positive, die kleiner als a ist. Es kann allerdings auch vorkommen, dass y negativ wird. Wir brauchen kaum zu bemerken, dass y auch durch die Kongruenz $ay \equiv m \pmod{b}$ und x durch die Gleichung $x = \frac{m-ay}{b}$ gefunden werden kann. — *Zum Beispiel* ist für den gegebenen Bruch $\frac{58}{77}$ die Zahl 4 der Wert des Ausdrucks $\frac{58}{11} \pmod{7}$. Daher zerlegt sich $\frac{58}{77}$ in $\frac{4}{7} + \frac{2}{11}$.

310.

Ist ein Bruch $\frac{m}{n}$ gegeben, dessen Nenner n das Produkt beliebig vieler paarweise teilerfremder Faktoren a, b, c, d usw. ist, so kann er nach dem vorigen Artikel zunächst in zwei mit den Nennern a und bcd usw. zerlegt werden; der zweite wieder in zwei mit den Nennern b und cd usw.; der letzte wiederum in zwei und so fort. Schließlich erhält der gegebene Bruch die Form

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \text{usw.}$$

Die Zähler $\alpha, \beta, \gamma, \delta$ usw. können offenbar positiv und kleiner als ihre jeweiligen Nenner gewählt werden, außer dem letzten. Sind die übrigen bestimmt, so ist der letzte nicht mehr beliebig und kann auch negativ oder größer als sein Nenner werden, da wir $m < n$ nicht voraussetzen. Dann ist es meist zweckmäßig, ihn in die Form $\frac{\varepsilon}{e} \mp k$ zu bringen, wobei ε positiv und kleiner als e, dagegen k eine ganze Zahl ist. Schließlich können a, b, c usw. offenbar als Primzahlen oder Primzahlpotenzen gewählt werden.

Beispiel. Der Bruch $\frac{391}{924}$, mit dem Nenner $= 4.3.7.11$, zerlegt sich auf diese Weise in $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ in $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ in $\frac{1}{7} - \frac{7}{11}$. Schreibt man daher $\frac{4}{11} - 1$ für $-\frac{7}{11}$, so erhält man $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311.

Ein Bruch $\frac{m}{n}$ lässt sich *nur auf eine Weise* in die Form $\frac{\alpha}{a} + \frac{\beta}{b} + \text{usw.} \mp k$ bringen, sodass α, β usw. positiv und kleiner als a, b usw. sind. Setzen wir nämlich

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{usw.} \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \text{usw.} \mp k'$$

und auch α', β' usw. positiv und kleiner als a, b usw. voraus, so gilt notwendig $\alpha = \alpha',\ \beta = \beta',\ \gamma = \gamma'$ usw. und $k = k'$. Denn durch Multiplikation mit $n = abc$ usw. ergibt sich offenbar $m \equiv \alpha bcd$ usw. $\equiv \alpha' bcd$ usw. (mod. a). Da bcd usw. zu a teilerfremd ist, gilt notwendig $\alpha \equiv \alpha'$, also $\alpha = \alpha'$, und ebenso $\beta = \beta'$ usw. Daraus folgt auch sofort $k = k'$. Da nun völlig beliebig ist, zu welchem Nenner der Zähler zuerst berechnet wird, lassen sich offenbar *alle* Zähler ebenso bestimmen wie α im vorigen Artikel, etwa β durch die Kongruenz βacd usw. $\equiv m$ (mod. b), γ durch γabd usw. $\equiv m$ (mod. c) usw. Die Summe aller so gefundenen Brüche ist entweder gleich dem gegebenen Bruch $\frac{m}{n}$, oder die Differenz ist eine ganze Zahl $= k$. Auf diese Weise erhalten wir zugleich eine Kontrolle der Rechnung. So liefern im Beispiel des vorigen Artikels die Werte der Ausdrücke $\frac{391}{231}$ (mod. 4), $\frac{391}{308}$ (mod. 3), $\frac{391}{132}$ (mod. 7), $\frac{391}{84}$ (mod. 11) unmittelbar die Zähler $1, 2, 1, 4$ zu den Nennern $4, 3, 7, 11$. Die Summe dieser Brüche übersteigt, wie man findet, den gegebenen Bruch um eins.

Umwandlung gewöhnlicher Brüche in Dezimalbrüche.

312.

Definition. Wird ein gewöhnlicher Bruch in einen Dezimalbruch umgewandelt, so nennen wir die Folge der Dezimalziffern[*)] ohne den etwa vorhandenen ganzzahligen Teil, ob sie endlich ist oder unendlich fortläuft, die *Mantisse* des Bruchs. Wir gebrauchen diesen sonst nur bei Logarithmen üblichen Ausdruck in einem weiteren Sinn. So ist *zum Beispiel* die Mantisse des Bruchs $\frac{1}{8}$ gleich 125, die von $\frac{35}{16}$ gleich 1875 und die von $\frac{2}{37}$ gleich $054054\ldots$, ins Unendliche fortgesetzt.

Aus dieser Definition folgt sofort, dass die Brüche $\frac{l}{n}, \frac{m}{n}$ mit demselben Nenner gleiche oder verschiedene Mantissen haben, je nachdem ihre Zähler l, m nach n kongruent oder inkongruent sind. Eine endliche Mantisse ändert sich nicht, wenn rechts beliebig viele Nullen angefügt werden. Die Mantisse des Bruchs $\frac{10m}{n}$ erhält man, indem man die erste Ziffer der Mantisse von $\frac{m}{n}$ entfernt. Allgemein findet man die Mantisse von $\frac{10^\nu m}{n}$, indem man die ersten ν Ziffern der Mantisse von $\frac{m}{n}$ entfernt. Die Mantisse von $\frac{1}{n}$ beginnt sofort mit einer signifikanten Ziffer, *das heißt*, einer von null verschiedenen, wenn n nicht > 10 ist. Gilt dagegen $n > 10$, ist der Nenner keiner Potenz von 10 gleich und besteht er aus k Ziffern, so sind die ersten $k-1$ Ziffern der Mantisse von $\frac{1}{n}$ Nullen, und erst die folgende, die k-te, ist signifikant. Daraus folgt leicht: Haben $\frac{l}{n}, \frac{m}{n}$ verschiedene Mantissen, *das heißt*, sind l, m nach n inkongruent, so können diese Mantissen sicher nicht in den ersten k Ziffern übereinstimmen, sondern müssen sich spätestens in der k-ten Ziffer unterscheiden.

313.

Aufgabe. *Aus dem gegebenen Nenner eines Bruchs $\frac{m}{n}$ und den ersten k Ziffern seiner Mantisse den Zähler m finden, den wir kleiner als n voraussetzen.*

Lösung. Man betrachte diese k Ziffern als ganze Zahl, multipliziere sie mit n und dividiere das Produkt durch $.10^k$, oder entferne die letzten k Ziffern. Ist der Quotient eine ganze Zahl, sind also die entfernten Ziffern Nullen, so ist er offenbar der gesuchte Zähler und die gegebene Mantisse vollständig. Andernfalls ist der gesuchte Zähler die nächstgrößere ganze Zahl, also jener Quotient um eins vermehrt, nachdem die folgenden Dezimalziffern weggelassen wurden. Der Grund dieser Regel ergibt sich so leicht aus den Bemerkungen am Ende des vorigen Artikels, dass eine ausführlichere Erklärung unnötig ist.

Beispiel. Weiß man, dass die ersten beiden Ziffern der Mantisse eines Bruchs mit dem Nenner 23 gleich 69 sind, so haben wir das Produkt $23.69 = 1587$. Entfernt man dessen letzte beiden Ziffern und addiert eins, so ergibt sich der gesuchte Zähler $= 16$.

[*)] Der Kürze wegen beschränken wir die folgende Untersuchung auf das gewöhnliche Dezimalsystem, da sie sich leicht auf jedes andere ausdehnen lässt.

314.

Wir beginnen mit Brüchen, deren Nenner Primzahlen oder Primzahlpotenzen sind, und zeigen später, wie sich die übrigen darauf zurückführen lassen. Zunächst bemerken wir sofort, dass die Mantisse eines Bruchs $\frac{a}{p^\mu}$, von dessen Zähler a wir stets voraussetzen, dass er durch die Primzahl p nicht teilbar ist, endlich ist und aus μ Ziffern besteht, wenn $p = 2$ oder $= 5$. Im ersten Fall ist diese als ganze Zahl betrachtete Mantisse $= 5^\mu a$, im zweiten $= 2^\mu a$. Dies ist so offensichtlich, dass es keiner Erklärung bedarf.

Ist dagegen p eine andere Primzahl, so ist $10^r a$ niemals durch p^μ teilbar, wie groß auch r gewählt wird. Daher muss die Mantisse von $F = \frac{a}{p^\mu}$ unendlich fortlaufen. Es sei 10^e die kleinste Potenz von 10, die nach dem Modul p^μ der Einheit kongruent ist. Man vergleiche Abschnitt III, wo wir gezeigt haben, dass e entweder der Zahl $(p-1)p^{\mu-1}$ gleich oder ein echter Teiler davon ist. Dann sieht man leicht, dass auch $10^e a$ die erste Zahl in der Reihe $10a, 100a, 1000a$ usw. ist, die nach demselben Modul der Zahl a kongruent ist. Nun entstehen nach Art. 312 die Mantissen der Brüche $\frac{10a}{p^\mu}, \frac{100a}{p^\mu} \ldots \frac{10^e a}{p^\mu}$, indem man von der Mantisse des Bruchs F die erste Ziffer, die ersten beiden $\ldots e$ Ziffern der Reihe nach entfernt. Daher wiederholen sich in dieser Mantisse offenbar nach den ersten e Ziffern, und nicht früher, dieselben Ziffern. Diese ersten e Ziffern, deren unendliche Wiederholung die Mantisse bildet, können wir die *Periode* dieser Mantisse oder des Bruchs F nennen. Offenbar ist die Länge der Periode, *das heißt*, die Anzahl ihrer Ziffern $(= e)$, vom Zähler a völlig unabhängig und nur durch den Nenner bestimmt. So ist *zum Beispiel* die Periode von $\frac{1}{11}$ gleich 09 und die von $\frac{3}{7}$ gleich 428571[*)].

315.

Kennt man also die Periode eines Bruchs, so kann seine Mantisse auf beliebig viele Ziffern fortgesetzt werden. Gilt ferner $b \equiv 10^\lambda a \pmod{p^\mu}$, so erhält man offenbar die Periode von $\frac{b}{p^\mu}$, indem man die ersten λ Ziffern der Periode von F, wobei wir $\lambda < e$ voraussetzen dürfen, hinter die übrigen $e - \lambda$ Ziffern stellt. Mit der Periode von F hat man somit zugleich die Perioden aller Brüche, deren Zähler den Zahlen $10a, 100a, 1000a$ usw. nach dem Nenner p^μ kongruent sind. So ergibt sich *zum Beispiel*, da $6 \equiv 3.10^2 \pmod 7$, die Periode von $\frac{6}{7}$ sofort aus der von $\frac{3}{7}$ als 857142.

Ist nach dem Modul p^μ die Zahl 10 eine Primitivwurzel, nach Art. 57, 89, so lässt sich aus der Periode von $\frac{1}{p^\mu}$ unmittelbar die Periode jedes anderen Bruchs $\frac{m}{p^\mu}$ gewinnen, dessen Zähler m durch p nicht teilbar ist. Man entfernt links so viele Ziffern und fügt sie rechts wieder an, wie der Index von m Einheiten hat, wenn 10 als Basis gewählt wird. Daraus wird deutlich, warum in diesem Fall in Tafel I stets die Zahl 10 als Basis gewählt wurde; siehe Art. 72.

[*)] Der angesehene Robertson bezeichnet Anfang und Ende der Periode durch zwei über die erste und die letzte Ziffer gesetzte Punkte (*Theory of circulating fractions, Philos. Trans.* 1769 *S.* 207), was wir hier nicht für nötig halten.

Ist dagegen 10 keine Primitivwurzel, so lassen sich aus der Periode von $\frac{1}{p^\mu}$ nur die Perioden derjenigen Brüche gewinnen, deren Zähler einer Potenz von 10 nach p^μ kongruent sind. Es sei 10^e die kleinste Potenz von 10, die nach p^μ der Einheit kongruent ist, ferner $(p-1)p^{\mu-1} = ef$. Als Basis wähle man eine solche Primitivwurzel r, dass der Index von 10 gleich f wird, nach Art. 71. In diesem System haben die Zähler der Brüche, deren Perioden aus der Periode von $\frac{1}{p^\mu}$ gewonnen werden können, die Indizes $f, 2f, 3f \ldots ef - f$. Ebenso gewinnt man aus der Periode von $\frac{r}{p^\mu}$ die Perioden der Brüche, deren Zähler $10r, 100r, 1000r$ usw. den Indizes $f+1, 2f+1, 3f+1$ usw. entsprechen. Aus der Periode des Bruchs mit dem Zähler rr, dessen Index 2 ist, gewinnt man die Perioden der Brüche, deren Zähler die Indizes $f+2, 2f+2, 3f+2$ usw. haben. Allgemein lassen sich aus der Periode des Bruchs mit dem Zähler r^i die Perioden der Brüche gewinnen, deren Zähler die Indizes $f+i, 2f+i, 3f+i$ usw. haben. Daraus folgt leicht: Kennt man nur die Perioden der Brüche mit den Zählern $1, r, rr, r^3 \ldots r^{f-1}$, so lassen sich alle übrigen allein durch Umstellung nach folgender Regel ableiten. Der Index des Zählers m des gegebenen Bruchs $\frac{m}{p^\mu}$ im System mit der Basis r sei $= i$, wobei wir ihn kleiner als $(p-1)p^{\mu-1}$ voraussetzen. Durch Division durch f setze man $i = \alpha f + \beta$, sodass α, β positive ganze Zahlen oder auch 0 sind und $\beta < f$ gilt. Dann entsteht die Periode von $\frac{m}{p^\mu}$ aus der Periode des Bruchs mit dem Zähler r^β, also 1, wenn $\beta = 0$, indem man die ersten α Ziffern dieser Periode hinter die übrigen stellt. Für $\alpha = 0$ behält man also diese Periode selbst. Dies erklärt hinreichend, warum wir beim Aufstellen der Tafel I der in Art. 72 erläuterten Regel gefolgt sind.

316.

Nach diesen Grundsätzen haben wir für alle Nenner der Form p^μ unter 1000 eine Tafel der nötigen Perioden aufgestellt. Wir werden sie bei Gelegenheit vollständig oder auch noch weiter fortgesetzt veröffentlichen. Hier möge Tafel III, die nur bis 100 reicht, als Beispiel genügen; sie braucht kaum eine Erklärung. Für die Nenner, nach denen 10 eine Primitivwurzel ist, enthält sie die Perioden der Brüche mit dem Zähler 1, nämlich für $7, 17, 19, 23, 29, 47, 59, 61, 97$. Für die übrigen gibt sie f Perioden zu den Zählern $1, r, rr, \dots r^{f-1}$, die durch die beigefügten Zahlen $(0), (1), (2)$ usw. unterschieden sind. Als Basis r wurde stets dieselbe Primitivwurzel wie in Tafel I gewählt. Daraus lässt sich also die Periode jedes Bruchs, dessen Nenner in dieser Tafel vorkommt, nach den Regeln des vorigen Artikels ermitteln, nachdem der Index des Zählers aus Tafel I berechnet wurde. Bei so kleinen Nennern können wir die Aufgabe aber ebenso leicht ohne Tafel I lösen. Durch gewöhnliche Division berechnen wir so viele Anfangsziffern der gesuchten Mantisse, wie nach Art. 313 nötig sind, um sie von allen anderen mit demselben Nenner zu unterscheiden; für Tafel III nicht mehr als 2. Dann durchsuchen wir sämtliche Perioden zum gegebenen Nenner, bis wir auf jene Anfangsziffern stoßen, die den Beginn der Periode zweifellos anzeigen. Wir müssen jedoch bemerken, dass diese Ziffern auch getrennt sein können: Die erste oder mehrere können das Ende einer Periode bilden, die übrige oder die übrigen deren Anfang.

Beispiel. Gesucht ist die Periode von $\frac{12}{19}$. Hier hat man nach dem Modul 19 aus Tafel I die Beziehung $\text{ind.}\, 12 = 2\,\text{ind.}\, 2 + \text{ind.}\, 3 = 39 \equiv 3 \pmod{18}$, nach Art. 57. Da es in diesem Fall nur eine Periode zum Zähler 1 gibt, müssen ihre ersten drei Ziffern an das Ende gestellt werden. So entsteht die gesuchte Periode 631578947368421052. — Der Beginn der Periode hätte sich ebenso leicht aus den ersten beiden Ziffern 63 finden lassen.

Sucht man die Periode von $\frac{45}{53}$, so gilt nach dem Modul 53 die Beziehung $\text{ind.}\, 45 = 2\,\text{ind.}\, 3 + \text{ind.}\, 5 = 49$. Die Anzahl der Perioden ist hier $4 = f$, und es gilt $49 = 12f + 1$. Daher müssen von der mit (1) bezeichneten Periode die ersten 12 Ziffern hinter die letzte gestellt werden. Die gesuchte Periode ist somit 8490566037735. Die Anfangsziffern 84 sind in diesem Fall in der Tafel getrennt.

Wir bemerken noch, dass sich mit Tafel III auch die Zahl finden lässt, die nach einem gegebenen Modul, der darin unter der Überschrift des Nenners vorkommt, einem gegebenen Index entspricht, wie wir in Art. 59 versprochen haben. Denn nach dem Vorangegangenen lässt sich offenbar die Periode des Bruchs finden, dessen Zähler, obwohl unbekannt, dem gegebenen Index entspricht. Es genügt, daraus so viele Anfangsziffern zu entnehmen, wie der Nenner Ziffern hat. Aus ihnen ergibt sich nach Art. 313 der Zähler, also die gesuchte Zahl zum gegebenen Index.

317.

Nach dem Vorangegangenen lässt sich die Mantisse jedes Bruchs, dessen Nenner eine Primzahl oder eine Primzahlpotenz innerhalb der Grenzen der Tafel ist, ohne Rechnung auf beliebig viele Ziffern bestimmen. Mithilfe der Untersuchungen am Anfang dieses Abschnitts reicht der Umfang der Tafel aber viel weiter: Er umfasst alle Brüche, deren Nenner Produkte von Primzahlen oder Primzahlpotenzen innerhalb ihrer Grenze sind. Denn ein solcher Bruch lässt sich in andere zerlegen, deren Nenner

diese Faktoren sind. Diese können auf beliebig viele Stellen in Dezimalbrüche umgewandelt werden; dann bleibt nur, sie zu addieren. Wir brauchen kaum zu bemerken, dass die letzte Ziffer der so entstehenden Summe kleiner als die richtige sein kann. Der Fehlbetrag kann aber offenbar nicht so viele Einheiten erreichen, wie einzelne Brüche addiert werden. Daher ist es zweckmäßig, diese auf einige Ziffern mehr zu berechnen, als man für den gegebenen Bruch an richtigen Ziffern benötigt. Als Beispiel betrachten wir den Bruch $\frac{6099380351}{1271808720} = F$[*)], dessen Nenner das Produkt der Zahlen $16, 9, 5, 49, 13, 47, 59$ ist. Nach den obigen Regeln findet man $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$. Diese einzelnen Brüche werden wie folgt in Dezimalbrüche umgewandelt:

$$
\begin{array}{rcllr}
1 & = & 1 & & \\
\frac{11}{16} & = & 0,6875 & & \\
\frac{4}{5} & = & 0,8 & & \\
\frac{4}{9} & = & 0,4444444444 & 4444444444 & 44 \\
\frac{22}{49} & = & 0,4489795918 & 3673469387 & 75 \\
\frac{5}{13} & = & 0,3846153846 & 1538461538 & 46 \\
\frac{7}{47} & = & 0,1489361702 & 1276595744 & 68 \\
\frac{52}{59} & = & 0,8813559322 & 0338983050 & 84 \\
\hline
F & = & 4,7958315233 & 1271954166 & 17
\end{array}
$$

Der Fehlbetrag dieser Summe gegenüber dem richtigen Wert ist sicher kleiner als fünf Einheiten an der letzten, zweiundzwanzigsten Stelle. Daher können die ersten einundzwanzig Ziffern dadurch nicht geändert werden. Setzt man die Rechnung auf mehr Ziffern fort, so erhält man anstelle der letzten beiden Ziffern 17 die Ziffern $1893936\ldots$ — Auch ohne unseren Hinweis wird jeder sehen, dass dieses Verfahren, gewöhnliche Brüche in Dezimalbrüche umzuwandeln, besonders für den Fall geeignet ist, dass viele Dezimalziffern verlangt werden. Genügen wenige, so können gewöhnliche Division oder Logarithmen meist ebenso bequem angewandt werden.

[*)] Dieser Bruch ist einer von denen, die der Quadratwurzel aus 23 so nahe wie möglich kommen; sein Überschuss ist kleiner als sieben Einheiten an der zwanzigsten Dezimalstelle.

318.

Da nun die Umwandlung der Brüche, deren Nenner aus mehreren verschiedenen Primzahlen zusammengesetzt sind, auf den Fall zurückgeführt ist, dass der Nenner eine Primzahl oder eine Primzahlpotenz ist, fügen wir über ihre Mantissen nur wenige Bemerkungen hinzu. Enthält der Nenner weder den Faktor 2 noch 5, so besteht auch hier die Mantisse aus Perioden. Denn auch in diesem Fall erreicht man in der Reihe $10, 100, 1000$ schließlich ein Glied, das nach dem Nenner der Einheit kongruent ist. Zugleich gibt dessen Exponent, der sich nach Art. 92 leicht bestimmen lässt, die vom Zähler unabhängige Länge der Periode an, sofern dieser zum Nenner teilerfremd ist. — Hat der Nenner dagegen die Form $2^\alpha 5^\beta N$, wobei N eine zu 10 teilerfremde Zahl ist und α und β Zahlen sind, von denen wenigstens eine nicht 0 ist, so beginnt die Mantisse nach den ersten α oder β Ziffern aus Perioden zu bestehen, je nachdem α oder β größer ist. Diese stimmen in ihrer Länge mit den Perioden von Brüchen mit dem Nenner N überein. Dies folgt sehr leicht daraus, dass sich jener Bruch in zwei andere mit den Nennern $2^\alpha 5^\beta$ und N zerlegen lässt, von denen der erste nach den ersten α oder β Ziffern abbricht. — Wir könnten über diesen Gegenstand viele weitere Bemerkungen hinzufügen, besonders über Kunstgriffe, eine Tafel wie III möglichst schnell aufzustellen. Der Kürze wegen lassen wir sie hier umso lieber weg, als schon sowohl der angesehene Robertson am angeführten Ort als auch der angesehene Bernoulli (*Nouv. Mém. de l'Ac. de Berlin* 1771 *p.* 273) vieles hierzu mitgeteilt haben.

Lösung der Kongruenz $xx \equiv A$ durch das Ausschlussverfahren.

319.

Die *Lösbarkeit* der Kongruenz $xx \equiv A \pmod{m}$, die mit der unbestimmten Gleichung $xx = A + my$ übereinstimmt, haben wir in Abschnitt IV (Artikel 146) so behandelt, dass nichts weiter zu wünschen übrig zu bleiben scheint. Was jedoch die Ermittlung der Unbekannten selbst betrifft, haben wir schon oben (Artikel 152) bemerkt, dass indirekte Verfahren den direkten bei weitem vorzuziehen sind. Ist m eine Primzahl, auf welchen Fall sich die übrigen leicht zurückführen lassen, so könnten wir zu diesem Zweck die Indextafel I, nach der Bemerkung in Artikel 316 mit III verbunden, verwenden, wie wir in Artikel 60 allgemeiner gezeigt haben; doch wäre dieses Verfahren auf den Umfang der Tafel beschränkt. Aus diesen Gründen hoffen wir, dass das folgende allgemeine und bequeme Verfahren den Liebhabern der Arithmetik willkommen sein wird.

Zunächst bemerken wir, dass es genügt, nur diejenigen Werte von x zu ermitteln, die positiv und nicht größer als $\frac{1}{2}m$ sind, da jeder andere Wert nach dem Modul m einem von ihnen oder dessen Negativem kongruent ist. Bei einem solchen Wert von x muss der Wert von y zwischen den Grenzen $-\frac{A}{m}$ und $\frac{1}{4}m - \frac{A}{m}$ liegen. Das Verfahren, das sich unmittelbar anbietet, bestünde also darin, für jeden innerhalb dieser Grenzen liegenden Wert von y (die Gesamtheit dieser Werte wollen wir mit Ω bezeichnen) den Wert von $A + my$, den wir mit V bezeichnen, zu berechnen und nur diejenigen beizubehalten, für die V ein Quadrat wird. Ist m eine kleine Zahl (*z. B.* unter 40), so ist dieser Versuch so kurz, dass er kaum einer Abkürzung bedarf; ist dagegen m groß, so lässt sich die Arbeit durch das folgende *Ausschlussverfahren* beliebig verkürzen.

320.

Es sei E eine beliebige ganze, zu m teilerfremde Zahl größer als 2, und alle ihre verschiedenen quadratischen Nichtreste (*d. h.* nach E inkongruenten Nichtreste) seien a, b, c usw.; schließlich seien die Wurzeln der Kongruenzen

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c \quad \text{usw. nach dem Modul } E$$

die Zahlen α, β, γ usw., die alle positiv und kleiner als E gewählt werden dürfen. Gibt man also y einen Wert, der einer der Zahlen α, β, γ usw. nach E kongruent ist, so ist der daraus entstehende Wert von $V = A + my$ einer der Zahlen a, b, c usw. kongruent, also ein Nichtrest von E, und kann daher kein Quadrat sein. Somit können aus Ω sofort alle Zahlen der Formen $Et + \alpha, Et + \beta, Et + \gamma$ usw. als unbrauchbar ausgeschlossen werden, und es genügt, die übrigen, deren Gesamtheit Ω' sei, zu erproben. Bei dieser Operation kann man der Zahl E den Namen *Ausschlusszahl* geben.

Nimmt man nun eine andere geeignete Zahl E' als Ausschlusszahl, so findet man auf genau dieselbe Weise ebenso viele Zahlen α', β', γ' usw., wie sie verschiedene quadratische Nichtreste hat, denen y nach dem Modul E' nicht kongruent sein kann. Daher darf man wiederum aus Ω' alle Zahlen der Formen $E't + \alpha', E't + \beta', E't + \gamma'$ usw. entfernen. So kann man mit immer weiteren Ausschlusszahlen fortfahren, bis die Menge der Zahlen aus Ω so weit verkleinert ist, dass es nicht schwieriger erscheint, alle übrigen tatsächlich zu erproben, als neue Ausschlüsse vorzunehmen.

Beispiel. Ist die Gleichung $xx = 22 + 97y$ gegeben, so sind die Grenzen der Werte von y gleich $-\frac{22}{97}$ und $24\frac{1}{4} - \frac{22}{97}$. Da der Wert 0 offenbar unbrauchbar ist, umfasst Ω also die Zahlen $1, 2, 3 \ldots 24$. Für $E = 3$ gibt es nur den einen Nichtrest $a = 2$; daraus folgt $\alpha = 1$. Somit sind aus Ω alle Zahlen der Form $3t + 1$ auszuschließen; die Anzahl der verbleibenden Zahlen Ω' ist 16. Ebenso hat man für $E = 4$ die Werte $a = 2, b = 3$, also $\alpha = 0, \beta = 1$; daher müssen die Zahlen der Formen $4t$ und $4t + 1$ verworfen werden, und es bleiben diese acht: $2, 3, 6, 11, 14, 15, 18, 23$. Ebenso findet man für $E = 5$, dass die Zahlen der Formen $5t$ und $5t + 3$ zu verwerfen sind; es bleiben $2, 6, 11, 14$. Die Ausschlusszahl 6 würde die Zahlen der Formen $6t + 1$ und $6t + 4$ entfernen; diese, die mit den Zahlen der Form $3t + 1$ übereinstimmen, fehlen aber bereits. Die Ausschlusszahl 7 entfernt die Zahlen der Formen $7t + 2, 7t + 3$, $7t + 5$ und lässt $6, 11, 14$ übrig. Setzt man diese für y ein, so erhält man der Reihe nach $V = 604, 1089, 1380$, wovon allein der zweite Wert ein Quadrat ist; daraus folgt $x = \mp 33$.

321.

Die mit der Ausschlusszahl E ausgeführte Operation entfernt unter den Werten von V, die den Werten von y in Ω entsprechen, alle quadratischen Nichtreste von E, lässt aber die Reste derselben Zahl unberührt. Daher ist leicht einzusehen, dass sich die Verwendung der Ausschlusszahlen E und $2E$ nicht unterscheidet, wenn E ungerade ist, da in diesem Fall E und $2E$ dieselben Reste und Nichtreste haben. Werden also die Zahlen $3, 4, 5$ usw. nacheinander als Ausschlusszahlen verwendet, so sind die Zahlen $6, 10, 14$ usw., die das Doppelte ungerader Zahlen sind, als überflüssig zu überspringen. Ferner ist klar, dass die beiden mit den Ausschlusszahlen E, E' ausgeführten Operationen alle Werte von V entfernen, die Nichtreste beider Zahlen E, E' oder einer von ihnen sind, und diejenigen übrig lassen, die Reste beider sind. Haben nun E und E' keinen gemeinsamen Teiler, so sind alle entfernten Zahlen Nichtreste und alle übrigen Reste des Produkts EE'. Daher bewirkt die Verwendung der Ausschlusszahl EE' in diesem Fall offenbar genau dasselbe wie die Verwendung der beiden Zahlen E, E' und ist somit nach diesen überflüssig. Man darf also auch alle Ausschlusszahlen überspringen, die sich in zwei teilerfremde Faktoren zerlegen lassen, und braucht nur Primzahlen, die m nicht teilen, oder Primzahlpotenzen zu verwenden. Schließlich ist klar, dass nach Verwendung der Ausschlusszahl p^μ, einer Potenz der Primzahl p, die Ausschlusszahl p oder p^ν bei $\nu < \mu$ überflüssig wird. Da nämlich p^μ unter den Werten von V nur seine Reste übrig gelassen hat, sind erst recht keine Nichtreste von p oder einer beliebigen niedrigeren Potenz p^ν mehr vorhanden. Ist aber p oder p^ν bereits vor p^μ verwendet worden, so kann die letztere offenbar nur solche Werte von V entfernen, die zugleich Reste von p (oder p^ν) und Nichtreste von p^μ sind. Daher genügt es, nur solche Nichtreste von p^μ für a, b, c usw. zu nehmen.

322.

Die Berechnung der Zahlen α, β, γ usw., die einer gegebenen Ausschlusszahl E entsprechen, wird durch die folgenden Bemerkungen erheblich verkürzt. Es seien $\mathfrak{A}$, $\mathfrak{B}, \mathfrak{C}$ usw. Wurzeln der Kongruenzen $my \equiv a, my \equiv b, my \equiv c$ usw. (mod. E) und k eine Wurzel von $my \equiv -A$; dann gilt offenbar $\alpha \equiv \mathfrak{A} + k, \beta \equiv \mathfrak{B} + k, \gamma \equiv \mathfrak{C} + k$ usw. Müsste man nun $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. tatsächlich durch Lösung dieser Kongruenzen ermitteln,

so wäre dieser Weg zur Bestimmung von α, β, γ usw. gewiss nicht kürzer als der oben gezeigte; doch ist dies keineswegs nötig. Ist nämlich erstens E eine Primzahl und m ein quadratischer Rest von E, so folgt aus Artikel 98, dass $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw., die die Werte der Ausdrücke $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}$ usw. (mod. E) sind, verschiedene Nichtreste von E sind und daher mit α, β, γ usw. vollständig übereinstimmen, wenn man von ihrer Reihenfolge absieht, die hier keine Rolle spielt. Ist dagegen unter derselben Voraussetzung m ein Nichtrest von E, so stimmen die Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. mit sämtlichen quadratischen Resten außer 0 überein. Ist E das Quadrat einer ungeraden Primzahl, $= pp$, und p bereits als Ausschlusszahl verwendet worden, so genügt es nach dem vorigen Artikel, für a, b, c usw. diejenigen Nichtreste von pp zu nehmen, die Reste von p sind, *d. h.* die Zahlen $p, 2p, 3p \ldots pp - p$ (also sämtliche Zahlen unter pp außer 0, die durch p teilbar sind). Daraus ist leicht einzusehen, dass sich für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. genau dieselben Zahlen ergeben müssen, nur in anderer Reihenfolge. Setzt man ebenso nach Verwendung der Ausschlusszahlen p und pp nun $E = p^3$, so genügt es, für a, b, c usw. die Produkte der einzelnen Nichtreste von p mit pp zu nehmen. Dann ergeben sich für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. entweder dieselben Zahlen oder die Produkte von pp mit den einzelnen Resten von p außer 0, je nachdem, ob m Rest oder Nichtrest von p ist. Nimmt man allgemein für E eine beliebige Primzahlpotenz, etwa p^μ, nachdem alle niedrigeren Potenzen bereits verwendet worden sind, so ergeben sich für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. die Produkte von $p^{\mu-1}$ entweder mit sämtlichen Zahlen kleiner als p, stets außer 0, wenn μ gerade ist; oder mit sämtlichen Nichtresten von p kleiner als p, wenn μ ungerade ist und mRp gilt; oder mit sämtlichen Resten, wenn mNp gilt. — Ist $E = 4$, also $a = 2, b = 3$, so hat man für $\mathfrak{A}, \mathfrak{B}$ entweder 2 und 3 oder 2 und 1, je nachdem, ob $m \equiv 1$ oder $\equiv 3$ (mod. 4) gilt. Setzt man nach Verwendung der Ausschlusszahl 4 nun $E = 8$, so hat man $\alpha = 5$, woraus sich für $\mathfrak{A}$ die Werte $5, 7, 1, 3$ ergeben, je nachdem, ob $m \equiv 1, 3, 5, 7$ (mod. 8) gilt. Ist nun allgemein E eine beliebige höhere Potenz von zwei, etwa 2^μ, nachdem die niedrigeren bereits verwendet worden sind, so muss man $a = 2^{\mu-1}, b = 3.2^{\mu-2}$ setzen, wenn μ gerade ist. Daraus folgt $\mathfrak{A} = 2^{\mu-1}, \mathfrak{B} = 3.2^{\mu-2}$ oder $= 2^{\mu-2}$, je nachdem, ob $m \equiv 1$ oder $\equiv 3$ gilt. Ist dagegen μ ungerade, so muss man $a = 5.2^{\mu-3}$ setzen; dann ist $\mathfrak{A}$ gleich dem Produkt der Zahl $2^{\mu-3}$ mit $5, 7, 1$ oder 3, je nachdem, ob $m \equiv 1, 3, 5$ oder 7 (mod. 8) gilt.

Sachkundige werden sich im Übrigen leicht einen Apparat ausdenken, mit dem die unbrauchbaren Werte von y *mechanisch* aus Ω entfernt werden können, nachdem die Zahlen α, β, γ usw. für so viele Ausschlusszahlen berechnet worden sind, wie nötig erscheinen; doch können wir hier weder darauf noch auf andere Hilfsmittel zur Verkürzung der Arbeit eingehen.

Lösung der unbestimmten Gleichung $mxx + nyy = A$ durch Ausschlüsse.

323.

In Abschnitt V haben wir gezeigt, wie man sämtliche Darstellungen einer gegebenen Zahl A durch die binäre Form $mxx + nyy$, also die Lösungen der unbestimmten Gleichung $mxx + nyy = A$, nach einem allgemeinen Verfahren findet, dessen Kürze ebenfalls nichts zu wünschen übrig zu lassen scheint, wenn sämtliche Werte des Ausdrucks $\sqrt{-mn}$ nach dem Modul A selbst und nach der durch ihre quadratischen Faktoren geteilten Zahl bereits vorliegen. Hier wollen wir jedoch für den Fall, dass mn positiv ist, eine Lösung erläutern, die viel bequemer als die direkte ist, wenn man für diese jene Werte erst berechnen muss. Wir setzen dabei voraus, dass die Zahlen m, n und A positiv und paarweise teilerfremd sind, da sich die übrigen Fälle leicht auf diesen zurückführen lassen. Offenbar genügt es auch, positive Werte von x, y zu ermitteln, weil die übrigen daraus allein durch Änderung der Vorzeichen folgen.

Offenbar muss x so beschaffen sein, dass $\frac{A-mxx}{n}$, wofür wir V schreiben wollen, positiv, ganzzahlig und ein Quadrat wird. Die erste Bedingung verlangt, dass x nicht größer als $\sqrt{\frac{A}{m}}$ ist; die zweite ist bei $n = 1$ von selbst erfüllt und verlangt andernfalls, dass der Wert des Ausdrucks $\frac{A}{m}$ (mod. n) ein quadratischer Rest von n ist. Bezeichnen wir sämtliche verschiedenen Werte des Ausdrucks $\sqrt{\frac{A}{m}}$ (mod. n) mit $\pm r, \pm r'$ usw., so muss x unter einer der Formen $nt + r, nt - r, nt + r'$ usw. enthalten sein. Am einfachsten wäre es daher, sämtliche Zahlen dieser Formen unterhalb der Grenze $\sqrt{\frac{A}{m}}$ (die Gesamtheit dieser Zahlen wollen wir mit Ω bezeichnen) für x einzusetzen und nur diejenigen beizubehalten, für die V ein Quadrat wird. Wie man diesen Versuch beliebig verkürzen kann, werden wir im nächsten Artikel zeigen.

324.

Das Ausschlussverfahren, mit dem wir dies erreichen wollen, besteht wie in der vorigen Untersuchung darin, mehrere Zahlen nach Belieben zu wählen, die auch hier *Ausschlusszahlen* heißen sollen, zu untersuchen, für welche Werte von x der Wert von V ein quadratischer Nichtrest dieser Ausschlusszahlen wird, und solche Werte von x aus Ω zu entfernen. Durch Überlegungen, die den in Artikel 321 dargelegten völlig entsprechen, ergibt sich, dass man nur Primzahlen oder Primzahlpotenzen als Ausschlusszahlen verwenden muss. Bei einer Ausschlusszahl der letzteren Art sind unter den Werten von V nur diejenigen ihrer Nichtreste auszuschließen, die Reste sämtlicher niedrigerer Potenzen derselben Primzahl sind, sofern die Ausschlüsse mit diesen bereits vorgenommen worden sind.

Die Ausschlusszahl sei also $E = p^\mu$, einschließlich des Falles $\mu = 1$, wobei p eine Primzahl ist, die m nicht teilt, und wir nehmen an[*)], dass p^ν die höchste Potenz derselben Primzahl ist, durch die n teilbar ist. Es seien a, b, c usw. quadratische Nichtreste von E: sämtliche, wenn $\mu = 1$, und die notwendigen, also diejenigen, die Reste der niedrigeren Potenzen sind, wenn $\mu > 1$. Man berechne die Wurzeln der Kongruenzen $mz \equiv A - na, mz \equiv A - nb, mz \equiv A - nc$ usw. (mod. $Ep^\nu = p^{\mu+\nu}$), die α, β, γ usw. seien. Dann ist leicht einzusehen, dass, wenn für einen Wert

[*)] Der Kürze wegen behandeln wir die beiden Fälle, in denen n durch p teilbar beziehungsweise nicht teilbar ist, gemeinsam; im letzteren muss man $\nu = 0$ setzen.

von x die Kongruenz $xx \equiv \alpha$ (mod. Ep^ν) gilt, der entsprechende Wert von $V \equiv a$ (mod. E), also ein Nichtrest von E wird; ebenso verhält es sich mit den übrigen Zahlen β, γ usw. Umgekehrt ist ebenso leicht einzusehen, dass, wenn ein Wert von x die Kongruenz $V \equiv a$ (mod. E) liefert, für denselben Wert $xx \equiv \alpha$ (mod. Ep^ν) gilt. Somit liefern alle Werte von x, für die xx keiner der Zahlen α, β, γ usw. nach dem Modul Ep^ν kongruent ist, solche Werte von V, die keiner der Zahlen a, b, c usw. nach dem Modul E kongruent sind. Man wähle nun unter den Zahlen α, β, γ usw. sämtliche quadratischen Reste von Ep^ν aus, die g, g', g'' usw. seien, berechne die Werte der Ausdrücke $\sqrt{g}, \sqrt{g'}.\sqrt{g''}$ usw. (mod. Ep^ν) und nehme an, dass sich daraus $\pm h, \pm h', \pm h''$ usw. ergeben. Dann ist klar, dass man sämtliche Zahlen der Formen $Ep^\nu t \pm h, Ep^\nu t \pm h', Ep^\nu t \pm h''$ usw. sicher aus Ω entfernen kann und dass keinem Wert von x, der nach diesem Ausschluss in Ω verbleibt, ein Wert von V der Formen $Eu + a, Eu + b, Eu + c$ usw. entsprechen kann. Ferner ist offenbar, dass solche Werte von V schon von selbst aus keinem Wert von x entstehen können, wenn sich unter den Zahlen α, β, γ usw. keine quadratischen Reste von Ep^ν finden; in diesem Fall kann man die Zahl E daher nicht als Ausschlusszahl verwenden. — Man kann beliebig viele solche Ausschlusszahlen anwenden und so die Menge der Zahlen in Ω beliebig verkleinern.

Sehen wir nun zu, ob man auch Primzahlen, die m teilen, oder Potenzen solcher Primzahlen als Ausschlusszahlen verwenden darf. Es sei B der Wert des Ausdrucks $\frac{A}{n}$ (mod. m). Offenbar wird V stets B nach dem Modul m kongruent, welcher Wert auch für x genommen wird; zur Lösbarkeit der gegebenen Gleichung ist daher notwendig, dass B ein quadratischer Rest von m ist. Bezeichnet nun p einen beliebigen ungeraden Primteiler von m, der nach Voraussetzung weder n noch A teilt und somit auch B nicht teilt, so ist für jeden Wert von x V ein Rest von p und damit auch jeder Potenz von p; daher können p und seine Potenzen nicht als Ausschlusszahlen dienen. Auf genau dieselbe Weise ist, wenn m durch 8 teilbar ist, zur Lösbarkeit der gegebenen Gleichung notwendig, dass $B \equiv 1$ (mod. 8) gilt. Dann wird auch V für jeden Wert von $x \equiv 1$ (mod. 8), und daher eignen sich die Zweierpotenzen nicht zum Ausschluss. — Wenn aber m durch 4, jedoch nicht durch 8 teilbar ist, so muss aus demselben Grund $B \equiv 1$ (mod. 4) gelten; der Wert des Ausdrucks $\frac{A}{n}$ (mod. 8) ist daher entweder 1 oder 5 und werde mit C bezeichnet. Man sieht leicht, dass für einen geraden Wert von x hier $V \equiv C$, für einen ungeraden dagegen $V \equiv C + 4$ (mod. 8) gilt. Daher sind die geraden Werte zu verwerfen, wenn $C = 5$, und die ungeraden, wenn $C = 1$. — Ist schließlich m durch 2, jedoch nicht durch 4 teilbar, so sei wie zuvor C der Wert des Ausdrucks $\frac{A}{n}$ (mod. 8), der $1, 3, 5$ oder 7 ist; und D sei der Wert von $\frac{\frac{1}{2}m}{n}$ (mod. 4), der 1 oder 3 ist. Da nun der Wert von V offenbar stets $\equiv C - 2Dxx$ (mod. 8) wird, also für gerades $x \equiv C$ und für ungerades $\equiv C - 2D$, folgt daraus leicht, dass alle ungeraden Werte von x zu verwerfen sind, wenn $C = 1$; alle geraden, wenn $C = 3$ und $D = 1$ oder $C = 7$ und $D = 3$; und dass sämtliche übrigen Werte $V \equiv 1$ (mod. 8), also einen Rest jeder Zweierpotenz liefern. In den anderen Fällen dagegen, nämlich wenn $C = 5$ oder $C = 3$ und $D = 3$ oder $C = 7$ und $D = 1$, wird $V \equiv 3, 5$ oder 7 (mod. 8), ob man x gerade oder ungerade nimmt. Daraus geht hervor, dass die gegebene Gleichung in diesen Fällen überhaupt keine Lösung besitzt.

Da wir im Übrigen auf genau dieselbe Weise, wie wir hier den Wert von x durch Ausschlüsse zu finden gezeigt haben, mit den nötigen Änderungen auch den Wert von y ermitteln können, lässt sich das Ausschlussverfahren stets auf zwei Arten zur Lösung des gegebenen Problems anwenden, sofern nicht $m = n = 1$, wobei beide zusammenfallen. Meist ist diejenige vorzuziehen, für die Ω weniger Glieder enthält, was man leicht im Voraus abschätzen kann. — Schließlich brauchen wir kaum zu bemerken, dass, wenn nach einigen Ausschlüssen *sämtliche* Zahlen aus Ω verschwunden sind, dies als sicheres Zeichen der Unlösbarkeit der gegebenen Gleichung anzusehen ist.

325.

Beispiel. Es sei die Gleichung $3xx + 455yy = 10857362$ gegeben, die wir auf zwei Arten lösen wollen: *erstens*, indem wir die Werte von x, dann die Werte von y ermitteln. Die Grenze der ersteren ist in diesem Fall $\sqrt{3619120\frac{2}{3}}$, die zwischen 1902 und 1903 liegt; der Wert des Ausdrucks $\frac{A}{3}$ (mod. 455) ist 354, und die Werte des Ausdrucks $\sqrt{354}$ (mod. 455) sind $\pm 82, \pm 152, \pm 173, \pm 212$. Daher besteht Ω aus den folgenden 33 Zahlen: $82, 152, 173, 212,\ 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083,\ 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902$. Die Zahl 3 lässt sich in diesem Fall nicht zum Ausschluss verwenden, weil sie m teilt. Für die Ausschlusszahl 4 haben wir $a = 2, b = 3$, also $\alpha = 0, \beta = 3$; $g = 0$, und die Werte des Ausdrucks $\sqrt{g}$ (mod. 4) sind 0 und 2. Somit sind alle Zahlen der Formen $4t$ und $4t+2$, *d. h.* alle geraden Zahlen, aus Ω zu entfernen; die sechzehn übrigen seien mit Ω' bezeichnet. Für $E = 5$, wobei diese Ausschlusszahl auch n teilt, haben die Kongruenzen $mz \equiv A - 2n$ und $mz \equiv A - 3n$ (mod. 25) die Wurzeln 9 und 24, die beide Reste von 25 sind; die Werte der Ausdrücke $\sqrt{9}$ und $\sqrt{24}$ (mod. 25) sind $\pm 3,\ \pm 7$. Entfernt man aus Ω' sämtliche Zahlen der Formen $25t \pm 3,\ 25t \pm 7$, so bleiben diese zehn (Ω''): $173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577$. Für $E = 7$ haben die Kongruenzen $mz \equiv A - 3n,\ mz \equiv A - 5n,\ mz \equiv A - 6n$ (mod. 49) die Wurzeln $32, 39, 18$, die sämtlich Reste von 49 sind, und die Werte der Ausdrücke $\sqrt{32}, \sqrt{39}, \sqrt{18}$ (mod. 49) sind $\pm 9, \pm 23, \pm 19$. Entfernt man aus Ω'' die Zahlen der Formen $49t \pm 9,\ 49t \pm 19,\ 49t \pm 23$, so bleiben diese fünf (Ω'''): 537, 737, $1083, 1213, 1517$. Für $E = 8$ haben wir $a = 5$, also $\alpha = 5$, einen Nichtrest von 8; daher lässt sich die Ausschlusszahl 8 nicht verwenden. Die Zahl 9 ist aus demselben Grund zu überspringen wie 3. Für $E = 11$ sind die Zahlen a, b usw. gleich $2, 6,\ 7, 8,\ 10$; $\nu = 0$; somit α, β usw. $= 8, 10, 5, 0, 1$, von denen drei Reste von 11 sind, nämlich $0, 1, 5$. Daraus folgt, dass aus Ω''' die Zahlen der Formen $11t,\ 11t \pm 1,\ 11t \pm 4$ zu verwerfen sind, worauf $537, 1083, 1213$ übrig bleiben. Bei der Probe ergeben sich für V der Reihe nach die Werte $21961, 16129, 14161$, von denen allein der zweite und dritte Quadrate sind. Die gegebene Gleichung besitzt daher zwei Lösungen mit positiven Werten von x, y, nämlich $x = 1083, y = 127$ und $x = 1213, y = 119$.

Zweitens. Will man die andere Unbekannte derselben Gleichung durch Ausschlüsse ermitteln, so bringe man diese in die Form $455xx + 3yy = 10857362$, indem man x mit y vertauscht, um sämtliche Bezeichnungen der Artikel 323, 324 beibehalten zu können. Die Grenze der Werte von x liegt hier zwischen 154 und 155; der Wert des Ausdrucks $\frac{A}{m}$ (mod. n) ist 1, und die Werte von $\sqrt{1}$ (mod. 3) sind $+1$ und -1. Daher enthält Ω sämtliche Zahlen der Formen $3t + 1$ und $3t - 1$, *d. h.* alle durch 3 nicht teilbaren Zahlen bis einschließlich 154, deren Anzahl 103 ist. Wendet man die oben gegebenen Regeln an, so findet man, dass für die Ausschlusszahlen 3; 4; 9; 11; 17; 19; 23 die Zahlen der Formen $9t \pm 4$; $4t$, $4t \pm 2$, also alle geraden Zahlen; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$ zu verwerfen sind. Nach deren Entfernung bleiben 119, 127 übrig, die allein V einen quadratischen Wert geben und dieselben Lösungen liefern, zu denen wir oben gelangt sind.

326.

Das vorangehende Verfahren ist schon für sich so bequem, dass es kaum etwas zu wünschen übrig lässt. Dennoch kann es durch verschiedene Hilfsmittel noch erheblich verkürzt werden, von denen wir hier nur wenige berühren können. Wir beschränken die Untersuchung daher auf den Fall, dass die Ausschlusszahl eine ungerade Primzahl ist, die A nicht teilt, oder eine Potenz einer solchen Primzahl, zumal sich die übrigen Fälle entweder darauf zurückführen oder durch ein ähnliches Verfahren behandeln lassen. Nehmen wir *erstens* an, dass die Ausschlusszahl $E = p$ eine Primzahl ist, die keine der Zahlen m, n teilt, und die Werte der Ausdrücke $\frac{A}{m}, -\frac{na}{m}, -\frac{nb}{m}, -\frac{nc}{m}$ usw. (mod. p) der Reihe nach $k, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. sind. Dann findet man die Zahlen α, β, γ usw. durch die Kongruenzen $\alpha \equiv k+\mathfrak{A},\ \beta \equiv k+\mathfrak{B},\ \gamma \equiv k+\mathfrak{C}$ usw. (mod. p). Die Zahlen $\mathfrak{A}$, $\mathfrak{B}, \mathfrak{C}$ usw. lassen sich jedoch durch ein Hilfsmittel, das dem in Artikel 322 verwendeten völlig entspricht, ohne Berechnung der Kongruenzen ermitteln. Sie stimmen entweder mit sämtlichen Nichtresten oder mit sämtlichen Resten von p, außer 0, überein, je nachdem, ob der Wert des Ausdrucks $-\frac{m}{n}$ (mod. p) oder, was hier auf dasselbe hinausläuft, die Zahl $-mn$ ein Rest oder ein Nichtrest von p ist. So hat man im *Beispiel* II des vorigen Artikels für $E = 17$ den Wert $k = 7$; $-mn = -1365 \equiv 12$ ist ein Nichtrest von 17. Daher sind die Zahlen $\mathfrak{A}, \mathfrak{B}$ usw. gleich $1, 2, 4, 8, 9, 13, 15, 16$ und die Zahlen α, β usw. gleich $8, 9, 11, 15, 16, 3, 5, 6$. Davon sind $8, 9, 15, 16$ Reste; somit ergeben sich für $\pm h, h'$ usw. die Werte $\pm 5, 3, 7, 4$. — Wer öfter solche Probleme zu lösen hat, wird sich die Arbeit erheblich erleichtern, wenn er für mehrere Primzahlen p die Werte von h, h' usw., die den einzelnen Werten von k $(1, 2, 3 \ldots p-1)$ entsprechen, unter beiden Voraussetzungen berechnet: dass $-mn$ Rest beziehungsweise Nichtrest von p ist. Ferner bemerken wir, dass die Anzahl der Zahlen $h, -h, h'$ usw. stets $\frac{1}{2}(p-1)$ ist, wenn sowohl k als auch $-mn$ Reste oder beide Nichtreste von p sind; $\frac{1}{2}(p-3)$, wenn die erste Zahl $R.$ und die zweite $NR.$ ist; und $\frac{1}{2}(p+1)$, wenn die erste $NR.$ und die zweite $R.$ ist. Den Beweis dieses Satzes müssen wir jedoch auslassen, um nicht zu ausführlich zu werden.

Zweitens lassen sich die Fälle, in denen E eine Primzahl ist, die n teilt, oder eine Potenz einer ungeraden Primzahl, die n teilt oder nicht teilt, noch bequemer behandeln. Wir fassen sämtliche Fälle zusammen und setzen unter Beibehaltung aller Bezeichnungen des Artikels 324 nun $n = n'p^\nu$, sodass n' durch p nicht teilbar ist. Die Zahlen a, b, c usw. sind die Produkte von $p^{\mu-1}$ entweder mit sämtlichen Zahlen kleiner als p, außer 0, oder mit sämtlichen Nichtresten von p unterhalb p, je nachdem, ob μ gerade oder ungerade ist; sie seien allgemein durch $up^{\mu-1}$ bezeichnet. Es sei k der Wert des Ausdrucks $\frac{A}{m}$ (mod. $p^{\mu+\nu}$). Dieser ist durch p nicht teilbar, weil dieselbe Eigenschaft bei A vorausgesetzt wird; ferner ist klar, dass sämtliche Zahlen α, β, γ usw. der Zahl k nach dem Modul p kongruent sind und daher p^μ nichts aus Ω ausschließt, wenn kNp gilt. Gilt dagegen kRp und somit auch $kRp^{\mu+\nu}$, so sei r ein Wert des Ausdrucks $\sqrt{k}$ (mod. $p^{\mu+\nu}$), der durch p nicht teilbar ist, und e der Wert von $-\frac{n'}{2mr}$ (mod. p). Dann gilt $\alpha \equiv rr + 2erap^\nu$ (mod. $p^{\mu+\nu}$), woraus leicht folgt, dass α ein Rest von $p^{\mu+\nu}$ ist und die Werte des Ausdrucks $\sqrt{\alpha}$ (mod. $p^{\mu+\nu}$) gleich $\pm(r + eap^\nu)$ sind. Somit sind sämtliche Zahlen h, h', h'' usw. durch $r + uep^{\mu+\nu-1}$ darstellbar. Schließlich folgt daraus leicht, dass die Zahlen h, h', h'' usw. entstehen, indem man r zu den Produkten von $p^{\mu+\nu-1}$ entweder mit sämtlichen Zahlen unter p,

außer 0, addiert, wenn μ gerade ist; oder mit sämtlichen Nichtresten von p unter dieser Grenze, wenn μ ungerade ist und eRp oder, was hier dasselbe bedeutet, $-2mrn'Rp$ gilt; oder mit sämtlichen Resten, außer 0, wenn μ ungerade ist und $-2mrn'Np$ gilt.

Sobald die Zahlen h, h' usw. für die einzelnen Ausschlusszahlen, die man verwenden will, ermittelt sind, lässt sich im Übrigen auch der Ausschluss selbst durch mechanische Operationen ausführen, die sich jeder in diesen Dingen Erfahrene leicht selbst ausdenken kann, wenn es der Mühe wert erscheint.

Schließlich müssen wir bemerken, dass jede Gleichung $axx + 2bxy + cyy = M$, in der $bb - ac$ eine negative Zahl $= -D$ ist, leicht auf die oben betrachtete Form zurückgeführt werden kann. Bezeichnen wir nämlich den größten gemeinsamen Teiler der Zahlen a, b mit m und setzen

$$a = ma'. \quad b = mb', \quad \frac{D}{m} = a'c - mb'b' = n, \quad a'x + b'y = x'$$

so ist jene Gleichung offenbar zu $mx'x' + nyy = a'M$ äquivalent und lässt sich nach den oben angegebenen Regeln lösen. Von deren Lösungen sind aber nur diejenigen beizubehalten, in denen $x' - b'y$ durch a' teilbar ist, aus denen sich also ganzzahlige Werte von x ergeben.

Ein anderes Verfahren zur Lösung der Kongruenz $xx \equiv A$, wenn A negativ ist.

327.

Wie die in Abschnitt V angegebene direkte Lösung der Gleichung $axx + 2bxy + cyy = M$ die Werte des Ausdrucks $\sqrt{(bb - ac)}$ (mod. M) als bekannt voraussetzt, so liefert umgekehrt für den Fall, dass $bb - ac$ negativ ist, die oben erläuterte indirekte Lösung ein sehr bequemes Verfahren zur Ermittlung jener Werte. Besonders bei einem sehr großen Wert von M ist es dem Verfahren des Artikels 322 und der folgenden Artikel bei weitem vorzuziehen. Wir nehmen jedoch an, dass M eine Primzahl ist oder wenigstens ihre Faktoren, falls sie zusammengesetzt ist, noch unbekannt sind. Wüsste man nämlich, dass die Primzahl p die Zahl M teilt und $M = p^\mu M'$ gilt, wobei M' den Faktor p nicht mehr enthält, so wäre es viel bequemer, die Werte des Ausdrucks $\sqrt{(bb - ac)}$ für die Moduln p^μ und M' einzeln zu ermitteln, die ersteren aus den Werten nach dem Modul p, Artikel 101, und die Werte nach dem Modul M durch deren Verbindung abzuleiten, Artikel 105.

Gesucht seien also sämtliche Werte des Ausdrucks $\sqrt{-D}$ (mod. M), wobei D und M als positiv und M unter einer Form der Teiler von $xx + D$ enthalten vorausgesetzt werden, Artikel 147 und die folgenden. Andernfalls stünde nämlich von vornherein fest, dass keine Zahlen dem gegebenen Ausdruck genügen können. Die gesuchten Werte, von denen stets je zwei entgegengesetzt sind, seien $\pm r, \pm r', \pm r''$ usw., und es gelte $D + rr = Mh$, $D + r'r' = Mh'$, $D + r''r'' = Mh''$ usw. Die Klassen, zu denen die Formen (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''). $(M, -r'', h'')$ usw. gehören, seien der Reihe nach mit $\mathfrak{C}, -\mathfrak{C}, \mathfrak{C}', -\mathfrak{C}', \mathfrak{C}'', -\mathfrak{C}''$ usw. und ihre Gesamtheit mit $\mathfrak{G}$ bezeichnet. Diese Klassen sind im Allgemeinen zwar als unbekannt anzusehen. Dennoch ist klar, *erstens*, dass sie sämtlich positiv und eigentlich primitiv sind, *zweitens*, dass sie alle zu demselben Geschlecht gehören, dessen *Charakter* sich leicht aus

der Beschaffenheit der Zahl M, *d. h.* aus ihren Beziehungen zu den einzelnen Primteilern von D und außerdem zu 4 oder 8, wenn diese nötig sind, erkennen lässt, Artikel 230. Da vorausgesetzt ist, dass M unter einer Form der Teiler von $xx + D$ enthalten ist, können wir von vornherein sicher sein, dass diesem Charakter notwendig ein Geschlecht positiver, eigentlich primitiver Formen der Determinante $-D$ entspricht, selbst wenn der Ausdruck $\sqrt{-D}$ (mod. M) möglicherweise keine Lösungen besitzt. Da dieses Geschlecht somit bekannt ist, lassen sich sämtliche darin enthaltenen Klassen ermitteln; sie seien C, C', C'' usw. und ihre Gesamtheit G.

Somit ist klar, dass jede Klasse $\mathfrak{C}$, $-\mathfrak{C}$ usw. mit einer Klasse in G identisch sein muss. Es kann auch vorkommen, dass mehrere Klassen in $\mathfrak{G}$ untereinander und somit mit derselben Klasse in G identisch sind. Enthält G nur eine einzige Klasse, so stimmen gewiss alle Klassen in $\mathfrak{G}$ mit dieser überein. Wählt man daher aus den Klassen C, C', C'' usw. die einfachsten Formen f, f', f'' usw., je eine aus jeder, so befindet sich unter diesen eine Form aus jeder Klasse in $\mathfrak{G}$. Ist nun $axx + 2bxy + cyy$ eine Form in der Klasse $\mathfrak{C}$, so gibt es durch sie zwei Darstellungen der Zahl M, die zum Wert r gehören; ist die eine $x = m, y = n$, so ist die andere $x = -m, y = -n$. Nur der Fall $D = 1$ ist auszunehmen, in dem es vier Darstellungen gibt; siehe Artikel 180.

Hieraus folgt, dass, wenn sämtliche Darstellungen der Zahl M durch die einzelnen Formen f, f', f'' usw. nach dem oben angegebenen indirekten Verfahren ermittelt und daraus die Werte des Ausdrucks $\sqrt{-D}$ (mod. M) abgeleitet werden, zu denen die einzelnen Darstellungen gehören, Artikel 154 und die folgenden, man *sämtliche* Werte dieses Ausdrucks erhält, und zwar jeden zweimal oder, wenn $D = 1$, viermal. *Q. E. F.* Finden sich unter f, f' usw. Formen, durch die M nicht darstellbar ist, so zeigt dies an, dass sie zu keiner Klasse in $\mathfrak{G}$ gehören und deshalb unberücksichtigt bleiben müssen. Lässt sich aber M durch keine jener Formen darstellen, so muss $-D$ ein quadratischer Nichtrest von M sein. — Bei diesen Operationen sind noch die folgenden Bemerkungen zu beachten.

I. Unter den hier verwendeten Darstellungen der Zahl M durch die Formen f, f' usw. sind solche zu verstehen, bei denen die Werte der Unbestimmten teilerfremd sind. Ergeben sich andere, bei denen diese Werte einen gemeinsamen Teiler μ haben, was nur vorkommen kann, wenn $\mu\mu$ die Zahl M teilt, und gewiss vorkommt, wenn $-D \,\mathrm{R}\, \frac{M}{\mu\mu}$ gilt, so müssen sie für den vorliegenden Zweck ganz unberücksichtigt bleiben, obwohl sie in anderer Hinsicht nützlich sein können.

II. Unter sonst gleichen Umständen ist die Arbeit offenbar umso leichter, je kleiner die Anzahl der Klassen f, f', f'' usw. ist, und daher am kürzesten, wenn D eine der 65 in Artikel 303 angegebenen Zahlen ist, für die jedes Geschlecht nur eine einzige Klasse enthält.

III. Da je zwei solche Darstellungen $x = m, y = n$ und $x = -m, y = -n$ stets zu demselben Wert gehören, genügt es offenbar, nur diejenigen Darstellungen zu betrachten, in denen y positiv ist. Verschiedene Darstellungen *dieser Art* entsprechen daher stets verschiedenen Werten des Ausdrucks $\sqrt{-D}$ (mod. M), sodass die Anzahl sämtlicher verschiedener Werte der Anzahl aller sich ergebenden Darstellungen dieser Art gleich ist, stets mit Ausnahme des Falles $D = 1$, in dem die erstere Anzahl die Hälfte der letzteren ist.

IV. Da mit dem einen der beiden entgegengesetzten Werte $+r, -r$ auch der andere unmittelbar bekannt ist, lassen sich die Operationen noch etwas verkürzen. Ergibt sich der Wert r aus einer Darstellung der Zahl M durch eine Form in der Klasse C, *d. h.* gilt $\mathfrak{C} = C$, so entsteht der entgegengesetzte Wert $-r$ offenbar aus einer Darstellung durch eine Form in der zu C entgegengesetzten Klasse. Diese unterscheidet sich von der Klasse C, sofern letztere nicht ambig ist. Sind also nicht sämtliche Klassen in G ambig, so braucht man von den übrigen nur die Hälfte zu betrachten, nämlich je eine aus jedem entgegengesetzten Paar. Die andere kann unberücksichtigt bleiben, da man schon ohne Rechnung voraussieht, dass sich aus ihr die entgegengesetzten Werte zu denen der ersteren ergeben. Ist dagegen C ambig, so entstehen daraus die beiden Werte r und $-r$ zugleich. Wurde nämlich aus C die ambige Form $axx + 2bxy + cyy$ gewählt und ergab sich der Wert r aus der Darstellung $x = m, y = n$, so ergibt sich der Wert $-r$ aus $x = -m - \frac{2bn}{a},\ y = n$.

V. Im Fall $D = 1$ gibt es insgesamt nur eine Klasse, aus der, wie wir annehmen dürfen, die Form $xx + yy$ gewählt worden sei. Ergibt sich der Wert r aus der Darstellung $x = m, y = n$, so ergibt sich derselbe aus $x = -m, y = -n;\ x = n, y = -m;$ $x = -n, y = m$ und der entgegengesetzte Wert $-r$ aus $x = m, y = -n; x = -m,$ $y = n;\ x = n, y = m;\ x = -n, y = -m$. Daher genügt von diesen acht Darstellungen, die eine einzige Zerlegung bilden, eine, wenn wir nur dem daraus erhaltenen Wert seinen entgegengesetzten zuordnen.

VI. Der Wert des Ausdrucks $\sqrt{-D}$ (mod. M), zu dem die Darstellung $M = amm + 2bmn + cnn$ gehört, ist nach Artikel 155 gleich $\mu(mb + nc) - \nu(ma + nb)$ oder einer beliebigen hierzu nach M kongruenten Zahl, wobei μ, ν so gewählt sind, dass $\mu m + \nu n = 1$ gilt. Bezeichnen wir einen solchen Wert mit v, so gilt

$$\begin{aligned} mv &\equiv \mu m(mb + nc) - \nu(M - mnb - nnc) \\ &\equiv (\mu m + \nu n)(mb + nc) \equiv mb + nc \text{ (mod. } M) \end{aligned}$$

Somit ist v ein Wert des Ausdrucks $\frac{mb+nc}{m}$ (mod. M); ebenso findet man, dass v ein Wert des Ausdrucks $-\frac{ma+nb}{n}$ (mod. M) ist. Diese Formeln sind häufig derjenigen vorzuziehen, aus der sie abgeleitet wurden.

328.

Beispiele. I. Gesucht sind sämtliche Werte des Ausdrucks $\sqrt{-1365}$ (mod. $5428681 = M$). Die Zahl M ist hier $\equiv 1, 1, 1, 6, 11$ (mod. $4, 3, 5, 7, 13$) und somit unter einer Form der Teiler von $xx + 1,\ xx + 3,\ xx - 5$ sowie unter einer Form der Nichtteiler von $xx + 7,\ xx - 13$, also unter einer Form der Teiler von $xx + 1365$ enthalten. Der Charakter des Geschlechts, in dem sich die Klassen $\mathfrak{G}$ befinden, ist daher $1, 4;\ R3;\ R5;\ N7;\ N13$. Dieses Geschlecht enthält nur eine Klasse, aus der wir die Form $6xx + 6xy + 229yy$ wählen. Um sämtliche Darstellungen der Zahl M durch diese zu finden, setzen wir $2x + y = x'$, woraus $3x'x' + 455yy = 2M$ folgen muss. Diese Gleichung besitzt vier Lösungen, in denen y positiv ist, nämlich $y = 127,\ x' = \pm 1083,\ y = 119,\ x' = \pm 1213$. Daraus ergeben sich vier Lösungen der Gleichung $6xx + 6xy + 229yy = M$, in denen y positiv ist:

x	478	−605	547	−666
y	127	127	119	119

Die erste Lösung liefert für v den Wert des Ausdrucks $\frac{30517}{478}$ oder $-\frac{3249}{127}$ (mod. M), woraus man 2350978 erhält; die zweite liefert den entgegengesetzten Wert -2350978, die dritte 2600262 und die vierte den entgegengesetzten Wert -2600262.

II. Sollen die Werte des Ausdrucks $\sqrt{-286}$ (mod. $4272943 = M$) gefunden werden, so ergibt sich als Charakter des Geschlechts, in dem die Klassen $\mathfrak{G}$ enthalten sind, 1 und $7, 8$; $R11$; $R13$. Es ist somit das Hauptgeschlecht, das drei Klassen enthält, dargestellt durch die Formen $(1, 0, 286)$, $(14, 6, 23)$, $(14, -6, 23)$. Die dritte darf man als der zweiten entgegengesetzt unberücksichtigt lassen. Durch die Form $xx + 286yy$ findet man zwei Darstellungen der Zahl M, in denen y positiv ist, nämlich $y = 103$, $x = \pm 1113$, woraus sich die Werte 1493445, -1493445 des gegebenen Ausdrucks ergeben. Durch die Form $(14, 6, 23)$ ist aber M nicht darstellbar; daraus folgt, dass es außer den beiden gefundenen keine weiteren Werte gibt.

III. Ist der Ausdruck $\sqrt{-70}$ (mod. 997331) gegeben, so müssen die Klassen $\mathfrak{G}$ in dem Geschlecht liegen, dessen Charakter 3 und $5, 8$; $R5$; $N7$ ist. Dieses enthält nur eine Klasse, deren darstellende Form $(5, 0, 14)$ ist. Führt man jedoch die Rechnung aus, so findet man, dass die Zahl 997331 durch die Form $(5, 0, 14)$ nicht darstellbar ist; daher muss -70 ein quadratischer Nichtrest jener Zahl sein.

Zwei Verfahren zur Unterscheidung von zusammengesetzten Zahlen und Primzahlen und zur Ermittlung der Faktoren der ersteren.

329.

Dass die Aufgabe, Primzahlen von zusammengesetzten Zahlen zu unterscheiden und die letzteren in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und den Fleiß und Scharfsinn der Mathematiker sowohl der älteren als auch der neueren Zeit beschäftigt hat, ist so bekannt, dass es überflüssig wäre, ausführlich darüber zu sprechen. Dennoch müssen wir zugeben, dass sämtliche bisher vorgeschlagenen Verfahren entweder auf sehr besondere Fälle beschränkt oder so mühsam und langwierig sind, dass sie schon bei Zahlen innerhalb der Grenzen der von verdienstvollen Männern aufgestellten Tafeln, also bei Zahlen, für die aufwendige Verfahren überflüssig sind, selbst die Geduld eines geübten Rechners erschöpfen; auf größere Zahlen lassen sie sich meist kaum anwenden. Jene allgemein verfügbaren Tafeln, von denen wir hoffen dürfen, dass sie nach und nach weiter fortgesetzt werden, reichen zwar in den meisten gewöhnlichen Fällen gewiss aus. Dennoch bietet sich einem erfahrenen Rechner nicht selten Gelegenheit, aus der Zerlegung großer Zahlen in Faktoren erhebliche Vorteile zu ziehen, die einen mäßigen Zeitaufwand reichlich aufwiegen. Außerdem scheint es die Würde der Wissenschaft zu verlangen, sämtliche Hilfsmittel zur Lösung eines so eleganten und berühmten Problems sorgfältig weiterzuentwickeln. Aus diesen Gründen zweifeln wir nicht, dass die beiden folgenden Verfahren, deren Wirksamkeit und Kürze wir aus langer Erfahrung bestätigen können, den Liebhabern der Arithmetik willkommen sein werden. Im Übrigen liegt es in der Natur der Aufgabe, dass *jedes* Verfahren zunehmend aufwendiger wird, je größer die Zahlen sind, auf die es angewandt wird. Bei den folgenden Verfahren wachsen die Schwierigkeiten jedoch sehr langsam; Zahlen mit sieben, acht oder sogar noch mehr Ziffern sind besonders durch das zweite stets mit Erfolg behandelt worden, und zwar mit der ganzen Geschwindigkeit, die man bei so großen Zahlen vernünftigerweise erwarten darf. Nach sämtlichen bisher bekannten Verfahren würden sie eine Arbeit verlangen, die selbst einem unermüdlichen Rechner unerträglich wäre.

Bevor man die folgenden Verfahren verwendet, ist es stets sehr nützlich, die Division der gegebenen Zahl durch einige der kleinsten Primzahlen zu versuchen, etwa durch $2, 3, 5, 7$ usw. bis 19 oder noch weiter. So vermeidet man nicht nur, es zu bereuen, einen solchen Teiler durch schwierige und aufwendige Verfahren gefunden zu haben, obwohl er sich durch bloße Division viel leichter hätte finden lassen[*)]; auch kann das zweite Verfahren, wenn keine dieser Divisionen gelingt, die dabei entstehenden *Reste* mit großem Nutzen verwenden. Ist zum Beispiel die Zahl 314159265 in ihre Faktoren zu zerlegen, so gelingt die Division durch 3 zweimal, danach auch die Division durch 5 und 7, sodass man $314159265 = 9.5.7.997331$ erhält. Daher genügt es, die Zahl 997331, die durch $11, 13, 17, 19$ nicht teilbar ist, genauer zu untersuchen. Ebenso werden wir bei der gegebenen Zahl 43429448 den Faktor 8 abtrennen und die aufwendigeren Verfahren auf den Quotienten 5428681 anwenden.

[*)] Umso mehr, als sich im Allgemeinen unter sechs Zahlen kaum eine findet, die durch keine der Zahlen $2, 3, 5 \ldots 19$ teilbar ist.

330.

Das ERSTE VERFAHREN beruht auf dem Satz, dass *jede positive oder negative Zahl, die quadratischer Rest einer anderen Zahl M ist, auch ein Rest jedes Teilers von M ist.* Bekanntlich ist, wenn M durch keine Primzahl unterhalb $\sqrt{M}$ teilbar ist, M gewiss eine Primzahl. Sind aber sämtliche Primzahlen unterhalb dieser Grenze, die M teilen, gleich p, q usw., so besteht M entweder aus diesen *allein* oder ihren Potenzen oder kann nur *einen* weiteren Primfaktor größer als $\sqrt{M}$ enthalten. Diesen findet man, indem man M durch p, q usw. so oft wie möglich dividiert. Bezeichnen wir die Gesamtheit aller Primzahlen unterhalb $\sqrt{M}$, mit Ausnahme derjenigen, durch die eine Division bereits erfolglos versucht worden ist, mit Ω, so genügt es offenbar, sämtliche Primteiler von M, die in Ω enthalten sind, zu finden. Weiß man nun auf irgendeinem Weg, dass eine Zahl r, die kein Quadrat ist, quadratischer Rest von M ist, so kann keine Primzahl, für die r ein $NR.$ ist, ein Teiler von M sein. Daher darf man aus Ω sämtliche solchen Primzahlen entfernen, die meist ungefähr die Hälfte aller ausmachen. Weiß man außerdem von einer weiteren Zahl, die kein Quadrat ist, r', dass sie ein Rest von M ist, so kann man unter den nach dem ersten Ausschluss in Ω verbleibenden Primzahlen wiederum diejenigen ausschließen, für die r' ein $NR.$ ist. Diese machen wiederum ungefähr die Hälfte aus, sofern die Reste r und r' unabhängig sind, *d. h.* sofern nicht der eine von selbst notwendig Rest sämtlicher Zahlen ist, von denen der andere Rest ist; dies wäre der Fall, wenn rr' ein Quadrat wäre. Sind noch weitere Reste von M bekannt, r'', r''' usw., die alle von den übrigen unabhängig sind[*)], so lassen sich mit jedem ähnliche Ausschlüsse vornehmen. Dadurch nimmt die Menge der Zahlen in Ω sehr rasch ab, sodass bald entweder alle entfernt sind, in welchem Fall M gewiss eine Primzahl ist, oder nur so wenige übrig bleiben, darunter offenbar sämtliche Primteiler von M, falls es solche gibt, dass die Division durch sie ohne Mühe versucht werden kann. Bei einer Zahl, die eine Million nicht wesentlich übersteigt, genügen meist sechs oder sieben Ausschlüsse reichlich; bei einer Zahl mit acht oder neun Ziffern neun oder zehn. Über zwei Punkte müssen wir nun noch sprechen: *erstens*, wie sich geeignete und genügend viele Reste von M finden lassen, und *zweitens*, wie man den Ausschluss selbst am bequemsten ausführt. Wir werden jedoch die Reihenfolge dieser Fragen umkehren, zumal die zweite zeigen wird, welche Reste sich für diesen Zweck besonders eignen.

[*)] Ist das Produkt beliebig vieler der Zahlen r, r', r'' usw. ein Quadrat, so ist jede von ihnen, etwa r, Rest jeder Primzahl, die keine dieser Zahlen teilt und die Rest der übrigen Zahlen r', r'' usw. ist. Damit also beliebig viele Reste als unabhängig betrachtet werden können, darf kein Produkt aus zweien, dreien usw. ein Quadrat sein.

331.

In Abschnitt IV haben wir ausführlich gezeigt, wie man die Primzahlen, deren Rest eine gegebene Zahl r ist (die wir als durch kein Quadrat teilbar voraussetzen dürfen), von denen unterscheidet, deren Nichtrest sie ist, oder die Teiler des Ausdrucks $xx - r$ von den Nichtteilern: Alle ersteren sind unter gewissen Formeln der Art $rz + a,\ rz + b$ usw. oder der Art $4rz + a,\ 4rz + b$ usw. enthalten, die letzteren unter anderen ähnlichen Formeln. Wenn r eine sehr kleine Zahl ist, lassen sich die Ausschlüsse mithilfe dieser Formeln sehr bequem durchführen; zum Beispiel sind alle Zahlen der Form $4z + 3$ auszuschließen, wenn $r = -1$ gilt; alle Zahlen der Formen $8z+3$ und $8z+5$, wenn $z = 2$ gilt, usw. Doch können wir nicht immer solche Reste der vorgelegten Zahl M finden, und für einen großen Wert von r ist die Anwendung der Formeln nicht bequem genug. Es ist daher ein gewaltiger Vorteil und erleichtert die Ausschlussarbeit außerordentlich, wenn für eine hinreichend große Menge positiver und negativer, durch kein Quadrat teilbarer Zahlen (r) bereits eine *Tafel* vorliegt, in der die Primzahlen, deren Reste die einzelnen (r) sind, von denen unterschieden werden, deren Nichtreste sie sind. Eine solche Tafel lässt sich ebenso einrichten wie die diesem Werk am Ende beigefügte und oben schon beschriebene Probe; damit sie aber für den gegenwärtigen Zweck hinreichend großen Nutzen bietet, müssen die am Rand stehenden Primzahlen (die Moduln) viel weiter, etwa mindestens bis 1000 oder 10000, fortgesetzt werden. Außerdem wird die Anwendung erheblich bequemer, wenn unter den Überschriften auch zusammengesetzte und negative Zahlen aufgenommen werden, obwohl dies, wie Abschnitt IV zeigt, nicht unbedingt nötig ist. Am bequemsten wird der Gebrauch einer solchen Tafel, wenn man ihre einzelnen senkrechten Spalten ausschneidet und auf Streifen oder Stäbe (ähnlich den Neperschen) klebt, sodass die jeweils benötigten, nämlich diejenigen zu den Zahlen r, r', r'' usw., den Resten der vorgelegten, in Faktoren zu zerlegenden Zahl, einzeln untersucht werden können. Legt man sie *richtig* neben die erste Spalte der Tafel (welche die Moduln enthält), das heißt so, dass die Stellen der einzelnen Stäbe, die derselben Primzahl der ersten Spalte entsprechen, mit ihr in gerader Richtung oder auf derselben waagerechten Linie liegen, so erkennt man offenbar auf einen Blick die Primzahlen, die nach den Ausschlüssen mit den Resten r, r', r'' in Ω übrig bleiben: Es sind gerade diejenigen Zahlen der ersten Spalte, neben denen sich auf *allen* benachbarten Stäben ein Strich befindet; alle Zahlen, neben denen auf *irgendeinem* Stab eine leere Stelle liegt, sind zu verwerfen. Ein Beispiel wird dies hinreichend verdeutlichen. Weiß man auf irgendeine Weise, dass die Zahlen $-6, +13, -14, +17, +37, -53$ Reste von 997331 sind, so sind die erste Spalte (die in diesem Fall bis 997, der Primzahl unmittelbar unter $\sqrt{997331}$, reichen muss) und die Streifen mit den Überschriften $-6, +13$ usw.

zusammenzulegen. Hier ist ein Teil des so entstehenden Schemas:

	-6	$+13$	-14	$+17$	$+37$	-53
3	–	–	–		–	–
5	–		–			
7	–		–		–	
11	–				–	
13		–	–	–		–
17		–		–		–
19			–	–		–
23		–	–			–
			usw.			
113		–	–			–
127	–	–	–	–	–	–
131	–	–	–			
			usw.			

Wie man hier auf einen Blick erkennt, dass von den Primzahlen, *die in diesem Teil des Schemas enthalten sind*, allein 127 nach den Ausschlüssen mit den Resten $-6, 13$ usw. in Ω übrig bleibt, so zeigt das vollständige, bis 997 fortgesetzte Schema, dass *überhaupt* keine andere in Ω übrig bleibt; versucht man die Division, so findet man, dass 997331 tatsächlich durch 127 teilbar ist. Auf diese Weise ist jene Zahl also in die Primfaktoren 127×7853 zerlegt[*)].

Aus dieser Darstellung geht außerdem hinreichend hervor, dass Reste, die nicht zu groß sind oder sich wenigstens in nicht zu große Primfaktoren zerlegen lassen, besonders nützlich sind: Der unmittelbare Gebrauch der Hilfstafel reicht nicht über die Zahlen in ihren Überschriften hinaus, und der mittelbare umfasst nur solche, die sich in Faktoren zerlegen lassen, welche in der Tafel enthalten sind.

332.

Wir werden drei verschiedene Verfahren angeben, um Reste einer gegebenen Zahl M zu finden. Ihrer Darstellung schicken wir zwei Beobachtungen voraus, mit deren Hilfe man aus weniger geeigneten Resten einfachere ableiten kann. *Erstens*: Ist eine Zahl akk, die durch das Quadrat kk teilbar ist (das als zu M teilerfremd vorausgesetzt wird), ein Rest von M, so ist auch a ein Rest; deshalb sind Reste, die durch große Quadrate teilbar sind, ebenso nützlich wie kleine, und wir werden voraussetzen, dass aus allen Resten, welche die folgenden Verfahren liefern, die quadratischen Faktoren sofort entfernt worden sind. *Zweitens*: Sind zwei oder mehr Zahlen Reste, so ist auch ihr Produkt ein Rest. Verbindet man diese Beobachtung mit der vorigen, so lässt sich sehr häufig aus mehreren Resten, die nicht alle einfach genug sind, ein anderer

[*)] Der Autor würde den recht umfangreichen Apparat der hier beschriebenen Tafel, den er für seinen eigenen Gebrauch anfertigen ließ, gern veröffentlichen, wenn die geringe Zahl derer, denen er nützlich sein kann, zur Deckung der Kosten eines solchen Unternehmens ausreichte. Möchte sich inzwischen ein Freund der Arithmetik, nachdem er die Grundsätze gründlich verstanden hat, aus eigener Kraft eine solche Tafel anlegen, so wird es dem Autor große Freude machen, ihm alle Hilfsmittel und Kunstgriffe brieflich mitzuteilen.

sehr einfacher ableiten, sofern jene viele gemeinsame Faktoren enthalten. Aus diesem Grund sind auch solche Reste sehr geeignet, die aus vielen nicht zu großen Faktoren bestehen, und es wird zweckmäßig sein, sie alle sofort in ihre Faktoren zu zerlegen. Die Bedeutung dieser Beobachtungen wird durch Beispiele und häufigen Gebrauch besser verständlich als durch Regeln.

I. Das einfachste und für diejenigen, die durch häufige Übung schon einige Gewandtheit erworben haben, bequemste Verfahren besteht darin, M oder allgemeiner irgendein Vielfaches von M auf beliebige Weise in zwei Teile $kM = a + b$ zu zerlegen (seien beide positiv oder einer positiv und der andere negativ). Ihr Produkt mit umgekehrtem Vorzeichen ist dann ein Rest von M; denn es ist $-ab \equiv aa \equiv bb \pmod{M}$ und daher $-ab \,R\, M$. Die Zahlen a, b sind so zu wählen, dass ihr Produkt durch ein großes Quadrat teilbar und der Quotient entweder klein oder wenigstens in nicht zu große Faktoren zerlegbar ist; dies lässt sich immer ohne Schwierigkeit erreichen. Besonders empfiehlt es sich, für a ein Quadrat oder das Doppelte oder Dreifache eines Quadrats usw. zu nehmen, das von der Zahl M um eine entweder kleine oder in bequeme Faktoren zerlegbare Zahl abweicht. So findet man zum Beispiel

$$\begin{aligned} 997331 &= 999^2 - 2.5.67 \\ &= 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2 \\ &= 3.575^2 + 11.31.4^2 = 3.577^2 - 7.13.4^2 \\ &= 3.578^2 - 7.19.37 = 11.299^2 + 2.3.5.29.4^2 \\ &= 11.301^2 + 5.12^2 \end{aligned}$$

usw. Daraus erhält man die folgenden Reste: $2.5.67$, -5.11, $-2.3.17$, $-3.11.31$, $3.7.13$, $3.7.19.37, -2.3.5.11.29$; die letzte Zerlegung liefert den Rest -5.11, den wir schon haben. Anstelle der Reste $-3.11.31$, $-2.3.5.11.29$ können wir $3.5.31$, $2.3.29$ nehmen, die aus ihrer Verbindung mit -5.11 entstehen.

II. Das zweite und dritte Verfahren beruhen darauf, dass, wenn zwei binäre Formen (A, B, C), (A', B', C') derselben Determinante M oder $-M$ oder allgemeiner $\pm kM$ zum selben Geschlecht gehören, die Zahlen AA', AC', $A'C$ Reste von kM sind. Dies erkennt man ohne Mühe daran, dass jede charakteristische Zahl der einen Form, etwa m, auch eine charakteristische Zahl der anderen ist und somit mA, mC, mA', mC' sämtlich Reste von kM sind. Ist also (a, b, a') eine reduzierte Form mit positiver Determinante M oder allgemeiner kM, und sind (a', b', a''), (a'', b'', a''') usw. Formen aus ihrer Periode, also ihr äquivalent und erst recht im selben Geschlecht enthalten, so sind die Zahlen aa', aa'', aa''' usw. sämtlich Reste von M. Eine große Anzahl von Formen einer solchen Periode lässt sich mithilfe des Algorithmus aus Artikel 187 sehr leicht berechnen; die einfachsten Reste ergeben sich meistens, wenn man $a = 1$ setzt; diejenigen, die zu große Faktoren enthalten, sind zu verwerfen. Hier sind die Anfänge der Perioden der Formen $(1, 998, -1327)$ und $(1, 1412, -918)$, deren Determinanten 997331, 1994662 sind:

$(1, \ 998, \ -1327)$	$(1, \ 1412, \ -918)$
$(-1327, \ 329, \ 670)$	$(-918, \ 1342, \ 211)$
$(670, \ 341, \ -1315)$	$(211, \ 1401, \ -151)$
$(-1315, \ 974, \ 37)$	$(-151, \ 1317, \ 1723)$
$(37, \ 987, \ -626)$	$(1723, \ 406, \ -1062)$
$(-626, \ 891, \ 325)$	$(-1062, \ 656, \ 1473)$
$(325, \ 734, \ -1411)$	$(1473, \ 817, \ -901)$
$(-1411, \ 677, \ 382)$	$(-901, \ 985, \ 1137)$
$(382, \ 851, \ -715)$	usw.

Es sind also Reste der Zahl 997331 sämtliche Zahlen $-1327, 670$ usw.; lässt man diejenigen mit zu großen Faktoren beiseite, so erhält man die folgenden: $2.5.67$, 37, $13, -17.83$, $-5.11.13$, $-2.3.17$, -2.59, -17.53. Den Rest $2.5.67$ sowie -5.11, der aus der Verbindung des dritten mit dem fünften entsteht, hatten wir schon oben gefunden.

III. Ist C irgendeine von der Hauptklasse verschiedene Klasse von Formen mit negativer Determinante $-M$ oder allgemeiner $-kM$ und ihre Periode $2C$, $3C$ usw. (Artikel 307), so gehören die Klassen $2C$, $4C$ usw. zum Hauptgeschlecht, dagegen $3C$, $5C$ usw. zum selben Geschlecht wie C. Ist also (a, b, c) eine (einfachste) Form aus C und (a', b', c') eine Form aus irgendeiner Klasse jener Periode, etwa aus nC, so ist entweder a' oder aa' ein Rest von M, je nachdem, ob n gerade oder ungerade ist (im ersten Fall offenbar auch c', im zweiten ac', ca' und cc'). Die Periode, das heißt die einfachsten Formen in ihren Klassen, lässt sich mit erstaunlicher Leichtigkeit entwickeln, wenn a sehr klein ist, insbesondere im Fall $= 3$, was sich immer erreichen lässt, wenn $kM \equiv 2 \pmod 3$ gilt. Hier ist der Anfang der Periode der Klasse, welche die Form $(3, 1, 332444)$ enthält:

C	$(3, \ 1, \ 332444)$	$6C$	$(729. \ -209, \ 1428)$
$2C$	$(9, \ -2, \ 110815)$	$7C$	$(476, \ 209, \ 2187)$
$3C$	$(27, \ 7, \ 36940)$	$8C$	$(1027, \ 342, \ 1085)$
$4C$	$(81, \ 34, \ 12327)$	$9C$	$(932, \ -437, \ 1275)$
$5C$	$(243, \ 34, \ 4109)$	$10C$	$(425, \ 12, \ 2347)$

Daraus gehen die Reste (unter Verwerfung der unbrauchbaren) 3.476, 1027, 1085, 425 hervor, oder (nach Entfernung der quadratischen Faktoren) 3.7.17, 13.79, 5.7.31, 17. Verbindet man diese passend mit den acht in II gefundenen Resten, so erhält man leicht die folgenden zwölf: -2.3, 13, $-2.7, 17$, 37, -53, -5.11, 79, -83, -2.59, $-2.5.31$, $2.5.67$; die ersten sechs sind dieselben, die wir in Artikel 331 verwendet haben. Die Reste 19 und -29 hätten hinzugefügt werden können, wenn wir auch die in I gefundenen hätten verwenden wollen; die übrigen dort erhaltenen hängen bereits von denen ab, die wir hier entwickelt haben.

333.

Das ZWEITE VERFAHREN, eine gegebene Zahl M in Faktoren zu zerlegen, geht von der Betrachtung der Werte eines Ausdrucks wie $\sqrt{-D}$ (mod. M) aus und stützt sich auf die folgenden Beobachtungen.

I. Ist M eine Primzahl oder eine Potenz einer Primzahl (wobei die Primzahl ungerade ist und D nicht teilt), so ist $-D$ ein Rest oder Nichtrest von M, je nachdem, ob M unter einer Form der Teiler oder einer Form der Nichtteiler von $xx + D$ enthalten ist; im ersten Fall hat der Ausdruck $\sqrt{-D}$ (mod. M) nur zwei verschiedene Werte, die entgegengesetzt sind.

II. Ist dagegen M zusammengesetzt, etwa $= pp'p''$ usw., wobei p, p', p'' usw. Primzahlen (verschiedene, ungerade, die D nicht teilen) oder Potenzen solcher Primzahlen bezeichnen, so ist $-D$ nur dann ein Rest von M, wenn es ein Rest der einzelnen p, p', p'' usw. ist, das heißt, wenn diese Zahlen alle unter Formen der Teiler von $xx + D$ enthalten sind. Bezeichnet man die Werte des Ausdrucks $\sqrt{-D}$ nach den Moduln p, p', p'' usw. jeweils mit $\pm r$, $\pm r'$, $\pm r''$ usw., so entstehen sämtliche Werte desselben Ausdrucks nach dem Modul M, indem man die Zahlen ermittelt, die nach p entweder $\equiv r$ oder $\equiv -r$, nach p' entweder $\equiv r'$ oder $\equiv -r'$ usw. sind. Ihre Anzahl ist daher $= 2^\mu$, wobei μ die Anzahl der Zahlen p, p', p'' usw. bezeichnet. Sind diese Werte also $R, -R, R', -R', R''$ usw., so gilt von selbst $R \equiv R$ nach allen p, p', p'' usw., aber nach keiner von ihnen $R \equiv -R$. Daher ist der größte gemeinsame Teiler von M und $R - R$ gleich M, und 1 ist der größte gemeinsame Teiler von M und $R + R$. Zwei Werte aber, die weder identisch noch entgegengesetzt sind, wie R und R', müssen nach einer oder mehreren der Zahlen p, p', p'' usw., jedoch nicht nach allen, kongruent sein, und nach den übrigen gilt $R \equiv -R'$; folglich ist das Produkt der ersteren der größte gemeinsame Teiler von M und $R - R'$ und das Produkt der letzteren der größte gemeinsame Teiler von M und $R + R'$. Daraus folgt leicht: Berechnet man alle größten gemeinsamen Teiler von M und den Differenzen zwischen den einzelnen Werten des Ausdrucks $\sqrt{-D}$ (mod. M) und einem beliebig gegebenen Wert, so enthält ihre Menge die Zahlen $1, p, p', p''$ usw. und alle Produkte aus je zweien, dreien usw. dieser Zahlen. *Auf diese Weise lassen sich also aus den Werten jenes Ausdrucks die Zahlen p, p', p'' usw. ermitteln.*

Da ferner das Verfahren aus Artikel 327 die einzelnen Werte auf die Werte von Ausdrücken der Form $\frac{m}{n}$ (mod. M) zurückführt, wobei der Nenner n zu M teilerfremd ist, brauchen diese Ausdrücke selbst für den gegenwärtigen Zweck nicht einmal berechnet zu werden. Denn der größte gemeinsame Teiler von M und der Differenz zwischen R und R', die mit $\frac{m}{n}$, $\frac{m'}{n'}$ übereinstimmen, ist offenbar auch der größte gemeinsame

Teiler von M und $nn'(R - R')$. Oder, was dasselbe ist, von M und $mn' - m'n$, zu dem $nn'(R - R')$ nach dem Modul M kongruent ist.

334.

Die vorstehenden Beobachtungen lassen sich auf unser Problem auf zwei Arten anwenden. Die erste entscheidet nicht nur, ob die vorgelegte Zahl M eine Primzahl oder zusammengesetzt ist, sondern liefert im letzteren Fall auch die Faktoren selbst; die zweite hat den Vorteil, dass sie meist eine raschere Rechnung ermöglicht, liefert aber manchmal die Faktoren der zusammengesetzten Zahlen, die auch sie vollständig von den Primzahlen unterscheidet, erst nach mehrmaliger Wiederholung.

I. Man suche eine negative Zahl $-D$, die ein quadratischer Rest von M ist; dazu können die in Artikel 332 unter I und II angegebenen Verfahren dienen. An sich ist die Wahl des Restes beliebig, und anders als beim vorigen Verfahren braucht D hier keine kleine Zahl zu sein; doch wird die Rechnung umso kürzer, je kleiner die Anzahl der Klassen binärer Formen in den einzelnen eigentlich primitiven Geschlechtern mit der Determinante $-D$ ist. Deshalb sind besonders solche Reste geeignet, die unter den 65 Zahlen aus Artikel 303 enthalten sind, falls sich solche anbieten. So wäre für $M = 997331$ von allen oben gefundenen negativen Resten -102 am besten geeignet. Man ermittle alle verschiedenen Werte des Ausdrucks $\sqrt{-D}$ (mod. M); ergeben sich nur zwei (entgegengesetzte), so ist M sicher eine Primzahl oder eine Potenz einer Primzahl; sind es mehr, etwa 2^μ, so ist M aus μ verschiedenen Primzahlen oder Potenzen von Primzahlen zusammengesetzt, die man als Faktoren mit dem Verfahren des vorigen Artikels ermitteln kann. Ob diese Faktoren Primzahlen oder Potenzen von Primzahlen sind, lässt sich an sich sehr leicht erkennen; außerdem zeigt schon das Verfahren, durch das man die Werte des Ausdrucks $\sqrt{-D}$ findet, von selbst alle Primzahlen an, von denen irgendeine Potenz M teilt. Ist nämlich M durch das Quadrat einer Primzahl π teilbar, so hat jene Rechnung sicher auch eine oder mehrere Darstellungen der Zahl M, $M = amm + 2bmn + cnn$, geliefert, in denen der größte gemeinsame Teiler der Zahlen m, n gleich π ist (und zwar deshalb, weil in diesem Fall $-D$ auch ein Rest von $\frac{M}{\pi\pi}$ ist). Ist dagegen keine Darstellung entstanden, in der m und n einen gemeinsamen Teiler haben, so ist dies ein sicheres Zeichen dafür, dass M durch kein Quadrat teilbar ist und daher alle p, p', p'' usw. Primzahlen sind.

Beispiel. Mit dem oben angegebenen Verfahren findet man vier Werte des Ausdrucks $\sqrt{-408}$ (mod. 997331), die mit den Werten von $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$ übereinstimmen; die größten gemeinsamen Teiler von 997331 mit $3.1664 - 113.2824$ und $3.1664 + 113.2824$, also mit 314120 und 324104, sind 7853 und 127, woraus wie oben $997331 = 127.7853$ folgt.

II. Man nehme irgendeine negative Zahl $-D$, sodass M unter einer Form der Teiler von $xx + D$ enthalten ist. An sich ist die Wahl einer solchen Zahl beliebig; der Bequemlichkeit halber ist aber vor allem darauf zu achten, dass die Anzahl der Klassen in den Geschlechtern mit der Determinante $-D$ möglichst klein ist. Eine solche Zahl zu finden, bereitet übrigens keine Schwierigkeit, wenn man durch Probieren vorgeht; denn gewöhnlich ist unter einer beträchtlichen Menge versuchter Zahlen M für ungefähr ebenso viele unter einer Form der Teiler wie unter einer Form der Nichtteiler enthalten. Es wird daher am zweckmäßigsten sein, den Versuch mit den 65 Zahlen aus

Artikel 303 (und zwar mit den größten) zu beginnen und, falls sich keine als geeignet erweisen sollte (was jedoch im Allgemeinen nur einmal unter 16384 Fällen eintritt), zu anderen überzugehen, bei denen die einzelnen Geschlechter je zwei Klassen enthalten. — Dann ermittle man die Werte des Ausdrucks $\sqrt{-D}$ (mod. M) und leite, wenn sich welche finden, daraus die Faktoren von M auf genau dieselbe Weise wie oben ab; ergeben sich dagegen keine Werte, sodass $-D$ ein Nichtrest von M ist, so kann M sicher weder eine Primzahl noch eine Potenz einer Primzahl sein. Wünscht man in diesem Fall die Faktoren selbst, so muss man entweder dieselbe Operation mit anderen Werten für D wiederholen oder zu einem anderen Verfahren greifen.

So findet man zum Beispiel durch Probieren, dass 997331 unter einer Form der Nichtteiler von $xx + 1848$, $xx + 1365$, $xx + 1320$, aber unter einer Form der Teiler von $xx + 840$ enthalten ist; für die Werte des Ausdrucks $\sqrt{-840}$ (mod. 997331) erhält man die Ausdrücke $\pm\frac{1272}{163}, \pm\frac{3288}{125}$, aus denen dieselben Faktoren wie zuvor folgen. — Wer weitere Beispiele wünscht, möge Artikel 328 heranziehen: Das erste zeigt, dass $5428681 = 307.17683$ gilt; das zweite, dass 4272943 eine Primzahl ist; das dritte, dass 997331 sicher aus mehreren Primzahlen zusammengesetzt ist.

* *
*

Der Umfang dieses Werkes hat uns hier nur erlaubt, die Hauptpunkte der beiden Verfahren zur Ermittlung der Faktoren auszuführen; eine eingehendere Untersuchung zusammen mit weiteren Hilfstafeln und anderen Hilfsmitteln behalten wir uns für eine andere Gelegenheit vor.

SIEBENTER ABSCHNITT

ÜBER

DIE GLEICHUNGEN, WELCHE DIE KREISTEILUNGEN BESTIMMEN.

335.

Unter den glänzendsten Fortschritten, welche die Mathematik durch die Arbeiten neuerer Mathematiker erfahren hat, nimmt die Theorie der vom Kreis abhängigen Funktionen zweifellos einen besonders hervorragenden Platz ein. Die größten Mathematiker neuerer Zeit haben dieser wunderbaren Art von Größen, zu der wir bei den verschiedenartigsten Untersuchungen so häufig gelangen und deren Hilfe kein Teil der gesamten Mathematik entbehren kann, ihren Fleiß und Scharfsinn so beharrlich gewidmet und daraus ein so weitreichendes Gebiet geschaffen, dass man kaum hätte erwarten können, irgendein Teil dieser Theorie, geschweige denn ein elementarer und gewissermaßen an ihrer Schwelle liegender, könne noch wesentliche Fortschritte erfahren. Ich spreche von der Theorie der trigonometrischen Funktionen zu den mit dem Umfang kommensurablen Bögen, oder von der Theorie der regelmäßigen Vielecke; dieser Abschnitt wird zeigen, wie wenig davon bisher entwickelt worden ist. Die Leser könnten sich wundern, dass eine solche Untersuchung gerade in diesem Werk angestellt wird, das hauptsächlich einem auf den ersten Blick ganz andersartigen Gegenstand gewidmet ist; doch wird die Behandlung selbst hinreichend deutlich machen, wie eng dieser Gegenstand mit der höheren Arithmetik verbunden ist.

Die Grundsätze der Theorie, deren Darstellung wir beginnen, reichen übrigens viel weiter, als wir sie hier ausdehnen. Sie lassen sich nicht nur auf die Kreisfunktionen, sondern mit gleichem Erfolg auf viele andere transzendente Funktionen anwenden, zum Beispiel auf diejenigen, die vom Integral $\int \frac{dx}{\sqrt{(1-x^4)}}$ abhängen, und außerdem auf verschiedene Arten von Kongruenzen. Da wir aber über jene transzendenten Funktionen ein umfangreiches besonderes Werk vorbereiten und die Kongruenzen in der Fortsetzung der arithmetischen Untersuchungen ausführlich behandelt werden sollen, schien es uns angebracht, hier nur die Kreisfunktionen zu betrachten. Ja, auch diese, die wir in größter Allgemeinheit behandeln könnten, werden wir mit den in den folgenden Artikeln darzulegenden Hilfsmitteln auf den einfachsten Fall zurückführen, sowohl der Kürze wegen als auch, damit die völlig neuen Grundsätze dieser Theorie leichter verstanden werden.

Die Untersuchung wird auf den einfachsten Fall zurückgeführt, in dem die Anzahl der Teile, in welche der Kreis geteilt werden soll, eine Primzahl ist.

336.

Bezeichnet man den Umfang des Kreises oder vier rechte Winkel mit P und setzt voraus, dass m, n ganze Zahlen sind und n das Produkt aus den paarweise teilerfremden Faktoren a, b, c usw. ist, so lässt sich der Winkel $A = \frac{mP}{n}$ nach Artikel 310 auf die Form $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{usw.})P$ bringen; die ihm entsprechenden trigonometrischen Funktionen lassen sich nach bekannten Verfahren aus den Funktionen zu den Teilen $\frac{\alpha P}{a}, \frac{\beta P}{b}$ usw. ableiten. Da man für a, b, c usw. Primzahlen oder Potenzen von Primzahlen nehmen kann, genügt es offenbar, die Teilung des Kreises in Teile zu betrachten, deren Anzahl eine Primzahl oder eine Primzahlpotenz ist; das Vieleck mit n Seiten erhält man dann unmittelbar aus den Vielecken mit a, b, c usw. Seiten. Hier werden wir die Untersuchung jedoch auf den Fall beschränken, in dem die Anzahl der Teile, in welche der Kreis geteilt werden soll, eine (ungerade) Primzahl ist, und zwar vor allem aus folgendem Grund. Bekanntlich lassen sich die Kreisfunktionen zum Winkel $\frac{mP}{pp}$ aus den Funktionen zu $\frac{mP}{p}$ durch Lösung einer Gleichung vom Grad p ableiten, und ebenso aus jenen durch eine Gleichung vom selben Grad die Funktionen zu $\frac{mP}{p^3}$ usw.; ist also das Vieleck mit p Seiten schon gegeben, so erfordert die Bestimmung des Vielecks mit p^λ Seiten notwendig die Lösung von $\lambda - 1$ Gleichungen vom Grad p. Zwar lässt sich die folgende Theorie auch auf diesen Fall ausdehnen, doch gelangt man auf diesem Weg ebenfalls zu ebenso vielen Gleichungen vom Grad p, die sich, wenn p eine Primzahl ist, in keiner Weise auf niedrigere Grade zurückführen lassen. So wird zum Beispiel unten gezeigt, dass sich das Vieleck mit 17 Seiten geometrisch konstruieren lässt; bei der Bestimmung des Vielecks mit 289 Seiten kann man dagegen eine Gleichung vom Grad 17 keinesfalls vermeiden.

Gleichungen für die trigonometrischen Funktionen der Bögen, die ein Teil oder mehrere Teile des ganzen Umfangs sind; Zurückführung der trigonometrischen Funktionen auf die Wurzeln der Gleichung $x^n - 1 = 0$.

337.

Es ist bekannt, dass sich die trigonometrischen Funktionen aller Winkel $\frac{kP}{n}$, wobei k sämtliche Zahlen $0, 1, 2 \ldots n-1$ durchläuft, durch die Wurzeln von Gleichungen vom Grad n ausdrücken lassen: nämlich die *Sinus* durch die Wurzeln von (I)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n.n-3}{1.2}x^{n-4} - \frac{1}{64}\frac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{usw.} \pm \frac{1}{2^{n-1}}nx = 0$$

die *Kosinus* durch die Wurzeln von (II)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n.n-3}{1.2}x^{n-4} - \frac{1}{64}\frac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{usw.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0$$

und schließlich die *Tangenten* durch die Wurzeln von (III)

$$x^n - \frac{n.n-1}{1.2}x^{n-2} + \frac{n.n-1.n-2.n-3}{1.2.3.4}x^{n-4} - \text{usw.} \pm nx = 0$$

Diese Gleichungen (die allgemein für jeden ungeraden Wert von n gelten, II aber auch für gerade Werte) lassen sich durch Setzen von $n = 2m+1$ leicht auf den Grad m zurückführen: I und III, indem man die linke Seite durch x dividiert und y für xx einsetzt. Gleichung II hat offenbar die Wurzel $x = 1$ $(= \cos 0)$, und von den übrigen sind stets je zwei gleich ($\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$ usw.); daher ist ihre linke Seite durch $x-1$ teilbar und der Quotient ein Quadrat. Zieht man daraus die Quadratwurzel, so wird Gleichung II auf

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{m-2.m-3}{1.2}x^{m-4} + \frac{1}{32}\frac{m-3.m-4}{1.2}x^{m-5} - \text{usw.} = 0$$

zurückgeführt, deren Wurzeln die Kosinus der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{mP}{n}$ sind. Weitere Zurückführungen dieser Gleichungen, jedenfalls für den Fall, dass n eine Primzahl ist, standen bisher nicht zur Verfügung.

Keine dieser Gleichungen ist jedoch so leicht zu behandeln und für unseren Zweck so geeignet wie $x^n - 1 = 0$, deren Wurzeln bekanntlich sehr eng mit den Wurzeln jener zusammenhängen. Schreibt man nämlich der Kürze wegen i für die imaginäre Größe $\sqrt{-1}$, so werden die Wurzeln der Gleichung $x^n - 1 = 0$ dargestellt durch

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r,$$

wobei für k sämtliche Zahlen $0, 1, 2 \ldots n-1$ zu nehmen sind. Da $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$ gilt, werden also die Wurzeln der Gleichung I durch $\frac{1}{2i}(r - \frac{1}{r})$ oder durch $i\frac{1-rr}{2r}$ dargestellt, die Wurzeln der Gleichung II durch $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+rr}{2r}$ und schließlich die Wurzeln der Gleichung III durch $\frac{i(1-rr)}{1+rr}$. Deshalb werden wir unsere Untersuchung auf die Betrachtung der Gleichung $x^n - 1 = 0$ gründen und dabei n als ungerade Primzahl voraussetzen. Um die Reihenfolge der Untersuchungen nicht unterbrechen zu müssen, schicken wir hier den folgenden Hilfssatz voraus.

338.

AUFGABE. *Zur gegebenen Gleichung*

$$(W) \dots z^m + Az^{m-1} + \text{usw.} = 0,$$

ist eine Gleichung (W') *zu finden, deren Wurzeln die* λ*-ten Potenzen der Wurzeln der Gleichung* (W) *sind, wobei* λ *einen gegebenen positiven ganzzahligen Exponenten bezeichnet. Lösung.* Bezeichnet man die Wurzeln der Gleichung W mit a, b, c usw., so müssen die Wurzeln der Gleichung W' gleich $a^\lambda, b^\lambda, c^\lambda$ usw. sein. Nach dem bekannten Newtonschen Satz kann man aus den Koeffizienten der Gleichung W die Summen beliebiger Potenzen der Wurzeln a, b, c usw. finden. Man suche also die Summen

$$a^\lambda + b^\lambda + c^\lambda + \text{usw.}, \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} \text{ usw. usw.}$$
$$\text{bis zu} \quad a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{usw.}$$

aus denen man dann umgekehrt nach demselben Satz die Koeffizienten der Gleichung W' ableiten kann. *Q. E. F.* — Zugleich geht daraus hervor, dass, wenn alle Koeffizienten in W rational sind, auch alle in W' rational werden. Auf einem anderen Weg lässt sich zwar beweisen, dass, wenn jene alle ganze Zahlen sind, auch diese alle ganze Zahlen werden; bei diesem für unseren Zweck nicht so nötigen Satz halten wir uns hier jedoch nicht auf.

339.

Die Gleichung $x^n - 1 = 0$ (unter der von nun an stets mitzuverstehenden Voraussetzung, dass n eine ungerade Primzahl ist) hat nur eine reelle Wurzel, $x = 1$; die übrigen $n - 1$ Wurzeln sind in der Gleichung

$$x^{n-1} + x^{n-2} + \text{usw.} + x + 1 = 0$$

enthalten und alle imaginär. Ihre Menge werden wir mit Ω und die Funktion

$$x^{n-1} + x^{n-2} + \text{usw.} + x + 1 \quad \text{mit} \quad X$$

bezeichnen. Ist also r irgendeine Wurzel aus Ω, so gilt $1 = r^n = r^{2n}$ usw. und allgemein $r^{en} = 1$ für jeden ganzzahligen Wert von e, ob positiv oder negativ; daraus ist klar, dass, wenn λ, μ nach n kongruente ganze Zahlen sind, $r^\lambda = r^\mu$ gilt. Sind dagegen λ, μ nach dem Modul n inkongruent, so sind r^λ und r^μ ungleich; denn in diesem Fall lässt sich eine ganze Zahl ν so wählen, dass $(\lambda - \mu)\nu \equiv 1 \pmod{n}$ gilt, woraus $r^{(\lambda-\mu)\nu} = r$ folgt und daher $r^{\lambda-\mu}$ sicher nicht $= 1$ ist. Ferner ist klar, dass jede Potenz von r ebenfalls eine Wurzel der Gleichung $x^n - 1 = 0$ ist; da die Größen $1 (= r^0), r, rr \dots r^{n-1}$ alle verschieden sind, stellen sie also sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ dar, und somit stimmen $r, rr, r^3 \dots r^{n-1}$ mit Ω überein. Allgemeiner folgt daraus leicht, dass Ω mit $r^e, r^{2e}, r^{3e} \dots r^{(n-1)e}$ übereinstimmt, wenn e irgendeine durch n nicht teilbare ganze Zahl ist, ob positiv oder negativ. Es gilt daher

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \dots (x - r^{(n-1)e})$$

woraus

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1,$$
$$\text{und} \quad 1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

folgt.

Zwei Wurzeln wie r und $\frac{1}{r}$ $(= r^{n-1})$ oder allgemein r^e und r^{-e} werden wir *reziprok* nennen; offenbar ist das Produkt der beiden einfachen Faktoren $x - r$ und $x - \frac{1}{r}$ reell, $= xx - 2x\cos\omega + 1$, wobei der Winkel ω entweder dem Winkel $\frac{P}{n}$ oder einem seiner Vielfachen gleich ist.

340.

Bezeichnet man also eine Wurzel aus Ω mit r, so werden sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ durch Potenzen von r ausgedrückt; ein auf beliebige Weise aus mehreren Wurzeln dieser Gleichung gebildetes Produkt lässt sich daher durch r^λ darstellen, wobei λ entweder 0 oder positiv und $< n$ ist. Bezeichnet nun $\varphi(t, u, v \ldots)$ eine ganzrationale algebraische Funktion der Unbestimmten t, u, v usw., die sich als Summe von Gliedern der Form $ht^\alpha u^\beta v^\gamma \ldots$ ausdrücken lässt, so ist klar: Setzt man für t, u, v usw. einige der Wurzeln der Gleichung $x^n - 1 = 0$ ein, etwa $t = a, u = b$, $v = c$ usw., so lässt sich $\varphi(a, b, c \ldots)$ auf die Form

$$A + A'r + A''rr + A'''r^3 + \ldots + A^\nu r^{n-1}$$

bringen, wobei die Koeffizienten A, A' usw. (von denen auch einige fehlen und somit $= 0$ sein können) bestimmte Größen sind. Außerdem sind alle diese Koeffizienten ganze Zahlen, wenn sämtliche bestimmten Koeffizienten in $\varphi(t, u, v \ldots)$, das heißt alle h, ganze Zahlen sind. Setzt man danach für $t, u, v \ldots$ jeweils $aa, bb, cc \ldots$ ein, so wird jedes Glied wie $ht^\alpha u^\beta v^\gamma \ldots$, das sich vorher auf r^σ zurückführen ließ, nun zu $r^{2\sigma}$. Daraus folgt leicht

$$\varphi(aa, bb, cc \ldots) = A + A'rr + A''r^4 + A'''r^6 + \ldots + A^\nu r^{2n-2}$$

Ebenso gilt allgemein für jeden ganzzahligen Wert von λ

$$\varphi(a^\lambda, b^\lambda, c^\lambda \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \ldots + A^\nu r^{(n-1)\lambda}$$

Dieser Satz ist von größter Bedeutung und bildet die Grundlage der folgenden Untersuchungen. — Daraus folgt außerdem

$$\varphi(1, 1, 1 \ldots) = \varphi(a^n, b^n, c^n \ldots) = A + A' + A'' + \ldots + A^\nu$$

sowie

$$\varphi(a, b, c \ldots) + \varphi(aa, bb, cc \ldots) + \varphi(a^3, b^3, c^3 \ldots) + \ldots + \varphi(a^n, b^n, c^n \ldots) = nA$$

Diese Summe ist also immer eine ganze, durch n teilbare Zahl, wenn alle bestimmten Koeffizienten in $\varphi(t, u, v \ldots)$ ganze Zahlen sind.

Theorie der Wurzeln der Gleichung $x^n - 1 = 0$ *(wobei* n *als Primzahl vorausgesetzt wird). Lässt man die Wurzel* 1 *weg, so sind die übrigen* (Ω) *in der Gleichung* $X = x^{n-1} + x^{n-2} + \text{usw.} + x + 1 = 0$ *enthalten. Die Funktion* X *lässt sich nicht in Faktoren niedrigeren Grades zerlegen, deren Koeffizienten alle rational sind.*

341.

Satz. *Ist die Funktion* X *durch die Funktion niedrigeren Grades*

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L$$

teilbar, so können die Koeffizienten $A, B \ldots L$ *nicht sämtlich ganze Zahlen sein.*

Beweis. Es sei $X = PQ$ und $\mathfrak{P}$ die Gesamtheit der Wurzeln der Gleichung $P = 0$, $\mathfrak{Q}$ die Gesamtheit der Wurzeln der Gleichung $Q = 0$, sodass Ω aus $\mathfrak{P}$ und $\mathfrak{Q}$ zusammen besteht. Ferner sei $\mathfrak{R}$ die Gesamtheit der zu den Wurzeln in $\mathfrak{P}$ reziproken Wurzeln, $\mathfrak{S}$ die Gesamtheit der zu den Wurzeln in $\mathfrak{Q}$ reziproken Wurzeln. Die in $\mathfrak{R}$ enthaltenen Wurzeln seien die Wurzeln der Gleichung $R = 0$ (die, wie man leicht sieht, $x^\lambda + \frac{K}{L}x^{\lambda-1} + \text{usw.} + \frac{A}{L}x + \frac{1}{L} = 0$ lautet), die in $\mathfrak{S}$ enthaltenen die Wurzeln der Gleichung $S = 0$. Offenbar bilden auch die Wurzeln $\mathfrak{R}$ und $\mathfrak{S}$ zusammen die Gesamtheit Ω, und es gilt $RS = X$. Wir unterscheiden nun vier Fälle.

I. Wenn $\mathfrak{P}$ mit $\mathfrak{R}$ übereinstimmt und daher $P = R$ gilt. In diesem Fall sind die Wurzeln in $\mathfrak{P}$ offenbar stets paarweise reziprok, und somit ist P das Produkt aus $\frac{1}{2}\lambda$ quadratischen Faktoren der Form $xx - 2x\cos\omega + 1$; da ein solcher Faktor $= (x - \cos\omega)^2 + \sin\omega^2$ ist, sieht man leicht, dass P für jeden reellen Wert von x notwendig einen positiven reellen Wert annimmt. Die Gleichungen, deren Wurzeln jeweils die Quadrate, Kuben, vierten Potenzen ... und Potenzen mit dem Exponenten $n - 1$ der Wurzeln in $\mathfrak{P}$ sind, seien $P' = 0$, $P'' = 0, P''' = 0, \ldots P^\nu = 0$, und die Werte, welche die Funktionen $P, P', P'' \ldots P^\nu$ bei Setzen von $x = 1$ annehmen, seien jeweils $p, p', p'' \ldots p^\nu$. Dann ist nach dem Vorhergehenden p eine positive Größe, und aus ganz demselben Grund sind auch p', p'' usw. positiv. Nun ist p der Wert der Funktion $(1-t)(1-u)(1-v)$ usw., den sie annimmt, wenn man für t, u, v usw. die Wurzeln in $\mathfrak{P}$ einsetzt; p' ist der Wert derselben Funktion, wenn man für t, u, v usw. die Quadrate jener Wurzeln einsetzt, usw.; außerdem ist der Wert für $t = 1, u = 1$, $v = 1$ usw. offenbar $= 0$. Daher ist die Summe $p + p' + p'' \ldots + p^\nu$ eine durch n teilbare ganze Zahl. Ferner sieht man leicht, dass das Produkt $PP'P'' \ldots = X^\lambda$ ist und daher $pp'p'' \ldots = n^\lambda$ gilt. Wären nun alle Koeffizienten in P rational, so wären nach Artikel 338 auch alle in P', P'' usw. rational; nach Artikel 42 müssten aber alle diese Koeffizienten ganze Zahlen sein. Daher wären auch p, p', p'' usw. sämtlich ganze Zahlen; da ihr Produkt n^λ ist und für ihre Anzahl $n - 1 > \lambda$ gilt, müssten notwendig einige von ihnen (mindestens $n-1-\lambda$) gleich $= 1$, die übrigen aber gleich n oder einer Potenz von n sein. Sind also g von ihnen gleich $= 1$, so ist die Summe $p + p' + \text{usw.}$ offenbar $\equiv g \pmod{n}$ und somit sicher nicht durch n teilbar. Die Annahme kann daher nicht bestehen.

II. Wenn $\mathfrak{P}$ und $\mathfrak{R}$ zwar nicht übereinstimmen, aber einige gemeinsame Wurzeln enthalten, sei $\mathfrak{T}$ deren Gesamtheit und $T = 0$ die Gleichung, deren Wurzeln sie sind. Dann ist T der größte gemeinsame Teiler der Funktionen P, R (wie aus der Theorie

der Gleichungen bekannt ist). Die Wurzeln in $\mathfrak{T}$ sind aber offenbar stets paarweise reziprok; daher können nach dem zuvor Bewiesenen die Koeffizienten in T nicht alle rational sein. Dies wären sie jedoch sicher, wenn alle in P und damit auch alle in R rational wären, wie unmittelbar aus der Art des Verfahrens zur Bestimmung des größten gemeinsamen Teilers folgt. Die Annahme ist daher absurd.

III. Wenn $\mathfrak{Q}$ und $\mathfrak{S}$ entweder übereinstimmen oder wenigstens gemeinsame Wurzeln enthalten, können auf genau dieselbe Weise die Koeffizienten in Q nicht alle rational sein; sie wären es aber, wenn alle in P rational wären. Dies ist also unmöglich.

IV. Haben dagegen weder $\mathfrak{P}$ mit $\mathfrak{R}$ noch $\mathfrak{Q}$ mit $\mathfrak{S}$ irgendeine gemeinsame Wurzel, so müssen alle Wurzeln $\mathfrak{P}$ in $\mathfrak{S}$ und alle $\mathfrak{Q}$ in $\mathfrak{R}$ enthalten sein, woraus $P = S$ und $Q = R$ folgt. Daher ist $X = PQ$ das Produkt aus P und R, das heißt

$$\begin{aligned} &\text{aus} \quad x^\lambda + Ax^{\lambda-1} \ldots + Kx + L \\ &\text{und} \quad x^\lambda + \frac{K}{L}x^{\lambda-1} \ldots + \frac{A}{L}x + \frac{1}{L} \end{aligned}$$

woraus durch Setzen von $x = 1$

$$nL = (1 + A \ldots + K + L)^2$$

folgt. Wären nun alle Koeffizienten in P rational und daher nach Artikel 42 auch ganze Zahlen, so müsste L, das den letzten Koeffizienten in X, nämlich die Einheit, teilen muss, notwendig $= \pm 1$ sein; daraus folgte, dass $\pm n$ eine Quadratzahl wäre. Da dies der Voraussetzung widerspricht, kann die Annahme nicht bestehen.

Aus diesem Satz geht also hervor, dass, wie man auch X in Faktoren zerlegt, deren Koeffizienten wenigstens zum Teil irrational sind und sich daher nur durch eine Gleichung höheren Grades bestimmen lassen.

Das Ziel der folgenden Untersuchungen wird erläutert.

342.

Das Ziel der folgenden Untersuchungen, das kurz zu erläutern nützlich sein wird, besteht darin, X SCHRITTWEISE in immer mehr Faktoren zu zerlegen und dabei ihre Koeffizienten durch Gleichungen möglichst niedrigen Grades zu bestimmen, bis man so zu Linearfaktoren oder zu den Wurzeln Ω selbst gelangt. Wir werden nämlich zeigen: Zerlegt man die Zahl $n-1$ auf beliebige Weise in ganzzahlige Faktoren α, β, γ usw. (für die man jeweils Primzahlen nehmen kann), so lässt sich X in α Faktoren vom Grad $\frac{n-1}{\alpha}$ zerlegen, deren Koeffizienten durch eine Gleichung vom Grad α bestimmt werden; jeder dieser Faktoren wiederum in β andere vom Grad $\frac{n-1}{\alpha\beta}$ mithilfe einer Gleichung vom Grad β usw. Bezeichnet also ν die Anzahl der Faktoren α, β, γ usw., so führt sich die Bestimmung der Wurzeln Ω auf die Lösung von ν Gleichungen der Grade α, β, γ usw. zurück. *Zum Beispiel* sind für $n = 17$, wo $n - 1 = 2.2.2.2$ gilt, vier quadratische Gleichungen zu lösen; für $n = 73$ drei quadratische und zwei kubische.

Da im Folgenden sehr oft Potenzen der Wurzel r zu betrachten sind, deren Exponenten wiederum Potenzen sind, und solche Ausdrücke nur mit Mühe zu setzen sind,

werden wir zur Erleichterung des Drucks künftig die folgende Abkürzung verwenden. Für r, rr, r^3 usw. schreiben wir $[1], [2], [3]$ usw. und allgemein für r^λ, wobei λ irgendeine ganze Zahl bezeichnet, $[\lambda]$. Solche Ausdrücke sind also noch nicht vollständig bestimmt, werden es aber, sobald für r oder $[1]$ eine bestimmte Wurzel aus Ω gewählt wird. Allgemein sind somit $[\lambda], [\mu]$ gleich oder ungleich, je nachdem, ob λ, μ nach dem Modul n kongruent oder inkongruent sind; ferner gilt $[0] = 1$; $[\lambda].[\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$; die Summe $[0]+[\lambda]+[2\lambda] \ldots +[(n-1)\lambda]$ ist entweder 0 oder n, je nachdem, ob λ durch n nicht teilbar oder teilbar ist.

Sämtliche Wurzeln Ω werden in gewisse Klassen (Perioden) eingeteilt.

343.

Ist für den Modul n die Zahl g eine Zahl derjenigen Art, die wir in Abschnitt III primitive Wurzel genannt haben, so sind die $n-1$ Zahlen $1, g, gg \ldots g^{n-2}$ den Zahlen $1, 2, 3 \ldots n-1$ nach dem Modul n kongruent, wenn auch in anderer Reihenfolge: Jede Zahl der einen Folge hat in der anderen eine kongruente Zahl. Daraus folgt unmittelbar, dass die Wurzeln $[1], [g], [gg] \ldots [g^{n-2}]$ mit Ω übereinstimmen; ganz ebenso stimmen allgemeiner

$$[\lambda], [\lambda g], [\lambda gg] \ldots [\lambda g^{n-2}] \quad \text{mit} \quad \Omega$$

überein, wobei λ irgendeine durch n nicht teilbare ganze Zahl bezeichnet. Da ferner $g^{n-1} \equiv 1 \pmod{n}$ gilt, sieht man ohne Mühe, dass die beiden Wurzeln $[\lambda g^\mu], [\lambda g^\nu]$ identisch oder verschieden sind, je nachdem, ob μ, ν nach $n-1$ kongruent oder inkongruent sind. Ist also G eine andere primitive Wurzel, so stimmen die Wurzeln $[1], [g] \ldots [g^{n-2}]$ auch mit $[1], [G] \ldots [G^{n-2}]$ überein, wenn man von der Reihenfolge absieht. Außerdem beweist man aber leicht: Ist e ein Teiler von $n-1$ und setzt man $n-1 = ef$, $g^e = h$, $G^e = H$, so sind auch die f Zahlen $1, h, hh \ldots h^{f-1}$ den Zahlen $1, H, H^2 \ldots H^{f-1}$ nach n kongruent (ohne Rücksicht auf die Reihenfolge). Nehmen wir nämlich $G \equiv g^\omega \pmod{n}$ an, und sei μ eine beliebige positive Zahl $< f$ und ν der kleinste Rest von $\mu\omega \pmod{f}$. Dann gilt $\nu e \equiv \mu\omega e \pmod{n-1}$, daher $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$ oder $H^\mu \equiv h^\nu$; das heißt, jede Zahl der letzteren Folge $1, H, H^2$ usw. hat in der Folge $1, h, hh \ldots$ eine kongruente Zahl, und ebenso umgekehrt. — Daraus ist klar, dass die f Wurzeln $[1], [h], [hh] \ldots [h^{f-1}]$ mit $[1], [H], [H^2] \ldots [H^{f-1}]$ identisch sind; allgemeiner sieht man auf dieselbe Weise leicht, dass

$$[\lambda], [\lambda h], [\lambda hh] \ldots [\lambda h^{f-1}]$$
$$\text{mit} \quad [\lambda], [\lambda H], [\lambda H^2] \ldots [\lambda H^{f-1}]$$

übereinstimmen. Die *Summe* von solchen f Wurzeln $[\lambda]+[\lambda h]+\text{usw.}+[\lambda h^{f-1}]$, die, da sie sich bei Wahl einer anderen primitiven Wurzel für g nicht ändert, als unabhängig von g anzusehen ist, bezeichnen wir mit $(f; \lambda)$; die *Gesamtheit* derselben Wurzeln nennen wir die *Periode* (f, λ), wobei die Reihenfolge der Wurzeln unbeachtet bleibt[*].

[*] Im Folgenden dürfen wir die Summe auch den Zahlenwert der Periode oder einfach die Periode nennen, wenn keine Mehrdeutigkeit zu befürchten ist.

— Bei der Darstellung einer solchen Periode ist es zweckmäßig, die einzelnen Wurzeln, aus denen sie besteht, auf den einfachsten Ausdruck zurückzuführen, nämlich für die Zahlen $\lambda, \lambda h, \lambda hh$ usw. die kleinsten Reste nach dem Modul n einzusetzen; nach deren Größe können, wenn man will, auch die Glieder der Periode geordnet werden.

Zum Beispiel besteht für $n = 19$, wo 2 eine primitive Wurzel ist, die Periode $(6, 1)$ aus den Wurzeln $[1], [8], [64], [512], [4096], [32768]$ oder $[1], [7], [8], [11], [12], [18]$. Ebenso besteht die Periode $(6, 2)$ aus $[2], [3], [5], [14], [16], [17]$. Die Periode $(6, 3)$ ist mit der vorigen identisch. Die Periode $(6, 4)$ enthält $[4], [6], [9], [10], [13], [15]$.

Verschiedene Sätze über die Perioden der Wurzeln Ω.

344.

Bei diesen Perioden ergeben sich unmittelbar die folgenden Beobachtungen:

I. Da $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$ usw. (mod. n) gilt, bestehen offenbar aus denselben Wurzeln, aus denen (f, λ) besteht, auch $(f, \lambda h), (f, \lambda hh)$ usw.; bezeichnet also allgemein $[\lambda']$ irgendeine Wurzel aus (f, λ), so ist diese Periode mit (f, λ') vollständig identisch. Haben also zwei Perioden mit gleich vielen Wurzeln (die wir *gleichartig* nennen werden) irgendeine Wurzel gemeinsam, so sind sie offenbar identisch. Daher können nicht zwei Wurzeln gemeinsam in einer Periode enthalten sein, während in einer anderen gleichartigen nur eine von ihnen vorkommt. Ferner ist klar: Gehören zwei Wurzeln $[\lambda], [\lambda']$ zu derselben Periode mit f Gliedern, so ist der Wert des Ausdrucks $\frac{\lambda'}{\lambda}$ (mod. n) irgendeiner Potenz von h kongruent, oder man kann $\lambda' \equiv \lambda g^{\nu e}$ (mod. n) setzen.

II. Ist $f = n - 1$, $e = 1$, so stimmt die Periode $(f, 1)$ offenbar mit Ω überein; in den übrigen Fällen besteht Ω aus e Perioden $(f, 1), (f, g), (f, gg) \ldots (f, g^{e-1})$. Diese Perioden sind also sämtlich voneinander verschieden, und offenbar stimmt jede andere gleichartige Periode (f, λ) mit einer von ihnen überein, sofern $[\lambda]$ zu Ω gehört, das heißt, wenn λ durch n nicht teilbar ist. Die Periode $(f, 0)$ oder (f, kn) besteht dagegen offenbar aus f Einheiten. Ebenso leicht sieht man, dass, wenn λ irgendeine durch n nicht teilbare Zahl ist, auch die Gesamtheit der e Perioden $(f, \lambda), (f, \lambda g)$, $(f, \lambda gg) \ldots (f, \lambda g^{e-1})$ mit Ω übereinstimmt. — So besteht *zum Beispiel* für $n = 19$, $f = 6$ die Gesamtheit Ω aus den drei Perioden $(6, 1), (6, 2), (6, 4)$, auf deren eine sich jede andere gleichartige außer $(6, 0)$ zurückführen lässt.

III. Ist $n - 1$ das Produkt aus drei positiven Zahlen a, b, c, so besteht offenbar jede Periode mit bc Gliedern aus b Perioden mit c Gliedern, nämlich (bc, λ) aus $(c, \lambda), (c, \lambda g^a), (c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$; daher werden diese als in jener enthalten bezeichnet. So besteht für $n = 19$ die Periode $(6, 1)$ aus den drei Perioden $(2, 1), (2, 8), (2, 7)$, deren erste die Wurzeln r, r^{18}, deren zweite r^8, r^{11} und deren dritte r^7, r^{12} enthält.

345.

Satz. *Es seien* $(f,\lambda),(f,\mu)$ *zwei gleichartige, identische oder verschiedene Perioden, und* (f,λ) *bestehe aus den Wurzeln* $[\lambda],[\lambda'],[\lambda'']$ *usw. Dann ist das Produkt aus* (f,λ) *und* (f,μ) *eine Summe von* f *gleichartigen Perioden, nämlich*

$$= (f,\lambda+\mu)+(f,\lambda'+\mu)+(f,\lambda''+\mu)+\text{usw.} = W$$

Beweis. Es sei wie oben $n-1=ef$; g sei eine primitive Wurzel für den Modul n und $h=g^e$, woraus nach dem Vorhergehenden $(f,\lambda)=(f,\lambda h)=(f,\lambda hh)$ usw. folgt. Das gesuchte Produkt ist daher

$$= [\mu].(f,\lambda)+[\mu h].(f,\lambda h)+[\mu hh].(f,\lambda hh)+\text{usw.}$$

und somit

$$\begin{array}{llll} =[\lambda+\mu] & +[\lambda h+\mu] & \ldots+[\lambda h^{f-1}+\mu] & \\ +[\lambda h+\mu h] & +[\lambda hh+\mu h] & \ldots+[\lambda h^{f}+\mu h] & \\ +[\lambda hh+\mu hh] & +[\lambda h^3+\mu hh] & \ldots+[\lambda h^{f+1}+\mu hh] & \text{usw.} \end{array}$$

Dieser Ausdruck enthält insgesamt ff Wurzeln. Summiert man hier jede senkrechte Spalte für sich, so erhält man offenbar

$$(f,\lambda+\mu)+(f,\lambda h+\mu)+\ldots+(f,\lambda h^{f-1}+\mu)$$

Man sieht ohne Mühe, dass dieser Ausdruck mit W übereinstimmt, da die Zahlen λ, λ',λ'' usw. nach Voraussetzung den Zahlen $\lambda,\lambda h,\lambda hh\ldots\lambda h^{f-1}$ nach dem Modul n kongruent sein müssen (in welcher Reihenfolge, ist hier gleichgültig) und daher auch

$$\begin{array}{c} \lambda+\mu,\ \lambda'+\mu,\ \lambda''+\mu \quad \text{usw.} \quad \text{den Zahlen} \\ \lambda+\mu,\ \lambda h+\mu,\ \lambda hh+\mu\ldots\lambda h^{f-1}+\mu. \quad \textit{Q. E. D.} \end{array}$$

Wir fügen diesem Satz die folgenden Folgerungen hinzu:

I. Bezeichnet k eine beliebige ganze Zahl, so ist das Produkt aus $(f,k\lambda)$ und $(f,k\mu)$

$$= (f,k(\lambda+\mu))+(f,k(\lambda'+\mu))+(f,k(\lambda''+\mu))+\text{usw.}$$

II. Da die einzelnen Teile, aus denen W besteht, entweder mit der Summe $(f,0)$, die $=f$ ist, oder mit einer von $(f,1),\ (f,g),\ (f,gg)\ldots(f,g^{e-1})$ übereinstimmen, lässt sich W auf die folgende Form bringen

$$W = af+b(f,1)+b'(f,g)+b''(f,gg) \\ +\ldots+b^{\varepsilon}(f,g^{e-1})$$

Dabei sind die Koeffizienten a,b,b' usw. positive ganze Zahlen (oder einige auch $=0$). Ferner ist klar: Das Produkt aus $(f,k\lambda)$ und $(f,k\mu)$ wird dann zu

$$= af+b(f,k)+b'(f,kg)+\ldots+b^{\varepsilon}(f,kg^{e-1})$$

So wird *zum Beispiel* für $n=19$ das Produkt aus der Summe (6.1) und sich selbst oder das Quadrat dieser Summe $= (6,2)+(6,8)+(6,9)+(6.12)+(6,13)+(6,19)=6+2(6,1)+(6,2)+2(6,4)$.

III. Da sich das Produkt aus jedem einzelnen Teil von W und einer gleichartigen Periode (f,ν) auf eine entsprechende Form bringen lässt, ist klar, dass auch das Produkt aus den drei Perioden $(f,\lambda).(f,\mu).(f,\nu)$ durch $cf + d(f,1) \ldots + d^{\varepsilon}(f,g^{e-1})$ dargestellt werden kann und die Koeffizienten c,d usw. ganze und positive Zahlen (oder $= 0$) sind; außerdem gilt für jeden beliebigen ganzzahligen Wert von k

$$(f,k\lambda).(f,k\mu).(f,k\nu) = cf + d(f,k) + d'(f,kg) + \text{usw.}$$

Ebenso erstreckt sich dieser Satz auf Produkte aus beliebig vielen gleichartigen Perioden, und es ist gleichgültig, ob diese Perioden sämtlich verschieden oder zum Teil oder sämtlich identisch sind.

IV. Daraus folgt: Werden in irgendeiner ganzrationalen algebraischen Funktion $F = \varphi(t,u,v\ldots)$ für die Unbestimmten t,u,v usw. jeweils die gleichartigen Perioden $(f,\lambda),(f,\mu),(f,\nu)$ usw. eingesetzt, so lässt sich ihr Wert auf die Form

$$A + B(f,1) + B'(f,g) + B''(f,gg) + \ldots + B^{\varepsilon}(f,g^{e-1})$$

bringen, und die Koeffizienten A,B,B' usw. sind sämtlich ganze Zahlen, wenn alle festen Koeffizienten in F ganze Zahlen sind. Werden danach für t,u,v usw. jeweils $(f,k\lambda),(f,k\mu),(f,k\nu)$ usw. eingesetzt, so führt sich der Wert von F auf $A + B(f,k) + B'(f,kg) + \text{usw.}$ zurück.

346.

Satz. *Nimmt man an, dass λ eine durch n nicht teilbare Zahl ist, und schreibt man der Kürze wegen p für (f,λ), so lässt sich jede andere gleichartige Periode (f,μ), wobei auch μ als durch n nicht teilbar vorausgesetzt wird, auf die folgende Form bringen*

$$\alpha + \beta p + \gamma pp + \ldots + \theta p^{e-1}$$

wobei die Koeffizienten α,β usw. feste rationale Größen sind.

Beweis. Wir bezeichnen zur Abkürzung die Perioden $(f,\lambda g),(f,\lambda gg),(f,\lambda g^3)$ usw. bis $(f,\lambda g^{e-1})$, deren Anzahl $e-1$ ist und mit deren einer (f,μ) notwendig übereinstimmt, mit p',p'',p''' usw. Man hat dann unmittelbar die Gleichung

$$0 = 1 + p + p' + p'' + p''' + \text{usw.} \quad . \ . \ . \ . \ . \quad \text{(I)}$$

Entwickelt man aber nach den Regeln des vorigen Artikels die Werte der Potenzen von p bis zur Potenz mit dem Exponenten $e-1$, so ergeben sich $e-2$ weitere Gleichungen der folgenden Art.

$$0 = pp + A + ap + a'p' + a''p'' + a'''p''' + \text{usw.} \quad . \ . \quad \text{(II)}$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{usw.} \quad . \ . \quad \text{(III)}$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{usw.} \quad . \ . \quad \text{(IV)} \quad \text{usw.}$$

Dabei sind sämtliche Koeffizienten A,a,a' usw., B,b,b' usw. usw. ganze Zahlen und, was sorgfältig zu beachten ist und aus dem vorigen Artikel unmittelbar folgt, von λ völlig unabhängig; *das heißt*, dieselben Gleichungen gelten auch dann noch, welchen

anderen Wert man λ auch gibt. Diese Bemerkung erstreckt sich offenbar auch auf Gleichung I, sofern man λ als durch n nicht teilbar annimmt. — Nehmen wir $(f,\mu) = p'$ an; denn man sieht sehr leicht, dass, wenn (f,μ) mit einer anderen der Perioden p'', p''' usw. übereinstimmt, zu den folgenden völlig analoge Schlüsse angewendet werden können. Da die Anzahl der Gleichungen I, II, III usw. $e-1$ ist, lassen sich die Größen p'', p''' usw., deren Anzahl $= e-2$ ist, nach bekannten Methoden daraus eliminieren, sodass sich eine von ihnen freie Gleichung der folgenden Art (Z) ergibt

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}pp + \text{usw.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

Dies kann so geschehen, dass alle Koeffizienten $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{N}$ ganze Zahlen und sicher nicht alle $= 0$ sind. Gilt hier nun nicht $\mathfrak{N} = 0$, so ist unmittelbar klar, dass sich p' daraus in der im Satz angegebenen Weise bestimmt. Es bleibt also zu zeigen, dass $\mathfrak{N} = 0$ nicht eintreten kann.

Nimmt man $\mathfrak{N} = 0$ an, so wird Gleichung Z zu $\mathfrak{M}p^{e-1} + \text{usw.} + \mathfrak{B}p + \mathfrak{A} = 0$; da sie sicher nicht über den Grad $e-1$ hinausgeht, können ihr nicht mehr als $e-1$ verschiedene Werte von p genügen. Da aber die Gleichungen, aus denen Z abgeleitet wurde, von λ unabhängig sind, ist klar, dass auch Z nicht von λ abhängt, also gilt, welche durch n nicht teilbare ganze Zahl man auch für λ nimmt. Daher wird Gleichung Z erfüllt, welcher von den e Summen $(f,1), (f,g), (f,gg) \ldots (f,g^{e-1})$ man p auch gleichsetzt. Daraus folgt unmittelbar, dass diese Summen nicht sämtlich ungleich sein können, sondern wenigstens zwei einander gleich sein müssen. Die eine von zwei solchen gleichen Summen enthalte die Wurzeln $[\zeta], [\zeta'], [\zeta'']$ usw., die andere $[\eta], [\eta'], [\eta'']$ usw.; wir nehmen an (was zulässig ist), dass alle Zahlen ζ, ζ', ζ'' usw., η, η', η'' usw. positiv und $< n$ sind; offenbar sind sie auch sämtlich verschieden und keine $= 0$. Die Funktion

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \text{usw.} - x^{\eta} - x^{\eta'} - x^{\eta''} - \text{usw.}$$

hat kein höheres Glied als x^{n-1}. Bezeichnen wir sie mit Y, so gilt offenbar $Y = 0$, wenn man $x = [1]$ setzt. Daher enthält Y den Faktor $x - [1]$, den sie mit der im Vorhergehenden durch X bezeichneten Funktion *gemeinsam* hat; dass dies aber absurd ist, lässt sich leicht zeigen. Hätte nämlich Y mit X irgendeinen gemeinsamen Faktor, so hätte der *größte* gemeinsame Teiler der Funktionen X, Y (dass dieser sicher nicht bis zum Grad $n-1$ reichen kann, geht schon daraus hervor, dass Y durch x teilbar ist) ausschließlich rationale Koeffizienten, wie aus der Art der Rechenoperationen zur Bestimmung des größten gemeinsamen Teilers zweier solcher Funktionen, deren Koeffizienten alle rational sind, unmittelbar folgt. In Artikel 341 haben wir aber gezeigt, dass X keinen Faktor eines Grades unter $n-1$ enthalten kann, dessen Koeffizienten sämtlich rational sind. Daher kann die Annahme, dass $\mathfrak{N} = 0$ gilt, nicht bestehen.

Beispiel. Für $n = 19,\ f = 6$ gilt $pp = 6 + 2p + p' + 2p''$; daraus und aus $0 = 1 + p + p' + p''$ folgt $p' = 4 - pp,\ p'' = -5 - p + pp$. Daher

$$\begin{aligned}
(6,2) &= 4 - (6,1)^2, \quad & (6,4) &= -5 - (6,1) + (6,1)^2 \\
(6,4) &= 4 - (6,2)^2, \quad & (6.1) &= -5 - (6,2) + (6,2)^2 \\
(6,1) &= 4 - (6,4)^2, \quad & (6,2) &= -5 - (6,4) + (6,4)^2
\end{aligned}$$

347.

Satz. *Ist $F = \varphi(t, u.v\ldots)$ eine symmetrische*[*)] *algebraische ganzrationale Funktion von f Unbestimmten t, u, v usw., und führt man nach Einsetzen der f in der Periode (f, λ) enthaltenen Wurzeln für diese Unbestimmten den Wert von F nach den Regeln des Artikels 340 auf die Form*

$$A + A'[1] + A''[2] + \text{usw.} = W$$

zurück, so haben die Wurzeln, die in diesem Ausdruck zu einer und derselben beliebigen Periode mit f Gliedern gehören, gleiche Koeffizienten.

Beweis. Es seien $[p], [q]$ zwei Wurzeln, die zu einer und derselben Periode gehören, und p, q seien positiv und kleiner als n. Dann ist zu zeigen, dass $[p]$ und $[q]$ in W denselben Koeffizienten haben. Es sei $q \equiv pg^{\nu e} \pmod{n}$; ferner seien die in (f, λ) enthaltenen Wurzeln $[\lambda], [\lambda'], [\lambda'']$ usw., wobei wir die Zahlen $\lambda, \lambda', \lambda''$ usw. als positiv und kleiner als n voraussetzen. Schließlich seien die kleinsten positiven Reste der Zahlen $\lambda g^{\nu e}, \lambda' g^{\nu e}, \lambda'' g^{\nu e}$ usw. nach dem Modul n die Zahlen μ, μ', μ'' usw.; diese sind offenbar mit den Zahlen $\lambda, \lambda', \lambda''$ usw. identisch, wenn auch in anderer Reihenfolge. Aus Artikel 340 folgt nun, dass sich

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}]\ldots) = (\text{I})$$

auf

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{usw.}$$

oder auf $\quad A + A'[\theta] + A''[\theta'] + \text{usw.} = (W')$

zurückführen lässt, wobei θ, θ' usw. die kleinsten Reste der Zahlen $g^{\nu e}, 2g^{\nu e}$ usw. nach dem Modul n bezeichnen. Daraus ist klar, dass $[q]$ in (W') denselben Koeffizienten hat wie $[p]$ in (W). Man sieht aber ohne Mühe, dass die Entwicklung des Ausdrucks (I) dasselbe ergibt wie die Entwicklung von $\varphi([\mu], [\mu'].[\mu'']$ usw.), da $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$ usw. (mod. n) gilt. Dieser Ausdruck ergibt seinerseits dasselbe wie $\varphi([\lambda], [\lambda'], [\lambda'']$ usw.), weil die Zahlen μ, μ', μ'' usw. sich von $\lambda, \lambda', \lambda''$ usw. nur in der Reihenfolge unterscheiden, auf die es bei einer symmetrischen Funktion nicht ankommt. Daraus folgt, dass W' mit W vollständig identisch ist; daher hat die Wurzel $[q]$ in W denselben Koeffizienten wie $[p]$. *Q. E. D.*

Daraus ist klar, dass sich W auf die Form

$$A + a(f, 1) + a'(f, g) + a''(f, gg)\ldots + a^{\varepsilon}(f, g^{e-1})$$

zurückführen lässt, wobei die Koeffizienten $A, a\ldots a^{\varepsilon}$ feste Größen sind, die außerdem ganze Zahlen sind, wenn alle rationalen Koeffizienten in F ganze Zahlen sind. — So führt sich *zum Beispiel*, wenn $n = 19$, $f = 6$, $\lambda = 1$ gilt und die Funktion φ die Summe der paarweisen Produkte der Unbestimmten bezeichnet, ihr Wert auf $3+(6, 1)+(6, 4)$ zurück.

[*)] Bekanntlich heißen diejenigen Funktionen symmetrisch, in denen alle Unbestimmten auf dieselbe Weise vorkommen, oder deutlicher, die sich nicht ändern, wie man auch die Unbestimmten untereinander vertauscht; solche Funktionen sind *zum Beispiel* die Summe aller Unbestimmten, ihr Produkt, die Summe ihrer paarweisen Produkte usw.

Ferner sieht man leicht: Setzt man danach für t, u, v usw. die Wurzeln aus einer anderen Periode $(f, k\lambda)$ ein, so wird der Wert von F zu

$$A + a(f,k) + a'(f,kg) + a''(f,kgg) + \text{usw.}$$

348.

In jeder Gleichung

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \ldots = 0$$

sind die Koeffizienten α, β, γ usw. symmetrische Funktionen der Wurzeln, nämlich α die Summe aller Wurzeln, β die Summe ihrer paarweisen Produkte, γ die Summe ihrer Produkte zu je dreien usw. Daher ist in der Gleichung, deren Wurzeln die in der Periode (f, λ) enthaltenen Wurzeln sind, der erste Koeffizient $= (f, \lambda)$, während sich jeder der übrigen auf eine Form wie

$$A + a(f,1) + a'(f,g) \ldots + a^{\varepsilon}(f, g^{e-1})$$

bringen lässt, wobei alle A, a, a' usw. ganze Zahlen sind. Außerdem ist klar, dass die Gleichung, deren Wurzeln die in irgendeiner anderen Periode $(f, k\lambda)$ enthaltenen Wurzeln sind, aus jener hervorgeht, wenn man in jedem Koeffizienten $(f, 1)$ durch (f, k) ersetzt; ebenso (f, g) durch (f, kg) und allgemein (f, p) durch (f, kp). Auf diese Weise kann man also e Gleichungen $z = 0, z' = 0, z'' = 0$ usw. angeben, deren Wurzeln die in $(f, 1)$, in (f, g), (f, gg) usw. enthaltenen Wurzeln sind, sobald die e Summen $(f, 1), (f, g), (f, gg)$ usw. bekannt sind oder vielmehr, sobald *eine* beliebige von ihnen gefunden ist, da sich nach Artikel 346 aus einer alle übrigen rational ableiten lassen. Damit ist zugleich die Funktion X in e Faktoren vom Grad f zerlegt; denn das Produkt aus den Funktionen z, z', z'' usw. ist offenbar $= X$.

Beispiel. Für $n = 19$ ist die Summe aller Wurzeln in der Periode $(6, 1) = (6, 1) = \alpha$; die Summe ihrer paarweisen Produkte ist $= 3 + (6, 1) + (6, 4) = \beta$; ebenso findet man für die Summe der Produkte zu je dreien $= 2 + 2(6, 1) + (6, 2) = \gamma$, für die Summe der Produkte zu je vieren $= 3 + (6, 1) + (6, 4) = \delta$, für die Summe der Produkte zu je fünfen $= (6, 1) = \varepsilon$ und für das Produkt aller Wurzeln $= 1$. Daher umfasst die Gleichung

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta xx - \varepsilon x + 1 = 0$$

sämtliche in $(6, 1)$ enthaltenen Wurzeln. Setzt man nun in den Koeffizienten α, β, γ usw. für $(6, 1), (6, 2), (6, 4)$ jeweils $(6, 2), (6, 4), (6, 1)$ ein, so erhält man die Gleichung $z' = 0$, welche die Wurzeln in $(6, 2)$ umfasst; wendet man dieselbe Vertauschung hier nochmals an, so erhält man die Gleichung $z'' = 0$, welche die Wurzeln in $(6, 4)$ umfasst, und das Produkt $zz'z''$ ist $= X$.

349.

Meist ist es bequemer, besonders wenn f eine große Zahl ist, die Koeffizienten β, γ usw. nach dem Newtonschen Satz aus den Potenzsummen der Wurzeln abzuleiten. Es ist nämlich unmittelbar klar, dass die Summe der Quadrate der in (f, λ) enthaltenen Wurzeln $= (f, 2\lambda)$, die Summe ihrer Kuben $= (f, 3\lambda)$ usw. ist. Schreiben wir also der Kürze wegen für $(f, \lambda), (f, 2\lambda), (f, 3\lambda)$ usw. q, q', q'' usw., so gilt

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'' \quad \text{usw.}$$

Dabei sind die Produkte aus zwei Perioden nach Artikel 345 sofort in Summen von Perioden umzuwandeln. So werden in unserem Beispiel, wenn wir für $(6, 1), (6, 2), (6, 4)$ jeweils p, p', p'' schreiben, die Größen $q, q', q'', q''', q'''', q'''''$ jeweils $= p, p', p', p'', p', p''$; daher

$$\begin{aligned} \alpha &= p, \quad 2\beta = pp - p' = 6 + 2p + 2p'' \\ 3\gamma &= (3 + p + p'')p - pp' + p' = 6 + 6p + 3p' \\ 4\delta &= (2 + 2p + p')p - (3 + p + p'')p' \\ &\qquad + pp' - p'' = 12 + 4p + 4p'' \quad \text{usw.} \end{aligned}$$

Es genügt übrigens, nur die Hälfte der Koeffizienten auf diese Weise zu berechnen. Denn es lässt sich ohne Schwierigkeit beweisen, dass die letzten in umgekehrter Reihenfolge entweder den ersten gleich sind, nämlich der letzte $= 1$, der vorletzte $= \alpha$, der davor $= \beta$ usw., oder aus diesen jeweils hervorgehen, wenn man für $(f, 1), (f, g)$ usw. $(f, -1), (f, -g)$ usw. oder $(f, n-1)$, $(f, n-g)$ usw. einsetzt. Der erste Fall tritt ein, wenn f gerade ist, der zweite, wenn f ungerade ist; der letzte Koeffizient ist aber stets $= 1$. Dies beruht auf dem Satz in Artikel 79; doch halten wir uns der Kürze wegen bei diesem Gegenstand nicht auf.

350.

Satz. *Es sei $n-1$ das Produkt aus drei positiven ganzen Zahlen α, β, γ; die Periode $(\beta\gamma, \lambda)$, die $\beta\gamma$ Glieder hat, bestehe aus β kleineren Perioden mit γ Gliedern, nämlich $(\gamma, \lambda).(\gamma, \lambda'), (\gamma, \lambda'')$ usw. Wir nehmen an, dass in einer Funktion von β Unbestimmten von derselben Art wie in Artikel 347, nämlich in $F = \varphi(t, u, v \ldots)$, für die Unbestimmten t, u, v usw. jeweils die Summen $(\gamma, \lambda), (\gamma, \lambda'), (\gamma, \lambda'')$ usw. eingesetzt werden und ihr Wert nach den Regeln des Artikels 345, IV, auf*

$$A + a(\gamma, 1) + a'(\gamma, g) \ldots + a^{\zeta}(\gamma, g^{\alpha\beta-\alpha}) \\ \ldots + a^{\theta}(\gamma, g^{\alpha\beta-1}) = W$$

zurückgeführt wird. Dann behaupte ich: Ist F eine symmetrische Funktion, so haben die Perioden in W, die in derselben Periode mit $\beta\gamma$ Gliedern enthalten sind, das heißt allgemein solche wie (γ, g^{μ}) und $(\gamma, g^{\alpha\nu+\mu})$, wobei ν eine beliebige ganze Zahl bezeichnet, dieselben Koeffizienten.

Beweis. Da die Periode $(\beta\gamma, \lambda g^{\alpha})$ mit $(\beta\gamma, \lambda)$ identisch ist, müssen die kleineren Perioden $(\gamma, \lambda g^{\alpha}), (\gamma, \lambda' g^{\alpha}), (\gamma, \lambda'' g^{\alpha})$ usw., aus denen die erstere offenbar besteht, mit denen übereinstimmen, aus denen die letztere besteht, wenn auch in anderer Reihenfolge. Nimmt man also an, dass nach ihrem jeweiligen Einsetzen für t, u, v usw. F in W' übergeht, so stimmt W' mit W überein. Nach Artikel 347 gilt aber

$$\begin{aligned} W' &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \\ &\quad \ldots + a^{\zeta}(\gamma, g^{\alpha\beta}) \ldots + a^{\theta}(\gamma, g^{\alpha\beta+\alpha-1}) \\ &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \\ &\quad \ldots + a^{\zeta}(\gamma, 1) \ldots + a^{\theta}(\gamma, g^{\alpha-1}) \end{aligned}$$

Da dieser Ausdruck mit W übereinstimmen muss, muss der erste, zweite, dritte usw. Koeffizient in W (von a an gerechnet) jeweils mit dem Koeffizienten an der entsprechenden Stelle aus $\alpha+1, \alpha+2, \alpha+3$ usw. übereinstimmen. Daraus folgt ohne Mühe, dass allgemein die Koeffizienten der Perioden $(\gamma, g^{\mu}), (\gamma, g^{\alpha+\mu}), (\gamma, g^{2\alpha+\mu}) \ldots (\gamma, g^{\nu\alpha+\mu})$, die an den Stellen $\mu+1, \alpha+\mu+1, 2\alpha+\mu+1 \ldots \nu\alpha+\mu+1$ stehen, einander gleich sein müssen. *Q. E. D.*

Daraus ist klar, dass sich W auf die Form

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1})$$

bringen lässt, wobei alle Koeffizienten A, a usw. ganze Zahlen sind, wenn alle festen Koeffizienten in F ganze Zahlen sind. Ferner sieht man leicht: Setzt man danach für die Unbestimmten in F die β Perioden mit γ Gliedern ein, die in einer anderen Periode mit $\beta\gamma$ Gliedern, nämlich in $(\beta\gamma, \lambda k)$, enthalten sind und offenbar $(\gamma, \lambda k), (\gamma, \lambda' k), (\gamma, \lambda'' k)$ usw. sind, so ist der daraus hervorgehende Wert $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1}k)$.

Übrigens ist klar, dass sich der Satz auch auf den Fall erstreckt, in dem $\alpha = 1$ oder $\beta\gamma = n-1$ gilt; hier sind nämlich *alle* Koeffizienten in W gleich, sodass sich W auf die Form $A + a(\beta\gamma, 1)$ zurückführt.

351.

Behalten wir also sämtliche Bezeichnungen des vorigen Artikels bei, so ist klar, dass sich jeder Koeffizient der Gleichung, deren Wurzeln die β Summen $(\gamma, \lambda), (\gamma, \lambda'), (\gamma, \lambda'')$ usw. sind, auf eine Form wie

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1})$$

zurückführen lässt und alle Zahlen A, a usw. ganze Zahlen sind. Die Gleichung, deren Wurzeln die β Perioden mit γ Gliedern sind, die in einer anderen Periode $(\beta\gamma, k\lambda)$ enthalten sind, geht aus jener hervor, wenn man überall in den Koeffizienten jede beliebige Periode $(\beta\gamma, \mu)$ durch $(\beta\gamma, k\mu)$ ersetzt. Ist also $\alpha = 1$, so werden sämtliche β Perioden mit γ Gliedern durch eine Gleichung vom Grad β bestimmt, deren einzelne Koeffizienten sich auf die Form $A + a(\beta\gamma, 1)$ bringen lassen *und daher bekannte Größen sind*, da $(\beta\gamma, 1) = (n-1, 1) = -1$ gilt. Ist dagegen $\alpha > 1$, so sind die Koeffizienten der Gleichung, deren Wurzeln sämtliche Perioden mit γ Gliedern sind, die in einer gegebenen Periode mit $\beta\gamma$ Gliedern enthalten sind, bekannte Größen, sobald die Zahlenwerte aller α Perioden mit $\beta\gamma$ Gliedern bekannt sind. — Übrigens lässt sich die Berechnung der Koeffizienten dieser Gleichungen oft bequemer ausführen, besonders wenn β nicht sehr klein ist, indem man zuerst die Potenzsummen der Wurzeln ermittelt und daraus nach dem Newtonschen Satz die Koeffizienten ableitet, ebenso wie oben in Artikel 349.

Beispiel I. Gesucht ist für $n = 19$ die Gleichung, deren Wurzeln die Summen $(6, 1)$, $(6, 2), (6, 4)$ sind. Bezeichnen wir diese Wurzeln jeweils mit p, p', p'' und die gesuchte Gleichung mit

$$x^3 - Axx + Bx - C = 0$$

so folgt

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p''$$

Daher ist

$$A = (18, 1) = -1$$

Ferner gilt

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'',$$
$$p'p'' = 3p + p' + 2p''$$

und damit

$$B = 6(p + p' + p'') = 6(18, 1) = -6$$

Schließlich erhält man

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'')$$
$$= 18 - 11 = 7$$

Daher lautet die gesuchte Gleichung

$$x^3 + xx - 6x - 7 = 0$$

Nach der anderen Methode haben wir

$$p + p' + p'' = -1$$

$$pp = 6 + 2p + p' + 2p'', \quad p'p' = 6 + 2p' + p'' + 2p,$$
$$p''p'' = 6 + 2p'' + p + 2p'$$

und somit

$$pp + p'p' + p''p'' = 18 + 5(p + p' + p'') = 13$$

sowie ebenso

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2$$

Daraus wird nach dem Newtonschen Satz dieselbe Gleichung wie zuvor abgeleitet.

II. Gesucht ist für $n = 19$ die Gleichung, deren Wurzeln die Summen $(2,1), (2,7), (2,8)$ sind. Bezeichnet man diese jeweils mit q, q', q'', so findet man

$$q + q' + q'' = (6,1),$$
$$qq' + qq'' + q'q'' = (6,1) + (6,4), \quad qq'q'' = 2 + (6,2)$$

Mit den Bezeichnungen des vorigen Beispiels ist daher die gesuchte Gleichung

$$x^3 - pxx + (p + p'')x - 2 - p' = 0$$

Die Gleichung, deren Wurzeln die Summen $(2,2), (2,3), (2,5)$ sind, die in $(6,2)$ enthalten sind, geht aus der vorhergehenden hervor, wenn man für p, p', p'' jeweils p', p'', p einsetzt; führt man dieselbe Substitution nochmals aus, so entsteht die Gleichung, deren Wurzeln die Summen $(2,4), (2,6)$. $(2,9)$ sind, die in $(6,4)$ enthalten sind.

Auf den vorhergehenden Untersuchungen beruht die Lösung der Gleichung $X = 0$.

352.

Die vorstehenden Sätze mit den angefügten Folgerungen enthalten die Hauptpunkte der gesamten Theorie, und das Verfahren zur Bestimmung der Werte der Wurzeln Ω kann nun kurz angegeben werden.

Zuerst wähle man eine Zahl g, die für den Modul n eine primitive Wurzel ist, und ermittle die kleinsten Reste der Potenzen von g bis g^{n-2} nach dem Modul n. Man zerlege $n - 1$ in Faktoren, und zwar in Primfaktoren, wenn man das Problem auf Gleichungen möglichst niedrigen Grades zurückführen will. Diese seien in völlig beliebiger Reihenfolge $\alpha, \beta, \gamma \ldots \zeta$, und man setze

$$\frac{n-1}{\alpha} = \beta\gamma \ldots \zeta = a, \qquad \frac{n-1}{\alpha\beta} = \gamma \ldots \zeta = b, \quad \text{usw.}$$

Man teile sämtliche Wurzeln Ω in α Perioden mit a Gliedern ein; jede einzelne von diesen wiederum in β Perioden mit b Gliedern, jede einzelne von diesen erneut in γ Perioden usw. Nach dem vorigen Artikel suche man die Gleichung vom Grad α, (A), deren Wurzeln jene α Summen mit a Gliedern sind; ihre Werte werden also durch Lösung dieser Gleichung bekannt.

Hier entsteht aber eine Schwierigkeit, da ungewiss erscheint, welcher Wurzel der Gleichung (A) die einzelnen Summen gleichzusetzen sind, nämlich welche Wurzel mit $(a,1)$, welche mit (a,g) usw. bezeichnet werden soll. Dies lässt sich folgendermaßen beheben. Mit $(a,1)$ kann man eine beliebige Wurzel der Gleichung (A) bezeichnen. Denn jede Wurzel dieser Gleichung ist eine Summe aus a Wurzeln von Ω, und es ist völlig beliebig, welche Wurzel aus Ω mit [1] bezeichnet wird. Daher dürfen wir offenbar annehmen, dass irgendeine der Wurzeln, aus denen eine beliebige gegebene Wurzel der Gleichung (A) besteht, durch [1] dargestellt wird; dann wird jene Wurzel der Gleichung (A) zu $(a,1)$. Die Wurzel [1] ist dadurch aber noch nicht vollständig bestimmt; es bleibt weiterhin völlig beliebig oder unbestimmt, welche der Wurzeln, die $(a,1)$ bilden, wir für [1] nehmen wollen. Sobald aber $(a,1)$ bestimmt ist, lassen sich daraus auch alle übrigen Summen mit a Gliedern rational ableiten (Artikel 346). Daraus geht zugleich hervor, dass man durch Lösung dieser Gleichung nur eine einzige Wurzel zu ermitteln braucht. — Für diesen Zweck kann auch das folgende, weniger direkte Verfahren verwendet werden. Man wähle für [1] eine bestimmte Wurzel, *das heißt*, man setze $[1] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, wobei man die ganze Zahl k beliebig, jedoch so wählt, dass sie durch n nicht teilbar ist. Dann bezeichnen auch [2], [3] usw. bestimmte Wurzeln und daher auch die Summen $(a,1), (a,g)$ usw. bestimmte Größen. Berechnet man diese mit leichter Feder aus Sinustafeln, nämlich so genau, dass sich entscheiden lässt, welche größer und welche kleiner sind, so kann kein Zweifel bleiben, durch welche Bezeichnungen die einzelnen Wurzeln der Gleichung (A) zu unterscheiden sind.

Sind auf diese Weise sämtliche α Summen mit a Gliedern gefunden, so suche man nach dem vorigen Artikel die Gleichung (B) vom Grad β, deren Wurzeln die β Summen mit b Gliedern sind, die in $(a,1)$ enthalten sind; sämtliche Koeffizienten dieser Gleichung sind bekannte Größen. Da noch beliebig ist, welche der $a = \beta b$ Wurzeln unter $(a,1)$ mit [1] bezeichnet wird, kann eine beliebige gegebene Wurzel der Gleichung (B) durch $(b,1)$ ausgedrückt werden, weil man offenbar annehmen darf, dass eine der b Wurzeln, aus denen sie besteht, mit [1] bezeichnet wird. Man suche also durch Lösung der Gleichung (B) eine beliebige Wurzel, setze sie $= (b,1)$ und leite daraus nach Artikel 346 alle übrigen Summen mit b Gliedern ab. Dadurch erhalten wir zugleich eine Probe für die Rechnung, da diejenigen Summen mit b Gliedern, die zu denselben Perioden mit a Gliedern gehören, stets bekannte Summen ergeben müssen. — In einigen Fällen kann es ebenso einfach sein, $\alpha - 1$ weitere Gleichungen vom Grad β zu ermitteln, deren Wurzeln jeweils die einzelnen β Summen mit b Gliedern sind, die in den übrigen Perioden mit a Gliedern, $(a,g), (a,gg)$ usw., enthalten sind, und *alle* Wurzeln sowohl dieser Gleichungen als auch der Gleichung B durch Lösung zu bestimmen. Dann muss man aber ebenso wie oben mithilfe einer Sinustafel entscheiden, welchen Perioden mit b Gliedern die einzelnen so erhaltenen Wurzeln gleichzusetzen sind. Für diese Entscheidung können auch verschiedene andere Kunstgriffe verwendet werden, die hier nicht vollständig erläutert werden können; einen für den Fall $\beta = 2$, der besonders nützlich ist und sich durch Beispiele kürzer als durch Regeln erläutern lässt, wird man jedoch in den folgenden Beispielen kennenlernen.

Sind auf diese Weise die Werte aller $\alpha\beta$ Summen mit b Gliedern gefunden, so können daraus auf ganz ähnliche Weise durch Gleichungen vom Grad γ sämtliche

$\alpha\beta\gamma$ Summen mit c Gliedern bestimmt werden. Man muss nämlich *entweder eine* Gleichung vom Grad γ, deren Wurzeln die γ Summen mit c Gliedern sind, die unter $(b, 1)$ enthalten sind, nach Artikel 350 ermitteln, durch ihre Lösung eine beliebige Wurzel finden und $= (c, 1)$ setzen und schließlich daraus nach Artikel 346 alle übrigen gleichartigen Summen ableiten; *oder* ebenso insgesamt $\alpha\beta$ Gleichungen vom Grad γ aufstellen, deren Wurzeln jeweils die γ Summen mit c Gliedern in den einzelnen Perioden mit b Gliedern sind, die Werte sämtlicher Wurzeln aller dieser Gleichungen durch Lösung bestimmen und schließlich ihre Reihenfolge ebenso wie oben mithilfe einer Sinustafel oder für $\gamma = 2$ durch den unten in den Beispielen zu zeigenden Kunstgriff festlegen.

Fährt man auf diese Weise fort, so erhält man offenbar schließlich sämtliche $\frac{n-1}{\zeta}$ Summen mit ζ Gliedern. Stellt man daher nach Artikel 348 die Gleichung vom Grad ζ auf, deren Wurzeln die ζ Wurzeln aus Ω sind, die in $(\zeta, 1)$ enthalten sind, so sind ihre Koeffizienten sämtlich bekannte Größen. Findet man durch Lösung eine beliebige Wurzel dieser Gleichung, so darf man diese $= [1]$ setzen, und alle übrigen Wurzeln Ω werden durch deren Potenzen erhalten. Wenn man will, können auch alle Wurzeln jener Gleichung durch Lösung ermittelt werden und außerdem durch Lösung von $\frac{n-1}{\zeta} - 1$ weiteren Gleichungen vom Grad ζ, die jeweils alle ζ Wurzeln in den einzelnen übrigen Perioden mit ζ Gliedern darstellen, alle übrigen Wurzeln Ω gefunden werden.

Übrigens ist klar, dass, sobald die erste Gleichung (A) gelöst ist oder die Werte aller α Summen mit a Gliedern bekannt sind, nach Artikel 348 unmittelbar auch die Zerlegung der Funktion X in α Faktoren vom Grad a gegeben ist. Ferner wird nach Lösung der Gleichung (B) oder nachdem die Werte aller $\alpha\beta$ Summen mit b Gliedern gefunden sind, jeder jener Faktoren wiederum in β oder X in $\alpha\beta$ Faktoren vom Grad b zerlegt usw.

353.

Erstes Beispiel für $n = 19$. Da hier $n - 1 = 3.3.2$ gilt, ist die Bestimmung der Wurzeln Ω auf die Lösung zweier kubischer Gleichungen und einer quadratischen Gleichung zurückzuführen. Dieses Beispiel wird umso leichter verständlich sein, als die nötigen Operationen größtenteils schon im Vorhergehenden enthalten sind. Wählt man für die primitive Wurzel g die Zahl 2, so ergeben sich die folgenden kleinsten Reste ihrer Potenzen (die Exponenten der Potenzen stehen in der ersten Zeile über den Resten):

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17
1.	2.	4.	8.	16.	13.	7.	14.	9.	18.	17.	15.	11.	3.	6.	12.	5.	10

Hieraus lässt sich nach den Artikeln 344 und 345 leicht die folgende Einteilung sämtlicher Wurzeln Ω in drei Perioden mit je sechs Gliedern und jeder einzelnen von diesen in drei Perioden mit je zwei Gliedern ableiten:

$$\Omega = (18,1)\begin{cases}(6,1)\begin{cases}(2,1)\ldots & [1],[18]\\ 2,8)\ldots & [8],[11]\\ (2,7)\ldots & [7],[12]\end{cases}\\ (6,2)\begin{cases}(2,2)\ldots & [2],[17]\\ (2,16)\ldots & [3],[16]\\ (2,14)\ldots & [5],[14]\end{cases}\\ (6,4)\begin{cases}(2,4)\ldots & [4],[15]\\ (2,13)\ldots & [6],[13]\\ (2,9)\ldots & [9],[10]\end{cases}\end{cases}$$

Die Gleichung (A), deren Wurzeln die Summen $(6,1),(6,2),(6,4)$ sind, ergibt sich als $x^3 + xx - 6x - 7 = 0$; eine ihrer Wurzeln findet man gleich $-1{,}2218761623$. Bezeichnen wir diese mit $(6,1)$, so wird

$$(6,2) = 4 - (6,1)^2 = 2{,}5070186441$$
$$(6,4) = -5 - (6,1) + (6,1)^2 = -2.2851424818$$

Damit ist X in drei Faktoren vom Grad 6 zerlegt, wenn diese Werte in Artikel 348 eingesetzt werden.

Die Gleichung (B), deren Wurzeln die Summen $(2,1),(2.7),(2,8)$ sind, lautet

$$x^3 - (6,1)xx + ((6,1) + (6,4))x - 2 - (6,2) = 0$$

oder

$$x^3 + 1{,}2218761623xx - 3{,}5070186441x - 4{,}5070186441 = 0$$

Eine ihrer Wurzeln findet man gleich $-1{,}3545631433$, die wir mit $(2,1)$ bezeichnen werden. Nach dem Verfahren von Artikel 346 erhält man aber die folgenden Gleichun-

gen, in denen der Kürze wegen q für $(2,1)$ geschrieben wird:

$$\begin{aligned}
&(2,2) = qq - 2, \quad (2,3) = q^3 - 3q,\\
&(2,4) = q^4 - 4qq + 2, \quad (2,5) = q^5 - 5q^3 + 5q\\
&(2,6) = q^6 - 6q^4 + 9qq - 2,\\
&(2,7) = q^7 - 7q^5 + 14q^3 - 7q\\
&(2,8) = q^8 - 8q^6 + 20q^4 - 16qq + 2,\\
&(2,9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q
\end{aligned}$$

Bequemer als nach den Regeln von Artikel 346 lassen sich diese Gleichungen im vorliegenden Fall durch die folgenden Überlegungen aufstellen. Setzt man

$$[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$$

so folgt

$$\begin{aligned}
[18] &= \cos\frac{18kP}{19} + i\sin\frac{18kP}{19}\\
&= \cos\frac{kP}{19} - i\sin\frac{kP}{19},
\end{aligned}$$

und daher $(2,1) = 2\cos\frac{kP}{19}$, sowie allgemein

$$[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19},$$

und daher $(2,\lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$ Ist also $\frac{1}{2}q = \cos\omega$, so gilt $(2,2) = 2\cos 2\omega, (2,3) = 2\cos 3\omega$ usw.; daraus erhält man nach den bekannten Gleichungen für die Kosinuswerte vielfacher Winkel dieselben Formeln wie oben. — Aus diesen Formeln ergeben sich nun die folgenden Zahlenwerte:

$(2,2) = -0{,}1651586909$	$(2,6) = 0{,}4909709743$
$(2,3) = 1{,}5782810188$	$(2,7) = -1{,}7589475024$
$(2,4) = -1{,}9727226068$	$(2,8) = 1{,}8916344834$
$(2,5) = 1{,}0938963162$	$(2,9) = -0{,}8033908493$

Die Werte von $(2,7), (2,8)$ können auch aus der Gleichung (B) gewonnen werden, deren beide übrigen Wurzeln sie sind. Der Zweifel, welche dieser Wurzeln $(2,7)$ und welche $(2,8)$ ist, lässt sich entweder durch eine Näherungsrechnung nach den vorstehenden Formeln oder durch Sinustafeln beheben. Schon ein flüchtiger Blick in diese zeigt, dass $(2,1) = 2\cos\omega$ gilt, wenn man $\omega = \frac{7}{19}P$ setzt; daraus muss

$$(2,7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P,$$

und $(2,8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$ folgen. Ebenso lassen sich die Summen $(2,2)$, $(2,3), (2,5)$ auch durch die Gleichung

$$x^3 - (6,2)xx + ((6,1) + (6,2))x - 2 - (6,4) = 0$$

finden, deren Wurzeln sie sind; die Ungewissheit, welche Wurzeln jeweils jenen Summen gleichzusetzen sind, wird auf genau dieselbe Weise wie zuvor beseitigt. Ebenso können auch die Summen $(2,4),(2,6),(2,9)$ durch die Gleichung

$$x^3 - (6,4)xx + ((6,2)+(6,4))x - 2 - (6,1) = 0$$

ermittelt werden.

Schließlich sind [1] und [18] die Wurzeln der Gleichung $xx - (2,1)x + 1 = 0$, von denen die eine $= \frac{1}{2}(2,1) + i\sqrt{(1 - \frac{1}{4}(2,1)^2)} = \frac{1}{2}(2,1) + i\sqrt{(\frac{1}{2} - \frac{1}{4}(2,2))}$, die andere $= \frac{1}{2}(2,1) - i\sqrt{(\frac{1}{2} - \frac{1}{4}(2,2))}$ ist; daraus ergeben sich die Zahlenwerte $= -0{,}6772815716 \pm 0{,}7357239107i$. Die sechzehn übrigen Wurzeln können entweder durch Entwicklung der Potenzen einer beliebigen dieser beiden Wurzeln oder durch Lösung von acht anderen ähnlichen Gleichungen abgeleitet werden. Bei dem letzteren Verfahren muss man entweder durch Sinustafeln oder durch den im folgenden Beispiel zu erläuternden Kunstgriff entscheiden, bei welcher Wurzel der imaginäre Teil das positive und bei welcher das negative Vorzeichen erhalten soll. So wurden die folgenden Werte gefunden, wobei das obere Zeichen zur ersten und das untere zur zweiten Wurzel gehören soll:

$$\begin{aligned}
&[1] \text{ und } [18] = -0{,}6772815716 \pm 0{,}7357239107i \\
&[2] \text{ und } [17] = -0{,}0825793455 \mp 0{,}9965844930i \\
&[3] \text{ und } [16] = 0{,}7891405094 \pm 0{,}6142127127i \\
&[4] \text{ und } [15] = -0{,}9863613034 \pm 0{,}1645945903i \\
&[5] \text{ und } [14] = 0{,}5469481581 \mp 0{,}8371664783i \\
&[6] \text{ und } [13] = 0{,}2454854871 \pm 0{,}9694002659i \\
&[7] \text{ und } [12] = -0{,}8794737512 \mp 0{,}4759473930i \\
&[8] \text{ und } [11] = 0{,}9458172417 \mp 0{,}3246994692i \\
&[9] \text{ und } [10] = -0.4016954247 \pm 0{,}9157733267i
\end{aligned}$$

354.

Zweites Beispiel für $n = 17$. Hier gilt $n - 1 = 2.2.2.2$, weshalb die Berechnung der Wurzeln Ω auf vier quadratische Gleichungen zurückzuführen ist. Als primitive Wurzel wählen wir hier die Zahl 3, deren Potenzen die folgenden kleinsten Reste nach dem Modul 17 liefern:

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15
1.	3.	9.	10.	13.	5.	15.	11.	16.	14.	8.	7.	4.	12.	2.	6

Hieraus ergeben sich die folgenden Einteilungen der Menge Ω in zwei Perioden mit je acht, vier mit je vier und acht mit je zwei Gliedern:

$$\Omega = (16,1)\left\{\begin{array}{l}(8,1)\left\{\begin{array}{l}(4,1)\left\{\begin{array}{l}(2,1)\ldots\ [1],[16]\\(2,13)\ldots\ [4],[13]\end{array}\right.\\(4,9)\left\{\begin{array}{l}(2,9)\ldots\ [8],[9]\\(2,15)\ldots\ [2],[15]\end{array}\right.\end{array}\right.\\(8,3)\left\{\begin{array}{l}(4,3)\left\{\begin{array}{l}(2,3)\ldots\ [3],[14]\\(2,5)\ldots\ [5],[12]\end{array}\right.\\(4.10)\left\{\begin{array}{l}(2,10)\ldots\ [7],[10]\\(2,11)\ldots\ [6],[11]\end{array}\right.\end{array}\right.\end{array}\right.$$

Die Gleichung (A), deren Wurzeln die Summen $(8,1),(8,3)$ sind, ergibt sich nach den Regeln von Artikel 351 als $xx + x - 4 = 0$. Ihre Wurzeln berechnet man zu $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}5615528128$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}5615528128$. Die erste setzen wir $= (8,1)$, weshalb die zweite notwendig $= (8,3)$ zu setzen ist.

Ferner ergibt sich die Gleichung, deren Wurzeln die Summen $(4,1)$ und $(4,9)$ sind, als $(B) : xx - (8,1)x - 1 = 0$. Ihre Wurzeln sind $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{(4 + (8,1)^2)} = \frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{(12 + 3(8,1) + 4(8,3))}$. Diejenige, bei der die Wurzelgröße das positive Vorzeichen erhält und deren Zahlenwert 2,0494811777 ist, setzen wir $= (4,1)$; dann muss die andere, bei der die Wurzelgröße negativ genommen wird und deren Wert $-0{,}4879283649$ ist, mit $(4,9)$ bezeichnet werden. Die übrigen Summen mit vier Gliedern, nämlich $(4,3)$ und $(4,10)$, können jedoch auf zwei Arten bestimmt werden. *Erstens* durch das Verfahren von Artikel 346, das die folgenden Formeln liefert, in denen zur Abkürzung für $(4,1)$ der Buchstabe p geschrieben wird:

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0{,}3441507314$$
$$(4,10) = \frac{3}{2} + 2p - pp - \frac{1}{2}p^3 = -2{,}9057035442$$

Dasselbe Verfahren liefert auch die Formel $(4,9) = -1 - 6p + pp + p^3$, aus der sich derselbe Wert ergibt, den wir zuvor angegeben haben. *Zweitens* lassen sich die Summen $(4,3)$, $(4,10)$ auch durch Lösung der Gleichung bestimmen, deren Wurzeln sie sind. Diese Gleichung lautet $xx - (8,3)x - 1 = 0$, weshalb ihre Wurzeln $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{(4+(8,3)^2)}$ oder $\frac{1}{2}(8,3)+\frac{1}{2}\sqrt{(12+4(8,1)+3(8,3))}$ und $\frac{1}{2}(8,3)-\frac{1}{2}\sqrt{(12+4(8,1)+3(8,3))}$ sind. Der Zweifel, *welche* Wurzel mit $(4,3)$ und welche mit $(4,10)$ bezeichnet werden muss, wird durch den folgenden Kunstgriff beseitigt, den wir in Artikel 352 erwähnt haben. Man entwickle das Produkt aus $(4,1) - (4,9)$ und $(4,3) - (4,10)$; dabei ergibt sich $2(8,1) - 2(8,3)$[*)] Der Wert dieses Ausdrucks ist nun offenbar positiv, nämlich $= +2\sqrt{17}$, und auch der erste Faktor des Produkts, $(4,1) - (4,9)$, ist positiv, nämlich $= +\sqrt{(12 + 3(8,1) + 4(8,3))}$. Daher muss notwendig auch der andere Faktor $(4,3) - (4,10)$ positiv sein, und folglich ist $(4,3)$ der *ersten* Wurzel, bei der das positive Vorzeichen vor der Wurzelgröße steht, und $(4,10)$ der zweiten gleichzusetzen. Hieraus ergeben sich dieselben Zahlenwerte wie oben.

Nachdem sämtliche Summen mit vier Gliedern gefunden sind, gehen wir zu den Summen mit zwei Gliedern über. Die Gleichung (C), deren Wurzeln $(2,1),(2,13)$ sind, die in $(4,1)$ enthalten sind, ergibt sich als $xx - (4,1)x + (4,3) = 0$. Ihre Wurzeln sind $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(-4(4,3) + (4,1)^2)}$ oder $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(4 + (4,9) - 2(4,3))}$. Diejenige, bei der die Wurzelgröße positiv genommen wird und deren Wert sich als $= 1{,}8649444588$ ergibt, setzen wir $= (2,1)$; dann wird $(2,13)$ der anderen gleich, deren Wert $= 0{,}1845367189$ ist. Will man die übrigen Summen mit zwei Gliedern nach dem Verfahren von Artikel 346 bestimmen, so können für $(2,2),(2,3),(2,4)$,

[*)] Das eigentliche Wesen dieses Kunstgriffs besteht darin, dass man a priori vorhersehen konnte, dass das entwickelte Produkt keine Summen mit vier Gliedern enthalten würde, sondern sich allein durch Summen mit acht Gliedern darstellen ließe. Den Grund dafür, der hier der Kürze wegen übergangen werden muss, werden mit dem Gegenstand Vertraute sehr leicht erkennen.

$(2,5),(2,6),(2,7),(2,8)$ dieselben Formeln verwendet werden, die wir im vorigen Beispiel für die ebenso bezeichneten Größen angegeben haben, nämlich $(2,2)$, (oder $(2,15)$), $=(2,1)^2-2$ usw. Will man sie dagegen lieber paarweise durch Lösung einer quadratischen Gleichung berechnen, so findet man für $(2,9),(2,15)$ die Gleichung $xx-(4,9)x+(4,10)=0$, deren Wurzeln $\frac{1}{2}(4,9)\pm\frac{1}{2}\sqrt{(4+(4,1)-2(4,10))}$ sind. Wie hier über das doppelte Vorzeichen zu entscheiden ist, lässt sich auf dieselbe Weise wie oben bestimmen. Entwickelt man nämlich das Produkt aus $(2,1)-(2,13)$ und $(2,9)-(2,15)$, so erhält man $-(4,1)+(4,9)-(4,3)+(4,10)$. Da dies offenbar negativ, der Faktor $(2,1)-(2,13)$ aber positiv ist, muss notwendig $(2,9)-(2,15)$ negativ sein; daher ist in dem zuvor angegebenen Ausdruck für $(2,15)$ das obere, positive und für $(2,9)$ das untere, negative Vorzeichen zu wählen. Daraus berechnet man $(2,9)=-1{,}9659461994$, $(2,15)=1{,}4780178344$. — Da ebenso aus der Entwicklung des Produkts aus $(2,1)-(2,13)$ und $(2,3)-(2,5)$ der Ausdruck $(4,9)-(4,10)$ und damit eine positive Größe hervorgeht, schließen wir, dass der Faktor $(2,3)-(2,5)$ positiv ist. Eine ähnliche Rechnung wie zuvor liefert dann

$$\begin{aligned}(2,3)&=\tfrac{1}{2}(4,3)+\tfrac{1}{2}\sqrt{(4+(4,10)-2(4,9))}\\&=0{,}8914767116\\(2,5)&=\tfrac{1}{2}(4,3)-\tfrac{1}{2}\sqrt{(4+(4,10)-2(4,9))}\\&=-0{,}5473259801\end{aligned}$$

Schließlich erhält man durch ganz entsprechende Operationen

$$\begin{aligned}(2,10)&=\tfrac{1}{2}(4,10)-\tfrac{1}{2}\sqrt{(4+(4,3)-2(4,1))}\\&=-1{,}7004342715\\(2,11)&=\tfrac{1}{2}(4,10)+\tfrac{1}{2}\sqrt{(4+(4,3)-2(4,1))}\\&=-1{,}2052692728\end{aligned}$$

Es bleibt, zu den Wurzeln Ω selbst herabzusteigen. Die Gleichung (D), deren Wurzeln [1] und [16] sind, lautet $xx-(2,1)x+1=0$, woraus sich die Wurzeln $\frac{1}{2}(2,1)\pm\frac{1}{2}\sqrt{((2,1)^2-4)}$ oder vielmehr $\frac{1}{2}(2,1)\pm i\sqrt{(4-(2,1)^2)}$ oder $\frac{1}{2}(2,1)\pm\frac{1}{2}i\sqrt{(2-(2,15))}$ ergeben. Für [1] wählen wir das obere, für [16] das untere Vorzeichen. Die vierzehn übrigen Wurzeln erhält man entweder durch die Potenzen von [1] oder durch Lösung von sieben quadratischen Gleichungen, von denen jede zwei Wurzeln liefert; dabei lässt sich die Ungewissheit über die Vorzeichen der Wurzelgrößen durch denselben Kunstgriff wie zuvor beseitigen. So sind [4] und [13] die Wurzeln der Gleichung $xx-(2,13)x+1=0$ und daher $\frac{1}{2}(2,13)\pm\frac{1}{2}i\sqrt{(2-(2,9))}$. Aus der Entwicklung des Produkts aus $[1]-[16]$ und $[4]-[13]$ ergibt sich aber $(2,5)-(2,3)$ und damit eine negative reelle Größe. Da nun $[1]-[16]$ gleich $+i\sqrt{(2-(2,15))}$ ist, also das Produkt der imaginären Größe i mit einer *positiven* reellen Größe, muss auch $[4]-[13]$ das Produkt von i mit einer *positiven* reellen Größe sein, da $ii=-1$ gilt. Daraus folgt, dass für [4] das obere und für [13] das untere Vorzeichen zu nehmen ist. Ebenso findet man für die Wurzeln [8] und [9] den Ausdruck $\frac{1}{2}(2,9)\pm\frac{1}{2}i\sqrt{(2-(2,1))}$. Da das Produkt aus $[1]-[16]$ und $[8]-[9]$ gleich $(2,9)-(2,10)$ und daher negativ ist, muss für [8] das obere und für [9] das untere Vorzeichen gewählt werden. Berechnen wir die übrigen

Wurzeln auf dieselbe Weise, so erhalten wir die folgenden Zahlenwerte, wobei die oberen Vorzeichen zu den ersten und die unteren zu den zweiten Wurzeln gehören sollen:

$$\begin{aligned}
[1],\ [16] \quad &\ldots \quad 0{,}9324722294 \pm 0{,}3612416662i \\
[2],\ [15] \quad &\ldots \quad 0{,}7390089172 \pm 0{,}6736956436i \\
[3],\ [14] \quad &\ldots \quad 0{,}4457383558 \pm 0{,}8951632914i \\
[4],\ [13] \quad &\ldots \quad 0{,}0922683595 \pm 0{,}9957341763i \\
[5],\ [12] \quad &\ldots \quad -0{,}2736629901 \pm 0{,}9618256432i \\
[6],\ [11] \quad &\ldots \quad -0{,}6026346364 \pm 0{,}7980172273i \\
[7],\ [10] \quad &\ldots \quad -0{,}8502171357 \pm 0{,}5264321629i \\
[8],\ [9] \quad &\ldots \quad -0{,}9829730997 \pm 0{,}1837495178i
\end{aligned}$$

* *
*

Das Vorstehende könnte zwar zur Lösung der Gleichung $x^n - 1 = 0$ und damit auch zur Bestimmung der trigonometrischen Funktionen ausreichen, die zu Bogen gehören, welche mit dem Umfang kommensurabel sind. Wegen der Bedeutung des Gegenstands können wir diese Untersuchung jedoch nicht abschließen, ohne zuvor aus der Fülle sowohl der ihn erläuternden Beobachtungen als auch der mit ihm verwandten oder von ihm abhängigen Sätze einiges hier anzufügen. Dabei werden wir vor allem solche auswählen, die sich ohne einen umfangreichen Apparat anderer Untersuchungen erledigen lassen; wir wollen sie nur als *Proben* dieser sehr umfassenden, künftig ausführlich zu behandelnden Theorie betrachtet wissen.

Weitere Untersuchungen über die Perioden der Wurzeln.
Summen mit einer geraden Anzahl von Gliedern sind reelle Größen.

355.

Da n stets als ungerade vorausgesetzt wird, gehört 2 zu den Faktoren von $n-1$, und die Menge Ω besteht aus $\frac{1}{2}(n-1)$ Perioden mit zwei Gliedern. Eine solche Periode wie $(2,\lambda)$ besteht aus den Wurzeln $[\lambda]$ und $[\lambda g^{\frac{1}{2}(n-1)}]$, wobei g wie oben eine beliebige primitive Wurzel für den Modul n bezeichnet. Es gilt aber $g^{\frac{1}{2}(n-1)} \equiv -1 \pmod{n}$ und daher $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (siehe Artikel 62), woraus $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$ folgt. Setzt man also $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$ und daher $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, so ergibt sich die Summe $(2,\lambda) = 2\cos\frac{kP}{n}$. Daraus ziehen wir hier nur den Schluss, dass der Wert jeder Summe mit zwei Gliedern eine reelle Größe ist. Da sich jede Periode, deren Gliederzahl gerade $= 2a$ ist, in a Perioden mit je zwei Gliedern zerlegen lässt, ist allgemeiner klar, dass der Wert jeder Summe, deren Gliederzahl gerade ist, stets eine reelle Größe ist. Wird also in Artikel 352 unter den Faktoren α, β, γ usw. der Faktor zwei für die letzte Stelle aufgespart, so werden sämtliche Operationen bis zu den Summen mit zwei Gliedern durch reelle Größen ausgeführt; imaginäre Größen werden erst dann eingeführt, wenn man von diesen Summen zu den Wurzeln selbst übergeht.

Über die Gleichung, die die Verteilung der Wurzeln Ω in zwei Perioden bestimmt.

356.

Die Hilfsgleichungen, durch die für jeden Wert von n die Summen bestimmt werden, welche die Menge Ω bilden, verdienen höchste Aufmerksamkeit: Sie hängen auf bemerkenswerte Weise mit den verborgensten Eigenschaften der Zahl n zusammen. Hier wollen wir die Untersuchung jedoch auf die folgenden zwei Fälle beschränken: *Erstens* behandeln wir die quadratische Gleichung, deren Wurzeln die Summen mit $\frac{1}{2}(n-1)$ Gliedern sind; *zweitens*, für den Fall, dass $n-1$ den Faktor 3 enthält, die kubische Gleichung, deren Wurzeln die Summen mit $\frac{1}{3}(n-1)$ Gliedern sind.

Schreiben wir der Kürze wegen m für $\frac{1}{2}(n-1)$ und bezeichnen wir mit g eine beliebige primitive Wurzel für den Modul n, so besteht die Menge Ω aus zwei Perioden $(m,1)$ und (m,g); die erste enthält die Wurzeln $[1], [gg], [g^4] \ldots [g^{n-3}]$, die zweite $[g]$, $[g^3], [g^5] \ldots [g^{n-2}]$. Die kleinsten positiven Reste der Zahlen $gg, g^4 \ldots g^{n-3}$ nach dem Modul n seien in beliebiger Reihenfolge R, R', R'' usw.; ebenso seien die Reste von $g, g^3, g^5 \ldots g^{n-2}$ gleich N, N', N'' usw. Dann stimmen die Wurzeln, aus denen $(m,1)$ besteht, mit $[1], [R], [R'], [R'']$ usw. überein und die Wurzeln der Periode (m,g) mit $[N], [N'], [N'']$ usw. Nun ist klar, dass sämtliche Zahlen $1, R, R', R''$ usw. *quadratische Reste* der Zahl n sind; da sie sämtlich verschieden und kleiner als n sind und ihre Anzahl $= \frac{1}{2}(n-1)$, also gleich der Anzahl aller positiven Reste von n unterhalb n ist, stimmen diese Reste genau mit jenen Zahlen überein. Daraus folgt unmittelbar, dass sämtliche Zahlen N, N', N'' usw., die sowohl untereinander als auch von $1, R, R'$ usw. verschieden sind und zusammen mit diesen alle Zahlen $1, 2, 3 \ldots n-1$ erschöpfen, mit sämtlichen positiven *quadratischen Nichtresten* von n unterhalb n übereinstimmen

müssen. Setzt man nun voraus, dass die Gleichung, deren Wurzeln die Summen $(m,1)$, (m,g) sind,

$$xx - Ax + B = 0$$

lautet, so gilt

$$A = (m,1) + (m,g) = -1, \quad B = (m,1) \times (m,g)$$

Das Produkt aus $(m,1)$ und (m,g) ist nach Artikel 345

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{usw.} = W$$

und lässt sich daher auf eine Form wie $\alpha(m,0) + \beta(m,1) + \gamma(m,g)$ bringen. Zur Bestimmung der Koeffizienten α, β, γ bemerken wir *erstens*, dass $\alpha + \beta + \gamma = m$ gilt (da die Anzahl der Summen in $W = m$ ist); *zweitens*, dass $\beta = \gamma$ gilt (dies folgt aus Artikel 350, weil das Produkt $(m,1) \times (m,g)$ eine symmetrische Funktion der Summen $(m,1), (m,g)$ ist, aus denen die größere Summe $(n-1,1)$ besteht); *drittens*: Da sämtliche Zahlen $N+1, N'+1, N''+1$ usw. strikt zwischen den Grenzen 2 und $n+1$ liegen, ist klar, dass entweder keine Summe in W auf $(m,0)$ zurückgeführt wird und daher $\alpha = 0$ gilt, wenn unter den Zahlen N, N', N'' usw. die Zahl $n-1$ nicht vorkommt; oder genau eine, nämlich (m,n), sodass $\alpha = 1$ gilt, wenn $n-1$ unter den Zahlen N, N', N'' usw. vorkommt. Daraus schließen wir, dass im ersten Fall $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$, im zweiten $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$ gilt. Zugleich folgt daraus, da die Zahlen β und γ notwendig ganz sind, dass der erste Fall eintritt, also $n-1$ (oder, was dasselbe ist, -1) unter den Nichtresten von n nicht vorkommt, wenn m gerade, also n von der Form $4k+1$ ist; der zweite Fall tritt dagegen ein, also $n-1$ oder -1 kommt unter den Nichtresten von n vor, wenn m ungerade, also n von der Form $4k+3$ ist[*)]. Daher ist das gesuchte Produkt wegen $(m,0) = m$, $(m,1) + (m,g) = -1$ im ersten Fall $= -\frac{1}{2}m$, im zweiten $= \frac{1}{2}(m+1)$, und die gesuchte Gleichung lautet in jenem Fall $xx + x - \frac{1}{4}(n-1) = 0$, deren Wurzeln $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$ sind, in diesem dagegen $xx + x + \frac{1}{4}(n+1) = 0$, deren Wurzeln $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$ sind.

Welche Wurzel aus Ω also auch für [1] gewählt wurde, die Differenz zwischen den Summen $\Sigma[\mathfrak{R}]$ und $\Sigma[\mathfrak{N}]$, wobei für $\mathfrak{R}$ sämtliche positiven quadratischen Reste und für $\mathfrak{N}$ sämtliche positiven quadratischen Nichtreste von n unterhalb n einzusetzen sind, ist $= \pm\sqrt{n}$ für $n \equiv 1$ und $= \pm i\sqrt{n}$ für $n \equiv 3 \pmod 4$. Ebenso folgt daraus leicht, wenn k eine beliebige ganze, durch n nicht teilbare Zahl bezeichnet, dass

$$\Sigma \cos \frac{k\mathfrak{R}P}{n} - \Sigma \cos \frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{und}$$
$$\Sigma \sin \frac{k\mathfrak{R}P}{n} - \Sigma \sin \frac{k\mathfrak{N}P}{n} = 0$$

für $n \equiv 1 \pmod 4$ gilt; dagegen ist für $n \equiv 3 \pmod 4$ jene Differenz $= 0$, diese $= \pm\sqrt{n}$. Diese Sätze sind wegen ihrer Eleganz sehr bemerkenswert. Übrigens bemerken

[*)] Auf diese Weise haben wir einen neuen Beweis des Satzes erhalten, dass -1 ein Rest aller Primzahlen von der Form $4k+1$ und ein Nichtrest aller der Form $4k+3$ ist, der oben (Artikel 108, 109 und 262) bereits auf mehrere verschiedene Arten bewiesen wurde. Will man diesen Satz lieber voraussetzen, so braucht man zur Unterscheidung der beiden verschiedenen Fälle die Bedingung nicht zu berücksichtigen, dass β, γ schon an sich ganze Zahlen sind.

wir, dass die oberen Vorzeichen immer gelten, wenn für k die Einheit oder allgemeiner ein quadratischer Rest von n genommen wird, die unteren, wenn für k ein Nichtrest gewählt wird, und dass sich diese Sätze unter Wahrung oder vielmehr Steigerung ihrer Eleganz auch auf beliebige zusammengesetzte Werte von n ausdehnen lassen. Über diese Dinge, die einer tieferen Untersuchung bedürfen, müssen wir hier jedoch schweigen und ihre Betrachtung einer anderen Gelegenheit vorbehalten

Beweis des in Abschnitt IV erwähnten Satzes.

357.

Die Gleichung vom Grad m, deren Wurzeln die m Wurzeln in der Periode $(m,1)$ sind, sei

$$x^m - ax^{m-1} + bx^{m-2} - \text{usw.} = 0$$

oder $z = 0$. Dann ist $a = (m,1)$, und jeder der übrigen Koeffizienten b usw. hat eine Form wie $\mathfrak{A} + \mathfrak{B}(m,1) + \mathfrak{C}(m,g)$, wobei $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ganze Zahlen sind (Artikel 348). Bezeichnen wir mit z' die Funktion, in die z übergeht, wenn überall $(m,1)$ durch (m,g) und (m,g) durch (m,gg) oder, was dasselbe ist, durch $(m,1)$ ersetzt wird, so sind die Wurzeln der Gleichung $z' = 0$ die in (m,g) enthaltenen Wurzeln, und das Produkt ist

$$zz' = \frac{x^n - 1}{x - 1} = X$$

Damit lässt sich z auf eine Form wie $R + S(m,1) + T(m,g)$ bringen, wobei R, S, T Polynome in x sind, deren sämtliche Koeffizienten ebenfalls ganze Zahlen sind. Dann gilt

$$z' = R + S(m,g) + T(m,1)$$

Schreiben wir nun der Kürze wegen p und q für $(m,1)$ bzw. (m,g), so folgt

$$\begin{aligned} 2z &= 2R + (S+T)(p+q) - (T-S)(p-q) \\ &= 2R - S - T - (T-S)(p-q) \end{aligned}$$

und ebenso

$$2z' = 2R - S - T + (T-S)(p-q)$$

Setzen wir daher

$$2R - S - T = Y, \quad T - S = Z$$

so ergibt sich $4X = YY - (p-q)^2 ZZ$ und, da $(p-q)^2 = \pm n$ gilt,

$$4X = YY \mp nZZ$$

Dabei gilt das obere Vorzeichen, wenn n von der Form $4k+1$ ist, das untere, wenn n von der Form $4k+3$ ist. Dies ist der Satz, dessen Beweis wir oben (Artikel 124) versprochen haben. Man sieht leicht, dass die beiden höchsten Glieder der Funktion Y stets $2x^m + x^{m-1}$ sind und das höchste Glied der Funktion Z gleich x^{m-1} ist. Die übrigen Koeffizienten, die offenbar sämtlich ganze Zahlen sind, ändern sich mit der unterschiedlichen Beschaffenheit der Zahl n und lassen sich nicht durch eine allgemeine analytische Formel angeben.

Beispiel. Für $n = 17$ ergibt sich die Gleichung, deren Wurzeln die acht in $(8,1)$ enthaltenen Wurzeln sind, nach den Regeln von Artikel 348 als

$$\begin{aligned} x^8 - px^7 + (4+p+2q)x^6 - (4p+3q)x^5 + (6+3p+5q)x^4 \\ - (4p+3q)x^3 + (4+p+2q)xx - px + 1 = 0 \end{aligned}$$

Daraus folgt

$$R = x^8 + 4x^6 + 6x^4 + 4xx + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$$

und hieraus

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5xx + x + 2$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + xx + x$$

Hier sind noch einige weitere Beispiele:

n	Y	Z
3	$2x + 1$	1
5	$2xx + x + 2$	x
7	$2x^3 + xx - x - 2$	$xx + x.$
11	$2x^5 + x^4 - 2x^3 + 2xx - x - 2$	$x^4 + x$
13	$2x^6 + x^5 + 4x^4 - x^3 + 4xx + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4xx - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5xx - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + xx + x$

Über die Gleichung für die Verteilung der Wurzeln Ω in drei Perioden.

358.

Wir gehen zur Betrachtung der kubischen Gleichungen über, durch die für den Fall, dass n von der Form $3k + 1$ ist, die drei Summen mit $\frac{1}{3}(n-1)$ Gliedern bestimmt werden, welche die Menge Ω bilden. Es sei g eine beliebige primitive Wurzel für den Modul n und wir setzen $\frac{1}{3}(n-1) = m$, wobei der so bestimmte Wert eine gerade ganze Zahl ist. Dann sind die drei Summen, aus denen Ω besteht, $(m, 1), (m, g), (m, gg)$, für die wir jeweils p, p', p'' schreiben werden. Offenbar enthält die erste die Wurzeln $[1], [g^3], [g^6] \ldots [g^{n-4}]$, die zweite $[g], [g^4] \ldots [g^{n-3}]$ und die dritte $[gg], [g^5] \ldots [g^{n-2}]$. Setzen wir voraus, dass die gesuchte Gleichung

$$x^3 - Axx + Bx - C = 0$$

lautet, so gilt

$$A = p + p' + p'', \quad B = pp' + p'p'' + pp'',$$
$$C = pp'p''$$

woraus sich sogleich $A = -1$ ergibt. Die kleinsten positiven Reste der Zahlen g^3, $g^6 \ldots g^{n-4}$ nach dem Modul n seien in beliebiger Reihenfolge $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw., und $\mathfrak{K}$ sei deren Menge nach Hinzunahme der Zahl 1. Ebenso seien $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ usw. die kleinsten Reste der Zahlen $g, g^4, g^7 \ldots g^{n-3}$ und $\mathfrak{K}'$ deren Menge; schließlich seien $\mathfrak{A}''$, $\mathfrak{B}'', \mathfrak{C}''$ usw. die kleinsten Reste von $gg, g^5, g^8 \ldots g^{n-2}$ und $\mathfrak{K}''$ deren Menge. Dann sind

sämtliche Zahlen in $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ verschieden und stimmen mit $1, 2, 3 \ldots n-1$ überein. Vor allem ist hier zu bemerken, dass die Zahl $n-1$ notwendig in $\mathfrak{K}$ vorkommt, da man leicht sieht, dass sie der Rest von $g^{\frac{3m}{2}}$ ist. Daraus folgt auch leicht, dass zwei Zahlen wie $h, n-h$ stets in *derselben* der drei Mengen $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ vorkommen. Ist nämlich die eine der Rest der Potenz g^{λ}, so ist die andere der Rest der Potenz $g^{\lambda+\frac{3m}{2}}$ oder der Potenz $g^{\lambda-\frac{3m}{2}}$, wenn $\lambda > \frac{3m}{2}$ gilt. Mit dem Zeichen $(\mathfrak{K}\mathfrak{K})$ bezeichnen wir die Anzahl der Zahlen in der Reihe $1, 2, 3 \ldots n-1$, die sowohl selbst als auch zusammen mit den unmittelbar folgenden, um eine Einheit größeren Zahlen in $\mathfrak{K}$ enthalten sind. Ebenso sei $(\mathfrak{K}\mathfrak{K}')$ die Anzahl der Zahlen in derselben Reihe, die selbst in $\mathfrak{K}$, deren unmittelbare Nachfolger aber in $\mathfrak{K}'$ enthalten sind. Damit ist zugleich die Bedeutung der Zeichen $(\mathfrak{K}\mathfrak{K}''), (\mathfrak{K}'\mathfrak{K}), (\mathfrak{K}'\mathfrak{K}'), (\mathfrak{K}'\mathfrak{K}''), (\mathfrak{K}''\mathfrak{K}), (\mathfrak{K}''\mathfrak{K}'), (\mathfrak{K}''\mathfrak{K}'')$ unmittelbar klar. Ich behaupte nun *erstens*, dass $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$ gilt. Sind nämlich h, h', h'' usw. sämtliche Zahlen der Reihe $1, 2, 3 \ldots n-1$, die selbst in $\mathfrak{K}$ enthalten sind, deren nächstgrößere Zahlen $h+1, h'+1, h''+1$ usw. aber in $\mathfrak{K}'$ enthalten sind, und deren Anzahl daher $= (\mathfrak{K}\mathfrak{K}')$ ist, so sind offenbar sämtliche Zahlen $n-h-1$, $n-h'-1, n-h''-1$ usw. in $\mathfrak{K}'$ und die nächstgrößeren $n-h, n-h'$ usw. in $\mathfrak{K}$ enthalten. Da es insgesamt $(\mathfrak{K}'\mathfrak{K})$ solche Zahlen gibt, kann gewiss nicht $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$ gelten; ebenso beweist man, dass $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$ nicht gelten kann. Daher müssen diese Zahlen notwendig gleich sein. Auf ganz dieselbe Weise beweist man $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. Zweitens: Da auf jede Zahl aus $\mathfrak{K}$ mit Ausnahme der größten, $n-1$, notwendig eine unmittelbar folgende Zahl kommt, die entweder in $\mathfrak{K}$, in $\mathfrak{K}'$ oder in $\mathfrak{K}''$ enthalten ist, ist die Summe $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ gleich der um eine Einheit verminderten Anzahl sämtlicher Zahlen in $\mathfrak{K}$, also $= m-1$. Aus einem ähnlichen Grund gilt

$$\begin{aligned}&(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'')\\ &= (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m\end{aligned}$$

Nach diesen Vorbereitungen entwickeln wir nach den Regeln von Artikel 345 das Produkt pp' in $(m, \mathfrak{A}'+1) + (m, \mathfrak{B}'+1) + (m, \mathfrak{C}'+1) +$ usw.. Dieser Ausdruck lässt sich, wie man leicht sieht, auf $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$ zurückführen. Da nach Artikel 345 I das Produkt $p'p''$ daraus entsteht, wenn man $(m,1), (m,g), (m,gg)$ jeweils durch $(m,g), (m,gg), (mg^3)$, das heißt p, p', p'' jeweils durch p', p'', p ersetzt, gilt $p'p'' = (\mathfrak{K}'\mathfrak{K})p' + (\mathfrak{K}'\mathfrak{K}')p'' + (\mathfrak{K}'\mathfrak{K}'')p$ und auf ganz ähnliche Weise $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$. Hieraus folgt unmittelbar *erstens*

$$B = m(p + p' + p'') = -m$$

zweitens: Da sich auf ähnliche Weise wie zuvor pp' auch pp'' auf $(\mathfrak{K}''\mathfrak{K})p + (\mathfrak{K}''\mathfrak{K}')p' + (\mathfrak{K}''\mathfrak{K}'')p''$ zurückführen lässt und dieser Ausdruck mit dem vorigen identisch sein muss, gilt notwendig $(\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}'\mathfrak{K}')$ und $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K})$. Setzen wir nun

$$\begin{aligned}(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}') &= a,\\ (\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') &= b,\\ (\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') &= c\end{aligned}$$

so ergibt sich $m-1 = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K}) + b + c$ und $a+b+c = m$, also $(\mathfrak{K}\mathfrak{K}) = a-1$. Damit sind jene neun unbekannten Größen auf drei, a, b, c, oder

vielmehr wegen der Gleichung $a+b+c=m$ auf zwei zurückgeführt. Schließlich ist klar, dass sich das Quadrat pp in $(m,1+1)+(m,\mathfrak{A}+1)+(m,\mathfrak{B}+1)+(m,\mathfrak{C}+1)+$ usw. entwickeln lässt. Unter den Teilen dieses Ausdrucks findet sich (m,n), das auf $(m,0)$ oder auf m zurückgeführt wird; die übrigen Teile lassen sich offenbar auf $(\mathfrak{K}\mathfrak{K})p+(\mathfrak{K}\mathfrak{K}')p'+(\mathfrak{K}\mathfrak{K}'')p''$ zurückführen, sodass $pp=m+(a-1)p+bp'+cp''$ gilt.

So haben wir durch die vorstehenden Untersuchungen diese vier Umformungen erhalten.

$$\begin{aligned} pp &= m+(a-1)p+bp'+cp'' \\ pp' &= bp+cp'+ap'' \\ pp'' &= cp+ap'+bp'' \\ p'p'' &= ap+bp'+cp'' \end{aligned}$$

Dabei besteht zwischen den drei Unbekannten a,b,c die Bedingungsgleichung

$$a+b+c=m \quad \ldots\ldots\ldots\ldots \text{ (I)}$$

und außerdem ist sicher, dass sie ganze Zahlen sind. Daraus folgt

$$\begin{aligned} C=p\times p'p'' &= app+bpp'+cpp'' \\ &= am+(aa+bb+cc-a)p \\ &\quad +(ab+bc+ac)p'+(ab+bc+ac)p'' \end{aligned}$$

Da aber $pp'p''$ eine symmetrische Funktion der Summen p,p',p'' ist, müssen die Koeffizienten, mit denen diese im vorstehenden Ausdruck multipliziert werden, notwendig gleich sein (Artikel 350). Daher erhalten wir die neue Gleichung

$$aa+bb+cc-a=ab+bc+ac \quad \ldots \text{ (II)}$$

und daraus $C=am+(ab+bc+ac)(p+p'+p'')$ oder, wegen I und $p+p'+p''=-1$,

$$C=aa-bc \quad \ldots\ldots \text{ (III)}$$

Obwohl nun C hier von drei Unbekannten abhängt, zwischen denen nur zwei Gleichungen bestehen, genügen diese dennoch zusammen mit der Bedingung, dass a,b,c ganze Zahlen sind, zur vollständigen Bestimmung von C. Um dies zu zeigen, schreiben wir die Gleichung II als

$$\begin{aligned} 12a+12b+12c+4 = {} & 36aa+36bb+36cc \\ & -36ab-36ac-36bc \\ & -24a+12b+12c+4 \end{aligned}$$

Die linke Seite wird nach I zu $=12m+4=4n$; die rechte lässt sich auf

$$(6a-3b-3c-2)^2+27(b-c)^2$$

oder, wenn wir k für $2a-b-c$ schreiben, auf $(3k-2)^2+27(b-c)^2$ zurückführen. Daraus ist klar, dass sich die Zahl $4n$ (das heißt allgemein das Vierfache einer beliebigen

Primzahl von der Form $3m + 1$) durch die Form $xx + 27yy$ darstellen lässt. Dies lässt sich zwar ohne Schwierigkeit aus der allgemeinen Theorie der binären Formen ableiten, doch ist es recht bemerkenswert, dass eine solche Zerlegung mit den Werten von a, b, c zusammenhängt. Die Zahl $4n$ lässt sich aber stets nur auf eine einzige Weise in ein Quadrat und das 27-Fache eines Quadrats zerlegen, was wir folgendermaßen beweisen*). Setzen wir

$$4n = tt + 27uu = t't' + 27u'u'$$

voraus, so gilt *erstens*

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16nn$$

zweitens

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16nn$$

drittens

$$(tu' + t'u)(tu' - t'u) = 4n(u'u' - uu)$$

Aus der dritten Gleichung folgt, dass n, da es eine Primzahl ist, eine der Zahlen $tu' + t'u, tu' - t'u$ teilt; aus der ersten und zweiten ist aber klar, dass jede dieser Zahlen kleiner als n ist. Daher muss diejenige, die durch n teilbar ist, notwendig $= 0$ sein, und somit auch $u'u' - uu = 0$, woraus $u'u' = uu$ und $t't' = tt$ folgt; jene beiden Zerlegungen unterscheiden sich also nicht. Setzen wir daher die Zerlegung von $4n$ in ein Quadrat und das 27-Fache eines Quadrats als bekannt voraus (man kann sie entweder nach dem direkten Verfahren von Abschnitt V oder nach dem in den Artikeln 323 und 324 angegebenen indirekten Verfahren ermitteln), gilt also $4n = MM + 27NN$, so sind die Quadrate $(3k-2)^2, (b-c)^2$ bestimmt, und wir haben nun anstelle der Gleichung II zwei Gleichungen erhalten. Man sieht aber leicht, dass nicht nur das Quadrat $(3k - 2)^2$, sondern auch die Wurzel $3k - 2$ selbst vollständig bestimmt ist. Da diese notwendig entweder $= +M$ oder $= -M$ sein muss, wird die Zweideutigkeit dadurch beseitigt, dass k eine ganze Zahl sein muss. Daher setzt man $3k - 2 = +M$ oder $= -M$, je nachdem, ob M von der Form $3z + 1$ oder $3z + 2$ ist†). Da nun $k = 2a - b - c = 3a - m$ gilt, ist $a = \frac{1}{3}(m + k),\ b + c = m - a = \frac{1}{3}(2m - k)$, sodass

$$\begin{aligned} C = aa - bc &= aa - \tfrac{1}{4}(b + c)^2 + \tfrac{1}{4}(b - c)^2 \\ &= \tfrac{1}{9}(m + k)^2 - \tfrac{1}{36}(2m - k)^2 + \tfrac{1}{4}NN \\ &= \tfrac{1}{12}kk + \tfrac{1}{3}km + \tfrac{1}{4}NN \end{aligned}$$

gilt; damit sind sämtliche Koeffizienten der gesuchten Gleichung gefunden. *Q.E.F.* — Diese Formel wird noch einfacher, wenn für NN sein Wert aus der Gleichung $(3k - 2)^2 + 27NN = 4n = 12m + 4$ eingesetzt wird; nach ausgeführter Rechnung ergibt sich

$$C = \tfrac{1}{9}(m + k + 3km) = \tfrac{1}{9}(m + kn)$$

*) Dieser Satz ließe sich unmittelbarer aus den Grundsätzen von Abschnitt V beweisen.

†) Offenbar kann M nicht von der Form $3z$ sein, da sonst $4n$ durch 3 teilbar wäre. — Die Zweideutigkeit, ob $b - c = N$ oder $= -N$ zu setzen ist, braucht hier nicht berücksichtigt zu werden und lässt sich auch der Natur der Sache nach auf keine Weise beseitigen, da sie von der Wahl der primitiven Wurzel g abhängt: Für einige primitive Wurzeln ist die Differenz $b - c$ positiv, für andere negativ.

Derselbe Wert lässt sich auch auf $(3k-2)NN+k^3-2kk+k-km+m$ zurückführen. Dieser Ausdruck ist zwar zur Anwendung weniger geeignet, zeigt aber unmittelbar, dass C, wie es sein soll, sicher eine ganze Zahl ist.

Beispiel. Für $n = 19$ gilt $4n = 49+27$, also $3k-2 = +7, k = 3$, $C = \frac{1}{9}(6+57) = 7$, und die gesuchte Gleichung ist $x^3 + xx - 6x - 7 = 0$, wie oben (Artikel 351). — Ebenso ergibt sich für $n = 7, 13, 31, 37, 43, 61, 67$ der Wert von k jeweils als $1, -1, 2, -3, -2, 1, -1$, woraus $C = 1, -1, 8, -11, -8, 9, -5$ folgt.

Obwohl das in diesem Artikel gelöste Problem recht verwickelt ist, wollten wir es dennoch nicht unterdrücken, sowohl wegen der Eleganz seiner Lösung als auch, weil es Gelegenheit gab, verschiedene Kunstgriffe anzuwenden, die auch bei anderen Fragen mit großem Nutzen verwendet werden können[*].

[*]Folgerung. Es sei ε eine Wurzel der Gleichung $x^3 - 1 = 0$; dann gilt $(p + \varepsilon p' + \varepsilon\varepsilon p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$. Man setze $\frac{M}{\sqrt{4n}} = \cos\varphi$, $\frac{N\sqrt{27}}{\sqrt{4n}} = \sin\varphi$; dann gilt

$$p = -\tfrac{1}{3} + \tfrac{2}{3}\cos\tfrac{1}{3}\varphi\sqrt{n};$$

$$M \equiv +1 \pmod 3; \quad 1 \equiv M(1.2.3\ldots m)^3 \pmod n$$

Setzt man $3x + 1 = y$ so wird die Gleichung $y^3 - 3ny - Mn = 0$.

Zurückführung der Gleichungen, mit denen die Wurzeln Ω gefunden werden, auf reine Potenzgleichungen.

359.

Die vorstehenden Untersuchungen betrafen das *Auffinden* der Hilfsgleichungen; nun wollen wir eine besonders bemerkenswerte Eigenschaft ihrer *Lösung* darlegen. Bekanntlich sind alle Bemühungen der größten Geometer, die allgemeine Lösung der Gleichungen über den vierten Grad hinaus oder (um genauer zu bestimmen, was ich suche) DIE ZURÜCKFÜHRUNG GEMISCHTER GLEICHUNGEN AUF REINE POTENZGLEICHUNGEN zu finden, bisher stets vergeblich gewesen, und es bleibt kaum ein Zweifel, dass dieses Problem eher etwas Unmögliches verlangt als etwas, das die Kräfte der heutigen Analysis übersteigt. (Man vergleiche unsere Bemerkungen zu diesem Gegenstand in *Demonstr. nova etc. art. 9.*) Dennoch steht fest, dass es unzählige gemischte Gleichungen jedes Grades gibt, die eine solche Zurückführung auf reine Potenzgleichungen zulassen, und wir hoffen, dass es den Geometern willkommen sein wird, wenn wir zeigen, dass unsere Hilfsgleichungen immer hierzu gehören. Wegen des großen Umfangs dieser Untersuchung geben wir jedoch hier nur die Hauptpunkte an, die zum Nachweis der Möglichkeit nötig sind, und verschieben die ausführlichere Behandlung, die dieser Gegenstand in hohem Maße verdient, auf ein anderes Mal. Vorauszuschicken sind einige allgemeine Beobachtungen über die Wurzeln der Gleichung $x^e - 1 = 0$, die auch den Fall einschließen, dass e zusammengesetzt ist.

I. Diese Wurzeln werden (wie aus den elementaren Lehrbüchern bekannt ist) durch $\cos\frac{kP}{e} + i\sin\frac{kP}{e}$ dargestellt, wobei für k die e Zahlen $0, 1, 2, 3 \ldots e-1$ oder beliebige andere, ihnen modulo e kongruente Zahlen zu nehmen sind. Eine Wurzel wird für $k = 0$ oder allgemein für k, wenn es durch e teilbar ist, $= 1$; jedem anderen Wert von k entspricht eine von 1 verschiedene Wurzel.

II. Da $(\cos\frac{kP}{e} + i\sin\frac{kP}{e})^\lambda = \cos\frac{\lambda kP}{e} + i\sin\frac{\lambda kP}{e}$, ist klar: Entspricht die Wurzel R einem Wert von k, der zu e teilerfremd ist, so ist in der Folge R, RR, R^3, usw., das Glied an der Stelle e zwar $= 1$, alle vorhergehenden Glieder sind aber von 1 verschieden. Daraus folgt sofort, dass alle e Größen $1, R, RR, R^3 \ldots R^{e-1}$ ungleich sind; und da sie offenbar alle die Gleichung $x^e - 1 = 0$ erfüllen, stellen sie sämtliche Wurzeln dieser Gleichung dar.

III. Schließlich hat man unter derselben Voraussetzung

$$1 + R^\lambda + R^{2\lambda} \ldots + R^{\lambda(e-1)} = 0$$

für jeden ganzzahligen Wert von λ, der nicht durch e teilbar ist; denn die Summe ist $= \frac{1-R^{\lambda e}}{1-R^\lambda}$, und der Zähler dieses Bruches wird $= 0$, der Nenner dagegen nicht $= 0$. Ist jedoch λ durch e teilbar, so wird jene Summe offenbar $= e$.

360.

Es sei, wie stets im Vorhergehenden, n eine Primzahl, g eine Primitivwurzel modulo n und $n-1$ das Produkt dreier positiver ganzer Zahlen α, β, γ. Der Kürze wegen werden wir die Untersuchung gleich so anlegen, dass sie auch die Fälle einschließt, in denen α gleich eins ist oder $\gamma = 1$ gilt; wenn $\gamma = 1$, sind anstelle der Summen $(\gamma, 1), (\gamma, g)$, usw., die Wurzeln $[1], [g]$, usw., zu nehmen. Wir setzen also voraus, dass

aus allen als bekannt angenommenen α Summen von $\beta\gamma$ Gliedern $(\beta\gamma, 1), (\beta\gamma, g)$, $(\beta\gamma, gg) \ldots (\beta\gamma, g^{\alpha-1})$ die Summen von γ Gliedern abzuleiten sind. Diese Aufgabe haben wir oben auf eine gemischte Gleichung vom Grad β zurückgeführt; nun wollen wir zeigen, wie man sie durch eine reine Potenzgleichung von demselben Grad löst. Zur Abkürzung bezeichnen wir die Summen

$$(\gamma, 1), (\gamma, g^{\alpha}), (\gamma, g^{2\alpha}) \ldots (\gamma, g^{\alpha\beta-\alpha})$$

innerhalb von $(\beta\gamma, 1)$ der Reihe nach mit $a, b, c \ldots m$; die Summen

$$(\gamma, g), (\gamma, g^{\alpha+1}) \ldots (\gamma, g^{\alpha\beta-\alpha+1})$$

innerhalb von $(\beta\gamma, g)$ der Reihe nach mit $a', b' \ldots m'$; die Summen

$$(\gamma, gg), (\gamma, g^{\alpha+2}) \ldots (\gamma, g^{\alpha\beta-\alpha+2})$$

der Reihe nach mit $a'', b'' \ldots m''$; und so weiter bis zu denjenigen, die in $(\beta\gamma, g^{\alpha-1})$ enthalten sind.

I. Nun bezeichne R unbestimmt eine Wurzel der Gleichung $x^{\beta} - 1 = 0$, und es werde angenommen, dass die Entwicklung der Potenz mit dem Exponenten β der Funktion

$$t = a + Rb + RRc \ldots + R^{\beta-1}m$$

nach den Regeln von Artikel 345

$$\begin{aligned} &N + Aa + Bb + Cc \ldots + Mm \\ &+ A'a' + B'b' + C'c' \ldots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ &+ \text{usw.} = T \end{aligned}$$

ergibt, wobei alle Koeffizienten N, A, B, A', usw., Polynome in R sein werden. Ferner werde angenommen, dass sich die Potenzen mit dem Exponenten β zweier anderer Funktionen

$$\begin{aligned} u &= R^{\beta}a + Rb + RRc \ldots + R^{\beta-1}m, \\ u' &= b + Rc + RRd \ldots + R^{\beta-2}m + R^{\beta-1}a \end{aligned}$$

der Reihe nach in U und U' entwickeln. Aus Artikel 350 erkennt man leicht, dass, da u' aus t hervorgeht, indem man die Summen $a, b, c \ldots m$ der Reihe nach mit b, c, $d \ldots a$ vertauscht,

$$\begin{aligned} U' &= N + Ab + Bc + Cd \ldots + Ma \\ &+ A'b' + B'c' + C'd' \ldots + M'a' \\ &+ A''b'' + B''c'' + C''d'' \ldots + M''a'' \\ &+ \text{usw.} \end{aligned}$$

sein wird.

Weiter ist klar: Da $u = Ru'$, wird $U = R^{\beta}U'$ sein, sodass wegen $R^{\beta} = 1$ die entsprechenden Koeffizienten in U und U' gleich sind. Schließlich unterscheiden sich

t und u nur dadurch, dass a in t mit der Einheit und in u mit R^β multipliziert wird. Daher erkennt man leicht, dass alle entsprechenden Koeffizienten (also diejenigen, mit denen dieselben Summen multipliziert werden) in T und U gleich sind und somit auch alle entsprechenden Koeffizienten in T und U'. Daraus folgt endlich $A = B = C$, usw., $= M$; $A' = B' = C'$, usw., $A'' = B'' = C''$, usw., usw. Dadurch lässt sich T auf eine Form wie

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, gg) \text{ usw.}$$

zurückführen, wobei jeder einzelne Koeffizient N, A, A', usw., auf eine Form wie

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{usw.}$$

gebracht werden kann, in der p, p', p'', usw., gegebene ganze Zahlen sind.

II. Nimmt man für R eine bestimmte Wurzel der Gleichung $x^\beta - 1 = 0$ (deren Lösung wir bereits als bekannt voraussetzen), und zwar eine solche, von der keine niedrigere Potenz als diejenige mit dem Exponenten β der Einheit gleich ist, so wird auch T eine bestimmte Größe sein, aus der sich t durch die reine Potenzgleichung $t^\beta - T = 0$ ableiten lässt. Da diese Gleichung aber β Wurzeln hat, nämlich t, $Rt, RRt \dots R^{\beta-1}t$, kann es zweifelhaft erscheinen, welche Wurzel man wählen muss. Dass diese Wahl völlig beliebig ist, wird jedoch auf folgende Weise leicht klar. Man muss sich erinnern, dass nach der Bestimmung aller Summen von $\beta\gamma$ Gliedern die Wurzel [1] nur insoweit bestimmt ist, als irgendeine der $\beta\gamma$ in $(\beta\gamma, 1)$ enthaltenen Wurzeln mit diesem Zeichen bezeichnet werden muss; und dass es daher völlig beliebig ist, welche der β Summen, aus denen $(\beta\gamma, 1)$ besteht, wir mit a bezeichnen wollen. Nehmen wir nun an, dass bei Bezeichnung einer bestimmten Summe mit a $t = \mathfrak{T}$ wird. Dann erkennt man leicht: Will man nachher die eben mit b bezeichnete Summe mit a bezeichnen, so werden diejenigen, die vorher $c, d \dots a, b$ waren, nun b, $c \dots m, a$, und der Wert von t wird jetzt $= \frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\beta-1}$. Ebenso wird, wenn man mit a die ursprünglich mit c bezeichnete Summe bezeichnen will, der Wert von t $\mathfrak{T}R^{\beta-2}$, und so weiter: t kann als gleich jeder der Größen $\mathfrak{T}, \mathfrak{T}R^{\beta-1}, \mathfrak{T}R^{\beta-2}$, usw., d. h. jeder Wurzel der Gleichung $x^\beta - T = 0$ angesehen werden, je nachdem man annimmt, dass diese oder jene in $(\beta\gamma, 1)$ enthaltene Summe mit $(\gamma, 1)$ bezeichnet wird. *Q. E. D.*

III. Nachdem die Größe t auf diese Weise bestimmt ist, muss man $\beta - 1$ andere suchen, die aus t hervorgehen, wenn man in seinem Ausdruck für R nacheinander $RR, R^3, R^4 \dots R^\beta$ einsetzt, nämlich

$$t' = a + RRb + R^4c \dots + R^{2\beta-2}m,$$
$$t'' = a + R^3b + R^6c \dots + R^{3\beta-3}m \text{ usw.}$$

Die letzte ist bereits bekannt, da sie offenbar $= a + b + c \dots + m = (\beta\gamma, 1)$ wird; die übrigen lassen sich folgendermaßen finden. Entwickelt man nach den Regeln von Artikel 345, ebenso wie vorher in I t^β, das Produkt $t^{\beta-2}t'$, so wird man mit einer dem vorigen Verfahren völlig entsprechenden Methode beweisen, dass sich das Ergebnis auf eine Form wie

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, gg) \text{ usw.} = T'$$

zurückführen lässt, in der $\mathfrak{N}, \mathfrak{A}, \mathfrak{A}'$, usw., Polynome in R sind, sodass T' eine bekannte Größe ist, aus der man $t' = \frac{T'tt}{T}$ erhält. Nimmt man in genau derselben Weise an,

dass die Entwicklung des Produkts $t^{\beta-3}t''\ T'''$ ergibt, so wird dieser Ausdruck eine ähnliche Form haben, und aus seinem bekannten Wert wird man daher t'' durch die Gleichung $t'' = \frac{T''t^3}{T}$ ableiten; ebenso wird t''' durch eine Gleichung wie $t''' = \frac{T''''t^4}{T}$ gefunden, in der T''' eine bekannte Größe ist, und so weiter.

Diese Methode wäre nicht anwendbar, wenn $t = 0$ eintreten könnte, woraus auch $T = T' = T''$, usw., $= 0$ sein müsste; doch lässt sich beweisen, dass dies unmöglich ist, auch wenn wir den Beweis wegen seiner Länge hier weglassen müssen. — Es gibt auch besondere Kunstgriffe, mit denen sich die Brüche $\frac{T'}{T}, \frac{T''}{T}$, usw., in *Polynome* in R verwandeln lassen, sowie kürzere Methoden, im Fall $\alpha = 1$ die Werte von t', t'', usw., zu finden. Dies alles müssen wir hier ohne weitere Erörterung übergehen.

IV. Sobald schließlich t, t', t'', usw., gefunden sind, hat man nach Beobachtung III des vorigen Artikels sofort $t + t' + t'' + \text{usw.} = \beta a$, womit der Wert von a bekannt ist; daraus lassen sich nach Artikel 346 die Werte aller übrigen Summen von γ Gliedern ableiten. — Die Werte von b, c, d, usw., können auch aus den folgenden Gleichungen gewonnen werden, deren Grund jedem aufmerksamen Leser leicht ersichtlich sein wird:

$$\beta b = R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{usw.}$$
$$\beta c = R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{usw.}$$
$$\beta d = R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \text{usw. usw.}$$

Von der großen Zahl der Beobachtungen zur vorstehenden Untersuchung berühren wir hier nur eine. Was die Lösung der reinen Potenzgleichung $x^\beta - T = 0$ angeht, so hat T offenbar in den meisten Fällen einen imaginären Wert $P + iQ$, sodass jene Lösung bekanntlich teils von der Teilung eines Winkels (dessen Tangens $= \frac{Q}{P}$ ist), teils von der Teilung eines Verhältnisses (der Einheit zu $\sqrt{(PP + QQ)}$) in β Teile abhängt. Dabei ist sehr bemerkenswert (was wir hier jedoch nicht weiter ausführen), dass sich der Wert von $\sqrt[\beta]{(PP + QQ)}$ stets *rational* durch schon bekannte Größen ausdrücken lässt, sodass außer der Ausziehung einer Quadratwurzel zur Lösung *nur* die Teilung eines Winkels erforderlich ist, z. B. für $\beta = 3$ nur die Dreiteilung eines Winkels.

Da schließlich nichts hindert, $\alpha = 1, \gamma = 1$ und somit $\beta = n - 1$ zu setzen, ist klar, dass sich die Lösung der Gleichung $x^n - 1 = 0$ sogleich auf die Lösung der reinen Potenzgleichung vom Grad $n-1$, nämlich $x^{n-1} - T = 0$, zurückführen lässt, wobei T durch die Wurzeln der Gleichung $x^{n-1} - 1 = 0$ bestimmt wird. Daraus folgt mithilfe der eben gemachten Beobachtung, dass die Teilung des ganzen Kreises in n Teile 1° die Teilung des ganzen Kreises in $n - 1$ Teile, 2° die Teilung eines anderen Bogens, der nach Ausführung jener Teilung konstruiert werden kann, in $n - 1$ Teile und 3° die Ausziehung einer einzigen Quadratwurzel erfordert; und es lässt sich tatsächlich zeigen, dass diese stets $\sqrt{n}$ ist.

Anwendung der vorstehenden Untersuchungen auf die trigonometrischen Funktionen. Eine Methode, die Winkel zu bestimmen, denen die einzelnen Wurzeln Ω entsprechen.

361.

Es bleibt uns noch, den Zusammenhang zwischen den Wurzeln Ω und den trigonometrischen Funktionen der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$ näher zu betrachten. Die Methode, die wir zum Auffinden der Wurzeln Ω angegeben haben, lässt noch ungewiss (sofern nicht während der Arbeit die Sinustafeln in der oben beschriebenen Weise benutzt wurden, was jedoch weniger unmittelbar wäre), *welche* Wurzeln den *einzelnen* Winkeln entsprechen, d. h. welche Wurzel $= \cos\frac{P}{n} + i\sin\frac{P}{n}$, welche $= \cos\frac{2P}{n} + i\sin\frac{2P}{n}$ ist, usw. Diese Ungewissheit lässt sich leicht beheben, wenn man bedenkt, dass die Kosinus der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{2n}$ fortwährend abnehmen (sofern man auch die Vorzeichen berücksichtigt) und ihre Sinus alle positiv sind; die Winkel $\frac{(n-1)P}{n}$, $\frac{(n-2)P}{n}, \frac{(n-3)P}{n} \ldots \frac{(n+1)P}{2n}$ dagegen haben der Reihe nach dieselben Kosinus wie jene, aber negative Sinus, deren absolute Beträge den Sinus jener Winkel gleich sind. Daher entsprechen von den Wurzeln Ω diejenigen beiden mit den größten reellen Teilen (die einander gleich sind) den Winkeln $\frac{P}{n}, \frac{(n-1)P}{n}$: dem ersten die Wurzel, in der die imaginäre Größe i mit einer positiven Größe multipliziert ist, dem zweiten diejenige, in der i mit einer negativen Größe multipliziert ist. Von den $n-3$ übrigen Wurzeln entsprechen wiederum diejenigen mit den größten reellen Teilen den Winkeln $\frac{2P}{n}$, $\frac{(n-2)P}{n}$, und so weiter. — Sobald die Wurzel, der der Winkel $\frac{P}{n}$ entspricht, erkannt ist, lassen sich diejenigen, die den übrigen Winkeln entsprechen, auch dadurch unterscheiden, dass, wenn jene $= [\lambda]$ gesetzt wird, den Winkeln $\frac{2P}{n}, \frac{3P}{n}, \frac{4P}{n}$, usw., offenbar die Wurzeln $[2\lambda], [3\lambda], [4\lambda]$, usw., entsprechen. So sieht man im Beispiel von Artikel 353 sofort, dass dem Winkel $\frac{1}{19}P$ keine andere Wurzel als [11] und dem Winkel $\frac{18}{19}P$ die Wurzel [8] entsprechen kann; ebenso entsprechen den Winkeln $\frac{2}{19}P, \frac{17}{19}P, \frac{3}{19}P, \frac{16}{19}P$, usw., die Wurzeln $[3], [16], [14], [5]$, usw. Im Beispiel von Artikel 354 entspricht dem Winkel $\frac{1}{17}P$ offenbar die Wurzel [1], dem Winkel $\frac{2}{17}P$ die Wurzel [2], usw. Auf diese Weise sind also die Kosinus und Sinus der Winkel $\frac{P}{n}, \frac{2P}{n}$, usw., vollständig bestimmt.

Tangens, Kotangens, Sekans und Kosekans werden aus Sinus und Kosinus ohne Division abgeleitet.

362.

Was die übrigen trigonometrischen Funktionen dieser Winkel angeht, so ließen sie sich aus den entsprechenden Kosinus und Sinus mit den allgemein bekannten Methoden leicht ableiten: nämlich die Sekans- und Tangenswerte, indem man die Einheit und die Sinus durch die Kosinus dividiert, sowie die Kosekans- und Kotangenswerte, indem man die Einheit und die Kosinus durch die Sinus dividiert. Bequemer erhält man jedoch dasselbe meist mit den folgenden Formeln, ohne Divisionen, allein durch Additionen. Es sei ω irgendeiner der Winkel $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$, und es sei $\cos\omega + i\sin\omega = R$, sodass R eine der Wurzeln Ω ist; dabei gilt

$$\cos\omega = \tfrac{1}{2}(R + \tfrac{1}{R}) = \frac{1+RR}{2R},$$
$$\sin\omega = \tfrac{1}{2i}(R - \tfrac{1}{R}) = \frac{i(1-RR)}{2R}$$

Daraus folgt

$$\sec\omega = \frac{2R}{1+RR}. \quad \operatorname{tang}\omega = \frac{i(1-RR)}{1+RR},$$
$$\operatorname{cosec}\omega = \frac{2Ri}{RR-1}, \quad \operatorname{cotang}\omega = \frac{i(RR+1)}{RR-1}$$

Nun wollen wir zeigen, wie man die Zähler dieser vier Brüche so umformen kann, dass sie durch ihre Nenner teilbar werden.

I. Wegen $R = R^{n+1} = R^{2n+1}$ wird $2R = R + R^{2n+1}$, welcher Ausdruck offenbar durch $1 + RR$ teilbar ist, da n ungerade ist. Daraus folgt

$$\sec\omega = R - R^3 + R^5 - R^7 \ldots + R^{2n-1}$$

und daher (da wegen $\sin\omega = -\sin(2n-1)\omega,\ \sin 3\omega = -\sin(2n-3)\omega$, usw., offenbar $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$ gilt)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega$$

oder schließlich (da $\cos\omega = \cos(2n-1)\omega,\ \cos 3\omega = \cos(2n-3)\omega$, usw.),

$$= 2(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega) \pm \cos n\omega$$

wobei das obere oder untere Vorzeichen gilt, je nachdem n die Form $4k+1$ oder $4k+3$ hat. Offenbar lässt sich diese Formel auch so darstellen:

$$\sec\omega = \pm(1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega)$$

II. Setzt man ebenso $1 - R^{2n+2}$ für $1 - RR$ ein, so ergibt sich

$$\operatorname{tang}\omega = i(1 - RR + R^4 - R^6 \ldots - R^{2n})$$

oder (da $1 - R^{2n} = 0,\ RR - R^{2n-2} = 2i\sin 2\omega,\ R^4 - R^{2n-4} = 2i\sin 4\omega$, usw.),

$$\operatorname{tang}\omega = 2(\sin 2\omega - \sin 4\omega + \sin 6\omega \ldots \mp \sin(n-1)\omega)$$

III. Da $1 + RR + R^4 \ldots + R^{2n-2} = 0$ gilt, wird

$$\begin{aligned} n &= n - 1 - RR - R^4 \ldots R^{2n-2} \\ &= (1-1) + (1-RR) + (1-R^4) \ldots + (1-R^{2n-2}) \end{aligned}$$

und jeder einzelne Teil dieser Summe ist durch $1 - RR$ teilbar. Daraus folgt

$$\begin{aligned} \frac{n}{1-RR} &= 1 + (1+RR) + (1+RR+R^4) \ldots \\ &\quad + (1 + RR + R^4 \ldots + R^{2n-4}) \\ &= (n-1) + (n-2)RR + (n-3)R^4 \ldots + R^{2n-4} \end{aligned}$$

sodass man durch Multiplikation mit 2, Subtraktion von

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

und erneute Multiplikation mit R

$$\begin{aligned} \frac{2nR}{1-RR} &= (n-1)R + (n-3)R^3 + (n-5)R^5 \ldots \\ &\quad - (n-3)R^{2n-3} - (n-1)R^{2n-1} \end{aligned}$$

erhält, woraus sich sofort ergibt:

$$\begin{aligned} \operatorname{cosec}\omega &= \frac{1}{n}\big((n-1)\sin\omega + (n-3)\sin 3\omega \ldots \\ &\quad - (n-1)\sin(2n-1)\omega\big) \\ &= \frac{2}{n}\big((n-1)\sin\omega + (n-3)\sin 3\omega \\ &\quad + \text{usw.} + 2\sin(n-2)\omega\big) \end{aligned}$$

Diese Formel lässt sich auch so darstellen:

$$\operatorname{cosec}\omega = -\frac{2}{n}(2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega)$$

IV. Durch Multiplikation des oben angegebenen Wertes von $\frac{n}{1-RR}$ mit $1+RR$ und Subtraktion von

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

ergibt sich

$$\frac{n(1+RR)}{1-RR} = (n-2)RR + (n-4)R^4 + (n-6)R^6 \ldots - (n-2)R^{2n-2}$$

woraus sofort folgt:

$$\begin{aligned} \operatorname{cotang}\omega &= \frac{1}{n}\big((n-2)\sin 2\omega + (n-4)\sin 4\omega \\ &\quad + (n-6)\sin 6\omega \ldots - (n-2)\sin(n-2)\omega \\ &= \frac{2}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega \ldots \\ &\quad + 3\sin(n-3)\omega + \sin(n-1)\omega) \end{aligned}$$

Diese Formel lässt sich auch folgendermaßen darstellen:

$$\operatorname{cotang}\omega = -\frac{2}{n}(\sin\omega + 3\sin 3\omega \ldots + (n-2)\sin(n-2)\omega)$$

Eine Methode, den Grad der Gleichungen für trigonometrische Funktionen schrittweise zu senken.

363.

Wie sich unter der Voraussetzung $n-1=ef$ die Funktion X in e Faktoren vom Grad f zerlegen lässt, sobald die Werte aller e Summen von f Gliedern bekannt sind (Artikel 348), so lässt sich dann auch, wenn man voraussetzt, dass $Z=0$ eine Gleichung vom Grad $n-1$ ist, deren Wurzeln die Sinus oder beliebige andere trigonometrische Funktionen der Winkel $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$ sind, die Funktion Z in e Faktoren vom Grad f zerlegen. Die Hauptpunkte dieses Verfahrens sind die folgenden.

Es bestehe Ω aus den e Perioden von f Gliedern $(f,1) = P, P'.P''$, usw.; die Periode P aus den Wurzeln $[1],[a],[b],[c]$, usw.; P' aus $[a'],[b'],[c']$, usw.; P'' aus $[a''],[b''],[c'']$, usw., usw. Der Wurzel $[1]$ entspreche der Winkel ω, also den Wurzeln $[a],[b]$, usw., die Winkel $a\omega, b\omega$, usw., den Wurzeln $[a'],[b']$, usw., die Winkel $a'\omega$, $b'\omega$, usw., und den Wurzeln $[a''],[b'']$, usw., die Winkel $a''\omega, b''\omega$, usw., usw. Dann erkennt man leicht, dass alle diese Winkel zusammengenommen mit den Winkeln $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$ hinsichtlich der trigonometrischen Funktionen[*)] übereinstimmen. Bezeichnet man daher die betreffende Funktion durch das dem Winkel vorangestellte Zeichen φ und setzt das Produkt aus den e Faktoren

$$x-\varphi\omega, \quad x-\varphi a\omega, \quad x-\varphi b\omega \quad \text{usw.}$$

$= Y$, das Produkt aus $x-\varphi a'\omega, x-\varphi b'\omega$, usw., $= Y'$, das Produkt aus $x-\varphi a''\omega$, $x-\varphi b''\omega$, usw., $= Y''$, und so weiter, so ist notwendig das Produkt $YY'Y''\ldots = Z$. Nun bleibt zu zeigen, dass sich alle Koeffizienten in den Funktionen Y, Y', Y'', usw., auf eine Form wie

$$A + B(f,1) + C(f,g) + D(f,gg) \ldots + L(f,g^{e-1})$$

zurückführen lassen. Danach sind offenbar alle als bekannt anzusehen, sobald die Werte aller Summen von f Gliedern bekannt sind. Dies werden wir folgendermaßen erreichen.

Wie $\cos\omega = \frac{1}{2}[1] + \frac{1}{2}[1]^{n-1}$, $\sin\omega = -\frac{1}{2}i[1] + \frac{1}{2}i[1]^{n-1}$, so lassen sich nach dem vorigen Artikel auch die übrigen trigonometrischen Funktionen des Winkels ω auf eine Form wie $\mathfrak{A}+\mathfrak{B}[1]+\mathfrak{C}[1]^2+\mathfrak{D}[1]^3+$usw. zurückführen. Man erkennt ohne Schwierigkeit, dass die Funktion des Winkels $k\omega$ dann $= \mathfrak{A}+\mathfrak{B}[k]+\mathfrak{C}[k]^2+\mathfrak{D}[k]^3+$usw. wird, wobei k eine beliebige ganze Zahl bezeichnet. Da nun jeder Koeffizient in Y ein symmetrisches Polynom in $\varphi\omega, \varphi a\omega, \varphi b\omega$, usw., ist, ist klar: Setzt man für diese Größen ihre Werte ein, so wird jeder Koeffizient ein symmetrisches Polynom in $[1],[a],[b]$, usw.; daher lassen sie sich nach Artikel 347 auf die Form $A+B(f,1)+C(f,g)+$usw. zurückführen. Mit genau derselben Begründung kann man auch alle Koeffizienten in Y', Y'', usw., auf eine ähnliche Form zurückführen. *Q. E. D.*

[*)] In dieser Hinsicht stimmen zwei Winkel überein, deren Differenz dem ganzen Kreisumfang oder irgendeinem Vielfachen davon gleich ist. Solche Winkel könnten wir *nach dem Kreisumfang kongruent* nennen, wenn man die Kongruenz in einem etwas weiteren Sinne verstehen wollte.

364.

Zum Problem des vorigen Artikels fügen wir noch einige Beobachtungen hinzu.

I. Da die einzelnen Koeffizienten in Y' Funktionen der in der Periode P' (die man $= (f, a')$ setzen darf) enthaltenen Wurzeln sind, die mit den durch die entsprechenden Koeffizienten gegebenen Funktionen der Wurzeln in P in Y übereinstimmen, ist aus Artikel 347 klar, dass sich Y' aus Y ableiten lässt, wenn man überall in Y für $(f, 1)$, $(f, g), (f, gg)$, usw., der Reihe nach $(f, a'), (f, a'g), (f, a'gg)$, usw., einsetzt. Ebenso wird Y'' aus Y abgeleitet, indem man überall in Y für $(f, 1), (f, g), (f, gg)$, usw., der Reihe nach $(f, a''), (f, a''g), (f, a''gg)$, usw., usw., einsetzt. Sobald also die Funktion Y entwickelt ist, folgen die übrigen Funktionen Y', Y'', usw., daraus ohne Schwierigkeit.

II. Setzt man

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{usw.}$$

voraus, so sind die Koeffizienten α, β, usw., der Reihe nach die Summe der Wurzeln der Gleichung $Y = 0$ d. h. der Größen $\varphi\omega, \varphi a\omega, \varphi b\omega$, usw., die Summe der Produkte aus je zweien und so weiter. Meist erhält man diese Koeffizienten aber viel bequemer mit einer der in Artikel 349 angegebenen ähnlichen Methode, indem man die Summe der Wurzeln $\varphi\omega, \varphi a\omega, \varphi b\omega$, usw., die Summe ihrer Quadrate, Kuben, usw., berechnet und daraus nach dem Newtonschen Satz jene Koeffizienten ableitet. — Bezeichnet φ den Tangens, Sekans, Kotangens oder Kosekans, so gibt es noch weitere Abkürzungen, die wir hier jedoch ohne Erörterung übergehen.

III. Besondere Betrachtung verdient der Fall, dass f gerade ist und daher jede Periode P, P', P'', usw., aus $\frac{1}{2}f$ Perioden von je zwei Gliedern besteht. Es bestehe P aus $(2, 1), (2, \mathfrak{a}), (2, \mathfrak{b}), (2, \mathfrak{c})$, usw. Dann stimmen die Zahlen $1, \mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, usw., und $n-1$, $n - \mathfrak{a}.n - \mathfrak{b}, n - \mathfrak{c}$, usw., zusammengenommen mit $1, a, b, c$, usw., überein oder sind ihnen wenigstens (was hier auf dasselbe hinausläuft) modulo n kongruent. Es gilt aber $\varphi(n-1)\omega = \pm\varphi\omega$, $\varphi(n - \mathfrak{a})\omega = \pm\varphi\mathfrak{a}\omega$, usw., wobei die oberen Vorzeichen gelten, wenn φ den Kosinus oder Sekans bezeichnet, die unteren, wenn φ den Sinus, Tangens, Kotangens oder Kosekans bezeichnet. Daraus folgt, dass in den ersten beiden Fällen unter den Faktoren, aus denen Y besteht, stets je zwei gleich sind und daher Y ein Quadrat ist, und zwar $Y = yy$, wenn y gleich dem folgenden Produkt gesetzt wird:

$$x - \varphi\omega,\ x - \varphi\mathfrak{a}\omega,\ x - \varphi\mathfrak{b}\omega \text{ usw.}$$

Ebenso sind in denselben Fällen die übrigen Funktionen Y', Y'', usw., Quadrate. Setzt man nämlich voraus, dass P' aus $(2, \mathfrak{a}'), (2, \mathfrak{b}'), (2, \mathfrak{c}')$, usw., P'' aus $(2, \mathfrak{a}'')$, $(2, \mathfrak{b}''), (2, \mathfrak{c}'')$, usw., usw., besteht und dass das Produkt aus $x - \varphi\mathfrak{a}'\omega, x - \varphi\mathfrak{b}'\omega$, $x - \varphi\mathfrak{c}'\omega$, usw., $= y'$, das Produkt aus $x - \varphi\mathfrak{a}''\omega, x - \varphi\mathfrak{b}''\omega$, usw., $= y''$ ist, und so weiter, so wird $Y' = y'y'$, $Y'' = y''y''$, usw. Auch die Funktion Z ist dann ein Quadrat (vgl. oben Artikel 337), dessen Quadratwurzel gleich dem Produkt aus y, y', y'', usw., ist. Ferner erkennt man leicht, dass y', y'', usw., ebenso aus y abgeleitet werden, wie wir oben in I gesagt haben, dass Y', Y'', usw., aus Y folgen. Auch jeder Koeffizient in y lässt sich auf die Form

$$A + B(f, 1) + C(f, g) + \text{usw.}$$

zurückführen, da die Summen der einzelnen Potenzen der Wurzeln der Gleichung $y = 0$ offenbar die Hälften der Potenzen der Wurzeln der Gleichung $Y = 0$ sind und sich somit auf eine solche Form zurückführen lassen. In den letzten vier Fällen dagegen ist Y das Produkt aus den Faktoren

$$xx - (\varphi\omega)^2,\ xx - (\varphi\mathfrak{a}\omega)^2,\ xx - (\varphi\mathfrak{b}\omega)^2 \text{ usw.}$$

und hat daher die Form

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{usw.}$$

Offenbar lassen sich die Koeffizienten λ, μ, usw., aus den Summen der Quadrate, vierten Potenzen, usw., der Wurzeln $\varphi\omega, \varphi\mathfrak{a}\omega, \varphi\mathfrak{b}\omega$, usw., ableiten; und ebenso verhalten sich die Funktionen Y', Y'', usw.

Beispiel I. Es sei $n = 17, f = 8$, und φ bezeichne den Kosinus. Daraus folgt

$$\begin{aligned} Z = \big(&x^8 + \tfrac{1}{2}x^7 - \tfrac{7}{4}x^6 - \tfrac{3}{4}x^5 + \tfrac{15}{16}x^4 \\ &+ \tfrac{5}{16}x^3 - \tfrac{5}{32}xx - \tfrac{1}{32}x + \tfrac{1}{256}\big)^2 \end{aligned}$$

und man muss daher $\sqrt{Z}$ in zwei Faktoren vierten Grades y, y' zerlegen. Die Periode $P = (8,1)$ besteht aus $(2,1),(2,9),(2,13),(2,15)$, weshalb y das Produkt aus den Faktoren

$$x - \varphi\omega,\ x - \varphi 9\omega,\ x - \varphi 13\omega,\ x - \varphi 15\omega$$

ist. Setzt man $\frac{1}{2}[k] + \frac{1}{2}[n-k]$ für $\varphi k\omega$ ein, so findet man

$$\begin{gathered} \varphi\omega + \varphi 9\omega + \varphi 13\omega + \varphi 15\omega = \tfrac{1}{2}(8,1), \\ (\varphi\omega)^2 + (\varphi 9\omega)^2 + (\varphi 13\omega)^2 + (\varphi 15\omega)^2 = 2 + \tfrac{1}{4}(8,1) \end{gathered}$$

Ebenso ist die Summe der Kuben $= \frac{3}{8}(8,1) + \frac{1}{8}(8,3)$, die Summe der vierten Potenzen $= 1\frac{1}{2} + \frac{5}{16}(8,1)$. Bestimmt man hieraus nach dem Newtonschen Satz die Koeffizienten in y, so ergibt sich

$$\begin{aligned} y = x^4 &- \tfrac{1}{2}(8,1)x^3 + \tfrac{1}{4}((8,1) + 2(8,3))xx \\ &- \tfrac{1}{8}((8,1) + 3(8,3))x + \tfrac{1}{16}((8,1) + (8,3)) \end{aligned}$$

Dagegen wird y' aus y abgeleitet, indem man $(8,1)$ mit $(8,3)$ vertauscht. Setzt man also für $(8,1),(8,3)$ die Werte $-\frac{1}{2} + \frac{1}{2}\sqrt{17}, -\frac{1}{2} - \frac{1}{2}\sqrt{17}$ ein, so ergibt sich

$$\begin{aligned} y = x^4 &+ (\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} + \tfrac{1}{8}\sqrt{17})xx \\ &+ (\tfrac{1}{4} + \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16} \end{aligned}$$

$$\begin{aligned} y' = x^4 &+ (\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} - \tfrac{1}{8}\sqrt{17})xx \\ &+ (\tfrac{1}{4} - \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16} \end{aligned}$$

Ebenso lässt sich $\sqrt{Z}$ in vier Faktoren zweiten Grades zerlegen, deren erster $(x - \varphi\omega)(x - \varphi 13\omega)$, zweiter $(x - \varphi 9\omega)(x - \varphi 15\omega)$, dritter $(x - \varphi 3\omega)(x - \varphi 5\omega)$ und vierter

$(x - \varphi 10\omega)(x - \varphi 11\omega)$ ist. Alle Koeffizienten dieser Faktoren können durch die vier Summen $(4,1),(4,9),(4,3),(4,10)$ ausgedrückt werden. Offenbar ist aber das Produkt aus dem ersten und zweiten Faktor y, das Produkt aus dem dritten und vierten y'.

Beispiel II. Soll bei unveränderten übrigen Voraussetzungen φ den Sinus bezeichnen, sodass

$$\begin{aligned} Z = x^{16} &- \tfrac{17}{4}x^{14} + \tfrac{119}{16}x^{12} - \tfrac{221}{32}x^{10} \\ &+ \tfrac{935}{256}x^8 - \tfrac{561}{512}x^6 + \tfrac{357}{2048}x^4 - \tfrac{51}{4096}xx + \tfrac{17}{65536} \end{aligned}$$

in zwei Faktoren achten Grades y, y' zu zerlegen ist, so ist y das Produkt aus vier quadratischen Faktoren

$$xx - (\varphi\omega)^2,\ xx - (\varphi 9\omega)^2,\ xx - (\varphi 13\omega)^2,\ xx - (\varphi 15\omega)^2$$

Da nun $\varphi k\omega = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$, wird

$$\begin{aligned} (\varphi k\omega)^2 &= -\tfrac{1}{4}[2k] + \tfrac{1}{2}[n] - \tfrac{1}{4}[2n-2k] \\ &= \tfrac{1}{2} - \tfrac{1}{4}[2k] - \tfrac{1}{4}[2n-2k] \end{aligned}$$

Hieraus ergibt sich für die Summe der Quadrate der Wurzeln $\varphi\omega, \varphi 9\omega, \varphi 13\omega.\varphi 15\omega$ der Wert $2 - \frac{1}{4}(8,1)$, für die Summe ihrer vierten Potenzen $= \frac{3}{2} - \frac{3}{16}(8,1)$, für die Summe ihrer sechsten Potenzen $= \frac{5}{4} - \frac{9}{64}(8,1) - \frac{1}{64}(8,3)$ und für die Summe ihrer achten Potenzen $\frac{35}{32} - \frac{27}{256}(8,1) - \frac{1}{32}(8,3)$. Daraus folgt

$$\begin{aligned} y = x^8 &- (2 - \tfrac{1}{4}(8,1))x^6 \\ &+ (\tfrac{3}{2} - \tfrac{5}{16}(8,1) + \tfrac{1}{8}(8,3))x^4 \\ &- (\tfrac{1}{2} - \tfrac{9}{64}(8,1) + \tfrac{5}{64}(8,3))xx \\ &+ \tfrac{1}{16} - \tfrac{5}{256}(8,1) + \tfrac{3}{256}(8,3) \end{aligned}$$

Man leitet y' aus y durch Vertauschung von $(8,1),(8,3)$ ab, sodass man durch Einsetzen der Werte dieser Summen

$$\begin{aligned} y = x^8 &- (\tfrac{17}{8} - \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} - \tfrac{7}{32}\sqrt{17})x^4 \\ &- (\tfrac{17}{32} - \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} - \tfrac{1}{64}\sqrt{17} \end{aligned}$$

$$\begin{aligned} y' = x^8 &- (\tfrac{17}{8} + \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} + \tfrac{7}{32}\sqrt{17})x^4 \\ &- (\tfrac{17}{32} + \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} + \tfrac{1}{64}\sqrt{17} \end{aligned}$$

erhält. Ebenso lässt sich Z in vier Faktoren zerlegen, deren Koeffizienten durch Summen von vier Gliedern ausgedrückt werden können; dabei ist das Produkt aus zweien y und das Produkt aus den beiden übrigen y'.

Teilungen des Kreises, die sich durch quadratische Gleichungen oder durch geometrische Konstruktionen ausführen lassen.

365.

Durch die vorstehenden Untersuchungen haben wir also die Teilung des Kreises in n Teile, wenn n eine Primzahl ist, auf die Lösung so vieler Gleichungen zurückgeführt, wie es Faktoren gibt, in die sich die Zahl $n-1$ zerlegen lässt; die Grade dieser Gleichungen werden durch die Größe der Faktoren bestimmt. Ist daher $n-1$ eine Potenz der Zahl 2, was für die Werte 3, 5, 17, 257, 65537, usw., von n eintritt, so führt die Teilung des Kreises auf lauter quadratische Gleichungen, und die trigonometrischen Funktionen der Winkel $\frac{P}{n}$, $\frac{2P}{n}$, usw., lassen sich durch mehr oder weniger komplizierte Quadratwurzeln (je nach der Größe von n) ausdrücken. In diesen Fällen lässt sich also die Teilung des Kreises in n Teile oder die Zeichnung eines regelmäßigen Vielecks mit n Seiten offenbar durch geometrische Konstruktionen ausführen. So erhält man z. B. für $n = 17$ aus den Artikeln 354 und 361 leicht den folgenden Ausdruck für den Kosinus des Winkels $\frac{1}{17}P$:

$$\begin{aligned} &-\tfrac{1}{16}+\tfrac{1}{16}\sqrt{17}+\tfrac{1}{16}\sqrt{(34-2\sqrt{17})} \\ &\quad+\tfrac{1}{8}\sqrt{(17+3\sqrt{17}-\sqrt{(34-2\sqrt{17})} \\ &\qquad-2\sqrt{(34+2\sqrt{17})}) \end{aligned}$$

Die Kosinus der Vielfachen dieses Winkels haben eine ähnliche Form, die Sinus aber ein Wurzelzeichen mehr. Es ist wahrlich sehr verwunderlich, dass, obwohl schon zu Euklids Zeiten die geometrische Teilbarkeit des Kreises in drei und fünf Teile bekannt war, diesen Entdeckungen während eines Zeitraums von 2000 Jahren nichts hinzugefügt wurde und alle Geometer es als gewiss verkündeten, dass sich außer diesen Teilungen und denjenigen, die sich von selbst daraus ergeben, nämlich den Teilungen in $15, 3.2^\mu, 5.2^\mu, 15.2^\mu$ sowie in 2^μ Teile, keine weiteren durch geometrische Konstruktionen ausführen ließen. — Ferner lässt sich leicht beweisen, dass, wenn die Primzahl $n = 2^m + 1$ ist, auch der Exponent m keine anderen Primfaktoren als die Zahl 2 enthalten kann und daher entweder $= 1$ oder $= 2$ oder einer höheren Potenz der Zahl 2 gleich sein muss. Wäre nämlich m durch irgendeine ungerade Zahl ζ (größer als die Einheit) teilbar und $m = \zeta\eta$, so wäre $2^m + 1$ durch $2^\eta + 1$ teilbar und daher notwendig zusammengesetzt. Alle Werte von n, bei denen wir auf bloß quadratische Gleichungen geführt werden, sind also in der Form $2^{2^\nu} + 1$ enthalten; so erhält man die fünf Zahlen 3, 5, 17, 257, 65537, wenn man $\nu = 0, 1, 2, 3, 4$ oder $m = 1, 2, 4, 8, 16$ setzt. Keineswegs lässt sich aber die Teilung des Kreises für *alle* in dieser Form enthaltenen Zahlen geometrisch ausführen, sondern nur für diejenigen, die Primzahlen sind. Zwar hatte Fermat, durch Induktion irregeführt, behauptet, alle in dieser Form enthaltenen Zahlen müssten Primzahlen sein; doch bemerkte der berühmte Euler als Erster, dass diese Regel schon für $\nu = 5$ oder $m = 32$ falsch ist, da die Zahl $2^{32} + 1 = 4294967297$ den Faktor 641 enthält.

Enthält dagegen $n-1$ andere Primfaktoren als 2, so gelangen wir immer zu höheren Gleichungen: nämlich zu einer oder mehreren kubischen Gleichungen, wenn 3 einmal oder mehrmals unter den Primfaktoren von $n-1$ vorkommt, zu Gleichungen fünften

Grades, wenn $n-1$ durch 5 teilbar ist, und so weiter; und wir können mit voller Strenge beweisen, dass sich diese höheren Gleichungen in keiner Weise vermeiden oder auf niedrigere zurückführen lassen, auch wenn uns die Grenzen dieses Werkes nicht erlauben, diesen Beweis hier zu geben. Wir glaubten dennoch, darauf hinweisen zu müssen, damit niemand hoffe, noch andere Teilungen als die von unserer Theorie nahegelegten, z. B. Teilungen in 7, 11, 13, 19, usw., Teile, auf geometrische Konstruktionen zurückzuführen und seine Zeit unnütz vergeude.

366.

Soll der Kreis in a^α Teile geteilt werden, wobei a eine Primzahl bezeichnet, so lässt sich dies offenbar geometrisch ausführen, wenn $a = 2$, aber für keinen anderen Wert von a, sofern $\alpha > 1$. Denn dann muss man außer den Gleichungen, die zur Teilung in a Teile erforderlich sind, notwendig noch $\alpha - 1$ weitere Gleichungen vom Grad a lösen; auch diese lassen sich in keiner Weise vermeiden oder im Grad senken. Die Grade der notwendigen Gleichungen lassen sich also allgemein aus den Primfaktoren der Zahl $(a-1)a^{\alpha-1}$ erkennen (also auch im Fall $\alpha = 1$).

Soll schließlich der Kreis in $N = a^\alpha b^\beta c^\gamma \ldots$ Teile geteilt werden, wobei a, b, c, usw., verschiedene Primzahlen bezeichnen, so genügt es, die Teilungen in $a^\alpha, b^\beta, c^\gamma$, usw., Teile ausgeführt zu haben (Artikel 336). Um daher die Grade der hierzu nötigen Gleichungen zu erkennen, muss man die Primfaktoren der Zahlen

$$(a-1)a^{\alpha-1}, \quad (b-1)b^{\beta-1}, \quad (c-1)c^{\gamma-1} \text{ usw.}$$

oder, was hier auf dasselbe hinausläuft, ihres Produkts betrachten. Man beachte, dass dieses Produkt die Anzahl der Zahlen ausdrückt, die zu N teilerfremd und kleiner als diese Zahl sind (Artikel 38). Geometrisch lässt sich die Teilung also nur dann ausführen, wenn diese Anzahl eine Zweierpotenz ist; enthält sie dagegen andere Primfaktoren als 2, etwa p, p', usw., so lassen sich Gleichungen vom Grad p, p', usw., in keiner Weise vermeiden. Daraus folgt allgemein: Damit sich der Kreis geometrisch in N Teile teilen lässt, muss N *entweder* 2 oder eine höhere Potenz von 2, *oder* eine Primzahl der Form $2^m + 1$, *oder* ein Produkt mehrerer solcher Primzahlen, *oder* das Produkt aus einer oder mehreren solchen Primzahlen mit 2 oder einer höheren Potenz von 2 sein. Kürzer gesagt darf N weder einen ungeraden Primfaktor enthalten, der nicht die Form $2^m + 1$ hat, noch irgendeinen Primfaktor der Form $2^m + 1$ mehr als einmal. Solche Werte von N unterhalb von 300 sind die folgenden 38: $2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272$.

NACHTRÄGE.

Zu Artikel 28. Die unbestimmte Gleichung $ax = by \pm 1$ wurde nicht zuerst vom berühmten Euler gelöst (wie dort gesagt wird), sondern schon von Bachet de Meziriac, einem Geometer des 17. Jahrhunderts und dem berühmten Herausgeber und Kommentator Diophants, dem der berühmte La Grange diese Ehre zugesprochen hat (*Add. à l'Algèbre d'Euler p.* 525, wo zugleich die Art der Methode angegeben ist). Bachet teilte seine Entdeckung in der zweiten Auflage seines Buches *Problèmes plaisans et délectables qui se font par les nombres*, 1624, mit; in der ersten Auflage (Lyon 1612), die ich allein einsehen konnte, findet sie sich noch nicht, wird aber bereits angekündigt.

Zu den Artikeln 151, 296, 297. Der berühmte Le Gendre hat seinen Beweis in seinem ausgezeichneten Werk *Essai d'une théorie des nombres*, S. 214 ff., erneut dargelegt, jedoch ohne wesentliche Änderung; daher bleibt diese Methode auch weiterhin allen in Artikel 297 vorgebrachten Einwänden ausgesetzt. Der Satz (auf dem eine der Annahmen beruht), dass sich in jeder arithmetischen Folge $l, l+k, l+2k$, usw., Primzahlen finden, wenn k und l keinen gemeinsamen Teiler haben, ist in diesem Werk zwar auf S. 12 ff. ausführlicher betrachtet worden; doch scheint den Anforderungen geometrischer Strenge noch nicht genügt zu sein. Aber auch dann, wenn dieser Satz vollständig bewiesen ist, bleibt die andere Annahme bestehen (dass es Primzahlen der Form $4n+3$ gibt, für die eine gegebene, positiv genommene Primzahl der Form $4n+1$ ein quadratischer Nichtrest ist), und ich weiß nicht, ob sie sich *streng* beweisen lässt, ohne das Fundamentaltheorem selbst schon *vorauszusetzen*. Ferner ist zu beachten, dass der berühmte Le Gendre diese letztere Annahme nicht stillschweigend gemacht, sondern sie auch selbst nicht verschwiegen hat, S. 221.

Zu den Artikeln 288—293. Über denselben Gegenstand, der hier als besondere Anwendung der Theorie der ternären Formen dargestellt und hinsichtlich Strenge und Allgemeinheit so vollständig behandelt zu sein scheint, dass nichts mehr zu wünschen bleibt, hat der berühmte Le Gendre im dritten Teil seines Werkes auf S. 321—400 eine viel umfangreichere Untersuchung angestellt.[*)] Er benutzte ganz andere Prinzipien und Methoden als wir, geriet auf diesem Wege jedoch in mehrere Schwierigkeiten, die es ihm unmöglich machten, die Hauptsätze durch einen strengen Beweis zu stützen. Diese Schwierigkeiten hat er selbst offen angegeben; doch lassen sie sich, wenn wir nicht irren, vielleicht leichter beheben als die Schwierigkeit, dass auch in dieser Untersuchung der eben erwähnte Satz (In jeder arithmetischen Folge, usw.) vorausgesetzt wird, S. 371, am Ende der Anmerkung.

Zu Artikel 306 VIII. Im dritten Tausend negativer Determinanten wurden 37 irreguläre gefunden, von denen 18 den Irregularitätsindex 2 und die 19 übrigen den Index 3 haben.

[*)] Auch ohne unseren Hinweis werden sich die Leser hüten, unsere ternären Formen mit dem zu verwechseln, was der berühmte Le Gendre *forme trinaire d'un nombre* genannt hat. Mit diesem Ausdruck bezeichnete er nämlich die Zerlegung einer Zahl in drei Quadrate.

Zum selben Artikel X. Die hier gestellte Frage konnte vor Kurzem vollständig gelöst werden. Diese Untersuchung, die mehrere Teile sowohl der höheren Arithmetik als auch der Analysis auf bemerkenswerte Weise erhellt, werden wir so bald wie möglich in der Fortsetzung dieses Werkes mitteilen. Sie hat auch gezeigt, dass der Koeffizient m in Artikel 304 $= \gamma\pi = 2{,}3458847616$ ist, wobei γ dieselbe Größe wie in Artikel 302 und π, wie dort, den halben Umfang eines Kreises vom Radius 1 bezeichnet.

TABELLEN.

Tabelle I. (Artikel 58, 91)

		2. 3. 5. 7. 11	13. 17. 19. 23. 29	31. 37. 41. 43. 47	53. 59. 61. 67. 71	73. 79. 83. 89
3	2	1				
5	2	1. 3				
7	3	2. 1. 5				
9	2	1. ∗. 5. 4				
11	2	1. 8. 4. 7				
13	6	5. 8. 9. 7. 11				
16	5	∗. 3. 1. 2. 1	3			
17	10	10. 11. 7. 9. 13	12			
19	10	17. 5. 2. 12. 6	13. 8			
23	10	8. 20. 15. 21. 3	12. 17. 5			
25	2	1. 7. ∗. 5. 16	19. 13. 18. 11			
27	2	1. ∗. 5. 16. 13	8. 15. 12. 11			
29	10	11. 27. 18. 20. 23	2. 7. 15. 24			
31	17	12. 13. 20. 4. 29	23. 1. 22. 21. 27			
32	5	∗. 3. 1. 2. 5	7. 4. 7. 6. 3	0		
37	5	11. 34. 1. 28. 6	13. 5. 25. 21. 15	27		
41	6	26. 15. 22. 39. 3	31. 33. 9. 36. 7	28. 32		
43	28	39. 17. 5. 7. 6	40. 16. 29. 20. 25	32. 35. 18		
47	10	30. 18. 17. 38. 27	3. 42. 29. 39. 43	5. 24. 25. 37		
49	10	2. 13. 41. ∗. 16	9. 31. 35. 32. 24	7. 38. 27. 36. 23		
53	26	25. 9. 31. 38. 46	28. 42. 41. 39. 6	45. 22. 33. 30. 8		
59	10	25. 32. 34. 44. 45	23. 14. 22. 27. 4	7. 41. 2. 13. 53	28	
61	10	47. 42. 14. 23. 45	20. 49. 22. 39. 25	13. 33. 18. 41. 40	51. 17	
64	5	∗. 3. 1. 10. 5	15. 12. 7. 14. 11	8. 9. 14. 13. 12	5. 1. 3	
67	12	29. 9. 39. 7. 61	23. 8. 26. 20. 22	43. 44. 19. 63. 64	3. 54. 5	
71	62	58. 18. 14. 33. 43	27. 7. 38. 5. 4	13. 30. 55. 44. 17	59. 29. 37. 11	
73	5	8. 6. 1. 33. 55	59. 21. 62. 46. 35	11. 64. 4. 51. 31	53. 5. 58. 50. 44	
79	29	50. 71. 34. 19. 70	74. 9. 10. 52. 1	76. 23. 21. 47. 55	7. 17. 75. 54. 33	4
81	11	25. ∗. 35. 22. 1	38. 15. 12. 5. 7	14. 24. 29. 10. 13	45. 53. 4. 20. 33	48. 52
83	50	3. 52. 81. 24. 72	67. 4. 59. 16. 36	32. 60. 38. 49. 69	13. 20. 34. 53. 17	43. 47
89	30	72. 87. 18. 7. 4	65. 82. 53. 31. 29	57. 77. 67. 59. 34	10. 45. 19. 32. 26	68. 46. 27
97	10	86. 2. 11. 53. 82	83. 19. 27. 79. 47	26. 41. 71. 44. 60	14. 65. 32. 51. 25	20. 42. 91. 18

TABELLE II. (Artikel 99).

	1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37	+41	+43	+47	+53	+59	+61	+67	+71	+73	+79	+83	+89	+97
3			—		—		—		—			—	—		—				—	—		—	—			—
5	—			—		—			—		—	—		—				—	—		—		—		—	
7		—			—	—				—	—		—		—		—			—	—		—			
11			—	—		—				—		—	—			—	—	—		—	—				—	—
13	—		—				—	—		—	—				—		—		—				—			
17	—	—					—	—	—						—	—	—	—		—				—	—	
19				—	—	—		—	—	—					—	—			—			—		—		
23		—	—				—			—	—	—		—		—		—			—	—				
29	—			—	—		—			—	—						—	—		—	—			—		
31		—		—	—				—			—		—		—		—		—	—					—
37	—		—		—	—							—	—		—	—			—	—	—		—		
41	—	—		—						—		—	—	—	—			—	—			—		—		
43						—	—	—		—		—		—	—	—	—	—		—			—	—		—
47		—	—		—			—					—			—	—	—	—		—		—	—	—	—
53	—				—	—	—	—			—		—		—	—	—	—							—	—
59			—	—	—			—	—		—			—			—	—			—		—			
61	—		—	—			—		—					—		—			—			—		—		—
67								—	—	—	—		—			—		—		—	—	—		—	—	
71		—	—	—					—		—		—		—						—	—	—	—	—	
73	—	—	—						—	—			—	—					—	—	—	—	—		—	—
79		—		—		—	—		—	—		—								—		—	—	—	—	—
83			—		—	—		—		—	—	—	—	—				—	—					—		
89	—	—		—		—		—								—	—			—	—	—	—		—	—
97	—	—	—			—						—			—	—	—		—			—	—		—	—

Tabelle III. (Artikel 316).

3	(0) . . 3; (1) . . 6
7	(0) . . 142857
9	(0) . . 1; (1) . . 2; (2) . . 4; (3) . . 8; (4) . . 7; (5) . . 5
11	(0) . . 09; (1) . . 18; (2) . . 36; (3) . . 72; (4) . . 45
13	(0) . . 076923; (1) . . 461538
17	(0) . . 0588235294 117647
19	(0) . . 0526315789 47368421
23	(0) . . 0434782608 6956521739 13
27	(0) . . 037; (1) . . 074; (2) . . 148; (3) . . 296; (4) . . 592; (5) . . 185
29	(0) . . 0344827586 2068965517 24137931
31	(0) . . 0322580645 16129; (1) . . 5483870967 74193
37	(0) . . 027; (1) . . 135; (2) . . 675; (3) . . 378; (4) . . 891; (5) . . 459 (6) . . 297; (7) . . 486; (8) . . 432; (9) . . 162; (10) . . 810; (11) . . 054
41	(0) . . 02439; (1) . . 14634; (2) . . 87804; (3) . . 26829; (4) . . 60975; (5) . . 65853; (6) . . 95121; (7) . . 70731
43	(0) . . 0232558139 5348837209 3; (1) . . 6511627906 9767441860 4
47	(0) . . 0212765957 4468085106 3829787234 0425531914 893617
49	(0) . . 0204081632 6530612244 8979591836 7346938775 51
53	(0) . . 0188679245 283; (1) . . 4905660377 358; (2) . . 7547169811 320; (3) . . 6226415094 339
59	(0) . . 0169491525 4237288135 5932203389 8305084745 7627118644 06779661
61	(0) . . 0163934426 2295081967 2131147540 9836065573 7704918032 7868852459
67	(0) . . 0149253731 3432835820 8955223880 597; (1) . . 1791044776 1194029850 7462686567 164
71	(0) . . 0140845070 4225352112 6760563380 28169; (1) . . 8732394366 1971830985 9154929577 46478
73	(0) . . 01369863; (1) . . 06849315; (2) . . 34246575; (3) . . 71232876; (4) . . 56164383 (5) . . 80821917; (6) . . 04109589; (7) . . 20547945; (8) . . 02739726
79	(0) . . 0126582278 481; (1) . . 3670886075 949; (2) . . 6455696202 531 (3) . . 7215189873 417; (4) . . 9240506329 113; (5) . . 7974683544 303
81	(0) . . 012345679; (1) . . 135802469; (2) . . 493827160; (3) . . 432098765; (4) . . 753086419; (5) . . 283950617
83	(0) . . 0120481927 7108433734 9397590361 4457831325 3 (1) . . 6024096385 5421686746 9879518072 2891566265 0
89	(0) . . 0112359550 5617977528 0898876404 4943820224 7191 (1) . . 3370786516 8539325842 6966292134 8314606741 5730
97	(0) . . 0103092783 5051546391 7525773195 8762886597 9381443298 9690721649 4845360824 7422680412 3711340206 185567

INHALT.

Widmung ..... S. 3.

Vorrede ..... S. 5.

Erster Abschnitt. Die Kongruenz von Zahlen im Allgemeinen ..... S. 9.

Kongruente Zahlen, Moduln, Reste und Nichtreste, Artikel 1 f.
Kleinste Reste, 4.
Elementare Sätze über kongruente Zahlen, 5.
Einige Anwendungen, 12.

Zweiter Abschnitt. Kongruenzen ersten Grades ..... S. 14.

Vorbereitende Sätze über Primzahlen, Faktoren usw., Artikel 13.
Lösung der Kongruenzen ersten Grades, 26.
Bestimmung einer Zahl, die nach gegebenen Moduln gegebenen Resten kongruent ist, 32.
Lineare Kongruenzen mit mehreren Unbekannten, 37.
Verschiedene Sätze, 38.

Dritter Abschnitt. Reste von Potenzen ..... S. 38.

Die Reste der Glieder einer mit der Einheit beginnenden geometrischen Folge bilden eine periodische Folge, Artikel 45.
Zuerst werden Primzahlmoduln betrachtet.
Setzt man den Modul $= p$, so teilt die Anzahl der Glieder der Periode die Zahl $p - 1$, Artikel 49.
Der Fermatsche Satz, 50.
Wie vielen Zahlen Perioden entsprechen, deren Gliederzahl ein gegebener Teiler von $p - 1$ ist, Artikel 52.
Primitive Wurzeln, Basen, Indizes, 57.
Der Algorithmus der Indizes, 58.
Die Wurzeln der Kongruenz $x^n \equiv A$, Artikel 60.
Der Zusammenhang der Indizes in verschiedenen Systemen, 69.
Für besondere Zwecke geeignete Basen, 72.
Eine Methode zur Bestimmung primitiver Wurzeln, 73.
Verschiedene Sätze über Perioden und primitive Wurzeln, 75.
(Der Wilsonsche Satz, 76).
Moduln, die Potenzen von Primzahlen sind, Artikel 82.
Moduln, die Zweierpotenzen sind, 90.
Aus mehreren Primzahlen zusammengesetzte Moduln, 92.

Vierter Abschnitt. Kongruenzen zweiten Grades ..... S. 73.

Quadratische Reste und Nichtreste, Artikel 94.
Ist der Modul eine Primzahl, so ist die Anzahl der Reste, die kleiner als er sind, gleich der Anzahl der Nichtreste, 96.
Ob eine zusammengesetzte Zahl Rest oder Nichtrest einer gegebenen Primzahl ist, hängt von der Beschaffenheit ihrer Faktoren ab, 98.
Zusammengesetzte Moduln, 100.
Ein allgemeines Kriterium dafür, ob eine gegebene Zahl Rest oder Nichtrest einer gegebenen Primzahl ist, 106.
Untersuchungen über Primzahlen, für die gegebene Zahlen Reste oder Nichtreste sind, 107.
Der Rest -1, Artikel 108.
Die Reste $+2$ und -2, Artikel 112.
Die Reste $+3$ und -3, Artikel 117.
Die Reste $+5$ und -5, Artikel 121.
Über ± 7, Artikel 124.
Vorbereitung der allgemeinen Untersuchung, 125.
Durch Induktion wird ein allgemeiner (*fundamentaler*) Satz aufgestellt, und Folgerungen werden daraus gezogen, 130.
Ein strenger Beweis dieses Satzes, 135.
Eine entsprechende Methode zum Beweis des Satzes aus Artikel 114, 145.
Lösung des allgemeinen Problems, 146.
Lineare Formen, die alle Primzahlen enthalten, für die eine beliebige gegebene Zahl Rest oder Nichtrest ist, 147.
Die Arbeiten anderer über diese Untersuchungen, 151.
Nicht reine Kongruenzen zweiten Grades, 152.

Fünfter Abschnitt. Formen und unbestimmte Gleichungen zweiten Grades ..... S. 120.

Das Ziel der Untersuchung; Definition und Bezeichnung der Formen, Artikel 153.
Darstellung von Zahlen; die Determinante, 154.
Werte des Ausdrucks $\sqrt{(bb-ac)}$ (mod. M), zu denen die Darstellung der Zahl M durch die Form (a, b, c) gehört, 155.
Eine Form, die eine andere enthält oder unter einer anderen enthalten ist; eigentliche und uneigentliche Transformationen, 157.
Eigentliche und uneigentliche Äquivalenz, 158.
Entgegengesetzte Formen, 159, benachbarte Formen, 160.
Gemeinsame Teiler der Koeffizienten von Formen, 161.
Der Zusammenhang aller gleichartigen Transformationen einer gegebenen Form in eine gegebene Form, 162.
Ambige Formen, 163.
Ein Satz über den Fall, dass eine Form unter einer anderen zugleich eigentlich und uneigentlich enthalten ist, 164.
Allgemeines über Darstellungen von Zahlen durch Formen und ihren Zusammenhang mit Transformationen, 166.

Formen negativer Determinante, 171.
Besondere Anwendungen auf die Zerlegung von Zahlen in zwei Quadrate, in ein Quadrat und das Doppelte eines Quadrats sowie in ein Quadrat und das Dreifache eines Quadrats, 182.
Formen positiver, nichtquadratischer Determinante, 183.
Formen mit quadratischer Determinante, Artikel 206.
Formen, die unter anderen enthalten, ihnen aber nicht äquivalent sind, 213.
Formen der Determinante 0, Artikel 215.
Die allgemeine Lösung sämtlicher unbestimmter Gleichungen zweiten Grades mit zwei Unbekannten durch ganze Zahlen, 216.
Historische Anmerkungen, 222.

Weitere Untersuchungen über Formen.

Einteilung der Formen gegebener Determinante in Klassen, Artikel 223; der Klassen in Ordnungen, 226.
Einteilung der Ordnungen in Geschlechter, 228.
Komposition der Formen, 234.
Komposition der Ordnungen, 245, der Geschlechter, 246, der Klassen, 249.
Bei gegebener Determinante enthalten die einzelnen Geschlechter derselben Ordnung gleich viele Klassen, 252.
Vergleich der Anzahlen von Klassen in den einzelnen Geschlechtern verschiedener Ordnungen, 253.
Die Anzahl der ambigen Klassen, 257.
Mindestens der Hälfte aller für eine gegebene Determinante angebbaren Charaktere können keine eigentlich primitiven Geschlechter entsprechen (bei negativer Determinante positive), 261.
Ein zweiter Beweis des Fundamentaltheorems und der übrigen Sätze über die Reste $-1, +2, -2$, 262.
Die Hälfte der Charaktere, denen keine Geschlechter entsprechen können, wird näher bestimmt, 263.
Eine besondere Methode zur Zerlegung von Primzahlen in zwei Quadrate, 265.

Ein Exkurs mit einer Abhandlung über ternäre Formen, Artikel 266 ff.

Einige Anwendungen auf die Theorie der binären Formen.
Bestimmung einer Form, aus deren Verdopplung eine gegebene binäre Form des Hauptgeschlechts entsteht, 286.
Allen Charakteren außer den in den Artikeln 262, 263 als unmöglich erkannten entsprechen tatsächlich Geschlechter, 287 III.
Die Theorie der Zerlegung sowohl von Zahlen als auch von binären Formen in drei Quadrate, 288.
Beweis der Fermatschen Sätze, dass jede ganze Zahl in drei Dreieckszahlen oder vier Quadrate zerlegt werden kann, 293.
Lösung der Gleichung $axx + byy + czz = 0$, Artikel 294.

Die Methode, mit der der berühmte Le Gendre das Fundamentaltheorem behandelte, 296.
Darstellung der Null durch beliebige ternäre Formen, 299.
Die allgemeine Lösung unbestimmter Gleichungen zweiten Grades mit zwei Unbekannten durch rationale Größen, 300.
Die durchschnittliche Anzahl der Geschlechter. 301; der Klassen, 302.
Ein besonderer Algorithmus der eigentlich primitiven Klassen; reguläre und irreguläre Determinanten usw., 305.

Sechster Abschnitt. Verschiedene Anwendungen der vorangegangenen Untersuchungen ..... S. 380.
Zerlegung von Brüchen in einfachere, Artikel 309.
Umwandlung gewöhnlicher Brüche in Dezimalbrüche, 312.
Lösung der Kongruenz $xx \equiv A$ durch die Ausschlussmethode, 319.
Lösung der unbestimmten Gleichung $mxx + nyy = A$ durch Ausschlüsse, 323.
Eine andere Methode zur Lösung der Kongruenz $xx \equiv A$ für den Fall, dass A negativ ist, Artikel 327.
Zwei Methoden, zusammengesetzte Zahlen von Primzahlen zu unterscheiden und die Faktoren der Ersteren zu bestimmen, 329.

Siebter Abschnitt. Gleichungen, welche die Kreisteilung bestimmen .... S. 412.
Die Untersuchung wird auf den einfachsten Fall zurückgeführt, in dem die Anzahl der Teile, in die der Kreis geteilt werden soll, eine Primzahl ist, Artikel 336.
Gleichungen für trigonometrische Funktionen von Bögen, die ein Teil oder mehrere Teile des ganzen Umfangs sind; Zurückführung der trigonometrischen Funktionen auf Wurzeln der Gleichung $x^n - 1 = 0$, Artikel 337.
Theorie der Wurzeln dieser Gleichung (wobei vorausgesetzt wird, dass n eine Primzahl ist).
Lässt man die Wurzel 1 weg, so sind die übrigen Wurzeln (Ω) in der Gleichung $X = x^{n-1} + x^{n-2} + \text{usw.} + x + 1 = 0$ enthalten.
Die Funktion X lässt sich nicht in Faktoren niedrigeren Grades zerlegen, deren Koeffizienten sämtlich rational sind, 341.
Das Ziel der folgenden Untersuchungen wird dargelegt, 342.
Alle Wurzeln Ω werden in bestimmte Klassen (Perioden) eingeteilt, 343.
Verschiedene Sätze über diese Perioden, 344 ff.
Auf diese Untersuchungen wird die Lösung der Gleichung $X = 0$ gegründet, Artikel 352.
Beispiele für $n = 19$, wobei die Aufgabe auf zwei kubische Gleichungen und eine quadratische zurückgeführt wird, und für $n = 17$, wobei sie auf vier quadratische zurückgeführt wird, Artikel 353. 354.
Weitere Untersuchungen über diesen Gegenstand.
Summen mit einer geraden Anzahl von Gliedern sind reelle Größen, 355.
Die Gleichung, welche die Einteilung der Wurzeln Ω in zwei Perioden bestimmt, 356.
Beweis des im vierten Abschnitt erwähnten Satzes, 357.
Die Gleichung zur Einteilung der Wurzeln Ω in drei Perioden, 358.

Zurückführung der Gleichungen, durch die die Wurzeln Ω gefunden werden, auf reine Gleichungen, 359.

Anwendung der vorangegangenen Untersuchungen auf trigonometrische Funktionen.

Eine Methode zur Bestimmung der Winkel, denen die einzelnen Wurzeln Ω entsprechen, 361.

Tangens, Kotangens, Sekans und Kosekans werden ohne Division aus Sinus und Kosinus abgeleitet, 362.

Eine Methode zur schrittweisen Senkung des Grades der Gleichungen für trigonometrische Funktionen, 363.

Kreisteilungen, die sich durch quadratische Gleichungen oder durch geometrische Konstruktionen ausführen lassen, 365.

Nachträge ..... S. 465.

Tabellen ..... S. 467.

Gedruckt in Goslar bei E. W. G. Kircher.

ANHANG.

HANDSCHRIFTLICHE AUFZEICHNUNGEN VON GAUSS.

Zu Artikel 40. *Kommt eine dritte Zahl C hinzu, so sei λ' der größte gemeinsame Teiler der Zahlen λ, C, und man bestimme Zahlen k, γ so, dass $k\lambda + \gamma C = \lambda'$ ist; daraus folgt $k\alpha A + k\beta B + \gamma C = \lambda'$. Offenbar ist aber λ' ein gemeinsamer Teiler der Zahlen $A, B.C$, und zwar der größte; denn gäbe es einen größeren $= \theta$, so wäre*

$$k\alpha.\frac{A}{\theta} + k\beta.\frac{B}{\theta} + \gamma.\frac{C}{\theta} = \frac{\lambda'}{\theta} \quad \textit{ganze Zahl, Q. E. A.}$$

Damit ist das Gesuchte erreicht, wenn man $k\alpha = a,\ k\beta = b,\ \gamma = c,\ \lambda' = \mu$ setzt.

Zu Artikel 114. *Der Beweis lässt sich eleganter so führen:* $(a^{3n} - a^n)^2 = 2 + (a^{4n} + 1)(a^{2n} - 2)$, $(a^{3n} + a^n)^2 = -2 + (a^{4n} + 1)(a^{2n} + 2)$, *und daher* $\sqrt{2} \equiv \pm(a^{3n} - a^n)$, $\sqrt{-2} \equiv \pm(a^{3n} + a^n) \pmod{8n+1}$

Zu den in Artikel 256 VI angegebenen 16 positiven Determinanten der Form $8n+5$, für die die Anzahl der eigentlich primitiven Klassen dreimal so groß ist wie die der uneigentlich primitiven, '37, .. 573', sind hinzugefügt: *677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997; somit sind es unter 125 insgesamt 31.*

Zu den Worten des Artikels 301: Auf diese Weise findet man für die Summe der Anzahlen der Geschlechter für Determinanten $-$: bis -100 das Ergebnis $= 234,4$, während sie tatsächlich 233 beträgt. — — *Von -1 bis -3000, Tabelle 11166, Formel 11167,9.*

Zu Artikel 336. *Wären alle Zahlen der Form $2^{2^m} + 1$ Primzahlen, so wäre ein hinreichend angenäherter Ausdruck für die Anzahl der hier betrachteten Zahlen (N), die kleiner als die gegebene Zahl M sind, der folgende:* $\frac{1}{2}\left(\frac{\log M}{\log 2}\right)^2$.

Zu dem Satz in Artikel 42 über die Teiler eines Polynoms mit ganzzahligen Koeffizienten — — *1797, 22. Juli.*

Zu den Worten des Artikels 130: Nachdem wir streng bewiesen haben, dass jede Primzahl der Form $4n+1$, sowohl positiv als auch negativ genommen, Nichtrest einer kleineren Primzahl ist, — — *Diesen Beweis entdeckten wir 1796, am 8. April.*

Zu Artikel 131. *Das Fundamentaltheorem wurde im März 1795 durch Induktion entdeckt. Der erste Beweis, der in diesem Abschnitt mitgeteilt wird, wurde im April 1796 gefunden.*

Zu den Worten des Artikels 133: Gehen wir bei der Untersuchung (des Fundamentaltheorems) noch allgemeiner vor. Betrachten wir zwei beliebige ungerade, zueinander teilerfremde Zahlen mit beliebigen Vorzeichen, P und Q. — — *1796, 29. April.*

Zu den Worten des Artikels 145: Außerdem hätten damals die Sätze über die Reste $+2$ und -2 vorausgesetzt werden müssen; da unser Beweis jedoch ohne diese Sätze vollständig geführt ist, gewinnen wir daraus eine neue Methode, sie zu beweisen. — — *1797, 4. Februar.*

Zur Überschrift des fünften Abschnitts: Formen und unbestimmte Gleichungen zweiten Grades. — — *Seit dem 22. Juni 1796.*

Zu den Worten des Artikels 234: .. wir gehen zu einem anderen höchst wichtigen, bisher von niemandem berührten Gegenstand über, der Komposition der Formen. — — *Diese Untersuchungen wurden im Herbst 1798 begonnen.*

Zu den Worten des Artikels 262: Aus diesem Prinzip können wir eine neue Methode gewinnen, nicht nur das Fundamentaltheorem, sondern auch die übrigen Sätze des vorigen Abschnitts über die Reste $-1, +2, -2$ zu beweisen, — — *Die Grundlagen dieser Methode zeigten sich zuerst 1796, am 27. Juli; ausgearbeitet und in ihre gegenwärtige Form gebracht wurden sie aber im Frühjahr 1800.*

Zu den Worten des Artikels 266: .. da aber noch mehrere hierher gehörige, und zwar besonders schöne Wahrheiten übrig bleiben, deren eigentliche Quelle in der Theorie der ternären Formen zweiten Grades zu suchen ist, schalten wir hier einen kurzen Exkurs über diese Theorie ein, — — *14. Februar 1799.*

Zu den Worten des Artikels 272: nämlich indem wir zuerst zeigen, wie sich jede ternäre Form auf eine einfachere Form zurückführen lässt, und dann, dass die Anzahl der einfachsten Formen (zu denen man durch solche Reduktionen gelangt) für jede gegebene Determinante endlich ist. — — *1800, 13. Februar.*

Zu den Worten des Artikels 287 III: Auf ganz ähnliche Weise wird bewiesen, dass in der uneigentlich primitiven Ordnung alle Charaktere, die nach den Vorschriften des Artikels 264 II, III allein als möglich erkannt werden, möglich sind, seien sie P oder Q. — Diese Sätze usw. — — *Sie wurden erstmals im April 1798 mit Beweisen versehen.*

Zu den Worten des Artikels 302: Die durchschnittliche Anzahl der Klassen aber (die keiner Definition bedürfen wird) wächst sehr regelmäßig, — — *Die erste Idee zu Beginn des Jahres 1799.*

Zu den Worten des Artikels 306 X: Schließlich bemerken wir: Da alle in diesem und im vorigen Artikel betrachteten Eigenschaften vor allem von der Zahl n abhängen, die etwas Ähnliches ist wie $p - 1$ im dritten Abschnitt, verdient diese Zahl die größte Aufmerksamkeit; daher wäre es höchst wünschenswert, einen allgemeinen Zusammenhang zwischen ihr und der zugehörigen Determinante zu entdecken. — — *Es ist uns wunschgemäß—und so vollständig—gelungen, dass nichts mehr zu wünschen übrig bleibt. 30. November—3. Dezember 1800.*

Zu Artikel 365. *Dass sich der Kreis geometrisch in 17 Teile teilen lässt, entdeckten wir 1796, am 30. März.*

SCHLUSSBEMERKUNG ZUR NEUEN AUSGABE.

Dieser erste Band von Gauss' Werken ist ein Wiederabdruck der sieben Abschnitte der Disquis. Arithm., die 1801 im Oktavformat erschienen. Der achte Abschnitt, auf den an mehreren Stellen verwiesen wird und den Gauss wohl anfangs mit den übrigen veröffentlichen wollte, findet sich unter seinen Handschriften. Da er dessen Ausarbeitung aber nicht in gleicher Weise abgeschlossen hat wie die der ersten sieben Abschnitte, wird er sich in dieser Ausgabe den arithmetischen Abhandlungen des Nachlasses anschließen.

Textänderungen wurden in den Disqu. Ar. nur an den folgenden Stellen vorgenommen:

In Artikel 125 wurden die beiden Einschübe (wenn > 5) und (> 17; aber $-13N3$, $-17N5$) eingefügt.

In Artikel 126. *Beweis.* wurde 'in der Reihe (I) sind a Glieder durch p teilbar, b Glieder durch p^2, c Glieder durch p^3 usw.' an die Stelle von 'in der Reihe (I) sind a Glieder durch p, aber nicht durch p^2 teilbar, b Glieder durch p^2, aber nicht durch p^3, c Glieder durch p^3, aber nicht durch p^4 usw.' gesetzt.

In Artikel 128 III folgten auf 'Denn wenn $+b$ oder $-b \equiv r \pmod{p}$ ist, so ist $bb \equiv rr \pmod{2p}$, und daher ist das Glied $\frac{1}{2}(a - bb)$ durch p teilbar.' in der Ausgabe von 1801 noch die Worte 'und noch viel mehr $2(a - bb)$.'; diese wurden weggelassen.

In Artikel 129 wurde überall $2\sqrt{a+1}$ an die Stelle von $2\sqrt{a}$ und demnach 9 an die Stelle von 4 als diejenige Zahl gesetzt, unter die a jedenfalls nicht sinkt.

In Artikel 139 lautete der Schluss der Untersuchung über den Fall (4): 'Man erkennt leicht, dass sich aus dieser Gleichung $a'pRh$, $\pm ahpRa'$, $\pm aa'hRp$ herleiten lässt; dies stimmt mit dem in (2) Gefundenen überein. In den übrigen Fällen ist der Beweis derselbe.' Dies wurde entsprechend der Anmerkung geändert, die Gauss dem Artikel 2 der Abhandlung *Theorematis arithmetici demonstratio nova* beigefügt hat: 'Es wird nicht unangebracht sein, hier einen kleinen Fehler anzugeben und zu berichtigen, der sich durch eine mir unbekannte Nachlässigkeit in die Darstellung jenes Beweises eingeschlichen hat. Auf Seite (108) sind von Zeile (14) an die folgenden Überlegungen einzusetzen: Man erkennt leicht, dass sich aus dieser Gleichung $a'pRh \ldots (\alpha)$; $\pm ahRa' \ldots (\delta)$; $\pm ahRp \ldots (\gamma)$ herleiten lässt. Aus (α), das mit (α) in (2) übereinstimmt, folgt ebenso wie dort, dass entweder zugleich hRp, hRa' oder hNp, hNa' gilt. Im ersten Fall würde aber aus (δ) folgen, dass aRa' gilt, entgegen der Voraussetzung; daher ist hNp und somit nach (γ) auch aNp.

In Artikel 171 wurde nach einer handschriftlichen Bemerkung 'in der A weder größer als $\sqrt{\frac{4}{3}D}$, C, noch kleiner als $2B$ ist' an die Stelle von 'in der A nicht $> \sqrt{\frac{4}{3}D}$, B nicht $> \frac{1}{2}A$, C nicht $< A$ ist' gesetzt.

In Artikel 174. *Zweite Methode.* wurde 'Da a nicht $> \sqrt{\frac{4}{3}D}$ sein wird, werden offenbar alle auf diese Weise entstehenden Formen reduziert sein.' an die Stelle von 'Entstehen auf diese Weise Formen, in denen $a > \sqrt{\frac{4}{3}D}$ ist, so sind sie zu verwerfen; alle übrigen werden dagegen offenbar reduziert sein.' gesetzt.

In Artikel 256 VI enthält die frühere Ausgabe unter den positiven Determinanten der Form $8n+5$, für die die Anzahl der Klassen in der eigentlich primitiven Ordnung dreimal so groß ist wie die in der uneigentlich primitiven, auch die Determinante 397; zu ihr gehören jedoch gleich viele Klassen beider Arten.

In Artikel 302 wird nach einer handschriftlichen Bemerkung die Anzahl der Klassen für das zweite Tausend negativer Determinanten mit 28595 angegeben und nicht mit 28603 wie in der früheren Ausgabe.

In Artikel 303 werden die Anzahlen der Determinanten für die Klassifikationen II. 4; II. 5; IV. 2 nach den im Nachlass gefundenen Tafeln mit 31, 44, 69 angegeben und nicht mit 32, 42, 68 wie in der früheren Ausgabe.

In Artikel 325 wurde '$23t,\ 23t\pm1,\ 23t\pm5,\ 23t\pm7,\ 23t\pm9,\ 23t\pm10$. Nach deren Streichung bleiben 119, 127 übrig, die allein V einen quadratischen Wert geben' an die Stelle von '$23t,\ 23t\pm5,\ 23t\pm7, 23t\pm9,\ 23t\pm10$. Nach deren Streichung bleiben 119, 127, 137 übrig, von denen nur die ersten beiden V einen quadratischen Wert geben.' gesetzt.

In Artikel 360 IV wurden die Worte 'während bei den meisten anderen kubischen Gleichungen, deren Wurzeln sämtlich reell sind, die Dreiteilung sowohl eines Winkels als auch eines Verhältnisses nicht vermieden werden kann.' weggelassen, die auf 'zum Beispiel für $\beta = 3$ allein die Dreiteilung eines Winkels' folgten und deren Unrichtigkeit Gauss in seinem Handexemplar vermerkt hat.

Die Anmerkungen auf den Seiten 80, 102, 133, 211, 263, 265, 449 sind dem handschriftlichen Nachlass entnommen.

Um die Übersicht zu erleichtern, wurde die äußere Form der neuen Ausgabe gegenüber dem Druck dieses Werkes von 1801 in einigen Punkten verändert. Dazu glaubte man sich umso mehr berechtigt, als Gauss nach eigener Aussage auch in anderen Punkten auf Platzersparnis Rücksicht nahm. Viele Formeln, die in der Textzeile standen, wurden gesondert herausgesetzt. Die Inhaltsangaben, die gesammelt vor dem Werk standen, wurden auch den einzelnen Abteilungen vorangestellt und nicht nur den Abschnitten wie in der ersten Ausgabe; die allgemeineren darunter wurden als Seitenüberschriften verwendet.

GÖTTINGEN,
GEDRUCKT IN DER DIETERICHSCHEN UNIVERSITÄTS-DRUCKEREI
W. FR. KAESTNER.

Carl Friedrich Gauss

Arithmetische Abhandlungen

Deutsche Übersetzung

Band II: arithmetische Abhandlungen, Besprechungen und Nachlassstudien

Mit OpenAI GPT-6.1 Sol KI-übersetzt ins Deutsche.

Diese Auswahl enthält die historischen Titelblätter und die ersten fünf vollständigen Abhandlungen des zweiten Bandes: Einen neuen Beweis eines arithmetischen Satzes (Artikel 1–7); die Summation einiger besonderer Reihen (Artikel 1–36); Neue Beweise und Erweiterungen des Fundamentaltheorems in der Theorie der quadratischen Reste, mit der Einleitung, dem fünften Beweis (Artikel 1–3), dem sechsten Beweis (Artikel 1–6) und dem neuen Algorithmus (Artikel 1–6); sowie beide Abhandlungen zur Theorie der biquadratischen Reste (Artikel 1–23 und 24–76). Es folgen fünf Selbstbesprechungen von 1808–1831 und sieben Besprechungen fremder Schriften von 1809–1831. Letztere behandeln irrationale Wurzelgrößen, die Faktorentafeln von Chernac und Burckhardt, Erchingers Siebzehneckkonstruktion und Seebers positive ternäre quadratische Formen.
Die Nachlassstudien enthalten die Lösung einer reinen Kongruenz, Lehre von den Resten, sechstes Kapitel, erster Teil (Artikel 237–252); die Allgemeinen Untersuchungen über Kongruenzen, achtes Kapitel (Artikel 330–375 wie gedruckt, einschließlich des unvollendeten Schlusses von Artikel 375), mit R. Dedekinds historischen Bemerkungen; und die Weitere Entwicklung der Untersuchungen über reine Gleichungen, vollständig wie gedruckt (Artikel 1–19), mit Dedekinds Bemerkungen. Es folgt das Fragment Beweis einiger Sätze über die Perioden der Klassen binärer quadratischer Formen, mit beiden Sätzen, dem unvollendeten Schluss des zweiten Beweises und Sterns historischer Bemerkung.
Es folgen die mit [I.] und [II.] bezeichneten Fassungen der ersten Abhandlung Über den Zusammenhang zwischen der Anzahl der Klassen, in die binäre quadratische Formen zerfallen, und ihrer Determinante, vollständig wie gedruckt, jeweils mit Titel und Artikeln 1–8. Die Fassung [II.] wurde 1837 vorgelegt. Es folgen die Fragmente III–X mit ihren historischen Herausgeberanmerkungen. Dazu kommen historische Bemerkungen zu [I.]–[X.]. Die Geometrische Seite der ternären Formen schließt sich mit ihren beiden Diagrammen, kristallographischen Tabellen und Scherings historischen Bemerkungen an.

Die ursprünglich deutschen Titelangaben, Besprechungen, der Abteilungstitel des Nachlasses, die Fragmente III–IV und VIII–X, die geometrischen Notizen und die historischen Bemerkungen sind in modernem Deutsch wiedergegeben. Ihre historischen Originale werden gesondert mitgeliefert. Der Nachlasstext Zur Theorie der biquadratischen Reste, Fassung [I.], ist vollständig wie gedruckt mit Artikeln 1–19 und allen fünf Diagrammen enthalten. Es folgt die Fassung [II.], Vorbereitungen zur allgemeinen Theorie der biquadratischen Reste, vollständig wie gedruckt mit beiden vorbereitenden Abschnitten und Artikeln 1–12. Die Fassung [III.], Theorie der biquadratischen Reste, folgt vollständig wie gedruckt mit Titel und Artikeln 1–14, einschließlich der gemeinsamen Überschrift 7–8. Es folgt die Fassung [IV.] vollständig wie gedruckt, Artikel 1–5; ihre zweite Methode endet nach dem vierten Schritt. Es folgt die Fassung [V.] vollständig wie gedruckt, Artikel 1–17, mit ihrer bearbeitbaren Gitterzeichnung. Es folgt die Fassung [VI.] vollständig wie gedruckt, Artikel 1–6. Scherings vollständige historische Bemerkungen zu [I.]–[VI.] folgen. Die ursprünglich deutschen Texte dieser Fassungen sind in modernem Deutsch wiedergegeben; ihre historischen Originale werden gesondert mitgeliefert. Zur Theorie der komplexen Zahlen folgt vollständig wie gedruckt: sechs Bruchstücke [I.]–[VI.] über die Zerlegung der Kuben, die nächste ganze Zahl, Mensuren von Zahlen, Einheiten und Kongruenzen, gefolgt von Scherings historischen Bemerkungen. Die ursprünglich deutschen Passagen sind in modernem Deutsch wiedergegeben; ihre historischen Originale werden gesondert mitgeliefert. Die vollständige historische Tafel des quadratischen Charakters der Primzahlen von 2 bis 997 als Reste in Bezug auf die Primzahlen von 3 bis 503 als Teiler folgt. Die vollständige historische Tafel zur Umwandlung gewöhnlicher Brüche mit Nennern aus dem ersten Tausend in Dezimalbrüche folgt. Die vollständige historische Tafel der Häufigkeit der Primzahlen mit ihren Matrizen und abschließenden Bemerkungen folgt. Der vollständige Brief von Gauss an Enke vom 24. Dezember 1849 mit seinen Tabellen und der Erörterung der Häufigkeit der Primzahlen folgt. Der ursprünglich deutsche Brief ist in modernem Deutsch wiedergegeben; sein historisches Original wird gesondert mitgeliefert. Die vollständige historische Tafel der Anzahl der Klassen binärer quadratischer Formen mit ihren negativen und positiven Determinanten und allen gedruckten Zusammenstellungen folgt. Historische Werte und Abkürzungen bleiben erhalten. Der deutsche Titel ist in modernem Deutsch wiedergegeben; die historische Quelle wird gesondert mitgeliefert.

Die vollständige historische Tafel zur Kreisteilung mit allen neun Faktorentafeln und ihren gedruckten Verzeichnissen folgt. Der ursprünglich deutsche Titel und die Überschriften sind in modernem Deutsch wiedergegeben; die historische Quelle wird gesondert mitgeliefert. Die Neue Quadratur des Kreises folgt mit ihren vier vollständigen gedruckten Rechnungen und der Bogentafel einschließlich ihrer historischen Leerstellen. Zur Berechnung der gewöhnlichen Logarithmen folgt vollständig wie gedruckt mit ihren Tafeln und dem eingeklammerten historischen Herausgeberbericht. Das deutsche Original wird gesondert mitgeliefert; der deutsche Leseband enthält eine moderne deutsche Fassung. Die ersten zehntausend Quadrate, die Indizes der Primzahlen im höheren Zahlenbereich und die Hilfstafel zur Lösung der unbestimmten Gleichung mit dem Ausschlussverfahren folgen vollständig wie gedruckt. Die deutschen Originaltexte werden gesondert mitgeliefert; der deutsche Leseband enthält moderne deutsche Fassungen. Der achte Abschnitt, Ausführlichere Betrachtung einiger Untersuchungen zur Kreisteilung, folgt bis zum vollständigen gedruckten Ende in Artikel 373 einschließlich der Unterbrechung in Artikel 371. Beide Briefe von Gauss an Dirichlet vom 13. September 1826 und 30. Mai 1828 folgen vollständig mit ihren Zahlentafeln. Die deutschen Originale werden gesondert mitgeliefert; der deutsche Leseband enthält moderne deutsche Fassungen. Andere Bände von Gauss' Werken liegen außerhalb dieses Lesebands. Der vollständige erste Band ist im gesammelten Leseband enthalten.

Historische Vorlage: Carl Friedrich Gauss, Werke, zweiter Band, zweiter Abdruck, Göttingen, 1876.

Mit OpenAI GPT-6.1 Sol KI-übersetzt ins Deutsche.

Es folgen Scherings vollständige historische Schlussbemerkungen, das historische Inhaltsverzeichnis und der Göttinger Druckvermerk. Die ursprünglich deutschen Passagen sind in modernem Deutsch wiedergegeben; die historischen Originale werden gesondert mitgeliefert.

Quellen und Terminologie der Übersetzungen

Historischer Text: Carl Friedrich Gauss, *Werke*, zweiter Band, zweiter Abdruck, Göttingen, 1876. Historische Herausgeberbeiträge behalten ihre eigene Urheberschaft und ihre Unterschriften. Ursprünglich deutsche Passagen sind im deutschen Leseband in modernem Deutsch wiedergegeben; ihre historischen Originale werden gesondert mitgeliefert.
Diese englischen und deutschen Ausgaben sind mit OpenAI GPT-6.1 Sol KI-übersetzt; auch der Satz wurde durch KI erstellt. Die folgenden menschlichen Übersetzer und Autoren sind mit ihren Schriften Quellen für die jeweils bezeichnete Terminologie und den Sprachgebrauch. Mathematische Vorlage bleibt Gauss' originalsprachlicher Text.

H. Maser.

Deutscher Übersetzer und Herausgeber, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Entsprechende arithmetische Passagen und deutsche mathematische Terminologie.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead und Adam Miller Hiltebeitel.

Übersetzer von Gauss' *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX-Ausgabe. Verwandte englische geometrische Terminologie und Ausdrucksweise.
`https://www.gutenberg.org/ebooks/36856`

Paul Taylor; Bernard Leak.

Taylors englische Übersetzung von Gauss' zweitem Beweis des Fundamentalsatzes der Algebra, mit Korrekturen von Leak, 1983. Verwandte englische algebraische Terminologie. Die herangezogene Online-Ausgabe nennt Dezember 1983 als Übersetzungsdatum, August 2003 für die LaTeX-Fassung und den 8. Juni 2007 als letztes Änderungsdatum der zugrunde liegenden Quelle. Ihre Danksagung nennt Mark Wainwright für die Rückgabe von Taylors Notizen und Nikita Danilov für die Korrektur von Tippfehlern.
`https://www.paultaylor.eu/misc/gauss.html`

Ulrich Görtz.

Algebra, WS 2021/22, 3.1.1–3.1.3 und Anfang von 3.1.4; *Lineare Algebra II*, SS 2021, 18.4. Zeitgenössischer deutscher arithmetischer und algebraischer Sprachgebrauch.
`https://math.ug/a-ws2122/sect0006.html`
`https://math.ug/la2-ss21/sec-quotient-ring.html`

Nikolay Moshchevitin.

Eine Bemerkung über positiv definite quadratische Formen und rationale Punkte, arXiv:1510.06214v3. Verwandte zeitgenössische deutsche Terminologie quadratischer Formen.
`https://arxiv.org/abs/1510.06214v3`

Ian O. Angell und Moreton Moore.

Projections of cubic crystals, IUCr, Tabelle 2. Englische kristallographische Nomenklatur.
IUCr: Projections of cubic crystals, Tabelle 2

Th. Hahn, H. Klapper, U. Müller und M. I. Aroyo.

Point groups and crystal classes, *International Tables for Crystallography A*, 2016, Kapitel 3.2. Namen der Kristallformen.
https://doi.org/10.1107/97809553602060000930

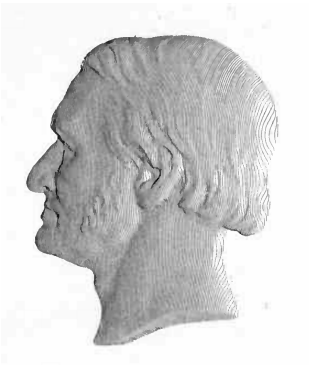
CARL FRIEDRICH GAUSS WERKE

BAND II.

CARL FRIEDRICH GAUSS

WERKE

ZWEITER BAND.



ZWEITER ABDRUCK

HERAUSGEGEBEN
VON DER
KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
ZU
GÖTTINGEN
1876.

EIN NEUER BEWEIS

EINES ARITHMETISCHEN SATZES

VON

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
VORGELEGT AM 15. JANUAR 1808.

Commentationes societatis regiae scientiarum Gottingensis. Vol. XVI.
Gottingae MDCCCVIII.

EIN NEUER BEWEIS
EINES ARITHMETISCHEN SATZES.

1.

Fragen der höheren Arithmetik zeigen sehr häufig eine eigentümliche Erscheinung, die in der Analysis viel seltener vorkommt und ihren Reiz erheblich steigert. Bei analytischen Untersuchungen können wir meist erst dann zu neuen Wahrheiten gelangen, wenn wir die Prinzipien, auf denen sie beruhen und die uns gleichsam den Weg zu ihnen öffnen müssen, zuvor gründlich beherrschen. In der Arithmetik dagegen treten sehr häufig durch Induktion und eine Art unerwarteten Glücks neue Wahrheiten von größter Eleganz hervor, deren Beweise so tief verborgen und in so große Dunkelheit gehüllt sind, dass sie sich allen Versuchen entziehen und selbst den scharfsinnigsten Untersuchungen den Zugang verwehren. Außerdem besteht zwischen arithmetischen Wahrheiten, die auf den ersten Blick völlig verschiedenartig erscheinen, ein so großer und wunderbarer Zusammenhang, dass wir nicht selten, während wir ganz anderes suchen, schließlich auf das Glücklichste zu dem so sehr ersehnten und zuvor in langen Überlegungen vergeblich gesuchten Beweis gelangen, und zwar auf einem ganz anderen Weg als dem erwarteten. Meist sind solche Wahrheiten aber von der Art, dass man auf mehreren sehr verschiedenen Wegen zu ihnen gelangen kann, und nicht immer sind die Wege, die sich zuerst anbieten, die kürzesten. Es muss daher gewiss hoch geschätzt werden, wenn es nach langer vergeblicher Untersuchung einer solchen Wahrheit, die dann zwar bewiesen wurde, aber auf ziemlich verborgenen Umwegen, schließlich gelingt, den einfachsten und eigentlichen Weg zu entdecken.

2.

Unter den im vorigen Artikel besprochenen Fragen nimmt der Satz einen hervorragenden Platz ein, der fast die gesamte Theorie der quadratischen Reste enthält und in den *Untersuchungen über höhere Arithmetik* (Abschnitt IV) mit dem Namen *Fundamentalsatz* ausgezeichnet ist. Als *erster* Entdecker dieses höchst eleganten Satzes ist ohne Zweifel der berühmte Legendre anzusehen, nachdem die großen Geometer Euler und Lagrange schon lange zuvor mehrere seiner besonderen Fälle durch Induktion entdeckt hatten. Ich halte mich hier nicht damit auf, die Beweisversuche dieser Männer aufzuzählen; wer möchte, möge das eben erwähnte Werk nachlesen. Zur Bestätigung des im vorigen Artikel Gesagten sei mir nur gestattet hinzuzufügen, was meine eigenen Versuche betrifft. Ich war im Jahr 1795 selbstständig auf den Satz gestoßen, als ich von allem, was in der höheren Arithmetik schon ausgearbeitet worden war, noch gar nichts wusste und von allen Hilfsmitteln der Literatur völlig abgeschnitten war. Doch ein ganzes Jahr lang quälte er mich und

entzog sich meinen angestrengtesten Bemühungen, bis ich schließlich den im vierten Abschnitt jenes Werkes gegebenen Beweis fand. Später boten sich mir drei weitere an, die auf ganz verschiedenen Prinzipien beruhen; einen davon habe ich im fünften Abschnitt gegeben, die übrigen, die ihm an Eleganz nicht nachstehen, werde ich bei anderer Gelegenheit veröffentlichen. Doch alle diese Beweise scheinen zwar hinsichtlich ihrer Strenge nichts zu wünschen übrigzulassen, sind aber aus zu verschiedenartigen Prinzipien hergeleitet, vielleicht mit Ausnahme des ersten, der jedoch mit recht mühsamen Überlegungen vorgeht und durch ziemlich weitläufige Rechnungen belastet ist. Ich zögere daher nicht auszusprechen, dass bisher ein *eigentlicher* Beweis gefehlt hat. Nun mögen die Sachkundigen beurteilen, ob der Beweis, den ich vor Kurzem entdeckt habe und den die folgenden Seiten enthalten, diesen Namen verdient.

3.

Satz. *Es sei p eine positive Primzahl; k eine beliebige, durch p nicht teilbare ganze Zahl; es seien*

A *Gesamtheit der Zahlen* $1,\ 2,\ 3\ \ldots.\ \frac{1}{2}(p-1)$

B *Gesamtheit dieser Zahlen* $\frac{1}{2}(p+1),\ \frac{1}{2}(p+3),\ \frac{1}{2}(p+5)\ \ldots.\ p-1$

Man bilde die Produkte aus k und den einzelnen Zahlen in A und nehme ihre kleinsten positiven Reste modulo p, die offenbar alle verschieden sind und teils zu A, teils zu B gehören. Gehören nun zu B insgesamt μ Reste, so ist k ein quadratischer Rest oder Nichtrest von p, je nachdem μ gerade oder ungerade ist.

Beweis. Die zu A gehörenden Reste seien $a,\ a'\ a''\ \ldots.$, die übrigen, zu B gehörenden $b, b', b'' \ldots.$. Offenbar sind die Ergänzungen der letzteren, $p-b, p-b', p-b'' \ldots.$, sämtlich von den Zahlen $a,\ a',\ a''\ \ldots.$ verschieden, füllen aber mit diesen zusammen die Gesamtheit A aus. Wir haben also

$$1\,.\,2\,.\,3\ \ldots.\ \tfrac{1}{2}(p-1) = aa'a''\ \ldots.\ (p-b)(p-b')(p-b'')\ \ldots.$$

Das letztere Produkt wird aber offenbar

$$\begin{aligned}&\equiv (-1)^{\mu} aa'a''\ \ldots.\ bb'b''\ \ldots.\ \equiv (-1)^{\mu} k\,.\,2k\,.\,3k\ \ldots.\ \tfrac{1}{2}(p-1)k\\ &\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}\,1\,.\,2\,.\,3\ \ldots.\ \tfrac{1}{2}(p-1) (\mathrm{mod}.p)\end{aligned}$$

Daher ist

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

oder $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, je nachdem μ gerade oder ungerade ist; daraus folgt unser Satz unmittelbar.

4.

Durch die Einführung einiger geeigneter Bezeichnungen können wir die folgenden Überlegungen erheblich verkürzen. Das Zeichen (k, p) soll uns daher die Anzahl derjenigen Produkte unter

$$k,\ 2k,\ 3k\ \ldots.\ \tfrac{1}{2}(p-1)k,$$

bezeichnen, deren kleinste positive Reste modulo p dessen Hälfte übersteigen. Ist ferner x eine beliebige nicht ganze Größe, so bezeichnen wir mit dem Zeichen $[x]$ die unmittelbar unter x liegende ganze Zahl, sodass $x - [x]$ stets eine positive Größe zwischen den Grenzen 0 und 1 ist. Die folgenden Beziehungen ergeben sich nun mit geringer Mühe:

I. $[x] + [-x] = -1$.

II. $[x] + h = [x + h]$, wenn h eine ganze Zahl ist.

III. $[x] + [h - x] = h - 1$.

IV. Ist $x - [x]$ ein Bruch kleiner als $\frac{1}{2}$, so ist $[2x] - 2[x] = 0$; ist aber $x - [x]$ größer als $\frac{1}{2}$, so ist $[2x] - 2[x] = 1$.

V. Liegt also der kleinste positive Rest der ganzen Zahl h modulo p unter $\frac{1}{2}p$, so ist $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 0$; liegt jener Rest aber über $\frac{1}{2}p$, so ist $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 1$.

VI. Daraus folgt sogleich $(k, p) =$

$$\left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \left[\frac{6k}{p}\right] \ldots. + \left[\frac{(p-1)k}{p}\right]$$
$$- 2\left[\frac{k}{p}\right] - 2\left[\frac{2k}{p}\right] - 2\left[\frac{3k}{p}\right] \ldots. - 2\left[\frac{\frac{1}{2}(p-1)k}{p}\right].$$

VII. Aus VI und I ergibt sich ohne Mühe

$$(k, p) + (-k, p) = \tfrac{1}{2}(p-1)$$

Daraus folgt, dass $-k$ dieselbe oder die entgegengesetzte Beziehung zu p hat (insofern es dessen quadratischer Rest oder Nichtrest ist) wie $+k$, je nachdem p die Form $4n + 1$ oder die Form $4n + 3$ hat. Im ersten Fall ist -1 offenbar ein Rest, im zweiten ein Nichtrest von p.

VIII. Die in VI gegebene Formel werden wir folgendermaßen umformen. Nach III ist

$$\left[\frac{(p-1)k}{p}\right] = k-1-\left[\frac{k}{p}\right],$$
$$\left[\frac{(p-3)k}{p}\right] = k-1-\left[\frac{3k}{p}\right],$$
$$\left[\frac{(p-5)k}{p}\right] = k-1-\left[\frac{5k}{p}\right]\ldots.$$

Wenden wir diese Ersetzungen auf die letzten $\frac{p\mp 1}{4}$ Glieder der oberen Reihe in jenem Ausdruck an, so erhalten wir

erstens, wenn p die Form $4n+1$ hat,

$$\begin{aligned}(k,p) = {} & \tfrac{1}{4}(k-1)(p-1) \\ & -2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\} \\ & -\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

zweitens, wenn p die Form $4n+3$ hat,

$$\begin{aligned}(k,p) = {} & \tfrac{1}{4}(k-1)(p+1) \\ & -2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\} \\ & -\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

IX. Für den besonderen Fall $k=+2$ folgt aus den eben gegebenen Formeln $(2,p) = \frac{1}{4}(p\mp 1)$, wobei das obere oder untere Zeichen zu nehmen ist, je nachdem p die Form $4n+1$ oder $4n+3$ hat. Somit ist $(2,p)$ gerade, also $2Rp$, wenn p die Form $8n+1$ oder $8n+7$ hat; dagegen ist $(2,p)$ ungerade und $2Np$, wenn p die Form $8n+3$ oder $8n+5$ hat.

5.

Satz. *Es sei x eine positive nicht ganze Größe, unter deren Vielfachen x, $2x$, $3x \ldots$. bis nx keines eine ganze Zahl ist; man setze $[nx] = h$, woraus leicht folgt, dass auch unter den Vielfachen der reziproken Größe $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x} \ldots$.. bis $\frac{h}{x}$ keine ganze Zahl vorkommt. Dann behaupte ich, es sei*

$$\left.\begin{array}{l} [x] + [2x] + [3x] \ldots + [nx] \\ + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \left[\frac{3}{x}\right] \ldots . + \left[\frac{h}{x}\right] \end{array}\right\} = nh.$$

Beweis. In der Reihe $[x] + [2x] + [3x] \ldots . + [nx]$, die wir $= \Omega$ setzen, sind die ersten Glieder bis einschließlich des Gliedes an der Stelle $\left[\frac{1}{x}\right]$ offenbar alle $= 0$; die folgenden bis zum Glied an der Stelle $\left[\frac{2}{x}\right]$ sämtlich $= 1$; die folgenden bis zum Glied an der Stelle $\left[\frac{3}{x}\right]$ sämtlich $= 2$, und so weiter. Daher ist

$$\left.\begin{array}{l} \Omega = 0 \times \left[\frac{1}{x}\right] \\ \quad + 1 \times \left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} \\ \quad + 2 \times \left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\} \\ \quad + 3 \times \left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} \\ \qquad \text{usw.} \\ \quad + (h-1)\left\{\left[\frac{h}{x}\right] - \left[\frac{h-1}{x}\right]\right\} \\ \quad + h\left\{n - \left[\frac{h}{x}\right]\right\} \end{array}\right\} = hn - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] \ldots . - \left[\frac{h}{x}\right]$$

Q. E. D.

6.

Satz. *Bezeichnen k, p beliebige positive ungerade, zueinander teilerfremde Zahlen, so ist*

$$\left.\begin{array}{l}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots.+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{array}\right\}=\tfrac{1}{4}(k-1)(p-1).$$

Beweis. Nehmen wir, was erlaubt ist, $k<p$ an, so ist $\frac{\frac{1}{2}(p-1)k}{p}$ kleiner als $\frac{1}{2}k$, aber größer als $\frac{1}{2}(k-1)$, also $\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=\frac{1}{2}(k-1)$. Daraus ergibt sich offenbar der vorliegende Satz unmittelbar aus dem vorhergehenden, wenn man dort $\frac{k}{p}=x$, $\frac{1}{2}(p-1)=n$, also $\frac{1}{2}(k-1)=h$ setzt.

Übrigens lässt sich auf ähnliche Weise beweisen, dass, wenn k eine zu p teilerfremde *gerade* Zahl ist, gilt:

$$\left.\begin{array}{l}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots.+\left[\frac{\frac{1}{2}kp}{k}\right]\end{array}\right\}=\tfrac{1}{4}k(p-1)$$

Doch halten wir uns bei diesem für unser Vorhaben nicht notwendigen Satz nicht auf.

7.

Aus der Verbindung des vorhergehenden Satzes mit der Aussage VIII des Artikels 4 folgt nun unmittelbar der Fundamentalsatz. Bezeichnen nämlich k, p beliebige verschiedene positive Primzahlen, und setzen wir

$$(k,p) + \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] \ldots . + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] = L$$

$$(p,k) + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] \ldots . + \left[\frac{\frac{1}{2}(k-1)p}{k}\right] = M$$

so ist nach VIII des Artikels 4 klar, dass L und M stets gerade Zahlen sind. Nach dem Satz des Artikels 6 ist aber

$$L + M = (k,p) + (p,k) + \tfrac{1}{4}(k-1)(p-1)$$

Wann immer also $\frac{1}{4}(k-1)(p-1)$ gerade ist, was geschieht, wenn für beide k, p oder wenigstens für eine von ihnen die Form $4n+1$ vorliegt, müssen (k,p) und (p,k) notwendig entweder beide gerade oder beide ungerade sein. Ist hingegen $\frac{1}{4}(k-1)(p-1)$ ungerade, was geschieht, wenn beide k, p die Form $4n+3$ haben, so muss notwendig eine der Zahlen (k,p), (p,k) gerade, die andere ungerade sein. Im ersten Fall sind daher die Beziehung von k zu p und die Beziehung von p zu k (insofern eine der beiden ein Rest oder Nichtrest der anderen ist) gleich, im zweiten entgegengesetzt.

Q. E. D.

SUMMATION

EINIGER BESONDERER

REIHEN

VON

CARL FRIEDRICH GAUSS

DER GESELLSCHAFT VORGELEGT AM XXIV. AUGUST MDCCCVIII.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. I.
Gottingae MDCCCXI.

SUMMATION

EINIGER BESONDERER REIHEN.

1.

Unter den bedeutenderen Wahrheiten, zu denen die Theorie der Kreisteilung den Zugang eröffnet hat, nimmt die in den Disquiss. Arithmet., Art. 356, angegebene Summation einen hervorragenden Platz ein. Das liegt sowohl an ihrer besonderen Eleganz und erstaunlichen Fruchtbarkeit, die eine andere Untersuchung später ausführlicher darzustellen Gelegenheit geben wird, als auch an den ungewöhnlichen Schwierigkeiten ihres strengen und vollständigen Beweises. Diese Schwierigkeiten hätte man umso weniger erwarten sollen, als sie weniger den Satz selbst als vielmehr eine gewisse Einschränkung des Satzes betreffen: Lässt man diese außer Betracht, so steht sofort ein Beweis zur Verfügung, der sich sehr leicht aus der in jenem Werk entwickelten Theorie ergibt. Der Satz wurde dort in folgender Form angegeben. Es sei n eine Primzahl; alle quadratischen Reste von n zwischen den Grenzen 1 und $n-1$ einschließlich seien unbestimmt durch a bezeichnet und alle Nichtreste zwischen denselben Grenzen durch b, schließlich bezeichne ω den Bogen $\frac{360^0}{n}$ und k eine beliebige feste ganze Zahl, die nicht durch n teilbar ist. Dann gilt

I. für einen Wert von n von der Form $4m+1$:

$$\begin{aligned}
\Sigma \cos ak\omega &= -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n} \\
\Sigma \cos bk\omega &= -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ und somit} \\
\Sigma \cos ak\omega - \Sigma \cos bk\omega &= \pm\sqrt{n} \\
\Sigma \sin ak\omega &= 0 \\
\Sigma \sin bk\omega &= 0
\end{aligned}$$

II. für einen Wert von n von der Form $4m+3$:

$$\begin{aligned}
\Sigma \cos ak\omega &= -\tfrac{1}{2} \\
\Sigma \cos bk\omega &= -\tfrac{1}{2} \\
\Sigma \sin ak\omega &= \pm\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin bk\omega &= \mp\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin ak\omega - \Sigma \sin bk\omega &= \pm\sqrt{n}
\end{aligned}$$

Diese Summationen sind an der angeführten Stelle mit voller Strenge bewiesen worden. Hier bleibt nur die Schwierigkeit, das *Vorzeichen* zu bestimmen, das vor den Wurzelausdruck zu setzen ist. Ohne Mühe lässt sich zwar zeigen, dass dieses Vorzeichen insofern von der Zahl k abhängt, als für alle

Werte von k, die quadratische Reste von n sind, stets *dasselbe* Vorzeichen gelten muss und für alle Werte von k, die quadratische Nichtreste von n sind, das entgegengesetzte. Damit kommt es nur auf den Wert $k = 1$ an: Sobald das für diesen Wert geltende Vorzeichen bekannt ist, stehen auch die Vorzeichen für alle übrigen Werte von k sofort zur Verfügung. Doch gerade bei dieser Frage, die auf den ersten Blick zu den leichteren zu gehören scheint, stoßen wir auf unerwartete Schwierigkeiten, und die Methode, unter deren Führung wir bisher ohne Hindernisse vorangekommen waren, verweigert jede weitere Hilfe.

2.

Bevor wir weitergehen, wird es nützlich sein, einige Beispiele unserer Summation zahlenmäßig durchzurechnen; zuvor sollen jedoch einige allgemeine Beobachtungen stehen.

I. Im Fall, dass n eine Primzahl von der Form $4m + 1$ ist, seien alle quadratischen Reste von n zwischen 1 und $\frac{1}{2}(n-1)$ einschließlich unbestimmt durch a' und alle Nichtreste zwischen denselben Grenzen durch b' dargestellt. Bekanntlich sind dann alle $n - a'$ unter den a und alle $n - b'$ unter den b enthalten. Da alle a', b', $n - a'$, $n - b'$ zusammen offenbar die gesamte Menge der Zahlen 1, 2, 3 .... $n - 1$ ausfüllen, umfassen alle a' zusammen mit allen $n-a'$ sämtliche a; ebenso umfassen alle b' zusammen mit allen $n-b'$ sämtliche b. Daher ist

$$\begin{aligned}
\Sigma \cos ak\omega &= \Sigma \cos a'k\omega + \Sigma \cos(n - a')k\omega \\
\Sigma \cos bk\omega &= \Sigma \cos b'k\omega + \Sigma \cos(n - b')k\omega \\
\Sigma \sin ak\omega &= \Sigma \sin a'k\omega + \Sigma \sin(n - a')k\omega \\
\Sigma \sin bk\omega &= \Sigma \sin b'k\omega + \Sigma \sin(n - b')k\omega
\end{aligned}$$

Da nun $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, $\sin(n - b')k\omega = -\sin b'k\omega$ gilt, ergibt sich unmittelbar

$$\begin{aligned}
\Sigma \sin ak\omega &= \Sigma \sin a'k\omega - \Sigma \sin a'k\omega = 0 \\
\Sigma \sin bk\omega &= \Sigma \sin b'k\omega - \Sigma \sin b'k\omega = 0
\end{aligned}$$

Die Summation der Kosinus nimmt dagegen die Form

$$\begin{aligned}
\Sigma \cos ak\omega &= 2\Sigma \cos a'k\omega \\
\Sigma \cos bk\omega &= 2\Sigma \cos b'k\omega
\end{aligned}$$

an, sodass gelten muss:

$$\begin{aligned}
1 + 4\Sigma \cos a'k\omega &= \pm\sqrt{n} \\
1 + 4\Sigma \cos b'k\omega &= \mp\sqrt{n} \\
2\Sigma \cos a'k\omega - 2\Sigma \cos b'k\omega &= \pm\sqrt{n}
\end{aligned}$$

II. Im Fall, dass n von der Form $4m + 3$ ist, ist die Ergänzung jedes Restes a zu n ein Nichtrest und die Ergänzung jedes b ein Rest. Somit stimmen sämtliche $n-a$ mit sämtlichen b und sämtliche $n-b$ mit sämtlichen a überein. Daraus folgt

$$\Sigma \cos ak\omega = \Sigma \cos(n-b)k\omega = \Sigma \cos bk\omega$$

Da also sämtliche a und b zusammen alle Zahlen 1, 2, $3 \ldots . n-1$ ausfüllen und somit $\Sigma \cos ak\omega + \Sigma \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \text{usw.} + \cos(n-1)k\omega = -1$ gilt, ergeben sich die Summationen

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$

unmittelbar. Ebenso ist

$$\Sigma \sin ak\omega = \Sigma \sin(n-b)k\omega = -\Sigma \sin bk\omega$$

woraus ersichtlich ist, wie von den beiden Summationen

$$2\Sigma \sin ak\omega = \pm\sqrt{n}$$
$$2\Sigma \sin bk\omega = \mp\sqrt{n}$$

die eine von der anderen abhängt.

3.

Hier folgen nun die Zahlenrechnungen für einige Beispiele:

I. Für $n = 5$ gibt es einen Wert von a', nämlich $a' = 1$, und einen Wert von b', nämlich $b' = 2$. Es ist

$$\cos\omega = +0{,}3090169944 \qquad \cos 2\omega = -0{,}8090169944$$

und somit $1 + 4\cos\omega = +\sqrt{5}$, $\quad 1 + 4\cos 2\omega = -\sqrt{5}$.

II. Für $n = 13$ gibt es drei Werte von a', nämlich 1, 3, 4, und ebenso viele Werte von b', nämlich 2, 5, 6. Daraus berechnen wir

$\cos\omega$	$= +0{,}8854560257$	$\cos 2\omega$	$= +0{,}5680647467$
$\cos 3\omega$	$= +0{,}1205366803$	$\cos 5\omega$	$= -0{,}7485107482$
$\cos 4\omega$	$= -0{,}3546048870$	$\cos 6\omega$	$= -0{,}9709418174$
Summe	$= +0{,}6513878190$	Summe	$= -1{,}1513878189$

Daher $1 + 4\Sigma \cos a'\omega = +\sqrt{13}$, $\quad 1 + 4\Sigma \cos b'\omega = -\sqrt{13}$.

III. Für $n = 17$ haben wir vier Werte von a', nämlich 1, 2, 4, 8, und ebenso viele Werte von b', nämlich 3, 5, 6, 7. Daraus berechnen sich die Kosinus:

$$\begin{array}{rcl|rcl} \cos\omega & = & +0{,}9324722294 & \cos 3\omega & = & +0{,}4457383558 \\ \cos 2\omega & = & +0{,}7390089172 & \cos 5\omega & = & -0{,}2736629901 \\ \cos 4\omega & = & +0{,}0922683595 & \cos 6\omega & = & -0{,}6026346364 \\ \cos 8\omega & = & -0{,}9829730997 & \cos 7\omega & = & -0{,}8502171357 \\ \hline \text{Summe} & = & +0{,}7807764064 & \text{Summe} & = & -1{,}2807764065 \end{array}$$

Daher $1 + 4\Sigma \cos a'\omega = +\sqrt{17}, \quad 1 + 4\Sigma \cos b'\omega = -\sqrt{17}$.

IV. Für $n = 3$ gibt es nur einen Wert von a, nämlich $a = 1$, dem

$$\sin\omega = +0{,}8660254038$$

entspricht. Daher $2\sin\omega = +\sqrt{3}$.

V. Für $n = 7$ gibt es drei Werte von a, nämlich 1, 2, 4. Daraus ergeben sich die Sinus:

$$\begin{array}{rcl} \sin\omega & = & +0{,}7818314825 \\ \sin 2\omega & = & +0{,}9749279122 \\ \sin 4\omega & = & -0{,}4338837391 \\ \hline \text{Summe} & = & +1{,}3228756556, \end{array} \text{ und somit } 2\Sigma \sin a\omega = +\sqrt{7}.$$

VI. Für $n = 11$ sind die Werte von a gleich 1, 3, 4, 5, 9. Ihnen entsprechen die Sinus:

$$\begin{array}{rcl} \sin\omega & = & +0{,}5406408175 \\ \sin 3\omega & = & +0{,}9898214419 \\ \sin 4\omega & = & +0{,}7557495744 \\ \sin 5\omega & = & +0{,}2817325568 \\ \sin 9\omega & = & -0{,}9096319954 \\ \hline \text{Summe} & = & +1{,}6583123952, \end{array} \text{ und daher } 2\Sigma \sin a\omega = +\sqrt{11}.$$

VII. Für $n = 19$ sind die Werte von a gleich 1, 4, 5, 6, 7, 9, 11, 16, 17. Ihnen entsprechen die Sinus:

$$\begin{aligned}
\sin\omega &= +0{,}3246994692\\
\sin 4\omega &= +0{,}9694002659\\
\sin 5\omega &= +0{,}9965844930\\
\sin 6\omega &= +0{,}9157733267\\
\sin 7\omega &= +0{,}7357239107\\
\sin 9\omega &= +0{,}1645945903\\
\sin 11\omega &= -0{,}4759473930\\
\sin 16\omega &= -0{,}8371664783\\
\sin 17\omega &= -0{,}6142127127\\
\hline
\text{Summe} &= +2{,}1794494718, \text{ und somit } 2\Sigma\sin a\omega = +\sqrt{19}.
\end{aligned}$$

4.

In allen diesen Beispielen erhält der Wurzelausdruck das positive Vorzeichen. Dasselbe bestätigt sich leicht auch für die größeren Werte $n = 23$, $n = 29$ usw.; daraus ergibt sich bereits eine hohe Wahrscheinlichkeit, dass dies ebenso allgemein gilt. Ein Beweis dieser Erscheinung lässt sich jedoch nicht aus den an der angeführten Stelle dargelegten Grundsätzen gewinnen; mit vollem Recht ist sie als Gegenstand einer tieferen Untersuchung anzusehen. Diese Abhandlung soll daher einen strengen Beweis dieses höchst eleganten Satzes vorlegen, der zuvor mehrere Jahre lang auf verschiedene Weise vergeblich versucht worden war und schließlich durch ungewöhnliche und recht subtile Überlegungen gelang. Zugleich werden wir den Satz unter Wahrung, oder vielmehr Steigerung, seiner Eleganz zu weit größerer Allgemeinheit führen. Als krönenden Abschluss werden wir schließlich den erstaunlichen und sehr engen Zusammenhang zwischen dieser Summation und einem anderen arithmetischen Satz von höchster Bedeutung zeigen. Wir hoffen, dass diese Untersuchungen den Geometern an sich willkommen sein werden und dass auch die Methoden, durch die wir all dies erreichen konnten und die bei anderen Gelegenheiten ebenfalls nützlich sein können, ihrer Aufmerksamkeit würdig erscheinen werden.

5.

Unser Beweis geht aus der Betrachtung einer besonderen Art von Reihen hervor, deren Glieder von Ausdrücken wie

$$\frac{(1-x^m)\,(1-x^{m-1})\,(1-x^{m-2})\ldots.(1-x^{m-\mu+1})}{(1-x)\,(1-xx)\,(1-x^3)\ldots..(1-x^\mu)}$$

abhängen. Der Kürze halber bezeichnen wir einen solchen Bruch mit (m, μ) und schicken zunächst einige allgemeine Beobachtungen über solche Funktionen voraus.

I. Ist m eine positive ganze Zahl kleiner als μ, so verschwindet die Funktion (m, μ) offenbar, da der Zähler den Faktor $1 - x^0$ enthält. Für $m = \mu$ stimmen die Faktoren im Zähler in umgekehrter Reihenfolge mit denen im Nenner überein, woraus $(\mu, \mu) = 1$ folgt. Für den Fall schließlich, dass m eine positive ganze Zahl größer als μ ist, gelten die Formeln

$$(\mu+1,\mu) = \frac{1-x^{\mu+1}}{1-x} = (\mu+1,1)$$
$$(\mu+2,\mu) = \frac{(1-x^{\mu+2})\,(1-x^{\mu+1})}{(1-x)\qquad(1-xx)} = (\mu+2,2)$$
$$(\mu+3,\mu) = \frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)\qquad(1-xx)\qquad(1-x^3)} = (\mu+3,3) \text{ usw.}$$

oder allgemein

$$(m,\mu) = (m, m-\mu)$$

II. Ferner bestätigt sich leicht, dass allgemein

$$(m,\mu+1) = (m-1,\mu+1) + x^{m-\mu-1}(m-1,\mu)$$

gilt. Da ebenso

$$(m-1,\mu+1) = (m-2,\mu+1) + x^{m-\mu-2}(m-2,\mu)$$
$$(m-2,\mu+1) = (m-3,\mu+1) + x^{m-\mu-3}(m-3,\mu)$$
$$(m-3,\mu+1) = (m-4,\mu+1) + x^{m-\mu-4}(m-4,\mu), \text{ usw.}$$

ist und diese Reihe bis zu

$$\begin{aligned}(\mu+2,\mu+1) &= (\mu+1,\mu+1) + x(\mu+1,\mu)\\ &= (\mu,\mu) + x(\mu+1,\mu)\end{aligned}$$

fortgesetzt werden kann, sofern m eine positive ganze Zahl größer als $\mu+1$ ist, ergibt sich

$$\begin{aligned}(m,\mu+1) = (\mu,\mu) &+ x(\mu+1,\mu) + xx(\mu+2,\mu)\\ &+ x^3(\mu+3,\mu) + \text{usw.}\\ &+ x^{m-\mu-1}(m-1,\mu)\end{aligned}$$

Daraus ist ersichtlich: Ist für einen bestimmten Wert von μ jede Funktion (m, μ) bei positivem ganzzahligem m ein Polynom, so muss auch jede Funktion $(m, \mu+1)$ ein Polynom sein. Da diese Voraussetzung für $\mu = 1$ zutrifft, gilt sie also auch für $\mu = 2$ und damit auch für $\mu = 3$ usw. Das heißt, allgemein ist für jeden positiven ganzzahligen Wert von m die Funktion (m, μ) ein Polynom; gleichbedeutend damit ist das Produkt

$$(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \dots (1 - x^{m-\mu+1})$$

teilbar durch

$$(1 - x)(1 - x^2)(1 - x^3) \dots (1 - x^\mu)$$

6.

Wir betrachten nun zwei Reihen, die beide zu unserem Ziel führen können. Die erste Reihe ist

$$1 - \frac{1-x^m}{1-x} + \frac{(1-x^m)\,(1-x^{m-1})}{(1-x)\,(1-xx)} - \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)\quad(1-xx)\quad(1-x^3)} + \text{usw.}$$

oder

$$1 - (m,1) + (m,2) - (m,3) + (m,4) - \text{usw.}$$

die wir der Kürze halber mit $f(x,m)$ bezeichnen. Zunächst ist unmittelbar ersichtlich, dass diese Reihe, sobald m eine positive ganze Zahl ist, nach ihrem Glied an der Stelle $m+1$ (wobei $= \pm 1$ gilt) *abbricht* und dass ihre Summe in diesem Fall daher ein endliches Polynom in x sein muss. Ferner ergibt sich aus Art. 5, II, dass allgemein für jeden Wert von m

$$\begin{aligned} 1 &= 1 \\ -(m,1) &= -(m-1,1) - x^{m-1} \\ +(m,2) &= +(m-1,2) + x^{m-2}(m-1,1) \\ -(m,3) &= -(m-1,3) - x^{m-3}(m-1,2), \text{ usw.} \end{aligned}$$

und somit

$$\begin{aligned} f(x,m) = 1 - x^{m-1} &- (1-x^{m-2})(m-1,1) \\ &+ (1-x^{m-3})(m-1,2) \\ &- (1-x^{m-4})(m-1,3) + \text{usw.} \end{aligned}$$

gilt. Offenbar ist aber

$$\begin{aligned} (1-x^{m-2})(m-1,1) &= (1-x^{m-1})(m-2,1) \\ (1-x^{m-3})(m-1,2) &= (1-x^{m-1})(m-2,2) \\ (1-x^{m-4})(m-1,3) &= (1-x^{m-1})(m-2,3), \text{ usw.} \end{aligned}$$

woraus wir die folgende Gleichung ableiten:

$$f(x,m) = (1-x^{m-1})f(x,m-2) \;.\;.\;.\;.\;.\;.\;.\;.\; [1]$$

7.

Da für $m = 0$ die Gleichung $f(x, m) = 1$ gilt, ergibt die soeben gefundene Formel

$$\begin{aligned} f(x,2) &= 1 - x \\ f(x,4) &= (1-x)(1-x^3) \\ f(x,6) &= (1-x)(1-x^3)(1-x^5) \\ f(x,8) &= (1-x)(1-x^3)(1-x^5)(1-x^7), \text{ usw.} \end{aligned}$$

oder allgemein für jeden geraden Wert von m:

$$f(x,m) = (1-x)(1-x^3)(1-x^5)\ldots.(1-x^{m-1}) \ldots [2].$$

Da hingegen für $m = 1$ die Gleichung $f(x, m) = 0$ gilt, ist auch

$$\begin{aligned} f(x,3) &= 0 \\ f(x,5) &= 0 \\ f(x,7) &= 0 \text{ usw.} \end{aligned}$$

oder allgemein für jeden ungeraden Wert von m:

$$f(x,m) = 0$$

Die letztere Summation hätte man im Übrigen schon daraus ableiten können, dass in der Reihe

$$1 - (m,1) + (m,2) - (m,3) + \text{usw.} + (m,m-1) - (m,m)$$

das letzte Glied das erste aufhebt, das vorletzte das zweite usw.

8.

Für unser Ziel genügt zwar der Fall, dass m eine positive ungerade ganze Zahl ist. Wegen der Eigenart des Gegenstands lohnt es sich aber, auch über die Fälle, in denen m gebrochen oder negativ ist, einiges hinzuzufügen. Unsere Reihe bricht dann offenbar nicht mehr ab, sondern läuft ins Unendliche; außerdem sieht man leicht, dass sie divergent wird, sobald x ein Wert kleiner als 1 gegeben wird. Ihre Summation muss daher auf Werte von x beschränkt werden, die größer als 1 sind.

Nach Formel [1] in Art. 6 haben wir

$$f(x,-2) = \frac{1}{1-\frac{1}{x}}$$

$$f(x,-4) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}}$$

$$f(x,-6) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}} \cdot \frac{1}{1-\frac{1}{x^5}}, \text{ usw.}$$

sodass sich der Wert der Funktion $f(x,m)$ auch für einen negativen geraden ganzzahligen Wert von m in endlichen Gliedern angeben lässt. Für die übrigen Werte von m werden wir die Funktion $f(x,m)$ dagegen auf folgende Weise in ein *unendliches Produkt* umwandeln.

Wenn m einem negativen *unendlichen* Wert zustrebt, geht die Funktion $f(x,m)$ über in

$$1 + \frac{1}{x-1} + \frac{1}{x-1} \cdot \frac{1}{xx-1} + \frac{1}{x-1} \cdot \frac{1}{xx-1} \cdot \frac{1}{x^3-1} + \text{usw.}$$

Diese Reihe ist also gleich dem unendlichen Produkt

$$\frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}} \cdot \frac{1}{1-\frac{1}{x^5}} \cdot \frac{1}{1-\frac{1}{x^7}} \text{ usw. bis ins Unendliche.}$$

Da ferner allgemein

$$f(x,m) = f(x,m-2\lambda) \,.\, (1-x^{m-1})(1-x^{m-3}) \\ (1-x^{m-5}) \,..\, (1-x^{m-2\lambda+1})$$

ist, gilt

$$f(x,m) = f(x,-\infty) \,.\, (1-x^{m-1})(1-x^{m-3})(1-x^{m-5}) \\ \text{usw. bis ins Unendliche.} \\ = \frac{1-x^{m-1}}{1-x^{-1}} \cdot \frac{1-x^{m-3}}{1-x^{-3}} \cdot \frac{1-x^{m-5}}{1-x^{-5}} \cdot \frac{1-x^{m-7}}{1-x^{-7}} \\ \text{usw. bis ins Unendliche.}$$

Dessen Faktoren nähern sich im weiteren Verlauf offenbar immer mehr der Einheit.

Besondere Aufmerksamkeit verdient der Fall $m = -1$. Hier ist

$$f(x,-1) = 1 + x^{-1} + x^{-3} + x^{-6} + x^{-10} + \text{usw.}$$

Diese Reihe ist also gleich dem unendlichen Produkt

$$\frac{1-x^{-2}}{1-x^{-1}} \cdot \frac{1-x^{-4}}{1-x^{-3}} \cdot \frac{1-x^{-6}}{1-x^{-5}} \text{ usw.}$$

oder, wenn wir x für x^{-1} schreiben,

$$1+x+x^3+x^6+\text{usw.} = \frac{1-xx}{1-x} \cdot \frac{1-x^4}{1-x^3} \cdot \frac{1-x^6}{1-x^5} \cdot \frac{1-x^8}{1-x^7} \text{ usw.}$$

Diese Gleichheit zwischen zwei recht verwickelten Ausdrücken, auf die wir bei anderer Gelegenheit zurückkommen werden, ist in der Tat sehr bemerkenswert.

9.

Als Zweites betrachten wir die folgende Reihe:

$$1 + x^{\frac{1}{2}} \frac{1-x^m}{1-x} + x \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)} + x^{\frac{3}{2}} \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)} + \text{usw.}$$

oder

$$1 + x^{\frac{1}{2}}(m,1) + x(m,2) + x^{\frac{3}{2}}(m,3) + xx(m,4) + \text{usw.}$$

die wir mit $F(x,m)$ bezeichnen. Wir beschränken diese Untersuchung auf den Fall, dass m eine positive ganze Zahl ist, sodass auch diese Reihe stets mit ihrem Glied an der Stelle $m+1$ abbricht, wobei $= x^{\frac{1}{2}m}(m,m)$ gilt. Da

$$(m,m) = 1, \quad (m,m-1) = (m,1), \quad (m,m-2) = (m,2), \text{ usw.}$$

ist, lässt sich die Reihe auch so darstellen:

$$F(x,m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m,1) + x^{\frac{1}{2}(m-2)}(m,2) + x^{\frac{1}{2}(m-3)}(m,3) + \text{usw.}$$

Daraus ergibt sich

$$(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = 1 + x^{\frac{1}{2}}(m,1) + x(m,2) + x^{\frac{3}{2}}(m,3) + \text{usw.} + x^{\frac{1}{2}} \,.\, x^m + x \,.\, x^{m-1}(m,1) + x^{\frac{3}{2}} \,.\, x^{m-2}(m,2) + \text{usw.}$$

Da nun (Art. 5, II)

$$\begin{aligned}(m,1)+x^m &= (m+1,1)\\ (m,2)+x^{m-1}(m,1) &= (m+1,2)\\ (m,3)+x^{m-2}(m,2) &= (m+1,3),\ \text{usw.}\end{aligned}$$

gilt, erhalten wir

$$(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = F(x,m+1)\ \ldots\ldots\ [3]$$

Es ist aber $F(x,0)=1$; daher gilt

$$\begin{aligned}F(x,1) &= 1+x^{\frac{1}{2}}\\ F(x,2) &= (1+x^{\frac{1}{2}})(1+x)\\ F(x,3) &= (1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}}),\ \text{usw.}\end{aligned}$$

oder allgemein

$$\begin{aligned}F(x,m) = (1+x^{\frac{1}{2}})&(1+x)(1+x^{\frac{3}{2}})\\ &\ldots.(1+x^{\frac{1}{2}m})\ \ldots.\quad [4]\end{aligned}$$

10.

Nach diesen vorbereitenden Untersuchungen wollen wir unserem Ziel nun näherkommen. Für einen Primzahlwert von n sind die Quadrate 1, 4, $9\ldots.(\frac{1}{2}(n-1))^2$ untereinander sämtlich inkongruent modulo n. Ihre kleinsten Reste nach diesem Modul müssen daher mit den Zahlen a übereinstimmen, und somit ist

$$\begin{aligned}\Sigma\cos ak\omega &= \cos k\omega+\cos 4k\omega+\cos 9k\omega\\ &\qquad +\text{usw.}+\cos(\tfrac{1}{2}(n-1))^2k\omega\\ \Sigma\sin ak\omega &= \sin k\omega+\sin 4k\omega+\sin 9k\omega\\ &\qquad +\text{usw.}+\sin(\tfrac{1}{2}(n-1))^2k\omega\end{aligned}$$

Da ferner dieselben Quadrate 1, 4, $9\ldots.(\frac{1}{2}(n-1))^2$ in umgekehrter Reihenfolge zu $(\frac{1}{2}(n+1))^2$, $(\frac{1}{2}(n+3))^2$, $(\frac{1}{2}(n+5))^2\ldots.(n-1)^2$ kongruent sind, gilt auch

$$\begin{aligned}\Sigma\cos ak\omega &= \cos(\tfrac{1}{2}(n+1))^2k\omega\\ &\qquad +\cos(\tfrac{1}{2}(n+3))^2k\omega+\text{usw.}+\cos(n-1)^2k\omega\\ \Sigma\sin ak\omega &= \sin(\tfrac{1}{2}(n+1))^2k\omega\\ &\qquad +\sin(\tfrac{1}{2}(n+3))^2k\omega+\text{usw.}+\sin(n-1)^2k\omega\end{aligned}$$

Wir setzen also

$$\begin{aligned} T &= 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega \\ &\quad + \text{usw.} + \cos(n-1)^2 k\omega \\ U &= \quad \sin k\omega + \sin 4k\omega + \sin 9k\omega \\ &\quad + \text{usw.} + \sin(n-1)^2 k\omega \end{aligned}$$

Dann ist

$$\begin{aligned} 1 + 2\Sigma \cos ak\omega &= T \\ 2\Sigma \sin ak\omega &= U \end{aligned}$$

Daraus ist ersichtlich, dass die in Art. 1 angegebenen Summationen von der Summation der Reihen T und U abhängen. Wir lassen daher die ersteren beiseite, richten unsere Untersuchung auf diese Reihen und führen sie so allgemein durch, dass sie sowohl Primzahlwerte von n als auch beliebige zusammengesetzte Werte umfasst. Wir setzen dabei voraus, dass die Zahl k zu n teilerfremd ist: Der Fall, dass k und n einen gemeinsamen Teiler haben, lässt sich ohne Mühe auf diesen zurückführen.

11.

Wir bezeichnen die imaginäre Größe $\sqrt{-1}$ mit i und setzen

$$\cos k\omega + i \sin k\omega = r$$

Dann ist $r^n = 1$, oder r ist eine Wurzel der Gleichung $r^n - 1 = 0$. Man sieht leicht, dass sämtliche Zahlen k, $2k$, $3k \ldots . (n-1)k$ nicht durch n teilbar und untereinander inkongruent modulo n sind. Daher sind die Potenzen von r

$$1,\ r,\ rr,\ r^3 \ldots . r^{n-1}$$

sämtlich verschieden, während jede von ihnen auch der Gleichung $x^n - 1 = 0$ genügt. Aus diesem Grund stellen diese Potenzen *alle* Wurzeln der Gleichung $x^n - 1 = 0$ dar.

Diese Schlüsse würden nicht gelten, wenn k mit n einen gemeinsamen Teiler hätte. Wäre nämlich ν ein solcher gemeinsamer Teiler, so wäre $k \,.\, \frac{n}{\nu}$ durch n teilbar und damit eine niedrigere Potenz als r^n, nämlich $r^{\frac{n}{\nu}}$, gleich der Einheit. In diesem Fall stellen die Potenzen von r also höchstens $\frac{n}{\nu}$ Wurzeln der Gleichung $x^n - 1 = 0$ dar, und tatsächlich ergeben sie ebenso viele verschiedene Wurzeln, wenn ν der *größte* gemeinsame Teiler der Zahlen k, n ist. In unserem Fall, in dem k und n als teilerfremd vorausgesetzt sind, lässt sich r zweckmäßig eine *eigentliche Wurzel* der Gleichung $x^n - 1 = 0$ nennen.

Im anderen Fall dagegen, in dem k und n einen (größten) gemeinsamen Teiler ν hätten, würde r eine *uneigentliche Wurzel* jener Gleichung heißen. Dann wäre aber dieselbe r offenbar eine eigentliche Wurzel der Gleichung $x^{\frac{n}{\nu}} - 1 = 0$. Die einfachste uneigentliche Wurzel ist die Einheit, und im Fall, dass n eine Primzahl ist, gibt es überhaupt keine anderen uneigentlichen Wurzeln.

12.

Setzen wir nun

$$W = 1 + r + r^4 + r^9 + \text{usw.} + \text{usw.} + r^{(n-1)^2}$$

so ist offenbar $W = T + iU$; somit ist T der reelle Teil von W, und U geht aus dem imaginären Teil von W hervor, wenn der Faktor i weggelassen wird. Damit führt sich die ganze Frage auf die Bestimmung der Summe W zurück. Hierzu lässt sich entweder die in Art. 6 betrachtete Reihe verwenden oder diejenige, deren Summation wir in Art. 9 gezeigt haben; die erstere ist jedoch weniger geeignet, wenn n gerade ist. Dennoch hoffen wir, dass es den Lesern willkommen sein wird, wenn wir den Fall, dass n ungerade ist, nach zwei Methoden behandeln.

Zunächst sei also n eine ungerade Zahl, r bezeichne eine beliebige eigentliche Wurzel der Gleichung $x^n - 1 = 0$, und in der Funktion $f(x, m)$ werde $x = r$ und $m = n - 1$ gesetzt. Daraus ergibt sich offenbar

$$\begin{aligned}
\frac{1 - x^m}{1 - x} &= \frac{1 - r^{-1}}{1 - r} = -r^{-1} \\
\frac{1 - x^{m-1}}{1 - xx} &= \frac{1 - r^{-2}}{1 - rr} = -r^{-2} \\
\frac{1 - x^{m-2}}{1 - x^3} &= \frac{1 - r^{-3}}{1 - r^3} = -r^{-3}, \text{ usw.}
\end{aligned}$$

bis hin zu

$$\frac{1 - x}{1 - x^m} = \frac{1 - r^{-m}}{1 - r^m} = -r^{-m}$$

(Es ist nicht überflüssig, darauf hinzuweisen, dass diese Gleichungen nur insoweit gelten, als r als eigentliche Wurzel vorausgesetzt ist: Wäre r eine uneigentliche Wurzel, so würden bei einigen dieser Brüche Zähler und Nenner zugleich verschwinden, und die Brüche würden somit unbestimmt).

Daraus leiten wir die folgende Gleichung ab:

$$\begin{aligned}
f(r, n-1) &= 1 + r^{-1} + r^{-3} + r^{-6} + \text{usw.} + r^{-\frac{1}{2}(n-1)n} \\
&= (1 - r)(1 - r^3)(1 - r^5) \ldots . (1 - r^{n-2})
\end{aligned}$$

Dieselbe Gleichung gilt weiterhin, wenn wir r durch r^λ ersetzen, wobei λ eine beliebige zu n teilerfremde ganze Zahl bezeichnet: Dann ist auch r^λ eine eigentliche Wurzel der Gleichung $x^n - 1 = 0$. Ersetzen wir also r durch r^{n-2} oder, was dasselbe ist, durch r^{-2}, so erhalten wir

$$\begin{aligned} &1 + r^2 + r^6 + r^{12} + \text{usw.} + r^{(n-1)n} \\ &\quad = (1 - r^{-2})(1 - r^{-6})(1 - r^{-10}) \dots (1 - r^{-2(n-2)}) \end{aligned}$$

Multiplizieren wir beide Seiten dieser Gleichung mit

$$r \,.\, r^3 \,.\, r^5 \,.\, \dots \,.\, r^{(n-2)} = r^{\frac{1}{4}(n-1)^2}$$

so ergibt sich wegen

$$\begin{aligned} r^{2+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-3)^2}, \\ r^{(n-1)n+\frac{1}{4}n-1)^2} &= r^{\frac{1}{4}(n+1)^2} \\ r^{6+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-5)^2}, \\ r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+3)^2} \\ r^{12+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-7)^2}, \\ r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+5)^2}, \text{ usw.} \end{aligned}$$

die folgende Gleichung:

$$\begin{aligned} &r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \text{usw.} + r + 1 \\ &+ r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} \\ &\quad + \text{usw.} + r^{\frac{1}{4}(2n-2)^2} \\ &\quad = (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \dots (r^{n-2} - r^{-n+2}) \end{aligned}$$

oder, wenn wir die Glieder der linken Seite anders anordnen,

$$\begin{aligned} &1 + r + r^4 + \text{usw.} + r^{(n-1)^2} \\ &\quad = (r - r^{-1})(r^3 - r^{-3}) \dots (r^{n-2} - r^{-n+2}) \quad .. \quad [5] \end{aligned}$$

13.

Die Faktoren auf der rechten Seite der Gleichung [5] lassen sich auch folgendermaßen schreiben:

$$\begin{aligned} r - r^{-1} &= -(r^{n-1} - r^{-n+1}) \\ r^3 - r^{-3} &= -(r^{n-3} - r^{-n+3}) \\ r^5 - r^{-5} &= -(r^{n-5} - r^{-n+5}), \text{ usw.} \end{aligned}$$

bis hin zu

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2})$$

Damit nimmt die Gleichung diese Form an:

$$\begin{aligned} W = (-1)^{\frac{1}{2}(n-1)}&(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \\ &\ldots . (r^{n-1} - r^{-n+1}) \end{aligned}$$

Multiplizieren wir diese Gleichung mit [5] in ihrer ursprünglichen Form, so ergibt sich

$$\begin{aligned} W^2 = (-1)^{\frac{1}{2}(n-1)}&(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \\ &\ldots . (r^{n-1} - r^{-n+1}) \end{aligned}$$

wobei $(-1)^{\frac{1}{2}(n-1)}$ entweder $= +1$ oder $= -1$ ist, je nachdem, ob n die Form $4\mu + 1$ oder die Form $4\mu + 3$ hat. Daraus folgt

$$\begin{aligned} W^2 = \pm r^{\frac{1}{2}n(n-1)}&(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \\ &\ldots . (1 - r^{-2(n-1)}) \end{aligned}$$

Nun sieht man ohne Mühe, dass r^{-2}, r^{-4}, $r^{-6} \ldots . r^{-2n+2}$ sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ mit Ausnahme der Wurzel $x = 1$ darstellen. Daher muss die folgende Gleichung identisch für eine Unbestimmte gelten:

$$\begin{aligned} &(x - r^{-2})(x - r^{-4})(x - r^{-6}) \ldots . (x - r^{-2n+2}) \\ &\quad = x^{n-1} + x^{n-2} + x^{n-3} + \text{usw.} + x + 1 \end{aligned}$$

Setzen wir also $x = 1$, so erhalten wir

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \ldots . (1 - r^{-2n+2}) = n$$

und da offenbar $r^{\frac{1}{2}n(n-1)} = 1$ ist, geht unsere Gleichung in die folgende über:

$$W^2 = \pm n \ldots . \ldots . \ldots . \text{ [6]}$$

In dem Fall, dass n die Form $4\mu + 1$ hat, ist somit

$$W = \pm\sqrt{n}, \quad \text{und somit} \quad T = \pm\sqrt{n}, \quad U = 0$$

Im anderen Fall dagegen, in dem n die Form $4\mu + 3$ hat, ist

$$W = \pm i\sqrt{n}, \quad \text{und somit} \quad T = 0, \quad U = \pm\sqrt{n}$$

14.

Die Methode des vorigen Artikels liefert nur den absoluten Wert der Summen T, U und lässt offen, ob für T im ersten Fall und für U im zweiten Fall $= +\sqrt{n}$ oder $= -\sqrt{n}$ zu setzen ist. Dies lässt sich aber, wenigstens für den Fall $k = 1$, anhand der Gleichung [5] folgendermaßen entscheiden. Da für $k = 1$

$$\begin{aligned} r - r^{-1} &= 2i \sin\omega \\ r^3 - r^{-3} &= 2i \sin 3\omega \\ r^5 - r^{-5} &= 2i \sin 5\omega \text{ usw.} \end{aligned}$$

ist, geht jene Gleichung über in

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega$$

In dem Fall, dass n die Form $4\mu + 1$ hat, finden sich nun in der Folge der ungeraden Zahlen

$$1,\ 3,\ 5,\ 7 \ldots . \tfrac{1}{2}(n-3), \quad \tfrac{1}{2}(n+1) \ldots . (n-2)$$

$\frac{1}{4}(n-1)$ Zahlen, die kleiner als $\frac{1}{2}n$ sind und denen offenbar positive Sinuswerte entsprechen. Die übrigen $\frac{1}{4}(n-1)$ dagegen sind größer als $\frac{1}{2}n$, und ihnen entsprechen negative Sinuswerte. Das Produkt sämtlicher Sinuswerte ist daher gleich einer positiven Größe, multipliziert mit $(-1)^{\frac{1}{4}(n-1)}$. Somit ist W gleich einer positiven reellen Größe, multipliziert mit i^{n-1} oder mit 1, da $i^4 = 1$ ist und $n-1$ durch 4 teilbar ist: Die Größe W ist also reell und positiv. Daher gilt notwendig

$$W = +\sqrt{n}, \quad T = +\sqrt{n}$$

Im anderen Fall, in dem n die Form $4\mu + 3$ hat, sind in der Folge der ungeraden Zahlen

$$1,\ 3,\ 5,\ 7 \ldots . \tfrac{1}{2}(n-1), \quad \tfrac{1}{2}(n+3) \ldots . (n-2)$$

die ersten $\frac{1}{4}(n+1)$ kleiner als $\frac{1}{2}n$, die übrigen $\frac{1}{4}(n-3)$ dagegen größer. Unter den Sinuswerten der Bögen ω, 3ω, $5\omega \ldots (n-2)\omega$ sind somit $\frac{1}{4}(n-3)$ negativ, und daher ist W das Produkt aus $i^{\frac{1}{2}(n-1)}$, einer positiven reellen Größe und $(-1)^{\frac{1}{4}(n-3)}$. Der dritte Faktor ist $= i^{\frac{1}{2}(n-3)}$ und ergibt mit dem ersten multipliziert $i^{n-2} = i$, da $i^{n-3} = 1$ ist. Somit gilt notwendig

$$W = +i\sqrt{n}, \quad \text{und} \quad U = +\sqrt{n}$$

15.

Wir werden nun zeigen, wie sich dieselben Ergebnisse aus der in Art. 9 betrachteten Reihe ableiten lassen. Ersetzen wir in der Gleichung [4] den Ausdruck $x^{\frac{1}{2}}$ durch $-y^{-1}$, so erhalten wir

$$1 - y^{-1}\frac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\frac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} - y^{-3}\frac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+4})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \text{usw.}$$

bis zum Glied an der Stelle $m+1$

$$= (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4}) \ldots (1 \pm y^{-m}) \ldots . \; [7]$$

Wählen wir hier für y eine eigentliche Wurzel der Gleichung $y^n - 1 = 0$, etwa r, und setzen zugleich $m = n-1$, so ist

$$\frac{1-y^{-2m}}{1-y^{-2}} = \frac{1-r^2}{1-r^{-2}} = -r^2$$
$$\frac{1-y^{-2m+2}}{1-y^{-4}} = \frac{1-r^4}{1-r^{-4}} = -r^4$$
$$\frac{1-y^{-2m+4}}{1-y^{-6}} = \frac{1-r^6}{1-r^{-6}} = -r^6$$

bis hin zu

$$\frac{1-y^{-2}}{1-y^{-2m}} = \frac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2}$$

Dabei ist zu beachten, dass keiner der Nenner $1-r^{-2}$, $1-r^{-4}$ usw. $= 0$ wird. Daher nimmt die Gleichung [7] diese Form an:

$$1 + r + r^4 + r^9 + \text{usw.} + r^{(n-1)^2} = (1-r^{-1})(1+r^{-2})(1-r^{-3}) \ldots . (1+r^{-n+1})$$

Multiplizieren wir auf der rechten Seite dieser Gleichung das erste Glied mit dem letzten, das zweite mit dem vorletzten usw., so erhalten wir

$$\begin{aligned}(1-r^{-1})(1+r^{-n+1}) &= r-r^{-1}\\ (1+r^{-2})(1-r^{-n+2}) &= r^{n-2}-r^{-n+2}\\ (1-r^{-3})(1+r^{-n+3}) &= r^3-r^{-3}\\ (1+r^{-4})(1-r^{-n+4}) &= r^{n-4}-r^{-n+4} \text{ usw.}\end{aligned}$$

Man sieht leicht, dass diese Teilprodukte das folgende Produkt ergeben:

$$\begin{aligned}&(r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\\ &\quad \ldots . (r^{n-4}-r^{-n+4})(r^{n-2}-r^{-n+2})\end{aligned}$$

Dieses ist somit

$$= 1+r+r^4+r^9+\text{usw.}+r^{(n-1)^2} = W$$

Diese Gleichung ist identisch mit der Gleichung [5], die in Art. 12 aus der ersten Reihe abgeleitet wurde; die übrigen Schlussfolgerungen ergeben sich dann auf dieselbe Weise wie in den Art. 13 und 14.

16.

Wir gehen zum anderen Fall über, in dem n eine gerade Zahl ist. Zunächst habe n die Form $4\mu+2$, sei also das Doppelte einer ungeraden Zahl. Offenbar liefern die Zahlen $\frac{1}{4}nn$, $(\frac{1}{2}n+1)^2-1$, $(\frac{1}{2}n+2)^2-4$ usw., oder allgemein $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$, bei Division durch $\frac{1}{2}n$ ungerade Quotienten und sind daher modulo n zu $\frac{1}{2}n$ kongruent. Daraus folgt, dass für eine eigentliche Wurzel r der Gleichung $x^n-1=0$, für die also $r^{\frac{1}{2}n}=-1$ ist, gilt:

$$\begin{aligned}r^{(\frac{1}{2}n)^2} &= -1\\ r^{(\frac{1}{2}n+1)^2} &= -r\\ r^{(\frac{1}{2}n+2)^2} &= -r^4\\ r^{(\frac{1}{2}n+2)^2} &= -r^9 \text{ usw.}\end{aligned}$$

Somit hebt in der Reihe

$$1+r+r^4+r^9+\text{usw.}+r^{(n-1)^2}$$

das Glied $r^{(\frac{1}{2}n)^2}$ das erste auf, das nächste das zweite usw., sodass sich ergibt:

$$W=0, \quad T=0, \quad U=0$$

17.

Es bleibt der Fall, in dem n die Form 4μ hat, also durch vier teilbar ist. Hier ist allgemein $(\frac{1}{2}n+\lambda)^2 - \lambda\lambda$ durch n teilbar, und somit gilt

$$r^{(\frac{1}{2}n+\lambda)^2} = r^{\lambda\lambda}$$

In der Reihe

$$1 + r + r^4 + r^9 + \text{usw.} + r^{(n-1)^2}$$

ist daher das Glied $r^{(\frac{1}{2}n)^2}$ dem ersten gleich, das nächste dem zweiten usw., sodass sich ergibt:

$$W = 2(1 + r + r^4 + r^9 + \text{usw.} + r^{(\frac{1}{2}n-1)^2})$$

Nehmen wir nun an, dass in der Gleichung [7] aus Art. 15 $m = \frac{1}{2}n - 1$ gesetzt und für y eine eigentliche Wurzel der Gleichung $y^n - 1 = 0$, etwa r, gewählt wird. Dann erhält die Gleichung, ebenso wie in Art. 15, die folgende Form:

$$\begin{aligned} &1 + r + r^4 + \text{usw.} + r^{(\frac{1}{2}n-1)^2} \\ &\quad = (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1}) \end{aligned}$$

oder

$$\begin{aligned} W = 2(1 - r^{-1})(1 + r^{-2})(1 - r^{-3})(1 + r^{-4}) \\ \ldots (1 - r^{-\frac{1}{2}n+1}) \quad .. \quad [8] \end{aligned}$$

Da ferner $r^{\frac{1}{2}n} = -1$ und folglich

$$\begin{aligned} 1 + r^{-2} &= -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2}) \\ 1 + r^{-4} &= -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4}) \\ 1 + r^{-6} &= -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6}) \text{ usw.} \end{aligned}$$

ist und das Produkt der Faktoren $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-4}$, $-r^{\frac{1}{2}n-6}$ usw. bis zu $-r^2$ gleich $= (-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}$ ist, lässt sich die vorige Gleichung auch folgendermaßen schreiben:

$$\begin{aligned} W = 2(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}(1 - r^{-1})(1 - r^{-2}) \\ (1 - r^{-3})(1 - r^{-4}) \ldots (1 - r^{-\frac{1}{2}n+1}) \end{aligned}$$

Da

$$\begin{aligned} 1 - r^{-1} &= -r^{-1}(1 - r^{-n+1}) \\ 1 - r^{-2} &= -r^{-2}(1 - r^{-n+2}) \\ 1 - r^{-3} &= -r^{-3}(1 - r^{-n+3}) \text{ usw.} \end{aligned}$$

ist, erhalten wir

$$\begin{aligned} &(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots (1 - r^{-\frac{1}{2}n+1}) \\ &\quad = (-1)^{\frac{1}{2}n-1}\, r^{-\frac{1}{8}nn+\frac{1}{4}n}(1 - r^{-\frac{1}{2}n-1}) \\ &\qquad (1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1}) \end{aligned}$$

und damit

$$\begin{aligned} W = 2(-1)^{\frac{3}{4}n-2}\, &r^{-\frac{1}{16}nn}(1 - r^{-\frac{1}{2}n-1}) \\ &(1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \dots . (1 - r^{-n+1}) \end{aligned}$$

Multiplizieren wir diesen Wert von W mit dem zuvor gefundenen und fügen auf beiden Seiten den Faktor $1 - r^{-\frac{1}{2}n}$ hinzu, so ergibt sich

$$\begin{aligned} (1 - r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3} &r^{-\frac{1}{4}n}(1 - r^{-1}.) \\ &(1 - r^{-2})(1 - r^{-3}) \dots . (1 - r^{-n+1}) \end{aligned}$$

Es ist aber

$$\begin{aligned} 1 - r^{-\frac{1}{2}n} &= 2 \\ (-1)^{n-3} &= -1 \\ r^{-\frac{1}{4}n} &= -r^{\frac{1}{4}n} \end{aligned}$$

$$(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots . (1 - r^{-n+1}) = n$$

Daraus folgt schließlich

$$W^2 = 2r^{\frac{1}{4}n}n \text{ . . . . . [9]}$$

Nun sieht man leicht, dass $r^{\frac{1}{4}n}$ entweder $= +i$ oder $= -i$ ist, je nachdem, ob k die Form $4\mu + 1$ oder die Form $4\mu + 3$ hat. Da ferner

$$2i = (1+i)^2, \quad -2i = (1-i)^2$$

ist, ergibt sich in dem Fall, dass k die Form $4\mu + 1$ hat,

$$W = \pm(1+i)\sqrt{n}, \quad \text{und somit} \quad T = U = \pm\sqrt{n}$$

im anderen Fall dagegen, in dem k die Form $4\mu + 3$ hat,

$$W = \pm(1-i)\sqrt{n}, \quad \text{und somit} \quad T = -U = \pm\sqrt{n}$$

18.

Die Methode des vorigen Artikels lieferte die absoluten Werte der Funktionen T, U und gab die Bedingungen an, unter denen ihnen gleiche oder entgegengesetzte Vorzeichen zu geben sind; die Vorzeichen selbst sind damit aber noch nicht bestimmt. Für den Fall $k = 1$ werden wir dies folgendermaßen ergänzen.

Setzen wir $\rho = \cos\frac{1}{2}\omega + i\sin\frac{1}{2}\omega$, sodass $r = \rho\rho$ ist. Wegen $\rho^n = -1$ lässt sich die Gleichung [8] offenbar folgendermaßen schreiben:

$$W = 2(1+\rho^{n-2})(1+\rho^{-4})(1+\rho^{n-6})(1+\rho^{-8})$$
$$\ldots(1+\rho^{-n+4})(1+\rho^2)$$

oder, wenn wir die Faktoren anders anordnen,

$$W = 2(1+\rho^2)(1+\rho^{-4})(1+\rho^6)(1+\rho^{-8})$$
$$\ldots(1+\rho^{-n+4})(1+\rho^{n-2})$$

Nun ist

$$1+\rho^2 = 2\rho\cos\frac{1}{2}\omega$$
$$1+\rho^{-4} = 2\rho^{-2}\cos\omega$$
$$1+\rho^{-6} = 2\rho^3\cos\frac{3}{2}\omega$$
$$1+\rho^{-8} = 2\rho^{-4}\cos 2\omega, \text{ usw.}$$

bis hin zu

$$1+\rho^{-n+4} = 2\rho^{-\frac{1}{2}n+2}, \cos(\frac{1}{4}n-1)\omega$$
$$1+\rho^{n-2} = 2\rho^{\frac{1}{2}n-1}\cos(\frac{1}{4}n-\frac{1}{2})\omega$$

Somit ergibt sich

$$W = 2^{\frac{1}{2}n}\rho^{\frac{1}{4}n}\cos\frac{1}{2}\omega\cos\omega\,\frac{3}{2}\omega$$
$$\ldots\,\cos(\frac{1}{4}n-\frac{1}{2})\omega$$

Die in dieses Produkt eingehenden Kosinuswerte sind offenbar sämtlich positiv, der Faktor $\rho^{\frac{1}{4}n}$ dagegen ist $= \cos 45^0 + i\sin 45^0 = (1+i)\sqrt{\frac{1}{2}}$. Daraus schließen wir, dass W das Produkt aus $1+i$ und einer positiven reellen Größe ist. Daher gilt notwendig

$$W = (1+i)\sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}$$

19.

Es wird sich lohnen, sämtliche bisher entwickelten Summationen hier in einer Übersicht zusammenzustellen. Allgemein gilt nämlich

$T =$	$U =$	für n der Form
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

und wenn wir $k = 1$ setzen, muss der Wurzelausdruck das positive Vorzeichen erhalten. Damit ist nun mit voller Strenge bewiesen, was wir in Art. 3 für Primzahlwerte von n durch Induktion bemerkt hatten. Es bleibt nur noch zu zeigen, wie sich die Vorzeichen in allen Fällen für beliebige Werte von k bestimmen lassen. Bevor wir diese Aufgabe jedoch in ihrer ganzen Allgemeinheit angehen können, müssen wir zunächst die Fälle näher betrachten, in denen n eine Primzahl oder eine Primzahlpotenz ist.

20.

Zunächst sei n eine ungerade Primzahl. Nach den Ausführungen in Art. 10 ist offenbar $W = 1 + 2\Sigma r^a = 1 + 2\Sigma R^{ak}$, wenn $R = \cos\omega + i\sin\omega$ gesetzt wird und a, ebenso wie dort, unbestimmt sämtliche quadratischen Reste von n zwischen 1 und $n-1$ bezeichnet. Bezeichnen wir ebenso durch b unbestimmt sämtliche quadratischen Nichtreste zwischen denselben Grenzen, so sieht man ohne Mühe, dass sämtliche Zahlen ak modulo n entweder zu sämtlichen a oder zu sämtlichen b kongruent sind (ohne Rücksicht auf ihre Reihenfolge), je nachdem, ob k ein Rest oder ein Nichtrest ist. Im ersten Fall ist daher

$$W = 1 + 2\Sigma R^a = 1 + R + R^4 + R^9 + \text{usw.} + R^{(n-1)^2}$$

und somit $W = +\sqrt{n}$, wenn n die Form $4\mu + 1$ hat, sowie $W = +i\sqrt{n}$, wenn n die Form $4\mu + 3$ hat.

Im anderen Fall dagegen, in dem k ein Nichtrest von n ist, gilt

$$W = 1 + 2\Sigma R^b$$

Da nun sämtliche a, b offenbar die gesamte Menge der Zahlen 1, 2, 3 ... ausfüllen und folglich

$$\Sigma R^a + \Sigma R^b = R + R^2 + R^3 + \text{usw.} + R^{n-1} = -1$$

ist, ergibt sich

$$W = -1 - 2\Sigma R^a = -(1 + R + R^4 + R^9 + \text{usw.} + R^{(n-1)^2})$$

und somit $W = -\sqrt{n}$, wenn n die Form $4\mu + 1$ hat, sowie $W = -i\sqrt{n}$, wenn n die Form $4\mu + 3$ hat.

Daraus folgt also:

Erstens, wenn n die Form $4\mu+1$ hat und k ein quadratischer Rest von n ist,

$$T = +\sqrt{n}, \quad U = 0$$

zweitens, wenn n die Form $4\mu+1$ hat und k ein Nichtrest von n ist,

$$T = -\sqrt{n}, \quad U = 0$$

drittens, wenn n die Form $4\mu+3$ hat und k ein Rest von n ist,

$$T = 0, \quad U = +\sqrt{n}$$

viertens, wenn n die Form $4\mu+3$ hat und k ein Nichtrest von n ist,

$$T = 0, \quad U = -\sqrt{n}$$

21.

Zweitens sei n das Quadrat oder eine höhere Potenz einer ungeraden Primzahl p, und es werde $n = p^{2\varkappa}q$ gesetzt, wobei q entweder $= 1$ oder $= p$ ist. Zunächst ist hier zu beachten, dass für eine beliebige ganze Zahl λ, die nicht durch $p^{\varkappa}$ teilbar ist, gilt:

$$\begin{aligned} & r^{\lambda\lambda} + r^{(\lambda+p^{\varkappa}q)^2} + r^{(\lambda+2p^{\varkappa}q)^2} + r^{(\lambda+3p^{\varkappa}q)^2} \\ & \quad + \text{usw.} + r^{(\lambda+n-p^{\varkappa}q)^3} \\ & = r^{\lambda\lambda}\{1 + r^{2\lambda p^{\varkappa}q} + r^{4\lambda p^{\varkappa}q} \\ & \quad + r^{6\lambda p^{\varkappa}q} + \text{usw.} + r^{2\lambda(n-p^{\varkappa}q)}\} \\ & = \frac{r^{\lambda\lambda}(1 - r^{2\lambda n})}{1 - r^{2\lambda p^{\varkappa}q}} = 0 \end{aligned}$$

Man erkennt dann leicht die Gleichung

$$W = 1 + r^{p^{2\varkappa}} + r^{4p^{2\varkappa}} + r^{9p^{2\varkappa}} + \text{usw.} + r^{(n-p^{\varkappa})^2}$$

Denn die übrigen Glieder der Reihe

$$1 + r + r^4 + r^9 + \text{usw.} + r^{(n-1)^2}$$

lassen sich in $(p^{\varkappa}-1)q$ Teilreihen mit jeweils $p^{\varkappa}$ Gliedern aufteilen, deren Summen durch die soeben angegebene Umformung verschwinden.

Daraus folgt im Fall $q = 1$, also wenn n eine Primzahlpotenz mit geradem Exponenten ist:

$$W = p^{\varkappa} = +\sqrt{n}, \text{ und somit } T = +\sqrt{n}, \quad U = 0$$

Im anderen Fall dagegen, in dem $q = p$, also n eine Primzahlpotenz mit ungeradem Exponenten ist, setzen wir $r^{p^{2\varkappa}} = \rho$. Dann ist ρ eine eigentliche Wurzel der Gleichung $x^p - 1 = 0$, und zwar $\rho = \cos\frac{k}{p}360^0 + i\sin\frac{k}{p}360^0$, und es ergibt sich

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(p^{\varkappa+1}-1)^2} \\ &= p^{\varkappa}(1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(p-1)^2}) \end{aligned}$$

Die Summe der Reihe $1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(p-1)^2}$ ist aber durch den vorigen Artikel bestimmt. Daraus folgt unmittelbar

$$\begin{aligned} W &= \pm\sqrt{n} = T, \quad \text{falls } p \text{ die Form } 4\mu + 1 \text{ hat} \\ W &= \pm i\sqrt{n} = iU, \quad \text{falls } p \text{ die Form } 4\mu + 3 \text{ hat} \end{aligned}$$

mit dem positiven oder negativen Vorzeichen, je nachdem, ob k ein Rest oder ein Nichtrest von p ist.

22.

Aus den Ausführungen in den Art. 20 und 21 lässt sich auch leicht der folgende Satz ableiten, der uns weiter unten von erheblichem Nutzen sein wird. Setzen wir

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{usw.} + r^{h(n-1)^2}$$

wobei h eine beliebige, nicht durch p teilbare ganze Zahl bezeichnet, so gilt in dem Fall $n = p$ oder wenn n eine Potenz von p mit ungeradem Exponenten ist:

$$\begin{aligned} W' &= W, \text{ falls } h \text{ ein quadratischer Rest von } p \text{ ist} \\ W' &= -W, \text{ falls } h \text{ ein quadratischer Nichtrest von } p \text{ ist} \end{aligned}$$

Denn offenbar geht W' aus W hervor, wenn für k der Ausdruck kh eingesetzt wird. Im ersten Fall sind aber k und kh hinsichtlich ihrer Eigenschaft als Reste oder Nichtreste von p gleichartig, im zweiten Fall verschiedenartig.

In dem Fall dagegen, dass n eine Potenz von p mit geradem Exponenten ist, gilt offenbar $W' = +\sqrt{n}$ und somit stets $W' = W$.

23.

In den Art. 20, 21 und 22 haben wir ungerade Primzahlen und deren Potenzen betrachtet. Es bleibt daher der Fall, in dem n eine Zweierpotenz ist.

Für $n = 2$ ist offenbar $W = 1 + r = 0$.

Für $n = 4$ ergibt sich $W = 1 + r + r^4 + r^9 = 2 + 2r$. Somit ist $W = 2 + 2i$, wenn k die Form $4\mu + 1$ hat, und $W = 2 - 2i$, wenn k die Form $4\mu + 3$ hat.

Für $n = 8$ haben wir $W = 1+r+r^4+r^9+r^{16}+r^{25}+r^{36}+r^{49} = 2+4r+2r^4 = 4r$. Daher ist

$$\begin{aligned} W &= (1+i)\sqrt{8}, \quad \text{wenn } k \text{ die Form } 8\mu+1 \text{ hat} \\ W &= (-1+i)\sqrt{8}, \quad \text{wenn } k \text{ die Form } 8\mu+3 \text{ hat} \\ W &= (-1-i)\sqrt{8}, \quad \text{wenn } k \text{ die Form } 8\mu+5 \text{ hat} \\ W &= (1-i)\sqrt{8}, \quad \text{wenn } k \text{ die Form } 8\mu+7 \text{ hat} \end{aligned}$$

Ist n eine höhere Zweierpotenz, so setzen wir $n = 2^{2\varkappa}q$, wobei q entweder $= 1$ oder $= 2$ und $\varkappa$ größer als 1 ist. Zunächst ist hier zu beachten, dass für eine beliebige ganze Zahl λ, die nicht durch $2^{\varkappa-1}$ teilbar ist, gilt:

$$\begin{aligned} &r^{\lambda\lambda} + r^{(\lambda+2^{\varkappa}q)^2} + r^{(\lambda+2.2^{\varkappa}q)^2} + r^{(\lambda+3.2^{\varkappa}q)^2} \\ &\quad + \text{usw.} + r^{(\lambda+n-2^{\varkappa}q)^2} \\ &= r^{\lambda\lambda}\{1 + r^{2^{\varkappa+1}\lambda q} + r^{2.2^{\varkappa+1}\lambda q} \\ &\quad + r^{3.2^{\varkappa+1}\lambda q} + \text{usw.} + r^{(2n-2^{\varkappa+1}q)\lambda}\} \\ &= \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2^{\varkappa+1}\lambda q}} = 0 \end{aligned}$$

Man erkennt dann leicht die Gleichung

$$W = 1 + r^{2^{2\varkappa-2}} + r^{4.2^{2\varkappa-2}} + r^{9.2^{2\varkappa-2}} + \text{usw.} + r^{(n-2^{\varkappa-1})^2}$$

Setzen wir $r^{2^{2\varkappa-2}} = \rho$, so ist ρ eine Wurzel der Gleichung $x^{4q} - 1 = 0$, und zwar $\rho = \cos\frac{k}{4q}360^0 + i\sin\frac{k}{4q}360^0$; dann ergibt sich

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(2^{\varkappa+1}q-1)^2} \\ &= 2^{\varkappa-1}(1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(4q-1)^2}) \end{aligned}$$

Die Summe der Reihe $1+\rho+\rho^4+\rho^9+\text{usw.}+\rho^{(4q-1)^2}$ ist aber durch unsere Ausführungen zu den Fällen $n=4$, $n=8$ bestimmt. Daraus schließen wir,

dass im Fall $q=1$, also wenn n eine Potenz der Zahl 4 ist,

$$W=(1+i)2^{\varkappa}=(1+i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 4\mu+1 \text{ hat}$$
$$W=(1-i)2^{\varkappa}=(1-i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 4\mu+3 \text{ hat}$$

gilt. Dies sind genau die für $n=4$ angegebenen Formeln;

im anderen Fall dagegen, in dem $q=2$, also n eine Zweierpotenz mit einem ungeraden Exponenten größer als 3 ist, gilt

$$W=(1+i)2^{\varkappa}\sqrt{2}=(1+i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 8\mu+1 \text{ hat}$$
$$W=(-1+i)2^{\varkappa}\sqrt{2}=(-1+i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 8\mu+3 \text{ hat}$$
$$W=(-1-i)2^{\varkappa}\sqrt{2}=(-1-i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 8\mu+5 \text{ hat}$$
$$W=(1-i)2^{\varkappa}\sqrt{2}=(1-i)\sqrt{n}, \quad \text{falls } k \text{ die Form } 8\mu+7 \text{ hat}$$

was ebenfalls vollständig mit den für $n=8$ angegebenen Formeln übereinstimmt.

24.

Auch hier wird es sich lohnen, das Verhältnis der Summe der Reihe

$$W'=1+r^h+r^{4h}+r^{9h}+\text{usw.}+r^{h(n-1)^2}$$

zu W zu bestimmen, wobei h eine beliebige ungerade ganze Zahl bezeichnet. Da W' aus W durch Ersetzen von k durch kh hervorgeht, hängt der Wert von W' ebenso von der Form der Zahl kh ab, wie W von der Form von k abhängt. Setzen wir $\frac{W'}{W}=l$, so gilt offenbar

I. im Fall $n=4$ oder einer höheren Zweierpotenz mit geradem Exponenten

$$l=1, \quad \text{falls } h \text{ die Form } 4\mu+1 \text{ hat}$$
$$l=-i, \quad \text{falls } h \text{ die Form } 4\mu+3 \text{ hat, und } k \text{ die Form } 4\mu+1 \text{ hat}$$
$$l=+i, \quad \text{falls } h \text{ die Form } 4\mu+3 \text{ hat, und } k \text{ dieselbe Form hat.}$$

II. im Fall $n = 8$ oder einer höheren Zweierpotenz mit ungeradem Exponenten

$l = 1$, falls h die Form $8\mu + 1$ hat,
$l = -1$, falls h die Form $8\mu + 5$ hat,
$l = +i$, falls entweder h die Form $8\mu + 3$ hat, und k die Form $4\mu + 1$ hat,
oder h die Form $8\mu + 7$ hat, und k die Form $4\mu + 3$ hat,
$l = -i$, falls entweder h die Form $8\mu + 3$ hat, und k die Form $4\mu + 3$ hat,
oder h die Form $8\mu + 7$ hat, und k die Form $4\mu + 1$ hat.

Durch die vorigen Artikel ist die Bestimmung der Summe W für die Fälle, in denen n eine Primzahl oder eine Primzahlpotenz ist, vollständig abgeschlossen. Es bleibt daher, auch die Fälle zu erledigen, in denen n aus mehreren Primzahlen zusammengesetzt ist; hierzu wird uns der folgende Satz den Weg bahnen:

25.

Satz. *Es sei n das Produkt zweier teilerfremder positiver ganzer Zahlen a, b, und es werde gesetzt*

$$P = 1 + r^{aa} + r^{4aa} + r^{9aa} + \text{usw.} + r^{(b-1)^2 aa}$$
$$Q = 1 + r^{bb} + r^{4bb} + r^{9bb} + \text{usw.} + r^{(a-1)^2 bb}$$

Dann behaupte ich, dass $W = PQ$ ist.

Beweis. Es bezeichne α unbestimmt die Zahlen $0, 1, 2, 3 \ldots . a - 1$, β die Zahlen $0, 1, 2, 3 \ldots . b - 1$ und ν die Zahlen $0, 1, 2, 3 \ldots . n - 1$. Dann gilt offenbar

$$P = \Sigma r^{aa\beta\beta}, \quad Q = \Sigma r^{bb\alpha\alpha}, \quad W = \Sigma r^{\nu\nu}$$

Somit ist $PQ = \Sigma r^{aa\beta\beta + bb\alpha\alpha}$, wenn für α und β sämtliche Werte in allen möglichen Kombinationen eingesetzt werden. Da ferner $2ab\alpha\beta = 2\alpha\beta n$ ist, ergibt sich $PQ = \Sigma r^{(a\beta + b\alpha)^2}$. Man sieht aber ohne Mühe, dass die einzelnen Werte von $a\beta + b\alpha$ voneinander verschieden und jeweils einem Wert von ν gleich sind. Daher ist $PQ = \Sigma r^{\nu\nu} = W$.

Außerdem ist zu beachten, dass r^{aa} eine eigentliche Wurzel der Gleichung $x^b - 1 = 0$ und r^{bb} eine eigentliche Wurzel der Gleichung $x^a - 1 = 0$ ist.

26.

Es sei nun n das Produkt dreier paarweise teilerfremder Zahlen a, b, c. Wird $bc = b'$ gesetzt, so sind offenbar auch a und b' teilerfremd; daher ist W das Produkt der beiden Faktoren

$$1 + r^{aa} + r^{4aa} + r^{9aa} + \text{usw.} + r^{(b'-1)^2 aa}$$
$$1 + r^{b'b'} + r^{4b'b'} + r^{9b'b'} + \text{usw.} + r^{(a-1)^2 b'b'}$$

Da aber r^{aa} eine eigentliche Wurzel der Gleichung $x^{bc} - 1 = 0$ ist, ist der erste Faktor selbst das Produkt aus

$$1 + \rho^{bb} + \rho^{4bb} + \rho^{9bb} + \text{usw.} + \rho^{(c-1)^2 bb}$$
$$1 + \rho^{cc} + \rho^{4cc} + \rho^{9cc} + \text{usw.} + \rho^{(b-1)^2 cc}$$

wenn $r^{aa} = \rho$ gesetzt wird. Daraus ist ersichtlich, dass W das Produkt der drei Faktoren

$$1 + r^{bbcc} + r^{4bbcc} + r^{9bbcc} + \text{usw.} + r^{(a-1)^2 bbcc}$$
$$1 + r^{aacc} + r^{4aacc} + r^{9aacc} + \text{usw.} + r^{(b-1)^2 aacc}$$
$$1 + r^{aabb} + r^{4aabb} + r^{9aabb} + \text{usw.} + r^{(c-1)^2 aabb}$$

ist, wobei r^{bbcc}, r^{aacc}, r^{aabb} jeweils eigentliche Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$ sind.

27.

Daraus folgt leicht allgemein: Ist n das Produkt beliebig vieler paarweise teilerfremder Faktoren a, b, c usw., so ist W das Produkt ebenso vieler Faktoren, nämlich

$$1 + r^{\frac{nn}{aa}} + r^{\frac{4nn}{aa}} + r^{\frac{9nn}{aa}} + \text{usw.} + r^{\frac{(a-1)^2 nn}{aa}}$$
$$1 + r^{\frac{nn}{bb}} + r^{\frac{4nn}{bb}} + r^{\frac{9nn}{bb}} + \text{usw.} + r^{\frac{(b-1)^2 nn}{bb}}$$
$$1 + r^{\frac{nn}{cc}} + r^{\frac{4nn}{cc}} + r^{\frac{9nn}{cc}} + \text{usw.} + r^{\frac{(c-1)^2 nn}{cc}}, \text{ usw.}$$

wobei $r^{\frac{nn}{aa}}$, $r^{\frac{nn}{bb}}$, $r^{\frac{nn}{cc}}$ usw. eigentliche Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$. $x^c - 1 = 0$ usw. sind.

28.

Aus diesen Grundsätzen ergibt sich nun unmittelbar der Weg zur vollständigen Bestimmung von W für einen beliebigen Wert von n. Zerlegen wir nämlich n in Faktoren a, b, c usw., die entweder verschiedene Primzahlen oder Potenzen verschiedener Primzahlen sind, und setzen $r^{\frac{nn}{aa}} = A$, $r^{\frac{nn}{bb}} = B$, $r^{\frac{nn}{cc}} = C$ usw., so sind A, B, C usw. eigentliche Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$ usw. und W das Produkt der Faktoren

$$1 + A + A^4 + A^9 + \text{usw.} + A^{(a-1)^2}$$
$$1 + B + B^4 + B^9 + \text{usw.} + B^{(b-1)^2}$$
$$1 + C + C^4 + C^9 + \text{usw.} + C^{(c-1)^2}$$

Diese einzelnen Faktoren lassen sich aber anhand unserer Ausführungen in den Art. 20, 21, 23 bestimmen, wodurch auch der Wert des Produkts bekannt wird. Es wird nützlich sein, die Regeln zur Bestimmung dieser Faktoren hier in einer Übersicht zusammenzustellen. Da die Wurzel $A = \frac{kn}{a} \cdot \frac{360^0}{a}$ ist, wird die Summe $1 + A + A^4 + A^9 + \text{usw.} + A^{(a-1)^2}$, die wir mit L bezeichnen, ebenso durch die Zahl $\frac{kn}{a}$ bestimmt, wie in unserer allgemeinen Untersuchung W durch k bestimmt wird. Nun sind zwölf Fälle zu unterscheiden.

I. Ist a eine Primzahl der Form $4\mu + 1$, etwa $= p$, oder eine Potenz einer solchen Primzahl mit ungeradem Exponenten und zugleich $\frac{kn}{a}$ ein quadratischer Rest von p, so ist $L = +\sqrt{a}$.

II. Bleiben die übrigen Bedingungen unverändert und ist $\frac{kn}{a}$ ein quadratischer Nichtrest von p, so ist $L = -\sqrt{a}$.

III. Ist a eine Primzahl der Form $4\mu + 3$, etwa $= p$, oder eine Potenz einer solchen Primzahl mit ungeradem Exponenten und zugleich $\frac{kn}{a}$ ein quadratischer Rest von p, so ist $L = +i\sqrt{a}$.

IV. Sind die übrigen Bedingungen wie in III und ist $\frac{kn}{a}$ ein quadratischer Nichtrest von p, so ist $L = -i\sqrt{a}$.

V. Ist a das Quadrat oder eine höhere Potenz einer (ungeraden) Primzahl mit geradem Exponenten, so ist $L = +\sqrt{a}$.

VI. Ist $a = 2$, so ist $L = 0$.

VII. Ist $a = 4$ oder eine höhere Zweierpotenz mit geradem Exponenten und hat zugleich $\frac{kn}{a}$ die Form $4\mu + 1$, so ist $L = (1 + i)\sqrt{a}$.

VIII. Sind die übrigen Bedingungen wie in VII und hat $\frac{kn}{a}$ die Form $4\mu + 3$, so ist $L = (1 - i)\sqrt{a}$.

IX. Ist $a = 8$ oder eine höhere Zweierpotenz mit ungeradem Exponenten und hat zugleich $\frac{kn}{a}$ die Form $8\mu + 1$, so ist $L = (1 + i)\sqrt{a}$.

X. Sind die übrigen Bedingungen wie in IX und hat $\frac{kn}{a}$ die Form $8\mu + 3$, so ist $L = (-1 + i)\sqrt{a}$.

XI. Bleiben die übrigen Bedingungen unverändert und hat $\frac{kn}{a}$ die Form $8\mu + 5$, so ist $L = (-1 - i)\sqrt{a}$.

XII. Bleiben die übrigen Bedingungen unverändert und hat $\frac{kn}{a}$ die Form $8\mu + 7$, so ist $L = (1 - i)\sqrt{a}$.

29.

Es sei beispielsweise $n = 2520 = 8 \,.\, 9 \,.\, 5 \,.\, 7$ und $k = 13$. Dann erhalten wir

für $a = 8$, nach Fall XII, $L = (1 - i)\sqrt{8}$
für den Faktor 9, nach Fall V, zugehörige Summe $= \sqrt{9}$
für den Faktor 5, nach Fall II, zugehörige Summe $= -\sqrt{5}$
für den Faktor 7, nach Fall III, zugehörige Summe $= +i\sqrt{7}$.

Somit ist $W = (1 - i) \,.\, (-i) \,.\, \sqrt{2520} = (-1 - i)\sqrt{2520}$.

Für denselben Wert von n sei $k = 1$; dann entsprechen den Faktoren die folgenden Summen:

zum Faktor 8 die Summe $(-1 + i)\sqrt{8}$
zum Faktor 9 die Summe $\sqrt{9}$
zum Faktor 5 die Summe $\sqrt{5}$
zum Faktor 7 die Summe $-i\sqrt{7}$

Daraus ergibt sich das Produkt $W = (1 + i)\sqrt{2520}$.

30.

Eine weitere Methode, die Summe W allgemein zu bestimmen, ergibt sich aus unseren Ausführungen in den Art. 22. 24. Setzen wir $\cos\omega + i\sin\omega = \rho$ und

$$\rho^{\frac{nn}{aa}} = \alpha, \quad \rho^{\frac{nn}{bb}} = \beta, \quad \rho^{\frac{nn}{cc}} = \gamma \text{ usw.}$$

so dass $r = \rho^k$, $A = \alpha^k$, $B = \beta^k$, $C = \gamma^k$ usw. gilt. Dann ist

$$1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(n-1)^2}$$

das Produkt der Faktoren

$$1 + \alpha + \alpha^4 + \alpha^9 + \text{usw.} + \alpha^{(a-1)^2}$$
$$1 + \beta + \beta^4 + \beta^9 + \text{usw.} + \beta^{(b-1)^2}$$
$$1 + \gamma + \gamma^4 + \gamma^9 + \text{usw.} + \gamma^{(c-1)^2}, \text{ usw.}$$

und somit W das Produkt der Faktoren

$$w = 1 + \rho + \rho^4 + \rho^9 + \text{usw.} + \rho^{(n-1)^2}$$

$$\mathfrak{A} = \frac{1 + A + A^4 + A^9 + \text{usw.} + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \text{usw.} + \alpha^{(a-1)^2}}$$

$$\mathfrak{B} = \frac{1 + B + B^4 + B^9 + \text{usw.} + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \text{usw.} + \beta^{(b-1)^2}}$$

$$\mathfrak{C} = \frac{1 + C + C^4 + C^9 + \text{usw.} + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \text{usw.} + \gamma^{(c-1)^2}}$$

Der erste Faktor w ist bereits durch die oben angegebenen Untersuchungen bestimmt (Art. 19); die übrigen Faktoren $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ usw. ergeben sich aus den Formeln der Art. 22. 24, die wir hier nochmals zusammenstellen, um alles beisammen zu haben[*]. Hier sind zwölf Fälle zu unterscheiden, nämlich

I. Ist a eine (ungerade) Primzahl $= p$ oder eine Potenz einer solchen Zahl mit ungeradem Exponenten und k ein quadratischer Rest von p, so ist der entsprechende Faktor $\mathfrak{A} = +1$.

II. Bleiben die übrigen Bedingungen unverändert und ist k ein quadratischer Nichtrest von p, so ist $\mathfrak{A} = -1$.

III. Ist a das Quadrat einer ungeraden Primzahl oder eine höhere Potenz derselben mit geradem Exponenten, so ist $\mathfrak{A} = +1$.

IV. Ist $a = 4$ oder eine höhere Zweierpotenz mit geradem Exponenten und hat zugleich k die Form $4\mu + 1$, so ist $\mathfrak{A} = +1$.

V. Sind die übrigen Bedingungen wie in IV, hat k die Form $4\mu + 3$ und $\frac{n}{a}$ die Form $4\mu + 1$, so ist $\mathfrak{A} = -i$.

VI. Sind die übrigen Bedingungen wie in IV, hat k die Form $4\mu + 3$ und $\frac{n}{a}$ die Form $4\mu + 3$, so ist $\mathfrak{A} = +i$.

VII. Ist $a = 8$ oder eine höhere Zweierpotenz mit ungeradem Exponenten und hat k die Form $8\mu + 1$, so ist $\mathfrak{A} = +1$.

VIII. Sind die übrigen Bedingungen wie in VII und hat k die Form $8\mu + 5$, so ist $\mathfrak{A} = -1$.

IX. Sind die übrigen Bedingungen wie in VII, hat k die Form $8\mu + 3$ und $\frac{n}{a}$ die Form $4\mu + 1$, so ist $\mathfrak{A} = +i$.

X. Sind die übrigen Bedingungen wie in VII, hat k die Form $8\mu + 3$ und $\frac{n}{a}$ die Form $4\mu + 3$, so ist $\mathfrak{A} = -i$.

XI. Sind die übrigen Bedingungen wie in VII, hat k die Form $8\mu + 7$ und $\frac{n}{a}$ die Form $4\mu + 1$, so ist $\mathfrak{A} = -i$.

XII. Sind die übrigen Bedingungen wie in VII, hat k die Form $8\mu + 7$ und $\frac{n}{a}$ die Form $4\mu + 3$, so ist $\mathfrak{A} = +i$.

[*] Was dort k und h war, ist hier offenbar $\frac{n}{a}$ und k für den zweiten Faktor, $\frac{n}{b}$ und k für den dritten Faktor usw.

Den Fall $a = 2$ übergehen wir; hier wäre $\mathfrak{A}$ zwar $= \frac{0}{0}$, also unbestimmt, doch gilt dann stets $W = 0$.

Die übrigen Faktoren $\mathfrak{B}, \mathfrak{C}$ usw. hängen von b, c usw. ebenso ab wie $\mathfrak{A}$ von a, soweit diese Zahlen in ihre Bestimmung eingehen.

31.

Nach dieser zweiten Methode gestaltet sich das erste Beispiel aus Art. 29 folgendermaßen:

Der Faktor w ist $= (1+i)\sqrt{2520}$
Für $a = 8$ ist der zugehörige Faktor $\mathfrak{A}$ nach Fall VIII $= -1$
Zum zweiten Faktor von n, 9, gehört der Faktor $+1$ (nach Fall III.)
Zum Faktor 5 gehört der Faktor -1 (nach Fall II.)
Zum Faktor 7 gehört der Faktor -1 (nach Fall II.)

Daraus ergibt sich das Produkt $W = (-1-i)\sqrt{2520}$, wie in Art. 29.

32.

Da sich der Wert von W nach *zwei* Methoden bestimmen lässt, von denen die eine auf den Beziehungen der Zahlen $\frac{nk}{a}$, $\frac{nk}{b}$, $\frac{nk}{c}$ usw. zu den Zahlen a, b, c usw. beruht, die andere dagegen von den Beziehungen von k zu den Zahlen a, b, c usw. abhängt, muss zwischen all diesen Beziehungen ein bedingter Zusammenhang bestehen, so dass jede von ihnen aus den übrigen bestimmbar sein muss. Nehmen wir an, alle Zahlen a, b, c usw. seien ungerade Primzahlen, und setzen wir $k = 1$. Wir teilen die Faktoren a, b, c usw. in zwei Klassen: Die eine enthält diejenigen von der Form $4\mu + 1$, die mit p, p', p'' usw. bezeichnet werden; die andere besteht aus denen von der Form $4\mu + 3$, die wir mit q, q', q'' usw. bezeichnen. Die Anzahl der Letzteren bezeichnen wir mit m. Dabei bemerken wir zunächst, dass n die Form $4\mu + 1$ hat, wenn m gerade ist (hierzu gehört auch der Fall, dass überhaupt keine Faktoren der zweiten Klasse vorhanden sind, also $m = 0$), dagegen n die Form $4\mu + 3$ hat, wenn m ungerade ist. Die Bestimmung von W nach der ersten Methode wird nun folgendermaßen ausgeführt. Die Zahlen $P, P'\ P''$ usw., Q, Q', Q'' usw. sollen von den Beziehungen der Zahlen $\frac{n}{p}$, $\frac{n}{p'}$, $\frac{n}{p''}$ usw., $\frac{n}{q}$, $\frac{n}{q'}$, $\frac{n}{q''}$ usw. zu den Zahlen p, p', p'' usw., q, q', q'' usw. jeweils so abhängen, dass wir setzen:

$$P = +1, \text{ wenn } \frac{n}{p} \text{ ein quadratischer Rest von } p \text{ ist}$$
$$P = -1, \text{ wenn } \frac{n}{p} \text{ ein quadratischer Nichtrest von } p \text{ ist}$$

und ebenso für die übrigen. Dann ist W das Produkt der Faktoren $P\sqrt{p}$, $P'\sqrt{p'}$, $P''\sqrt{p''}$ usw. $iQ\sqrt{q}$, $iQ'\sqrt{q'}$, $iQ''\sqrt{q''}$ usw., also

$$W = PP'P'' \ldots QQ'Q'' \ldots i^m\sqrt{n}$$

Nach der zweiten Methode oder vielmehr unmittelbar nach den Regeln des Art. 19 gilt

$$W = +\sqrt{n}, \text{ wenn } n \text{ die Form } 4\mu + 1 \text{ hat,}$$
$$\text{oder gleichbedeutend, wenn } m \text{ gerade ist}$$
$$W = +i\sqrt{n}, \text{ wenn } n \text{ die Form } 4\mu + 3 \text{ hat,}$$
$$\text{oder wenn } m \text{ ungerade ist.}$$

Beide Fälle lassen sich gemeinsam durch die folgende Formel ausdrücken:

$$W = i^{mm}\sqrt{n}$$

Daraus folgt also

$$PP'P'' \ldots QQ'Q'' \ldots = i^{mm-m}$$

Nun ist $i^{mm-m} = 1$, wenn m die Form 4μ oder $4\mu+1$ hat, und $= -1$, wenn m die Form $4\mu + 2$ oder $4\mu + 3$ hat. Daraus leiten wir den folgenden höchst eleganten Satz ab:

Satz. *Es bezeichnen a, b, c usw. verschiedene positive ungerade Primzahlen, deren Produkt $= n$ gesetzt wird; unter ihnen seien m von der Form $4\mu+3$, die übrigen von der Form $4\mu + 1$. Die Anzahl derjenigen unter diesen Zahlen a, b, c usw., von denen jeweils $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$ usw. Nichtreste sind, ist gerade, wenn m die Form 4μ oder $4\mu + 1$ hat, dagegen ungerade, wenn m die Form $4\mu + 2$ oder $4\mu + 3$ hat.*

Setzen wir beispielsweise $a = 3$, $b = 5$, $c = 7$, $d = 11$, so haben wir drei Zahlen von der Form $4\mu + 3$, nämlich 3, 7 und 11; dabei gilt $5 \,.\, 7 \,.\, 11\, R3$; $3 \,.\, 7 \,.\, 11\, R5$; $3 \,.\, 5 \,.\, 11\, R7$; $3 \,.\, 5 \,.\, 7\, N11$, also ist allein $\frac{n}{d}$ ein Nichtrest von d.

33.

Das berühmte *Fundamentaltheorem* über quadratische Reste ist nichts anderes als ein besonderer Fall des soeben entwickelten Satzes. Beschränken wir nämlich die Anzahl der Zahlen a, b, c usw. auf *zwei*, so müssen, wenn nur eine von ihnen oder keine die Form $4\mu+3$ hat, offenbar entweder zugleich aRb, bRa oder zugleich aNb, bNa gelten; haben dagegen beide die Form $4\mu+3$, so muss die eine ein Nichtrest der anderen und diese ein Rest jener sein. Hier liegt also ein *vierter* Beweis dieses höchst wichtigen Satzes vor, dessen ersten und zweiten Beweis wir in den Disquisitiones Arithmeticae und dessen dritten wir kürzlich in einer besonderen Abhandlung gegeben haben (*Commentt. T. XVI*); zwei weitere, die wiederum auf völlig anderen Grundsätzen beruhen, werden wir später darlegen. Es ist wahrlich höchst erstaunlich, dass dieser so schöne Satz, der anfangs allen Versuchen so hartnäckig entgangen war, später auf so vielen, himmelweit voneinander entfernten Wegen erreicht werden konnte.

34.

Auch die übrigen Sätze, die gewissermaßen eine Ergänzung zum Fundamentaltheorem bilden, nämlich diejenigen, durch die man die Primzahlen erkennt, von denen $-1, +2$ und -2 Reste oder Nichtreste sind, lassen sich aus denselben Grundsätzen ableiten. Wir beginnen mit dem Rest $+2$.

Setzen wir $n = 8a$, wobei a eine Primzahl ist, und $k = 1$, so ist nach der Methode des Art. 28 W das Produkt zweier Faktoren. Der eine ist $+\sqrt{a}$ oder $+i\sqrt{a}$, wenn 8 oder gleichbedeutend 2 ein quadratischer Rest von a ist; dagegen $-\sqrt{a}$ oder $-i\sqrt{a}$, wenn 2 ein Nichtrest von a ist. Der zweite Faktor ist

$$\begin{aligned}
&(1+i)\sqrt{8}, \quad \text{wenn } a \text{ die Form } 8\mu+1 \text{ hat}\\
&(-1+i)\sqrt{8}, \quad \text{wenn } a \text{ die Form } 8\mu+3 \text{ hat}\\
&(-1-i)\sqrt{8}, \quad \text{wenn } a \text{ die Form } 8\mu+5 \text{ hat}\\
&(1-i)\sqrt{8}, \quad \text{wenn } a \text{ die Form } 8\mu+7 \text{ hat}
\end{aligned}$$

Nach Art. 18 ist aber stets $W = (1+i)\sqrt{n}$; teilt man diesen Wert durch die vier Werte des zweiten Faktors, so erkennt man, dass der erste Faktor

$$\begin{aligned}
&+\sqrt{a}, \quad \text{wenn } a \text{ die Form } 8\mu+1 \text{ hat}\\
&-i\sqrt{a}, \quad \text{wenn } a \text{ die Form } 8\mu+3 \text{ hat}\\
&-\sqrt{a}, \quad \text{wenn } a \text{ die Form } 8\mu+5 \text{ hat}\\
&+i\sqrt{a}, \quad \text{wenn } a \text{ die Form } 8\mu+7 \text{ hat}
\end{aligned}$$

sein muss. Daraus folgt unmittelbar, dass 2 im ersten und vierten Fall ein Rest von a, im zweiten und dritten Fall dagegen ein Nichtrest sein muss.

35.

Die Primzahlen, von denen -1 ein Rest oder Nichtrest ist, lassen sich mithilfe des folgenden Satzes leicht erkennen, der auch für sich genommen recht bemerkenswert ist.

Satz. *Das Produkt der beiden Faktoren*

$$\begin{aligned}
W' &= 1 + r^{-1} + r^{-4} + \text{usw.} + r^{-(n-1)^2}\\
W &= 1 + r + r^4 + \text{usw.} + r^{(n-1)^2}
\end{aligned}$$

ist $= n$, wenn n ungerade ist; oder $= 0$, wenn n das Doppelte einer ungeraden Zahl ist; oder $= 2n$, wenn n durch vier teilbar ist.

Beweis. Da offenbar

$$\begin{aligned} W &= r + r^4 + r^9 + \text{usw.} + r^{nn} \\ &= r^4 + r^9 + \text{usw.} + r^{(n+1)^2} \\ &= r^9 + \text{usw.} + r^{(n+2)^2} \quad \text{usw.} \end{aligned}$$

gilt, lässt sich das Produkt WW' auch folgendermaßen darstellen:

$$\begin{aligned} & 1 + r + r^4 + r^9 + \text{usw.} + r^{(n-1)^2} \\ & + r^{-1}(r + r^4 + r^9 + r^{16} + \text{usw.} + r^{nn}) \\ & + r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \text{usw.} + r^{(n+1)^2}) \\ & + r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \text{usw.} + r^{(n+2)^2}) \\ & \text{usw.} \\ & + r^{-(n-1)^2}(r^{(n-1)^2} + r^{nn} + r^{(n+1)^2} \\ & \qquad + r^{(n+2)^2} + \text{usw.} + r^{(2n-2)^2}) \end{aligned}$$

Summiert man diesen Ausdruck senkrecht, so erhält man

$$\begin{aligned} & n \\ & + r(1 + rr + r^4 + r^6 + \text{usw.} + r^{2n-2}) \\ & + r^4(1 + r^4 + r^8 + r^{12} + \text{usw.} + r^{4n-4}) \\ & + r^9(1 + r^6 + r^{12} + r^{18} + \text{usw.} + r^{6n-6}) \\ & + \text{usw.} \\ & + r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} \\ & \qquad + r^{6n-6} + \text{usw.} + r^{2(n-1)^2}) \end{aligned}$$

Ist nun n ungerade, so sind die einzelnen Teile dieses Ausdrucks außer dem ersten, n, sämtlich $= 0$; denn der zweite ist offenbar $\frac{r(1-r^{2n})}{1-rr}$, der dritte $\frac{r^4(1-r^{4n})}{1-r^4}$ usw. Ist dagegen n gerade, so muss außerdem der Teil

$$r^{\frac{1}{4}nn}(1 + r^n + r^{2n} + r^{3n} + \text{usw.} + r^{nn-n})$$

ausgenommen werden, der $= nr^{\frac{1}{4}nn}$ ist. Im ersten Fall ist daher $WW' = n$, im zweiten dagegen $= n + nr^{\frac{1}{4}nn}$; nun ist $r^{\frac{1}{4}nn} = +1$, wenn n durch vier teilbar ist, und dann ergibt sich $WW' = 2n$; dagegen gilt $r^{\frac{1}{4}nn} = -1$, wenn n das Doppelte einer ungeraden Zahl ist, so dass dann $WW' = 0$ herauskommt. Q. E. D.

36.

Nach Art. 22 steht fest, dass für eine ungerade Primzahl n der Quotient $\frac{W'}{W} = +1$ oder $= -1$ ist, je nachdem, ob -1 ein Rest oder Nichtrest von n ist. Daher muss im ersten Fall $W^2 = +n$, im zweiten $W^2 = -n$ gelten; nach Art. 13 schließen wir somit, dass der erste Fall nur eintreten kann, wenn n die Form $4\mu + 1$ hat, und der zweite, wenn n die Form $4\mu + 3$ hat.

Aus der Verbindung der für die Reste $+2$ und -1 gefundenen Bedingungen folgt schließlich unmittelbar, dass -2 ein Rest jeder Primzahl von der Form $8\mu+1$ oder $8\mu+3$ und ein Nichtrest jeder Primzahl von der Form $8\mu+5$ oder $8\mu + 7$ ist.

NEUE BEWEISE UND ERWEITERUNGEN DES FUNDAMENTALTHEOREMS IN DER THEORIE DER QUADRATISCHEN RESTE

VON

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN AM 10. FEBRUAR 1817 VORGELEGT.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. IV.
Gottingae MDCCCXVIII.

NEUE BEWEISE UND ERWEITERUNGEN DES FUNDAMENTALTHEOREMS IN DER THEORIE DER QUADRATISCHEN RESTE.

Das Fundamentaltheorem über quadratische Reste, das zu den schönsten Wahrheiten der höheren Arithmetik gehört, wurde zwar durch Induktion leicht entdeckt, aber mit weit größerer Mühe bewiesen. In diesem Gebiet kommt es häufig vor, dass die Beweise der einfachsten Wahrheiten, die sich dem Forschenden durch Induktion wie von selbst darbieten, tief verborgen liegen und erst nach vielen vergeblichen Versuchen endlich ans Licht gebracht werden können, vielleicht auf einem ganz anderen Weg als dem, auf dem man sie gesucht hatte. Dann geschieht es nicht selten, dass sich, sobald ein Weg gefunden ist, nach und nach *mehrere* weitere eröffnen, die zum selben Ziel führen: einige kürzer und unmittelbarer, andere gleichsam auf Umwegen und ausgehend von ganz anderen Grundsätzen, zwischen denen und der gestellten Frage man kaum einen Zusammenhang vermutet hätte. Dieser erstaunliche Zusammenhang zwischen tiefer verborgenen Wahrheiten verleiht solchen Betrachtungen nicht nur einen besonderen Reiz; er verdient auch deshalb sorgfältige Untersuchung und Aufklärung, weil sich daraus nicht selten neue Hilfsmittel oder Fortschritte für die Wissenschaft selbst ergeben.

Obwohl daher der hier behandelte arithmetische Satz durch die früheren Bemühungen, die vier völlig verschiedene Beweise geliefert haben[*)], vollständig erledigt erscheinen mag, kehre ich dennoch zu demselben Gegenstand zurück und füge zwei weitere Beweise hinzu, die gewiss neues Licht darauf werfen werden. Der erste ist dem dritten insofern verwandt, als er von demselben Lemma ausgeht; danach verfolgt er jedoch einen anderen Weg, so dass er mit Recht als neuer Beweis gelten kann, der an Eleganz jenem dritten wenn nicht überlegen, so doch keineswegs unterlegen erscheinen wird. Der sechste Beweis beruht dagegen auf einem völlig anderen, feineren Grundsatz und liefert ein neues Beispiel für den erstaunlichen Zusammenhang zwischen arithmetischen Wahrheiten, die auf den ersten Blick sehr weit voneinander entfernt liegen. Diesen beiden Beweisen ist ein neuer, sehr einfacher Algorithmus beigegeben, um zu entscheiden, ob eine gegebene ganze Zahl ein quadratischer Rest oder Nichtrest einer gegebenen Primzahl ist.

[*)] Zwei sind im vierten und fünften Abschnitt der *Disquisitiones Arithmeticae* dargelegt, der dritte in einer besonderen Abhandlung (*Commentt. Soc. Gotting. Vol. XVI*); der vierte ist in die Abhandlung *Summatio quarundam serierum singularium* aufgenommen (*Commentt. Recentiores, Vol. I*).

Es gab noch einen anderen Grund, die schon vor neun Jahren versprochenen neuen Beweise gerade jetzt zu veröffentlichen. Als ich im Jahr 1805 begann, die Theorie der kubischen und biquadratischen Reste zu untersuchen, einen weit schwierigeren Gegenstand, erlebte ich nahezu denselben Verlauf wie einst in der Theorie der quadratischen Reste. Die Sätze, die diese Fragen vollständig erschöpfen und eine erstaunliche Analogie zu den Sätzen über quadratische Reste erkennen lassen, wurden sogleich durch Induktion entdeckt, sobald sie auf einem geeigneten Weg gesucht wurden; alle Versuche jedoch, in jeder Hinsicht vollständige Beweise dafür zu gewinnen, blieben lange Zeit vergeblich. Gerade dies spornte mich an, den schon bekannten Beweisen über quadratische Reste mit solchem Eifer immer weitere hinzuzufügen, getragen von der Hoffnung, unter vielen verschiedenen Methoden könne die eine oder andere etwas zur Erhellung des verwandten Gegenstands beitragen. Diese Hoffnung war keineswegs vergeblich, und auf unermüdliche Arbeit folgten schließlich gute Ergebnisse. Bald wird es möglich sein, die Früchte meiner Nachtarbeit ans Licht der Öffentlichkeit zu bringen; bevor ich jedoch dieses schwierige Werk in Angriff nehme, habe ich beschlossen, noch einmal zur Theorie der quadratischen Reste zurückzukehren, alles noch darin zu Erledigende abzuschließen und so von diesem Teil der höheren Arithmetik gleichsam Abschied zu nehmen.

FÜNFTER BEWEIS DES FUNDAMENTALTHEOREMS IN DER THEORIE DER QUADRATISCHEN RESTE.

1.

In der Einleitung haben wir bereits gesagt, dass der fünfte und der dritte Beweis von demselben Lemma ausgehen. Der Bequemlichkeit halber erschien es uns angebracht, es hier in einer für die vorliegende Untersuchung passenden Bezeichnung zu wiederholen.

LEMMA. *Es sei m eine Primzahl (positiv und ungerade) und M eine ganze, durch m nicht teilbare Zahl. Man nehme die kleinsten positiven Reste der Zahlen*

$$M,\ 2M,\ 3M,\ 4M\ \ldots\ldots\ \tfrac{1}{2}(m-1)M$$

modulo m. Diese sind teils kleiner als $\frac{1}{2}m$, teils größer; die Anzahl der Letzteren sei $= n$. Dann ist M ein quadratischer Rest oder Nichtrest von m, je nachdem, ob n gerade oder ungerade ist.

BEWEIS. Diejenigen unter diesen Resten, die kleiner als $\frac{1}{2}m$ sind, seien a, b, c, d usw., die übrigen, die größer als $\frac{1}{2}m$ sind, dagegen $a',\ b',\ c',\ d'$ usw. Die Ergänzungen der Letzteren zu m, nämlich
$m-a',\ m-b',\ m-c',\ m-d'$ usw., sind offenbar sämtlich kleiner als $\frac{1}{2}m$ und sowohl untereinander als auch von den Resten $a,\ b,\ c,\ d$ usw. verschieden. Zusammen mit diesen bilden sie daher, wenn auch in anderer Reihenfolge, genau alle Zahlen $1,\ 2,\ 3,\ 4 \ldots . \frac{1}{2}(m-1)$. Setzen wir also das Produkt

$$1\,.\,2\,.\,3\,.\,4\,\ldots\ldots\,\tfrac{1}{2}(m-1) = P$$

so gilt

$$P = abcd\ldots . \times (m-a')(m-b')(m-c')(m-d')\ldots .$$

und damit

$$(-1)^n P = abcd\ldots . \times (a'-m)(b'-m)(c'-m)(d'-m)\ldots .$$

Ferner gilt modulo m

$$\begin{aligned} PM^{\frac{1}{2}(m-1)} &\equiv abcd\,..\times a'b'c'd'\,..\\ &\equiv abcd\,..\times (a'-m)(b'-m)(c'-m)(d'-m)\,.. \end{aligned}$$

und damit

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n$$

Hieraus folgt $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, wobei das obere oder untere Vorzeichen zu nehmen ist, je nachdem, ob n gerade oder ungerade ist. Mithilfe des in den *Disquisitiones Arithmeticae*, Art. 106, bewiesenen Satzes ergibt sich daraus unmittelbar die Richtigkeit des Lemmas.

2.

Satz. *Es seien m, M positive ungerade ganze Zahlen, die zueinander teilerfremd sind, und n sei die Anzahl derjenigen unter den kleinsten positiven Resten der Zahlen*

$$M,\ 2M,\ 3M \ldots\ldots \tfrac{1}{2}(m-1)M$$

modulo m, die größer als $\frac{1}{2}m$ sind. Ebenso sei N die Anzahl derjenigen unter den kleinsten positiven Resten der Zahlen

$$m,\ 2m,\ 3m \ldots\ldots \tfrac{1}{2}(M-1)m$$

modulo M, die größer als $\frac{1}{2}M$ sind. Dann sind die drei Zahlen n, N, $\frac{1}{4}(m-1)(M-1)$ entweder sämtlich gerade, oder eine ist gerade und die beiden anderen sind ungerade.

Beweis. Wir bezeichnen

mit f die Sammlung der Zahlen $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(m-1)$.
mit f' die Sammlung der Zahlen $m-1,\ m-2,\ m-3 \ldots\ldots \frac{1}{2}(m+1)$
mit F die Sammlung der Zahlen $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(M-1)$
mit F' die Sammlung der Zahlen $M-1,\ M-2,\ M-3 \ldots\ldots \frac{1}{2}(M+1)$

Damit gibt n an, wie viele Zahlen Mf ihre kleinsten positiven Reste modulo m in der Sammlung f' haben. Ebenso gibt N an, wie viele Zahlen mF ihre kleinsten positiven Reste modulo M in der Sammlung F' haben. Schließlich bezeichne

φ die Sammlung der Zahlen $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(mM-1)$
φ' die Sammlung der Zahlen $mM-1,\ mM-2,\ mM-3 \ldots\ldots \frac{1}{2}(mM+1)$

Jede ganze, durch m nicht teilbare Zahl muss modulo m entweder einem Rest aus f oder einem Rest aus f' kongruent sein. Ebenso ist jede ganze, durch M nicht teilbare Zahl modulo M entweder einem Rest aus F oder einem Rest aus F' kongruent. Daher lassen sich alle Zahlen in φ, unter denen offenbar keine zugleich durch m und M teilbar ist, folgendermaßen in acht Klassen einteilen.

I. Die erste Klasse enthält die Zahlen, die modulo m einer Zahl aus f, modulo M aber einer Zahl aus F kongruent sind. Ihre Anzahl bezeichnen wir mit α.

II. Die Zahlen, die modulo m, M jeweils Zahlen aus f, F' kongruent sind; ihre Anzahl setzen wir $= \beta$.

III. Die Zahlen, die modulo m, M jeweils Zahlen aus f', F kongruent sind; ihre Anzahl setzen wir $= \gamma$.

IV. Die Zahlen, die modulo m, M jeweils Zahlen aus f', F' kongruent sind; ihre Anzahl sei $= \delta$.

V. Die Zahlen, die durch m teilbar, modulo M aber Resten aus F kongruent sind.

VI. Die Zahlen, die durch m teilbar, modulo M aber Resten aus F' kongruent sind.

VII. Die Zahlen, die durch M teilbar, modulo m aber Resten aus f kongruent sind.

VIII. Die Zahlen, die durch M teilbar, modulo m aber Resten aus f' kongruent sind.

Offenbar umfassen die Klassen V und VI zusammen alle Zahlen mF. Die Anzahl der in VI enthaltenen Zahlen ist $= N$, also ist die Anzahl der in V enthaltenen Zahlen $\frac{1}{2}(M-1) - N$. Ebenso enthalten die Klassen VII und VIII zusammen alle Zahlen Mf; in der Klasse VIII finden sich n Zahlen, in der Klasse VII dagegen $\frac{1}{2}(m-1) - n$.

Auf genau dieselbe Weise werden alle Zahlen in φ' in acht Klassen IX . . XVI eingeteilt. Behalten wir dabei dieselbe Reihenfolge bei, so sieht man leicht, dass die Zahlen in den Klassen

IX, X, XI, XII, XIII, XIV, XV, XVI

jeweils die Ergänzungen zu mM der Zahlen in den Klassen

IV, III, II, I, VI, V, VIII, VII

sind, so dass sich in der Klasse IX δ Zahlen, in der Klasse X γ Zahlen usw. finden. Nehmen wir nun alle Zahlen der ersten Klasse mit allen Zahlen der neunten zusammen, so erhalten wir offenbar alle Zahlen unterhalb mM, die modulo m einer Zahl aus f, modulo M aber einer Zahl aus F kongruent sind. Deren Anzahl ist, wie man leicht sieht, gleich der Anzahl aller Kombinationen jeder einzelnen Zahl aus f mit jeder einzelnen aus F. Wir haben daher

$$\alpha + \delta = \tfrac{1}{4}(m-1)(M-1)$$

und aus ähnlichem Grund gilt auch

$$\beta + \gamma = \tfrac{1}{4}(m-1)(M-1)$$

Nehmen wir alle Zahlen der Klassen II, IV und VI zusammen, so erhalten wir offenbar alle Zahlen unterhalb $\frac{1}{2}mM$, die einem Rest aus F' modulo M kongruent sind. Dieselben Zahlen lassen sich aber auch so darstellen:

$$F',\ M+F',\ 2M+F',\ 3M+F' \ldots . \tfrac{1}{2}(m-3)M+F'$$

Ihre Gesamtzahl ist daher $= \frac{1}{4}(m-1)(M-1)$, oder es gilt

$$\beta+\delta+N = \tfrac{1}{4}(m-1)(M-1)$$

Ebenso lässt sich aus der Vereinigung aller Zahlen der Klassen III, IV und VIII folgern:

$$\gamma+\delta+n = \tfrac{1}{4}(m-1)(M-1)$$

Aus diesen vier Gleichungen ergeben sich die folgenden:

$$\begin{aligned} 2\alpha &= \tfrac{1}{4}(m-1)(M-1)+n+N \\ 2\beta &= \tfrac{1}{4}(m-1)(M-1)+n-N \\ 2\gamma &= \tfrac{1}{4}(m-1)(M-1)-n+N \\ 2\delta &= \tfrac{1}{4}(m-1)(M-1)-n-N \end{aligned}$$

von denen jede die Richtigkeit des Satzes zeigt.

3.

Nehmen wir nun an, m und M seien Primzahlen, so ergibt sich das Fundamentaltheorem unmittelbar aus der Verbindung des vorhergehenden Satzes mit dem Lemma aus Art. 1. Denn offenbar gilt:

I. Wenn die Zahlen m, M beide die Form $4k+1$ haben oder nur eine von ihnen, ist die Zahl $\frac{1}{4}(m-1)(M-1)$ gerade. Daher sind n und N entweder beide gerade oder beide ungerade, also ist entweder jede der Zahlen m und M ein quadratischer Rest der anderen oder jede ein quadratischer Nichtrest der anderen.

II. Wenn dagegen beide Zahlen m, M die Form $4k+3$ haben, ist $\frac{1}{4}(m-1)(M-1)$ ungerade. Daher ist eine der Zahlen n, N gerade und die andere ungerade; folglich ist eine der Zahlen m, M ein quadratischer Rest der anderen und diese ein quadratischer Nichtrest der ersteren. Q. E. D.

SECHSTER BEWEIS DES FUNDAMENTALTHEOREMS IN DER THEORIE DER QUADRATISCHEN RESTE.

1.

SATZ. *Es bezeichne p eine Primzahl (positiv und ungerade), n eine positive ganze, durch p nicht teilbare Zahl und x eine unbestimmte Größe. Dann ist die Funktion*

$$1 + x^n + x^{2n} + x^{3n} + \text{usw.} + x^{np-n}$$

teilbar durch

$$1 + x + xx + x^3 + \text{usw.} + x^{p-1}$$

BEWEIS. Man nehme eine positive ganze Zahl g so, dass $gn \equiv 1 \pmod{p}$ gilt, und setze $gn = 1 + hp$. Dann gilt

$$\begin{aligned}\frac{1 + x^n + x^{2n} + x^{3n} + \text{usw.}\, x^{np-n}}{1 + x + xx + x^3 + \text{usw.}\, x^{p-1}} &= \frac{(1-x^{np})(1-x)}{(1-x^n)(1-x^p)} \\ &= \frac{(1-x^{np})(1-x^{gn}-x+x^{hp+1})}{(1-x^n)(1-x^p)} \\ &= \frac{1-x^{np}}{1-x^p}\cdot\frac{1-x^{gn}}{1-x^n} - \frac{x(1-x^{np})}{1-x^n}\cdot\frac{1-x^{hp}}{1-x^p}\end{aligned}$$

und dieser Ausdruck ist offenbar ein Polynom. Q. E. D.

Jedes Polynom in x, das durch $\frac{1-x^{np}}{1-x^n}$ teilbar ist, ist daher auch durch $\frac{1-x^p}{1-x}$ teilbar.

2.

Es bezeichne α eine positive primitive Wurzel modulo p; das heißt, α sei eine positive ganze Zahl, deren Potenzen $1, \alpha, \alpha\alpha, \alpha^3 \ldots\ldots \alpha^{p-2}$ modulo p als kleinste positive Reste ohne Rücksicht auf die Reihenfolge genau die Zahlen $1, 2, 3, 4 \ldots\ldots p-1$ haben. Bezeichnen wir ferner mit fx die Funktion

$$x + x^\alpha + x^{\alpha\alpha} + x^{\alpha^3} + \text{usw.} + x^{\alpha^{p-2}} + 1$$

so ist offenbar $fx - 1 - x - xx - x^3 - \text{usw.} - x^{p-1}$ durch $1 - x^p$ teilbar und damit erst recht durch $\frac{1-x^p}{1-x} = 1 + x + xx + x^3 + \text{usw.} + x^{p-1}$. Durch diese letzte Funktion ist daher auch fx selbst teilbar. Da x eine unbestimmte Größe darstellt, folgt daraus, dass auch $f(x^n)$ durch $\frac{1-x^{np}}{1-x^n}$ und somit nach dem vorhergehenden Artikel auch durch $\frac{1-x^p}{1-x}$ teilbar ist, sofern n eine ganze, durch p nicht teilbare Zahl ist. Ist dagegen n eine ganze, durch p teilbare Zahl, so sind die einzelnen Glieder der Funktion $f(x^n)$, jeweils um eins vermindert, durch $1 - x^p$ teilbar. Daher ist in diesem Fall auch $f(x^n) - p$ durch $1 - x^p$ und somit auch durch $\frac{1-x^p}{1-x}$ teilbar.

3.

SATZ. *Setzt man*

$$x - x^{\alpha} + x^{\alpha\alpha} - x^{\alpha^3} + x^{\alpha^4} - \text{usw.} - x^{\alpha^{p-2}} = \xi$$

so ist $\xi\xi \mp p$ *durch* $\frac{1-x^p}{1-x}$ *teilbar. Dabei ist das obere Vorzeichen zu nehmen, wenn* p *die Form* $4k+1$ *hat, das untere, wenn* p *die Form* $4k+3$ *hat.*

BEWEIS. Man sieht leicht, dass von den folgenden $p-1$ Funktionen

$$\begin{aligned}
&+ x\xi - xx + x^{\alpha+1} - x^{\alpha\alpha+1} \\
&\qquad + \text{usw.} + x^{\alpha^{p-2}+1} \\
&- x^{\alpha}\xi - x^{2\alpha} + x^{\alpha\alpha+\alpha} - x^{\alpha^3+\alpha} \\
&\qquad + \text{usw.} + x^{\alpha^{p-1}+\alpha} \\
&+ x^{\alpha\alpha}\xi - x^{2\alpha\alpha} + x^{\alpha^3+\alpha\alpha} - x^{\alpha^4+\alpha\alpha} \\
&\qquad + \text{usw.} + x^{\alpha^p+\alpha\alpha} \\
&- x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} \\
&\qquad + \text{usw.} + x^{\alpha^{p+1}+\alpha^3}
\end{aligned}$$

usw. bis zu

$$-x^{\alpha^{p-2}}\xi - x^{2\alpha^{p-2}} + x^{\alpha^{p-1}+\alpha^{p-2}} - x^{\alpha^p+\alpha^{p-2}} + \text{usw.} + x^{\alpha^{2p-4}+\alpha^{p-2}}$$

die erste $= 0$ ist, jede der übrigen dagegen durch $1-x^p$ teilbar. Daher ist auch ihre Summe durch $1-x^p$ teilbar; sie ergibt sich zu

$$\begin{aligned}
&= \xi\xi - (f(xx) - 1) + (f(x^{\alpha+1}) - 1) - (f(x^{\alpha\alpha+1}) - 1) \\
&\qquad + (f(x^{\alpha^3+1}) - 1) - \text{usw.} \\
&\qquad + (f(x^{\alpha^{p-2}+1}) - 1) \\
&= \xi\xi - f(xx) + f(x^{\alpha+1}) - f(x^{\alpha\alpha+1}) \\
&\qquad + f(x^{\alpha^3+1}) - \text{usw.} + f(x^{\alpha^{p-2}+1}) = \Omega
\end{aligned}$$

Damit ist dieser Ausdruck Ω auch durch $\frac{1-x^p}{1-x}$ teilbar. Unter den Exponenten $2,\ \alpha+1,\ \alpha\alpha+1,\ \alpha^3+1 \ldots\ldots \alpha^{p-2}+1$ ist nun nur einer durch p teilbar, nämlich $\alpha^{\frac{1}{2}(p-1)}+1$. Nach dem vorhergehenden Artikel sind daher die folgenden einzelnen Glieder des Ausdrucks Ω

$$f(xx), \quad f(x^{\alpha+1}), \quad f(x^{\alpha\alpha+1}), \quad (fx^{\alpha^3+1}) \quad \text{usw.}$$

mit alleiniger Ausnahme des Gliedes $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$ durch $\frac{1-x^p}{1-x}$ teilbar. Diese Glieder dürfen daher weggelassen werden, so dass die folgende Funktion weiterhin durch $\frac{1-x^p}{1-x}$ teilbar bleibt:

$$\xi\xi \mp f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$$

Dabei gilt das obere oder untere Vorzeichen, je nachdem, ob p die Form $4k+1$ oder die Form $4k+3$ hat. Da außerdem $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})-p$ durch $\frac{1-x^p}{1-x}$ teilbar ist, ist auch $\xi\xi \mp p$ durch $\frac{1-x^p}{1-x}$ teilbar. Q. E. D.

Damit das doppelte Vorzeichen keine Zweideutigkeit hervorruft, bezeichnen wir mit ε die Zahl $+1$ oder -1, je nachdem, ob p die Form $4k+1$ oder $4k+3$ hat. Damit ist $\frac{(1-x)(\xi\xi-\varepsilon p)}{1-x^p}$ ein Polynom in x, das wir mit Z bezeichnen.

4.

Es sei q eine positive ungerade Zahl, also $\frac{1}{2}(q-1)$ eine ganze Zahl. Dann ist $(\xi\xi)^{\frac{1}{2}(q-1)} - (\varepsilon p)^{\frac{1}{2}(q-1)}$ durch $\xi\xi - \varepsilon p$ und somit auch durch $\frac{1-x^p}{1-x}$ teilbar. Wir setzen $\varepsilon^{\frac{1}{2}(q-1)} = \delta$ und

$$\xi^{q-1} - \delta p^{\frac{1}{2}(q-1)} = \frac{1-x^p}{1-x} \cdot Y$$

Dann ist Y ein Polynom in x, und es gilt $\delta = .+1$, wenn für eine der Zahlen p, q oder auch für beide die Form $4k+1$ vorliegt; dagegen gilt $\delta = -1$, wenn beide p, q die Form $4k+3$ haben.

5.

Nehmen wir nun an, auch q sei eine Primzahl, die von p verschieden ist. Nach dem in den *Disquisitiones Arithmeticae*, Art. 51, bewiesenen Satz ist offenbar

$$. \quad \xi^q - (x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{usw.} - x^{q\alpha^{p-2}})$$

durch q teilbar oder von der Form qX, wobei X ein Polynom in x ist, dessen numerische Koeffizienten ebenfalls ganze Zahlen sind (was auch für die übrigen hier vorkommenden Polynome Z, Y, W vorauszusetzen ist). Für den Modul p und die primitive Wurzel α bezeichnen wir den Index der Zahl q mit μ; das heißt, es gelte $q \equiv \alpha^\mu \pmod{p}$. Die Zahlen $q,\ q\alpha,\ q\alpha\alpha,\ q\alpha^3 \ldots\ldots q\alpha^{p-2}$ sind daher modulo p jeweils den Zahlen $\alpha^\mu,\ \alpha^{\mu+1},\ \alpha^{\mu+2} \ldots . \alpha^{p-2},\ 1,\ \alpha,\ \alpha\alpha \ldots . \alpha^{\mu-1}$ kongruent, also sind

$$\begin{aligned}
&x^q - x^{\alpha^\mu}\\
&x^{q\alpha} - x^{\alpha^{1+1}}\\
&x^{q\alpha\alpha} - x^{\alpha^{\mu+2}}\\
&x^{q\alpha^3} - x^{\alpha^{\mu+3}}\\
&\quad .\\
&\quad .\\
&\quad .\\
&\quad .\\
&x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}}\\
&x^{q\alpha^{p-\mu-1}} - x\\
&x^{q\alpha^{p-\mu}} - x^\alpha\\
&x^{q\alpha^{p-\mu+1}} - x^{\alpha\alpha}\\
&\quad .\\
&\quad .\\
&\quad .\\
&\quad .\\
&x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}}
\end{aligned}$$

durch $1 - x^p$ teilbar. Nehmen wir diese Größen abwechselnd mit positivem und negativem Vorzeichen und addieren sie, so sieht man, dass $1 - x^p$ die Funktion

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{usw.} - x^{q\alpha^{p-2}} \mp \xi$$

teilt. Dabei gilt das obere oder untere Vorzeichen, je nachdem, ob μ gerade oder ungerade ist, das heißt, ob q ein quadratischer Rest oder Nichtrest von p ist. Wir setzen daher

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{usw.} - x^{q\alpha^{p-2}} - \gamma\xi = (1 - x^p)W$$

mit $\gamma = +1$ oder $\gamma = -1$, je nachdem, ob q ein quadratischer Rest oder Nichtrest von p ist; dabei ist W offenbar ein Polynom.

6.

Nach diesen Vorbereitungen leiten wir aus der Verbindung der vorhergehenden Gleichungen die folgende her:

$$\begin{aligned} q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ + \frac{1 - x^p}{1 - x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ + Y\xi\xi - W\xi(1 - x)) \end{aligned}$$

Nehmen wir an, dass die Division der Funktion ξX durch

$$x^{p-1} + x^{p-2} + x^{p-3} + \text{usw.} + x + 1$$

den Quotienten U mit dem Rest T ergibt, oder dass gilt:

$$\xi X = \frac{1 - x^p}{1 - x} \cdot U + T$$

Dabei sind U, T Polynome, deren numerische Koeffizienten ebenfalls ganze Zahlen sind, und T hat einen sicher niedrigeren Grad als der Divisor. Dann gilt

$$\begin{aligned} qT - \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ = \frac{1 - x^p}{1 - x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ + Y\xi\xi - W\xi(1 - x) - qU) \end{aligned}$$

Diese Gleichung kann offenbar nur bestehen, wenn sowohl die linke als auch die rechte Seite für sich verschwindet. Daher ist $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ durch q teilbar, ebenso auch $\delta p^{\frac{1}{2}(q-1)} - \gamma$; somit ist wegen $\delta\delta = 1$ auch die Zahl $p^{\frac{1}{2}(q-1)} - \gamma\delta$ durch q teilbar.

Bezeichnet nun β die positiv oder negativ genommene Einheit, je nachdem, ob p ein quadratischer Rest oder Nichtrest der Zahl q ist, so ist $p^{\frac{1}{2}(q-1)} - \beta$ durch q teilbar und damit auch $\beta - \gamma\delta$. Dies ist nur möglich, wenn $\beta = \gamma\delta$ gilt. Daraus folgt unmittelbar das Fundamentaltheorem. Nämlich:

I. Wenn die Zahlen p, q beide die Form $4k + 1$ haben oder nur eine von ihnen, so dass $\delta = +1$ gilt, ist $\beta = \gamma$. Daher ist entweder zugleich q ein quadratischer Rest von p und p ein quadratischer Rest von q, oder zugleich q ein Nichtrest von p und p ein Nichtrest von q.

II. Wenn beide p, q die Form $4k+3$ haben, so dass $\delta = -1$ gilt, ist $\beta = -\gamma$. Daher ist entweder zugleich q ein quadratischer Rest von p und p ein Nichtrest von q, oder zugleich q ein Nichtrest von p und p ein Rest von q.

Q. E. D.

Ein neuer Algorithmus zur Entscheidung, ob eine gegebene positive ganze Zahl quadratischer Rest oder Nichtrest einer gegebenen positiven Primzahl ist.

1.

Bevor wir die neue Lösung dieser Aufgabe darstellen, wollen wir die in den *Disquisitiones Arithmeticae* angegebene Lösung kurz wiederholen. Sie lässt sich mit Hilfe des Fundamentaltheorems und der folgenden bekannten Sätze recht rasch durchführen:

I. Die Beziehung der Zahl a zur Zahl b (ob jene ein quadratischer Rest oder Nichtrest dieser ist) ist dieselbe wie die der Zahl c zu b, wenn $a \equiv c \pmod{b}$ gilt.

II. Ist a das Produkt der Faktoren $\alpha, \beta, \gamma, \delta$ usw. und b eine Primzahl, so hängt die Beziehung von a zu b folgendermaßen von der Beziehung dieser Faktoren zu b ab: a ist ein quadratischer Rest von b oder ein Nichtrest, je nachdem, ob eine gerade oder ungerade Anzahl dieser Faktoren Nichtreste von b sind. Ein Faktor, der ein Quadrat ist, braucht daher bei dieser Untersuchung überhaupt nicht berücksichtigt zu werden; ist ein Faktor dagegen eine Potenz einer ganzen Zahl mit ungeradem Exponenten, so kann diese ganze Zahl selbst an seine Stelle treten.

III. Die Zahl 2 ist ein quadratischer Rest jeder Primzahl der Form $8m + 1$ oder $8m + 7$, dagegen ein Nichtrest jeder Primzahl der Form $8m + 3$ oder $8m + 5$.

Es sei also eine Zahl a gegeben, deren Beziehung zu einer Primzahl b gesucht wird. Für a ist, falls sie größer als b ist, zunächst ihr kleinster positiver Rest modulo b einzusetzen. Zerlegt man diesen Rest in seine Primfaktoren, so führt Satz II die Frage darauf zurück, die Beziehung jedes dieser Faktoren zu b zu bestimmen. Die Beziehung des Faktors 2 (wenn er einmal, dreimal, fünfmal usw. vorkommt) ist nach Satz III bekannt; die Beziehung jedes übrigen Faktors hängt nach dem Fundamentaltheorem von der Beziehung von b selbst zu diesem Faktor ab. Anstelle der einen Beziehung der gegebenen Zahl zur Primzahl b sind also nun mehrere Beziehungen der Zahl b zu anderen ungeraden Primzahlen zu untersuchen, die kleiner als b sind. Diese Aufgaben werden auf dieselbe Weise auf kleinere Moduln zurückgeführt, und diese aufeinanderfolgenden Reduktionen müssen offenbar schließlich enden.

2.

Zur Erläuterung dieser Lösung sei die Beziehung der Zahl 103 zu 379 gesucht. Da 103 bereits kleiner als 379 und selbst eine Primzahl ist, ist unmittelbar das Fundamentaltheorem anzuwenden. Es besagt, dass die gesuchte Beziehung derjenigen der Zahl 379 zu 103 entgegengesetzt ist. Diese ist wiederum gleich der Beziehung der Zahl 70 zu 103, die ihrerseits von den Beziehungen der Zahlen 2, 5, 7 zu 103 abhängt. Die erste dieser Beziehungen

ist nach Satz III bekannt. Die zweite hängt nach dem Fundamentaltheorem von der Beziehung der Zahl 103 zu 5 ab, die nach Satz I gleich der Beziehung von 3 zu 5 ist; diese hängt wiederum nach dem Fundamentaltheorem von der Beziehung von 5 zu 3 ab, die nach Satz I gleich der nach Satz III bekannten Beziehung von 2 zu 3 ist. Ebenso hängt die Beziehung von 7 zu 103 nach dem Fundamentaltheorem von der Beziehung von 103 zu 7 ab, die nach Satz I gleich der Beziehung von 5 zu 7 ist; diese hängt wiederum nach dem Fundamentaltheorem von der Beziehung von 7 zu 5 ab, die nach Satz I gleich der nach Satz III bekannten Beziehung von 2 zu 5 ist. Wollen wir nun diese Analyse in eine Synthese umsetzen, so lässt sich die Entscheidung der Frage auf vierzehn Schritte zurückführen. Wir geben sie hier vollständig an, damit die größere Eleganz der neuen Lösung umso deutlicher hervortritt.

1. Die Zahl 2 ist ein quadratischer Rest der Zahl 103 (Satz III).
2. Die Zahl 2 ist ein quadratischer Nichtrest der Zahl 3 (Satz III).
3. Die Zahl 5 ist ein quadratischer Nichtrest der Zahl 3 (aus I und 2).
4. Die Zahl 3 ist ein quadratischer Nichtrest der Zahl 5 (Fundamentaltheorem und 3).
5. Die Zahl 103 ist ein quadratischer Nichtrest der Zahl 5 (I und 4).
6. Die Zahl 5 ist ein quadratischer Nichtrest der Zahl 103 (Fundamentaltheorem und 5).
7. Die Zahl 2 ist ein quadratischer Nichtrest der Zahl 5 (Satz III).
8. Die Zahl 7 ist ein quadratischer Nichtrest der Zahl 5 (I und 7).
9. Die Zahl 5 ist ein quadratischer Nichtrest der Zahl 7 (Fundamentaltheorem und 8).
10. Die Zahl 103 ist ein quadratischer Nichtrest der Zahl 7 (I und 9).
11. Die Zahl 7 ist ein quadratischer Rest der Zahl 103 (Fundamentaltheorem und 10).
12. Die Zahl 70 ist ein quadratischer Nichtrest der Zahl 103 (II, 1, 6, 11).
13. Die Zahl 379 ist ein quadratischer Nichtrest der Zahl 103 (I und 12).
14. Die Zahl 103 ist ein quadratischer Rest der Zahl 379 (Fundamentaltheorem und 13).

Im Folgenden verwenden wir der Kürze wegen das in *Comment. Gotting. Vol. XVI* eingeführte Zeichen. Mit $[x]$ bezeichnen wir die Größe x selbst, wenn x eine ganze Zahl ist, und die größte ganze Zahl unterhalb von x, wenn x nicht ganzzahlig ist. Damit ist $x - [x]$ stets nichtnegativ und kleiner als eins.

3.

Aufgabe. *Es seien a, b positive, zueinander teilerfremde ganze Zahlen, und es sei $[\frac{1}{2}a] = a'$ gesetzt. Gesucht ist die Summe*

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \left[\frac{3b}{a}\right] + \left[\frac{4b}{a}\right] + \text{usw.} + \left[\frac{a'b}{a}\right]$$

LÖSUNG. Bezeichnen wir eine solche Summe der Kürze wegen mit $\varphi(a, b)$, so gilt auch

$$\varphi(b, a) = \left[\frac{a}{b}\right] + \left[\frac{2a}{b}\right] + \left[\frac{3a}{b}\right] + \text{usw.} + \left[\frac{b'a}{b}\right]$$

wenn wir $[\frac{1}{2}b] = b'$ setzen. Im dritten Beweis des Fundamentaltheorems wurde gezeigt, dass für ungerade a und b gilt:

$$\varphi(a, b) + \varphi(b, a) = a'b'$$

Mit derselben Methode lässt sich die Gültigkeit dieses Satzes leicht auch auf den Fall ausdehnen, dass eine der Zahlen a, b ungerade ist, wie wir dort bereits angedeutet haben. Man teile a durch b, wie bei dem Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen; dabei sei β der Quotient und c der Rest. Dann teile man b durch c usw., so dass die folgenden Gleichungen entstehen:

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \varepsilon e + f \text{ usw.} \end{aligned}$$

Auf diese Weise erreichen wir in der ständig abnehmenden Folge der Zahlen b, c, d, e, f usw. schließlich die Eins, da a und b nach Voraussetzung teilerfremd sind. Die letzte Gleichung lautet daher

$$k = \lambda l + 1$$

Da offenbar

$$\begin{aligned} \left[\frac{a}{b}\right] &= \left[\beta + \frac{c}{b}\right] = \beta + \left[\frac{c}{b}\right] \\ \left[\frac{2a}{b}\right] &= \left[2\beta + \frac{2c}{b}\right] = 2\beta + \left[\frac{2c}{b}\right] \\ \left[\frac{3a}{b}\right] &= \left[3\beta + \frac{3c}{b}\right] = 3\beta + \left[\frac{3c}{b}\right] \end{aligned}$$

usw.. gilt, erhalten wir

$$\varphi(b, a) = \varphi(b, c) + \tfrac{1}{2}\beta(b'b' + b')$$

und damit

$$\varphi(a, b) = a'b' - \tfrac{1}{2}\beta(b'b' + b') - \varphi(b, c)$$

Setzen wir $[\frac{1}{2}c] = c'$, $[\frac{1}{2}d] = d'$ $[\frac{1}{2}e] = e'$ usw., so ergibt sich durch ähnliche Überlegungen

$$\begin{aligned}\varphi(b,c) &= b'c' - \tfrac{1}{2}\gamma(c'c' + c') - \varphi(c,d)\\ \varphi(c,d) &= c'd' - \tfrac{1}{2}\delta(d'd' + d') - \varphi(d,e).\\ \varphi(d,e) &= d'e' - \tfrac{1}{2}\varepsilon(e'e' + e') - \varphi(e,f)\end{aligned}$$

usw., bis hin zu

$$\varphi(k,l) = k'l' - \tfrac{1}{2}\lambda(l'l' + l') - \varphi(l,1)$$

Da offenbar $\varphi(l,1) = 0$ ist, erhalten wir hieraus die Formel

$$\begin{aligned}\varphi(a,b) = {} & a'b' - b'c' + c'd' - d'e' + \text{usw.} \pm k'l'\\ & - \tfrac{1}{2}\beta(b'b' + b') + \tfrac{1}{2}\gamma(c'c' + c') - \tfrac{1}{2}\delta(d'd' + d')\\ & + \tfrac{1}{2}\varepsilon(e'e' + e') - \text{usw.} \mp \tfrac{1}{2}\lambda(l'l' + l')\end{aligned}$$

4.

Aus dem dritten Beweis folgt nun leicht, dass die Beziehung der Zahl b zu a, sofern a eine Primzahl ist, unmittelbar am Wert der Summe $\varphi(a, 2b)$ erkannt wird. Je nachdem, ob diese Summe gerade oder ungerade ist, ist b ein quadratischer Rest von a oder ein Nichtrest. Zu demselben Zweck kann auch die Summe $\varphi(a,b)$ selbst verwendet werden, allerdings mit der Einschränkung, dass der Fall eines ungeraden b von dem eines geraden zu unterscheiden ist. Es gilt nämlich:

I. Ist b ungerade, so ist b ein quadratischer Rest oder Nichtrest von a, je nachdem, ob $\varphi(a,b)$ gerade oder ungerade ist.

II. Ist b gerade, so gilt dieselbe Regel, wenn außerdem a die Form $8n+1$ oder $8n+7$ hat; hat dagegen bei einem geraden Wert von b der Modul a die Form $8n+3$ oder $8n+5$, so ist die entgegengesetzte Regel anzuwenden: b ist ein quadratischer Rest von a, wenn $\varphi(a,b)$ ungerade ist, dagegen ein Nichtrest, wenn $\varphi(a,b)$ gerade ist.

All dies folgt sehr leicht aus Artikel 4 des dritten Beweises.

5.

Beispiel. Ist die Beziehung der Zahl 103 zur Primzahl 379 gesucht, so haben wir zur Berechnung der Summe $\varphi(379, 103)$:

$$\begin{array}{r|r|l} a = 379 & a' = 189 & \\ b = 103 & b' = 51 & \beta = 3 \\ c = 70 & c' = 35 & \gamma = 1 \\ d = 33 & d' = 16 & \delta = 2 \\ e = 4 & e' = 2 & \varepsilon = 8 \end{array}$$

und damit

$$\begin{aligned} \varphi(379, 103) &= 9639 - 1785 + 560 - 32 - 3978 + 630 - 272 + 24 \\ &= 4786 \end{aligned}$$

Also ist 103 ein quadratischer Rest der Zahl 379. Wollen wir stattdessen die Summe $(379, 206)$ für denselben Zweck verwenden, so erhalten wir das folgende Schema:

$$\begin{array}{r|r|l} 379 & 189 & \\ 206 & 103 & 1 \\ 173 & 86 & 1 \\ 33 & 16 & 5 \\ 8 & 4 & 4 \end{array}$$

Hieraus ergibt sich

$$\begin{aligned} \varphi(379, 206) &= 19467 - 8858 + 1376 - 64 - 5356 + 3741 - 680 + 40 \\ &= 9666 \end{aligned}$$

Somit ist 103 ein quadratischer Rest der Zahl 379.

6.

Um die Beziehung der Zahl b zu a zu entscheiden, brauchen die einzelnen Glieder der Summe $\varphi(a, b)$ nicht berechnet zu werden; es genügt zu wissen, wie viele von ihnen ungerade sind. Unsere Regel lässt sich daher auch so angeben:

Es sei wie oben $a = \beta b + c,\ b = \gamma c + d,\ c = \delta d + e$ usw., bis in der Folge der Zahlen $a,\ b,\ c,\ d,\ e$ usw. die Eins erreicht ist. Man setze $[\frac{1}{2}a] = a',\ [\frac{1}{2}b] = b',\ [\frac{1}{2}c] = c'$ usw. Ferner sei μ die Anzahl der ungeraden Zahlen in der Folge a', b', c' usw., auf die unmittelbar eine ungerade Zahl folgt, und ν die Anzahl der ungeraden Zahlen in der Folge β, γ, δ usw., denen in der Folge b', c', d' usw. jeweils eine Zahl der Form $4n + 1$ oder $4n + 2$ entspricht. Dann ist b ein quadratischer Rest oder Nichtrest von a, je nachdem, ob $\mu + \nu$ gerade oder ungerade ist. Ausgenommen ist allein der Fall, dass zugleich b gerade ist und a die Form $8n + 3$ oder $8n + 5$ hat; hier gilt die entgegengesetzte Regel.

In unserem Beispiel folgt in der Folge a', b', c', d', e' zweimal unmittelbar auf eine ungerade Zahl wieder eine ungerade; also ist $\mu = 2$; in der Folge $\beta', \gamma', \delta', \varepsilon'$ kommen zwar zwei ungerade Zahlen vor, ihnen entsprechen jedoch in der Folge b', c', d', e' Zahlen der Form $4n + 3$, so dass $\nu = 0$ ist. Damit ist $\mu + \nu$ gerade, und folglich ist 103 ein quadratischer Rest der Zahl 379.

THEORIE

DER BIQUADRATISCHEN RESTE

ERSTE ABHANDLUNG

VON

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT AM 5. APRIL 1825 VORGELEGT.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VI.
Göttingen MDCCCXXVIII.

THEORIE DER BIQUADRATISCHEN RESTE.

ERSTE ABHANDLUNG.

1.

Die Theorie der quadratischen Reste lässt sich auf wenige grundlegende Sätze zurückführen, die zu den schönsten Kleinodien der höheren Arithmetik gehören. Bekanntlich wurden sie zunächst durch induktive Beobachtung leicht entdeckt und dann auf vielfältige Weise so bewiesen, dass nichts mehr zu wünschen übrig bleibt.

Die Theorie der kubischen und biquadratischen Reste verlangt dagegen eine sehr viel tiefere Untersuchung. Als wir 1805 begannen, sie zu erforschen, fanden wir neben den Ergebnissen, die gleichsam an der Schwelle liegen, einige besondere Sätze, die sowohl durch ihre Einfachheit als auch durch die Schwierigkeit ihrer Beweise sehr bemerkenswert sind. Bald erkannten wir jedoch, dass die bis dahin verwendeten Prinzipien der Arithmetik keineswegs ausreichen, um die allgemeine Theorie zu begründen. Diese verlangt vielmehr notwendig, das Gebiet der höheren Arithmetik gleichsam unendlich viele Male zu erweitern. Was darunter zu verstehen ist, wird in der Fortsetzung dieser Untersuchungen völlig deutlich werden. Sobald wir dieses neue Gebiet betreten hatten, eröffnete uns die induktive Beobachtung sogleich einen Zugang zu den einfachsten Sätzen, die die gesamte Theorie umfassen. Ihre Beweise lagen aber so tief verborgen, dass sie erst nach vielen vergeblichen Versuchen schließlich ans Licht gebracht werden konnten.

Da wir nun daran gehen, diese Studien zu veröffentlichen, beginnen wir mit der Theorie der biquadratischen Reste. In dieser ersten Abhandlung werden wir diejenigen Untersuchungen darlegen, die sich schon diesseits des erweiterten Gebiets der Arithmetik abschließen ließen. Sie bahnen gleichsam den Weg dorthin und tragen zugleich einige neue Entwicklungen zur Theorie der Kreisteilung bei.

2.

Den Begriff des biquadratischen Restes haben wir in Artikel 115 der *Disquisitiones Arithmeticae* eingeführt: Eine ganze Zahl a, positiv oder negativ, heißt biquadratischer Rest der ganzen Zahl p, wenn a modulo p einer vierten Potenz kongruent sein kann, und biquadratischer Nichtrest, wenn keine solche Kongruenz besteht. In allen folgenden Untersuchungen setzen wir, sofern wir nicht ausdrücklich etwas anderes sagen, voraus, dass der Modul p eine ungerade positive Primzahl ist und dass a nicht durch p teilbar ist, da sich alle übrigen Fälle sehr leicht auf diesen zurückführen lassen.

3.

Offenbar ist jeder biquadratische Rest von p auch quadratischer Rest derselben Zahl, und somit jeder quadratische Nichtrest auch biquadratischer Nichtrest. Dieser Satz lässt sich auch umkehren, wenn p eine Primzahl der Form $4n + 3$ ist. Ist nämlich in diesem Fall a ein quadratischer Rest von p, so setzen wir $a \equiv bb \pmod{p}$. Dabei ist b entweder quadratischer Rest von p oder Nichtrest. Im ersten Fall setzen wir $b \equiv cc$, woraus $a \equiv c^4$ folgt; also ist a ein biquadratischer Rest von p. Im zweiten Fall ist $-b$ ein quadratischer Rest von p (denn -1 ist Nichtrest jeder Primzahl der Form $4n + 3$). Setzt man $-b \equiv cc$, so folgt wie zuvor $a \equiv c^4$, und a ist ein biquadratischer Rest von p. Zugleich sieht man leicht, dass die Kongruenz $x^4 \equiv a \pmod{p}$ in diesem Fall außer $x \equiv c$ und $x \equiv -c$ keine weiteren Lösungen hat. Da diese unmittelbar einleuchtenden Sätze die gesamte Theorie der biquadratischen Reste für Primzahlmoduln der Form $4n + 3$ erschöpfen, schließen wir solche Moduln ganz aus unserer Untersuchung aus und beschränken diese auf Primzahlmoduln der Form $4n + 1$.

4.

Ist also p eine Primzahl der Form $4n + 1$, so lässt sich der Satz des vorigen Artikels nicht umkehren: Es kann quadratische Reste geben, die nicht zugleich biquadratische Reste sind. Dies geschieht, wenn ein quadratischer Rest dem Quadrat eines quadratischen Nichtrestes kongruent ist. Setzt man nämlich $a \equiv bb$, wobei b ein quadratischer Nichtrest von p ist, und könnte die Kongruenz $x^4 \equiv a$ durch einen Wert $x \equiv c$ erfüllt werden, so wäre $c^4 \equiv bb$, also das Produkt $(cc - b)(cc + b)$ durch p teilbar. Dann müsste p entweder den Faktor $cc - b$ oder den anderen Faktor $cc + b$ teilen; das heißt, entweder $+b$ oder $-b$ wäre quadratischer Rest von p und folglich wären es beide (da -1 ein quadratischer Rest ist), entgegen der Voraussetzung.

Man könnte also alle ganzen Zahlen, die nicht durch p teilbar sind, auf drei Klassen verteilen: Die erste enthielte die biquadratischen Reste, die zweite diejenigen biquadratischen Nichtreste, die zugleich quadratische Reste sind, und die dritte die quadratischen Nichtreste. Offenbar genügt es, nur die Zahlen $1, 2, 3 \ldots . p - 1$ so einzuteilen. Die Hälfte würde zur dritten Klasse gehören, während sich die andere Hälfte auf die erste und zweite Klasse verteilen würde.

5.

Es ist jedoch besser, vier Klassen folgendermaßen festzulegen.

Es sei A die Sammlung aller biquadratischen Reste von p zwischen 1 und $p-1$, einschließlich der Grenzen, und e ein beliebig gewählter quadratischer Nichtrest von p. Ferner sei B die Sammlung der kleinsten positiven Reste der Produkte eA modulo p, und C, D seien entsprechend die Sammlungen der kleinsten positiven Reste der Produkte eeA, e^3A modulo p. Dann sind offenbar die einzelnen Zahlen in B voneinander verschieden, ebenso diejenigen in C und diejenigen in D; die Null kann unter keiner dieser Zahlen vorkommen. Ferner sind alle Zahlen in A und C quadratische Reste von p, alle Zahlen in B und D hingegen quadratische Nichtreste. Daher kann keine der Sammlungen A, C eine Zahl mit B oder D gemeinsam haben. Aber auch A und C können keine Zahl gemeinsam haben, ebenso wenig B und D. Nehmen wir nämlich an,

I. eine Zahl aus A, etwa a, komme auch in C vor und sei dort aus dem ihr kongruenten Produkt eea' entstanden, wobei a' eine Zahl aus A ist. Man setze $a \equiv \alpha^4$, $a' \equiv \alpha'^4$ und wähle eine ganze Zahl Θ so, dass $\Theta\alpha' \equiv 1$ gilt. Dann ist $ee\alpha'^4 \equiv \alpha^4$, und durch Multiplikation mit Θ^4 folgt

$$ee \equiv \alpha^4\Theta^4$$

Also wäre ee ein biquadratischer Rest und somit e ein quadratischer Rest, entgegen der Voraussetzung.

II. Nimmt man ebenso an, eine Zahl gehöre zu beiden Sammlungen B, D und sei aus den Produkten ea, e^3a' entstanden, wobei a, a' Zahlen aus A sind, so würde aus der Kongruenz $ea \equiv e^3a'$ die Kongruenz $a \equiv eea'$ folgen. Man hätte also eine Zahl, die aus dem Produkt eea' entsteht und sowohl zu C als auch zu A gehört, was wir gerade als unmöglich erwiesen haben.

Ferner lässt sich leicht beweisen, dass *alle* quadratischen Reste von p zwischen 1 und $p-1$, einschließlich der Grenzen, notwendig entweder in A oder in C vorkommen und alle quadratischen Nichtreste von p zwischen diesen Grenzen notwendig entweder in B oder in D. Denn

I. Jeder solche quadratische Rest, der zugleich biquadratischer Rest ist, liegt nach Voraussetzung in A.

II. Einen quadratischen Rest h (kleiner als p), der zugleich biquadratischer Nichtrest ist, schreibe man als $\equiv gg$, wobei g ein quadratischer Nichtrest ist. Man wähle eine ganze Zahl γ so, dass $e\gamma \equiv g$ gilt. Dann ist γ ein quadratischer Rest von p, den wir als $\equiv kk$ schreiben. Daraus folgt

$$h \equiv gg \equiv ee\gamma\gamma \equiv eek^4$$

Da der kleinste Rest von k^4 in A liegt, muss die Zahl h, die durch Multiplikation dieses Restes mit ee entsteht, in C liegen.

III. Es bezeichne h einen quadratischen Nichtrest von p zwischen 1 und $p-1$. Man ermittle zwischen denselben Grenzen eine ganze Zahl g so, dass $eg \equiv h$ gilt. Dann ist g ein quadratischer Rest und liegt daher entweder in A oder in C. Im ersten Fall findet sich h offenbar unter den Zahlen B, im zweiten unter den Zahlen D.

Aus alledem folgt, dass sich sämtliche Zahlen $1, 2, 3 \ldots . p-1$ so auf die vier Listen A, B, C, D verteilen, dass jede in einer davon vorkommt; jede Liste muss daher $\frac{1}{4}(p-1)$ Zahlen enthalten. Bei dieser Einteilung stehen die Zahlen, die zu A und C gehören, durch das Wesen dieser Klassen fest. Die Unterscheidung zwischen B und D ist dagegen insofern beliebig, als sie von der Wahl der Zahl e abhängt, die selbst immer zu B gehört. Wählt man an ihrer Stelle eine Zahl aus D, so werden die Klassen B, D vertauscht.

6.

Da -1 ein quadratischer Rest von p ist, setzen wir $-1 \equiv ff \pmod{p}$. Die vier Wurzeln der Kongruenz $x^4 \equiv 1$ sind dann $1, f, -1, -f$. Ist also a ein biquadratischer Rest von p, etwa $\equiv \alpha^4$, so sind die vier Wurzeln der Kongruenz $x^4 \equiv a$ die Zahlen $\alpha, f\alpha, -\alpha, -f\alpha$, die offenbar paarweise inkongruent sind. Sammelt man also die kleinsten positiven Reste der vierten Potenzen $1, 16, 81, 256 \ldots . (p-1)^4$, so sind immer je vier gleich. Man erhält somit $\frac{1}{4}(p-1)$ verschiedene biquadratische Reste, die die Sammlung A bilden. Sammelt man die kleinsten Reste der vierten Potenzen nur bis $(\frac{1}{2}p - \frac{1}{2})^4$, so kommt jeder zweimal vor.

7.

Das Produkt zweier biquadratischer Reste ist offenbar ein biquadratischer Rest: Multipliziert man zwei Zahlen der Klasse A, so gehört der kleinste positive Rest ihres Produkts wieder zu dieser Klasse. Ebenso liegen die kleinsten Reste der Produkte einer Zahl aus B mit einer Zahl aus D oder einer Zahl aus C mit einer Zahl aus C in A.

In B liegen die Reste der Produkte $A.B$ und $C.D$; in C diejenigen der Produkte $A.C$, $B.B$ und $D.D$; und schließlich in D diejenigen der Produkte $A.D$ und $B.C$.

Die Beweise sind so unmittelbar, dass es genügt, einen anzudeuten. Es seien etwa c und d Zahlen aus C und D, und es sei $c \equiv eea$, $d \equiv e^3a'$, wobei a, a' Zahlen aus A bezeichnen. Dann ist e^4aa' ein biquadratischer Rest, sein kleinster Rest gehört also zu A. Für das Produkt gilt $cd \equiv e.e^4aa'$; sein kleinster Rest liegt daher in B.

Nun lässt sich auch leicht entscheiden, zu welcher Klasse ein Produkt mehrerer Faktoren gehört. Gibt man den Klassen A, B, C, D entsprechend die Charaktere $0, 1, 2, 3$, so ist der Charakter des Produkts entweder die Summe der Charaktere der einzelnen Faktoren oder deren kleinster Rest modulo 4.

8.

Es schien lohnend, diese elementaren Sätze ohne die Theorie der Potenzreste zu entwickeln. Zieht man diese heran, so lässt sich alles noch sehr viel leichter beweisen.

Es sei g eine primitive Wurzel für den Modul p, also eine Zahl, bei der in der Folge der Potenzen $g, gg, g^3 \ldots.$ keine vor g^{p-1} modulo p der Einheit kongruent ist. Dann stimmen die kleinsten positiven Reste der Zahlen $1, g, gg, g^3 \ldots. g^{p-2}$, von ihrer Reihenfolge abgesehen, mit $1, 2, 3 \ldots. p-1$ überein und verteilen sich folgendermaßen auf vier Klassen:

zu	kleinste Reste der Zahlen
A	$1,\ g^4, g^8, g^{12} \ldots. g^{p-5}$
B	$g,\ g^5, g^9, g^{13} \ldots. g^{p-4}$
C	$gg, g^6, g^{10}, g^{14} \ldots. g^{p-3}$
D	$g^3, g^7, g^{11}, g^{15} \ldots. g^{p-2}$

Daraus ergeben sich alle vorhergehenden Sätze unmittelbar.

So wie hier die Zahlen $1, 2, 3 \ldots. p-1$ auf vier Klassen verteilt wurden, deren Sammlungen wir mit A, B, C, D bezeichnen, kann man *jede* ganze Zahl, die nicht durch p teilbar ist, nach ihrem kleinsten Rest modulo p einer dieser Klassen zuordnen.

9.

Wir bezeichnen mit f den kleinsten Rest der Potenz $g^{\frac{1}{4}(p-1)}$ modulo p. Da $ff \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ gilt (*Disquis. Arithm.*, Artikel 62), hat das Zeichen f hier offenbar dieselbe Bedeutung wie in Artikel 6. Die Potenz $g^{\frac{1}{4}\lambda(p-1)}$, wobei λ eine positive ganze Zahl bezeichnet, ist also modulo p der Zahl $1, f, -1, -f$ kongruent, je nachdem λ entsprechend die Form $4m, 4m+1, 4m+2, 4m+3$ hat oder der kleinste Rest von g^λ entsprechend in A, B, C, D liegt. Dies gibt ein sehr einfaches Kriterium dafür, welcher Klasse eine gegebene Zahl h, die nicht durch p teilbar ist, zuzuordnen ist: h gehört zu A, B, C oder D, je nachdem die Potenz $h^{\frac{1}{4}(p-1)}$ modulo p der Zahl $1, f, -1$ oder $-f$ kongruent ist.

Als Folgerung ergibt sich, dass -1 stets zur Klasse A gehört, wenn p die Form $8n+1$ hat, und zur Klasse C, wenn p die Form $8n+5$ hat. Ein von der Theorie der Potenzreste unabhängiger Beweis dieses Satzes lässt sich leicht aus dem gewinnen, was wir in Artikel 115, III der *Disquisitiones Arithmeticae* gezeigt haben.

10.

Da *alle* primitiven Wurzeln für den Modul p aus den Resten der Potenzen g^λ hervorgehen, wenn man für λ alle zu $p-1$ teilerfremden Zahlen nimmt, sieht man leicht, dass diese Wurzeln gleichmäßig auf B und D verteilt sind, wobei die Basis g stets in B liegt. Wählt man anstelle von g eine andere

primitive Wurzel aus B als Basis, so bleibt die Einteilung dieselbe; wählt man dagegen eine primitive Wurzel aus D als Basis, so werden die Klassen B und D vertauscht.

Beruht die Einteilung auf dem Kriterium des vorigen Artikels, so hängt die Unterscheidung zwischen B und D davon ab, welche Wurzel der Kongruenz $xx \equiv -1 \pmod{p}$ wir als charakteristische Zahl f wählen.

11.

Damit sich die feineren Untersuchungen, die wir nun beginnen, leichter durch Beispiele veranschaulichen lassen, geben wir hier die Konstruktion der Klassen für alle Moduln unter 100 an. Für jeden haben wir die kleinste primitive Wurzel gewählt.

$$p = 5$$
$$g = 2, \ f = 2$$

A	1
B	2
C	4
D	3

$$p = 13$$
$$g = 2, \ f = 8$$

A	1, 3, 9
B	2, 5, 6
C	4, 10, 12
D	7, 8, 11

$$p = 17$$
$$g = 3, \ f = 13$$

A	1, 4, 13, 16
B	3, 5, 12, 14
C	2, 8, 9, 15
D	6, 7, 10, 11

$$p = 29$$
$$g = 2, \ f = 12$$

A	1, 7, 16, 20, 23, 24, 25
B	2, 3, 11, 14, 17, 19, 21
C	4, 5, 6, 9, 13, 22, 28
D	8, 10, 12, 15, 18, 26, 27

$$p = 37$$
$$g = 2,\ f = 31$$

A	$1, 7, 9, 10, 12, 16, 26, 33, 34$
B	$2, 14, 15, 18, 20, 24, 29, 31, 32$
C	$3, 4, 11, 21, 25, 27, 28, 30, 36$
D	$5, 6, 8, 13, 17, 19, 22, 23, 35$

$$p = 41$$
$$g = 6,\ f = 32$$

A	$1, 4, 10, 16, 18, 23, 25, 31, 37, 40$
B	$6, 14, 15, 17, 19, 22, 24, 26, 27, 35$
C	$2, 5, 8, 9, 20, 21, 32, 33, 36, 39$
D	$3, 7, 11, 12, 13, 28, 29, 30, 34, 38$

$$p = 53$$
$$g = 2,\ f = 30$$

A	$1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49$
B	$2, 3, 19, 20, 26, 30, 31, 32, 35, 39, 41, 45, 48$
C	$4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43, 52$
D	$5, 8, 12, 14, 18, 21, 22, 23, 27, 33, 34, 50, 51$

$$p = 61$$
$$g = 2,\ f = 11$$

A	$1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58$
B	$2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55$
C	$3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60$
D	$6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59$

$$p = 73$$
$$g = 5,\ f = 27$$

A	$1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72$
B	$5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68$
C	$3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70$
D	$11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62$

$$p = 89$$
$$g = 3,\ \ f = 34$$

A	$1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44.\ 45,$
	$50, 57, 64, 67, 73, 78, 81, 85, 87, 88$
B	$3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46,$
	$48, 56, 61, 65, 66, 75, 77, 82, 83, 86$
C	$5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47,$
	$49, 53, 55, 68, 69, 71, 72, 79, 80, 84$
D	$13, 15.\ 19, 26, 27, 29.\ 30, 31, 35, 37, 38.\ 51,$
	$52, 54, 58, 59, 60, 62, 63, 70, 74, 76$

$$p = 97$$
$$g = 5,\ \ f = 22$$

A	$1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47,$
	$50, 54, 61, 62, 64, 73, 75, 81, 88, 91, 93, 96$
B	$5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45,$
	$52, 56, 67, 68, 74, 76, 77, 78, 80, 83, 84, 92$
C	$2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48,$
	$49, 53, 65.\ 66, 70, 72, 79, 85, 86, 89, 94, 95$
D	$7, 10, 15, 26, 28, 34, 37, 38, 39.\ 40, 42, 46,$
	$51, 55, 57, 58, 59, 60, 63, 69, 71, 82, 87, 90$

12.

Da 2 quadratischer Rest aller Primzahlen der Form $8n + 1$, hingegen Nichtrest aller Primzahlen der Form $8n + 5$ ist, liegt für Primzahlmoduln der ersten Form 2 in der Klasse A oder C, für Moduln der zweiten Form dagegen in B oder D. Der Unterschied zwischen B und D ist nicht wesentlich, da er allein von der Wahl der Zahl f abhängt; daher lassen wir die Moduln der Form $8n + 5$ vorerst beiseite. Durch eine *induktive Untersuchung* der Moduln der Form $8n + 1$ finden wir, dass 2 zu A gehört für $p = 73, 89, 113, 233, 257, 281, 337, 353$ usw.; dagegen gehört 2 zu C für $p = 17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457$ usw.

Da ferner für einen Primzahlmodul der Form $8n+1$ die Zahl -1 ein biquadratischer Rest ist, gehört -2 offenbar stets zur selben Klasse wie $+2$.

13.

Vergleicht man die Beispiele des vorigen Artikels miteinander, so scheint sich zumindest auf den ersten Blick kein einfaches Kriterium anzubieten, das die ersten Moduln von den zweiten unterscheidet. Dennoch gibt es *zwei* solche Kriterien, die sich durch besondere Eleganz und Einfachheit auszeichnen. Die folgenden Überlegungen werden den Weg zu einem von ihnen bahnen.

Der Modul p lässt sich als Primzahl der Form $8n+1$ auf genau eine Weise in der Form $aa + 2bb$ darstellen (*Disquiss. Arithm.*, Artikel 182, II). Dabei setzen wir voraus, dass die Wurzeln a, b positiv genommen werden. Offenbar ist a ungerade und b gerade; wir setzen $b = 2^\lambda c$, wobei c ungerade ist. Nun bemerken wir:

I. Da $p \equiv aa \pmod{c}$ gilt, ist p ein quadratischer Rest von c und somit auch von jedem der Primfaktoren, in die c zerlegt wird. Umgekehrt sind nach dem Fundamentaltheorem diese einzelnen Primfaktoren quadratische Reste von p, und damit ist auch ihr Produkt c ein quadratischer Rest von p. Da dies auch für die Zahl 2 gilt, ist b offenbar ein quadratischer Rest von p, und somit sind bb und auch $-bb$ biquadratische Reste.

II. Daher muss $-2bb$ zu derselben Klasse gehören wie die Zahl 2. Da $aa \equiv -2bb$ gilt, liegt 2 offenbar in der Klasse A oder in der Klasse C, je nachdem a ein quadratischer Rest von p oder ein quadratischer Nichtrest ist.

III. Nehmen wir nun an, a sei in seine Primfaktoren zerlegt. Diejenigen der Form $8m+1$ oder $8m+7$ seien mit $\alpha, \alpha', \alpha''$ usw. bezeichnet, diejenigen der Form $8m+3$ oder $8m+5$ mit β, β', β'' usw.; die Anzahl der letzteren sei $= \mu$. Da $p \equiv 2bb \pmod{a}$ gilt, ist p ein quadratischer Rest derjenigen Primfaktoren von a, deren quadratischer Rest 2 ist, also der Faktoren $\alpha, \alpha', \alpha''$ usw.; dagegen ist es ein quadratischer Nichtrest derjenigen Faktoren, deren quadratischer Nichtrest 2 ist, also der Faktoren β, β', β'' usw. Umgekehrt sind daher nach dem Fundamentaltheorem die einzelnen $\alpha, \alpha', \alpha''$ usw. quadratische Reste von p, die einzelnen β, β', β'' usw. hingegen quadratische Nichtreste. Wir schließen also, dass das Produkt a ein quadratischer Rest von p oder ein Nichtrest ist, je nachdem μ gerade oder ungerade ist.

IV. Man bestätigt leicht, dass das Produkt aller $\alpha, \alpha', \alpha''$ usw. die Form $8m+1$ oder $8m+7$ hat und dass dies auch für das Produkt aller β, β', β'' usw. gilt, wenn deren Anzahl gerade ist. In diesem Fall muss also auch das Produkt a die Form $8m+1$ oder $8m+7$ haben. Ist dagegen beim Produkt aller β, β', β'' usw. die Anzahl der Faktoren ungerade, so hat es die Form $8m+3$ oder $8m+5$, und dasselbe gilt in diesem Fall auch für das Produkt a.

Aus alledem ergibt sich der elegante Satz:

Hat a die Form $8m+1$ oder $8m+7$, so liegt die Zahl 2 in A; hat dagegen a die Form $8m+3$ oder $8m+5$, so liegt die Zahl 2 in C.

Dies bestätigen die Beispiele des vorigen Artikels. Die ersten Moduln werden nämlich folgendermaßen zerlegt: $73 = 1 + 2 \,.\, 36$, $89 = 81 + 2 \,.\, 4$, $113 = 81 + 2 \,.\, 16$, $233 = 225 + 2 \,.\, 4$, $257 = 225 + 2 \,.\, 16$, $281 = 81 + 2 \,.\, 100$, $337 = 49 + 2 \,.\, 144$, $353 = 225 + 2 \,.\, 64$; die zweiten dagegen folgendermaßen: $17 = 9 + 2 \,.\, 4$, $41 = 9 + 2 \,.\, 16$, $97 = 25 + 2 \,.\, 36$, $137 = 9 + 2 \,.\, 64$, $193 = 121 + 2 \,.\, 36$, $241 = 169 + 2 \,.\, 36$, $313 = 25 + 2 \,.\, 144$, $401 = 9 + 2 \,.\, 196$, $409 = 121 + 2 \,.\, 144$, $433 = 361 + 2 \,.\, 36$, $449 = 441 + 2 \,.\, 4$, $457 = 169 + 2 \,.\, 144$.

14.

Die Zerlegung der Zahl p in ein Quadrat und das Doppelte eines Quadrats hat einen so bemerkenswerten Zusammenhang mit der Einteilung der Zahl 2 ergeben, dass es lohnend scheint zu untersuchen, ob die Zerlegung in zwei Quadrate, die bekanntlich auch für p möglich ist, vielleicht zu einem ähnlichen Ergebnis führt. Hier stehen daher die Zerlegungen der Zahlen p, für die 2 zur folgenden Klasse gehört:

A	C
$9 + 64$	$1 + 16$
$25 + 64$	$25 + 16$
$49 + 64$	$81 + 16$
$169 + 64$	$121 + 16$
$1 + 256$	$49 + 144$
$25 + 256$	$225 + 16$
$81 + 256$	$169 + 144$
$289 + 64$	$1 + 400$
	$9 + 400$
	$289 + 144$
	$49 + 400$
	$441 + 16$

Zunächst bemerken wir, dass von den beiden Quadraten, in die p zerlegt wird, eines ungerade sein muss, das wir $= aa$ setzen, und das andere gerade, das wir $= bb$ setzen. Da aa die Form $8n + 1$ hat, entsprechen den Werten von b, die das Doppelte einer ungeraden Zahl sind, offenbar Werte von p der Form $8n+5$. Diese bleiben hier bei unserer induktiven Untersuchung ausgeschlossen, da für sie die Zahl 2 in der Klasse B oder D läge. Für Werte von p der Form $8n + 1$ muss hingegen b durch vier teilbar sein. Wenn wir der induktiven Beobachtung vertrauen dürfen, die die angegebene Tabelle vor Augen führt, so gehört die Zahl 2 zur Klasse A für alle Moduln, bei denen b die Form $8n$ hat, und zur Klasse C für alle Moduln, bei denen b die Form $8n + 4$ hat. Dieser Satz verlangt jedoch eine sehr viel tiefere Untersuchung als derjenige, den wir im vorigen Artikel gewonnen haben. Seinem Beweis müssen mehrere

vorbereitende Untersuchungen darüber vorausgehen, in welcher Reihenfolge die Zahlen der Sammlungen A, B, C, D aufeinanderfolgen.

15.

Wir bezeichnen die Anzahl der Zahlen aus A, auf die unmittelbar eine Zahl aus A, B, C, D folgt, entsprechend mit $(00), (01), (02), (03)$; ebenso die Anzahl der Zahlen aus B, auf die eine Zahl aus A, B, C, D folgt, entsprechend mit $(10), (11), (12), (13)$. Entsprechend seien in C jeweils $(20), (21), (22), (23)$ Zahlen und in D jeweils $(30), (31), (32), (33)$ Zahlen enthalten, auf die eine Zahl aus A, B, C, D folgt. Wir wollen diese sechzehn Anzahlen a priori bestimmen. Damit die Leser die allgemeinen Überlegungen leichter mit Beispielen vergleichen können, erschien es zweckmäßig, hier die Zahlenwerte der Einträge des Schemas (S)

$$\begin{array}{cccc} (00), & (01), & (02), & (03) \\ (10), & (11), & (12), & (13) \\ (20). & (21), & (22), & (23) \\ (30), & (31), & (32), & (33) \end{array}$$

für jeden Modul anzugeben, dessen Klasseneinteilung wir in Artikel 11 angegeben haben.

$p = 5$	$p = 13$	$p = 17$	$p = 29$
$0, 1, 0.\ 0$	$0, 1, 2, 0$	$0, 2, 1, 0$	$2.\ 3, 0.\ 2$
$0, 0, 0, 1$	$1, 1, 0, 1$	$2, 0, 1, 1$	$1, 1, 2, 3$
$0, 0, 0, 0$	$0, 1, 0, 1$	$1, 1, 1, 1$	$2, 1, 2.\ 1$
$0, 0, 1, 0$	$1, 0, 1, 1$	$0, 1, 1, 2$	$1, 2, 3, 1$

$p = 37$	$p = 41$	$p = 53$	$p = 61$
$2, 1, 2, 4$	$0, 4, 3, 2$	$2, 3, 6, 2$	$4, 3, 2, 6$
$2, 2, 4, 1$	$4, 2, 2, 2$	$4, 4, 2, 3$	$3, 3, 6, 3$
$2, 2, 2, 2$	$3, 2, 3, 2$	$2, 4, 2, 4$	$4, 3, 4, 3$
$2, 4, 1, 2$	$2, 2, 2, 4$	$4, 2, 3, 4$	$3, 6, 3, 3$

$p = 73$	$p = 89$	$p = 97$
$5, 6, 4, 2$	$3, 8, 6, 4$	$2, 6, 7, 8$
$6, 2, 5, 5$	$8, 4, 5, 5$	$6, 8, 5, 5$
$4, 5, 4, 5$	$6, 5, 6, 5$	$7, 5, 7, 5$
$2, 5, 5, 6$	$4, 5, 5, 8$	$8, 5, 5, 6$

Da sich die Moduln der Formen $8n+1$ und $8n+5$ unterschiedlich verhalten, müssen wir sie getrennt behandeln. Wir beginnen mit den ersten.

16.

Das Zeichen (00) gibt an, auf wie viele verschiedene Weisen die Gleichung $\alpha+1=\alpha'$ erfüllt werden kann, wobei α, α' beliebige Zahlen aus A bezeichnen. Für einen Modul der Form $8n+1$, wie wir ihn hier voraussetzen, gehören α' und $p-\alpha'$ zu derselben Sammlung. Daher können wir eleganter sagen, (00) bezeichne die Anzahl der verschiedenen Möglichkeiten, die Gleichung $1+\alpha+\alpha'=p$ zu erfüllen. Offenbar kann an die Stelle dieser Gleichung auch die Kongruenz $1+\alpha+\alpha' \equiv 0 \pmod{p}$ treten.

Ebenso

bezeichnet (01) die Anzahl der Lösungen der Kongruenz $1+\alpha+\beta \equiv 0 \pmod{p}$
(02) die Anzahl der Lösungen der Kongruenz $1+\alpha+\gamma \equiv 0$
(03) die Anzahl der Lösungen der Kongruenz $1+\alpha+\delta \equiv 0$
(11) die Anzahl der Lösungen der Kongruenz $1+\beta+\beta' \equiv 0$ usw.

Dabei bezeichnen β und β' beliebige Zahlen aus B, γ Zahlen aus C und δ Zahlen aus D. Daraus erhalten wir unmittelbar die folgenden sechs Gleichungen:

$$(01)=(10), \quad (02)=(20), \quad (03)=(30),$$
$$(12)=(21), \quad (13)=(31), \quad (23)=(32)$$

Aus jeder gegebenen Lösung der Kongruenz $1+\alpha+\beta \equiv 0$ erhält man eine Lösung von $1+\delta+\delta' \equiv 0$, indem man für δ die Zahl zwischen $1 \ldots . p-1$ wählt, die $\beta\delta \equiv 1$ erfüllt (sie gehört offenbar zu D), und für δ' den kleinsten positiven Rest des Produkts $\alpha\delta$ (der ebenfalls zu D gehört). Ebenso ist der Rückweg von einer gegebenen Lösung von $1+\delta+\delta' \equiv 0$ zu einer Lösung von $1+\alpha+\beta \equiv 0$ möglich: Man wählt β so, dass $\beta\delta \equiv 1$ gilt, und setzt zugleich $\alpha \equiv \beta\delta'$. Beide Kongruenzen haben also gleich viele Lösungen, das heißt $(01)=(33)$.

Ebenso leiten wir aus der Kongruenz $1+\alpha+\gamma \equiv 0$ die Kongruenz $\gamma'+\gamma''+1 \equiv 0$ her, wenn wir γ' aus C so wählen, dass $\gamma\gamma' \equiv 1$ gilt, und γ'' aus derselben Sammlung kongruent zum Produkt $\alpha\gamma'$. Daraus folgt leicht, dass diese beiden Kongruenzen gleich viele Lösungen haben, also $(02)=(22)$.

Ebenso erhalten wir aus $1+\alpha+\delta \equiv 0$ die Kongruenz $\beta+\beta'+1 \equiv 0$, wenn wir β, β' so wählen, dass $\beta\delta \equiv 1$, $\beta\alpha \equiv \beta'$ gilt. Damit ist $(03)=(11)$.

Schließlich gewinnen wir aus $1+\beta+\gamma \equiv 0$ auf dieselbe Weise sowohl $\delta+1+\beta' \equiv 0$ als auch $\gamma'+\delta'+1 \equiv 0$ und schließen daraus $(12)=(13)=(23)$.

Wir haben somit zwischen unseren sechzehn Unbekannten elf Gleichungen erhalten, sodass sich die Unbekannten auf fünf reduzieren und das Schema S folgendermaßen geschrieben werden kann:

$$\begin{array}{llll} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i \end{array}$$

Drei weitere Bedingungsgleichungen lassen sich leicht hinzufügen. Auf jede Zahl aus A, mit Ausnahme der letzten, $p-1$, muss eine Zahl aus einer der Sammlungen A, B, C oder D folgen. Also gilt

$$(00) + (01) + (02) + (03) = 2n - 1$$

und ebenso

$$(10) + (11) + (12) + (13) = 2n$$
$$(20) + (21) + (22) + (23) = 2n$$
$$(30) + (31) + (32) + (33) = 2n$$

In den gerade eingeführten Zeichen ergeben die ersten drei Gleichungen:

$$h + i + k + l = 2n - 1$$
$$i + l + 2m = 2n$$
$$k + m = n$$

Die vierte wird mit der zweiten identisch. Mithilfe dieser Gleichungen lassen sich drei Unbekannte eliminieren, womit alle sechzehn bereits auf zwei reduziert sind.

17.

Um sie vollständig zu bestimmen, untersuchen wir zweckmäßig die Anzahl der Lösungen der Kongruenz

$$1 + \alpha + \beta + \gamma \equiv 0 \pmod{p}$$

wobei α, β, γ beliebige Zahlen aus A, B, C bezeichnen. Offenbar ist der Wert $\alpha = p - 1$ nicht zulässig, da $\beta + \gamma \equiv 0$ nicht gelten kann. Setzt man für α nacheinander die übrigen Werte ein, so erhält man h, i, k, l Werte von $1 + \alpha$, die entsprechend zu A, B, C, D gehören. Für jeden *gegebenen* Wert von $1 + \alpha$ in A, etwa $1 + \alpha = \alpha^0$, hat die Kongruenz $\alpha^0 + \beta + \gamma \equiv 0$ so viele Lösungen wie $1 + \beta' + \gamma' \equiv 0$ (man setze $\beta \equiv \alpha^0\beta'$, $\gamma \equiv \alpha^0\gamma'$), also $(12) = m$ Lösungen. Ebenso hat für jeden gegebenen Wert von $1 + \alpha$ in B, etwa $1 + \alpha = \beta^0$, die Kongruenz $\beta^0 + \beta + \gamma \equiv 0$ so viele Lösungen wie $1 + \alpha' + \beta' \equiv 0$ (man setze $\beta \equiv \beta^0\alpha'$, $\gamma \equiv \beta^0\beta'$), also $(01) = i$ Lösungen. Entsprechend lässt sich für jeden gegebenen Wert von $1 + \alpha$ in C, etwa $1 + \alpha = \gamma^0$, die Kongruenz $\gamma^0 + \beta + \gamma \equiv 0$ auf so viele verschiedene Weisen lösen wie $1 + \delta + \alpha' \equiv 0$ (man setze $\beta \equiv \gamma^0\delta$, $\gamma \equiv \gamma^0\alpha'$); die Anzahl der Lösungen ist also $(03) = l$. Schließlich hat für jeden gegebenen Wert von $1+\alpha$ in D, etwa $1+\alpha = \delta^0$, die Kongruenz $\delta^0 + \beta + \gamma \equiv 0$ so viele Lösungen wie $1 + \gamma' + \delta' \equiv 0$ (man setze $\beta \equiv \delta^0\gamma'$, $\gamma \equiv \delta^0\delta'$), also $(23) = m$ Lösungen. Zählt man alles zusammen, so hat die Kongruenz $1 + \alpha + \beta + \gamma \equiv 0$ offenbar

$$hm + ii + kl + lm$$

verschiedene Lösungen.

Ganz ebenso erhalten wir, wenn für β nacheinander die einzelnen Zahlen aus B eingesetzt werden, dass die Summe $1+\beta$ entsprechend $(10),(11),(12),(13)$ oder i,l,m,m Werte annimmt, die zu A,B,C,D gehören. Für jeden *gegebenen* Wert von $1+\beta$ aus diesen Sammlungen hat die Kongruenz $1+\beta+\alpha+\gamma\equiv 0$ entsprechend $(02),(31),(20),(13)$ oder k,m,k,m verschiedene Lösungen. Die Gesamtzahl aller Lösungen ist damit

$$= ik + lm + km + mm$$

Zum selben Wert gelangen wir, wenn wir die Rechnung auf die Werte der Summe $1+\gamma$ gründen.

18.

Aus diesen beiden Ausdrücken für dieselbe Anzahl ergibt sich die Gleichung

$$0 = hm + ii + kl - ik - km - mm$$

und daraus durch Elimination von h mithilfe von $h = 2m - k - 1$

$$0 = (k-m)^2 + ii + kl - ik - kk - m$$

Die letzten beiden Gleichungen aus Artikel 16 liefern $k = \frac{1}{2}(l+i)$. Setzt man diesen Wert ein, so wird $ii+kl-ik-kk$ zu $\frac{1}{4}(l-i)^2$, und die vorige Gleichung geht nach Multiplikation mit 4 über in

$$0 = 4(k-m)^2 + (l-i)^2 - 4m$$

Da $4m = 2(k+m) - 2(k-m) = 2n - 2(k-m)$ gilt, folgt

$$2n = 4(k-m)^2 + 2(k-m) + (l-i)^2$$

oder

$$8n + 1 = (4(k-m)+1)^2 + 4(l-i)^2$$

Setzen wir also

$$4(k-m)+1 = a, \quad 2l - 2i = b$$

so haben wir

$$p = aa + bb$$

Bekanntlich lässt sich p auf genau eine Weise in zwei Quadrate zerlegen, wobei das ungerade als aa und das gerade als bb zu nehmen ist. Damit sind aa, bb vollständig bestimmte Zahlen. Aber auch a selbst ist vollständig bestimmt: Die Quadratwurzel ist positiv oder negativ zu nehmen, je nachdem die positive Wurzel die Form $4M+1$ oder $4M+3$ hat. Über die Bestimmung des Vorzeichens von b werden wir gleich sprechen.

Verbindet man diese neuen Gleichungen mit den drei letzten Gleichungen aus Artikel 16, so sind die fünf Zahlen h, i, k, l, m durch a, b und n folgendermaßen vollständig bestimmt:

$$\begin{aligned} 8h &= 4n - 3a - 5 \\ 8i &= 4n + a - 2b - 1 \\ 8k &= 4n + a - 1 \\ 8l &= 4n + a + 2b - 1 \\ 8m &= 4n - a + 1 \end{aligned}$$

Wollen wir anstelle von n lieber den Modul p einführen, so hat das Schema S, dessen einzelne Einträge zur Vermeidung von Brüchen mit 16 multipliziert sind, folgende Gestalt:

$p - 6a - 11$	$p + 2a - 4b - 3$	$p + 2a - 3$	$p + 2a + 4b - 3$
$p + 2a - 4b - 3$	$p + 2a + 4b - 3$	$p - 2a + 1$	$p - 2a + 1$
$p + 2a - 3$	$p - 2a + 1$	$p + 2a - 3$	$p - 2a + 1$
$p + 2a + 4b - 3$	$p - 2a + 1$	$p - 2a + 1$	$p + 2a - 4b - 3$

19.

Es bleibt zu zeigen, wie man das Vorzeichen für b festlegt. In Artikel 10 haben wir bereits bemerkt, dass die Unterscheidung zwischen B und D, die an sich nicht wesentlich ist, von der Wahl der Zahl f abhängt. Für diese muss eine der beiden Wurzeln der Kongruenz $xx \equiv -1$ genommen werden, und die beiden Sammlungen werden vertauscht, wenn man statt der einen Wurzel die andere wählt. Das gerade angegebene Schema zeigt, dass eine entsprechende Vertauschung mit einem Wechsel des Vorzeichens von b verbunden ist. Es lässt sich daher vorhersehen, dass zwischen dem Vorzeichen von b und der Zahl f ein Zusammenhang bestehen muss. Um ihn zu finden, bemerken wir zunächst: Bezeichnet μ eine nichtnegative ganze Zahl und nimmt man für z alle Zahlen $1, 2, 3 \ldots . p-1$, so gilt modulo p entweder $\Sigma z^\mu \equiv 0$ oder $\Sigma z^\mu \equiv -1$, je nachdem μ nicht durch $p-1$ teilbar oder dadurch teilbar ist. Der letzte Teil des Satzes folgt daraus, dass für einen Wert von μ, der durch $p-1$ teilbar ist, die Beziehung $z^\mu \equiv 1$ gilt; den ersten Teil beweisen wir folgendermaßen. Bezeichnet g eine primitive Wurzel, so stimmen alle z mit den kleinsten Resten aller g^y überein, wenn man für y alle Zahlen $0, 1, 2, 3 \ldots . p-2$ nimmt. Daher gilt $\Sigma z^\mu \equiv \Sigma g^{\mu.y}$. Nun ist

$$\Sigma g^{\mu y} = \frac{g^{\mu(p-1)} - 1}{g^\mu - 1}, \quad \text{also}$$
$$(g^\mu - 1)\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0$$

Für einen Wert von μ, der nicht durch $p-1$ teilbar ist, kann g^μ nicht 1 kongruent sein; das heißt, $g^\mu - 1$ kann nicht durch p teilbar sein. Daraus folgt $\Sigma z^\mu \equiv 0$. Q. E. D.

Entwickelt man nun die Potenz $(z^4+1)^{\frac{1}{4}(p-1)}$ nach dem Binomialtheorem, so ergibt der vorige Hilfssatz

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \text{ (mod. } p)$$

Die kleinsten Reste aller z^4 liefern aber sämtliche Zahlen in A, wobei jede viermal vorkommt. Unter den kleinsten Resten von z^4+1 haben wir daher

$$\begin{array}{ll} 4(00) & \text{zu } A \\ 4(01) & \text{zu } B \\ 4(02) & \text{zu } C \\ 4(03) & \text{zu } D \end{array}$$

zu diesen Klassen gehörige, und vier sind $= 0$ (nämlich für $z^4 \equiv p-1$). Aus den Kriterien für die Sammlungen A, B, C, D folgt

$$\begin{aligned} \Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv\ & 4(00) + 4f(01) \\ & - 4(02) - 4f(03) \end{aligned}$$

und damit

$$-2 \equiv 4(00) + 4f(01) - 4(02) - 4f(03)$$

oder, wenn man für $(00), (01)$ usw. die im vorigen Artikel gefundenen Werte einsetzt,

$$-2 \equiv -2a - 2 - 2bf$$

Wir schließen also, dass stets $a+bf \equiv 0$ gelten muss, oder nach Multiplikation mit f

$$b \equiv af$$

Diese Kongruenz bestimmt das Vorzeichen von b, wenn die Zahl f bereits gewählt ist, oder die Zahl f, wenn das Vorzeichen von b anderweitig vorgeschrieben wird.

20.

Nachdem wir unsere Aufgabe für Moduln der Form $8n+1$ vollständig gelöst haben, wenden wir uns dem anderen Fall zu, in dem p die Form $8n+5$ hat. Diesen können wir kürzer behandeln, da sich alle Überlegungen nur wenig von den vorangegangenen unterscheiden.

Da für einen solchen Modul -1 zur Klasse C gehört, liegen die Ergänzungen der Zahlen aus den Sammlungen A, B, C, D zur Summe p jeweils in den Klassen C, D, A, B. Daraus folgt leicht, dass

das Zeichen	die Anzahl der Lösungen der Kongruenz bezeichnet
(00)	$1+\alpha+\gamma \equiv 0$
(01)	$1+\alpha+\delta \equiv 0$
(02)	$1+\alpha+\alpha' \equiv 0$
(03)	$1+\alpha+\beta \equiv 0$
(10)	$1+\beta+\gamma \equiv 0$
(11)	$1+\beta+\delta \equiv 0$
(12)	$1+\beta+\alpha \equiv 0$
(13)	$1+\beta+\beta' \equiv 0$
(20)	$1+\gamma+\gamma' \equiv 0$
(21)	$1+\gamma+\delta \equiv 0$
(22)	$1+\gamma+\alpha \equiv 0$
(23)	$1+\gamma+\beta \equiv 0$
(30)	$1+\delta+\gamma \equiv 0$
(31)	$1+\delta+\delta' \equiv 0$
(32)	$1+\delta+\alpha \equiv 0$
(33)	$1+\delta+\beta \equiv 0$

Daraus erhalten wir sofort sechs Gleichungen:

$$(00) = (22), \quad (01) = (32), \quad (03) = (12),$$
$$(10) = (23), \quad (11) = (33), \quad (21) = (30)$$

Multiplizieren wir die Kongruenz $1+\alpha+\gamma \equiv 0$ mit einer Zahl γ' aus der Sammlung C, die so gewählt ist, dass $\gamma\gamma' \equiv 1$, und setzen wir für γ'' den kleinsten Rest des Produkts $\alpha\gamma'$, der offenbar ebenfalls zur Sammlung C gehört, so ergibt sich $\gamma' + \gamma'' + 1 \equiv 0$, woraus wir $(00) = (20)$ folgern.

Ganz ebenso erhalten wir die Gleichungen $(01) = (13)$, $(03) = (31)$, $(10) = (11) = (21)$.

Mit diesen elf Gleichungen können wir unsere sechzehn Unbekannten auf fünf zurückführen und das Schema S so darstellen:

$$\begin{array}{cccc} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m \end{array}$$

Außerdem haben wir die Gleichungen

$$\begin{aligned} (00) + (01) + (02) + (03) &= 2n + 1 \\ (10) + (11) + (12) + (13) &= 2n + 1 \\ (20) + (21) + (22) + (23) &= 2n \\ (30) + (31) + (32) + (33) &= 2n + 1 \end{aligned}$$

oder, mit den eben eingeführten Bezeichnungen, diese drei (I):

$$\begin{aligned} h + i + k + l &= 2n + 1 \\ 2m + i + l &= 2n + 1 \\ h + m &= n \end{aligned}$$

Mit ihrer Hilfe können wir unsere Unbekannten somit bereits auf zwei zurückführen.

Die übrigen Gleichungen leiten wir aus der Anzahl der Lösungen der Kongruenz $1 + \alpha + \beta + \gamma \equiv 0$ her (auch hier bezeichnen α, β, γ unbestimmte Zahlen aus den Sammlungen A, B, C, jeweils in dieser Reihenfolge). Wir beachten *erstens*, dass $1 + \alpha$ jeweils h, i, k, l Zahlen aus A, B, C, D liefert und dass es für jeden gegebenen Wert von α in diesen vier Fällen jeweils m, l, i, m Lösungen gibt. Die Gesamtzahl der Lösungen ist daher

$$= hm + il + ik + lm$$

Zweitens liefert $1 + \beta$ jeweils m, m, l, i Zahlen aus A, B, C, D, und für jeden *gegebenen* Wert von β gibt es in diesen vier Fällen jeweils h, m, h, m Lösungen. Die Gesamtzahl der Lösungen ist daher

$$= hm + mm + hl + im$$

Daraus leiten wir die Gleichung

$$0 = mm + hl + im - il - ik - lm$$

her. Mit der aus (I) gewonnenen Gleichung $k = 2m - h$ wird daraus

$$0 = mm + hl + hi - il - im - lm$$

Aus den Gleichungen I haben wir außerdem $l + i = 1 + 2h$, also

$$2i = 1 + 2h + (i - l)$$
$$2l = 1 + 2h - (i - l)$$

Setzen wir diese Werte in die vorangegangene Gleichung ein, so ergibt sich

$$0 = 4mm - 4m - 1 - 8hm + 4hh + (i - l)^2$$

Ersetzen wir hier schließlich $4m$ durch $2(h + m) - 2(h - m)$ oder, nach der letzten Gleichung in I, durch $2n - 2(h - m)$, so erhalten wir

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (i - l)^2$$

und somit

$$8n + 5 = (4(h - m) + 1)^2 + 4(i - l)^2$$

Setzen wir also

$$4(h - m) + 1 = a, \quad 2i - 2l = b$$

so wird

$$p = aa + bb$$

Da auch in diesem Fall p nur auf eine einzige Weise in zwei Quadrate zerlegt werden kann, von denen eines gerade und das andere ungerade ist, sind aa und bb vollständig bestimmte Zahlen: Offenbar muss aa gleich dem ungeraden Quadrat und bb gleich dem geraden gesetzt werden. Außerdem ist das *Vorzeichen* von a so zu wählen, dass $a \equiv 1 \pmod 4$, und das Vorzeichen von b so, dass $b \equiv af \pmod p$, wie sich durch ganz ähnliche Überlegungen wie im vorangegangenen Artikel leicht beweisen lässt.

Damit werden die fünf Zahlen h, i, k, l, m durch a, b und n wie folgt bestimmt:

$$8h = 4n + a - 1$$
$$8i = 4n + a + 2b + 3$$
$$8k = 4n - 3a + 3$$
$$8l = 4n + a - 2b + 3$$
$$8m = 4n - a + 1$$

Bevorzugen wir Ausdrücke durch p, so lauten die Einträge des Schemas S, mit 16 multipliziert:

$p + 2a - 7$	$p + 2a + 4b + 1$	$p - 2a + 1$	$p + 2a - 4b + 1$
$p - 2a - 3$	$p - 2a - 3$	$p + 2a - 4b + 1$	$p + 2a + 4b + 1$
$p + 2a - 7$	$p - 2a - 3$	$p + 2a - 7$	$p - 2a - 3$
$p - 2a - 3$	$p + 2a - 4b + 1$	$p + 2a + 4b + 1$	$p - 2a - 3$

21.

Nachdem wir unsere Aufgabe gelöst haben, kehren wir zur Hauptuntersuchung zurück und bestimmen nun vollständig die Sammlung, zu der die Zahl 2 gehört.

I. Hat p die Form $8n+1$, so wissen wir bereits, dass die Zahl 2 entweder in der Sammlung A oder in der Sammlung C liegt. Im ersten Fall sieht man leicht, dass auch die Zahlen $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ zu A gehören, im zweiten dagegen zu C. Nun beachten wir, dass, wenn α und $\alpha+1$ aufeinanderfolgende Zahlen der Sammlung A sind, auch $p-\alpha-1$, $p-\alpha$ solche Zahlen sind. Gleichbedeutend damit sind Zahlen der Sammlung A, auf die eine Zahl derselben Sammlung folgt, stets einander paarweise zugeordnet (α und $p-1-\alpha$). Ihre Anzahl, (00), ist daher immer gerade, sofern nicht eine Zahl sich selbst zugeordnet ist, das heißt, sofern nicht $\frac{1}{2}(p-1)$ zu A gehört; in diesem Fall ist ihre Anzahl ungerade. Daraus folgern wir, dass (00) ungerade ist, wenn 2 zur Sammlung A gehört, und gerade, wenn 2 zu C gehört. Wir haben aber

$$16(00) = aa + bb - 6a - 11$$

oder, wenn wir $a = 4q+1$, $b = 4r$ setzen (siehe Artikel 14),

$$(00) = qq - q + rr - 1$$

Da $qq-q$ offenbar stets gerade ist, ist (00) ungerade oder gerade, je nachdem, ob r gerade oder ungerade ist. Somit gehört 2 zu A oder zu C, je nachdem, ob b die Form $8m$ oder die Form $8m+4$ hat. Dies ist genau der Satz, den wir in Artikel 14 durch induktive Untersuchung gefunden haben.

II. Den anderen Fall, in dem p die Form $8n+5$ hat, können wir ebenso vollständig behandeln. Die Zahl 2 gehört hier entweder zu B oder zu D. Man sieht leicht, dass im ersten Fall $\frac{1}{2}(p-1)$ zu B und $\frac{1}{2}(p+1)$ zu D gehört, im zweiten dagegen $\frac{1}{2}(p-1)$ zu D und $\frac{1}{2}(p+1)$ zu B. Nun beachten wir: Ist β eine Zahl aus B, auf die eine Zahl aus D folgt, so liegt auch $p-\beta-1$ in B und $p-\beta$ in D. Zahlen mit dieser Eigenschaft sind also stets paarweise einander zugeordnet. Ihre Anzahl, (13), ist daher gerade, außer wenn eine von ihnen sich selbst zugeordnet ist, das heißt, wenn $\frac{1}{2}(p-1)$ zu B und $\frac{1}{2}(p+1)$ zu D gehört; dann ist (13) ungerade. Daraus folgern wir, dass (13) gerade ist, wenn 2 zu D gehört, und ungerade, wenn 2 zu B gehört. Wir haben aber

$$16(13) = aa + bb + 2a + 4b + 1$$

oder, wenn wir $a = 4q+1$, $b = 4r+2$ setzen,

$$(13) = qq + q + rr + 2r + 1$$

Somit ist (13) ungerade, wenn r gerade ist; umgekehrt ist (13) gerade, wenn r ungerade ist. Daraus folgern wir, dass 2 zu B gehört, wenn b die Form $8m+2$ hat, und zu D, wenn b die Form $8m+6$ hat.

Das Ergebnis dieser Untersuchungen lässt sich so aussprechen:

Die Zahl 2 *gehört zur Sammlung* A, B, C *oder* D*, je nachdem, ob die Zahl* $\frac{1}{2}b$ *die Form* $4m$*,* $4m+1$*,* $4m+2$ *oder* $4m+3$ *hat.*

22.

In den *Disquisitiones Arithmeticae* haben wir die allgemeine Theorie der Kreisteilung und der Lösung der Gleichung $x^p - 1 = 0$ dargelegt. Unter anderem haben wir gezeigt, dass, wenn μ ein Teiler der Zahl $p-1$ ist, die Funktion $\frac{x^p-1}{x-1}$ in μ Faktoren vom Grad $\frac{p-1}{\mu}$ mithilfe einer Hilfsgleichung vom Grad μ zerlegt werden kann. Neben der allgemeinen Theorie dieser Zerlegung haben wir in jenem Werk die besonderen Fälle $\mu = 2$ oder $\mu = 3$ in den Artikeln 356–358 gesondert betrachtet und gezeigt, wie man die Hilfsgleichung a priori angeben kann, also ohne das Schema der kleinsten Reste der Potenzen einer primitiven Wurzel zum Modul p aufzustellen. Auch ohne unseren Hinweis werden aufmerksame Leser den sehr engen Zusammenhang zwischen dem nächsten Fall dieser Theorie, nämlich $\mu = 4$, und den hier in den Artikeln 15–20 entwickelten Untersuchungen leicht erkennen. Mit ihrer Hilfe lässt sich auch dieser Fall ohne Schwierigkeit vollständig behandeln. Doch behalten wir uns diese Behandlung für eine andere Gelegenheit vor. Deshalb haben wir es vorgezogen, die Untersuchung in der vorliegenden Abhandlung in rein arithmetischer Form durchzuführen, ohne die Theorie der Gleichung $x^p - 1 = 0$ irgendwie einzubeziehen. Stattdessen fügen wir als abschließende Zugabe noch einige neue, rein arithmetische Sätze hinzu, die mit dem bisher behandelten Gegenstand sehr eng zusammenhängen.

23.

Entwickelt man die Potenz $(x^4+1)^{\frac{1}{2}(p-1)}$ nach dem Binomialtheorem, so treten drei Glieder auf, in denen der Exponent von x durch $p-1$ teilbar ist, nämlich

$$x^{2(p-1)}, \quad Px^{p-1} \quad \text{und } 1$$

wobei P den mittleren Koeffizienten

$$\frac{\frac{1}{2}(p-1)\,.\,\frac{1}{2}(p-3)\,.\,\frac{1}{2}(p-5)\,.\,\ldots\,.\,\frac{1}{4}(p+3)}{1\,.\,2\,.\,3\,.\,\ldots\,.\,\frac{1}{4}(p-1)}$$

bezeichnet. Setzen wir also für x der Reihe nach die Zahlen $1, 2, 3 \ldots p-1$ ein, so erhalten wir nach dem Hilfssatz in Artikel 19

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2 - P$$

Beachten wir aber das in Artikel 19 Dargelegte und außerdem, dass die Zahlen der Sammlungen A, B, C, D, zur Potenz mit dem Exponenten $\frac{1}{2}(p-1)$ erhoben, modulo p jeweils zu den Zahlen $+1, -1, +1, -1$ kongruent sind, so sehen wir leicht, dass

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv 4(00) - 4(01) + 4(02) - 4(03)$$

und somit nach den Schemata am Ende der Artikel 18, 20

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2a - 2$$

gilt. Der Vergleich dieser beiden Werte liefert einen besonders eleganten Satz: Wir haben

$$P \equiv 2a \pmod{p}$$

Bezeichnen wir die vier Produkte

$$\begin{array}{l} 1\,.\,2\,.\,3\,.\,\ldots\,.\,\frac{1}{4}(p-1) \\ \frac{1}{4}(p+3)\,.\,\frac{1}{4}(p+7)\,.\,\frac{1}{4}(p+11)\,.\,\ldots\,.\,\frac{1}{2}(p-1) \\ \frac{1}{2}(p+1)\,.\,\frac{1}{2}(p+3)\,.\,\frac{1}{2}(p+5)\,.\,\ldots\,.\,\frac{3}{4}(p-1) \\ \frac{1}{4}(3p+1)\,.\,\frac{1}{4}(3p+5)\,.\,\frac{1}{4}(3p+9)\,.\,\ldots\,.\,(p-1) \end{array}$$

jeweils mit q, r, s, t, so lässt sich der vorangegangene Satz als

$$2a \equiv \frac{r}{q} \pmod{p}$$

schreiben.

Da jeder Faktor von q seine Ergänzung zu p in t hat, gilt $q \equiv t \pmod{p}$, wenn die Anzahl der Faktoren gerade ist, also wenn p die Form $8m+1$ hat, dagegen $q \equiv -t$, wenn die Anzahl der Faktoren ungerade ist oder p die Form $8m+5$ hat. Ebenso gilt im ersten Fall $r \equiv s$, im zweiten $r \equiv -s$. In beiden Fällen gilt $qr \equiv st$, und da bekanntlich $qrst \equiv -1$, gilt $qqrr \equiv -1$, und somit $qr \equiv \pm f \pmod{p}$. Verbinden wir diese Kongruenz mit dem eben gefundenen Satz, so erhalten wir $rr \equiv \pm 2af$ und daher nach den Artikeln 19, 20

$$2b \equiv \pm rr \pmod{p}^{*)}$$

Es ist sehr bemerkenswert, dass sich die Zerlegung der Zahl p in zwei Quadrate durch völlig direkte Rechenoperationen finden lässt: Die Wurzel des ungeraden Quadrats ist der absolut kleinste Rest von $\frac{r}{2q}$, die Wurzel des geraden Quadrats dagegen der absolut kleinste Rest von $\frac{1}{2}rr$ zum Modul p. Den Ausdruck $\frac{r}{2q}$, der für $p = 5$ den Wert $= 1$ hat, kann man für größere Werte von p auch so schreiben:

$$\frac{6 \,.\, 10 \,.\, 14 \,.\, 18 \,.\, \ldots \,.\, (p-3)}{2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, \ldots \,.\, \frac{1}{4}(p-1)}$$

Da wir aber außerdem wissen, mit welchem Vorzeichen diese Formel die Wurzel des ungeraden Quadrats liefert, nämlich mit demjenigen, durch das sie stets die Form $4m+1$ hat, verdient es besondere Aufmerksamkeit, dass bisher kein ähnliches allgemeines Kriterium für das Vorzeichen der Wurzel des geraden Quadrats gefunden werden konnte. Wer ein solches findet und uns mitteilt, dem werden wir sehr dankbar sein. Einstweilen erschien es angebracht, hier die Werte der Zahlen a, b, f anzufügen, die sich für Werte von p unter 200 aus den kleinsten Resten der Ausdrücke $\frac{r}{2q}$, $\frac{1}{2}rr$, qr ergeben.

*) und $\{(a \mp b)q\}^2 \equiv a \equiv \left(\frac{r-qrr}{2}\right)^2$

p	a	b	f
5	+1	+2	2
13	−3	−2	5
17	+1	−4	13
29	+5	+2	12
37	+1	−6	31
41	+5	+4	9
53	−7	−2	23
61	+5	−6	11
73	−3	−8	27
89	+5	−8	34
97	+9	+4	22
101	+1	−10	91
109	−3	+10	33
113	−7	+8	15
137	−11	+4	37
149	−7	−10	44
157	−11	−6	129
173	+13	+2	80
181	+9	+10	162
193	−7	+12	81
197	+1	−14	183

THEORIE

DER BIQUADRATISCHEN RESTE

ZWEITE ABHANDLUNG

VON

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT AM 15. APRIL 1831 VORGELEGT.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VII.
Göttingen MDCCCXXXII.

THEORIE DER BIQUADRATISCHEN RESTE.

ZWEITE ABHANDLUNG.

24.

In der ersten Abhandlung ist alles, was zur biquadratischen Klassifikation der Zahl $+2$ erforderlich ist, vollständig behandelt worden. Wir denken uns nämlich alle durch den Modul p (der als Primzahl der Form $4n+1$ vorausgesetzt wird) nicht teilbaren Zahlen auf vier Sammlungen A, B, C, D verteilt, je nachdem sie zur Potenz mit dem Exponenten $\frac{1}{4}(p-1)$ erhoben modulo p zu $+1$, $+f$, -1, $-f$ kongruent werden; dabei bezeichnet f eine der beiden Wurzeln der Kongruenz $ff \equiv -1 \pmod{p}$. Wir haben gefunden, dass die Entscheidung, welcher Sammlung die Zahl $+2$ zuzurechnen ist, von der Zerlegung der Zahl p in zwei Quadrate abhängt: Setzt man $p = aa + bb$, wobei aa das ungerade und bb das gerade Quadrat bezeichnet, und nimmt man ferner an, dass die *Vorzeichen* von a, b so gewählt sind, dass $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$, so muss die Zahl $+2$ zur Sammlung A, B, C, D gehören, je nachdem $\frac{1}{2}b$ die Form $4n$, $4n+1$, $4n+2$, $4n+3$ hat.

Daraus folgt auch unmittelbar eine Regel zur Klassifikation der Zahl -2. Da -1 zur Klasse A gehört, wenn $\frac{1}{2}b$ gerade ist, im ungeraden Fall aber zur Klasse C, gehört nach dem Satz in Artikel 7 die Zahl -2 zur Klasse A, B, C, D, je nachdem $\frac{1}{2}b$ die Form $4n$, $4n+3$, $4n+2$, $4n+1$ hat.

Diese Sätze lassen sich auch folgendermaßen ausdrücken:

Es gehört	$+2$	-2
zur Sammlung	wenn b modulo 8 kongruent ist zu	
A	0	0
B	$2a$	$6a$
C	$4a$	$4a$
D	$6a$	$2a$

Man sieht leicht, dass die so ausgesprochenen Sätze nicht mehr von der Bedingung $a \equiv 1 \pmod{4}$ abhängen, sondern auch dann gelten, wenn $a \equiv 3 \pmod{4}$, sofern die andere Bedingung $af \equiv b \pmod{p}$ erhalten bleibt.

Ebenso leicht sieht man, dass sich der Inhalt dieser Sätze elegant in einer einzigen Formel zusammenfassen lässt, nämlich:

Werden a und b positiv genommen, so gilt stets

$$b^{\frac{1}{2}ab} \equiv a^{\frac{1}{2}ab}\, 2^{\frac{1}{4}(p-1)} \pmod{p}$$

25.

Sehen wir nun, wie weit die induktive Untersuchung auf die Klassifikation der Zahl 3 hinweist. Setzt man die Tabelle in Artikel 11 weiter fort (wobei stets die kleinste primitive Wurzel genommen wird), so zeigt sie, dass +3 gehört

zur Sammlung

A für			B für			C für			D für		
p	a	b	p	a	b	p	a	b	p	a	b
13	−3	+2	17	+1	−4	37	+1	−6	5	+1	+2
109	−3	+10	29	+5	+2	61	+5	−6	41	+5	−4
181	+9	+10	53	−7	+2	73	−3	−8	149	−7	+10
193	−7	−12	89	+5	−8	97	+9	+4	173	+13	+2
229	−15	+2	101	+1	+10	157	−11	−6			
277	+9	+14	113	−7	−8	241	−15	−4			
			137	−11	−4						
			197	+1	−14						
			233	+13	+8						
			257	+1	−16						
			269	+13	+10						
			281	+5	+16						
			293	+17	+2						

Zumindest auf den ersten Blick erkennen wir keinen einfachen Zusammenhang zwischen den Werten der Zahlen a, b, denen dieselbe Sammlung entspricht. Bedenken wir aber, dass sich eine entsprechende Entscheidung in der Theorie der quadratischen Reste für die Zahl −3 durch eine einfachere Regel treffen lässt als für die Zahl +3, so besteht die Hoffnung auf einen ebenso günstigen Erfolg in der Theorie der biquadratischen Reste. Wir finden, dass −3 zur Sammlung gehört

A für			B für			C für			D für		
p	a	b	p	a	b	p	a	b	p	a	b
37	+1	−6	5	+1	+2	13	−3	+2	29	+5	+2
61	+5	−6	17	+1	−4	73	−3	−8	41	+5	−4
157	−11	−6	89	+5	−8	97	+9	+4	53	−7	+2
193	−7	−12	113	−7	−8	109	−3	+10	101	+1	+10
			137	−11	−4	181	+9	+10	197	+1	−14
			149	−7	+10	229	−15	+2	269	+13	+10
			173	+13	+2	241	−15	−4	293	+17	+2
			233	+13	+8	277	+9	+14			
			257	+1	−16						
			281	+5	+16						

Hier zeigt sich die induktiv gefundene Regel unmittelbar. Die Zahl -3 gehört nämlich zur Sammlung

A, wenn b durch 3 teilbar ist, d. h. $b \equiv 0 \pmod 3$
B, wenn $a + b$ durch 3 teilbar ist, d. h. $b \equiv 2a \pmod 3$
C, wenn a durch 3 teilbar ist, d. h. $a \equiv 0 \pmod 3$
D, wenn $a - b$ durch 3 teilbar ist, d. h. $b \equiv a \pmod 3$

26.

Wir finden, dass die Zahl $+5$ der folgenden Sammlung zuzurechnen ist:

A für $p =$ 101, 109, 149, 181, 269
B für $p =$ 13, 17, 73, 97, 157, 193, 197, 233, 277, 293
C für $p =$ 29, 41, 61, 89, 229, 241, 281
D für $p =$ 37, 53, 113, 137, 173, 257

Betrachten wir die Werte der Zahlen a, b, die den einzelnen p entsprechen, so erkennen wir die Regel hier ebenso leicht wie bei der Klassifikation der Zahl -3. Wir gelangen nämlich zur Sammlung

A, wenn $b \equiv 0 \pmod 5$
B, wenn $b \equiv a$
C, wenn $a \equiv 0$
D, wenn $b \equiv 4a$

Offenbar erfassen diese Regeln alle Fälle, denn für $b \equiv 2a$ oder $b \equiv 3a \pmod 5$ wäre $aa + bb \equiv 0$, Q. E. A., da nach Voraussetzung p eine von 5 verschiedene Primzahl ist.

27.

Ebenso weist die induktive Untersuchung, auf die Zahlen -7, -11, $+13$, $+17$, -19, -23 angewandt und hinreichend weit fortgesetzt, auf folgende Regeln hin:

Für die Zahl -7

A	$a \equiv 0$, oder $b \equiv 0 \pmod 7$
B	$b \equiv 4a$, oder $b \equiv 5a$
C	$b \equiv a$, oder $b \equiv 6a$
D	$b \equiv 2a$, oder $b \equiv 3a$

Für die Zahl -11.

A	$b \equiv 0$, $5a$, oder $6a \pmod{11}$
B	$b \equiv a$, $3a$ oder $4a$
C	$a \equiv 0$, oder $b \equiv 2a$ oder $9a$
D	$b \equiv 7a$, $8a$ oder $10a$

Für die Zahl +13.

A	$b \equiv 0,\ 4a,\ 9a$ (mod. 13)
B	$b \equiv 6a,\ 11a,\ 12a$
C	$a \equiv 0;\ b \equiv 3a,\ 10a$
D	$b \equiv a,\ 2a,\ 7a$

Für die Zahl +17.

A	$a \equiv 0;\ b \equiv 0,\ a,\ 16a$ (mod. 17)
B	$b \equiv 2a,\ 6a,\ 8a,\ 14a$
C	$b \equiv 5a,\ 7a,\ 10a,\ 12a$
D	$b \equiv 3a,\ 9a,\ 11a,\ 15a$

Für die Zahl −19.

A	$b \equiv 0,\ 2a,\ 5a,\ 14a,\ 17a$ (mod. 19)
B	$b \equiv 3a,\ 7a,\ 11a,\ 13a,\ 18a$
C	$a \equiv 0;\ b \equiv 4a,\ 9a,\ 10a,\ 15a$
D	$b \equiv a,\ 6a,\ 8a,\ 12a,\ 16a$

Für die Zahl −23.

A	$a \equiv 0;\ b \equiv 0,\ 7a,\ 10a,\ 13a,\ 16a$ (mod. 23)
B	$b \equiv 2a,\ 3a,\ 4a,\ 11a,\ 15a,\ 17a$
C	$b \equiv a,\ 5a,\ 9a,\ 14a,\ 18a,\ 22a$
D	$b \equiv 6a,\ 8a,\ 12a,\ 19a,\ 20a,\ 21a$

28.

Die so durch induktive Untersuchung gewonnenen besonderen Sätze bestätigen sich, soweit diese Untersuchung fortgesetzt wird, und zeigen eine besonders schöne Gestalt der Kriterien. Vergleicht man sie aber miteinander, um allgemeine Schlüsse daraus zu ziehen, so bieten sich sogleich die folgenden Beobachtungen dar.

Die Kriterien dafür, welcher Sammlung die Primzahl $\pm q$ zuzurechnen ist (mit dem oberen oder unteren Vorzeichen, je nachdem q die Form $4n + 1$ oder $4n + 3$ hat), hängen von den Formen der Zahlen a, b ab, wenn man diese bezüglich des Moduls q miteinander vergleicht. Es gilt nämlich:

I. Ist $a \equiv 0 \pmod{q}$, so gehört $\pm q$ zu einer bestimmten Sammlung, und zwar zu A für $q = 7,\ 17,\ 23$ und zu C für $q = 3,\ 11,\ 13,\ 19$. Daraus entsteht die Vermutung, dass der erste Fall allgemein gilt, wenn q die Form $8n \pm 1$ hat, der zweite dagegen, wenn q die Form $8n \pm 3$ hat. Übrigens sind die Sammlungen B und D bereits ohne induktive Untersuchung ausgeschlossen, wenn der Wert von a durch q teilbar ist. Dann gilt $p \equiv bb \pmod{q}$, das heißt, p ist ein quadratischer Rest von q, und daher muss nach dem Fundamentalsatz $\pm q$ ein quadratischer Rest von p sein.

II. Ist dagegen a nicht durch q teilbar, so hängt das Kriterium vom Wert des Ausdrucks $\frac{b}{a} \pmod{q}$ ab. Dieser Ausdruck lässt zwar q verschiedene Werte zu, nämlich $0,\ 1,\ 2,\ 3 \ldots . q-1$; hat aber q die Form $4n+1$, so müssen die beiden Werte des Ausdrucks $\sqrt{-1} \pmod{q}$ ausgeschlossen werden. Diese können offenbar keine Werte des Ausdrucks $\frac{b}{a} \pmod{q}$ sein, da $p = aa + bb$ stets als eine von q verschiedene Primzahl vorausgesetzt wird. Somit ist die Anzahl der zulässigen Werte des Ausdrucks $\frac{b}{a} \pmod{q} = q - 2$ für $q \equiv 1 \pmod{4}$, während sie $= q$ für $q \equiv 3 \pmod{4}$ bleibt.

Diese Werte verteilen sich nun auf vier Klassen: Einige, die wir unbestimmt mit α bezeichnen, entsprechen der Sammlung A, andere, mit β bezeichnet, der Sammlung B, andere, γ, der Sammlung C, und schließlich die übrigen, δ, der Sammlung D. Die Zahl $\pm q$ ist also der Sammlung A, B, C, D zuzurechnen, je nachdem $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, $b \equiv \delta a \pmod{q}$ gilt.

Doch das *Gesetz* dieser Verteilung scheint tiefer verborgen, obwohl einige allgemeine Eigenschaften leicht zu erkennen sind. Die Anzahl der Werte ist in drei Klassen gleich, nämlich $= \frac{1}{4}(q-1)$ oder $\frac{1}{4}(q+1)$, während sie in einer (und zwar in derselben, die der Sammlung mit dem Kriterium $a \equiv 0$ entspricht) um eins kleiner ist. Dadurch wird die Gesamtzahl der verschiedenen Kriterien für jede einzelne Sammlung gleich, nämlich $= \frac{1}{4}(q-1)$ oder $\frac{1}{4}(q+1)$. Ferner bemerken wir, dass 0 stets in der ersten Klasse (unter den α) vorkommt und dass die Ergänzungen der Zahlen $\alpha, \beta, \gamma, \delta$ zu q, also $q-\alpha$, $q-\beta$, $q-\gamma$, $q-\delta$, jeweils in der ersten, vierten, dritten und zweiten Klasse liegen. Schließlich sehen wir, dass die Werte der Ausdrücke $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta} \pmod{q}$ zur ersten, vierten, dritten und zweiten Klasse gehören, wenn das Kriterium $a \equiv 0$ der Sammlung A entspricht, dagegen jeweils zur dritten, zweiten, ersten und vierten Klasse, wenn sich das Kriterium $a \equiv 0$ auf die Sammlung C bezieht. Doch darauf beschränkt sich ungefähr, was sich durch induktive Untersuchung erreichen lässt, sofern wir uns nicht allzu kühn anmaßen wollen, das vorwegzunehmen, was später aus den eigentlichen Quellen geschöpft werden wird.

29.

Bevor wir weitergehen, ist zu bemerken, dass die Kriterien für Primzahlen (positiv genommen, wenn sie die Form $4n + 1$ haben, negativ, wenn sie die Form $4n + 3$ haben) zur Entscheidung für alle übrigen Zahlen ausreichen, sofern man den Satz aus Artikel 7 und die Kriterien für -1 und ± 2 hinzunimmt.

Sucht man zum Beispiel Kriterien für die Zahl $+3$, so gelten die in Artikel 25 angegebenen Kriterien, die sich auf -3 beziehen, auch für $+3$, wenn $\frac{1}{2}b$ gerade ist. Dagegen sind die Sammlungen A, B, C, D mit den Sammlungen C, D, A, B zu vertauschen, wenn $\frac{1}{2}b$ ungerade ist. Daraus ergeben sich folgende Regeln:

$+3$ gehört

zur Sammlung	wenn
A	$b \equiv 0 \pmod{12}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 2 \pmod 4$
B	$b \equiv 8a$ oder $10a \pmod{12}$
C	$b \equiv 6a \pmod{12}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 4$
D	$b \equiv 2a$ oder $4a \pmod{12}$

Ebenso erhält man die Kriterien für ± 6 durch Verbindung der Kriterien für ∓ 2 und -3, nämlich:

$+6$ gehört

zur Sammlung	wenn
A	$b \equiv 0,\quad 2a, 22a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 4a \pmod 8$
B	$b \equiv 4a,\quad 6a,\quad 8a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 2a \pmod 8$
C	$b \equiv 10a, 12a, 14a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 8$
D	$b \equiv 16a, 18a, 20a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 6a \pmod 8$

-6 dagegen gehört

zur Sammlung	wenn
A	$b \equiv 0,\quad 10a, 14a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 4a \pmod 8$
B	$b \equiv 4a,\quad 8a, 18a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 6a \pmod 8$
C	$b \equiv 2a, 12a, 22a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 8$
D	$b \equiv 6a, 16a, 20a \pmod{24}$; oder zugleich $a \equiv 0 \pmod 3,\ b \equiv 2a \pmod 8$

Auf dieselbe Weise werden die Kriterien für die Zahl $+21$ aus den Kriterien für -3 und -7 zusammengestellt; die Kriterien für -105 aus denen für -1, -3, $+5$, -7 usw.

30.

Die induktive Untersuchung eröffnet somit eine überaus reiche Ernte besonderer Sätze, die mit dem Satz für die Zahl 2 verwandt sind. Doch ein gemeinsames Band fehlt, strenge Beweise fehlen, da die Methode, mit der wir in der ersten Abhandlung die Behandlung der Zahl 2 abgeschlossen haben, keine weitere Anwendung zulässt. Es gibt zwar verschiedene Methoden, mit denen sich Beweise für einzelne Fälle gewinnen ließen, insbesondere für diejenigen, die die Verteilung der quadratischen Reste auf die Sammlungen A, C betreffen. Wir halten uns jedoch nicht bei ihnen auf, da eine allgemeine, *alle* Fälle umfassende Theorie unser Ziel sein muss. Nachdem wir im Jahr 1805 begonnen hatten, dieser Frage unsere Überlegungen zu widmen, gelangten wir bald zu der Überzeugung, dass die eigentliche Quelle der allgemeinen Theorie in einer Erweiterung des Bereichs der Arithmetik zu suchen sei, wie wir bereits in Artikel 1 angedeutet haben.

Während sich die höhere Arithmetik bei den bisher behandelten Fragen allein mit reellen ganzen Zahlen befasst, erstrahlen die Sätze über biquadratische Reste erst dann in ihrer ganzen Einfachheit und eigentlichen Schönheit, wenn der Bereich der Arithmetik auf *imaginäre* Größen ausgedehnt wird. Ohne Einschränkung bilden dann Zahlen der Form $a + bi$ ihren Gegenstand, wobei i wie üblich die imaginäre Größe $\sqrt{-1}$ bezeichnet und a, b uneingeschränkt alle reellen ganzen Zahlen zwischen $-\infty$ und $+\infty$ durchlaufen. Solche Zahlen werden wir *komplexe ganze Zahlen* nennen; dabei werden die reellen Zahlen als eine darin enthaltene Art aufgefasst und den komplexen Zahlen nicht gegenübergestellt. Die vorliegende Abhandlung wird sowohl die elementare Lehre von den komplexen Zahlen als auch die ersten Anfänge der Theorie der biquadratischen Reste darstellen, deren allseitige Vollendung wir in einer nachfolgenden Fortsetzung unternehmen werden[*)].

[*)] Wenigstens beiläufig ist hier noch zu bemerken, dass sich der so bestimmte Bereich besonders für die Theorie der biquadratischen Reste eignet. Die Theorie der kubischen Reste muss entsprechend auf die Betrachtung von Zahlen der Form $a + bh$ gegründet werden, wobei h eine imaginäre Wurzel der Gleichung $h^3 - 1 = 0$ ist, etwa $h = -\frac{1}{2} + \sqrt{\frac{3}{4}} \, . \, i$; ebenso wird die Theorie der Reste höherer Potenzen die Einführung anderer imaginärer Größen erfordern.

31.

Zunächst führen wir einige Benennungen ein, die eine kürzere und klarere Darstellung ermöglichen.

Der Bereich der komplexen Zahlen $a + bi$ enthält

I. die reellen Zahlen, bei denen $b = 0$ gilt, und darunter je nach der Beschaffenheit von a

   1) die Null,

   2) die positiven Zahlen,

   3) die negativen Zahlen;

II. die imaginären Zahlen, bei denen b von null verschieden ist. Hier unterscheiden wir wiederum

   1) imaginäre Zahlen ohne reellen Teil, also solche, bei denen $a = 0$ gilt;

   2) imaginäre Zahlen mit reellem Teil, wobei b nicht null ist und auch $a = 0$ nicht gilt.

Die ersteren kann man, wenn man will, rein imaginäre Zahlen, die letzteren gemischt imaginäre Zahlen nennen.

In dieser Theorie verwenden wir vier Einheiten, $+1$, -1, $+i$, $-i$, die einfach positiv, negativ, positiv imaginär und negativ imaginär heißen sollen.

Die drei Produkte einer beliebigen komplexen Zahl mit -1, $+i$, $-i$ nennen wir ihre *Gefährten* oder *die ihr assoziierten Zahlen.* Mit Ausnahme der Null (die sich selbst assoziiert ist) sind also stets vier *verschiedene* Zahlen einander assoziiert.

Dagegen nennen wir die Zahl, die aus einer komplexen Zahl durch Vertauschung von i mit $-i$ entsteht, die zu ihr *konjugierte* Zahl. Unter den imaginären Zahlen sind demnach stets zwei *verschiedene* Zahlen konjugiert, während die reellen Zahlen sich selbst konjugiert sind, sofern man diese Benennung auf sie ausdehnen will.

Das Produkt einer komplexen Zahl mit der zu ihr konjugierten Zahl nennen wir die *Norm* jeder der beiden. Bei einer reellen Zahl ist daher ihr Quadrat als ihre Norm anzusehen.

Im Allgemeinen haben wir acht zusammenhängende Zahlen, nämlich

$$\begin{array}{r|r} a+bi & a-bi \\ -b+ai & -b-ai \\ -a-bi & -a+bi \\ b-ai & b+ai \end{array}$$

wobei wir zwei Gruppen von vier assoziierten Zahlen und vier Paare konjugierter Zahlen sehen; die gemeinsame Norm aller ist $aa+bb$. Die acht Zahlen reduzieren sich jedoch auf vier verschiedene, wenn entweder $a = \pm b$ oder für eine der beiden Zahlen $a, b = 0$ gilt.

Aus den angeführten Definitionen ergibt sich unmittelbar Folgendes:

Zum Produkt zweier komplexer Zahlen ist das Produkt der zu ihnen konjugierten Zahlen konjugiert.

Dasselbe gilt für ein Produkt aus mehr Faktoren sowie für Quotienten.

Die Norm des Produkts zweier komplexer Zahlen ist gleich dem Produkt ihrer Normen.

Auch dieser Satz erstreckt sich auf Produkte aus beliebig vielen Faktoren und auf Quotienten.

Die Norm jeder komplexen Zahl (mit Ausnahme der Null, die wir von nun an meist stillschweigend ausschließen) ist eine *positive* Zahl.

Ferner steht nichts im Wege, unsere Definitionen auf gebrochene oder sogar irrationale Werte von a, b auszudehnen; doch soll $a + bi$ nur dann eine komplexe ganze Zahl heißen, wenn *jede* der Zahlen a, b ganz ist, und nur dann rational, wenn *jede* der Zahlen a, b rational ist.

32.

Die Rechenregeln für komplexe Zahlen sind allgemein bekannt: Durch Einführung der Norm wird die Division auf die Multiplikation zurückgeführt, denn es gilt

$$\frac{a+bi}{c+di} = (a+bi) \,.\, \frac{c-di}{cc+dd} = \frac{ac+bd}{cc+dd} + \frac{bc-ad}{cc+dd} \,.\, i$$

Die Quadratwurzel wird mithilfe der Formel

$$\sqrt{(a+bi)} = \pm\left(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} + i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}}\right)$$

gezogen, wenn b positiv ist, oder mithilfe der Formel

$$\sqrt{(a+bi)} = \pm\left(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} - i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}}\right)$$

wenn b negativ ist. Beim Nutzen der Umformung der komplexen Größe $a+bi$ in $r(\cos\varphi + i\sin\varphi)$ zur Erleichterung der Rechnungen brauchen wir uns hier nicht aufzuhalten.

33.

Eine komplexe ganze Zahl, die sich in zwei von den Einheiten verschiedene Faktoren[*)] zerlegen lässt, nennen wir eine zusammengesetzte komplexe Zahl; eine Zahl, die keine solche Zerlegung in Faktoren zulässt, soll dagegen eine komplexe Primzahl heißen. Daraus folgt unmittelbar, dass jede zusammengesetzte reelle Zahl auch eine zusammengesetzte komplexe Zahl ist. Eine reelle Primzahl kann jedoch eine zusammengesetzte komplexe Zahl sein, und dies gilt für die Zahl 2 sowie für alle positiven reellen Primzahlen der Form $4n+1$ (mit Ausnahme der Zahl 1), da sich diese bekanntlich in zwei positive Quadrate zerlegen lassen. Zum Beispiel gilt $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$, $13 = (3+2i)(3-2i)$, $17 = (1+4i)(1-4i)$ usw.

Dagegen sind positive reelle Primzahlen der Form $4n+3$ stets komplexe Primzahlen. Wäre nämlich eine solche Zahl $q = (a+bi)(\alpha+\beta i)$, so wäre auch $q = (a-bi)(\alpha-\beta i)$ und daher $qq = (aa+bb)(\alpha\alpha+\beta\beta)$. Nun lässt sich aber qq nur auf eine einzige Weise in positive, die Einheit übersteigende Faktoren zerlegen, nämlich in $q \times q$. Daher müsste $q = aa+bb = \alpha\alpha+\beta\beta$ gelten, Q. E. A.; denn die Summe zweier Quadrate kann nicht die Form $4n+3$ haben.

Die negativen reellen Zahlen behalten offenbar dieselben Benennungen wie die positiven; dasselbe gilt für die rein imaginären Zahlen.

Es bleibt somit zu zeigen, wie man unter den gemischt imaginären Zahlen die zusammengesetzten von den Primzahlen unterscheidet. Dies geschieht durch den folgenden

Satz. *Jede gemischt imaginäre ganze Zahl $a+bi$ ist eine komplexe Primzahl oder eine zusammengesetzte Zahl, je nachdem, ob ihre Norm eine reelle Primzahl oder eine zusammengesetzte Zahl ist.*

Beweis. I. Da die Norm einer zusammengesetzten komplexen Zahl stets eine zusammengesetzte Zahl ist, muss eine komplexe Zahl, deren Norm eine reelle Primzahl ist, offenbar eine komplexe Primzahl sein. Q. E. P.

II. Ist aber die Norm $aa+bb$ zusammengesetzt, so sei p eine positive reelle Primzahl, die sie teilt. Nun sind zwei Fälle zu unterscheiden.

1) Hat p die Form $4n+3$, so kann bekanntlich $aa+bb$ nur dann durch p teilbar sein, wenn p beide Zahlen a, b teilt. Daher ist $a+bi$ eine zusammengesetzte Zahl.

[*)] Oder, was dasselbe ist, in solche, deren Normen größer als die Einheit sind.

2) Hat p nicht die Form $4n+3$, so lässt sich diese Zahl sicher in zwei Quadrate zerlegen. Wir setzen daher $p = \alpha\alpha + \beta\beta$. Da

$$(a\alpha + b\beta)(a\alpha - b\beta) = aa(\alpha\alpha + \beta\beta) - \beta\beta(aa + bb)$$

gilt und dieser Ausdruck somit durch p teilbar ist, muss p einen der Faktoren $a\alpha + b\beta$, $a\alpha - b\beta$ teilen. Da ferner

$$(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 = (a\alpha - b\beta)^2 + (b\alpha + a\beta)^2 = (aa + bb)(\alpha\alpha + \beta\beta)$$

gilt und dieser Ausdruck somit durch pp teilbar ist, muss im ersten Fall auch $b\alpha - a\beta$, im zweiten $b\alpha + a\beta$ durch p teilbar sein. Daher ist im ersten Fall

$$\frac{a+bi}{\alpha+\beta i} = \frac{a\alpha+b\beta}{p} + \frac{b\alpha-a\beta}{p} \,.\, i$$

eine komplexe ganze Zahl, im zweiten dagegen

$$\frac{a+bi}{\alpha-\beta i} = \frac{a\alpha-b\beta}{p} + \frac{b\alpha+a\beta}{p} \,.\, i$$

eine ganze Zahl. Da also die gegebene Zahl durch $\alpha + \beta i$ oder durch $\alpha - \beta i$ teilbar ist und die Norm des Quotienten $= \frac{aa+bb}{p}$ nach Voraussetzung von der Einheit verschieden ist, ist $a + bi$ offenbar in beiden Fällen eine zusammengesetzte komplexe Zahl. Q. E. S.

34.

Den gesamten Bereich der komplexen Primzahlen erschöpfen somit die folgenden vier Arten:

1) die vier Einheiten $1, +i, -1, -i$, die wir jedoch bei der Behandlung von Primzahlen meist stillschweigend als ausgeschlossen betrachten werden;

2) die Zahl $1 + i$ mit ihren drei assoziierten Zahlen $-1 + i$, $-1 - i$, $1 - i$;

3) die positiven reellen Primzahlen der Form $4n + 3$ mit jeweils drei assoziierten Zahlen;

4) die komplexen Zahlen, deren Normen reelle, die Einheit übersteigende Primzahlen der Form $4n + 1$ sind. Jeder gegebenen Norm dieser Art entsprechen stets acht komplexe Primzahlen und nicht mehr, da sich eine solche Norm nur auf eine einzige Weise in zwei Quadrate zerlegen lässt.

35.

Wie sich die reellen ganzen Zahlen in gerade und ungerade und die ersteren wiederum in durch vier teilbare Zahlen und in das Doppelte einer ungeraden Zahl einteilen, so ergibt sich unter den komplexen Zahlen eine ebenso wesentliche Unterscheidung. Sie sind nämlich

entweder durch $1 + i$ nicht teilbar, nämlich Zahlen $a + bi$, bei denen eine der beiden Zahlen a, b ungerade und die andere gerade ist;

oder durch $1+i$, aber nicht durch 2 teilbar, wenn beide Zahlen a, b ungerade sind;

oder durch 2 teilbar, wenn beide Zahlen a, b gerade sind.

Die Zahlen der ersten Klasse kann man passend *ungerade komplexe Zahlen*, die der zweiten *halbgerade*, die der dritten *gerade* nennen.

Ein Produkt aus mehreren komplexen Faktoren ist stets ungerade, wenn alle Faktoren ungerade sind; halbgerade, wenn ein Faktor halbgerade und die übrigen ungerade sind; dagegen gerade, wenn unter den Faktoren mindestens zwei halbgerade oder mindestens einer gerade ist.

Die Norm jeder ungeraden komplexen Zahl hat die Form $4n + 1$; die Norm einer halbgeraden Zahl hat die Form $8n + 2$; schließlich ist die Norm einer geraden Zahl das Produkt einer Zahl der Form $4n + 1$ mit der Zahl 4 oder einer höheren Potenz von zwei.

36.

Da die Beziehung zwischen vier assoziierten komplexen Zahlen der Beziehung zwischen zwei entgegengesetzten reellen Zahlen analog ist (also Zahlen, die dem absoluten Wert nach gleich und mit entgegengesetzten Vorzeichen versehen sind) und unter diesen gewöhnlich und mit Recht die positive als primär angesehen wird, entsteht die Frage, ob sich unter vier assoziierten komplexen Zahlen eine ähnliche Unterscheidung festlegen lässt und ob sie als nützlich anzusehen ist. Zur Entscheidung muss man bedenken, dass das Unterscheidungsprinzip so beschaffen sein muss, dass das Produkt zweier Zahlen, die unter ihren jeweiligen assoziierten Zahlen als primär gelten, stets unter seinen eigenen assoziierten Zahlen primär ist. Doch wir gelangen bald zu der Überzeugung, dass es ein solches Prinzip überhaupt nicht gibt, wenn die Unterscheidung nicht auf ganze Zahlen beschränkt wird; eine *nützliche* Unterscheidung wird sogar auf ungerade Zahlen zu beschränken sein. Für diese lässt sich das angestrebte Ziel aber auf zweierlei Weise erreichen. Nämlich:

I. Das Produkt zweier Zahlen $a+bi, a'+b'i$, bei denen a, a' die Form $4n+1$ haben und b, b' gerade sind, besitzt dieselbe Eigenschaft, sodass der reelle Teil $\equiv 1 \pmod 4$ und der imaginäre Teil gerade ist. Man sieht leicht, dass unter vier assoziierten ungeraden Zahlen nur eine diese Form hat.

II. Ist eine Zahl $a+bi$ so beschaffen, dass $a-1$ und b entweder beide durch vier teilbar oder beide das Doppelte einer ungeraden Zahl sind, so besitzt ihr Produkt mit einer komplexen Zahl derselben Form wieder dieselbe Form; und man sieht leicht, dass unter vier assoziierten ungeraden Zahlen nur eine diese Form hat.

Von diesen beiden annähernd gleich geeigneten Prinzipien werden wir das letztere wählen: Unter vier assoziierten ungeraden komplexen Zahlen betrachten wir diejenige als primär, die nach dem Modul $2+2i$ der positiven Einheit kongruent ist. So lassen sich mehrere bemerkenswerte Sätze kürzer aussprechen. Zum Beispiel sind die komplexen Primzahlen $-1+2i$, $-1-2i$, $+3+2i$, $+3-2i$, $+1+4i$, $+1-4i$ usw. primär, ebenso die reellen Zahlen -3, -7, -11, -19 usw., die offenbar stets mit negativem Vorzeichen zu nehmen sind. Die zu einer ungeraden primären komplexen Zahl konjugierte Zahl ist ebenfalls primär.

Für halbgerade und gerade Zahlen im Allgemeinen wäre eine ähnliche Unterscheidung zu willkürlich und zu wenig nützlich. Von den assoziierten Primzahlen $1+i$, $1-i$, $-1+i$, $-1-i$ können wir zwar eine vor den übrigen als primär auswählen; auf zusammengesetzte Zahlen werden wir eine solche Unterscheidung aber nicht ausdehnen.

37.

Sind unter den Faktoren einer zusammengesetzten komplexen Zahl solche, die selbst zusammengesetzt sind, und werden diese wiederum in ihre Faktoren zerlegt, so gelangt man offenbar schließlich zu Primfaktoren; das heißt, jede zusammengesetzte Zahl ist in Primfaktoren zerlegbar. Sind darunter solche, die nicht primär sind, so ersetzen wir jede durch das Produkt der assoziierten primären Zahl mit i, -1 oder $-i$. So lässt sich offenbar jede zusammengesetzte komplexe Zahl M auf die Form

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \dots .$$

bringen, wobei A, B, C usw. verschiedene primäre komplexe Primzahlen sind und $\mu = 0, 1, 2$ oder 3 ist. Für diese Zerlegung ergibt sich der Satz, dass sie nur auf eine einzige Weise möglich ist. Bei flüchtiger Betrachtung könnte dieser Satz zwar an sich selbstverständlich erscheinen, doch bedarf er jedenfalls eines Beweises. Den Weg dazu bereitet der folgende

Satz. *Das Produkt $M = A^{\alpha} B^{\beta} C^{\gamma} \dots$, in dem A, B, C usw. verschiedene primäre komplexe Primzahlen bezeichnen, kann durch keine primäre komplexe Primzahl teilbar sein, die nicht unter A, B, C usw. vorkommt.*

Beweis. Es sei P eine primäre komplexe Primzahl, die nicht unter A, B, C usw. enthalten ist, und es seien p, a, b, c usw. die Normen der Zahlen P, A, B, C usw. Daraus folgt leicht, dass die Norm von $M = a^{\alpha} b^{\beta} c^{\gamma}$ usw. ist. Diese Zahl müsste daher, wenn M durch P teilbar wäre, durch p teilbar sein. Da die

einzelnen Normen entweder reelle Primzahlen (aus der Folge $2, 5, 13, 17$ usw.) oder Quadrate reeller Primzahlen (aus der Folge $9, 49, 121$ usw.) sind, kann dies offenbar nur eintreten, wenn p mit einer der Normen a, b, c usw. identisch ist. Wir nehmen daher $p = a$ an. Da aber P, A nach Voraussetzung verschiedene primäre komplexe Primzahlen sind, sieht man leicht, dass diese Bedingungen nur dann zugleich bestehen können, wenn P, A konjugierte imaginäre komplexe Zahlen sind und somit $p = a$ eine ungerade reelle Primzahl ist (nicht das Quadrat einer Primzahl). Wir setzen daher $A = k + li$, $P = k - li$. Indem wir Begriff und Zeichen der Kongruenz auf komplexe ganze Zahlen ausdehnen, erhalten wir $A \equiv 2k \pmod{P}$, woraus leicht folgt:

$$M \equiv 2^\alpha k^\alpha B^\beta C^\gamma \ldots . \pmod{P}$$

Wird also M als durch P teilbar angenommen, so ist auch

$$2^\alpha k^\alpha B^\beta C^\gamma \ldots .$$

durch P teilbar und daher die Norm dieser Zahl, die

$$= 2^{2\alpha} k^{2\alpha} b^\beta c^\gamma \ldots .$$

ist, durch p teilbar. Da jedoch 2 und k sicher nicht durch p teilbar sind, folgt daraus, dass p mit einer der Zahlen b, c usw. identisch sein muss; sei zum Beispiel $p = b$. Daraus schließen wir aber, dass entweder $B = k + li$ oder $B = k - li$ gilt, das heißt entweder $B = A$ oder $B = P$, beides gegen die Voraussetzung.

Aus diesem Satz folgt der andere, dass die Zerlegung in Primfaktoren nur auf eine einzige Weise möglich ist, sehr leicht durch Schlüsse, die denjenigen völlig analog sind, die wir in den *Disquisitiones Arithmeticae* für reelle Zahlen verwendet haben (Artikel 16). Daher wäre es überflüssig, uns hier damit aufzuhalten.

38.

Wir gehen nun zur Kongruenz von Zahlen nach komplexen Moduln über. Zu Beginn dieser Untersuchung ist jedoch anzugeben, wie sich der Bereich der komplexen Größen anschaulich darstellen lässt.

Jede reelle Größe lässt sich durch eine Strecke auf einer nach beiden Seiten unendlichen Geraden ausdrücken, die von einem beliebigen Anfangspunkt aus genommen und nach einer beliebigen, als Einheit gewählten Strecke gemessen wird. Sie lässt sich daher durch den anderen Endpunkt darstellen, wobei die Punkte auf der einen Seite des Anfangspunktes positive, auf der anderen negative Größen darstellen. Ebenso lässt sich jede komplexe Größe durch einen Punkt in einer unendlichen Ebene darstellen, in der eine bestimmte Gerade den reellen Größen zugeordnet ist: die komplexe Größe $x + iy$ durch

den Punkt mit der Abszisse $= x$ und der Ordinate $= y$, wobei diese auf der einen Seite der Abszissenlinie positiv, auf der anderen negativ genommen wird. So kann man sagen, dass jede komplexe Größe den Unterschied zwischen der Lage des ihr zugeordneten Punktes und der Lage des Anfangspunktes misst. Die positive Einheit bezeichnet dabei eine beliebige festgelegte Verschiebung in einer beliebigen festgelegten Richtung, die negative Einheit eine gleich große Verschiebung in der entgegengesetzten Richtung und die imaginären Einheiten gleich große Verschiebungen in den beiden senkrechten seitlichen Richtungen.

Auf diese Weise wird die Metaphysik der Größen, die wir imaginär nennen, erheblich erhellt. Wird der Anfangspunkt mit (0) bezeichnet und werden zwei komplexe Größen m, m' den Punkten M, M' zugeordnet, deren Lage bezüglich (0) sie ausdrücken, so ist die Differenz $m - m'$ nichts anderes als die Lage des Punktes M bezüglich des Punktes M'. Stellt dagegen das Produkt mm' die Lage des Punktes N bezüglich (0) dar, so sieht man leicht, dass diese Lage durch die Lage des Punktes M bezüglich (0) ebenso bestimmt wird wie die Lage des Punktes M' durch die Lage des der positiven Einheit entsprechenden Punktes. Man kann daher passend sagen, dass die Lagen der den komplexen Größen mm' $m, m', 1$ entsprechenden Punkte eine *Proportion* bilden. Eine ausführlichere Behandlung behalten wir uns jedoch für eine andere Gelegenheit vor. Die Schwierigkeiten, in die man die Theorie der imaginären Größen verstrickt glaubt, sind großenteils aus ungeeigneten Benennungen entstanden (haben doch manche sogar den missklingenden Namen unmöglicher Größen gebraucht). Wären wir von den Begriffen ausgegangen, die zweidimensionale Mannigfaltigkeiten darbieten, wie sie in größter Reinheit in unseren Raumanschauungen erscheinen, und hätten wir die positiven Größen direkte, die negativen inverse und die imaginären seitliche Größen genannt, so wäre an die Stelle von Verwicklungen Einfachheit und an die Stelle von Dunkelheit Klarheit getreten.

39.

Das im vorigen Artikel Dargelegte bezieht sich auf stetige komplexe Größen. In der Arithmetik, die sich nur mit ganzen Zahlen befasst, wird das Bild der komplexen Zahlen ein System gleich weit voneinander entfernter Punkte sein, die auf gleich weit voneinander entfernten Geraden so angeordnet sind, dass sie die unendliche Ebene in unendlich viele gleiche Quadrate zerlegen. Alle durch eine gegebene komplexe Zahl $a + bi = m$ teilbaren Zahlen bilden ebenfalls unendlich viele Quadrate, mit den Seiten $= \sqrt{(aa + bb)}$ oder den Flächeninhalten $= aa + bb$. Die letzteren Quadrate sind gegen die ersteren geneigt, sofern keine der beiden Zahlen $a, b = 0$ ist. Jeder durch den Modul m nicht teilbaren Zahl entspricht ein Punkt entweder innerhalb eines solchen Quadrates oder auf einer zwei Quadraten gemeinsamen Seite; der letztere Fall kann jedoch nur eintreten, wenn a, b einen gemeinsamen Teiler haben. Ferner

ist klar, dass nach dem Modul m kongruente Zahlen in ihren Quadraten entsprechende Lagen einnehmen. Sammeln wir daher alle Zahlen innerhalb eines bestimmten Quadrates sowie alle, die etwa auf zwei einander nicht gegenüberliegenden Seiten liegen, und fügen schließlich eine durch m teilbare Zahl hinzu, so erhalten wir leicht ein vollständiges System inkongruenter Reste nach dem Modul m: Jede ganze Zahl muss einem von ihnen und nur einem einzigen kongruent sein. Es wäre auch nicht schwierig zu zeigen, dass die Anzahl dieser Reste der Norm des Moduls gleich ist, nämlich $= aa + bb$. Doch erscheint es ratsam, diesen sehr wichtigen Satz auf eine andere, rein arithmetische Weise zu beweisen.

40.

Satz. *Nach einem gegebenen komplexen Modul $m = a + bi$, dessen Norm $aa + bb = p$ ist und für den a, b teilerfremd sind, ist jede komplexe ganze Zahl einem Rest aus der Folge $0, 1, 2, 3 \ldots p - 1$ und nicht mehreren kongruent.*

Beweis. I. Es seien α, β ganze Zahlen mit $\alpha a + \beta b = 1$. Dann ist

$$i = \alpha b - \beta a + m(\beta + \alpha i)$$

Für eine gegebene komplexe ganze Zahl $A + Bi$ haben wir daher

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha B i)$$

Bezeichnen wir mit h den kleinsten positiven Rest der Zahl $A + (\alpha b - \beta a)B$ nach dem Modul p und setzen

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki)$$

so ist

$$A + Bi = h + m(\beta B + ak + (\alpha B - bk)i)$$

oder

$$A + Bi \equiv h (\text{mod. } m). \qquad \text{Q. E. P.}$$

II. Sind zwei reelle Zahlen h, h' derselben komplexen Zahl nach dem Modul m kongruent, so sind sie auch einander kongruent. Wir setzen daher $h - h' = m(c + di)$, woraus folgt:

$$(h - h')(a - bi) = p(c + di)$$

und somit

$$(h - h')a = pc, \quad (h - h')b = -pd$$

sowie wegen $a\alpha + b\beta = 1$

$$h - h' = p(c\alpha - d\beta), \text{ d. h. } h \equiv h' (\text{mod. } p)$$

Sind also h und h' verschieden, so können sie nicht beide zugleich in der Sammlung der Zahlen $0, 1, 2, 3 \ldots p - 1$ enthalten sein. Q. E. S.

41.

Satz. *Nach einem komplexen Modul* $m = .\,a+bi$, *dessen Norm* $aa+bb = p$ *ist und für den* a, b *nicht teilerfremd sind, sondern den größten gemeinsamen Teiler* λ *haben (den wir positiv genommen voraussetzen), ist jede komplexe Zahl einem Rest* $x+yi$ *kongruent, bei dem* x *eine der Zahlen* $0, 1, 2, 3 \ldots . \frac{p}{\lambda} - 1$ *und* y *eine der Zahlen* $0, 1, 2, 3 \ldots . \lambda - 1$ *ist, und zwar genau einem unter allen* p *Resten dieser Form.*

Beweis. I. Wählen wir ganze Zahlen α, β mit $\alpha a + \beta b = \lambda$, so ist $\lambda i = \alpha b - \beta a + m(\beta + \alpha i)$. Es sei nun $A + Bi$ eine gegebene komplexe Zahl, y der kleinste positive Rest von B nach dem Modul λ und x der kleinste positive Rest von $A + (\alpha b - \beta a) \,.\, \frac{B-y}{\lambda}$ nach dem Modul $\frac{p}{\lambda}$; wir setzen

$$A + (\alpha b - \beta a) \,.\, \frac{B-y}{\lambda} = x + \frac{p}{\lambda} \,.\, k$$

Dann ist

$$\begin{aligned} A + Bi - (x + yi) &= \frac{p}{\lambda} \,.\, k + (B-y)i - (\alpha b - \beta a)\frac{B-y}{\lambda} \\ &= \frac{p}{\lambda} \,.\, k + \frac{B-y}{\lambda} \,.\, m(\beta + \alpha i) \\ &= \left(\frac{a}{\lambda} - \frac{b}{\lambda} \,.\, i\right) km + \frac{B-y}{\lambda}(\beta + \alpha i)m \end{aligned}$$

also durch m teilbar, oder gleichbedeutend $A + Bi \equiv x + yi (\text{mod. } m)$ Q. E. P.

II. Wir nehmen an, dass nach dem Modul m derselben komplexen Zahl zwei Zahlen $x+yi, x'+y'i$ kongruent sind, die daher auch einander nach dem Modul m kongruent sind. Umso mehr sind sie nach dem Modul λ kongruent, also gilt $y \equiv y' (\text{mod.} \lambda)$. Werden daher beide y, y' als unter den Zahlen $0, 1, 2, 3 \ldots . \lambda - 1$ enthalten vorausgesetzt, so muss $y = y'$ gelten. Damit gilt aber auch $x \equiv x' (\text{mod. } m)$, das heißt, $x - x'$ ist durch m teilbar und folglich die ganze Zahl $\frac{x-x'}{\lambda}$ durch $\frac{a}{\lambda} + \frac{b}{\lambda} \,.\, i$, oder

$$\frac{x-x'}{\lambda} \equiv 0 \left(\text{mod.} \frac{a}{\lambda} + \frac{b}{\lambda} \,.\, i\right)$$

Da nun $\frac{a}{\lambda}, \frac{b}{\lambda}$ teilerfremd sind, folgt aus dem zweiten Teil des Satzes im vorigen Artikel, dass $\frac{x-x'}{\lambda}$ auch durch die Norm der Zahl $\frac{a}{\lambda} + \frac{b}{\lambda} \,.\, i$, also durch die Zahl $\frac{p}{\lambda\lambda}$, teilbar ist, und somit $x - x'$ durch $\frac{p}{\lambda}$. Werden also auch beide x, x' als in der Sammlung der Zahlen $0, 1, 2, 3 \ldots . \frac{p}{\lambda} - 1$ enthalten vorausgesetzt, so muss $x = x'$ gelten, oder die Reste $x + yi, x' + y'i$ sind identisch. Q. E. S.

Ferner ist offenbar auch der Fall hierher zu rechnen, in dem der Modul reell ist, also $b = 0$ und folglich $\lambda = \pm a$, sowie der Fall, in dem der Modul rein imaginär ist, also $a = 0$ und folglich $\lambda = \pm b$. In beiden Fällen gilt $\frac{p}{\lambda} = \lambda$.

42.

Ordnet man somit alle nach einem gegebenen Modul einander kongruenten komplexen Zahlen derselben Klasse und inkongruente Zahlen verschiedenen Klassen zu, so gibt es insgesamt p Klassen, die den ganzen Bereich der ganzen Zahlen erschöpfen, wobei p die Norm des Moduls bezeichnet. Eine Sammlung ebenso vieler Zahlen, aus jeder Klasse eine genommen, stellt ein vollständiges System inkongruenter Reste dar, wie wir es in den Artikeln 40, 41 angegeben haben. In jenem System beruhte die Wahl der ihre Klassen gleichsam vertretenden Reste auf dem Prinzip, in jeder Klasse einen Rest $x + yi$ zu wählen, für den y den kleinsten Wert hat, und unter allen mit demselben kleinsten Wert von y denjenigen, für den x den kleinsten Wert hat; dabei sind negative Werte sowohl für x als auch für y ausgeschlossen. Für andere Zwecke wird man jedoch andere Prinzipien verwenden. Besonders zu beachten ist die Wahl solcher Reste, die bei Division durch den Modul die einfachsten Quotienten ergeben. Sind $\alpha+\beta i, \alpha'+\beta' i, \alpha''+\beta'' i$ usw. die bei Division kongruenter Zahlen durch den Modul entstehenden Quotienten, so sind offenbar sowohl die Differenzen der Größen $\alpha, \alpha', \alpha''$ usw. untereinander als auch die Differenzen zwischen den Größen β, β', β'' usw. ganze Zahlen. Es ist klar, dass stets ein Rest vorhanden ist, für den α und β zwischen den Grenzen 0 und 1 liegen, die erstere eingeschlossen, die letztere ausgeschlossen. Einen solchen Rest nennen wir einfach einen kleinsten Rest. Wenn man es vorzieht, kann man stattdessen auch die Grenzen $-\frac{1}{2}$ und $+\frac{1}{2}$ wählen, die eine eingeschlossen, die andere ausgeschlossen; einen dieser Beschränkung entsprechenden Rest nennen wir *absolut kleinsten.*

Bezüglich $\cdot$ dieser kleinsten Reste ergeben sich folgende Aufgaben.

43.

Den kleinsten Rest einer gegebenen komplexen Zahl $A + Bi$ nach dem Modul $a+bi$, mit der Norm $= p$, findet man wie folgt. Ist $x+yi$ der gesuchte kleinste Rest, so ist $(x + yi)(a - bi)$ der kleinste Rest des Produkts $(A + Bi)(a - bi)$ nach dem Modul $(a + bi)(a - bi)$, also nach dem Modul p. Wir setzen daher

$$aA + bB = Fp + f, \quad aB - bA = Gp + g$$

sodass f, g die kleinsten Reste der Zahlen $aA+bB, aB-bA$ nach dem Modul p sind. Dann ist

$$x + yi = \frac{f + gi}{a - bi}$$

oder

$$x = \frac{af - bg}{p} = A - aF + bG$$
$$y = \frac{ag + bf}{p} = B - aG - bF$$

Offenbar müssen die kleinsten Reste f, g entweder zwischen den Grenzen 0 und $p-1$ oder zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ genommen werden, je nachdem, ob der einfach kleinste oder der absolut kleinste Rest der komplexen Zahl verlangt wird.

44.

Ein vollständiges System kleinster Reste für einen gegebenen Modul lässt sich auf mehrere Arten aufstellen. Das erste Verfahren bestimmt zunächst die Grenzen, innerhalb deren die reellen Glieder liegen müssen, und gibt dann für jeden Wert innerhalb dieser Grenzen die Grenzen der imaginären Teile an. Das allgemeine Kriterium für einen kleinsten Rest $x + yi$ nach dem Modul $a + bi$ besteht darin, dass sowohl $ax + by = \xi$ als auch $ay - bx = \eta$ zwischen den Grenzen 0 und $aa + bb$ liegen, wenn es sich um einfach kleinste Reste handelt, oder zwischen $-\frac{1}{2}(aa + bb)$ und $+\frac{1}{2}(aa + bb)$, wenn absolut kleinste Reste verlangt werden; dabei ist eine Grenze ausgeschlossen. Besondere Regeln würden die Unterscheidung der Fälle erfordern, die aus den verschiedenen Vorzeichen der Zahlen a, b entstehen. Da die Entwicklung dieser Unterscheidung keine Schwierigkeit bietet, halten wir uns hier nicht dabei auf; es genüge, die Art des Verfahrens an einem einzigen Beispiel darzulegen.

Für den Modul $5 + 2i$ müssen die einfach kleinsten Reste $x + yi$ so beschaffen sein, dass sowohl $5x + 2y = \xi$ als auch $5y - 2x = \eta$ einer der Zahlen $0, 1, 2, 3 \ldots 28$ gleich ist. Die Gleichung $29x = 5\xi - 2\eta$ zeigt, dass die positiven Werte von x nicht größer als $\frac{5.28}{29}$ und die negativen, vom Vorzeichen abgesehen, nicht größer als $\frac{2.28}{29}$ sein können. Alle zulässigen Werte von x sind daher $-1, 0, 1, 2, 3, 4$. Für $x = -1$ muss $2y$ einer der Zahlen $5, 6, 7 \ldots 33$ und $5y$ einer der Zahlen $-2, -1, 0, 1 \ldots 26$ gleich sein; somit ist der kleinste Wert von y $+3$, der größte $+5$. Behandelt man die übrigen Werte von x ebenso, so entsteht die folgende Tabelle aller kleinsten Reste:

x	y
-1	$3, 4, 5$
0	$0, 1, 2, 3, 4, 5$
$+1$	$1, 2, 3\,.\,4, 5\,.\,6$
$+2$	$1, 2, 3, 4, 5, 6$
$+3$	$2, 3, 4\,.\,5, 6$
$+4$	$2, 3, 4$

Ebenso müssen für die absolut kleinsten Reste ξ und η einer der Zahlen $-14, -13, -12 \ldots . + 14$ gleich sein. Daher kann $29x$ nicht außerhalb der Grenzen $-7 \,.\, 14$ und $+7 \,.\, 14$ liegen, und somit muss x einer der Zahlen $-3, -2, -1, 0, 1, 2, 3$ gleich sein. Für $x = -3$ ist $2y = \xi - 5x = \xi + 15$ einer der Zahlen $1, 2, 3 \ldots . 29$ gleich, $5y = \eta + 2x = \eta - 6$ dagegen einer der Zahlen $-20, -19, -18 \ldots . + 8$; daraus ergibt sich für y der einzige Wert $+1$. Behandeln wir die übrigen Werte von x auf dieselbe Weise, so erhalten wir die Tabelle aller absolut kleinsten Reste:

x	y
-3	$+1$
-2	$-2, -1, 0, +1, +2$
-1	$-3, -2, -1, 0, +1, +2$
0	$-2, -1, 0, +1, +2$
$+1$	$-2, -1, 0, +1, +2, +3$
$+2$	$-2, -1, 0, +1, +2$
$+3$	-1

45.

Bei der Anwendung des zweiten Verfahrens wird es zweckmäßig sein, zwei Fälle zu unterscheiden.

Im ersten Fall, in dem a und b keinen gemeinsamen Teiler haben, setzen wir $a\alpha + \beta b = 1$, und es sei k der kleinste positive Rest von $\beta a - \alpha b$ nach dem Modul p. Die Identitäten

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b),$$
$$b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b)$$

zeigen dann, dass $ak \equiv -b, bk \equiv a (\text{mod. } p)$ gilt. Setzen wir also wie oben $ax + by = \xi$,

$ay - bx = \eta$, so gilt $\eta \equiv k\xi$, $\xi \equiv -k\eta (\text{mod. } p)$. Alle Zahlen $\xi + \eta i$, denen einfach kleinste Reste $x + yi$ entsprechen, erhält man daher, indem man entweder für ξ der Reihe nach die Werte $0, 1, 2, 3 \ldots . p-1$ und für η die kleinsten positiven Reste der Produkte $k\xi$ nach dem Modul p nimmt, oder in anderer Reihenfolge für η jene Werte und für ξ die kleinsten Reste der Produkte $-k\eta$. Aus jedem $\xi + \eta i$ findet man dann das entsprechende $x + yi$ nach der Formel

$$x + yi = \frac{\xi + \eta i}{a - bi} = \frac{a\xi - b\eta}{p} + \frac{a\eta + b\xi}{p} \,.\, i$$

Ferner ist klar, dass η, wenn ξ um eins wächst, entweder um k zunimmt oder um $p-k$ abnimmt und somit $x+yi$

$$\text{entweder die Änderung } \frac{a-kb}{p}+\frac{ak+b}{p}\,.\,i$$
$$\text{oder diese } \frac{a-kb}{p}+b+\left(\frac{ak+b}{p}-a\right)i$$

erfährt. Diese Bemerkung dient dazu, die Aufstellung zu erleichtern.

Werden schließlich absolut kleinste Reste $x+yi$ verlangt, so ändern sich diese Vorschriften offenbar nur insofern, als ξ der Reihe nach die Werte zwischen den Grenzen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ beizulegen sind, während für η die absolut kleinsten Reste der Produkte $k\xi$ genommen werden müssen. Hier folgt eine Tabelle der auf diese Weise angeordneten kleinsten Reste für den Modul $5+2i$:

Einfach kleinste Reste.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
0	0	$10+25i$	$+5i$	$20+21i$	$+2+5i$
$1+17i$	$-1+3i$	$11+13i$	$+1+3i$	$21+9i$	$+3+3i$
$2+5i$	$+i$	$12+i$	$+2+i$	$22+26i$	$+2+6i$
$3+22i$	$+1+4i$	$13+18i$	$+1+4i$	$23+14i$	$+3+4i$
$4+10i$	$+2i$	$14+6i$	$+2+2i$	$24+2i$	$+4+2i$
$5+27i$	$-1+5i$	$15+23i$	$+1+5i$	$25+19i$	$+3+5i$
$6+15i$	$+3i$	$16+11i$	$+2+3i$	$26+7i$	$+4+3i$
$7+3i$	$+1+i$	$17+28i$	$+1+6i$	$27+24i$	$+3+6i$
$8+20i$	$+4i$	$18+16i$	$+2+4i$	$28+12i$	$+4+4i$
$9+8i$	$+1+2i$	$19+4i$	$+3+2i$		

Absolut kleinste Reste.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
$-14-6i$	$-2-2i$	$-4-10i$	$-2i$	$+5-2i$	$+1$
$-13+11i$	$-3+i$	$-3+7i$	$-1+i$	$+6-14i$	$+2-2i$
$-12-i$	$-2-i$	$-2-5i$	$-i$	$+7+3i$	$+1+i$
$-11-13i$	$-1-3i$	$-1+12i$	$-1+2i$	$+8-9i$	$+2-i$
$-10+4i$	-2	0	0	$+9+8i$	$+1+2i$
$-9-8i$	$-1-2i$	$+1-12i$	$+1-2i$	$+10-4i$	$+2$
$-8+9i$	$-2+i$	$+2+5i$	$+i$	$+11+13i$	$+1+3i$
$-7-3i$	$-1-i$	$+3-7i$	$+1-i$	$+12+i$	$+2+i$
$-6+14i$	$-2+2i$	$+4+10i$	$+2i$	$+13-11i$	$+3-i$
$-5+2i$	-1			$+14+6i$	$+2+2i$

Der zweite Fall, in dem a, b nicht teilerfremd sind, lässt sich leicht auf den vorigen zurückführen. Es sei λ der größte gemeinsame Teiler der Zahlen a, b, und es sei $a=\lambda a'$, $b=\lambda b'$. Ferner bezeichne F einen beliebigen kleinsten Rest nach dem Modul λ, wobei der Modul als komplexe Zahl betrachtet wird:

Es stelle also eine beliebige Zahl $x+yi$ dar, für die x, y entweder zwischen den Grenzen 0 und λ oder zwischen $-\frac{1}{2}\lambda$ und $+\frac{1}{2}\lambda$ liegen, je nachdem, ob es sich um einfach kleinste oder absolut kleinste Reste handelt. Weiter bezeichne F' einen beliebigen kleinsten Rest nach dem Modul $a' + b'i$. Dann stellt $(a' + b'i)F + F'$ einen beliebigen kleinsten Rest nach dem Modul $a + bi$ dar, und ein vollständiges System dieser Reste entsteht, wenn alle Werte von F mit allen Werten von F' kombiniert werden.

46.

Zwei komplexe Zahlen heißen teilerfremd, wenn sie außer den Einheiten keine anderen gemeinsamen Teiler besitzen. Sind solche gemeinsamen Teiler vorhanden, so heißen diejenigen größte gemeinsame Teiler, deren Norm am größten ist.

Liegt die Zerlegung zweier gegebener Zahlen in Primfaktoren vor, so wird der größte gemeinsame Teiler genauso bestimmt wie bei reellen Zahlen (*Disquiss. Ar.* Artikel 18). Zugleich ergibt sich daraus, dass alle gemeinsamen Teiler zweier gegebener Zahlen auch ihren auf diese Weise gefundenen größten gemeinsamen Teiler teilen müssen. Da schon von selbst klar ist, dass die drei ihm assoziierten Zahlen ebenfalls gemeinsame Teiler sind, wird es stets vier Zahlen und nicht mehr geben, die größte gemeinsame Teiler zu nennen sind; ihre Norm ist ein Vielfaches der Norm jedes anderen gemeinsamen Teilers.

Liegt die Zerlegung zweier gegebener Zahlen in einfache Faktoren nicht vor, so findet man den größten gemeinsamen Teiler mithilfe eines ähnlichen Algorithmus wie bei reellen Zahlen. Es seien m, m' die beiden gegebenen Zahlen, und durch wiederholte Division bilde man die Folge m'', m''' usw., sodass m'' der absolut kleinste Rest von m nach dem Modul m', dann m''' der absolut kleinste Rest von m' nach dem Modul m'' ist, und so fort. Bezeichnet man die Normen der Zahlen m, m', m'', m''' usw. der Reihe nach mit p, p', p'', p''' usw., so ist $\frac{p''}{p'}$ die Norm des Quotienten $\frac{m''}{m'}$ und daher nach der Definition eines absolut kleinsten Restes gewiss nicht größer als $\frac{1}{2}$; dasselbe gilt für $\frac{p'''}{p''}$ usw. Die positiven reellen ganzen Zahlen p', p'', p''' usw. bilden also eine stetig abnehmende Folge, sodass man schließlich notwendig zum Glied 0 gelangt. Oder, was dasselbe ist: In der Folge m, m', m'', m''' usw. gelangen wir schließlich zu einem Glied, das das vorhergehende ohne Rest teilt. Es sei dies $m^{(n+1)}$, und wir setzen

$$\begin{aligned} m &= km' + m'' \\ m' &= k'm'' + m''' \\ m'' &= k''m''' + m'''' \end{aligned}$$

und so fort bis zu

$$m^{(n)} = k^{(n)}m^{(n+1)}$$

Durchläuft man diese Gleichungen in umgekehrter Reihenfolge, so ergibt sich, dass $m^{(n+1)}$ jedes der vorhergehenden Glieder $m^{(n)} \ldots . m'', m', m$ teilt.

Durchläuft man dieselben Gleichungen dagegen in direkter Reihenfolge, so ist ersichtlich, dass jeder gemeinsame Teiler der Zahlen m, m' auch jedes folgende Glied teilt. Der erste Schluss zeigt, dass $m^{(n+1)}$ ein gemeinsamer Teiler der Zahlen m, m' ist; der zweite, dass dieser Teiler ein größter ist.

Wird der letzte Rest $m^{(n+1)}$ einer der vier Einheiten $1, -1, i, -i$ gleich, so zeigt dies, dass m und m' teilerfremd sind.

47.

Kombiniert man die Gleichungen des vorigen Artikels unter Weglassung der letzten so, dass $m'', m''', m'''' \ldots . m^{(n)}$ eliminiert werden, so entsteht eine Gleichung der Form

$$m^{(n+1)} = hm + h'm'$$

wobei h, h' ganze Zahlen sind; und zwar gilt, wenn man die in *Disquiss. Ar.* Artikel 27 eingeführte Bezeichnung verwenden will,

$$\begin{aligned} h &= \pm[k', k'', k''' \ldots . k^{(n-1)}] \\ &= \pm[k^{(n-1)}, k^{(n-2)} \ldots . k'', k'] \\ h' &= \mp[k, k', k'', k''' \ldots . k^{(n-1)}] \\ &= \mp[k^{(n-1)}, k^{(n-2)} \ldots . k'', k', k] \end{aligned}$$

mit den oberen oder unteren Vorzeichen, je nachdem, ob n gerade oder ungerade ist. Diesen Satz sprechen wir folgendermaßen aus:

Ein größter gemeinsamer Teiler zweier komplexer Zahlen m, m' lässt sich auf die Form $hm + h'm'$ bringen, wobei h, h' ganze Zahlen sind.

Dies gilt offenbar sowohl für den größten gemeinsamen Teiler, zu dem der Algorithmus des vorigen Artikels geführt hat, als auch für seine drei Assoziierten. Für diese sind anstelle der Koeffizienten h, h' entweder $hi, h'i$ oder $-h, -h'$ oder $-hi, -h'i$ zu nehmen.

Sind daher die Zahlen m, m' teilerfremd, so lässt sich die folgende Gleichung erfüllen:

$$1 = hm + h'm'$$

Es seien zum Beispiel die Zahlen $31 + 6i = m$, $11 - 20i = m'$ gegeben. Hier finden wir

$$\begin{aligned} k &= i, & m'' &= +11 - 5i \\ k' &= +1 - i, & m''' &= +5 - 4i \\ k'' &= +2, & m'''' &= +1 + 3i \\ k''' &= -1 - 2i, & m''''' &= +i \\ k'''' &= +3 - i \end{aligned}$$

und daraus

$$\begin{aligned} [k', k'', k'''] &= -6 - 5i \\ [k, k', k'', k'''] &= +4 - 10i \end{aligned}$$

und somit

$$m'''' = i = (6 + 5i)m + (4 - 10i)m'$$

sowie

$$1 = (5 - 6i)m + (-10 - 4i)m'$$

was sich durch Ausführen der Rechnung bestätigt.

48.

Durch das Vorhergehende ist alles vorbereitet, was zur Theorie der Kongruenzen ersten Grades in der Arithmetik komplexer Zahlen erforderlich ist. Da diese Theorie jedoch von der für die Arithmetik reeller Zahlen geltenden nicht wesentlich verschieden und in den *Disquisitiones Arithmeticae* ausführlich dargelegt ist, wird es genügen, hier die Hauptpunkte anzuführen.

I. Die Kongruenz $mt \equiv 1 \pmod{m'}$ ist der unbestimmten Gleichung $mt + m'u = 1$ gleichwertig. Wird dieser durch die Werte $t = h, u = h'$ genügt, so wird die allgemeine Lösung der Kongruenz durch $t \equiv h \pmod{m'}$ dargestellt. Die Bedingung der Lösbarkeit ist, dass der Modul m' mit dem Koeffizienten m keinen gemeinsamen Teiler hat.

II. Die Lösung der Kongruenz $ax + b \equiv c \pmod{M}$ in dem Fall, in dem a, M teilerfremd sind, hängt von der Lösung der folgenden ab:

$$at \equiv 1 \pmod{M}$$

Genügt ihr $t = h$, so ist die allgemeine Lösung der ersteren in der Formel enthalten:

$$x \equiv (c - b)h \pmod{M}$$

III, Die Kongruenz $ax + b \equiv c \pmod{M}$ in dem Fall, in dem a, M einen gemeinsamen Teiler λ haben, ist der folgenden gleichwertig:

$$\frac{a}{\lambda} \cdot x \equiv \frac{c - b}{\lambda} \left(\mathrm{mod.} \frac{M}{\lambda}\right)$$

Wird also für λ der größte gemeinsame Teiler der Zahlen a, M genommen, so wird die Lösung der gegebenen Kongruenz auf den vorigen Fall zurückgeführt. Es ist klar, dass zur Lösbarkeit notwendig und hinreichend ist, dass λ auch die Differenz $c - b$ teilt.

49.

Bisher haben wir nur elementare Dinge berührt, die wir jedoch des Zusammenhangs wegen nicht weglassen durften. In tieferen Untersuchungen ähnelt die Arithmetik komplexer Zahlen der Arithmetik reeller Zahlen darin, dass elegantere und einfachere Sätze entstehen, wenn wir nur solche Moduln zulassen, die Primzahlen sind. Ihre Ausdehnung auf zusammengesetzte Moduln ist nämlich meist eher weitläufig als schwierig und erfordert eher Arbeit als Kunst. Daher werden wir uns im Folgenden vor allem mit Primzahlmoduln befassen.

50.

Es bezeichne X eine Funktion der Unbestimmten x von der folgenden Form:

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \text{usw.} + Mx + N;$$

wobei n eine positive reelle ganze Zahl, A, B, C usw. reelle oder imaginäre ganze Zahlen und m eine komplexe ganze Zahl ist. Auch hier nennen wir eine ganze Zahl eine *Wurzel* der Kongruenz $X \equiv 0 \pmod{m}$, wenn sie, für x eingesetzt, für X einen durch den Modul m teilbaren Wert ergibt. Lösungen durch nach dem Modul kongruente Wurzeln betrachten wir nicht als verschieden.

Ist der Modul eine Primzahl, so kann auch hier eine solche Kongruenz vom Grad n nicht mehr als n verschiedene Lösungen besitzen. Bezeichne α eine beliebige feste ganze Zahl (komplex), so lässt sich X durch Division durch $x - \alpha$ bei unbestimmt gelassener Veränderlicher auf die Form $X = (x - \alpha)X' + h$ bringen, wobei h eine feste ganze Zahl und X' eine Funktion vom Grad $n-1$ mit ganzzahligen Koeffizienten ist. Ist nun α eine Wurzel der Kongruenz $X \equiv 0 \pmod{m}$, so ist offenbar h durch m teilbar; oder es gilt bei unbestimmt gelassener Veränderlicher $X \equiv (x - \alpha)X' \pmod{m}$.

Bezeichnet ebenso β eine feste ganze Zahl und wird X' auf die Form $(x - \beta)X'' + h'$ gebracht, so ist X'' eine Funktion vom Grad $n-2$ mit ganzzahligen Koeffizienten. Wird aber β als Wurzel der Kongruenz $X \equiv 0$ vorausgesetzt, so muss sie auch $(\beta - \alpha)X' \equiv 0$ und auch $X' \equiv 0$ erfüllen, sofern die Wurzeln α, β inkongruent sind. Daraus schließen wir, dass auch h' durch m teilbar sein muss, oder dass bei unbestimmt gelassener Veränderlicher $X \equiv (x - \alpha)(x - \beta)X'' \pmod{m}$ gilt.

Kommt auf ähnliche Weise eine dritte, zu den vorigen inkongruente Wurzel γ hinzu, so gilt bei unbestimmt gelassener Veränderlicher $X \equiv (x - \alpha)(x - \beta)(x - \gamma)X'''$, wobei X''' eine Funktion vom Grad $n - 3$ mit ganzzahligen Koeffizienten ist. So lässt sich weiter fortfahren, und zugleich ist klar, dass der Koeffizient des höchsten Gliedes in jeder Funktion $= A$ ist, den wir als durch m nicht teilbar voraussetzen dürfen; andernfalls müsste die Kongruenz $X \equiv 0$ wesentlich einem niedrigeren Grad zugerechnet werden. Sind also n inkongruente Wurzeln vorhanden, etwa $\alpha, \beta, \gamma \ldots . \nu$, so gilt bei unbestimmt gelassener Veränderlicher

$$X \equiv A(x - \alpha)(x - \beta)(x - \gamma) \ldots . (x - \nu) \pmod{m}$$

Das Einsetzen eines neuen, zu jeder der Zahlen $\alpha, \beta, \gamma \ldots . \nu$ inkongruenten Wertes würde folglich für X sicher einen durch m nicht teilbaren Wert ergeben, woraus die Richtigkeit des Satzes von selbst folgt.

Dieser Beweis stimmt im Wesentlichen mit demjenigen überein, den wir in *Disq. Ar.* Artikel 43 gegeben haben und dessen einzelne Schritte für komplexe Zahlen ebenso gelten wie für reelle.

51.

Was im dritten Abschnitt der *Disquisitiones Arithmeticae* über Potenzreste gegeben wurde, gilt größtenteils mit geringfügigen Änderungen auch in der Arithmetik komplexer Zahlen; ja, meist könnten sogar die Beweise der Sätze beibehalten werden. Damit jedoch nichts fehlt, werden wir die Hauptsätze mit kurzen Beweisen anführen. Dabei ist stets vorauszusetzen, dass der Modul eine Primzahl ist.

Satz. *Bezeichnet k eine durch den Modul m, mit der Norm $= p$, nicht teilbare ganze Zahl, so gilt $k^{p-1} \equiv 1 \pmod{m}$.*

Beweis. Es mögen a, b, c usw. ein vollständiges System inkongruenter Reste nach dem Modul m bilden, wobei jedoch der durch m teilbare Rest weggelassen ist, sodass die Anzahl dieser Zahlen, deren Sammlung wir mit C bezeichnen, $= p - 1$ ist. Ferner sei C' die Sammlung der Produkte ka, kb, kc usw. Nach Voraussetzung ist keines dieser Produkte durch m teilbar; daher hat jedes einen kongruenten Rest in der Sammlung C. Es lässt sich also $ak \equiv a', bk \equiv b', ck \equiv c'$ usw. (mod. m) setzen, sodass die Zahlen a', b', c' usw. selbst in der Sammlung C vorkommen. Die Sammlung der Zahlen a', b', c' usw. bezeichnen wir mit C''. Es seien P, P', P'' die Produkte aus den einzelnen Zahlen der Sammlungen C, C', C'' in derselben Reihenfolge, also

$$\begin{aligned} P &= abc\ldots. \\ P' &= k^{p-1}abc\ldots. = k^{p-1}P \\ P'' &= a'b'c'\ldots. \end{aligned}$$

Da die Zahlen der Sammlung C'' der Reihe nach den Zahlen der Sammlung C' kongruent sind, gilt $P'' \equiv P'$ oder $P'' \equiv k^{p-1}P$. Da aber leicht zu sehen ist, dass je zwei Zahlen der Sammlung C'' inkongruent und daher alle voneinander verschieden sind, stimmen die Zahlen der Sammlung C'' notwendig mit denen der Sammlung C vollständig überein, nur in anderer Reihenfolge; somit gilt $P'' = P$. Also ist $(k^{p-1} - 1)P$ durch m teilbar. Da m eine Primzahl ist, die keinen der einzelnen Faktoren von P teilt, muss notwendig $k^{p-1} - 1$ durch m teilbar sein. Q. E. D.

52.

Satz. *Bezeichnet k wie im vorigen Artikel eine durch den Modul m nicht teilbare ganze Zahl und t den kleinsten Exponenten (außer 0), für den $k^t \equiv 1 \pmod{m}$ gilt, so ist t ein Teiler jedes anderen Exponenten u, für den $k^u \equiv 1 \pmod{m}$ gilt.*

Beweis. Wäre t kein Teiler von u, so sei gt das nächstgrößere Vielfache von u über u, sodass $gt - u$ eine positive ganze Zahl kleiner als t ist. Aus $k^t \equiv 1, k^u \equiv 1$ folgt $0 \equiv k^{gt} - k^u \equiv k^u(k^{gt-u} - 1)$ und daher $k^{gt-u} \equiv 1$; es gibt also eine Potenz von k mit einem Exponenten kleiner als t, die der Einheit kongruent ist, gegen die Voraussetzung.

Als Folgerung ergibt sich daraus, dass t gewiss die Zahl $p-1$ teilt.

Solche Zahlen k, für die $t = p-1$ gilt, nennen wir auch hier *primitive Wurzeln* für. den Modul m. Dass es solche wirklich gibt, werden wir nun zeigen.

53.

Man zerlege die Zahl $p-1$ in ihre Primfaktoren, sodass

$$p-1 = a^\alpha b^\beta c^\gamma \dots .$$

gilt, wobei a, b, c usw. verschiedene positive reelle Primzahlen bezeichnen. Es seien A, B, C usw. durch m nicht teilbare ganze Zahlen (komplex), die jeweils den Kongruenzen

$$x^{\frac{p-1}{a}} \equiv 1, \quad x^{\frac{p-1}{b}} \equiv 1, \quad x^{\frac{p-1}{c}} \equiv 1 \quad \text{usw.}$$

nach dem Modul m *nicht* genügen. Dass es solche gibt, ist aus dem Satz des Artikels 50 ersichtlich. Schließlich sei h nach dem Modul m dem Produkt

$$A^{\frac{p-1}{a^\alpha}} B^{\frac{p-1}{b^\beta}} C^{\frac{p-1}{c^\gamma}} \dots .$$

kongruent. Dann behaupte ich, dass h eine primitive Wurzel ist.

Beweis. Bezeichnet t den Exponenten der niedrigsten der Einheit kongruenten Potenz h^t, so wäre, wenn h keine primitive Wurzel wäre, t ein echter Teiler von $p-1$, oder $\frac{p-1}{t}$ eine die Einheit übersteigende ganze Zahl. Offenbar liegen die reellen Primfaktoren dieser ganzen Zahl unter a, b, c usw. Wir nehmen daher, was erlaubt ist, an, dass $\frac{p-1}{t}$ durch a teilbar ist, und setzen $p-1 = atu$. Wegen $h^t \equiv 1$ gilt dann auch $h^{tu} \equiv 1$, oder

$$A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \dots . \equiv 1$$

Offenbar ist aber $\frac{p-1}{ab^\beta}$ eine ganze Zahl, also

$$B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} = \left(B^{p-1}\right)^{\frac{p-1}{ab^\beta}} \equiv 1$$

und ebenso $C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \equiv 1$ und so fort; daher muss $A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$ gelten. Nun bestimme man eine positive ganze Zahl λ derart, dass

$$\lambda b^\beta c^\gamma \dots . \equiv 1 \pmod{a}$$

gilt. Dies ist möglich, da die Primzahl a die Zahl $b^\beta c^\gamma \dots .$ nicht teilt; wir setzen $\lambda b^\beta c^\gamma \dots . = 1 + a\mu$. Offenbar gilt $A^{\lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$; oder, da $\lambda \,.\, \frac{p-1}{a^\alpha} \,.\, \frac{p-1}{a} = (1+a\mu)\frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}$, haben wir $A^{(p-1)\mu} \,.\, A^{\frac{p-1}{a}} \equiv 1$. Weil von selbst $A^{(p-1)\mu} \equiv 1$ gilt, folgt daraus auch $A^{\frac{p-1}{a}} \equiv 1$, gegen die Voraussetzung. Die Annahme, dass t ein echter Teiler von $p-1$ ist, kann also nicht bestehen, und somit ist h notwendig eine primitive Wurzel.

54.

Es sei h eine primitive Wurzel für den Modul m, mit der Norm $= p$. Die Glieder der Folge

$$1, h, hh, h^3 \ldots . h^{p-2}$$

sind dann einander inkongruent. Daraus folgt leicht, dass jede durch den Modul nicht teilbare ganze Zahl einem dieser Glieder kongruent sein muss; diese Folge stellt also ein vollständiges System inkongruenter Reste unter Ausschluss der Null dar. Der Exponent der Potenz, der eine gegebene Zahl kongruent ist, kann ihr *Index* heißen, wobei h als *Basis* betrachtet wird. Hier folgen einige Beispiele, in denen wir neben jeden Index den absolut kleinsten Rest gesetzt haben.

Erstes Beispiel.

$$m = 5 + 4i, \quad p = 41, \quad h = 1 + 2i$$

Ind.	Rest	Ind.	Rest	Ind.	Rest	Ind.	Rest	Ind.	Rest
0	$+1$	8	-4	16	$-2+2i$	24	$+2i$	32	$+1+i$
1	$+1+2i$	9	$-3+i$	17	$-1+2i$	25	$-3i$	33	$+1+3i$
2	$+1-i$	10	$-i$	18	$+4i$	26	$+2+2i$	34	$+2$
3	$+3+i$	11	$+2-i$	19	$+1+3i$	27	$+2+i$	35	-3
4	$-2i$	12	$-1-i$	20	-1	28	$+4$	36	$+2-2i$
5	$+3i$	13	$+1-3i$	21	$-1-2i$	29	$+3-i$	37	$+1-2i$
6	$-2-2i$	14	-2	22	$-1+i$	30	$+i$	38	$-4i$
7	$-2-i$	15	$+3$	23	$-3-i$	31	$-2+i$	39	$-1-3i$

Zweites Beispiel.

$$m = 7, \quad p = 49, \quad h = 1 + 2i$$

Ind.	Rest	Ind.	Rest	Ind.	Rest	Ind.	Rest	Ind.	Rest
0	$+1$	10	$-1-i$	20	$+2i$	30	$+2-2i$	40	$+3$
1	$+1+2i$	11	$+1-3i$	21	$+3+2i$	31	$-1+2i$	41	$+3-i$
2	$-3-3i$	12	$-i$	22	$-1+i$	32	$+2$	42	$-2-2i$
3	$+3-2i$	13	$+2-i$	23	$-3-i$	33	$+2-3i$	43	$+2+i$
4	$-3i$	14	$-3+3i$	24	-1	34	$+1+i$	44	$-2i$
5	$-1-3i$	15	$-2-3i$	25	$-1-2i$	35	$-1+3i$	45	$-3-2i$
6	$-2+2i$	16	-3	26	$+3+3i$	36	$+i$	46	$+1-i$
7	$+1-2i$	17	$-3+i$	27	$-3+2i$	37	$-2+i$	47	$+3+i$
8	-2	18	$+2+2i$	28	$+3i$	38	$+3-3i$		
9	$-2+3i$	19	$-2-i$	29	$+1+3i$	39	$+2+3i$		

55.

Wir fügen einige Bemerkungen über primitive Wurzeln und die Berechnung von Indizes hinzu und lassen die Beweise ihrer Einfachheit wegen weg.

I. In einem gegebenen System entsprechen nach dem Modul $p-1$ kongruente Indizes nach dem Modul m kongruenten Resten, und umgekehrt.

II. Reste, die zu $p-1$ teilerfremden Indizes entsprechen, sind selbst primitive Wurzeln, und umgekehrt.

III. Wird eine primitive Wurzel h als Basis genommen und ist der Index einer anderen primitiven Wurzel h' gleich t und umgekehrt t' der Index von h, wenn h' als Basis genommen wird, so gilt $tt' \equiv 1 \pmod{p-1}$. Sind unter denselben Voraussetzungen die Indizes einer anderen Zahl in diesen beiden Systemen der Reihe nach u, u', so gilt $tu' \equiv u, t'u \equiv u' \pmod{p-1}$.

IV. Werden die Zahlen $1, 1+i$ und jeweils ihre drei Assoziierten als zu trivial von den betrachteten Moduln ausgeschlossen, so bleiben die Primzahlen übrig, die wir in Artikel 34 an dritter und vierter Stelle aufgeführt haben. Die Normen der letzteren sind reelle Primzahlen der Form $4n+1$, die der ersteren dagegen Quadrate ungerader reeller Primzahlen; in beiden Fällen ist also $p-1$ durch 4 teilbar.

V. Bezeichnen wir den Index der Zahl -1 mit u, so gilt $2u \equiv 0 \pmod{p-1}$, also entweder $u \equiv 0$ oder $u \equiv \frac{1}{2}(p-1)$. Da aber der Index 0 dem Rest $+1$ entspricht, muss der Index der Zahl -1 notwendig $\frac{1}{2}(p-1)$ sein.

VI. Bezeichnen wir ebenso mit u den Index der Zahl i, so gilt $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$, also entweder $u \equiv \frac{1}{4}(p-1)$ oder $u \equiv \frac{3}{4}(p-1)$. Hier hängt die Mehrdeutigkeit jedoch von der Wahl der primitiven Wurzel ab. Ist nämlich bei der als Basis genommenen primitiven Wurzel h der Index der Zahl i gleich $\frac{1}{4}(p-1)$, so wird er $\frac{3}{4}(p-1)$, wenn h^μ als Basis genommen wird, wobei μ eine positive ganze Zahl der Form $4n+3$ bezeichnet, die zu $p-1$ teilerfremd ist, zum Beispiel die Zahl $p-2$ selbst; und umgekehrt. Daher gibt die eine Hälfte der primitiven Wurzeln der Zahl i den Index $\frac{1}{4}(p-1)$, die andere den Index $\frac{3}{4}(p-1)$. Für jene Basen hat offenbar $-i$ den Index $\frac{3}{4}(p-1)$, für diese den Index $\frac{1}{4}(p-1)$.

VII. Ist der Modul eine positive reelle Primzahl der Form $4n+3$, etwa $= q$, und somit $p = qq$, so sind die Indizes aller reellen Zahlen durch $q+1$ teilbar. Bezeichnet nämlich t den Index der reellen Zahl k, so gilt wegen $k^{q-1} \equiv \pmod{q}$ auch $(q-1)t \equiv 0 \pmod{qq-1}$, und somit ist $\frac{t}{q+1}$ eine ganze Zahl. Ebenso sind die Indizes rein imaginärer Zahlen wie ki durch $\frac{1}{2}(q+1)$ teilbar. Daher ist klar, dass primitive Wurzeln für solche Moduln nur unter gemischten Zahlen zu suchen sind.

VIII. Dagegen lassen sich für einen Modul m, der eine gemischte komplexe Primzahl ist und dessen Norm p folglich eine reelle Primzahl der Form $4n+1$ ist, beliebige primitive Wurzeln auch unter reellen Zahlen wählen, unter denen sich sogar ein vollständiges System inkongruenter Reste angeben lässt (Artikel 40). Offenbar ist jede reelle Zahl, die für den komplexen Modul m eine primitive Wurzel ist, zugleich in der Arithmetik reeller Zahlen eine primitive Wurzel für den Modul p, und umgekehrt.

56.

Obwohl die Theorie quadratischer Reste und Nichtreste in der Arithmetik komplexer Zahlen in der Theorie biquadratischer Reste selbst enthalten ist, werden wir ihre Hauptsätze hier gesondert vortragen, bevor wir zu der letzteren übergehen. Der Kürze wegen behandeln wir jedoch nur den Hauptfall, in dem der Modul eine ungerade komplexe Primzahl ist.

Es sei m ein solcher Modul und p seine Norm. Offenbar kann eine ganze Zahl, die nicht durch m teilbar ist, was hier stets vorauszusetzen ist, einem Quadrat nach dem Modul m kongruent sein oder nicht, je nachdem, ob ihr Index bei einer als Basis genommenen primitiven Wurzel gerade oder ungerade ist. Im ersten Fall heißt diese ganze Zahl quadratischer Rest von m, im zweiten Nichtrest. Daraus folgt, dass unter $p-1$ Zahlen, die ein vollständiges System inkongruenter, durch m nicht teilbarer Reste darstellen, die eine Hälfte zu den quadratischen Resten und die andere zu den quadratischen Nichtresten gehört. Jeder anderen Zahl außerhalb dieses Systems ist in dieser Hinsicht derselbe Charakter zuzuweisen wie der ihr kongruenten Zahl des Systems.

Ferner folgt daraus, dass das Produkt zweier quadratischer Reste ebenso wie das Produkt zweier Nichtreste ein quadratischer Rest ist, dagegen das Produkt eines quadratischen Restes und eines Nichtrestes ein Nichtrest. Allgemein ist ein Produkt aus beliebig vielen Faktoren ein quadratischer Rest oder Nichtrest, je nachdem, ob die Anzahl der Nichtreste unter den Faktoren gerade oder ungerade ist.

Zur Unterscheidung quadratischer Reste von Nichtresten bietet sich sogleich das folgende allgemeine Kriterium an:

Eine durch den Modul nicht teilbare Zahl k ist ein quadratischer Rest oder Nichtrest desselben, je nachdem, ob $k^{\frac{1}{2}(p-1)} \equiv 1$ oder $k^{\frac{1}{2}(p-1)} \equiv -1 \pmod{m}$ gilt.

Die Richtigkeit dieses Satzes folgt unmittelbar daraus, dass bei einer beliebigen als Basis genommenen primitiven Wurzel der Index der Potenz $k^{\frac{1}{2}(p-1)}$ entweder $\equiv 0$ oder $\equiv \frac{1}{2}(p-1)$ wird, je nachdem, ob der Index der Zahl k gerade oder ungerade ist.

57.

Für einen gegebenen Modul lässt sich ein vollständiges System inkongruenter Reste leicht in zwei Klassen, quadratische Reste und Nichtreste, teilen; damit sind zugleich allen übrigen Zahlen ihre Klassen zugewiesen. Eine weit tiefere Untersuchung erfordert dagegen die Frage nach Kriterien, die jene Moduln, für die eine gegebene Zahl quadratischer Rest ist, von denen unterscheiden, für die sie Nichtrest ist.

Die reellen Einheiten $+1$ und -1 sind in der Arithmetik komplexer Zahlen tatsächlich Quadrate und daher auch quadratische Reste für *jeden* Modul. Ebenso leicht folgt aus dem Kriterium des vorigen Artikels, dass i, und ebenso $-i$, quadratischer Rest jedes Moduls ist, dessen Norm p die Form $8n+1$ hat, dagegen Nichtrest jedes Moduls, dessen Norm die Form $8n+5$ hat. Da es offenbar keinen Unterschied macht, ob m oder eine der dazu assoziierten Zahlen $im, -m, -im$ als Modul genommen wird, dürfen wir voraussetzen, dass der Modul die primäre Zahl unter seinen Assoziierten ist (Artikel 36, II). Setzen wir also den Modul $= a+bi$, so dürfen wir a als ungerade und b als gerade annehmen. Dann gilt stets $aa \equiv 1 \pmod 8$, während bb entweder $\equiv 0$ oder $\equiv 4 \pmod 8$ ist, je nachdem, ob b durch vier teilbar oder das Doppelte einer ungeraden Zahl ist. Somit sind $+i$ und $-i$ im ersten Fall offenbar quadratische Reste des Moduls, im zweiten Nichtreste.

58.

Da die Entscheidung über den Charakter einer zusammengesetzten Zahl, ob sie quadratischer Rest oder Nichtrest ist, von den Charakteren ihrer Faktoren abhängt, genügt es offenbar, die Entwicklung von Kriterien zur Unterscheidung der Moduln, für die eine gegebene Zahl k quadratischer Rest ist, von denen, für die sie Nichtrest ist, auf solche Werte von k zu beschränken, die Primzahlen und überdies primär unter ihren Assoziierten sind. Bei dieser Untersuchung liefert das *Untersuchen von Zahlenbeispielen* sogleich sehr elegante Sätze.

Beginnen wir mit der Zahl $1+i$, die sich als quadratischer Rest der Moduln

$$-1+2i,\ +3-2i,\ -5-2i,\ -1-6i,\ +5+4i,\ +5-4i,$$
$$-7,\ +7+2i,\ -5+6i,\quad \text{usw.}$$

und als quadratischer Nichtrest der folgenden erweist:

$$-1-2i,\ -3,\ +3+2i,\ +1+4i,\ +1-4i,\ -5+2i,$$
$$-1+6i,\ +7-2i,\ -5-6i,\ -3+8i,\ -3-8i,$$
$$+5+8i,\ +5-8i,\ +9+4i,\ +9-4i\quad \text{usw.}$$

Betrachten wir diese Übersicht aufmerksam, in die wir von je vier assoziierten Moduln stets den primären aufgenommen haben, so sehen wir leicht,

dass alle Moduln $a+bi$ in der ersten Klasse $a+b \equiv +1 \pmod 8$ erfüllen, die in der zweiten dagegen $a+b \equiv -3 \pmod 8$. Nehmen wir anstelle des primären Moduls m den Assoziierten $-m$, so muss dieses Kriterium offenbar dahin geändert werden, dass für Moduln der ersten Klasse $a+b \equiv -1$ und für die der zweiten $\equiv +3 \pmod 8$ gilt. So ist allgemein, sofern uns die Untersuchung der Zahlenbeispiele nicht getäuscht hat und $a+bi$ eine Primzahl bezeichnet, in der a ungerade. b gerade ist, $1+i$ ein quadratischer Rest oder Nichtrest derselben, je nachdem, ob $a+b \equiv \pm 1$ oder $\equiv \pm 3 \pmod 8$ gilt.

Für die Zahl $-1-i$ gilt dieselbe Regel wie für $1+i$. Betrachten wir dagegen $1-i$ als Produkt aus $-i$ und $1+i$, so kommt $1-i$ offenbar derselbe Charakter zu, der $1+i$ beizulegen ist, wenn b durch vier teilbar ist, dagegen der entgegengesetzte, wenn b das Doppelte einer ungeraden Zahl ist. Daraus folgt leicht, dass $1-i$ ein quadratischer Rest der Primzahl $a+bi$ ist, wenn $a-b \equiv \pm 1$ gilt, dagegen ein Nichtrest, wenn $a-b \equiv \pm 3 \pmod 8$ gilt; dabei ist stets a als ungerade und b als gerade vorauszusetzen.

Dieser zweite Satz lässt sich auch aus dem ersten mithilfe eines allgemeineren Satzes ableiten, den wir folgendermaßen aussprechen:

In der Theorie quadratischer Reste ist der Charakter der Zahl $\alpha+\beta i$ bezüglich des Moduls $a+bi$ derselbe wie der der Zahl $\alpha-\beta i$ bezüglich des Moduls $a-bi$.

Der Beweis dieses Satzes ergibt sich daraus, dass beide Moduln dieselbe Norm p haben und dass, wenn $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ durch $a+bi$ teilbar ist, auch $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ durch $a-bi$ teilbar ist, während, wenn $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ durch $a+bi$ teilbar ist, auch $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ durch $a-bi$ teilbar sein muss.

59.

Gehen wir nun zu ungeraden Primzahlen über.

Wir finden, dass $-1+2i$ ein quadratischer Rest der Moduln $+3+2i$, $+1-4i$, $-5+2i$, $-5-2i$, $-1-6i$, $+7-2i$, $-3+8i$, $+5+8i$, $+5-8i$, $+9+4i$ usw. ist,

ein Nichtrest dagegen der Moduln $-1-2i$, -3, $+3-2i$, $+1+4i$, $-1+6i$, $+5+4i$, $+5-4i$, -7, $+7+2i$, $-5+6i$, $-5-6i$, $-3-8i$, $+9-4i$ usw.

Führen wir die Moduln der ersten Klasse auf ihre absolut kleinsten Reste nach dem Modul $-1+2i$ zurück, so finden wir nur $+1$ und -1, nämlich $+3+2i \equiv -1$, $+1-4i \equiv -1$, $-5+2i \equiv +1$, $-5-2i \equiv -1$ usw.

Dagegen erweisen sich alle Moduln der zweiten Klasse nach dem Modul $-1+2i$ entweder $+i$ oder $-i$ kongruent.

Die Zahlen $+1, -1$ sind aber selbst quadratische Reste des Moduls $-1+2i$, während $+i$ und $-i$ dessen Nichtreste sind. Soweit man daher der Untersuchung von Zahlenbeispielen vertrauen darf, ergibt sich der folgende Satz: Die Zahl $-1+2i$ ist ein quadratischer Rest oder Nichtrest der Primzahl $a+bi$, je nachdem, ob diese ein quadratischer Rest oder Nichtrest von $-1+2i$ ist, sofern $a+bi$ unter den vier Assoziierten primär ist, oder vielmehr, wenn a ungerade und b gerade ist.

Aus diesem Satz folgen ohne Weiteres entsprechende Sätze über die Zahlen $+1-2i$, $-1-2i$, $+1+2i$.

60.

Untersuchen wir auf ähnliche Weise Zahlenbeispiele für -3 oder $+3$, so finden wir, dass beide quadratische Reste der Moduln $+3+2i$, $+3-2i$, $-1+6i$, $-1-6i$, -7, $-5+6i$, $-5-6i$, $-3+8i$, $-3-8i$, $+9+4i$, $+9-4i$ usw. sind,

Nichtreste dagegen von $-1+2i$, $-1-2i$, $+1+4i$, $+1-4i$, $-5+2i$, $-5-2i$, $+5+4i$, $+5-4i$, $+7+2i$, $+7-2i$, $+5+8i$, $+5-8i$ usw.

Die ersteren sind nach dem Modul 3 einer der vier Zahlen $+1, -1, +i, -i$ kongruent, die letzteren dagegen einer von $+1+i, +1-i, -1+i, -1-i$. Jene sind gerade die quadratischen Reste der Zahl 3, diese deren Nichtreste.

Diese Untersuchung von Zahlenbeispielen zeigt somit, dass die Primzahl $a+bi$, vorausgesetzt, dass a ungerade und b gerade ist, zur Zahl -3, und auch zu $+3$, dieselbe Beziehung hat wie diese zu jener, insofern eine ein quadratischer Rest oder Nichtrest der anderen ist.

Dehnen wir eine ähnliche Untersuchung auf andere Primzahlen aus, so finden wir dieses höchst elegante Reziprozitätsgesetz überall bestätigt und gelangen zu dem folgenden Fundamentalsatz über quadratische Reste in der Arithmetik komplexer Zahlen:

Bezeichnen $a+bi, A+Bi$ Primzahlen derart, dass a, A ungerade und b, B gerade sind, so ist entweder jede ein quadratischer Rest der anderen oder jede ein Nichtrest der anderen.

Trotz der großen Einfachheit des Satzes ist sein Beweis jedoch mit großen Schwierigkeiten verbunden. Bei diesen halten wir uns hier nicht auf, da der Satz selbst nur ein besonderer Fall eines allgemeineren Satzes ist, der den Inhalt der Theorie biquadratischer Reste gleichsam ausschöpft. Zu dieser gehen wir daher nun über.

61.

Was in Artikel 2 der vorigen Abhandlung über den Begriff des biquadratischen Restes und Nichtrestes gesagt wurde, dehnen wir auch auf die Arithmetik komplexer Zahlen aus. Wie dort beschränken wir auch hier die Untersuchung auf Moduln, die Primzahlen sind. Zugleich ist meist stillschweigend vorauszusetzen, dass der Modul so gewählt ist, dass er unter seinen Assoziierten primär, also $\equiv 1$ nach dem Modul $2+2i$ ist, und dass die Zahlen, deren Charakter als biquadratische Reste oder Nichtreste betrachtet wird, durch den Modul nicht teilbar sind.

Für einen gegebenen Modul könnten somit die durch ihn nicht teilbaren Zahlen in drei Klassen eingeteilt werden: Die erste enthielte die biquadratischen Reste, die zweite diejenigen biquadratischen Nichtreste, die quadratische Reste sind, die dritte die quadratischen Nichtreste.

Doch auch hier ist es besser, anstelle der dritten Klasse zwei aufzustellen, sodass es insgesamt vier gibt.

Wird eine beliebige primitive Wurzel als Basis genommen, so haben die biquadratischen Reste durch 4 teilbare Indizes, also solche der Form $4n$; diejenigen Nichtreste, die quadratische Reste sind, haben Indizes der Form $4n+2$; schließlich haben die quadratischen Nichtreste teils Indizes der Form $4n+1$, teils solche der Form $4n+3$. Auf diese Weise ergeben sich zwar vier Klassen, doch wäre der Unterschied zwischen den beiden letzten kein absoluter: Er hinge von der Wahl der als Basis genommenen primitiven Wurzel ab. Denn man sieht leicht, dass die eine Hälfte der primitiven Wurzeln einem gegebenen quadratischen Nichtrest einen Index der Form $4n+1$, die andere Hälfte einen Index der Form $4n+3$ gibt. Um diese Mehrdeutigkeit zu beseitigen, setzen wir stets eine primitive Wurzel voraus, bei der der Index $\frac{1}{4}(p-1)$ zur Zahl $+i$ gehört (vgl. Artikel 55, VI). So entsteht eine Klasseneinteilung, die sich kürzer und unabhängig von primitiven Wurzeln folgendermaßen aussprechen lässt.

Die *erste* Klasse enthalte diejenigen Zahlen k, für die $k^{\frac{1}{4}(p-1)} \equiv 1$ gilt; diese Zahlen sind die biquadratischen Reste des Moduls.

Die *zweite* Klasse enthalte diejenigen, für die $k^{\frac{1}{4}(p-1)} \equiv i$ gilt.

Die *dritte* diejenigen, für die $k^{\frac{1}{4}(p-1)} \equiv -1$ gilt.

Schließlich die *vierte* diejenigen, für die $k^{\frac{1}{4}(p-1)} \equiv -i$ gilt.

Die dritte Klasse enthält diejenigen biquadratischen Nichtreste, die quadratische Reste sind; die quadratischen Nichtreste verteilen sich auf die zweite und vierte Klasse.

Den Zahlen dieser Klassen legen wir der Reihe nach die *biquadratischen Charaktere* $0, 1, 2, 3$ bei. Definieren wir den Charakter λ einer Zahl k nach dem Modul m als den Exponenten jener Potenz von i, der die Zahl $k^{\frac{1}{4}(p-1)}$ kongruent ist, so sind offenbar nach dem Modul 4 kongruente Charaktere als gleichwertig anzusehen. Vorerst ist dieser Begriff auf Moduln beschränkt,

die Primzahlen sind: In der Fortsetzung dieser Untersuchungen werden wir zeigen, wie er auch auf zusammengesetzte Moduln angewandt werden kann.

62.

Um eine ausgedehnte Untersuchung von Zahlenbeispielen zu den Charakteren der Zahlen zu erleichtern, fügen wir hier eine übersichtliche Tabelle hinzu. Mit ihrer Hilfe lässt sich der Charakter jeder gegebenen Zahl bezüglich eines Moduls, dessen Norm den Wert 157 nicht übersteigt, mit wenig Arbeit erhalten, sofern die folgenden Bemerkungen beachtet werden.

Da der Charakter einer zusammengesetzten Zahl gleich der Summe der Charaktere ihrer einzelnen Faktoren oder ihr nach dem Modul 4 kongruent ist, genügt es, wenn wir für einen gegebenen Modul die Charaktere der Primzahlen angeben können. Da ferner die Charaktere der Einheiten $-1, i, -i$ offenbar den Zahlen $\frac{1}{2}(p-1), \frac{1}{4}(p-1), \frac{3}{4}(p-1)$ nach dem Modul 4 kongruent sind, genügt es auch, die Charaktere der unter ihren Assoziierten primären Zahlen anzugeben. Da schließlich nach dem Modul m kongruente Moduln denselben Charakter haben, genügt es, die Charaktere solcher Zahlen in die Tabelle aufzunehmen, die in einem System absolut kleinster Reste enthalten sind. Außerdem zeigt eine ähnliche Schlussfolgerung wie in Artikel 58, dass, wenn für den Modul $a + bi$ der Charakter der Zahl $A + Bi$ gleich λ ist und für den Modul $a - bi$ λ' der Charakter der Zahl $A - Bi$ ist, stets $\lambda \equiv -\lambda' \pmod 4$ gilt, oder gleichbedeutend $\lambda + \lambda'$ durch 4 teilbar ist. Daher genügt es, Moduln in die Tabelle aufzunehmen, in denen b entweder 0 oder positiv ist.

Wird zum Beispiel der Charakter der Zahl $11 - 6i$ bezüglich des Moduls $-5 - 6i$ gesucht, so ersetzen wir diese Zahlen durch $11 + 6i, -5 + 6i$. Sodann bestimmen wir (Artikel 43) den absolut kleinsten Rest der Zahl $11 + 6i$ nach dem Modul $-5+6i$; er ist $-1-4i = -1\times(1+4i)$. Da für den Modul $-5+6i$ der Charakter von -1 gleich 30, der Charakter der Zahl $1 + 4i$ nach der Tabelle dagegen 2 ist, ergibt sich 32 oder 0 als Charakter der Zahl $11 + 6i$ für den Modul $-5 + 6i$ und nach der letzten Bemerkung somit auch als Charakter der Zahl $11 - 6i$ für den Modul $-5 - 6i$. Wird ebenso der Charakter der Zahl $-5 + 6i$ bezüglich des Moduls $11 + 6i$ gesucht, so zerlegt sich ihr absolut kleinster Rest $1 - 5i$ in die Faktoren $-i\ 1 + i,\ 3 - 2i$, denen die Charaktere $117, 0, 1$ entsprechen. Der gesuchte Charakter ist daher 118 oder 2; derselbe Charakter ist auch der Zahl $-5 - 6i$ bezüglich des Moduls $11 - 6i$ beizulegen.

Modul.	Charakter.	Zahlen.
-3	3	$1+i$
$+3+2i$	3	$1+i$
$+1+4i$	1	$-1+2i$
	3	$1+i$
$-5+2i$	0	$-1-2i$
	1	$1+i$
	2	$-1+2i$
$-1+6i$	0	-3
	1	$1+i,\ -1+2i$

Modul.	Charakter.	Zahlen.
$-1+6i$	2	$-1-2i$
$+5+4i$	0	$1+i$
	1	-3
	3	$-1+2i,\ -1-2i$
-7	0	-3
	1	$-1+2i,\ 3-2i$
	2	$1+i$
	3	$-1-2i,\ 3+2i$
$+7+2i$	0	$1+i,\ 3+2i,\ 3-2i,\ 1-4i$
	1	-3
	2	$-1-2i,\ 1+4i$
	3	$-1+2i$
$-5+6i$	0	$1+i,\ -3,\ 3+2i,\ 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\ -1-2i$
$-3+8i$	0	$-1+2i,\ 3-2i,\ 1-4i$
	1	$1+i,\ 3+2i$
	2	-3
	3	$-1-2i,\ 1+4i,\ -5+2i$
$+5+8i$	0	$-1-2i$
	1	$-5-2i,\ -1+6i$
	2	$-1+2i,\ 3-2i$
	3	$1+i,\ -3,\ 3+2i,\ 1+4i,\ 1-4i$
$+9+4i$	0	$-1+2i,\ 3+2i$
	1	$1+i,\ -1-2i,\ 3-2i$
	2	$-3,\ 1+4i$
	3	$1-4i,\ -5+2i$
$-1+10i$	0	$1+i,\ -1+2i,\ -1-2i,\ 3+2i$
	1	-3
	2	$3-2i,\ -5+2i,\ 5-4i$
	3	$1+4i,\ 1-4i$

Modul.	Charakter.	Zahlen.
$+3+10i$	1	$1+i,\ -1-2i,\ 1-4i$
	2	$-3,\ 3+2i,\ 1+4i,\ -5-2i$
	3	$-1+2i,\ 3-2i$
$-7+8i$	0	$1+i,\ -7$
	1	$3+2i,\ 3-2i,\ 1-4i,\ -5-2i$
	2	$-1-2i,\ 1+4i,\ -5+2i,\ -1-6i$
	3	$-1+2i,\ -3,\ -1+6i$
-11	0	-3
	1	$1+i,\ 3-2i,\ 1+4i,\ -5+2i,\ 5+4i$
	2	$-1+2i,\ -1-2i$
	3	$3+2i,\ 1-4i,\ -5-2i,\ 5-4i$
$-11+4i$	0	$1+i,\ -1+2i,\ 3+2i,\ 5+4i$
	1	$-1-2i,\ -1+6i$
	2	$-5+2i$
	3	$-3,\ 3-2i,\ 1+4i,\ 1-4i,\ -5-2i$
$+7+10i$	0	$1+4i,\ 1-4i,\ -1+6i,\ -1-6i$
	1	$-1+2i,\ 3+2i,\ -5+2i$
	2	$1+i,\ 3-2i$
	3	$-1-2i,\ -3,\ -5-2i$
$+11+6i$	0	$1+i,\ -1+2i,\ -3,\ 1+4i,\ 1-4i,\ -7$
	1	$-1-2i,\ 3+2i,\ 3-2i$
	2	$-5-2i,\ -1+6i,\ 5-4i$
	3	$-5+2i,\ 5+4i,\ 7-2i.$

63.

Wir werden nun versuchen, durch die Untersuchung von Zahlenbeispielen gemeinsame Kriterien für die Moduln zu finden, für die eine gegebene Primzahl denselben Charakter hat. Die Moduln setzen wir stets als primär unter ihren Assoziierten voraus, also als solche Zahlen $a+bi$, für die entweder $a \equiv 1, b \equiv 0$ oder $a \equiv 3, b \equiv 2 \pmod 4$ gilt.

Für die Zahl $1+i$, mit der wir beginnen, lässt sich die in den Beispielen erkennbare Regel leichter erfassen, wenn wir die Moduln der ersten Art, für die $a \equiv 1, b \equiv 0$ gilt, von den Moduln der zweiten Art, für die $a \equiv 3, b \equiv 2$ gilt, trennen. Mithilfe der Tabelle des vorigen Artikels finden wir die folgenden Zuordnungen:

Charakter	Moduln der ersten Art.
0	$5+4i,\ -7+8i,\ -7-8i,\ -11+4i$
1	$1-4i,\ -3+8i,\ -3-8i,\ 9+4i,\ -11$
2	$5-4i,\ -7,\ -11-4i$
3	$-3,\ 1+4i,\ 5+8i,\ 5-8i,\ 9-4i$

Betrachten wir diese siebzehn Beispiele aufmerksam, so finden wir in allen den Charakter $\equiv \frac{1}{4}(a-b-1) \pmod 4$.

Ebenso gelten die Zuordnungen

Charakter	Moduln der zweiten Art.
0	$3-2i,\ -1-6i,\ 7+2i,\ -5+6i,\ -1+10i,\ 11+6i$
1	$-5+2i,\ -1+6i,\ 7-2i,\ -1-10i,\ 3+10i$
2	$-1+2i,\ -5-2i,\ 3-10i,\ 7+10i$
3	$-1-2i,\ 3+2i,\ -5-6i,\ 7-10i,\ 11-6i$

In allen diesen zwanzig Beispielen findet man bei einiger Aufmerksamkeit den Charakter $\equiv \frac{1}{4}(a-b-5) \pmod 4$.

Diese beiden Regeln lassen sich leicht zu einer für beide Arten von Moduln gültigen Regel zusammenfassen, wenn wir bedenken, dass $\frac{1}{4}bb$ für Moduln der ersten Art $\equiv 0$, für Moduln der zweiten Art dagegen $\equiv 1 \pmod 4$ ist. Somit ist der Charakter der Zahl $1+i$ bezüglich jedes primen, unter seinen Assoziierten primären Moduls $\equiv \frac{1}{4}(a-b-1-bb) \pmod 4$.

Nebenbei ist zu bemerken, dass, da $(b+1)^2$ stets die Form $8n+1$ hat oder gleichbedeutend $\frac{1}{4}(2b+bb)$ gerade ist, jener Charakter stets gerade oder ungerade ist, je nachdem, ob $\frac{1}{4}(a+b-1)$ gerade oder ungerade ist. Das stimmt mit der in Artikel 58 angegebenen Regel für den quadratischen Charakter überein.

Da $\frac{1}{4}(a-b-1), \frac{1}{4}(a-b+3)$ ganze Zahlen sind, von denen eine gerade, die andere ungerade ist, ist ihr Produkt gerade, oder gleichbedeutend $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod 4$. Daher kann anstelle des angegebenen Ausdrucks für den biquadratischen Charakter auch der folgende genommen werden:

$$\frac{1}{4}(a-b-1-bb) - \frac{1}{8}(a-b-1)(a-b+3) = \frac{1}{8}(-aa+2ab-3bb+1)$$

Diese Form empfiehlt sich auch dadurch, dass sie nicht auf primäre Moduln beschränkt ist, sondern nur voraussetzt, dass a ungerade und b gerade ist. Denn unter dieser Voraussetzung ist offenbar entweder $a + bi$ oder $-a - bi$ unter seinen Assoziierten primär, und der Wert jener Formel ist für beide Moduln derselbe.

64.

Gehen wir von der letzten im vorigen Artikel gefundenen Regel aus, so finden wir

Zahl	Charakter $\equiv$
$-1+i$	$\frac{1}{8}(aa+2ab-bb-1)$
$-1-i$	$\frac{1}{8}(-aa+2ab+bb+1)$
$+1-i$	$\frac{1}{8}(aa+2ab+3bb-1)$

Das folgt sogleich daraus, dass der Charakter von i gleich $\frac{1}{4}(aa+bb-1)$, der von -1 dagegen $\frac{1}{2}(aa+bb-1) \equiv \frac{1}{2}bb$ ist, da $aa-1$ stets die Form $8n$ hat. Diese vier Regeln sind offenbar, obwohl sie bisher aus der Untersuchung von Zahlenbeispielen gewonnen wurden, so miteinander verbunden, dass mit dem abgeschlossenen Beweis einer von ihnen zugleich die drei übrigen bewiesen sind. Es ist kaum nötig zu bemerken, dass auch in diesen Regeln nur a als ungerade und b als gerade vorausgesetzt wird.

Will man Formeln verwenden, die auf primäre Moduln beschränkt sind, so kann man die folgende Form benutzen:

Zahl	Charakter $\equiv$
$-1+i$	$\frac{1}{4}(-a-b+1-bb)$
$-1-i$	$\frac{1}{4}(a-b-1+bb)$
$+1-i$	$\frac{1}{4}(-a-b+1+bb)$

Die einfachsten Formeln ergeben sich, wenn wir wie zu Beginn unserer Untersuchung von Zahlenbeispielen Moduln der ersten und zweiten Art unterscheiden. Die Charaktere sind

Zahl	Für Moduln der ersten Art	Für Moduln der zweiten Art
$-1+i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b-3)$
$-1-i$	$\frac{1}{4}(a-b-1)$	$\frac{1}{4}(a-b+3)$
$+1-i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b+5)$

65.

Für die Zahl $-1+2i$, zu der wir nun übergehen, verwenden wir ebenfalls dieselbe Unterscheidung zwischen den Moduln $a+bi$, für die $a \equiv 1, b \equiv 0$ gilt, und denen, für die $a \equiv 3, b \equiv 2$ gilt. Die Tabelle in Artikel 62 zeigt für jene Zahl die folgenden Zuordnungen:

Charakter	Moduln der ersten Art
0	$-3+8i,\ +5-8i,\ +9+4i,\ -11+4i$
1	$+1+4i,\ +5-4i,\ -7,\ -3-8i$
2	$+1-4i,\ +5+8i,\ -7-8i,\ -11$
3	$-3,\ +5+4i,\ +9-4i,\ -7+8i,\ -11-4i$

Führen wir jeden dieser Moduln auf seinen absolut kleinsten Rest nach dem Modul $-1+2i$ zurück, so sehen wir, dass alle, denen der Charakter 0 entspricht, $\equiv 1$ sind; diejenigen, denen der Charakter 1 entspricht, sind $\equiv i$; diejenigen, deren Charakter 2 ist, werden $\equiv -1$; schließlich werden alle, deren Charakter 3 ist, $\equiv -i$. Die Charaktere der Zahlen $1, i, -1, -i$ für den Modul $-1+2i$ sind aber selbst der Reihe nach $0, 1, 2, 3$. Somit ist in allen diesen 17 Beispielen der Charakter der Zahl $-1+2i$ bezüglich eines Moduls $a+bi$ der ersten Art mit dem Charakter dieser Zahl bezüglich des Moduls $-1+2i$ identisch.

Ebenso findet man mithilfe der Tabelle die Zuordnungen

Charakter	Moduln der zweiten Art
0	$+3+2i,\ -5-2i,\ -1+10i,\ -1-10i,\ +11+6i$
1	$+3-2i,\ -1+6i,\ -5-6i,\ +7+10i,\ +7-10i$
2	$-5+2i,\ -1-6i,\ +7-2i$
3	$-1-2i,\ +7+2i,\ -5+6i,\ +3+10i,\ +3-10i,\ +11-6i$

Führt man diese Moduln auf ihre kleinsten Reste nach dem Modul $-1+2i$ zurück, so erweisen sich alle, denen der Reihe nach die Charaktere $0, 1, 2, 3$ entsprechen, den Zahlen $-1, -i, +1, +i$ kongruent. Diese Zahlen selbst haben aber, wenn umgekehrt $-1+2i$ als Modul genommen wird, der Reihe nach die Charaktere $2, 3, 0, 1$. Somit unterscheidet sich in allen diesen 19 Beispielen der Charakter der Zahl $-1+2i$ bezüglich eines Moduls der zweiten Art um zwei Einheiten vom Charakter dieser Zahl bezüglich der als Modul genommenen Zahl $-1+2i$.

Ferner sieht man ohne Mühe, dass für die Zahl $-1-2i$ ganz Ähnliches gilt.

66.

Für die Zahl -3 lassen wir die Unterscheidung zwischen Moduln der ersten und zweiten Art weg, da das Ergebnis zeigt, dass sie hier überflüssig ist. Es gelten somit die Zuordnungen

Charakter	Moduln
0	$-1+6i,\ -1-6i,\ -7,\ -5+6i,$ $-5-6i,\ -11,\ 11+6i,\ 11-6i$
1	$-1-2i,\ 1-4i,\ -5+2i,\ 5+4i,\ 7+2i,$ $5-8i,\ -1+10i,\ -7-8i,\ -11-4i,\ 7-10i$
2	$3+2i,\ 3-2i,\ -3+8i,\ -3-8i,$ $9+4i,\ 3+10i,\ 3-10i$
3	$-1+2i,\ 1+4i,\ -5-2i,\ 5-4i,\ 7-2i,$ $5+8i,\ -1-10i,\ -7+8i,\ -11+4i,\ 7+10i$

Führen wir diese Moduln auf ihre kleinsten Reste nach dem Modul 3 zurück, so sehen wir, dass diejenigen, denen der Charakter 0 entspricht, teils $\equiv 1$, teils $\equiv -1$ sind; diejenigen, deren Charakter 1 ist, werden entweder $\equiv 1-i$ oder $\equiv -1+i$; diejenigen, deren Charakter 2 ist, werden entweder $\equiv i$ oder $\equiv -i$; schließlich sind diejenigen, denen der Charakter 3 zukommt, entweder $\equiv 1+i$ oder $\equiv -1-i$. Aus dieser Untersuchung von Zahlenbeispielen schließen wir daher, dass der Charakter der Zahl -3 für einen Modul, der eine unter ihren Assoziierten primäre Primzahl ist, mit dem Charakter dieser Zahl selbst identisch ist, wenn 3 oder gleichbedeutend -3 als Modul betrachtet wird.

67.

Eine ähnliche Untersuchung von Zahlenbeispielen für andere Primzahlen zeigt, dass die Zahlen $3 \pm 2i, -1 \pm 6i, 7 \pm 2i, -5 \pm 6i$ usw. Sätze liefern, die dem in Artikel 65 für die Zahl $-1 + 2i$ gefundenen ähnlich sind, dass sich dagegen die Zahlen $1 \pm 4i, 5 \pm 4i, -3 \pm 8i, 5 \pm 8i, 9 \pm 4i$ usw. ebenso verhalten wie die Zahl -3. Die Untersuchung von Zahlenbeispielen führt somit zu einem höchst eleganten Satz,. den man entsprechend der Theorie quadratischer Reste in der Arithmetik reeller Zahlen den FUNDAMENTALSATZ der Theorie biquadratischer Reste nennen darf, nämlich:

Bezeichnen $a+bi, a'+b'i$ verschiedene, unter ihren jeweiligen Assoziierten primäre Primzahlen, also solche, die der Einheit nach dem Modul $2 + 2i$ kongruent sind, so ist der biquadratische Charakter der Zahl $a+bi$ bezüglich des Moduls $a'+b'i$ mit dem Charakter der Zahl $a'+b'i$ bezüglich des Moduls $a+bi$ identisch, wenn entweder beide Zahlen $a+bi, a'+b'i$ oder wenigstens eine von ihnen zur ersten Art gehören, also nach dem Modul 4 der Einheit kongruent sind. Dagegen unterscheiden sich jene Charaktere um zwei Einheiten, wenn keine der Zahlen $a + bi, a' + b'i$ zur ersten Art gehört, also wenn beide nach dem Modul 4 der Zahl $3 + 2i$ kongruent sind.

Trotz der großen Einfachheit dieses Satzes zählt sein Beweis jedoch zu den tiefsten Geheimnissen der höheren Arithmetik. Zumindest beim gegenwärtigen Stand lässt er sich nur durch die subtilsten Untersuchungen erschließen, die weit über die Grenzen der vorliegenden Abhandlung hinausgingen. Daher behalten wir uns die Veröffentlichung dieses Beweises sowie die Entwicklung des Zusammenhangs zwischen diesem Satz und jenen, die wir am Anfang dieser Abhandlung durch die Untersuchung von Zahlenbeispielen festzustellen begonnen haben, für eine dritte Abhandlung vor. Zum Abschluss geben wir jedoch schon hier an, was zum Beweis der in Artikel 63. 64 vorgeschlagenen Sätze erforderlich ist.

68.

Wir beginnen mit Primzahlen $a + bi$, für die $b = 0$ gilt (der dritten Art in Artikel 34). Damit die Zahl unter ihren Assoziierten primär ist, muss hier also a eine negative reelle Primzahl der Form $-(4n + 3)$ sein, für die wir $-q$ schreiben; solche Zahlen sind $-3, -7, -11, -19$ usw. Bezeichnet λ den Charakter der Zahl $1 + i$, wenn jene Zahl als Modul genommen wird, so muss gelten

$$i^\lambda \equiv (1+i)^{\frac{1}{4}(qq-1)} \equiv 2^{\frac{1}{8}(qq-1)} \cdot i^{\frac{1}{8}(qq-1)} \pmod{q}$$

Bekanntlich ist aber 2 ein quadratischer Rest oder Nichtrest von q, je nachdem, ob q die Form $8n + 7$ oder die Form $8n + 3$ hat. Daraus schließen wir, dass allgemein

$$2^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{4}(q+1)} \equiv i^{\frac{1}{2}(q+1)} \pmod{q}$$

gilt, und somit folgt durch Erheben zur Potenz mit dem Exponenten $\frac{1}{4}(q+1)$

$$2^{\frac{1}{8}(qq-1)} \equiv i^{\frac{1}{8}(q+1)^2} \pmod{q}$$

Die vorhergehende Gleichung nimmt daher die Form

$$i^\lambda \equiv i^{\frac{1}{8}(q+1)^2 + \frac{1}{8}(qq-1)} \equiv i^{\frac{1}{4}(qq+q)} \pmod{q}$$

an, woraus

$$\lambda \equiv \frac{1}{4}(qq+q) \equiv \frac{1}{4}(q+1)^2 - \frac{1}{4}(q+1) \pmod{4}$$

folgt; oder, da $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$ gilt, $\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(a-1) \pmod{4}$. Das ist gerade der Satz von Artikel 63 für den Fall $b = 0$.

69.

Viel schwieriger sind jedoch solche Moduln $a + bi$ zu behandeln, für die $b = 0$ nicht gilt (Zahlen der vierten Art aus Art. 34); mehrere Untersuchungen müssen daher vorausgehen. Die Norm $aa + bb$, die eine reelle Primzahl der Form $4n + 1$ sein wird, bezeichnen wir mit p.

Es sei S die Sammlung aller einfach kleinsten Reste für den Modul $a+bi = m$ unter Ausschluss der Null, sodass die Anzahl der in S enthaltenen Zahlen $= p - 1$ ist. Es bezeichne $x + yi$ eine beliebige Zahl dieses Systems, und wir setzen $ax + by = \xi, ay - bx = \eta$. Dann sind ξ, η ganze Zahlen zwischen den Grenzen 0 und p, *ohne die Grenzen selbst*. Denn im vorliegenden Fall, in dem a, b teilerfremd sind, zeigen die Formeln aus Art. 45, nämlich $\eta \equiv k\xi, \xi \equiv -k\eta \pmod{p}$, dass keine der Zahlen $\xi, \eta = 0$ sein kann, ohne dass die andere zugleich verschwindet, sodass $x = 0, y = 0$ wird; diese Kombination haben wir bereits ausgeschlossen. Das Kriterium dafür, dass die Zahl $x + yi$ in S enthalten ist, besteht also darin, dass die vier Zahlen $\xi, \eta, p - \xi, p - \eta$ positiv sind.

Ferner bemerken wir, dass für keine solche Zahl $\xi = \eta$ gelten kann. Daraus würde nämlich $p(x+y) = a(\xi+\eta)+b(\xi-\eta) = 2a\xi$ folgen, was widersinnig ist, da keiner der Faktoren $2, a, \xi$ durch p teilbar ist. Ebenso zeigt die Gleichung $p(x-y+a+b) = 2a\xi+(a+b)(p-\xi-\eta)$, dass $\xi+\eta = p$ nicht gelten kann. Da die Zahlen $\xi - \eta, p - \xi - \eta$ daher entweder positiv oder negativ sein müssen, gewinnen wir daraus eine Unterteilung des Systems S in vier Sammlungen C, C', C'', C''', denen wir die Zahlen folgendermaßen zuordnen:

In die Sammlung	Zahlen, für die
C	$\xi - \eta$ positiv, $p - \xi - \eta$ positiv
C'	$\xi - \eta$ positiv, $p - \xi - \eta$ negativ
C''	$\xi - \eta$ negativ, $p - \xi - \eta$ negativ
C'''	$\xi - \eta$ negativ, $p - \xi - \eta$ positiv

Das Kriterium für eine Zahl der Sammlung C ist also eigentlich sechsfach: Die sechs Zahlen $\xi, \eta, p - \xi, p - \eta, \xi - \eta, p - \xi - \eta$ müssen positiv sein. Doch die Bedingungen 2, 5 und 6 schließen die übrigen offenbar bereits ein. Entsprechendes gilt für die Sammlungen C', C'', C''', sodass die vollständigen Kriterien dreifach sind, nämlich:

Für die Sammlung	Folgende Zahlen müssen positiv sein
C	η, $\xi - \eta$, $p - \xi - \eta$
C'	$p - \xi$, $\xi - \eta$, $\xi + \eta - p$
C''	$p - \eta$, $\eta - \xi$, $\xi + \eta - p$
C'''	ξ, $\eta - \xi$, $p - \xi - \eta$

Auch ohne unseren Hinweis wird jeder leicht erkennen, dass bei der geometrischen Darstellung komplexer Zahlen (siehe Art. 39) die Zahlen des Systems S im Inneren des Quadrats liegen, dessen Seiten die Punkte verbinden, die die Zahlen $0, a+bi, (1+i)(a+bi), i(a+bi)$ darstellen, und dass die Unterteilung des Systems S der Teilung des Quadrats durch seine Diagonalen entspricht. Hier haben wir jedoch rein arithmetische Überlegungen vorgezogen und überlassen der Kürze halber die Veranschaulichung durch eine geometrische Darstellung dem erfahrenen Leser.

70.

Sind vier komplexe Zahlen $r = x + yi, r' = x' + y'i, r'' = x'' + y''i, r''' = x''' + y'''i$ so miteinander verbunden, dass $r' = m + ir, r'' = m + ir' = (1 + i)m - r, r''' = m + ir'' = im - ir$ gilt, und nimmt man an, dass die erste, r, zur Sammlung C gehört, so gehören die übrigen r', r'', r''' der Reihe nach zu den Sammlungen C', C'', C'''. Setzt man nämlich $\xi = ax + by, \eta = ay - bx, \xi' = ax' + by', \eta' = ay' - bx', \xi'' = ax'' + by'', \eta'' = ay'' - bx'', \xi''' = ax''' + by''', \eta''' = ay''' - bx'''$, so findet man

$$\begin{aligned} \eta = p - \xi' = p - \eta'' = \xi''' \\ \xi - \eta = \xi' + \eta' - p = \eta'' - \xi'' = p - \xi''' - \eta''' \\ p - \xi - \eta = \xi' - \eta' = \xi'' + \eta'' - p = \eta''' - \xi''' \end{aligned}$$

woraus die Richtigkeit des Satzes mithilfe der Kriterien unmittelbar folgt. Da wiederum $r = m + ir'''$ gilt, sieht man leicht: Gehört r nach Voraussetzung zu C', so gehören die Zahlen r', r'', r''' der Reihe nach zu C'', C''', C; gehört jene zu C'', so gehören diese zu C''', C, C'; und gehört jene schließlich zu C''', so gehören diese zu C, C', C''.

Zugleich folgt daraus, dass die einzelnen Sammlungen C, C', C'', C''' gleich viele Zahlen enthalten, nämlich $\frac{1}{4}(p-1)$.

37.

Satz. *Es bezeichne k eine ganze Zahl, die durch m nicht teilbar ist. Multipliziert man jede Zahl der Sammlung C mit k und verteilt die einfach kleinsten Reste der Produkte nach dem Modul m auf die Sammlungen C, C', C'', C''', wobei die Anzahlen der zu diesen einzelnen Sammlungen gehörigen Reste der Reihe nach mit c, c', c'', c''' bezeichnet werden, so ist der Charakter der Zahl k bezüglich des Moduls $m \equiv c' + 2c'' + 3c'''$ (mod 4).*

Beweis. Es seien jene c kleinsten Reste, die zu C gehören, $\alpha, \beta, \gamma, \delta$ usw.; ferner seien die c' Reste, die zu C' gehören, $m+i\alpha', m+i\beta', m+i\gamma', m+i\delta'$ usw.; weiter seien die c'' Reste, die zu C'' gehören, $(1+i)m-\alpha'', (1+i)m-\beta'', (1+i)m-\gamma'', (1+i)m-\delta''$ usw.; und schließlich seien die c''' Reste, die zu C''' gehören, $im-i\alpha''', im-i\beta''', im-i\gamma''', im-i\delta'''$ usw. Wir betrachten nun vier Produkte, nämlich:

1) das Produkt aus allen $\frac{1}{4}(p-1)$ Zahlen, die die Sammlung C bilden:

2) das Produkt der Produkte, die durch Multiplikation jeder dieser Zahlen mit k entstanden sind;

3) das Produkt aus den kleinsten Resten dieser Produkte, also aus den Zahlen $\alpha, \beta, \gamma, \delta$ usw., $m+i\alpha', m+i\beta'$ usw. usw.

4) das Produkt aus allen $c+c'+c''+c'''$ Zahlen $\alpha, \beta, \gamma, \delta$ usw., $\alpha', \beta', \gamma', \delta'$ usw., $\alpha'', \beta'', \gamma'', \delta''$ usw.

Bezeichnen wir diese vier Produkte der Reihe nach mit P, P', P'', P''', so gilt offenbar

$$P' = k^{\frac{1}{4}(p-1)}P, \quad P' \equiv P'', \quad P'' \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

und daher

$$Pk^{\frac{1}{4}(p-1)} \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

Es ist aber leicht zu sehen, dass die Zahlen $\alpha', \beta', \gamma', \delta'$ usw., $\alpha'', \beta'', \gamma''$, δ'' usw., $\alpha''', \beta''', \gamma''', \delta'''$ usw. sämtlich zur Sammlung C gehören und sowohl untereinander als auch von den Zahlen $\alpha, \beta, \gamma, \delta$ usw. verschieden sind, ebenso wie diese selbst untereinander verschieden sind. Alle diese Zahlen zusammen müssen daher, wenn man von ihrer Reihenfolge absieht, mit allen Zahlen, die die Sammlung C bilden, vollständig übereinstimmen. Daraus folgt $P = P'''$, also

$$Pk^{\frac{1}{4}(p-1)} \equiv Pi^{c'+2c''+3c'''} \pmod{m}$$

Da schließlich keiner der einzelnen Faktoren des Produkts P durch m teilbar ist, folgt

$$k^{\frac{1}{4}(p-1)} \equiv i^{c'+2c''+3c'''} \pmod{m}$$

sodass $c'+2c''+3c'''$ der Charakter der Zahl k bezüglich des Moduls m ist. Q. E. D.

72.

Um den allgemeinen Satz des vorigen Artikels auf die Zahl $1+i$ anzuwenden, müssen wir die Sammlung C erneut in zwei kleinere Sammlungen G und G' unterteilen. Zur Sammlung G rechnen wir die Zahlen $x+yi$, für die $ax+by = \xi$ kleiner als $\frac{1}{2}p$ ist, zur anderen Sammlung G' diejenigen, für die ξ größer als $\frac{1}{2}p$ ist. Die Anzahlen der in den Sammlungen G, G' enthaltenen Zahlen bezeichnen wir der Reihe nach mit g, g', sodass $g + g' = \frac{1}{4}(p-1)$ gilt.

Das vollständige Kriterium für die zu G gehörigen Zahlen besteht also darin, dass die drei Zahlen $\eta, \xi - \eta, p - 2\xi$ positiv sind. Denn die dritte Bedingung für die Sammlung C, nach der $p - \xi - \eta$ positiv sein muss, ist in diesen Bedingungen bereits enthalten, da $p - \xi - \eta = (\xi - \eta) + (p - 2\xi)$ gilt. Ebenso besteht das vollständige Kriterium für die zu G' gehörigen Zahlen in positiven Werten der drei Zahlen $\eta, p - \xi - \eta, 2\xi - p$.

Daraus folgt leicht, dass das Produkt einer beliebigen Zahl der Sammlung G mit der Zahl $1 + i$ zur Sammlung C''' gehört. Setzt man nämlich

$$(x + yi)(1 + i) = x' + y'i, \quad \text{und} \quad ax' + by' = \xi', \; ay' - bx' = \eta', \text{ erhält man}$$
$$\xi' = \xi - \eta, \quad \eta' - \xi' = 2\eta, \quad p - \xi' - \eta' = p - 2\xi$$

so ist das Kriterium dafür, dass die Zahl $x + yi$ zur Sammlung G gehört, identisch mit dem Kriterium dafür, dass die Zahl $x' + y'i$ zur Sammlung C''' gehört.

Auf genau dieselbe Weise zeigt man, dass das Produkt einer beliebigen Zahl der Sammlung G' mit $1 + i$ zur Sammlung C'' gehört.

Geben wir also im vorigen Artikel k den Wert $1+i$, so gilt $c = 0, c' = 0, c'' = g', c''' = g$, und der Charakter der Zahl $1 + i$ wird $3g + 2g' = \frac{1}{2}(p-1) + g$. Da die Charaktere der Zahlen $i, -1$ $\frac{1}{4}(p-1), \frac{1}{2}(p-1)$ sind, sind die Charaktere der Zahlen $-1 + i, -1 - i, 1 - i$ der Reihe nach $\frac{3}{4}(p-1) + g, g, \frac{1}{4}(p-1) + g$. Somit kommt es nun ganz auf die Bestimmung der Zahl g an.

73.

Was wir in den Art. 69—72 dargelegt haben, ist eigentlich unabhängig von der Voraussetzung, dass m eine primäre Zahl ist. Von nun an nehmen wir jedoch wenigstens an, dass a ungerade und b gerade ist und außerdem a, b und $a - b$ positive Zahlen sind. Zunächst müssen wir die Grenzen der Werte von x in der Sammlung G bestimmen.

Setzt man $ay - bx = \eta, (a + b)x - (a - b)y = \zeta, p - 2ax - 2by = \theta$, so besteht das Kriterium für die Zahlen $x + yi$, die zur Sammlung G gehören, in den drei Bedingungen, dass η, ζ, θ positive Zahlen sind. Da $px = (a - b)\eta + a\zeta, p(a - 2x) = a\theta + 2b\eta$ gilt, müssen offenbar x und $2a - x$ positive Zahlen sein, oder x muss einer der Zahlen $1, 2, 3 \ldots \frac{1}{2}(a - 1)$ gleich sein. Da ferner $(a - b)\theta = 2b\zeta + p(a - b - 2x)$ gilt, ist klar: Solange x kleiner als $\frac{1}{2}(a - b)$ ist, schließt die zweite Bedingung (nach der ζ positiv sein muss) die dritte (dass θ positiv sein muss) bereits ein. Ist dagegen x größer als $\frac{1}{2}(a - b)$, so ist die zweite Bedingung bereits in der dritten enthalten. Für die Werte von x, nämlich $1, 2, 3 \ldots \frac{1}{2}(a - b - 1)$, braucht man daher nur dafür zu sorgen, dass η und ζ positiv werden, oder dass y größer als $\frac{bx}{a}$ und kleiner als $\frac{(a+b)x}{a-b}$ ist. Für einen solchen gegebenen Wert von x beträgt die Gesamtzahl der Zahlen $x + yi$ somit

$$\left[\frac{(a + b)x}{a - b}\right] - \left[\frac{bx}{a}\right]$$

wenn wir die Klammern in derselben Bedeutung verwenden, in der wir sie bereits an verschiedenen anderen Stellen gebraucht haben (vgl. *Theorematis arithm. dem. nova*, Art. 4, und *Theorematis fund. in doctr. de residuis quadr.* usw., *Algorithm. nov.*, Art. 3). Für die Werte von x, nämlich $\frac{1}{2}(a-b+1), \frac{1}{2}(a-b+3) \ldots . \frac{1}{2}(a-1)$, genügt es dagegen, η und θ positive Werte zu geben, oder y größer als $\frac{bx}{a}$ und kleiner als $\frac{p-2ax}{2b}$ oder $\frac{1}{2}b + \frac{aa-2ax}{2b}$ zu machen. Für einen solchen gegebenen Wert von x beträgt die Gesamtzahl der Zahlen $x+yi$ daher

$$\left[\frac{1}{2}b + \frac{aa - 2ax}{2b}\right] - \left[\frac{bx}{a}\right]$$

Daraus folgt, dass die Anzahl der Zahlen der Sammlung G

$$g = \Sigma\left[\frac{(a + b)x}{a - b}\right] + \Sigma\left[\frac{1}{2}b + \frac{aa - 2ax}{2b}\right] - \Sigma\left[\frac{bx}{a}\right]$$

ist; dabei erstreckt sich die erste Summe über alle ganzzahligen Werte von x von 1 bis $\frac{1}{2}(a - b - 1)$, die zweite von $\frac{1}{2}(a - b + 1)$ bis $\frac{1}{2}(a - 1)$ und die dritte von 1 bis $\frac{1}{2}(a - 1)$.

Verwenden wir das Zeichen φ in derselben Bedeutung wie an der angeführten Stelle (*Theorematis fund.* usw., *Algor. nov.*, Art. 3), sodass also

$$\varphi(t,u) = \left[\frac{u}{t}\right] + \left[\frac{2u}{t}\right] + \left[\frac{3u}{t}\right] \ldots . + \left[\frac{t'u}{t}\right]$$

gilt, wobei t, u beliebige positive Zahlen und t' die Zahl $[\frac{1}{2}t]$ bezeichnen, so wird jener erste Term $= \varphi(a-b, a+b)$, der dritte $= -\varphi(a,b)$; der zweite wird dagegen

$$= \frac{1}{4}bb + \Sigma\left[\frac{aa-2ax}{2b}\right]$$

Schreibt man jedoch die Terme in umgekehrter Reihenfolge, so gilt

$$\begin{aligned}\Sigma\left[\frac{aa-2ax}{2b}\right] &= \left[\frac{a}{2b}\right] + \left[\frac{3a}{2b}\right] + \left[\frac{5a}{5b}\right] + \ldots . + \left[\frac{(b-1)a}{2b}\right] \\ &= \varphi(2b,a) - \varphi(b,a)\end{aligned}$$

Unsere Formel nimmt daher die folgende Gestalt an:

$$g = \varphi(a-b, a+b) + \varphi(2b,a) - \varphi(a,b) - \varphi(b,a) + \frac{1}{4}bb$$

Betrachten wir zunächst den Term $\varphi(a-b, a+b)$, der unmittelbar in $\varphi(a-b, 2b) + 1 + 2 + 3 +$ usw. $+ \frac{1}{2}(a-b-1)$ oder in

$$\varphi(a-b,2b) + \frac{1}{8}((a-b)^2 - 1)$$

übergeht.

Da ferner nach dem allgemeinen Satz $\varphi(t,u) + \varphi(u,t) = [\frac{1}{2}t] \,.\, [\frac{1}{2}u]$ gilt, wenn t, u teilerfremde positive ganze Zahlen sind, haben wir

$$\varphi(a-b,2b) = \frac{1}{2}b(a-b-1) - \varphi(2b, a-b)$$

und somit

$$\varphi(a-b,a+b) = \frac{1}{8}(aa+2ab-3bb-4b-1) - \varphi(2b,a-b)$$

Ordnen wir die Teile von $\varphi(2b, a-b)$ folgendermaßen an:

$$\left[\frac{a-b}{2b}\right] + \left[\frac{3(a-b)}{2b}\right] + \left[\frac{5(a-b)}{2b}\right] + \text{ usw. } + \left[\frac{(b-1)(a-b)}{2b}\right]$$
$$+ \left[\frac{a-b}{b}\right] + \left[\frac{2(a-b)}{b}\right] + \left[\frac{3(a-b)}{b}\right] + \text{ usw. } + \left[\frac{\frac{1}{2}b(a-b)}{b}\right]$$

Die zweite Reihe wird offenbar

$$\begin{aligned}&= \varphi(b, a-b) = \varphi(b,a) - 1 - 2 - 3 - \text{ usw. } - \frac{1}{2}b\\ &= \varphi(b,a) - \frac{1}{8}(bb+2b)\end{aligned}$$

Die erste Reihe stellen wir nach Umkehrung ihrer Gliederfolge so dar:

$$\begin{aligned}&\left[\frac{1}{2}(a+1-b) - \frac{a}{2b}\right] + \left[\frac{1}{2}(a+3-b) - \frac{3a}{2b}\right]\\ &+ \left[\frac{1}{2}(a+5-b) - \frac{5a}{2b}\right] + \text{usw.} + \left[\frac{1}{2}(a-1) - \frac{(b-1)a}{2b}\right]\end{aligned}$$

Dieser Ausdruck. Da für eine ganze Zahl t und eine gebrochene Zahl u allgemein $[t-u] = t-1-[u]$ gilt, geht er in den folgenden über:

$$\begin{aligned}&\frac{1}{8}b(2a-4-b) - \left[\frac{a}{2b}\right] - \left[\frac{3a}{2b}\right] - \left[\frac{5a}{2b}\right] - \text{ usw. } - \left[\frac{(b-1)a}{2b}\right]\\ &= \frac{1}{8}b(2a-4-b) - \varphi(2b,a) + \varphi(b,a)\end{aligned}$$

Daraus folgt

$$\varphi(2b, a-b) = 2\varphi(b,a) - \varphi(2b,a) + \frac{1}{4}b(a-3-b)$$

und daher

$$\varphi(a-b, a+b) = \varphi(2b,a) - 2\varphi(b,a) + \frac{1}{8}(aa-bb+2b-1)$$

Setzen wir diesen Wert in die oben angegebene Formel für g ein und außerdem $\varphi(a,b) + \varphi(b,a) = \frac{1}{4}b(a-1)$, so erhalten wir

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \frac{1}{8}(aa-2ab+bb+4b-1)$$

74.

Durch genau dieselben Überlegungen erledigt sich der Fall, in dem a, b positiv bleiben, aber $a-b$ negativ oder $b-a$ positiv ist. Die Gleichungen $p(a-2x) = 2b\eta + a\theta$, $p(b-a+2x) = 2b\zeta + (b-a)\theta$ zeigen, dass $\frac{1}{2}a - x$ und $x + \frac{1}{2}(b-a)$ positiv sein müssen und somit x einer der Zahlen $-\frac{1}{2}(b-a-1), -\frac{1}{2}(b-a-3), -\frac{1}{2}(b-a-5) \ldots + \frac{1}{2}(a-1)$ gleich sein muss. Ferner folgt aus der Gleichung $px + (b-a)\eta = a\zeta$, dass für negative Werte von x die Bedingung, nach der η positiv sein muss, bereits in der Bedingung enthalten ist, nach der ζ positiv sein muss; das Umgekehrte gilt, wenn x ein positiver Wert gegeben wird. Die Werte von y müssen daher für einen bestimmten negativen Wert von x zwischen $\frac{(a+b)x}{a-b}$ und $\frac{p-2ax}{2b}$, für einen positiven Wert von x dagegen zwischen $\frac{bx}{a}$ und $\frac{p-2ax}{2b}$ liegen. Für $x=0$ sind diese Grenzen offenbar 0 und $\frac{p-2ax}{2b}$, wobei der Wert $y=0$ selbst ausgeschlossen ist. Daraus folgt

$$g = -\Sigma\left[\frac{(a+b)x}{a-b}\right] + \Sigma\left[\frac{1}{2}b + \frac{aa-2ax}{2b}\right] - \Sigma\left[\frac{bx}{a}\right]$$

wobei sich die erste Summe über alle negativen Werte von. x von -1 bis $-\frac{1}{2}(b-a-1)$ erstreckt, die zweite über alle Werte von x von $-\frac{1}{2}(b-a-1)$ bis $\frac{1}{2}(a-1)$ und die dritte über alle positiven Werte von x von $+1$ bis $\frac{1}{2}(a-1)$. So ergibt die erste Summe $-\varphi(b-a, b+a)$, die zweite wie im vorigen Artikel $\frac{1}{4}bb + \varphi(2b,a) - \varphi(b,a)$ und schließlich die dritte $-\varphi(a,b)$, also gilt

$$g = -\varphi(b-a,b+a) + \varphi(2b,a) - \varphi(b,a) - \varphi(a,b) + \frac{1}{4}bb$$

Nun erhält man auf dieselbe Weise wie im vorigen Artikel

$$\begin{aligned}\varphi(b-a,b+a) &= \varphi(b-a,2b) - \frac{1}{8}((b-a)^2-1)\\ &= \frac{1}{8}(3bb-2ab-aa-4b+1) - \varphi(2b,b-a)\end{aligned}$$

sowie

$$\varphi(2b,b-a) = \varphi(2b,a) - 2\varphi(b,a) + \frac{1}{4}b(b-1-a)$$

und somit

$$\varphi(b-a,b+a) = 2\varphi(b,a) - \varphi(2b,a) + \frac{1}{8}(bb-aa-2b+1)$$

und schließlich

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \frac{1}{8}(aa-2ab+bb+4b-1)$$

Damit ist bewiesen, dass dieselbe Formel für g gilt, ob $a-b$ positiv oder negativ ist, sofern a, b positiv sind.

75.

Um eine weitere Reduktion zu erreichen, setzen wir

$$L = \left[\frac{a}{2b}\right] + \left[\frac{2a}{2b}\right] + \left[\frac{3a}{2b}\right] + \text{usw.} + \left[\frac{\frac{1}{2}ba}{2b}\right]$$

$$M = \left[\frac{(\frac{1}{2}b+1)a}{2b}\right] + \left[\frac{(\frac{1}{2}b+2)a}{2b}\right] + \left[\frac{(\frac{1}{2}b+3)a}{2b}\right] + \text{usw.} + \left[\frac{ba}{2b}\right]$$

$$N = \left[\frac{a+b}{2b}\right] + \left[\frac{2a+b}{2b}\right] + \left[\frac{3a+b}{2b}\right] + \text{usw.} + \left[\frac{\frac{1}{2}ba+b}{2b}\right]$$

Man sieht leicht, dass allgemein $[u]+[u+\frac{1}{2}] = [2u]$ gilt, welche reelle Größe u auch bezeichnen mag. Daher gilt $L+N = \varphi(b,a)$, und da offenbar $L+M = \varphi(2b,a)$ ist, folgt

$$\varphi(2b,a) - \varphi(b,a) = M - N$$

Ferner ist ersichtlich, dass die Summe aus dem ersten Glied der Reihe N und dem vorletzten Glied der Reihe M, nämlich $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right]$, $= \frac{1}{2}(a-1)$ wird und dass dieselbe Summe aus dem zweiten Glied der Reihe N und dem drittletzten Glied der Reihe M entsteht, und so weiter. Da auch das letzte Glied der Reihe $M = \frac{1}{2}(a-1)$ ist, das letzte Glied der Reihe N dagegen $= \left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$, wobei das obere oder untere Vorzeichen gilt, je nachdem a die Form $4n+1$ oder $4n-1$ hat, erhalten wir

$$M + N = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1)$$

und daher

$$\varphi(2b,a) - \varphi(b,a) = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1) - 2N$$

Die in den Art. 73 und 74 gefundene Formel für g geht somit in die folgende über:

$$g = \frac{1}{8}((a+b)^2 - 1) + 2n - 4N$$

wobei $a \mp 1 = 4n$ gesetzt wird und n eine ganze Zahl ist. Da daraus $1 = 16nn - 8an + aa$ folgt, lässt sich diese Formel auch so darstellen:

$$g = \frac{1}{8}(-aa + 2ab + bb + 1) + 4(\frac{1}{2}(a+1)n - nn - N)$$

Da g der Charakter der Zahl $-1-i$ für den Modul $a+bi$ ist, ist dieser Charakter daher $\equiv \frac{1}{8}(-aa+2ab+bb+1) \pmod 4$. Das ist genau der oben (Art. 64) durch Untersuchung von Beispielen gefundene Satz; daraus folgen unmittelbar die Sätze über die Charaktere der Zahlen $1+i$, $1-i$, $-1+i$. Somit sind diese vier Sätze für den Fall, dass a und b positiv sind, nun streng bewiesen.

76.

Bleibt a positiv und ist b negativ, so setzen wir $b = -b'$, sodass b' positiv wird. Es ist nun bewiesen, dass für den Modul $a + b'i$ der Charakter der Zahl $-1 - i \equiv \frac{1}{8}(-aa + 2ab' + b'b' + 1) \pmod 4$ ist. Daher ist der Charakter der Zahl $-1 + i$ für den Modul $a - b'i$ nach dem in Art. 62 angegebenen Satz $\equiv \frac{1}{8}(aa - 2ab' - b'b' - 1)$, das heißt, der Charakter der Zahl $-1 + i$ für den Modul $a + bi$ wird $\equiv \frac{1}{8}(aa + 2ab - bb - 1)$. Das ist genau der in Art. 64 angegebene Satz, aus dem die drei übrigen über die Charaktere der Zahlen $1 + i$, $1 - i$, $-1 - i$ unmittelbar folgen. Somit sind diese Sätze auch für den Fall bewiesen, dass b negativ ist, also für alle Fälle, in denen a positiv ist.

Ist schließlich a negativ, so setzen wir $a = -a'$, $b = -b'$. Nach dem bereits Bewiesenen ist der Charakter der Zahl $1 + i$ bezüglich des Moduls $a' + b'i$ $\equiv \frac{1}{8}(-a'a' + 2a'b' - 3b'b' + 1) \pmod 4$, und es ist gleichgültig, ob wir die Zahl $a' + b'i$ oder ihre entgegengesetzte Zahl $-a' - b'i$ als Modul nehmen. Also ist der Charakter der Zahl $1 + i$ bezüglich des Moduls $a + bi$ offenbar $\equiv \frac{1}{8}(-aa + 2ab - 3bb + 1)$, und Entsprechendes gilt für die Charaktere der Zahlen $1 - i$, $-1 + i$, $-1 - i$.

Daraus schließen wir, dass der Beweis der Sätze über die Charaktere der Zahlen $1 + i$, $1 - i$, $-1 + i$, $-1 - i$ (Art. 63. 64) keiner Einschränkung mehr unterliegt.

BESPRECHUNGEN

EIGENER

SCHRIFTEN.

Göttingische gelehrte Anzeigen. 1808 Mai 12.

Eine vom Herrn Professor Gauss am 15. Januar dieses Jahres der Königlichen Gesellschaft der Wissenschaften vorgelegte Abhandlung,

Theorematis arithmetici demonstratio nova,

deren Inhalt wir hier noch vorstellen müssen, behandelt den berühmten Fundamentalsatz der Lehre von den quadratischen Resten, der sowohl in der gesamten *höheren Arithmetik* als auch in den angrenzenden Teilen der Analysis eine so wichtige Rolle spielt. Bekanntlich heißt eine ganze Zahl a *quadratischer Rest* der ganzen Zahl b, wenn es Zahlen der Form $xx - a$ gibt, die durch b teilbar sind; im entgegengesetzten Fall heißt a *quadratischer Nichtrest* von b. Die Zahl a kann positiv oder negativ sein, b wird dagegen stets als positiv angesehen. Die höhere Arithmetik lehrt, dass alle Primzahlen b, für die eine gegebene Zahl a quadratischer Rest ist, in bestimmten linearen Formen enthalten sind, während andere lineare Formen alle Primzahlen enthalten, von denen a Nichtrest ist. So ist zum Beispiel -1 quadratischer Rest aller Primzahlen der Form $4n+1$ und quadratischer Nichtrest aller Primzahlen der Form $4n+3$; ferner ist $+2$ quadratischer Rest aller Primzahlen der Formen $8n+1$, $8n+7$, dagegen quadratischer Nichtrest aller Primzahlen der Formen $8n+3$, $8n+5$. Es gibt unendlich viele ähnliche spezielle Sätze; sie alle lassen sich aber aus der Verbindung der beiden angeführten mit dem folgenden allgemeinen Satz ableiten: Zwei verschiedene positive (ungerade) Primzahlen, p, q, stehen stets in *derselben* wechselseitigen Beziehung (das heißt, die eine ist quadratischer Rest oder Nichtrest der anderen, je nachdem die andere Rest oder Nichtrest der ersten ist), wenn entweder beide die Form $4n+1$ haben oder wenigstens eine diese Form hat. Ihre wechselseitige Beziehung ist dagegen entgegengesetzt (das heißt, die eine ist Nichtrest der anderen, wenn diese Rest von jener ist, und umgekehrt), wenn *beide* zugleich die Form $4n+3$ haben. Das ist der erwähnte Fundamentalsatz, den man in mehr als einer Gestalt ausdrücken kann. Die hier gewählte ist diejenige, in der er in der Abhandlung des Herrn Professor Gauss neu bewiesen wird.

Die schönsten Sätze der höheren Arithmetik, insbesondere auch die hier behandelten, haben die Eigenart, dass sie anhand von Zahlenbeispielen leicht entdeckt werden können, ihre Beweise dagegen äußerst tief verborgen liegen und nur durch sehr tiefgehende Untersuchungen aufzuspüren sind. Gerade das verleiht der höheren Arithmetik jenen zauberischen Reiz, der sie zum Lieblingsgebiet der führenden Mathematiker gemacht hat, ganz abgesehen von ihrem unerschöpflichen Reichtum, in dem sie alle anderen Teile der reinen Mathematik so weit übertrifft. Die beiden oben erwähnten speziellen Sätze

waren schon FERMAT bekannt, der nach eigener Aussage auch ihre Beweise besaß. Ob er sich darin täuschte, können wir nicht entscheiden, da er nie etwas darüber veröffentlicht hat. Für möglich dürfen wir es aber gewiss halten, da es mehrere Beispiele von Selbsttäuschung bei anderen großen Mathematikern gibt, insbesondere bei EULER, LEGENDRE und auch bei FERMAT selbst. Den ersten Beweis des ersten dieser Sätze gab EULER. Den anderen zu beweisen gelang diesem großen Mathematiker jedoch trotz seiner eifrigen, über viele Jahre fortgesetzten Bemühungen nicht; erst LAGRANGE war es vorbehalten, diese Lücke zu schließen. Beide Mathematiker bewiesen auch verschiedene andere spezielle Sätze; eine größere Anzahl aber, die sie anhand von Zahlenbeispielen fanden, entzog sich stets ihren Beweisversuchen. Es ist indessen ein merkwürdiges Spiel des Zufalls, dass beide Mathematiker auf diesem Weg nicht den allgemeinen Fundamentalsatz entdeckten, der sich so einfach formulieren lässt. Zuerst hat ihn, wenn auch in etwas anderer Gestalt, LEGENDRE in der *Histoire de l'Académie des Sciences de Paris* 1785 vorgetragen. Sowohl dort als auch später in seinem Werk *Essai d'une théorie des nombres* versuchte dieser ausgezeichnete Analyst, den Beweis auf sehr scharfsinnige Untersuchungen zu gründen. Diese führten dennoch nicht zum gewünschten Ziel, das, wenn wir uns nicht irren, auf diesem Weg auch nicht erreicht werden konnte.

Der Verfasser der Abhandlung, der diese Besprechung gewidmet ist, betrat das Gebiet der höheren Arithmetik zu einer Zeit, als ihm alle früheren Arbeiten anderer Mathematiker auf diesem Gebiet völlig unbekannt waren. Diesem Umstand ist hauptsächlich zuzuschreiben, dass er überall einen ganz eigenen Weg eingeschlagen hat. Jenen Fundamentalsatz fand er zwar schon sehr früh anhand von Zahlenbeispielen; doch erst ein ganzes Jahr später gelang es ihm nach vielen Schwierigkeiten und vergeblichen Versuchen, den ersten vollkommen strengen Beweis zu finden, der im vierten Abschnitt seiner *Disquisitiones Arithmeticae* entwickelt wird. Dieser Beweis beruht jedoch auf sehr mühsamen und weitläufigen Ausführungen. Später fand er noch drei andere Beweise, die zwar von dieser Unbequemlichkeit frei sind, dafür aber andere sehr tiefgehende und ihrem Inhalt nach völlig andersartige Untersuchungen voraussetzen. Einer dieser Beweise ist ebenfalls im angeführten Werk in Art. 262 mitgeteilt; die beiden anderen werden zu gegebener Zeit bekannt gemacht werden. Es blieb also immer der Wunsch, einen kürzeren Beweis zu finden, der von andersartigen Untersuchungen unabhängig wäre. Der Verfasser hofft daher, dass die Freunde der höheren Arithmetik mit Vergnügen einen fünften Beweis aufnehmen werden, der in der vorliegenden Abhandlung auf weniger als fünf Seiten dargestellt wird und in jeder Hinsicht nichts zu wünschen übrig zu lassen scheint. Bei der gedrängten Kürze dieses Beweises können wir hier freilich nur eine unvollkommene Vorstellung von seinem Verlauf geben. Mehr

wäre hier umso überflüssiger, als der Band XVI der *Commentationes*, in dem er bereits abgedruckt ist, demnächst erscheinen wird.

Die Grundlage des Beweises ist der folgende neue Satz: Es sei p eine (positive ungerade) Primzahl und k eine beliebige ganze Zahl, die durch p nicht teilbar ist. Wenn ferner unter den Resten, die bei der Division der $\frac{1}{2}(p-1)$ Produkte k, $2k$, $3k \ldots . \frac{1}{2}(p-1)k$ durch p entstehen, insgesamt μ größer als $\frac{1}{2}p$ sind (also $\frac{1}{2}(p-1) - \mu$ kleiner als $\frac{1}{2}p$), so ist k quadratischer Rest von p, wenn μ gerade ist, dagegen quadratischer Nichtrest, wenn μ ungerade ist. Die Zahl μ, die nur von k und p abhängt, bezeichnen wir mit dem Zeichen (k, p). Durch eine Folge von Schlüssen, die sich nicht auszugsweise wiedergeben lassen, wird nun gezeigt, dass für zwei teilerfremde ungerade Zahlen k und p die Zahl $(k, p) + (p, k) + \frac{1}{4}(k-1)(p-1)$ stets *gerade* ist. Daraus folgt, dass immer dann, wenn k und p beide die Form $4n+3$ haben, eine der Zahlen (k, p), (p, k) gerade und die andere ungerade sein muss. In allen anderen Fällen dagegen, also wenn beide Zahlen k und p oder wenigstens eine von ihnen die Form $4n+1$ haben, müssen entweder $.(k, p)$, (p, k) beide zugleich gerade oder beide zugleich ungerade sein. Zusammen mit dem obigen Satz ergibt sich daraus der Fundamentalsatz unmittelbar.—Auf demselben Weg, auf dem diese Ergebnisse gefunden werden, wird in der Abhandlung zugleich ein neuer Beweis der beiden oben erwähnten speziellen Sätze gegeben: Man zeigt nämlich leicht, dass $(-1, p) = \frac{1}{2}(p-1)$ gilt, also eine gerade oder ungerade Zahl ist, je nachdem p die Form $4n+1$ oder $4n+3$ hat; ebenso gilt $(2, p) = \frac{1}{4}(p-1)$, wenn p die Form $4n+1$ hat, und $(2, p) = \frac{1}{4}(p+1)$, wenn p die Form $4n+3$ hat. Daher ist $(2, p)$ gerade, wenn p die Form $8n+1$ oder $8n+7$ hat, dagegen ungerade, wenn p die Form $8n+3$ oder $8n+5$ hat.

Göttingische Gelehrte Anzeigen. 1808 September 19.

Eine vom Herrn Professor Gauss der Königlichen Gesellschaft der Wissenschaften vorgelegte Vorlesung,

Summatio quarumdam serierum singularium,

soll eine bemerkenswerte Untersuchung zur Kreisteilung, deren Grundlage bereits in den *Disquisitionibus Arithmeticis* gelegt war, ausführlicher und in größerer Allgemeinheit entwickeln, sie mit vollständigen Beweisen versehen und ihren unerwarteten Zusammenhang mit anderen wichtigen Wahrheiten zeigen. Es bezeichne n eine Primzahl, k eine beliebige ganze Zahl, die durch n nicht teilbar ist, und ω den Bogen $\frac{1}{n}360°$. Die verschiedenen, unter den Zahlen $1, 2, 3, 4, \ldots . n-1$ vorkommenden quadratischen Reste von n seien mit a, a', a'' usw. bezeichnet; die nach deren Ausschluss verbleibenden Zahlen, also die quadratischen Nichtreste von n, dagegen mit b, b', b'' usw. Dann ist im angeführten Werk in Art. 356 bewiesen, dass in dem Fall, in dem n die Form $4n+1$ hat,

$$\left.\begin{array}{l}\cos ak\omega + \cos a'k\omega + \cos a''k\omega + \text{usw.} \\ -\cos bk\omega - \cos b'k\omega - \cos b''k\omega - \text{usw.}\end{array}\right\} = \pm\sqrt{n}.$$

und

$$\left.\begin{array}{l}\sin ak\omega + \sin a'k\omega + \sin a''k\omega + \text{usw.} \\ -\sin bk\omega - \sin b'k\omega - \sin b''k\omega - \text{usw.}\end{array}\right\} = 0$$

gilt, während in dem Fall, in dem n die Form $4m+3$ hat, die Summe der ersten Reihe $= 0$ und die der zweiten $= \pm\sqrt{n}$ wird. Das Vorzeichen der Wurzelgröße hängt vom Wert der Zahl k oder vielmehr von ihrer Beziehung zu n ab und lässt sich für *alle* Werte von k bei einem gegebenen Wert von n leicht bestimmen, sobald es für *einen* bestimmt ist. Man kann nämlich zeigen, dass für alle Werte von k, die quadratische Reste von n sind, stets *dasselbe* Vorzeichen gilt und dann das entgegengesetzte für alle quadratischen Nichtreste von n. Da die Untersuchung im angeführten Werk bereits so weit geführt war und nur noch die Bestimmung des Vorzeichens für irgendeinen Wert von k fehlte, hätte man glauben sollen, dass sich nach Erledigung der Hauptsache diese genauere Bestimmung leicht ergänzen ließe. Das lag umso näher, als die Untersuchung von Zahlenbeispielen sofort ein äußerst einfaches Ergebnis liefert: Für $k = 1$ oder für alle Werte, die quadratische Reste von n sind, muss die Wurzelgröße in den obigen Formeln stets *positiv* genommen werden. Doch bei der Suche nach einem Beweis dieser Beobachtung stoßen wir auf ganz unerwartete Schwierigkeiten. Das Verfahren, das so befriedigend zur

Bestimmung des absoluten Werts jener Reihen führte, erweist sich als völlig unzureichend, wenn die Vorzeichen vollständig bestimmt werden sollen. Den *metaphysischen* Grund dieses Phänomens (um den bei französischen Mathematikern üblichen Ausdruck zu gebrauchen) muss man darin suchen, dass die Analysis bei der Kreisteilung zwischen den Bögen $\omega, 2\omega, 3\omega \ldots (n-1)\omega$ keinen Unterschied macht, sondern sie alle auf dieselbe Weise erfasst. Da die Untersuchung dadurch ein neues Interesse erhält, fand Herr Professor Gauss darin gewissermaßen eine Aufforderung, nichts unversucht zu lassen, um die Schwierigkeit zu überwinden. Erst nach vielen und verschiedenartigen vergeblichen Versuchen gelang ihm dies auf einem auch für sich bemerkenswerten Weg. Er geht nämlich von der Summation einiger Reihen aus, deren Glieder die folgende Form haben:

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)\ (1-xx)\ (1-x^3)\ldots.(1-x^\mu)}$$

Bezeichnen wir der Kürze halber eine solche Funktion mit (m, μ), die, wie in der Abhandlung gezeigt wird, stets ein *Polynom* in x ist, so brechen die Reihen

$$1-(m,1)+(m,2)-(m,3)+\text{usw.}$$

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+\text{usw.}$$

nach dem Glied an Stelle $m+1$ ab, sofern m eine positive ganze Zahl bezeichnet. Für gerade Werte von m wird die Summe der ersten Reihe

$$=(1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1})$$

und $=0$ für ungerade Werte von m; die Summe der zweiten Reihe wird dagegen stets

$$=(1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}})\ldots(1+x^{\frac{1}{2}m})$$

Auch für gebrochene und negative Werte von m führt die Summation dieser Reihen zu interessanten Ergebnissen, obwohl diese für den gegenwärtigen Zweck nicht nötig sind. Wir begnügen uns damit, hier nur eines davon anzugeben. Die unendliche Reihe

$$1+x+x^3+x^6+x^{10}+\text{usw.}$$

deren Exponenten die Dreieckszahlen sind, ist das Produkt aus den Faktoren

$$\frac{1-xx}{1-x}\times\frac{1-x^4}{1-x^3}\times\frac{1-x^6}{1-x^5}\times\frac{1-x^8}{1-x^7}\ \text{usw.}$$

oder, wenn man es vorzieht, aus

$$(1+x)^2(1+xx)^2(1+x^3)^2(1+x^4)^2 \text{ usw.}$$

multipliziert mit

$$(1-x)(1-xx)1-x^3)(1-x^4) \text{ usw.}$$

Darzulegen, wie diese Summationen auf den Hauptgegenstand angewandt werden, würde uns hier zu weit führen. Wir dürfen die Leser umso eher auf die Abhandlung selbst verweisen, als sie bald im Druck erscheinen wird. Die oben angeführten Summationen sind nur ein spezieller Fall der Summation der folgenden Reihen:

$$1+\cos k\omega+\cos 4k\omega+\cos 9k\omega+\text{usw.}+\cos(n-1)^2k\omega=T$$

$$\sin k\omega+\sin 4k\omega+\sin 9k\omega+\text{usw.}+\sin(n-1)^2k\omega=U$$

die in der Abhandlung für alle Werte von k und ohne die Einschränkung behandelt wird, dass n eine Primzahl sein muss. Es wird nämlich gezeigt, dass

$$T=\pm\sqrt{n},\quad T=\pm\sqrt{n},\quad T=0,\quad T=0$$

und

$$U=\pm\sqrt{n},\quad U=0,\quad U=0,\quad U=\pm\sqrt{n}$$

gilt, je nachdem n die Formen $4m, 4m+1, 4m+2, 4m+3$ der Reihe nach hat. Das Vorzeichen der Wurzelgröße hängt hier wiederum von k ab. Seine Bestimmung, die die Unterscheidung vieler einzelner Fälle erfordert, wird auf zwei verschiedenen Wegen so entwickelt und bewiesen, dass nichts zu wünschen übrig bleiben wird. Der Vergleich dieser beiden Wege führt außerdem zu dem folgenden sehr bemerkenswerten Satz: Ist n das Produkt aus beliebig vielen verschiedenen ungeraden Primzahlen a, b, c, d usw., von denen insgesamt μ die Form $4m+3$ haben, und kommen unter jenen Faktoren insgesamt ν vor, von denen jeder das Produkt der übrigen (also der Reihe nach $\frac{n}{a}, \frac{n}{b}, \frac{n}{c}, \frac{n}{d}$ usw.) zum quadratischen Nichtrest hat, so ist ν gerade, wenn μ die Form $4m$ oder $4m+1$ hat, dagegen ungerade, wenn μ die Form $4m+2$ oder $4m+3$ hat. Der bekannte Fundamentalsatz über die quadratischen Reste ist nur ein spezieller Fall dieses Satzes; umgekehrt lässt sich der eben angegebene Satz leicht aus diesem Fundamentalsatz ableiten. Durch diese Untersuchungen besitzt man also zugleich einen vierten Beweis dieses wichtigen Satzes, den der Verfasser zuerst auf zwei ganz verschiedenen Wegen in den *Disquisitionibus Arithmeticis* und vor Kurzem auf einem dritten, ebenso verschiedenen Weg in einer eigenen Abhandlung bewiesen hatte.

Göttingische gelehrte Anzeigen. 1817 März 10.

Am 10. Februar reichte Herr Hofrat Gauss der Königlichen Gesellschaft eine Vorlesung mit dem Titel ein:

Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae.

Es ist eine Besonderheit der höheren Arithmetik, dass sich so viele ihrer schönsten Sätze mit größter Leichtigkeit durch die Untersuchung von Zahlenbeispielen entdecken lassen, während ihre Beweise keineswegs naheliegen. Oft findet man diese erst nach vielen vergeblichen Versuchen mithilfe tiefgehender Untersuchungen und glücklicher Kombinationen. Dieses bemerkenswerte Phänomen entspringt der oft wunderbaren Verknüpfung der verschiedenartigen Lehren in diesem Teil der Mathematik. Eben deshalb lassen sich Sätze, für die man anfangs jahrelang vergeblich einen Beweis gesucht hatte, später häufig auf mehreren ganz verschiedenen Wegen beweisen. Sobald ein neuer Satz anhand von Zahlenbeispielen entdeckt ist, muss man die Auffindung *irgendeines* Beweises freilich als erstes Erfordernis ansehen. Ist dies aber gelungen, so darf man in der höheren Arithmetik die Untersuchung nicht immer für abgeschlossen und die Suche nach anderen Beweisen für überflüssigen Luxus halten. Denn zum einen findet man gewöhnlich die schönsten und einfachsten Beweise nicht zuerst; zum anderen macht gerade die Einsicht in die wunderbare Verknüpfung der Wahrheit der höheren Arithmetik einen Hauptreiz dieses Studiums aus und führt nicht selten wiederum zur Entdeckung neuer Wahrheiten. Aus diesen Gründen ist hier die Auffindung neuer Beweise für schon bekannte Wahrheiten oft als mindestens ebenso wichtig anzusehen wie die Entdeckung der Wahrheit selbst. Kennern der höheren Arithmetik sind diese Überlegungen nicht neu. Bekanntlich besteht ein großer Teil von Eulers Verdiensten um sie darin, Beweise für Sätze gefunden zu haben, die schon Fermat, wie es scheint anhand von Zahlenbeispielen, entdeckt hatte.

Die Lehre von den quadratischen Resten veranschaulicht das eben Gesagte. Sie beruht hauptsächlich auf dem sogenannten Fundamentaltheorem: Die wechselseitigen Beziehungen zweier (ungerader positiver) Primzahlen zueinander (insofern die eine quadratischer Rest oder Nichtrest der anderen ist) sind gleich, wenn eine oder beide Primzahlen die Form $4k+1$ haben, dagegen entgegengesetzt, wenn beide Primzahlen die Form $4k+3$ haben. Für Leser, die mit der höheren Arithmetik weniger vertraut sind, erinnern wir daran, dass eine ganze Zahl quadratischer Rest einer anderen heißt, wenn die erste durch Addition eines Vielfachen der zweiten ein Quadrat ergeben kann; Nichtrest dagegen, wenn dies unmöglich ist. Die Geschichte dieses schönen Satzes,

der sich anhand von Zahlenbeispielen äußerst leicht finden lässt, wollen wir hier nicht vollständig wiederholen. Wir bemerken nur, dass der Verfasser der vorliegenden Abhandlung nach anfangs ziemlich lange vergeblich angestellten Untersuchungen nach und nach bereits vier ganz verschiedene Beweise gegeben hat. Zwei davon stehen in den *Disquisitionibus Arithmeticis*; der dritte bildet den Gegenstand einer eigenen Abhandlung im sechzehnten Band der Commentationes, und der vierte ist in die Abhandlung *summatio quarumdam serierum singularium* im ersten Band der *Commentationes recentiores* eingearbeitet. Zu diesen beiden Abhandlungen kann man unsere Besprechungen von 1808, Mai 12 und September 19, heranziehen; dort finden sich auch ausführlichere historische Nachweise. Dass der Verfasser bei diesen vier Beweisen nicht stehen geblieben ist, obwohl jeder für sich an Strenge nichts zu wünschen übrig lässt, bedarf bei den Freunden der höheren Arithmetik keiner Rechtfertigung. Dennoch hätte er sich wahrscheinlich nicht so eifrig bemüht, noch weitere Beweise hinzuzufügen, wenn ihn nicht ein besonderer Umstand dazu veranlasst hätte, der hier erwähnt werden muss. Seit dem Jahr 1805 hatte er begonnen, sich mit den Theorien der kubischen und biquadratischen Reste zu beschäftigen, die noch weitaus reichhaltiger und interessanter sind als die Theorie der quadratischen Reste. Bei diesen Untersuchungen zeigten sich dieselben Erscheinungen wie bei jener, nur gleichsam in vergrößertem Maßstab. Sobald der richtige Weg eingeschlagen war, fand man anhand von Zahlenbeispielen sogleich eine Anzahl höchst einfacher Sätze, die diese Theorien ganz ausschöpfen, den Sätzen über quadratische Reste überraschend ähnlich sind und insbesondere auch ein Gegenstück zum Fundamentaltheorem bieten. Doch waren hier die Schwierigkeiten, völlig befriedigende Beweise für diese Sätze zu finden, noch viel größer. Erst nach vielen Versuchen, die über eine beträchtliche Reihe von Jahren fortgesetzt wurden, erreichte der Verfasser schließlich sein Ziel. Die große Analogie zwischen den Sätzen über quadratische und über höhere Reste ließ vermuten, dass es auch für beide analoge Beweise geben müsse. Die zuerst für quadratische Reste gefundenen Beweisarten ließen sich jedoch auf höhere Reste überhaupt nicht anwenden; gerade dies war der Beweggrund, für die ersteren immer weitere neue Beweise zu suchen. Der Verfasser wünscht daher, dass man die vorliegende Abhandlung, die noch einige neue Hilfsmittel für die Theorie der quadratischen Reste erschließt, als Vorläuferin der Theorie der kubischen und biquadratischen Reste betrachtet. Diese will er künftig veröffentlichen; ihre Gegenstände gehören zu den schwierigsten der höheren Arithmetik.

Die vorliegende Abhandlung besteht aus drei voneinander unabhängigen Teilen. Sie enthält den fünften und sechsten Beweis des Fundamentaltheorems und eine neue, mit dem dritten Beweis zusammenhängende Methode, $\cdot$ um zu entscheiden, ob eine gegebene ganze Zahl quadratischer Rest oder Nichtrest einer gegebenen Primzahl ist. Unter den ersten vier Beweisen war der dritte

unstreitig derjenige, der die größte Einfachheit mit der Unabhängigkeit von andersartigen Untersuchungen verband. Deshalb hat ihn auch LEGENDRE in die neue Ausgabe seines *Essai d'une théorie des nombres* aufgenommen. Der *fünfte* Beweis scheint dem dritten in beiden Hinsichten mindestens gleichzukommen. Beide Beweise sind insofern verwandt, als sie von demselben Satz ausgehen; in ihrer weiteren Durchführung sind sie jedoch völlig voneinander verschieden. Dieser Satz lautet: Es sei m eine (positive ungerade) Primzahl und M eine ganze, durch m nicht teilbare Zahl. Wenn ferner unter den Resten, die bei Division der Produkte

$$M,\ 2M,\ 3M,\ 4M \ldots\ldots \tfrac{1}{2}(m-1)M$$

durch m entstehen, die Anzahl derjenigen, die größer als $\frac{1}{2}m$ sind, mit n bezeichnet wird, so ist M quadratischer Rest oder Nichtrest von m, je nachdem n gerade oder ungerade ist. Um nun zum Beweis des Fundamentaltheorems zu gelangen, nimmt man an, dass auch M eine ungerade positive Primzahl ist und N bezüglich M und m dasselbe bedeutet wie n bezüglich m und M. Ob N gerade oder ungerade ist, entscheidet also, ob m quadratischer Rest oder Nichtrest von M ist. Durch eine sehr kurze Folge von Schlüssen zeigt der Verfasser, dass die Anzahl aller positiven ganzen Zahlen, die zugleich kleiner als $\frac{1}{2}mM$ sind, bei Division durch m einen Rest kleiner als $\frac{1}{2}m$ und bei Division durch M einen Rest kleiner als $\frac{1}{2}M$ lassen,

$$= \tfrac{1}{8}(m-1)(M-1) + \tfrac{1}{2}n + \tfrac{1}{2}N$$

und folglich stets

$$\tfrac{1}{4}(m-1)(M-1) + n + N$$

eine gerade Zahl ist. Hat also mindestens eine der Zahlen m, M die Form $4k+1$, sodass $\frac{1}{4}(m-1)(M-1)$ gerade ist, so ist auch $n+N$ gerade; folglich sind n und N entweder beide gerade oder beide ungerade. Haben dagegen sowohl m als auch M die Form $4k+3$, so ist $n+N$ notwendig ungerade, also eine der Zahlen n, N gerade und die andere ungerade. Zusammen mit dem obigen Satz folgt daraus unmittelbar das Fundamentaltheorem.

Der *sechste* Beweis ist ebenso kurz und elegant wie der fünfte, beruht aber auf etwas kunstvolleren Kombinationen. Der beschränkte Raum dieser Blätter erlaubt nur, unter Weglassung der Einzelheiten, den Hauptgedanken zu berühren. Es bezeichnen:

p, q zwei (verschiedene positive ungerade) Primzahlen,

α eine sogenannte *primitive Wurzel* zum Modul p, also eine durch p nicht teilbare (hier positive) ganze Zahl, für die keine niedrigere Potenz als α^{p-1} modulo p zu eins kongruent ist

x eine unbestimmte Größe

ξ die Funktion

$$x - x^\alpha + x^\zeta - x^\eta + x^\theta - \text{usw.} - x^\lambda$$

wobei der bequemeren Drucklegung wegen $\zeta, \eta, \theta \ldots \lambda$ anstelle der Zahlen $\alpha\alpha, \alpha^3, \alpha^4 \ldots \alpha^{p-2}$ stehen;

ε die Einheit, positiv genommen, wenn p die Form $4k+1$, negativ, wenn p die Form $4k+3$ hat;

δ die Einheit, positiv genommen, wenn mindestens eine der Zahlen p, q die Form $4k+1$ hat, negativ, wenn beide die Form $4k+3$ haben;

γ die Einheit, positiv genommen, wenn q quadratischer Rest von p ist, negativ, wenn q quadratischer Nichtrest von p ist;

β die Einheit, positiv genommen, wenn p quadratischer Rest von q, negativ, wenn p quadratischer Nichtrest von q ist.

Nach diesen Vorbereitungen folgt leicht aus Art. 51 der *Disquisitiones Arithmeticae*, dass die Funktion

$$\xi^q - x^q + x^{q\alpha} - x^{q\zeta} + x^{q\eta} - x^{q\theta} + \text{usw.} + x^{q\lambda}$$

nach dem Ausmultiplizieren nur durch q teilbare Koeffizienten hat. Setzt man diese Funktion $= qX$, so ist X ein *Polynom*, dessen Koeffizienten ebenfalls ganze Zahlen sind. Durch Schlüsse, auf die hier näher einzugehen zu weit führen würde, wird in der Abhandlung bewiesen, dass die Funktion $qX\xi$ bei Division durch $x^{p-1} + x^{p-2} + x^{p-3} + x^{p-4} + \text{usw.} + x + 1$ den Rest

$$\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$$

lässt, dass also bei Division der Funktion $X\xi$ durch denselben Divisor der Rest

$$\frac{\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)}{q}$$

entsteht. Diese Größe muss daher eine ganze Zahl sein. Da $\delta\delta = 1$ ist, folgt daraus leicht, dass

$$p^{\frac{1}{2}(q-1)} - \gamma\delta$$

durch q teilbar sein muss. Nach einem bekannten Satz ist auch $p^{\frac{1}{2}(q-1)} - \beta$ durch q teilbar. Somit muss $\beta = \gamma\delta$ gelten, woraus wiederum unmittelbar das Fundamentaltheorem folgt.

Das Fundamentaltheorem kann zusammen mit einigen bekannten Sätzen zu einer ziemlich kurzen Lösung der Aufgabe dienen, zu entscheiden, ob eine gegebene positive ganze Zahl quadratischer Rest oder Nichtrest einer gegebenen Primzahl ist, wie in der Abhandlung ausführlich gezeigt wird. Weiteres Nachdenken über den dritten Beweis des Fundamentaltheorems führte den Verfasser jedoch zu einer noch viel geschmeidigeren Lösung. Sie bildet den dritten Teil der Abhandlung. Hier geben wir nur ihre abschließende Regel an und lassen die Herleitung aus Gründen der Kürze weg. Soll entschieden werden, ob die positive ganze Zahl b, die durch die Primzahl a nicht teilbar ist, quadratischer Rest oder Nichtrest von dieser ist, so bilde man genau wie bei der Suche nach dem größten gemeinsamen Teiler von a und b die Gleichungen

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \varepsilon e + f \text{ usw.} \end{aligned}$$

bis man in der Folge der Zahlen a, b, c, d, e, f usw. auf .die Einheit kommt. Man. bezeichne die Zahlen $\frac{1}{2}a$, $\frac{1}{2}b$, $\frac{1}{2}c$, $\frac{1}{2}d$ usw., unter Weglassung ihres Bruchteils $\frac{1}{2}$, sofern einige der Zahlen a, b, c, d usw. ungerade sind, mit a', b', c', d' usw. Man nenne μ die Anzahl der in der Folge a', b', c', d' usw. vorkommenden Paare unmittelbar aufeinanderfolgender ungerader Zahlen. Schließlich nenne man ν die Anzahl der ungeraden Zahlen in der Folge $\beta, \gamma, \delta, \varepsilon$ usw., denen in der Folge b', c', d', e' usw. der Reihe nach eine Zahl der Form $4k+1$ oder $4k+2$ entspricht. Dann ist b quadratischer Rest oder Nichtrest von a, je nachdem $\mu + \nu$ gerade oder ungerade ist, mit der einzigen Ausnahme, dass zugleich b gerade ist und a die Form $8k+3$ oder $8k+5$ hat. In diesem Fall gilt die entgegengesetzte Regel: Ein gerades $\mu + \nu$ zeigt an, dass b quadratischer Nichtrest von a ist, ein ungerades $\mu + \nu$ dagegen, dass b quadratischer Rest von a ist.

.Göttingische gelehrta Anzeigen. 1825 April 11.

Am 5. April legte Herr Hofrat Gauss der Königlichen Gesellschaft eine Vorlesung mit dem Titel vor:

Theoria Residuorum Biquadraticorum, Commentatio prima.

Die Theorie der quadratischen Reste bildet bekanntlich einen der interessantesten Teile der höheren Arithmetik. Nach vielfach wiederholten Untersuchungen kann man sie jetzt als vollendet und abgeschlossen betrachten. Nachrichten zu ihrer Geschichte finden sich in diesen Blättern von 1808 Mai 12 und September 19 sowie von 1817 März 10. An der letzten Stelle wurden auch bereits einige vorläufige Angaben zu den Nachforschungen gemacht, die der Verfasser der vorliegenden Abhandlung seit dem Jahr 1805 über die verwandte, ebenso fruchtbare und interessante, aber viel schwierigere Theorie der kubischen und biquadratischen Reste angestellt hatte. Obwohl er schon damals die wesentlichen Grundzüge dieser Theorie kannte, haben ihn bisher andere Arbeiten daran gehindert, etwas davon zu veröffentlichen. Erst jetzt konnte er sich mit der Ausarbeitung eines Teils dieser Untersuchungen befassen. Den Anfang macht die Theorie der biquadratischen Reste, die mit der Theorie der quadratischen Reste näher verwandt ist als die der kubischen. Die vorliegende Abhandlung soll jedoch diesen überaus reichhaltigen Gegenstand noch keineswegs ausschöpfen. Die Entwicklung der *allgemeinen* Theorie, die eine ganz eigene Erweiterung des Gebiets der höheren Arithmetik verlangt, bleibt einer künftigen Fortsetzung vorbehalten. In diese erste Abhandlung sind diejenigen Untersuchungen aufgenommen, die sich ohne eine solche Erweiterung vollständig darstellen ließen. Von den Ergebnissen kann diese Besprechung nur einen Teil hervorheben.

Eine ganze Zahl a heißt biquadratischer Rest der ganzen Zahl p, wenn es Zahlen der Form $x^4 - a$ gibt, die durch p teilbar sind; biquadratischer Nichtrest dagegen, wenn keine Zahlen dieser Form durch p teilbar sein können. Offenbar sind alle biquadratischen Reste von p zugleich quadratische Reste derselben Zahl und damit alle quadratischen Nichtreste auch biquadratische Nichtreste. Nicht alle quadratischen Reste sind jedoch zugleich biquadratische Reste. Es genügt, die Untersuchungen auf den Fall zu beschränken, dass p eine Primzahl der Form $4n + 1$ und a nicht durch p teilbar ist, da sich alle anderen Fälle leicht darauf zurückführen lassen.

Die Untersuchungen dieses Gegenstands gliedern sich in zwei Teile, je nachdem, ob p oder a als gegeben betrachtet wird. Der erste ist viel weniger schwierig als der zweite und im Vergleich zu ihm als ganz elementar anzusehen. Alles Wesentliche, was darüber zu sagen ist, enthält die Abhandlung vollständig.

Aus dem zweiten Teil werden hier dagegen erst einige besondere Fälle behandelt, die sich ohne allzu große Vorbereitungen erledigen ließen und der künftig zu gebenden allgemeinen Theorie vorarbeiten können. Es sind die Fälle, in denen $a = -1$ und $a = \pm 2$ gesetzt wird. Der erste bereitet keinerlei Schwierigkeit: Schon in den *Disquisitiones Arithmeticae* wurde gezeigt, dass -1 biquadratischer Rest von p ist, wenn p die Form $8n + 1$ hat, dagegen nur quadratischer Rest und biquadratischer Nichtrest von p, wenn p die Form $8n + 5$ hat. Ganz anders verhält es sich mit dem Fall $a = \pm 2$. Zwar ist seit Langem bekannt, dass $+2$ und -2 quadratische und damit auch biquadratische Nichtreste von p sind, wenn p die Form $8n + 5$ hat, und wenigstens quadratische Reste, wenn p die Form $8n+1$ hat. Ebenso ist bekannt, dass bei dieser Form von p entweder $+2$ und -2 zugleich biquadratische Reste oder zugleich biquadratische Nichtreste sind: Die Entscheidung, welcher dieser beiden Fälle eintritt, erfordert jedoch eine Untersuchung viel höherer Art. Dafür entwickelt die Abhandlung zwei verschiedene Kriterien.

Das erste Kriterium hängt mit der Zerlegung der Zahl p in ein Quadrat und das Doppelte eines Quadrats zusammen. Bekanntlich ist diese Zerlegung (da, wie schon bemerkt, p als Primzahl vorausgesetzt wird) stets und nur auf eine Weise möglich. Setzt man $p = gg + 2hh$, so ist ± 2 biquadratischer Rest von p, wenn g die Form $8n + 1$ oder $8n + 7$ hat, dagegen biquadratischer Nichtrest, wenn g die Form $8n + 3$ oder $8n + 5$ hat.

Das zweite Kriterium hängt mit der Zerlegung der Zahl p in zwei Quadrate zusammen, die bekanntlich ebenfalls stets und nur auf eine Weise möglich ist. Setzt man $p = ee + ff$ und nimmt an, dass ee das ungerade und ff das gerade Quadrat bezeichnet, so folgt schon aus der vorausgesetzten Form $p = 8n + 1$, dass auch $\frac{1}{2}f$ eine gerade Zahl ist. Also hat f entweder die Form $8m$ oder die Form $8m + 4$: Im ersten Fall ist ± 2 biquadratischer Rest, im anderen biquadratischer Nichtrest von p.

Wir deuten hier nur die Bemerkung an, zu der die höhere Arithmetik so oft Anlass gibt: Nicht so sehr die Schönheit und Einfachheit der Sätze selbst, sondern vielmehr die Schwierigkeit ihrer Beweise macht sie besonders bemerkenswert. Sobald man einen Zusammenhang zwischen dem Verhalten der Zahl ± 2 und den beiden angeführten Zerlegungen der Zahl p vermutet, lässt sich dieser Zusammenhang anhand von Zahlenbeispielen äußerst leicht entdecken. Doch schon beim ersten Kriterium ist der Beweis nicht ganz leicht; beim zweiten liegt er viel tiefer verborgen und ist eng mit anderen subtilen Hilfsuntersuchungen verbunden, die ihrerseits zu einer bemerkenswerten Erweiterung der Theorie der Kreisteilung führen. Gerade diese wunderbare Verknüpfung der Wahrheiten ist es. die, wie schon oft bemerkt wurde, der höheren Arithmetik einen so eigenen Reiz verleiht. Diese Beweise selbst lassen sich hier natürlich nicht auszugsweise wiedergeben; man muss sie in der Abhandlung selbst nachlesen.

Ein paar andere neue arithmetische Sätze, die ebenfalls eng mit dem Beweis des zweiten Kriteriums verbunden sind, verdienen aber wegen ihrer Einfachheit hier noch besonders hervorgehoben zu werden.

Ist p eine Primzahl der Form $4k+1$ und setzt man diese Zahl $= ee + ff$, sodass ee das ungerade und ff das gerade Quadrat bezeichnet, und setzt man ferner

$$1 \,.\, 2 \,.\, 3 \,.\, \ldots\ldots \; k = q$$

$$(k+1)(k+2)(k+3) \,.\, \ldots \,.\, 2k = r$$

so ist stets $\pm e$ der kleinste Rest, der bei Division von $\frac{r}{2q}$ durch p entsteht, und $\pm f$ der kleinste Rest, den man bei Division von $\frac{1}{2}rr$ durch p erhält (der kleinste Rest ist dabei stets zwischen den Grenzen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ zu nehmen). Die Zahl $\frac{r}{2q}$, die für $p = 5$ den Wert 1 hat, kann man für größere Werte von p auch in die folgende Form bringen:

$$\frac{6 \,.\, 10 \,.\, 14 \,.\, 18 \,.\, \ldots \,.\, (p-3)}{2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, \ldots \,.\, k}$$

Es ist sehr bemerkenswert, dass sich die Zahl p so auf ganz direktem Weg in zwei Quadrate zerlegen lässt. Fast noch bemerkenswerter ist aber ein dabei auftretender Nebenumstand: Dieses Verfahren liefert die Wurzel des ungeraden Quadrats, e, stets mit positivem Vorzeichen, wenn e, positiv genommen, die Form $4m+1$ hat, und mit negativem, wenn e, positiv genommen, die Form $4m+3$ hat. Für das Vorzeichen, mit dem die Wurzel des geraden Quadrats, f, aus dieser Rechnung hervorgeht, hat sich dagegen bisher überhaupt keine allgemeine Regel finden lassen, weder a priori noch anhand von Zahlenbeispielen. Am Schluss der Abhandlung empfiehlt der Verfasser daher diesen Gegenstand den Freunden der höheren Arithmetik zur weiteren Untersuchung, überzeugt, dass ihr Gelingen zugleich eine ergiebige Quelle neuer Erweiterungen dieses schönen Teils der Mathematik erschließen werde.

Göttingische gelehrte Anzeigen. 1831, 23. April.

Eine Vorlesung, die Hofrat Gauss der Königlichen Gesellschaft am 15. April überreicht hat:

Theoria residuorum biquadraticorum, commentatio secunda,

setzt die bereits im sechsten Band der *Commentationes novae* abgedruckte Abhandlung fort, die seinerzeit auch in unseren Blättern, im Jahr 1825, am 11. April, angezeigt wurde. Auch diese Fortsetzung, obwohl mehr als doppelt so umfangreich wie die erste Abhandlung, erschöpft den überaus reichen Gegenstand noch nicht. Die Vollendung des Ganzen wird erst einer künftigen dritten Abhandlung vorbehalten bleiben.

Obwohl wir die Grundbegriffe dieser Lehren und den Inhalt der ersten Abhandlung bei allen, die höhere Arithmetik studiert haben, als bekannt voraussetzen können, wollen wir jene Begriffe hier doch kurz in Erinnerung bringen. Dies soll den Freunden dieses Teils der Mathematik dienen, die die erste Abhandlung nicht gleich zur Hand haben. In Bezug auf eine beliebige ganze Zahl p heißt eine andere ganze Zahl k ein biquadratischer Rest, wenn es Zahlen der Form $x^4 - k$ gibt, die durch p teilbar sind; im entgegengesetzten Fall heißt sie biquadratischer Nichtrest von p. Es genügt hier, sich auf den Fall zu beschränken, dass p eine Primzahl der Form $4n+1$ und k durch diese Primzahl nicht teilbar ist, da alle anderen Fälle entweder für sich klar sind oder sich auf diesen zurückführen lassen.

Für einen solchen *gegebenen* Wert von p zerfallen sämtliche durch p nicht teilbaren Zahlen in *vier* Klassen. Eine enthält die biquadratischen Reste, eine zweite diejenigen biquadratischen Nichtreste, die quadratische Reste von p sind; auf die beiden übrigen verteilen sich die biquadratischen Nichtreste, die zugleich quadratische Nichtreste sind. Das Prinzip dieser Aufteilung besteht darin, dass stets entweder $k^n - 1$ oder $k^n + 1$ oder $k^n - f$ oder $k^n + f$ durch p teilbar ist. Dabei bedeutet f eine ganze Zahl, die $ff + 1$ durch p teilbar macht. Jeder, der die elementare Terminologie kennt, sieht von selbst, wie sich diese Worterklärungen darin ausdrücken lassen.

Die Theorie dieser Klassifikation ist in der ersten Abhandlung vollständig ausgeführt: sowohl für den unmittelbar einleuchtenden Fall $k = -1$ als auch für die Fälle $k = \pm 2$, die subtile Hilfsuntersuchungen erfordern. Am Anfang der gegenwärtigen Abhandlung wird nun zu größeren Werten von k übergegangen. Zunächst braucht man aber nur solche Werte zu betrachten, die selbst Primzahlen sind. Dabei zeigt sich, dass die Ergebnisse am einfachsten ausfallen, wenn man die Werte positiv oder negativ nimmt, je nachdem sie ihrem Betrag nach die Form $4m+1$ oder $4m+3$ haben. Die Untersuchung von

Zahlenbeispielen liefert hier sofort und mit großer Leichtigkeit eine reiche Ernte neuer Lehrsätze, von denen wir nur einige anführen. Die Nummerierung der Klassen mit $1, 2, 3, 4$ bezieht sich auf die Fälle, in denen k^n jeweils zu $1, f, -1, -f$ kongruent ist. Zugleich wird für f stets derjenige Wert angenommen, der $a + bf$ durch p teilbar macht, wenn $aa + bb$ die Zerlegung von p in ein ungerades und ein gerades Quadrat darstellt. So findet man durch die Untersuchung von Zahlenbeispielen, dass -3 jeweils zur Klasse $1, 2, 3, 4$ gehört, je nachdem $b, a + b, a, a - b$ durch 3 teilbar ist; dass $+5$ der Reihe nach zu diesen Klassen gehört, je nachdem $b, a - b, a, a + b$ durch 5 teilbar ist; dass -7 in die Klasse 1 fällt, wenn a oder b; in die Klasse 2, wenn $a - 2b$ oder $a - 3b$; in die Klasse 3, wenn $a - b$ oder $a + b$; in die Klasse 4, wenn $a + 2b$ oder $a + 3b$ durch 7 teilbar ist, wobei die Teilbarkeit in jedem dieser Fälle die Bedingung ist. Ähnliche Sätze ergeben sich für die Zahlen $-11, +13, +17, -19, -23$ usw. So leicht sich aber all diese besonderen Sätze durch die Untersuchung von Zahlenbeispielen entdecken lassen, so schwer scheint es, auf diesem Weg ein allgemeines Gesetz für diese Formen zu finden, auch wenn manches Gemeinsame bald auffällt. Noch viel schwerer ist es, Beweise für diese Lehrsätze zu finden. Die in der ersten Abhandlung für die Zahlen $+2$ und -2 verwendeten Methoden lassen sich hier nicht mehr anwenden. Andere Methoden könnten zwar ebenfalls das erledigen, was die erste und dritte Klasse betrifft, erweisen sich aber zur Begründung *vollständiger* Beweise als ungeeignet.

Man erkennt daher bald, dass dieses reiche Gebiet der höheren Arithmetik nur auf ganz neuen Wegen zugänglich ist. Der Verfasser hatte schon in der ersten Abhandlung angedeutet, dass dazu eine eigentümliche Erweiterung des gesamten Feldes der höheren Arithmetik wesentlich erforderlich ist, ohne damals näher zu erklären, worin sie besteht. Die gegenwärtige Abhandlung soll diesen Gegenstand ins Licht setzen.

Es geht um nichts anderes, als dass für die wahre Begründung der Theorie der biquadratischen Reste das Feld der höheren Arithmetik, das man sonst nur auf die reellen ganzen Zahlen erstreckte, auch auf die imaginären ausgedehnt werden muss. Diesen muss das völlig gleiche Bürgerrecht wie jenen eingeräumt werden. Sobald man das eingesehen hat, erscheint jene Theorie in einem ganz neuen Licht, und ihre Ergebnisse gewinnen eine höchst überraschende Einfachheit.

Bevor jedoch in diesem erweiterten Zahlengebiet die Theorie der biquadratischen Reste selbst entwickelt werden kann, müssen auch die ihr vorangehenden Lehren der höheren Arithmetik an dieser Erweiterung teilnehmen, die bisher nur für reelle Zahlen behandelt worden sind. Von diesen vorbereitenden Untersuchungen können wir hier nur einiges anführen. Der Verfasser nennt eine Größe $a + bi$, in der a und b reelle Größen bedeuten und i der Kürze wegen für $\sqrt{-1}$ steht, eine komplexe ganze Zahl, wenn zugleich a und b ganze Zahlen sind. Die komplexen Größen stehen also nicht den reellen

gegenüber, sondern enthalten diese als den besonderen Fall, dass $b = 0$. Für einen bequemeren Gebrauch mussten mehrere Begriffsbildungen zu komplexen Größen eigene Benennungen erhalten, die wir in dieser Anzeige jedoch zu umgehen versuchen werden.

So wie in der Arithmetik der reellen Zahlen nur von zwei Einheiten, der positiven und der negativen, die Rede ist, so haben wir in der Arithmetik der komplexen Zahlen vier Einheiten: $+1$, -1, $+i$, $-i$. Eine komplexe ganze Zahl heißt *zusammengesetzt*, wenn sie das Produkt zweier ganzzahliger Faktoren ist, die keine Einheiten sind. Eine komplexe Zahl, die eine *solche* Zerlegung in Faktoren nicht zulässt, heißt dagegen eine komplexe Primzahl. So ist beispielsweise die reelle Zahl 3 auch als komplexe Zahl eine Primzahl, während 5 als komplexe Zahl zusammengesetzt ist $= (1 + 2i)(1 - 2i)$. Wie in der höheren Arithmetik der reellen Zahlen spielen die Primzahlen auch in diesem erweiterten Gebiet der Wissenschaft eine Hauptrolle.

Nimmt man eine komplexe ganze Zahl $a + bi$ als Modul an, so lassen sich $aa+bb$ paarweise nicht kongruente komplexe Zahlen angeben, und nicht mehr, zu deren einer jede vorgegebene ganze komplexe Zahl kongruent sein muss. Man kann sie ein vollständiges System inkongruenter Reste nennen. Die sogenannten kleinsten und absolut kleinsten Reste in der Arithmetik der reellen Zahlen haben auch hier ihr genaues Gegenstück. So besteht beispielsweise für den Modul $1 + 2i$ das vollständige System der absolut kleinsten Reste aus den Zahlen 0, 1, i, -1 und $-i$. Fast sämtliche Untersuchungen der ersten vier Abschnitte der *Disquisitiones Arithmeticae* finden mit einigen Abwandlungen auch in der erweiterten Arithmetik ihren Platz. Das berühmte Theorem von Fermat nimmt hier beispielsweise folgende Gestalt an: Ist $a + bi$ eine komplexe Primzahl und k eine durch sie nicht teilbare komplexe Zahl, so gilt stets $k^{aa+bb-1} \equiv 1$ für den Modul $a + bi$. Besonders bemerkenswert ist aber, dass das Fundamentaltheorem für die quadratischen Reste in der Arithmetik der komplexen Zahlen sein genaues und hier sogar einfacheres Gegenstück hat. Sind nämlich $a + bi$, $A + Bi$ komplexe Primzahlen, wobei a und A ungerade, b und B gerade sind, so ist die erste quadratischer Rest der zweiten, wenn die zweite quadratischer Rest der ersten ist; dagegen ist die erste quadratischer Nichtrest der zweiten, wenn die zweite quadratischer Nichtrest der ersten ist.

Wenn die Abhandlung nach diesen Voruntersuchungen zur Lehre von den biquadratischen Resten selbst übergeht, legt sie zunächst anstelle der bloßen Unterscheidung zwischen biquadratischen Resten und Nichtresten eine Aufteilung der durch den Modul nicht teilbaren Zahlen in vier Klassen fest. Ist nämlich der Modul eine komplexe Primzahl $a + bi$, wobei stets a ungerade und b gerade vorausgesetzt wird und der Kürze wegen p für $aa+bb$ steht, und ist k eine komplexe, durch $a + bi$ nicht teilbare Zahl, so ist stets $k^{\frac{1}{4}(p-1)}$ zu einer der Zahlen $+1, +i, -1, -i$ kongruent. Dadurch werden sämtliche durch $a+bi$ nicht teilbaren Zahlen in vier Klassen aufgeteilt, denen der Reihe nach

der biquadratische Charakter $0, 1, 2, 3$ zugeordnet wird. Offenbar bezieht sich der Charakter 0 auf die biquadratischen Reste, die übrigen auf die biquadratischen Nichtreste, und zwar so, dass dem Charakter 2 zugleich quadratische · Reste entsprechen, den Charakteren 1 und 3 dagegen quadratische Nichtreste.

Man erkennt leicht, dass es vor allem darauf ankommt, diesen Charakter nur für solche Werte von k bestimmen zu können, die selbst komplexe Primzahlen sind. Hier führt die Untersuchung von Zahlenbeispielen sofort zu höchst einfachen Ergebnissen.

Setzt man zunächst $k = 1+i$, so zeigt sich, dass der Charakter dieser Zahl stets $\equiv \frac{1}{8}(-aa+2ab-3bb+1) (\mathrm{mod.}\ 4)$ wird. Ähnliche Ausdrücke findet man für die Fälle $k = 1-i$, $k = -1+i$, $k = -1-i$.

Ist dagegen $k = \alpha + \beta i$ eine Primzahl mit ungeradem α und geradem β, so ergibt sich durch die Untersuchung von Zahlenbeispielen sehr leicht ein zum Fundamentaltheorem für die quadratischen Reste ganz analoges Reziprozitätsgesetz. Es lässt sich am einfachsten folgendermaßen ausdrücken:

Sind sowohl $\alpha+\beta-1$ als auch $a+b-1$ durch 4 teilbar (auf diesen Fall lassen sich alle übrigen leicht zurückführen), und bezeichnet man den Charakter von $\alpha+\beta i$ in Bezug auf den Modul $a+bi$ mit λ, dagegen den Charakter von $a+bi$ in Bezug auf den Modul $\alpha+\beta i$ mit l, so gilt $\lambda = l$, wenn eine der Zahlen β, b (oder beide) durch 4 teilbar ist. dagegen $\lambda = l \pm 2$, wenn keine der Zahlen β, b durch 4 teilbar ist.

Diese Sätze enthalten im Grunde alles Wesentliche der Theorie der biquadratischen Reste. So leicht es aber war, sie durch die Untersuchung von Zahlenbeispielen zu entdecken, so schwer ist es, strenge Beweise für sie zu geben, besonders für den zweiten, das Fundamentaltheorem der biquadratischen Reste. Wegen des großen Umfangs, den die gegenwärtige Abhandlung bereits erreicht hat, sah sich der Verfasser gezwungen, die Darstellung des Beweises für den letzteren Satz, den er seit 20 Jahren besitzt, einer künftigen dritten Abhandlung vorzubehalten. Die vorliegende Abhandlung enthält dagegen noch den vollständigen Beweis des ersteren Satzes über $1+i$ (von dem die anderen Sätze für $1-i$, $-1+i$, $-1-i$ abhängen). Dieser kann bereits eine Vorstellung von der Verwicklung des Gegenstandes geben.

Wir haben noch einige allgemeine Anmerkungen hinzuzufügen. Die Verlegung der Lehre von den biquadratischen Resten in das Gebiet der komplexen Zahlen könnte manchem, der mit der Natur der imaginären Größen weniger vertraut und in falschen Vorstellungen über sie befangen ist, anstößig und unnatürlich erscheinen. Sie könnte die Meinung hervorrufen, die Untersuchung werde dadurch gleichsam in die Luft gestellt, erhalte einen schwankenden Halt und entferne sich ganz von der Anschaulichkeit. Nichts wäre unbegründeter als eine solche Meinung. Im Gegenteil lässt die Arithmetik der komplexen Zahlen die anschaulichste Veranschaulichung zu. Der Verfasser hat in seiner diesmaligen Darstellung zwar eine rein arithmetische Behandlung gewählt,

aber auch die nötigen Hinweise zu dieser Veranschaulichung gegeben, die die Einsicht lebendiger macht und deshalb sehr zu empfehlen ist. sie werden selbstständig denkenden Lesern genügen. So wie die absoluten ganzen Zahlen durch eine Reihe gleich weit voneinander entfernter Punkte auf einer Geraden dargestellt werden, in der der Anfangspunkt die Zahl 0, der nächste die Zahl 1 usw. vertritt; und so wie man zur Darstellung der negativen Zahlen diese Reihe nur auf der entgegengesetzten Seite des Anfangspunkts unbegrenzt verlängern muss: so braucht man zur Darstellung der komplexen ganzen Zahlen lediglich hinzuzufügen, dass jene Reihe in einer bestimmten unbegrenzten Ebene liegt und parallel zu ihr auf beiden Seiten eine unbeschränkte Anzahl ähnlicher Reihen in gleichen Abständen voneinander angenommen wird. Statt einer Reihe von Punkten haben wir dann ein System von Punkten vor uns, die sich auf zwei Arten in Reihen von Reihen ordnen lassen und die ganze Ebene in gleiche Quadrate einteilen. Der nächste Punkt bei 0 in der ersten Nebenreihe auf der einen Seite der Reihe, die die reellen Zahlen darstellt, bezieht sich dann auf die Zahl i, ebenso der nächste Punkt bei 0 in der ersten Nebenreihe auf der anderen Seite auf $-i$ usw. Bei dieser Darstellung lassen sich die Ausführung der arithmetischen Operationen mit komplexen Größen, die Kongruenz, die Bildung eines vollständigen Systems inkongruenter Zahlen für einen gegebenen Modul usw. in einer Weise veranschaulichen, die nichts zu wünschen übrig lässt.

Andererseits wird dadurch die wahre Metaphysik der imaginären Größen in ein neues helles Licht gestellt.

Unsere allgemeine Arithmetik, deren Umfang die Geometrie der Alten so weit übertrifft, ist ganz eine Schöpfung der neueren Zeit. Ursprünglich vom Begriff der absoluten ganzen Zahlen ausgehend, hat sie ihr Gebiet schrittweise erweitert: Zu den ganzen Zahlen kamen die gebrochenen, zu den rationalen die irrationalen, zu den positiven die negativen, zu den reellen die imaginären hinzu. Jeder dieser Fortschritte geschah aber zunächst mit furchtsam zögernden Schritten. Die ersten Algebraiker nannten die negativen Wurzeln der Gleichungen noch falsche Wurzeln. Das sind sie auch, wenn die Aufgabe, auf die sie sich beziehen, in einer Form gestellt ist, in der die gesuchte Größe ihrer Beschaffenheit nach kein Entgegengesetztes zulässt. Aber so wenig man in der *allgemeinen* Arithmetik Bedenken hat, gebrochene Zahlen aufzunehmen, obwohl es so viele zählbare Dinge gibt, bei denen eine Bruchzahl sinnlos ist, ebenso wenig durfte man dort den negativen Zahlen die gleichen Rechte wie den positiven deshalb versagen, weil unzählige Dinge kein Entgegengesetztes zulassen. Die Realität der negativen Zahlen ist hinreichend gerechtfertigt, da sie in unzähligen anderen Fällen ein angemessenes Substrat finden. Darüber besteht freilich schon seit langer Zeit Klarheit. Die den reellen Größen gegenübergestellten imaginären dagegen—früher. und hier und da noch heute, wenn auch unpassend, *unmögliche* genannt—sind noch immer

weniger eingebürgert als bloß geduldet. Sie erscheinen daher eher als ein an sich inhaltsleeres Zeichenspiel, dem man ein denkbares Substrat unbedingt abspricht, ohne jedoch den reichen Tribut verschmähen zu wollen, den dieses Zeichenspiel schließlich zum Schatz der Verhältnisse reeller Größen beiträgt.

Der Verfasser betrachtet diesen höchst wichtigen Teil der Mathematik seit vielen Jahren aus einem anderen Blickwinkel, unter dem man den imaginären Größen ebenso gut einen Gegenstand zugrunde legen kann wie den negativen. Bisher fehlte jedoch ein Anlass, diese Sicht öffentlich und ausdrücklich darzulegen. Aufmerksame Leser werden ihre Spuren allerdings leicht in der 1799 erschienenen Schrift über Gleichungen und in der Preisschrift über die Umbildung der Flächen wiederfinden. In der gegenwärtigen Abhandlung werden ihre Grundzüge kurz angegeben; sie bestehen in Folgendem.

Positive und negative Zahlen lassen sich nur dort anwenden, wo das Gezählte ein Entgegengesetztes hat, das, mit ihm vereinigt gedacht, der Vernichtung gleichzusetzen ist. Genau betrachtet gilt diese Voraussetzung nur dort, wo nicht Substanzen (für sich denkbare Gegenstände), sondern Beziehungen zwischen jeweils zwei Gegenständen gezählt werden. Dabei wird vorausgesetzt, dass diese Gegenstände auf bestimmte Art in eine Reihe geordnet sind, beispielsweise $A, B, C, D \ldots$, und dass die Beziehung von A zu B als gleich der Beziehung von B zu C usw. gelten kann. Zum Begriff der Entgegensetzung gehört hier nichts weiter als der *Austausch* der Glieder der Beziehung. Gilt also die Beziehung (oder der Übergang) von A zu B als $+1$, so muss die Beziehung von B zu A durch -1 dargestellt werden. Soweit eine solche Reihe auf beiden Seiten unbegrenzt ist, stellt also jede reelle ganze Zahl die Beziehung eines beliebig als Anfang gewählten Gliedes zu einem bestimmten Glied der Reihe dar.

Sind die Gegenstände aber so beschaffen, dass sie sich nicht in eine einzige, wenn auch unbegrenzte Reihe ordnen lassen, sondern nur in Reihen von Reihen, oder, gleichbedeutend damit, bilden sie eine Mannigfaltigkeit von zwei Dimensionen; und verhalten sich die Beziehungen einer Reihe zu einer anderen oder die Übergänge zwischen ihnen ähnlich wie zuvor die Übergänge von einem Glied einer Reihe zu einem anderen Glied derselben Reihe, so braucht man offenbar zum Messen des Übergangs von einem Glied des Systems zu einem anderen außer den bisherigen Einheiten $+1$ und -1 noch zwei weitere, einander ebenfalls entgegengesetzte Einheiten $+i$ und $-i$. Dabei muss aber noch vorausgesetzt werden, dass die Einheit i stets den Übergang von einem gegebenen Glied einer Reihe zu einem *bestimmten* Glied der unmittelbar angrenzenden Reihe bezeichnet. Auf diese Weise lässt sich das System also auf zwei Arten in Reihen von Reihen ordnen.

Der Mathematiker sieht von der Beschaffenheit der Gegenstände und vom Inhalt ihrer Beziehungen vollständig ab. Er hat es nur damit zu tun, die Beziehungen zu zählen und miteinander zu vergleichen. Insofern darf er die

Gleichartigkeit, die er den durch $+1$ und -1 bezeichneten Beziehungen an sich zuschreibt, auf alle vier Elemente $+1$, -1, $+i$ und $-i$ ausdehnen.

Anschaulich werden diese Verhältnisse nur durch eine Darstellung im Raum. Der einfachste Fall liegt vor, wenn kein Grund besteht, die Symbole der Gegenstände anders als quadratisch anzuordnen: Man teilt eine unbegrenzte Ebene durch zwei Systeme paralleler Linien, die sich rechtwinklig kreuzen, in Quadrate und wählt die Schnittpunkte als Symbole. Jeder solche Punkt A hat hier vier Nachbarn. Bezeichnet man die Beziehung von A zu einem benachbarten Punkt mit $+1$, so ist die mit -1 zu bezeichnende Beziehung von selbst bestimmt. Dagegen kann man für $+i$ nach Belieben eine der beiden anderen wählen, also den zu $+i$ gehörenden Punkt *rechts* oder *links* nehmen. Sobald man vorwärts und rückwärts *in* der Ebene sowie oben und unten in Bezug auf ihre beiden Seiten einmal nach Belieben festgelegt hat, ist dieser Unterschied zwischen rechts und links *in sich* völlig bestimmt. Unsere Anschauung dieses Unterschieds können wir anderen allerdings *nur* vermitteln, indem wir auf tatsächlich vorhandene materielle Dinge zeigen[*)]. Auch wenn man sich über Letzteres entschieden hat, sieht man jedoch, dass es von unserer Willkür abhing, welche der beiden sich in einem Punkt kreuzenden Reihen wir als Hauptreihe und welche Richtung darin wir als auf positive Zahlen bezogen ansehen wollten. Ferner sieht man: Will man die zuvor als $+i$ behandelte Beziehung für $+1$ nehmen, muss man notwendig die zuvor durch -1 bezeichnete Beziehung für $+i$ nehmen. In der Sprache der Mathematiker heißt das: $+i$ ist eine mittlere Proportionalgröße zwischen $+1$ und -1 oder entspricht dem Zeichen $\sqrt{\ }-1$. Wir sagen absichtlich nicht *die* mittlere Proportionalgröße, denn $-i$ hat offenbar den gleichen Anspruch. Damit ist die Möglichkeit, für $\sqrt{\ }-1$ eine anschauliche Bedeutung anzugeben, vollkommen gerechtfertigt. Mehr braucht es nicht, um diese Größe in das Gebiet der Gegenstände der Arithmetik aufzunehmen.

[*)] Beide Bemerkungen hat bereits KANT gemacht. Man begreift aber nicht, wie dieser scharfsinnige Philosoph in der ersten einen Beweis für seine Ansicht finden zu können glaubte, dass der Raum *nur* Form unserer äußeren Anschauung sei, da die zweite so klar das Gegenteil beweist und zeigt, dass der Raum unabhängig von unserer Anschauungsart eine reelle Bedeutung haben muss.

Wir glaubten, den Freunden der Mathematik mit dieser kurzen Darstellung der Hauptpunkte einer neuen Theorie der sogenannten imaginären Größen einen Dienst zu erweisen. Wenn man diesen Gegenstand bisher aus einem falschen Blickwinkel betrachtet und dabei eine geheimnisvolle Dunkelheit gefunden hat, so liegt das größtenteils an den wenig passenden Benennungen. Hätte man $+1$, -1, $\sqrt{-1}$ beispielsweise direkte, inverse und laterale Einheit genannt statt positive, negative und imaginäre (oder gar unmögliche) Einheit, so hätte von solcher Dunkelheit kaum die Rede sein können. Der Verfasser hat sich vorbehalten, den Gegenstand, der in der vorliegenden Abhandlung eigentlich nur nebenbei berührt wird, künftig vollständiger zu behandeln. Dabei wird auch die Frage beantwortet werden, warum die Beziehungen zwischen Dingen, die eine Mannigfaltigkeit von mehr als zwei Dimensionen bilden, nicht noch weitere Arten von Größen liefern können, die in der allgemeinen Arithmetik zulässig sind.

BESPRECHUNGEN

FREMDER

SCHRIFTEN.

Göttingische gelehrte Anzeigen. 1809, 11. März.

Recherches sur l'irréductibilité Arithmétique et Géométrique des nombres et de leurs puissances. 1808. (Ohne Druckort. 25 S. in großem Quartformat.)

Eine Schrift mit dem Ziel, irrationale Wurzelgrößen in der Form rationaler Größen darzustellen. Wir müssen uns damit begnügen, die Freunde der Mathematik auf dieses kleine Werk aufmerksam gemacht zu haben. Denn der Umfang dieser Blätter erlaubt uns nicht, hier ausführlicher den eigentümlichen Blickwinkel des Verfassers und seine von der üblichen ganz abweichende Behandlung der Wurzelgrößen darzustellen und zu prüfen.

Göttingische Gelehrte Anzeigen. 1812, 23. März.

Cribrum Arithmeticum, sive tabula continens numeros primos a compositis segregatos, occurrentes in serie numerorum ab unitate progredientium usque ad decies centena milia et ultra haec ad viginti millia (1020000). *Numeris compositis, per* 2, 3, 5 *non dividuis, adscripti sunt divisores simplices, non minimi tantum, sed omnino omnes. Confecit* Ladislaus Chernac, *Pannonius, A. L. M. Philos. et Medic. Doctor, in almo lyceo Daventriensi philosophiae professor. Daventriae* 1811. (Auf Kosten des Verfassers, gedruckt bei J. H. Lange. XXII und 1022 S. in großem Quartformat.)

Der vollständige Titel dieses wichtigen und sehr verdienstvollen Werks bezeichnet den Inhalt bereits hinreichend: Es ist eine durch ebenso sorgfältige wie mühsame mehrjährige Arbeit berechnete Tafel aller Primfaktoren sämtlicher durch 2, 3 und 5 nicht teilbaren Zahlen von 1 bis 1020000, sauber und, soweit wir bei gelegentlichen Prüfungen feststellen konnten, sehr korrekt gedruckt. Wie wertvoll ein solches Geschenk an die Arithmetik ist, kann jeder leicht beurteilen, der häufig mit größeren Zahlen rechnet. Der Verfasser verdient doppelten Dank: sowohl für die höchst mühsame Arbeit selbst, durch die er seinen Namen den unvergesslichen Namen von Rhaeticus, Pitiscus, Brigg, Vlacq, Wolfram, Taylor und anderen zugesellt hat, als auch für den gewiss sehr erheblichen Druckaufwand, für den sich sonst wohl kaum ein Verleger gefunden hätte. Schon öfter wurden solche Tafeln berechnet, wenn auch meist in geringerem Umfang, blieben aber entweder ganz im Manuskript oder wurden nicht vollständig gedruckt. Bekanntlich ermunterte Lambert früher nach besten Kräften zur Fortsetzung der oft gedruckten Pellschen Tafel, die bis 100000 reicht. Nach einer Mitteilung von Bernoulli in Lamberts Briefwechsel hatte Oberreit sie bis 500000 fortgeführt; eine Abschrift

davon war in Schulzes Hände gelangt. Anton Felkel hatte sie, wie in der Monatl. Correspondenz, Band 2, S. 223 berichtet wird, im Manuskript bis zu zwei Millionen vollendet und wollte sie später bis 2460000 liefern. Was davon in Wien auf öffentliche Kosten bereits gedruckt worden war, wurde jedoch im Türkenkrieg zu Patronen verarbeitet, weil sich keine Käufer fanden! So ging eine verdienstvolle Arbeit vieler Jahre für die Öffentlichkeit verloren. Umso mehr hielten wir es für unsere Pflicht, hier das Erscheinen des gegenwärtigen Werks anzuzeigen. Die erste Million steht nun jedem zum Gebrauch zur Verfügung; wer Gelegenheit und Eifer für diesen Gegenstand hat, möge daher seine Mühe auf das Weitere richten.

Göttingische gelehrte Anzeigen. 1814, 3. November.

Tables des diviseurs pour tous les nombres du deuxième million, ou plus exactement depuis 1020000 *à* 2028000, *avec les nombres premiers qui s'y trouvent. Par* J. Ch. Burckhardt, *membre de l'institut impérial, du bureau des longitudes de France, et de plusieurs autres sociétés savantes. Paris*, 1814. *Mme Ve Courcier.* (VIII. und 112 S. in Folio.)

Früher, als wir bei der Anzeige der Chernacschen Faktorentafel für die erste Million zu hoffen gewagt hätten, können wir bereits die Vollendung und das Erscheinen einer ähnlichen Tafel für die zweite Million melden. Der verdienstvolle Verfasser, dessen Name allein schon größte Sorgfalt und Genauigkeit verbürgt, hat durch diese mühsame Arbeit alle Freunde der Arithmetik sehr verpflichtet. Chernacs Tafel für die erste Million enthält alle Primfaktoren, Burckhardts Tafel für die zweite dagegen jeweils nur den kleinsten Teiler. Die vollständige Zerlegung einer Zahl der zweiten Million erfordert daher die Division durch den kleinsten Teiler und das Nachschlagen des Quotienten in der Chernacschen Tafel. Diese kleine Mühe fällt jedoch gegenüber dem großen Vorteil, die Tafel auf so viel kleinerem Raum zu besitzen, gar nicht ins Gewicht. Dabei bleibt die Aussicht, die Tafel mit der Zeit noch bis zu zehn Millionen erweitert zu sehen. Die Unterbringung in dem kleinen Band ermöglichte der Verfasser teils durch die Beschränkung auf den kleinsten Teiler, teils durch einen möglichst sparsamen Druck. Bezeichnet a unbestimmt eine der achtzig Zahlen unter 300, die durch 2, 3 und 5 nicht teilbar sind, so ist jede durch 2, 3 und 5 nicht teilbare Zahl in der Form $300n + a$ enthalten. Alle achtzig Zahlen, für die n denselben Wert hat, stehen in einer einzigen senkrechten Spalte; jede Seite enthält dreißig solcher Spalten. Jede Seite umfasst also von neuntausend in natürlicher Reihenfolge aufeinanderfolgenden Zahlen alle, die durch 2, 3 oder 5 nicht teilbar sind.

Die Methode, mit der Herr Burckhardt seine Tafel erstellt hat, verdient hier besondere Erwähnung. Er ließ ein Netz in Kupfer stechen, in dem 81 waagerechte und 78 senkrechte Linien ein in 80×77, also 6160 kleine Quadrate geteiltes Rechteck bildeten, und davon die nötige Anzahl Abzüge herstellen. An der Seite konnten die achtzig Werte von a gleich mit eingestochen werden; die Werte von $300n$ schrieb man in fortlaufender Reihenfolge mit der Feder über die 77 senkrechten Spalten. Jedes Blatt stellt so alle durch 2, 3 und 5 nicht teilbaren Zahlen dar, die sich unter jeweils 23100 in natürlicher Reihenfolge aufeinanderfolgenden Zahlen befinden; 44 Blätter genügen, um eine ganze Million zu umfassen. Man sieht leicht, dass die Zahlen, deren kleinster Teiler 7 oder 11 ist, auf jedem folgenden Blatt in derselben Reihenfolge wiederkehren. Diese Teiler konnten daher gleich in die Kupferplatte gestochen werden und erschienen so auf jedem Blatt von selbst an den richtigen Stellen. Um nun die folgenden Teiler, beispielsweise 13, einzutragen, nahm Herr B. von einem überzähligen Blatt der Breite nach nur 13 Spalten. Er betrachtete dieses als den Anfang seiner Tafel und schnitt alle Quadrate aus, die den Teiler 13 enthalten mussten. Dieses Gitter brauchte er dann nur auf die ersten dreizehn Spalten des ersten Blattes, danach auf die nächsten dreizehn usw. zu legen, um sofort alle Stellen zu sehen, die, soweit sie nicht schon 7 oder 11 enthielten, mit 13 auszufüllen waren. Ebenso verfuhr er danach mit dem Teiler 17 usw. Bis zum Teiler 73 reichten die überzähligen Blätter auf diese Weise aus. Für die größeren Teiler 79, 83 usw. scheint Herr B. den Rahmen aus zwei oder mehreren Teilen zusammengesetzt zu haben. Bei den Teilern über 500 zog Herr B. dagegen vor, die Vielfachen durch Addition zu ermitteln, wobei er für den anderen Faktor nur Primzahlen zu nehmen brauchte. Wir halten das ganze Verfahren für höchst zweckmäßig und würden es allen zur Nachahmung empfehlen, die die Tafel vielleicht noch weiter fortsetzen möchten. Für die dritte und vierte Million hat der Verfasser inzwischen selbst schon einen großen Teil der Rechnungen ausgeführt. Wir haben daher begründete Hoffnung, auch diese bald im Druck zu sehen.

Göttingische gelehrte Anzeigen. 1816, 7. November.

Tables des diviseurs pour tous les nombres du troisième million, ou plus exactement, depuis 2028000 *à* 3036000, *avec les nombres premiers qui s'y trouvent; par* J. Chr. Burckhardt, *membre de l'académie royale des sciences, du bureau des longitudes de France et de plusieurs autres sociétés savantes. Paris* 1816. *Mme Ve Courcier.* (112 S. in Folio.)

Da wir bei der Anzeige der Faktorentafel für die zweite Million bereits die Berechnungsmethode des verdienstvollen Verfassers und die Einrichtung der Tafel selbst ausführlich beschrieben haben, können wir uns hier mit der bloßen Anzeige des Erscheinens der Tafel für die dritte Million begnügen. Bald dürfen wir vom Verfasser auch noch die auf dieselbe Art dargestellte Tafel für die *erste* Million erwarten, sodass die ganze Tafel bis über drei Millionen nur einen mäßig großen Band ausmachen wird. Dafür gebührt dem Verfasser der Dank aller Freunde der Arithmetik. Sie sehen durch diese mühsame Arbeit ein Bedürfnis in einem Umfang erfüllt, der alles weit übersteigt, was man noch vor wenigen Jahren zu hoffen wagen konnte.

Göttingische gelehrte Anzeigen. 1817, 9. August.

Tables des diviseurs, pour tous les nombres du premier million, ou plus exactement depuis 1 *à* 1020000, *avec les nombres premiers qui s'y trouvent; par* J. Chr. Burckhardt, *membre de l'académie des sciences dans l'institut royal, du bureau des longitudes de France, et de plusieurs autres sociétés savantes. Paris* 1817. *Mme Ve Courcier.* (114 S. in Folio.)

Mit Verweis auf unsere Anzeigen der Tafeln für die zweite und dritte Million kündigen wir jetzt nur das tatsächliche · Erscheinen dieser Faktorentafeln für die erste Million an. Wir besitzen damit nun ein zusammenhängendes Ganzes für die ersten drei Millionen. Für die gegenwärtige erste Million benutzte der Verfasser teils das *Cribrum Arithmeticum* von Chernac, teils eine handschriftliche Tafel von Schenmark, die die Bibliothek des Königlichen Instituts besitzt. Letztere war allerdings nicht ganz mit aller wünschenswerten Sorgfalt erstellt worden. Wenn beide voneinander abwichen, war die Entscheidung, welche von beiden recht hatte, oft ziemlich mühsam. In der Chernacschen Tafel fand sich nur eine sehr geringe Anzahl von Fehlern, die Herr Burckhardt hier mitgeteilt hat.

Auch für die vierte, fünfte und sechste Million hat der Verfasser die Materialien bereits größtenteils bereit. Er bietet an, diese Fortsetzung zu liefern, wenn der Verleger durch einen hinreichenden Absatz der ersten drei Millionen ermutigt wird. Es wäre in der Tat sehr zu bedauern, wenn die Früchte einer so mühsamen und nützlichen Arbeit der Welt vorenthalten würden.

Göttingische gelehrte Anzeigen. 19. Dezember 1825.

Der Königlichen Gesellschaft ist im Namen von Herrn Erchinger aus Thuningen im Königreich Würtemberg eine kleine Abhandlung vorgelegt worden, die die

Geometrische Konstruktion des regelmäßigen Siebzehnecks

zum Gegenstand hat. Die allgemeine Theorie der regelmäßigen Vielecke hat bekanntlich durch ihre enge Verbindung mit der höheren Arithmetik eine neue Gestalt und einen erweiterten Umfang erhalten. Ein, wenn auch verhältnismäßig kleiner, Teil davon ist die Theorie der Vielecke, die sich geometrisch konstruieren lassen. Seit der Zeit der Griechen wusste man, dass das Dreieck, das Fünfeck, das Fünfzehneck und alle Vielecke, die daraus durch Verdopplung oder wiederholte Verdopplung der Seitenzahl entstehen, diese Eigenschaft haben; man glaubte und behauptete wohl auch ausdrücklich, dass dies die einzigen seien. Die höhere Arithmetik hat gezeigt, dass dies ein Irrtum war: Indem sie die wahren Quellen der ganz allgemeinen Theorie offenlegte, ergab sich von selbst, dass es außer den genannten Vielecken noch unzählige andere gibt, die sich geometrisch konstruieren lassen und unter denen das Siebzehneck das einfachste ist. Dabei zeigt sich im hellsten Licht die Überlegenheit der Analysis, die das Allgemeinste wie das Besondere mit gleicher Leichtigkeit umfasst, über die Geometrie, die immer beim Besonderen stehen bleiben muss, beim Fortschreiten von einfacheren zu zusammengesetzteren Fällen durch stets wachsende Verwicklungen aufgehalten wird und jenen nächsten Fall nach den bekannten wohl kaum jemals ohne fremde Hilfe erreicht hätte. Dennoch bleibt es wichtig, interessant und wünschenswert, auch rein geometrische Behandlungen fortwährend zu pflegen und der Geometrie wenigstens einen Teil der neuen Felder zu erschließen, die die Analysis erobert. Dem Rezensenten ist nicht bekannt, dass bisher jemand die Konstruktion des Siebzehnecks öffentlich behandelt hätte, außer Herrn Pauker in den Schriften der Kurländischen Gesellschaft und in seiner Geometrie. Davon verschieden und stärker im rein geometrischen Geist durchgeführt ist die Konstruktion von Herrn Erchinger, die im Folgenden besteht. (Die zugehörige Figur, eine gerade Linie, auf der nacheinander die Punkte $DBGAIFCE$ liegen, kann sich jeder selbst zeichnen.) Man wähle eine beliebige gerade Linie AB und verlängere sie rückwärts und vorwärts nach C und D, sodass $AC \times BC = AD \times BD = 4AB \times AB$ gilt. Ferner bestimme man die Punkte E, G an beiden Seiten der verlängerten Linie CA, sodass $AE \times EC = AG \times CG = AB \times AB$, und den Punkt F auf der Seite A der verlängerten Linie BA, sodass $AF \times DF = AB \times AB$ gilt. Schließlich teile

man AE in I, sodass $AI \times EI = AB \times AF$ gilt, wobei AI der kleinere und EI der größere Abschnitt von AE ist. Dann bilde man ein Dreieck, in dem zwei Seiten jeweils $= AB$ und die dritte $= AI$ sind. Beschreibt man um dieses Dreieck einen Kreis, so ist AI die Seite des in diesen Kreis eingeschriebenen regelmäßigen Siebzehnecks.

Prüft man die Richtigkeit dieser Konstruktion durch Vergleich mit der in Art. 354 der *Disquisitiones Arithmeticae* als Beispiel entwickelten Theorie des Siebzehnecks, so erkennt man leicht, dass sie lediglich die geometrische Übersetzung der Gleichungen ist, zu denen die Anwendung der allgemeinen Theorie führt. Tatsächlich sind die Entfernungen der Punkte C, D, E, F, G, I von A genau die Größen, die dort mit (8.1), (8.3), (4.1), (4.3), (4.9), (2.1) bezeichnet sind, wenn man das positive und negative Zeichen durch die Lage ausdrückt und die Entfernung des Punktes B von A im selben Sinn $= -1$ setzt. Das eigentliche Verdienst der Abhandlung von Herrn Erchinger liegt jedoch weniger in der Aufstellung der Konstruktion selbst, da die Analysis bereits den einfachsten Weg vorgezeichnet hatte, als in der rein geometrischen Begründung ihrer Richtigkeit. Diese ist mit so vorbildlicher, mühevoller Sorgfalt durchgeführt, um alles nicht rein Elementare zu vermeiden, dass sie dem Verfasser zur Ehre gereicht und den Wunsch weckt, sein tatsächlich nicht gewöhnliches mathematisches Talent möge jede Ermutigung finden.

Göttingische gelehrte Anzeigen. 9. Juli 1831.

Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen von Ludwig August Seeber, *Dr. der Philosophie, ordentlicher Professor der Physik an der Universität in Freiburg. Freiburg im Breisgau* 1831. (248 S. in 4.)

Die Funktionen zweier unbestimmter Größen x und y von der Gestalt $axx + 2bxy + cyy$, wobei a, b, c bestimmte ganze Zahlen bezeichnen, bilden bekanntlich unter dem Namen *quadratische Formen* oder, wenn eine weitere Unterscheidung nötig ist, *binäre quadratische Formen* einen der interessantesten und reichhaltigsten Gegenstände der höheren Arithmetik. Dabei stellen sich zunächst folgende Aufgaben: zu entscheiden, ob eine solche gegebene Form eine andere $a'x'x' + 2b'x'y' + c'y'y'$ enthält, also durch eine Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, in der $\alpha, \beta, \gamma, \delta$ ganze Zahlen sind, in diese überführt werden kann; ob eine solche Beziehung zwischen zwei Formen gegenseitig ist, in welchem Fall die Formen äquivalent heißen; ferner in beiden Fällen alle möglichen Umformungen der einen in die andere anzugeben; schließlich alle möglichen Darstellungen einer gegebenen ganzen Zahl durch eine gegebene Form mit ganzzahligen Werten der unbestimmten Größen zu finden. Diese Aufgaben sind in den *Disquisitiones Arithmeticae* vollständig gelöst, bilden aber nur den bei Weitem kleineren Teil des dortigen Abschnitts über quadratische Formen. Die folgenden feineren Untersuchungen erfordern zum Teil eine vorläufige Bearbeitung eines um eine Stufe höheren und viel größere Schwierigkeiten bietenden Gebiets: der Lehre von ähnlichen Funktionen dreier unbestimmter Größen x, y, z, die also die Gestalt $axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$ haben und ternäre quadratische Formen heißen. Die Lösung der Hauptaufgaben zu diesen ternären Formen ist in dem genannten Werk entwickelt, jedoch nur so weit, wie es für den angegebenen Zweck nötig war. Nach einem Abstand von dreißig Jahren hat nun der Verfasser des vorliegenden Werks diese Untersuchungen als Erster wieder aufgenommen und für eine Hauptgattung der ternären Formen, nämlich die positiven, das in den *Disquisitiones Arithmeticae* unvollendet Gelassene vervollständigt. Denjenigen, die sich eingehender mit der höheren Arithmetik beschäftigt haben, könnten wir mit wenigen Worten sagen, was in dem vorliegenden Werk neu geleistet wird. Um aber auch anderen verständlich zu sein, müssen wir uns etwas mehr Ausführlichkeit gestatten. Das tun wir umso lieber, als diese Untersuchungen auch außerhalb der höheren Arithmetik ein eigenes Interesse haben.

Die Eigenschaften einer binären Form $axx + 2bxy + cyy$ hängen vor allem von der Zahl $bb - ac$ ab, die daher die Determinante dieser Form heißt. Zwei äquivalente Formen haben immer gleiche Determinanten. Aber nicht al-

le Formen mit einer gegebenen Determinante sind deshalb schon äquivalent. Vielmehr zerfallen solche Formen in eine kleinere oder größere, stets jedoch endliche Anzahl von Klassen, sodass Formen derselben Klasse untereinander äquivalent sind, Formen verschiedener Klassen dagegen nicht. Durch Formen mit positiver Determinante lassen sich positive und negative Zahlen gleichermaßen darstellen; durch Formen mit negativer Determinante dagegen nur Zahlen, die dasselbe Vorzeichen wie a und c haben. Daher unterscheidet man hier positive und negative Formen. Die einfachsten Formen in jeder Klasse haben bestimmte Kriterien, heißen reduzierte Formen und können als Vertreter der ganzen Klasse betrachtet werden.

Ähnliche Verhältnisse für die ternären Formen sind in den *Disquisitiones Arithmeticae* nachgewiesen. Die Determinante der ternären Form

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

ist die Zahl

$$aa'a' + bb'b' + cc'c' - abc - 2a'b'c'$$

Auch hier ist die Gleichheit der Determinanten für die Äquivalenz zweier Formen notwendig, aber nicht hinreichend. Vielmehr zerfallen sämtliche Formen mit einer bestimmten Determinante in eine endliche Anzahl von Klassen, in denen jeweils die einfachsten Formen reduziert heißen und gleichsam alle übrigen vertreten können. Mit dem Unterschied zwischen positiven und negativen Formen verhält es sich hier aber anders als bei den binären Formen. Für jede gegebene Determinante, ob positiv oder negativ, gibt es einerseits Formen, durch die positive und negative Zahlen gleichermaßen darstellbar sind (indifferente Formen), andererseits Formen, durch die sich entweder nur positive oder nur negative Zahlen darstellen lassen (positive oder negative Formen). Positive Formen gibt es aber nur für negative Determinanten und negative Formen nur für positive. Im Übrigen ist von selbst klar, dass die Eigenschaft einer Form, indifferent, positiv oder negativ zu sein, zugleich der ganzen Klasse zukommt, zu der sie gehört. Das vorliegende Werk beschränkt sich auf positive Formen, deren Determinanten also negativ sein müssen. Alles, was für diese gilt, überträgt sich offensichtlich von selbst auf die negativen Formen, während die im Werk ganz ausgeschlossenen indifferenten Formen eine völlig andere Behandlung erfordern.

In den *Disquisitiones Arithmeticae* war, wie schon erwähnt, die Theorie der ternären Formen nur so weit entwickelt, wie es für den dortigen Zweck nötig war. Daher war die Aufgabe, die Äquivalenz zweier gegebener ternärer Formen zu entscheiden, noch nicht in voller Allgemeinheit gelöst. Zwar war dort gezeigt worden, wie man zu jeder vorgegebenen Form eine äquivalente Form der einfachsten Art findet und dass es für jede gegebene Determinante nur endlich viele solche reduzierten Formen geben kann. Da aber jede Klasse mehrere solche reduzierten Formen enthält, die sich nicht in allen Fällen

sofort als äquivalent erweisen, fehlte noch ein Kriterium, mit dem sich ihre Äquivalenz oder Nichtäquivalenz sicher erkennen lässt. Diesem Bedürfnis hat der Verfasser des vorliegenden Werks für die positiven Formen nun vollständig und mit vorbildlicher Gründlichkeit entsprochen. Sein Verfahren ist allerdings etwas anders eingekleidet, als wir die Sache gerade dargestellt haben und wie sie sich darstellen müsste, wenn man in den Begriff der reduzierten positiven Formen nur die wesentlichsten Bedingungen größter Einfachheit aufnimmt. Bei positiven Formen bestehen diese darin, dass die ihrer Natur nach positiven Zahlen a, b, c nicht kleiner sein dürfen als jeweils b' oder c', a' oder c', a' oder b', ohne Rücksicht auf die Vorzeichen. Herr Seeber hat den Begriff der reduzierten Formen um solche Bedingungen ergänzt, dass es in jeder Klasse immer nur eine solche Form geben kann, aber eine geben muss. Wegen eines schönen, von Herrn Seeber aus beobachteten Fällen gewonnenen Satzes, der weiter unten noch erwähnt wird, geben wir hier die Hauptbedingungen an, die Herr S. in den Begriff der reduzierten Formen aufgenommen hat: 1) Unter den Zahlen a', b', c' dürfen nicht zwei entgegengesetzte Vorzeichen haben; 2) ohne Rücksicht auf das Vorzeichen dürfen $2b'$ und $2c'$ nicht größer als a sein, ferner a und $2a'$ nicht größer als b und b nicht größer als c; 3) wenn a', b', c' zugleich negativ sind, darf die doppelte Summe dieser Zahlen nicht größer als $a + b$ sein. Die übrigen für einige Sonderfälle hinzukommenden Bedingungen können wir hier übergehen.

Den Hauptinhalt des Werks bilden nun zunächst die Lösung der Aufgabe, zu jeder gegebenen positiven Form eine äquivalente zu finden, die nach der festgelegten Definition den Charakter einer reduzierten Form hat, und dann der strenge Beweis des Satzes, dass zwei nicht identische reduzierte Formen nicht äquivalent sein können, oder, was dasselbe ist, dass jede Klasse nur eine reduzierte Form enthält. Dem Geist der Gründlichkeit, mit dem diese Gegenstände durchgeführt sind, müssen wir volle Gerechtigkeit widerfahren lassen. Und wenn wir dabei die sehr große, vielleicht manchen abschreckende Weitläufigkeit bedauern müssen, da die Lösung des Problems 41 Seiten und der Beweis des Satzes 91 Seiten einnimmt, so soll dies doch keineswegs als Tadel verstanden werden. Wenn ein schwieriges Problem zu lösen oder ein schwieriger Satz zu beweisen ist, besteht der erste und mit gebührendem Dank anzuerkennende Schritt stets darin, dass überhaupt eine Lösung oder ein Beweis gefunden wird. Die Frage, ob dies nicht leichter und einfacher hätte geschehen können, bleibt so lange müßig, wie die Möglichkeit nicht zugleich durch die Ausführung entschieden wird. Wir halten es daher für verfrüht, hier bei dieser Frage zu verweilen. — Der übrige Teil des Werks enthält hauptsächlich die mit gleicher Gründlichkeit ausgeführten Lösungen folgender Aufgaben: zu entscheiden, ob eine gegebene Form eine andere gegebene, ihr nicht äquivalente Form enthält; alle möglichen Transformationen einer gegebenen Form in eine gegebene äquivalente oder nur in ihr enthaltene Form

zu finden; schließlich für eine gegebene Determinante alle möglichen Klassen positiver ternärer Formen anzugeben.

Wir müssen noch bemerken, dass Herr SEEBER die Gestalt der ternären Formen etwas anders gefasst hat als die *Disquisitiones Arithmeticae*, wo die Koeffizienten der Produkte yz, xz, xy mit Bedacht als gerade Zahlen vorausgesetzt waren. Herr S. lässt dagegen auch ungerade zu und bezeichnet daher mit a', b', c', was oben mit $2a'$, $2b'$, $2c'$ bezeichnet war. Die dadurch erreichte größere Allgemeinheit ist offensichtlich nur scheinbar oder doch überflüssig, da sich alles, was über solche Formen mit ungeraden Koeffizienten gesagt werden kann, auch von selbst ergibt, wenn man stattdessen ihr Doppeltes betrachtet. Wir können diese Änderung daher nicht billigen, zumal sie auch einen gewissen Verlust an Einfachheit mit sich bringt. Eine Folge davon ist, dass das, was Herr SEEBER Determinante nennt, immer das Vierfache der Zahl ist, die in den *Disquisitiones Arithmeticae* diesen Namen trägt. In dieser Besprechung haben wir die Terminologie der *Disquisitiones Arithmeticae* beibehalten.

Beim zuletzt genannten Problem, für jede gegebene Determinante alle möglichen reduzierten Formen anzugeben, hat Herr SEEBER einen Satz benutzt, um Grenzen für die ersten drei Koeffizienten zu erhalten. Danach kann ihr Produkt abc nicht größer als das Dreifache der Determinante sein. Diesen Satz hat Herr SEEBER streng bewiesen. In der Vorrede bemerkt er jedoch, er habe unter mehr als 600 untersuchten Fällen keinen einzigen gefunden, in dem jenes Produkt das Doppelte der Determinante überschritten hätte. Daher hält er es für höchst wahrscheinlich, dass diese engere Grenze allgemein gilt; einen strengen Beweis habe er aber nicht finden können. Da dieser von Herrn SEEBER aus beobachteten Fällen gewonnene Satz sowohl an sich bemerkenswert als auch für eine kürzere Lösung der genannten Aufgabe wichtig ist, wollen wir hier einen sehr einfachen Beweis hinzufügen und damit auch unsererseits in dieser Besprechung zur Vervollkommnung der Theorie beitragen. Dabei sind zwei Fälle zu unterscheiden.

I. Wenn keine der Zahlen a', b', c' negativ ist, setze man

$$b - 2a' = d, \quad c - 2b' = e, \quad a - 2c' = f$$
$$c - 2a' = g, \quad a - 2b' = h, \quad b - 2c' = i$$

Aus der Definition der reduzierten positiven Formen folgt sofort: Wenn

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

eine solche Form ist, ist keine dieser sechs Zahlen negativ. Ebenso versteht sich von selbst, dass a, b, c positiv sind. Bezeichnet man nun die (negative) Determinante der Form mit $-D$, so gilt die identische Gleichung, von der man sich leicht durch Ausmultiplizieren überzeugt,

$$2D - abc = aa'd + bb'e + cc'f + a'hi + b'gi + c'gh + ghi$$

in der keiner der sieben Terme rechts negativ sein kann. Folglich ist abc nicht größer als $2D$. Dasselbe folgt auf die gleiche Weise aus der identischen Gleichung

$$2D - abc = aa'g + bb'h + cc'i + a'ef + b'df + c'de + def$$

II. Wenn keine der Zahlen a', b', c' positiv ist, setze man

$$\begin{aligned} b + 2a' &= d, \quad c + 2b' = e, \quad a + 2c' = f \\ c + 2a' &= g, \quad a + 2b' = h, \quad b + 2c' = i \end{aligned}$$

$$\begin{aligned} b + c + 2a' + 2b' + 2c' &= k \\ a + c + 2a' + 2b' + 2c' &= l \\ a + b + 2a' + 2b' + 2c' &= m \end{aligned}$$

und die Determinante der Form wie zuvor $= -D$. Nach der Definition der reduzierten positiven Formen kann keine der neun Zahlen $d, e, f, g, h, i, k, l, m$ negativ sein. Aus der identischen Gleichung

$$\begin{aligned} 6D - 3abc = & - aa'(d + 2k) - bb'(e + 2l) - cc'(f + 2m) \\ & - a'hi - b'gi - c'gh + def + 2ghi \end{aligned}$$

in der alle Terme rechts positiv oder null sind, weil a', b', c' nicht positiv, sondern negativ oder null sind, ergibt sich daher, dass $3abc$ nicht größer als $6D$ oder abc nicht größer als $2D$ sein kann. Dasselbe folgt ebenso aus der identischen Gleichung

$$\begin{aligned} 6D - 3abc = & - aa'(g + 2k) - bb'(h + 2l) - cc'(i + 2m) \\ & - a'ef - b'df - c'de + 2def + ghi \end{aligned}$$

Beide Gleichungen sind symmetrisch. Verzichtet man auf vollständige Symmetrie, so lässt sich der Beweis mit noch weniger Termen führen, zum Beispiel durch die identische Gleichung

$$\begin{aligned} 8D - 4abc = & - 2aa'(g + k) - 2bb'(e + l) - 4cc'm \\ & + (c + e)df + (c + g)hi \end{aligned}$$

Wir wollen nun noch einiges über die Bedeutung der positiven binären und ternären quadratischen Formen außerhalb der höheren Arithmetik hinzufügen. Die negativen Formen gesondert zu behandeln ist unnötig, und die indifferenten entziehen sich dieser Behandlung ganz.

Die positive binäre Form $axx + 2bxy + cyy$ stellt allgemein das Quadrat der Entfernung zweier unbestimmter Punkte in einer Ebene dar, deren Koordinaten sich in Bezug auf zwei gegeneinander geneigte Achsen, deren Winkel den Kosinus $= \frac{b}{\sqrt{ac}}$ hat, um $x\sqrt{a}$, $y\sqrt{c}$ unterscheiden. Wenn x und y also nur *ganze* Zahlen bedeuten sollen, bezieht sich die Form auf ein System von in Parallelogrammen angeordneten Punkten, die in den Schnittpunkten zweier Systeme paralleler Geraden liegen. Die Geraden jedes Systems haben gleiche Abstände voneinander: Die Abstände des einen Systems, parallel zu den Geraden des zweiten gemessen, sind $= \sqrt{a}$, die Abstände des anderen, parallel zu den Geraden des ersten gemessen, $= \sqrt{c}$; die Neigung der beiden Systeme ist die oben angegebene. So erscheint die Ebene vollständig in gleiche Parallelogramme geteilt, deren Eckpunkte das Punktesystem bilden, ohne dass irgendeiner dieser Punkte ins Innere eines Parallelogramms fallen kann. Die mit positivem Vorzeichen genommene Determinante, also $ac - bb$, bedeutet das Quadrat des Flächeninhalts eines elementaren Parallelogramms. Ein und dasselbe System solcher Punkte kann auf unendlich viele verschiedene Arten in Parallelogramme eingeteilt und daher auf ebenso viele verschiedene Formen bezogen werden. Alle diese verschiedenen Formen sind aber, wie es in der Fachsprache heißt, äquivalent, und der Flächeninhalt eines elementaren Parallelogramms bleibt immer derselbe. Zwei nicht äquivalente Formen, von denen aber die eine die andere enthält, beziehen sich auf dasselbe Punktesystem: die erste Form auf das ganze System, die zweite auf einen Teil. Zwei Formen, die in der Fachsprache uneigentlich äquivalent (improprie aequivalentes) heißen, beziehen sich auf zwei gleiche, aber entgegengesetzt liegende Punktesysteme, wobei man sich die Ebene umgekehrt gelegt denkt, und so weiter.

Auf die gleiche Weise bedeutet die positive ternäre Form

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

allgemein das Quadrat der Entfernung zweier unbestimmter Punkte im Raum, deren Koordinaten in Bezug auf drei Achsen (1), (2), (3) die Unterschiede $x\sqrt{a}$, $y\sqrt{b}$, $z\sqrt{c}$ ergeben: Die Kosinus der Winkel zwischen den Achsen (2) und (3), (1) und (3), (1) und (2) sind jeweils $\frac{a'}{\sqrt{bc}}$, $\frac{b'}{\sqrt{ac}}$, $\frac{c'}{\sqrt{ab}}$. Wenn x, y, z hier nur ganze Zahlen bedeuten sollen, bezieht sich die Form auf ein System von in Parallelepipeden angeordneten Punkten, die also durch die Schnittpunkte dreier Systeme paralleler, gleichabständiger Ebenen entstehen. Der ganze Raum erscheint so vollständig in gleiche Parallelepipede geteilt, deren Eckpunkte jenes Punktesystem bilden. Das Quadrat des Rauminhalts eines elementaren Parallelepipeds ist gleich der mit positivem Vorzeichen genommenen Determinante der ternären Form. Äquivalente Formen vertreten ein und dasselbe Punktesystem, nur auf andere Achsen oder Grundebenen bezogen. Ebenso finden alle anderen Hauptbestandteile der Theorie der ternären Formen hier

ihre geometrische Bedeutung: das Enthaltensein einer Form in einer anderen, die Darstellung einer bestimmten Zahl oder einer unbestimmten binären Form durch eine ternäre, die Lehre von den zugeordneten ternären Formen (formae adiunctae), der Wegfall des Unterschieds zwischen eigentlicher und uneigentlicher Äquivalenz, das Wesen der reduzierten Formen und so weiter. Wir müssen uns jedoch auf die obigen Andeutungen beschränken, zumal das vorliegende Werk, das die ternären Formen ausschließlich aus rein arithmetischer Sicht betrachtet, nur mittelbar dazu Anlass gegeben hat. Man wird daraus wenigstens erkennen, welch reiches Feld sich hier für Untersuchungen eröffnet, die nicht nur für sich ein hohes theoretisches Interesse haben, sondern auch zu einer ebenso bequemen wie allgemeinen Behandlung aller Beziehungen zwischen den Kristallformen dienen können. Auf die Einzelheiten dieser Anwendung einzugehen ist hier nicht der Ort. Wir dürfen jedoch nicht übergehen, dass, obwohl ursprünglich angenommen wurde, a, b, c, a', b', c' bezeichneten ganze Zahlen, der größte Teil der Lehre von den ternären Formen und insbesondere das für jene Anwendung Erforderliche auch unabhängig von dieser Voraussetzung gültig bleibt. Tatsächlich führen zwar die Angaben von Haüy bei den meisten Kristallarten auf sehr einfache ganzzahlige Werte der Koeffizienten der ternären Formen, die sich auf die entsprechende Anordnung des Punktesystems beziehen. Die genaueren späteren Messungen von Wollaston, Malus, Biot, Kupffer und anderen widersprechen dem jedoch und lassen es zweifelhaft erscheinen, ob rationale Verhältnisse dieser Koeffizienten überall der Natur entsprechen. Wenn man in der Theorie aber die Beschränkung auf ganzzahlige Koeffizienten nicht weglassen will, lassen sich jedenfalls immer ganze Zahlen finden, die den Messergebnissen beliebig nahe kommen, da es dabei nur auf die Verhältnisse untereinander und nicht auf absolute Werte ankommt.

Schließlich wollen wir dem oben angeführten Satz von Seeber noch seine geometrische Bedeutung geben. Wenn ein Parallelepiped so beschaffen ist, dass keine seiner zwölf Kanten, von denen jeweils vier gleich sind, größer ist als irgendeine der zwölf Diagonalen der Seitenflächen, die paarweise gleich sind, oder irgendeine der vier Diagonalen des Parallelepipeds, dann ist sein mit $\sqrt{2}$ multiplizierter Rauminhalt nicht kleiner als der Rauminhalt eines aus denselben Kanten gebildeten rechtwinkligen Parallelepipeds.

HANDSCHRIFTLICHER

NACHLASS.

LÖSUNG DER KONGRUENZ $X^m - 1 \equiv 0$.

LEHRE VON DEN RESTEN. SECHSTES KAPITEL. ERSTER TEIL.

237.

In Kapitel III haben wir gezeigt, dass die Kongruenz $x^n \equiv 1$, wenn eine Primzahl p als Modul genommen wird, μ Wurzeln hat, wobei μ der größte gemeinsame Teiler der Zahlen n und $p-1$ ist, und dass diese Wurzeln mit denen der Kongruenz $x^\mu \equiv 1$ genau übereinstimmen. Es genügt daher, den Fall zu betrachten, dass n ein Teiler von $p-1$ ist. Dass sich aber nicht nur die Lösung der Kongruenz $x^n - 1 \equiv 0$, sondern auch die jeder anderen Kongruenz für beliebige Moduln aus ihrer Lösung für Primzahlmoduln ableiten lässt, wurde schon an verschiedenen Stellen gezeigt und wird weiter unten (Kapitel VIII) ausführlicher entwickelt.

238.

Doch auch hier brauchen wir nicht stehen zu bleiben. In demselben Kapitel III haben wir dargelegt, dass die Lösung der Kongruenz $x^n \equiv 1$ von der Lösung ähnlicher Kongruenzen $x^a \equiv 1$, $x^b \equiv 1$ usw. abhängt, wobei a, b usw. Primzahlen oder Primzahlpotenzen sind und n das Produkt dieser Zahlen ist. Sind nämlich A, B usw. jeweils beliebige Wurzeln der Kongruenzen $x^a \equiv 1$, $x^b \equiv 1$ usw., so ist ihr Produkt $AB\ldots$ eine der Wurzeln der Kongruenz $x^n \equiv 1$. Unsere Untersuchungen beschränken sich daher auf die Lösung der Kongruenz $x^n \equiv 1 \pmod{p}$, wobei p eine Primzahl und n eine Primzahl oder Primzahlpotenz und zugleich ein Teiler von $p-1$ ist.

239.

Aus Kapitel III ist ferner bekannt, dass es unter den Wurzeln der Kongruenz $x^n \equiv 1$ immer solche gibt, durch deren Potenzen sich alle übrigen darstellen lassen. Bezeichnet also r eine solche Wurzel (wir haben sie oben *primitiv* genannt, wenn $n = p-1$, und behalten diesen Ausdruck hier bei, wenn auch in weiterem Sinn), so sind alle Wurzeln der gegebenen Kongruenz

$$1,\ r,\ rr,\ r^3 \quad \ldots\ldots \quad r^{n-1}$$

Wir müssen daher alle Anstrengungen darauf richten, solche Wurzeln zu finden, da sich die übrigen von selbst ergeben, sobald diese gefunden sind. Der Kürze halber bezeichnen wir jede Potenz von r durch ihren in Klammern eingeschlossenen Exponenten. Dabei bezeichnet (0) die Eins, (1) eine beliebige primitive Wurzel der Kongruenz $x^n \equiv 1$, (2) das Quadrat von (1) usw., sodass die Folge (0), (1), (2), (3), $\ldots$ $(n-1)$ alle Wurzeln umfasst. Ferner ist bekannt, dass (k) immer eine solche primitive Wurzel ist, wenn k zu n

teilerfremd ist, also in unserem Fall, in dem n eine Potenz der Primzahl t, $= t^\nu$, ist, immer dann, wenn t die Zahl k nicht teilt. Die Zeichen (1), (2) usw. sind für sich genommen offensichtlich unbestimmt. Sobald aber (1) ein bestimmter Wert gegeben wird, sind auch alle übrigen bestimmt.

240.

Da wir vor den übrigen vor allem die primitiven Wurzeln untersuchen wollen, müssen wir diese zunächst von den anderen trennen. Das geschieht, indem wir aus der Folge $(0), (1), (2) \ldots (n-1)$ alle Terme (k) entfernen, bei denen k durch t teilbar ist. Ist aber n eine Primzahl oder $\nu = 1$, so ist nur (0) zu entfernen. Bevor wir die verbleibenden Wurzeln untersuchen, empfehlen wir dem Leser nachdrücklich, sich einige Beispiele zu bilden, damit er alles, was ohne diese vielleicht zu allgemein gehalten erschiene, konkret vor sich sieht. Wir fügen ein Beispiel hinzu; dadurch wird es aber nicht überflüssig, andere selbstständig auszuarbeiten.

Es sei $p = 29$; $n = 7$. Die sieben Wurzeln der Kongruenz $x^7 \equiv 1 \pmod{29}$ sind dann $1, 7, 16, 20, 23, 24, 25$. Da n eine Primzahl ist, sind alle diese Wurzeln außer 1 primitiv. Setzt man also $7 = (1)$, so haben die Zeichen folgende Bedeutungen:

(0)	(1)	(2)	(3)	(4)	(5)	(6)
1	7	20	24	23	16	25

Man wird sich außerdem erinnern, dass die Zeichen (n) und (0), $(n+1)$ und (1) usw. und allgemein (a) und (b) gleichbedeutend sind, wenn $a \equiv b \pmod{n}$.

241.

Für unser Vorhaben müssen wir aber noch auf eine andere Weise vorgehen. Wir behalten nämlich nur die Terme (k), bei denen k nicht durch t teilbar ist; ihre Anzahl ist $\frac{t-1}{t} . n = \lambda$. Alle diese Zahlen oder ihnen modulo n kongruente Zahlen lassen sich durch aufeinanderfolgende Potenzen einer Zahl darstellen. Diese sei $= \rho$; dann werden alle primitiven Wurzeln der Kongruenz $x^n \equiv 1$ so bezeichnet:

$$(1) \quad (\rho) \quad (\rho^2) \quad (\rho^3) \quad \ldots . \quad (\rho^{\lambda-1})$$

Durch dieses Verfahren erreichen wir, dass sämtliche nicht primitiven Wurzeln vollständig ausgeschlossen werden. Die Gründe und Vorteile werden weiter unten deutlicher. In unserem Beispiel können wir also $\rho = 3$ setzen; die primitiven Wurzeln der Kongruenz $x^7 \equiv 1$ sind dann folgendermaßen angeordnet:

	(1)	(3)	(3^2)	(3^3)	(3^4)	(3^5)
oder	(1)	(3)	(2)	(6)	(4)	(5)
das sind	7	24	20	25	23	16

242.

Damit der Leser das Ziel der folgenden Untersuchungen kennt, ist es zweckmäßig, den Satz anzugeben, den wir beweisen und erläutern wollen.

Hat die Zahl λ, die $= t^{\nu-1}\,.\,t-1$ ist, die Primfaktoren a, b, c, d usw., und ist $\lambda = a^\alpha b^\beta c^\gamma \ldots$, so hängt die Lösung der Kongruenz $x^n - 1 \equiv 0$ von der Lösung von $\alpha + \beta + ..$ Kongruenzen niedrigeren Grades ab, von denen α den Grad a, β den Grad b, γ den Grad c haben usw.

In unserem Beispiel hängt also die Lösung der Kongruenz $x^7 \equiv 1$ von einer Kongruenz zweiten und einer weiteren dritten Grades ab. Allgemein erkennt man, dass der Grad dieser Kongruenzen niemals vom Modul p abhängt. Um zum Beweis dieses Satzes zu gelangen, müssen wir aber einige Sätze über den Zusammenhang zwischen Kongruenzen und ihren Wurzeln vorausschicken, obwohl diese Untersuchungen eigentlich erst im achten Kapitel weiterzuverfolgen sind.

243.

Satz. *Die Kongruenz*

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots . + N \equiv 0 \text{ (Primzahlmodul)}$$

sei so beschaffen, dass nach dem Ausmultiplizieren des Produkts aus den m Faktoren $x - r$, $x - r'$, $x - r''$, $x - r'''$ ..., das $x^m + ax^{m-1} + bx^{m-2} \ldots + n$ ergebe, die Beziehungen $A \equiv a$, $B \equiv b$, $C \equiv c$ usw. modulo p gelten. Dann sind die Größen $r, r', r'' \ldots$ Wurzeln der gegebenen Kongruenz, und sie hat keine anderen.

Beweis. I. Es gilt immer

$$\begin{aligned} x^m + Ax^{m-1} + Bx^{m-2} + \ldots \\ \equiv x^m + ax^{m-1} + bx^{m-2} + \ldots \pmod{p} \end{aligned}$$

Die rechte Seite der Kongruenz wird aber $= 0$, wenn man $x = r$, $x = r'$, $x = r''$ usw. setzt. Für diese Werte von x wird daher die linke Seite $\equiv 0 \pmod{p}$. Damit ist der erste Teil bewiesen.

II. Würde noch ein weiterer Wert ρ, der keiner der Zahlen r, r' usw. kongruent ist, die gegebene Kongruenz erfüllen, so wäre

$$\begin{aligned} 0 &\equiv \rho^m + A\rho^{m-1} + B\rho^{m-2} + \ldots \\ &\equiv \rho^m + a\rho^{m-1} + b\rho^{m-2} + \ldots \\ &\equiv (\rho - r)(\rho - r')(\rho - r'')(\rho - r''') \ldots \end{aligned}$$

Da aber keiner der Faktoren $\rho - r$, $\rho - r'$, $\rho - r''$ usw. $\equiv 0$ ist, ist es unmöglich, dass ihr Produkt $\equiv 0$ ist, weil p eine Primzahl ist. Außer den Wurzeln r, r' usw. gibt es also keine anderen. Damit ist der zweite Teil bewiesen.

244.

AUFGABE. *Es seien $r, r', r'' \ldots$ unbekannte Größen, deren Anzahl $= m$, deren Summe $= \alpha$, deren Summe der Quadrate $= \beta$, deren Summe der Kuben $= \gamma \ldots$ und deren Summe der Potenzen mit Exponenten m gleich $= \mu$ sei. Gegeben seien aber nicht diese Zahlen selbst, deren Anzahl ebenfalls $= m$ ist, sondern andere Zahlen α', β', γ' usw., die ihnen einzeln modulo p kongruent sind, wobei dieser Modul eine Primzahl und $> m$ sei. Gesucht ist eine Kongruenz des Grades m, deren Wurzeln r, r', r'' usw. sind.*

Lösung. Man betrachte r, r', r'' usw. als Wurzeln einer Gleichung

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \ldots = 0$$

und bestimme ihre Koeffizienten A, B, C usw. nach der bekannten Methode, wobei nur die Kongruenz an die Stelle der Gleichheit tritt. Man setze also

$$\begin{aligned} -A &\equiv \alpha' \\ -2B &\equiv \beta' + A\alpha' \\ -3C &\equiv \gamma' + A\beta' + B\alpha' \\ -4D &\equiv \delta' + A\gamma' + B\beta' + C\alpha' \\ &\text{usw.} \\ -mN &\equiv \mu' + A\lambda' + \text{usw.} \end{aligned}$$

Diese Koeffizienten können nicht unbestimmt sein, weil alle Zahlen $1, 2, 3 \ldots m < p$. Ich behaupte, dass die Kongruenz

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots + N \equiv 0$$

die gesuchte ist.

Beweis. Die Gleichung, deren Wurzeln r, r', r'', r''' usw. sind, sei

$$x^m + ax^{m-1} + bx^{m-2} + \ldots = 0$$

Dann gilt

$$\begin{aligned} -a &= \alpha \\ -2b &= \beta + a\alpha \\ -3c &= \gamma + a\beta + b\alpha \\ -4d &= \delta + a\gamma + b\beta + c\alpha \\ &\text{usw.} \end{aligned}$$

Daraus wird jedem klar, dass

$$a \equiv A, \quad b \equiv B, \quad c \equiv C \text{ usw. } (\text{mod. } p)$$

Also sind nach dem vorigen Abschnitt die Zahlen r, r', r'' usw., die Wurzeln der *Gleichung*

$$x^m + ax^{m-1} + bx^{m-2} + \ldots = 0$$

sind, zugleich Wurzeln der *Kongruenz*

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots \equiv 0 \qquad \text{Q. E. D.}$$

Wir überlassen es den Lesern, sich Beispiele zu bilden.

245.

Wir kehren zu unserem Vorhaben zurück. Mit den in den Abschnitten 242 und zuvor verwendeten Zeichen wollen wir zeigen: Ist λ das Produkt beliebiger Faktoren efg usw., so können die primitiven Wurzeln der Kongruenz $x^n \equiv 1$, deren Anzahl λ ist, so in e Klassen eingeteilt werden, dass die Summen der jeweils derselben Klasse zugeordneten Wurzeln durch eine Kongruenz des Grades e gegeben werden. Setzt man diese als bekannt voraus, so lässt sich jede Klasse weiter so in f Gruppen unterteilen, dass die Summe jeder Gruppe durch eine Kongruenz des Grades f gegeben wird. Diese Gruppen lassen sich wiederum unterteilen usw., bis man zu den einzelnen Wurzeln gelangt.

246.

Definition. Die Gesamtheit *aller* Terme, die in einer solchen Form $(\rho^{ke+\alpha})$ (Abschnitt 241) enthalten sind, nennen wir eine *vollständige Periode* oder einfach eine *Periode*. Dabei bezeichnet e einen beliebigen Teiler von λ, α eine beliebige gegebene Zahl und k alle ganzen Zahlen von 0 bis $\frac{\lambda}{e} - 1$. Der Kürze halber bezeichnen wir eine solche Periode mit $(e * \alpha)$. So bilden in unserem Beispiel die Terme

	(1), (2), (4)	Perioden	$(2 * 0)$	,
	(3), (6), (5)		$(2 * 1)$	
diese aber	(1), (6)	diese	$(3 * 0)$	
	(3), (4)		$(3 * 1)$	
	(2), (5)		$(3 * 2)$	

Wenn nun alle Terme auf beliebige Weise in Perioden verteilt werden, die einzelnen Perioden wiederum in kleinere Perioden usw., so behaupten wir, dass damit das im vorigen Abschnitt Versprochene erreicht wird.

Bevor wir diese Darstellung selbst beginnen, zeigen wir jedoch, dass die Bildung einer solchen Periode nichts Unbestimmtes enthält, obwohl sie von

den beiden in gewisser Weise willkürlichen Größen r, ρ abhängt. Wie auch immer diese Größen gewählt werden, kommen stets dieselben Terme in dieselbe Periode, sofern vorgeschrieben ist, wie viele Terme die Periode enthalten soll.

Das Kriterium dafür, dass zwei Terme A, B in derselben Periode liegen, ergibt sich daraus, dass beide in einer solchen Form $(\rho^{ke+\alpha})$ enthalten sind, also $A \equiv r^{\rho^{ke+\alpha}}$, $B \equiv r^{\rho^{k'e+\alpha}} \pmod{p}$. Dabei ist r eine primitive Wurzel der Kongruenz $x^n \equiv 1 \pmod{p}$ und ρ eine primitive Wurzel der Kongruenz $x^\lambda \equiv 1 \pmod{n}$; siehe oben.

Zu beweisen ist: Werden anstelle der Zahlen r, ρ andere, etwa s, σ, gewählt, so sind A und B in ähnlichen Formen $s^{\sigma^{le+\beta}}$, $s^{\sigma^{l'e+\beta}}$ enthalten.

Es sei $s^m \equiv r \pmod{p}$; $\sigma^\mu \equiv \rho \pmod{n}$ und $m \equiv \sigma^\zeta \pmod{n}$, was möglich ist, weil r, ρ primitive Wurzeln sind. Dabei ist m zu n und μ zu λ teilerfremd (Kapitel III). Durch die entsprechenden Substitutionen erhalten wir

$$A \equiv s^{\sigma^{\mu ke+\mu\alpha+\zeta}}, \qquad B = s^{\sigma^{\mu k'e+\mu\alpha+\zeta}} \qquad \text{Q. E. D.}$$

247.

Satz. *Das Produkt zweier gleichartiger Perioden lässt sich unabhängig von der Zahl p durch Addition gleichartiger Perioden und gegebener Zahlen bilden.*

(Perioden heißen gleichartig, wenn sie gleich viele Terme enthalten oder die Zahl e dieselbe ist.)

Beispiel. Es sei $n = 7$. Das Produkt der Perioden $(1) + (6)$ und $(2) + (5)$ ist wegen $(a) \times (b) = (a + b)$ gleich $(3) + (6) + (8) + (11)$, besteht also aus den Perioden $(3) + (4)$ und $(1) + (6)$.

Beweis. Es sei $\frac{\lambda}{e} = f$, und die gegebenen Perioden seien $(e*\alpha)$ und $(e*\beta)$ oder die Summen

$$(\rho^\alpha) + (\rho^{\alpha+e}) + (\rho^{\alpha+2e}) + \ldots + (\rho^{\alpha+(f-1)e}) \;\ldots\ldots\; P$$
$$(\rho^\beta) + (\rho^{\beta+e}) + (\rho^{\beta+2e}) + \ldots + (\rho^{\beta+(f-1)e}) \;\ldots\ldots\; Q$$

Das Produkt PQ besteht aus f^2 Termen. Diese ordne man folgendermaßen an. Man bilde f Zeilen, deren jede aus f Termen besteht. Die erste enthalte das Produkt von P mit (ρ^β), die zweite das Produkt $P\,.\,(\rho^{\beta+e})$ usw. usw. In der ersten Zeile nehme das aus dem Term (ρ^α) entstehende Produkt die erste Stelle ein, das aus $(\rho^{\alpha+e})$ entstehende die zweite, und so weiter der Reihe nach. In der zweiten Zeile weise man die erste Stelle dem aus $(\rho^{\alpha+e})$ entstehenden Produkt zu, die zweite dem aus $(\rho^{\alpha+2e})$ entstehenden usw. und schließlich die letzte dem aus (ρ^α) entstehenden. Die dritte beginne mit dem aus $(\rho^{\alpha+2e})$ entstehenden Produkt, und so fahre man fort; auf das Produkt aus dem letzten Term folgen die Produkte aus dem ersten und zweiten usw.

usw. Bezeichnet man also die aufeinanderfolgenden Terme der Periode P mit $1, 2, 3 \ldots z$ und die der Periode Q mit $\mathrm{I}, \mathrm{II}, \mathrm{III}, \ldots . Z$, so ordne man die Teile von PQ folgendermaßen an:

$$\begin{aligned} &1 \,.\, \mathrm{I} + 2 \,.\, \mathrm{I} + 3 \,.\, \mathrm{I} + 4 \,.\, \mathrm{I} + \ldots + z \,.\, \mathrm{I} \\ &2 \,.\, \mathrm{II} + 3 \,.\, \mathrm{II} + 4 \,.\, \mathrm{II} + \ldots . + 1 \,.\, \mathrm{II} \\ &3 \,.\, \mathrm{III} + 4 \,.\, \mathrm{III} + \ldots + 1 \,.\, \mathrm{III} + 2 \,.\, \mathrm{III} \\ &\qquad \text{usw.} \quad \text{usw.} \end{aligned}$$

Dann fasse man alle Terme, die in den einzelnen Zeilen dieselbe Stelle einnehmen, zu f Gruppen zusammen. Ich behaupte:
1° Ist irgendein Term $\equiv 1$, so sind alle übrigen Terme derselben Gruppe ebenfalls $\equiv 1$
2° Jede Gruppe, in der kein Term $\equiv 1$ ist, bildet eine Periode. — Sobald dies bewiesen ist, haben wir unser Ziel offensichtlich erreicht.

Die allgemeine Form einer solchen Gruppe ist

$$\begin{gathered} (\rho^{\alpha+ke} + \rho^{\beta}), \quad (\rho^{\alpha+(k+1)e} + \rho^{\beta+e}), \quad (\rho^{\alpha+(k+2)e} + \rho^{\beta+2e}), \\ \ldots \; (\rho^{\alpha+(k+f-1)e} + \rho^{\beta+(f-1)e}) \end{gathered}$$

Denn für $\rho^{\alpha+(k-1)e}$ kann auch $\rho^{\alpha+(k+f-1)e}$ geschrieben werden, weil $ef = \lambda$ und $\rho^{\lambda} \equiv 1 \pmod{n}$ gelten, und ebenso für die vorhergehenden Terme. Man setze $\rho^{\alpha+ke} + \rho^{\beta} \equiv \rho^{\chi} \pmod{n}$, was erlaubt ist, sofern nicht $\rho^{\alpha+ke} + \rho^{\beta}$ durch n teilbar ist[*)]. Dann lässt sich die Gruppe so darstellen: (ρ^{χ}), $(\rho^{\chi+e})$, $(\rho^{\chi+2e}) \ldots (\rho^{\chi+(f-1)e})$. Sie ist offensichtlich die Periode $(e * \chi)$. Ist dagegen $\rho^{\alpha+ke} + \rho^{\beta}$ durch n teilbar, so sind alle Terme der Gruppe $\equiv (0)$, also $\equiv 1$. Q. E. D.

Anmerkung. Dieser Beweis zeigt zugleich ein sehr einfaches Verfahren, um das Produkt zu entwickeln. Weiter unten geben wir ein anderes, das zwar diesen Vorzug nicht hat, aber wegen seiner Einfachheit nicht unbeachtlich erscheint.

[*)] Die Aussage muss etwas anders formuliert werden, wenn n allgemein eine Primzahlpotenz bezeichnet; ist es dagegen eine Primzahl, so muss nichts geändert werden.

248.

Alle kleineren Perioden, die eine größere Periode bilden, nennen wir ein Periodensystem. So erhalten die Perioden

$$(ef * \alpha), \quad (ef * f + \alpha), \quad (ef * 2f + \alpha) \ \ldots . \ (ef * (e-1)f + \alpha)$$

aus denen die Periode $(f * \alpha)$ besteht, diesen Namen. Das System ist *ordnungsgemäß angeordnet*, wenn die Zahlen hinter dem Zeichen $*$, hier α, $f+\alpha$, $2f+\alpha$, eine arithmetische Folge mit Differenz f bilden. Schließlich heißen die Systeme *gleichartig*, wenn sowohl die kleineren als auch die größeren Perioden gleichartig sind.

Satz. *Werden die Perioden zweier gleichartiger, ordnungsgemäß angeordneter Systeme miteinander multipliziert, nämlich die erste mit der ersten, die zweite mit der zweiten, die dritte mit der dritten usw., so lässt sich die Summe aller Produkte aus gegebenen Zahlen und Perioden bilden, die der größeren Periode gleichartig sind.*

Beweis. Die Systeme seien

$$\begin{aligned} &(ef * \alpha), \quad (ef * \alpha + f), \quad (ef * \alpha + 2f) \ldots \\ &(ef * \beta), \quad (ef * \beta + f), \quad (ef * \beta + 2f) \ldots \end{aligned}$$

Die Produkte der einzelnen Perioden des ersten Systems mit den entsprechenden Perioden des zweiten bestehen nach dem vorigen Abschnitt aus ganzen Zahlen und gleichartigen Perioden. Betrachtet man die Entstehung dieser Perioden mit etwas Aufmerksamkeit, so erkennt man: Besteht $(ef*\alpha)\times(ef*\beta)$ aus einer ganzen Zahl N und den Perioden $(ef * A)$, $(ef * B)$, $(ef * C)$ usw., so ergeben sich die Produkte

$$\begin{aligned} &(ef * \alpha + f) \times (ef * \beta + f) \text{ aus } N \text{ und Perioden} \\ &\qquad (ef * A + f), \quad (ef * B + f), \quad (ef * C + f) \text{ usw.} \\ &(ef * \alpha + 2f) \times (ef * \beta + 2f) \text{ aus } N \text{ und Perioden} \\ &\qquad (ef * A + 2f), \quad (ef * B + 2f), \quad (ef * C + 2f) \text{ usw.} \end{aligned}$$

und allgemein

$$\begin{aligned} &(ef * \alpha + \mu f) \times (ef * \beta + \mu f) \text{ aus } N \text{ und Perioden} \\ &\qquad (ef * A + \mu f), \quad (ef * B + \mu f), \quad (ef * C + \mu f) \text{ usw.} \end{aligned}$$

Daraus folgt unmittelbar, dass die Summe aller Perioden

$$eN + (f * A) + (f * B) + (f * C) \text{ usw.} \qquad \text{Q. E. D.}$$

ist. Auch dieser Beweis liefert ein Verfahren, um jene Summe zu finden.

249.

Dieser Satz lässt sich leicht noch verallgemeinern: Hat man beliebig viele gleichartige, ordnungsgemäß angeordnete Systeme und bildet die Produkte aller ersten Perioden, aller zweiten usw., so besteht die Summe all dieser Produkte aus Zahlen und größeren Perioden. Nimmt man alle diese Systeme als gleich an, so besteht die Summe der Potenzen aller Perioden bei beliebigem Exponenten aus Zahlen und Perioden, die der größeren gleichartig sind. Schon daraus wird das Ziel dieser Untersuchungen klar. Es sei $\lambda = efgh\ldots$. Man zerlege alle primitiven Wurzeln in e Perioden A, A', A'' usw., jede dieser Perioden wiederum in f: B, B', B'' usw., und jede davon in g: C, C', C'' usw. Die Summe aller Perioden ist gegeben, nämlich $\equiv -1$. Nach dem gerade Dargelegten sind aber auch

$$(A)^2 + (A')^2 + (A'')^2 + (A''')^2 + \text{usw.}$$
$$(A)^3 + (A')^3 + (A'')^3 + (A''')^3 + \text{usw.}$$
$$\text{usw. usw.}$$

gegeben.

Daraus lässt sich nach Abschnitt 244 eine Kongruenz des Grades e finden, deren Wurzeln A, A', A'' usw. sind. Setzt man diese nun als bekannt voraus, so zerlege man jede Periode in kleinere:

$$\begin{array}{lllll} A & \text{in} & B, & B', & B''\ldots \\ A' & \text{in} & B^{(n)}, & B^{(n+1)}, & B^{(n+2)}\ldots \end{array}$$
usw.

Also ist $B + B' + B'' + \ldots \equiv A$ gegeben. Nun bestehen aber

$$(B)^2 + (B')^2 + (B'')^2 + \ldots$$
$$(B)^3 + (B')^3 + (B'')^3 + \ldots$$
$$\text{usw.}$$

aus Einheiten und den Perioden A, A', A'' usw. Daher sind B, B', B'' usw. durch eine Kongruenz des Grades f gegeben, aus der sie gefunden werden können. Ebenso lassen sich die Perioden bestimmen, aus denen A', A'' usw. bestehen. Daraus wird jeder erkennen, dass sich jede Periode auf genau dieselbe Weise in kleinere unterteilen lässt, bis man zu den Wurzeln selbst gelangt.

250.

Bei der Anwendung dieser Regeln tritt aber eine Schwierigkeit auf, die wir beseitigen müssen. Da jede Kongruenz mehrere Wurzeln hat, müssen wir sehen, welches Zeichen jeder zuzuweisen ist, damit sie sich richtig voneinander unterscheiden lassen. Die Bezeichnung der Perioden hängt von den Zahlen r, ρ

ab, die beliebig gewählt werden können. Daher muss auch der Bezeichnung etwas Willkürliches anhaften. Die Zahl ρ muss allerdings schon zu Beginn festgelegt werden. Das Wesen unserer Methode besteht vor allem darin, aus größeren Perioden kleinere abzuleiten. Ohne die richtige Anordnung der Perioden, die wir durch die *Zeichen* erreicht haben, ist das aber nicht möglich. Wir müssen daher dafür sorgen, dass alle Perioden, sobald sie gefunden sind, durch ihre Zeichen unterschieden werden.

Die Periode A sei mit $(e * \alpha)$ bezeichnet und in f Perioden B, C, D usw. zerlegt, die bezeichnet werden sollen. Jede ist offenbar in einer solchen Form $(ef * ke + \alpha)$ enthalten. Ich behaupte aber, dass man für eine von ihnen, B, die Zahl k beliebig wählen und daraus die Anordnung der übrigen ableiten kann.

Es sei R eine beliebige primitive Wurzel der Kongruenz $x^n \equiv 1$, und B bestehe aus den Termen $R^\mu + R^\nu +$ usw.. Es sei $\frac{1}{\mu}\rho^{ke+\alpha} \equiv \frac{1}{\upsilon} \pmod{n}$. Da der Wert von r beliebig ist, sofern nur A das Zeichen $(e * \alpha)$ erhält, was offensichtlich von selbst geschieht, setze man $r \equiv R^\upsilon \pmod{p}$. Dann ist der erste Term von B gleich $r^{\rho^{ke+\alpha}}$, und B darf mit $(ef * ke + \alpha)$ bezeichnet werden. Hätten wir anstelle von R^μ den Term R^ν betrachtet, so hätten wir einen anderen Wert von r erhalten. Man erkennt aber leicht, dass für jede beliebige Wurzel ρ die Wurzel $r\ \frac{\lambda}{ef}$ verschiedene Werte haben kann.

251.

Wir wollen nun sehen, wie man nach der Bezeichnung einer Periode die übrigen durch ihre Zeichen unterscheidet. Dazu müssen wir aber eine andere Methode suchen, um die übrigen Perioden zu finden. Denn soweit diese wie A selbst Wurzeln einer Kongruenz sind, ist unter ihnen keine Reihenfolge erkennbar. Wir nehmen an, A sei mit $(ef * 0)$ bezeichnet. Aus dem Vorhergehenden folgt dann

$$\begin{aligned} A^2 &\text{ hat die Form } M + N(ef * 0) + O(ef * 1) + P(ef * 2) + \ldots \\ A^3 &\text{ hat die Form } M' + N'(ef * 0) + O'(ef * 1) + \ldots \\ &\text{usw.} \\ A^{ef-1} &\text{ hat die Form } M^* + N^*(ef * 0) + O^*(ef * 1) + \ldots \end{aligned}$$

Hinzu kommt die Kongruenz

$$(ef * 0) + (ef * 1) + \ldots + (ef * ef - 1) \equiv -1$$

Wir haben also $cf - 1$ lineare Kongruenzen und ebenso viele unbekannte Größen, die sich daher durch Elimination bestimmen lassen.

Anmerkung. Es kann vorkommen, dass die unbekannten Größen durch Ausdrücke der Form $\frac{V}{Wp}$ gegeben sind. Wie dieser Schwierigkeit abzuhelfen ist, zeigen wir weiter unten. Hier wollen wir uns nicht damit aufhalten, weil dieser Fall nur sehr selten auftreten kann.

252.

Dies möge im Allgemeinen über die Lösung reiner Kongruenzen genügen. An verschiedenen Stellen weiter unten wird noch vieles über sie gesagt werden. Insbesondere lässt sich vieles aus der Lösung reiner Gleichungen hierher übertragen; darauf werden wir an der jeweiligen Stelle hinzuweisen nicht versäumen. Wir fügen noch ein Beispiel hinzu, dessen Vergleich mit den Regeln den weniger Geübten alles deutlicher machen wird.

Es sei $n = 31$, $p = 311$, gesucht sind also die Wurzeln der Kongruenz $x^{31} - 1 \equiv 0 \pmod{311}$. Zunächst ist eine primitive Wurzel der Kongruenz $y^{30} - 1 \equiv \pmod{31}$ zu suchen, etwa $y \equiv 3$. Wir setzen daher $\rho \equiv 3$ und teilen zunächst alle primitiven Wurzeln der gegebenen Kongruenz in 5 Perioden ein, nämlich

$$\begin{array}{ll} (5*0) & \ldots\ldots \quad (1)+(26)+(25)+(30)+(5)+(6) \\ (5*1) & \ldots\ldots \quad (3)+(16)+(13)+(28)+(15)+(18) \\ (5*2) & \ldots\ldots \quad (9)+(17)+(8)+(22)+(14)+(23) \\ (5*3) & \ldots\ldots \quad (27)+(20)+(24)+(4)+(11)+(7) \\ (5*4) & \ldots\ldots \quad (19)+(29)+(10)+(12)+(2)+(21) \end{array}$$

Die erforderlichen Rechnungen ergeben für die Summe der Perioden $\equiv -1$, für die ihrer Quadrate $\equiv 25$, Kuben $\equiv 26$, vierten Potenzen $\equiv 249$ und fünften Potenzen $\equiv 564$.

Die Perioden sind daher die Wurzeln der Kongruenz

$$x^5 + x^4 - 12x^3 - 21x^2 + x + 5 \equiv 0$$

Weiter findet man

$$(5*0)^2 \equiv 6 + 2(5*0) + 2(5*3) + (5*4)$$
$$(5*0)^3 \equiv 12 + 15(5*0) + 4(5*1) + 3(5*2) + 6(5*3) + 6(5*4)$$
$$(5*0)^4 \equiv 90 + 60(5*0) + 28(5*1) + 26(5*2) + 49(5*3) + 38(5*4)$$

und daraus durch Elimination

$$5(5*1) \equiv 3(5*0)^4 - (5*0)^3 - 33(5*0)^2 - 24(5*0) + 15$$
$$5(5*2) \equiv -2(5*0)^4 - (5*0)^3 + 22(5*0)^2 + 31(5*0)$$
$$5(5*3) \equiv (5*0)^4 - 2(5*0)^3$$
$$5(5*4) \equiv -2(5*0)^4 + 4(5*0)^3$$

Eine Wurzel der gefundenen Kongruenz ist $\equiv 17$. Setzt man also $(5*0) \equiv 17$, so ist $(5*1) \equiv 183$, $(5*2) \equiv 263$, $(5*3) \equiv 91$, $(5*4) \equiv 67$.

Nun teile man jede der gefundenen Perioden wiederum in drei, nämlich

$$\begin{array}{ll} (5*0) & \text{in } (15*0),\ (15*5),\ (15*10) \\ & \text{oder in } (1)+(30),\ (26)+(5),\ (25)+(6) \\ (5*1) & \text{in } (15*1),\ (15*6),\ (15*11) \\ & \text{oder in } (3)+(28),\ (16)+(15),\ (13)+(18) \\ & \text{usw.} \qquad \text{usw.} \end{array}$$

Die Perioden, in die die folgenden zerlegt sind, seien Wurzeln der jeweils angegebenen Kongruenzen:

$$\begin{array}{lll} (5*0) & \text{Wurzeln der Kongruenzen sind} & x^3+Ax^2+Bx+C\equiv 0 \\ (5*1) & & x^3+A'x^2+B'x+C'\equiv 0 \\ (5*2) & & x^3+A''x^2+B''x+C''\equiv 0 \\ & \text{usw.} & \end{array}$$

Dann ist

$$\begin{array}{lll} A\equiv -(5*0), & B\equiv (5*0)+(5*3), & C\equiv -2-(5*4) \\ A'\equiv -(5*1), & B'\equiv (5*1)+(5*4), & C'\equiv -2-(5*0) \\ \text{usw.} & \text{usw.} & \text{usw.} \end{array}$$

Daher

$$\begin{array}{lll} (15*0),\ (15*5),\ (15*10) & \text{sind Wurzeln} & \\ (15*1),\ (15*6),\ (15*11) & \text{der Kongruenzen} & x^3-17x^2+108x-60\equiv 0 \\ (15*2),\ (15*7),\ (15*12) & & \\ (15*3),\ (15*8),\ (15*13) & & \\ (15*4),\ (15*9),\ (15*14) & & \end{array}$$

Hier gilt aber

$$(15*0)^3-3(15*0)\equiv(15*1)$$
$$(15*1)^3-3(15*1)\equiv(15*2)$$
$$\text{usw.}$$

Setzt man daher eine der Wurzeln der ersten Kongruenz, 10, als $(15*0)$, so erhält man

$$\begin{array}{llll} (15*0)\equiv & 10 & (15*5)\equiv & (15*10)\equiv \\ (15*1)\equiv & 37 & (15*6)\equiv & (15*11)\equiv \\ (15*2)\equiv & -151 & (15*7)\equiv & (15*12)\equiv \\ (15*3)\equiv & -39 & (15*8)\equiv & (15*13)\equiv \\ (15*4)\equiv & -112 & (15*9)\equiv & (15*14)\equiv \end{array}$$

Schließlich nehme man die Terme, aus denen die einzelnen Perioden bestehen. Dann sind

(1), (30)	Wurzeln der Kongruenzen	$x^2 - (15 * 0)x + 1 \equiv 0$
(3), (28)		$x^2 - (15 * 1)x + 1 \equiv 0$

usw.

Die Wurzeln der ersten Kongruenz sind 126 und 195, die somit primitive Wurzeln der Kongruenz $x^{31} \equiv 1$ sind. Aus ihnen lassen sich die übrigen ohne Mühe ableiten.

ALLGEMEINE UNTERSUCHUNGEN ÜBER KONGRUENZEN.

LEHRE VON DEN RESTEN, ACHTES KAPITEL.

330.

Die in den vorigen Abschnitten dargestellten Ergebnisse über Kongruenzen betreffen nur die einfachsten Fälle und wurden meist mit besonderen Methoden gewonnen. In diesem Abschnitt wollen wir versuchen, die Theorie der Kongruenzen, soweit es gegenwärtig möglich ist, auf höhere Grundsätze zurückzuführen, etwa so, wie man die Theorie der *Gleichungen* zu betrachten pflegt. Mit dieser besteht, wie wir schon mehrfach bemerkt haben, eine bemerkenswerte Analogie. Da sich alle algebraischen Kongruenzen mit einer einzigen Unbekannten auf die Form

$$X \equiv 0$$

bringen lassen, wobei X eine algebraische Funktion der Unbekannten x ohne Brüche ist, müssen zunächst solche Funktionen betrachtet werden.

331.

Sind P, Q Funktionen der Unbestimmten x von der Form

$$A + Bx + Cxx + Dx^3 + \ldots$$
$$H + Ix + Kxx + Lx^3 + \ldots$$

(solche wollen wir künftig stets einfach als *Funktionen* bezeichnen), und sind in beiden die Koeffizienten gleicher Potenzen von x nach irgendeinem Modul kongruent, so heißen die *Funktionen nach diesem Modul kongruent*. Offenbar nehmen kongruente Funktionen kongruente Werte an, wenn für die Unbestimmte gleiche oder kongruente Werte eingesetzt werden. Was wir in den Kapiteln I und II über *Zahlen* bewiesen haben, gilt meist auch für Funktionen. Sind also $P \equiv P'$, $Q \equiv Q'$, $R \equiv R'$ usw., so gelten offenbar $P+Q+R$ usw. $\equiv P'+Q'+R'+$ usw.; $P-Q \equiv P'-Q'$; $PQ \equiv P'Q'$; PQR usw. $\equiv P'Q'R'$ usw. Die Beweise sind sehr leicht und lassen sich ähnlich wie in Kapitel I führen.

Ist $PQ \equiv R$, so bezeichnen wir die Funktion Q durch $\frac{R}{P}$ unter Angabe des Moduls und sagen, Q sei der Quotient, wenn R durch P nach diesem Modul geteilt wird. Offenbar können an die Stelle von Q alle ihr kongruenten Funktionen treten, die wir sämtlich als *einen einzigen* Wert betrachten. Weiter unten werden wir jedoch zeigen, in welchen Fällen ein solcher Quotient mehrere, also inkongruente Werte haben kann.

332.

Ist der Modul eine Primzahl und enthält der Divisor Q nur einen einzigen Term Hx^h, dessen Koeffizient H nicht durch den Modul teilbar ist, ist also nur H nicht $\equiv 0$, so kann der Quotient nicht mehrere Werte haben. Denn wären $QA \equiv P$ und $QB \equiv P$, so wäre $Q(A-B) \equiv 0$. Es sei nun

$$Q \equiv .. + Hx^h + Ix^{h+1} + \text{usw.}$$

wobei H nicht durch p teilbar sei, und

$$A - B \equiv Lx^l + Mx^{l+1} + \text{usw.}$$

wobei L nicht durch p teilbar sei (diese Form wird $A-B$ haben, weil wir voraussetzen, dass A nicht $\equiv B$ ist). Dann wäre $Q(A-B) \equiv HLx^{h+l} + \text{usw.} \equiv 0$. Das ist absurd, weil HL nicht $\equiv 0$ ist.

Es lassen sich nun leicht Regeln angeben, um die Funktion P durch Q zu teilen, sofern dies möglich ist. Es sei

$$P \equiv ax^\alpha + bx^{\alpha+1} + cx^{\alpha+2} + \text{usw.} + kx^\kappa$$
$$Q \equiv mx^\mu + nx^{\mu+1} + qx^{\mu+2} + \text{usw.} + tx^\tau$$

wobei a, k, m, t nicht durch den Modul teilbar seien. Dann muss α nicht $< \mu$ und κ nicht $< \tau$ sein. Die Division lässt sich ähnlich wie beim gewöhnlichen algebraischen Rechnen ausführen, wenn man nur stets für den Quotienten eine ganze Zahl nimmt. Der Quotient wird nämlich immer die Form $\frac{r}{m}$ haben, was nach dem Modul bestimmt werden muss. Bleibt nun, nachdem $\kappa+\mu-\alpha-\tau+1$ Terme gefunden sind, ein Rest, so hat dieser die Form

$$Ax^{\kappa+\mu-\tau+1} + Bx^{\kappa+\mu-\tau+2} + .. + Cx^\kappa$$

Sind dabei nicht alle Koeffizienten $A, B, C .. \equiv 0$, so lässt sich P nicht durch Q teilen.

Offenbar hätte man die Division auch mit den Termen höchsten Grades, kx^κ, tx^τ, beginnen können. Die Rechnung wird leichter, wenn man Q auf die Form

$$mx^\mu(1 + qx + rxx + \text{usw.})$$

bringt. Setzt man $mv \equiv 1$, so ergibt sich daraus

$$\frac{P}{Q} \equiv \frac{vP : x^\mu}{1 + qx + \text{usw.}}$$

Danach lässt sich die Division mit den gewöhnlichen Methoden zu Ende führen.

333.

Satz. *Ist $x \equiv a$ eine Wurzel der Kongruenz $\xi \equiv 0$, so lässt sich ξ durch $x - a$ nach dem Modul der Kongruenz teilen.*

Beweis. Ließe sie sich nämlich nicht teilen, so wäre $\xi \equiv (x-a)\xi' + b$, wobei b nicht durch den Modul teilbar wäre. Setzt man nun $x \equiv a$, so wird ξ nach Voraussetzung $\equiv 0$, also $(x-a)\xi' + b \equiv 0$. Dann gilt aber auch $(x-a)\xi' \equiv 0$, und daher muss b notwendig $\equiv 0$ sein.

334.

Aufgabe. *Zu zwei gegebenen Funktionen ihren gemeinsamen Teiler (höchsten Grades) nach einem gegebenen Modul finden.*

Lösung. Die Funktionen seien A, B, und der Grad von A sei mindestens so groß wie der von B. Man teile A durch B. Geht dies ohne Rest, so ist B der gesuchte gemeinsame Teiler. Bleibt ein Rest C, so hat dieser einen niedrigeren Grad als B. Es sei also

$$A \equiv aB + C, \quad B \equiv bC + D, \quad C \equiv cD + E, \quad \text{usw.}$$

wobei A, B, C, D, a, b, c usw. Funktionen seien und die Grade der Funktionen A, B, C, D usw. eine abnehmende Folge bilden. Geht schließlich eine Division auf, etwa $D \equiv dE$, so ist der letzte Divisor der gesuchte gemeinsame Teiler. Geht keine auf, so gelangt man schließlich zu einem Rest, der keinen Grad hat, also zu einer *Zahl*. In diesem Fall haben die Funktionen A, B aber keinen gemeinsamen Teiler.

Beweis. Teilt der Divisor E die vorhergehende Funktion ohne Rest, so teilt er, wie leicht ersichtlich, alle vorhergehenden. Daher ist E ein gemeinsamer Teiler der Funktionen A, B. Damit ist die erste Behauptung bewiesen. Gäbe es aber einen Teiler höheren Grades, etwa E', so würde dieser wegen $C \equiv A - aB$ auch C und ebenso D usw., also auch E teilen: Eine Funktion höheren Grades würde eine Funktion niedrigeren Grades teilen. Das ist absurd. Damit ist die zweite Behauptung bewiesen. Hieraus erkennt man auch, dass man, wenn ein gemeinsamer Teiler irgendeines Grades existiert, nicht zu einem Rest ohne Grad gelangen kann. Sonst würde nämlich eine Funktion ohne Grad durch eine Funktion irgendeines Grades geteilt, was absurd ist.

335.

Satz. *Sind A, B nach dem Modul p teilerfremde Funktionen und hat A den Grad α, B den Grad β, so lassen sich Funktionen P, Q mit Graden finden, die jeweils $< \beta$, $< \alpha$ sind, sodass*

$$PA + QB \equiv 1 \ (mod.\, p)$$

Beweis. In diesem Fall gilt nämlich

$$A \equiv aB + C, \quad B \equiv bC + D, \quad \text{usw.} \quad K \equiv kL + M$$

wobei die Grade der Funktionen $A, B, C, D, \ldots K, L, M$ fortwährend abnehmen und M keinen Grad hat. Man bilde nun die Folgen

$$\begin{array}{cccccc} a, & a', & a'', & a''', & \ldots & a^{(\kappa)} \\ 1, & b, & b', & b'', & \ldots & b^{(\kappa-1)} \end{array}$$

so, dass

$$\begin{array}{cccc} a' \equiv ba + 1 & a'' \equiv ca' + a & a''' \equiv da'' + a' & \text{usw.} \\ b' \equiv cb + 1 & b'' \equiv db' + b & b''' \equiv eb'' + b' & \text{usw.} \end{array}$$

Dann gilt

$$A - aB \equiv +C, \quad bA - a'B \equiv -D, \quad b'A - a''B \equiv +E, \quad \text{usw.}$$

wie leicht ersichtlich, und daher schließlich

$$b^{(\kappa-1)}A - a^{(\kappa)}B \equiv \pm M$$

Es sei nun $\frac{1}{\pm M} \equiv \mu$. Setzt man $P \equiv \mu b^{(\kappa-1)}$, $Q \equiv -\mu a^{(\kappa)}$, so erhält man

$$PA + QB \equiv 1$$

Weiter ist offenbar

$$\begin{array}{c} \text{Grad von } B + \text{Grad von } a = \text{Grad von } A. \\ \text{Grad von } C + \text{Grad von } b = .\text{Grad von } B \\ \text{usw.} \\ \text{Grad von } L + \text{Grad von } k = \text{Grad von } K \end{array}$$

Also gilt

$$\text{Grad von } L + \text{Summe der Grade von } a, b, \ldots k = \text{Grad von } A$$

Der Grad von $a^{(\kappa)}$ ist offenbar und damit auch

$$\text{Grad von } Q = \text{Summe der Grade von } a, b, c, \ldots \text{ d. h. } = \alpha - \text{Grad von } L$$

Somit ist

$$\text{Grad von } P = \beta - \text{Grad von } L \qquad \text{Q. E. D.}$$

336.

Hieraus folgt, dass man, wenn M der gemeinsame Teiler höchsten Grades der Funktionen A, B ist, stets setzen kann

$$AP + BQ \equiv M$$

Beispiele zum vorigen Satz lasse ich der Kürze halber weg. Die Leser werden es aber nicht versäumen, sich durch Beispiele im Umgang mit solchen Aufgaben zu üben. Es lohnt sich auch, darauf hinzuweisen, dass der vorige Satz für Funktionen gilt, die ohne einen Modul betrachtet werden, sofern ihre Koeffizienten rationale Zahlen sind. Das ergibt sich von selbst aus der Art des Beweises. Wir können uns jedoch nicht damit aufhalten. Ähnliches wird der Leser im Folgenden auch ohne Hinweis bemerken.

Hat A weder mit B noch mit C einen gemeinsamen Teiler irgendeines Grades, so hat sie auch mit dem Produkt BC keinen gemeinsamen Teiler. Es sei nämlich

$$PA + QB \equiv 1, \quad \text{dann gilt} \quad PAC + QBC \equiv C$$

Hätte nun A mit BC einen gemeinsamen Teiler M, so würde dieser auch C teilen, entgegen der Voraussetzung. Allgemein ist also eine Funktion A, die zu B, C, D usw. teilerfremd ist, auch zum Produkt aller teilerfremd.

Haben A, B, C, D usw. keinen allen gemeinsamen Teiler, so lässt sich erreichen, dass

$$PA + QB + RC + SD + \text{usw.} \equiv 1$$

Der gemeinsame Teiler höchsten Grades von A und B sei M, der von M und C sei M', der von M' und D sei M'' usw. Offenbar hat das letzte Glied dieser Folge nach Voraussetzung keinen Grad. Daher lässt sich setzen

$$aA + bB \equiv M, \quad mM + cC \equiv M', \quad m'M' + dD \equiv M'', \quad \text{usw.}$$

Nach den entsprechenden Einsetzungen ergibt sich die Richtigkeit des Satzes.

337.

Satz. *Sind A, B, C usw. nach dem Modul p zueinander teilerfremde Funktionen (haben also je zwei keinen gemeinsamen Teiler), und ist die Funktion M nach demselben Modul durch jede einzelne teilbar, so ist sie auch durch das Produkt aller teilbar.*

Beweis. Man kann nämlich $PA + QB \equiv 1$ setzen, und daher gilt

$$\frac{M}{A}Q + \frac{M}{B}P \equiv \frac{M}{AB}$$

Da nun C zu AB teilerfremd ist, ist M auch durch ABC und ebenso durch $ABCD$ usw. teilbar.

338.

Hat die Kongruenz $\xi \equiv 0$ die Wurzeln $x \equiv a$, $x \equiv b$, $x \equiv c$ usw., so lässt sich ξ durch das Produkt aus $(x-a)$, $(x-b)$, $(x-c)$ usw. teilen. Da nämlich $a, b, c.$ usw. als inkongruent vorausgesetzt werden, sind die Funktionen $x - a, x - b, x - c$ usw. zueinander teilerfremd. Da ξ durch jede einzelne teilbar ist, ist sie auch durch das Produkt aller teilbar. Die Anzahl der Wurzeln kann daher den Grad der Kongruenz nicht übersteigen. Das ist der versprochene Beweis dieses Satzes.

Zugleich zeigt sich aber, dass die Lösung der Kongruenzen nur einen Teil einer viel tiefer gehenden Untersuchung bildet, nämlich der Zerlegung von Funktionen in Faktoren. Offenbar hat die Kongruenz $\xi \equiv 0$ keine reellen Wurzeln, wenn ξ keine Faktoren ersten Grades besitzt. Das hindert aber nicht daran, dass sich ξ in Faktoren zweiten, dritten oder höheren Grades zerlegen lässt, aus denen man ihr gewissermaßen *imaginäre* Wurzeln zuschreiben könnte. Hätten wir uns tatsächlich eine ähnliche Freiheit nehmen und solche imaginären Größen einführen wollen, wie es die neueren Mathematiker getan haben, so hätten wir alle folgenden Untersuchungen unvergleichlich verkürzen können. Dennoch haben wir es vorgezogen, alles aus Grundsätzen abzuleiten[*)].

339.

Funktionen heißen nach einem bestimmten Modul *prim*, wenn sie sich nach diesem Modul durch keine Funktionen niedrigeren Grades teilen lassen.

So sind alle Funktionen ersten Grades prim; Funktionen zweiten Grades sind entweder prim oder aus zwei Funktionen ersten Grades zusammengesetzt. Daher ist ξ eine Primfunktion zweiten Grades, wenn die Kongruenz $\xi \equiv 0$ keine reellen Wurzeln zulässt. Zum Beispiel ist $xx + x + 1$ für den Modul 5 prim, weil

$$xx + x + 1 \equiv (x-2)^2 - 3 \pmod 5$$

und 3 ein quadratischer Nichtrest von 5 ist.

Diese Primfunktionen verdienen vor allem unsere Aufmerksamkeit. Zwar können andere als solche ersten Grades nicht zum Auffinden reeller Wurzeln dienen; eine eingehendere Betrachtung empfiehlt sich jedoch sowohl wegen ihrer bemerkenswerten Eigenschaften als auch wegen anderer vorzüglicher Wahrheiten, die sich aus ihnen ableiten lassen.

[*)] Vielleicht werden wir bei einer anderen Gelegenheit unsere Ansicht hierzu ausführlicher darlegen.

340.

Satz. *Jede Funktion ist entweder prim oder aus Primfunktionen zusammengesetzt. Im zweiten Fall lässt sie sich nur auf eine einzige Weise aus Primfunktionen zusammensetzen.*

Beweis. Ist nämlich die vorgelegte Funktion A nicht prim, so ist sie durch eine andere Funktion B niedrigeren Grades teilbar. Ist B keine Primfunktion, so ist sie durch eine andere Funktion C niedrigeren Grades teilbar. Fährt man so fort, so muss man schließlich zu einer Primfunktion gelangen. Sonst wäre diese Folge unendlich, was absurd ist, da die Grade fortwährend abnehmen. Ist nun die letzte Primfunktion L, so teilt sie alle vorhergehenden. Daher ist $A \equiv LA'$, und A' hat einen niedrigeren Grad als A. Wiederholt man dies, so erhält man $A' \equiv L'A''$ usw. Offenbar muss man schließlich zu einer Primfunktion gelangen, und daher ist $A \equiv$ einem Produkt aus Primfunktionen L, L', L'' usw. . Damit ist die erste Behauptung bewiesen.

Wäre nun auch $A \equiv MM'M''$ usw., und wären nicht alle L, L', L'' usw. dieselben wie alle M, M', M'' usw., so lasse man die Funktionen weg, die beiden Folgen gemeinsam sind. Es mögen $\lambda, \lambda', \lambda'' \ldots$; $\mu, \mu', \mu'', \ldots$ übrig bleiben. Dann ist μ zu $\lambda, \lambda', \lambda''$ usw., also auch zum Produkt $\lambda\lambda'\lambda''$ usw. teilerfremd. Dennoch müsste gelten

$$\lambda\lambda'\lambda''\ldots \equiv \mu\mu'\mu''\ldots \text{ d. h. } \frac{\lambda\lambda'\lambda''\ldots}{\mu} \equiv \mu'\mu''\ldots \quad \text{ein Widerspruch}$$

341.

Die erste Hauptaufgabe dieser Untersuchungen besteht darin, die Anzahl der Primfunktionen jedes Grades zu bestimmen. Für einen bestimmten Modul ist nämlich die Anzahl aller verschiedenen (inkongruenten) Funktionen jeden Grades endlich. Von diesen sind einige aus Primfunktionen niedrigeren Grades zusammengesetzt, andere selbst prim; daher ist auch die Anzahl der letzteren endlich. Eine strenge Entwicklung dieses Gegenstandes ist recht heikel. Wir werden mit den einfacheren Fällen beginnen.

Setzt man den Modul $= p$, so ist die Anzahl aller verschiedenen Funktionen des Grades n von der Form

$$x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \text{usw.}$$

gleich p^n. Die Anzahl der Koeffizienten $.A, B\,.C$ usw. ist nämlich n, und jeder kann unabhängig von den übrigen $\equiv 0, 1, 2, 3\ldots(p-1) (\text{mod. } p)$ sein. Aus der Kombinatorik ergeben sich daher p^n verschiedene Kombinationen, die somit die Gesamtheit aller verschiedenen Funktionen dieses Grades bestimmen.

So gibt es p Funktionen ersten Grades, nämlich $x, x+1, x+2$ bis $x+p-1$, ferner pp Funktionen zweiten Grades usw.

342.

Wir haben schon darauf hingewiesen, dass alle Funktionen ersten Grades als prim anzusehen sind. Beschränken wir uns also, was für unser Vorhaben genügt, auf die Funktionen, deren höchster Term den Koeffizienten 1 hat, so gibt es p Funktionen ersten Grades oder einer Dimension.

Alle Funktionen zweiten Grades sind entweder aus zwei Funktionen ersten Grades zusammengesetzt oder prim. Aus der Kombinatorik ist bekannt, dass sich p verschiedene Dinge bei zugelassenen Wiederholungen auf $\frac{p.p+1}{1.2}$ verschiedene Arten kombinieren lassen. Daher gibt es ebenso viele Funktionen, die aus zwei Primfunktionen ersten Grades zusammengesetzt sind, und somit $pp - \frac{p.p+1}{1.2} = \frac{1}{2}(pp - p)$ Primfunktionen zweiten Grades.

Ebenso sind von allen Funktionen dritten Grades, deren Anzahl p^3 ist, diejenigen auszuschließen, die aus drei Primfunktionen ersten Grades zusammengesetzt sind und deren Anzahl $\frac{p.p+1.p+2}{1.2.3}$ ist. Dazu kommen diejenigen, die aus einer Primfunktion ersten und einer zweiten Grades zusammengesetzt sind und deren Anzahl $p \,.\, \frac{1}{2}(pp-p)$ ist. Lässt man diese weg, so bleiben $\frac{1}{3}(p^3 - p)$ übrig. So viele Primfunktionen dritten Grades gibt es also. Offenbar kann man auf diese Weise stets fortfahren.

343.

Um diese Rechnungen leichter auszuführen und zugleich den Weg zur Entwicklung des allgemeinen Gesetzes zu bahnen, wollen wir die Sache allgemein betrachten. Der Kürze halber bezeichnen wir mit (1) die Anzahl der Primfunktionen ersten Grades, mit (2) die Anzahl der Primfunktionen zweiten Grades, ferner mit (1^2) die Anzahl der aus zwei Primfunktionen ersten Grades zusammengesetzten Funktionen usw. usw. Allgemein bezeichnen wir mit $(1^\alpha 2^\beta 3^\gamma \ldots)$ die Anzahl aller aus Primfunktionen zusammengesetzten Funktionen, und zwar aus α ersten, β zweiten, γ dritten Grades usw. Ihr Grad ist also $\alpha + 2\beta + 3\gamma +$ usw. Aus dem Vorhergehenden und der Kombinatorik ergibt sich dann

$$(1^\alpha 2^\beta 3^\gamma 4^\delta \ldots) = (1^\alpha)(2^\beta)(3^\gamma)(4^\delta)\,..$$

$$(1^\alpha) = \frac{(1)\,.\,(1) + 1\,.\,(1) + 2\,.\,(1) + 3 \ldots (1) + \alpha - 1}{1\,.\,2\,.\,3\,.\,4 \ldots \alpha}$$

oder allgemein

$$(a^\alpha) = \frac{(a)\,.\,(a) + 1\,.\,(a) + 2\,.\,(a) + 3 \ldots (a) + \alpha - 1}{1\,.\,2\,.\,3\,.\,4 \ldots \alpha}$$

Sammelt man schließlich alle verschiedenen Arten, die Zahl n durch Addition aus den Zahlen $1, 2, 3, \ldots$ zusammenzusetzen, und bezeichnet diese Arten mit $\alpha \,.\, 1 + \beta \,.\, 2 + \gamma \,.\, 3 + \text{usw.}$, so ist offenbar die Summe aller dieser Ausdrücke $(1^\alpha 2^\beta 3^\gamma \,..)$ gleich der Anzahl aller Funktionen des Grades n, also $= p^n$. So ist

$$\begin{aligned} p &= (1) \\ pp &= (1^2) + (2) \\ p^3 &= (1^3) + (1 \,.\, 2) + (3) \\ p^4 &= (1^4) + (1^2 \,.\, 2) + (1 \,.\, 3) + (2^2) + (4) \\ &\text{usw.} \end{aligned}$$

Offenbar geht in den Ausdruck p^n außer den Größen $(1), (2), (3)$ usw. auch (n) ein. Daraus erkennt man, wie sich alle Größen aus den vorhergehenden bestimmen lassen. So findet man

$$\begin{array}{lll} (1) = p & (4) = \frac{1}{4}(p^4 - pp) & (7) = \frac{1}{7}(p^7 - p) \\ (2) = \frac{1}{2}(pp - p) & (5) = \frac{1}{5}(p^5 - p) & (8) = \frac{1}{8}(p^8 - p^4) \\ (3) = \frac{1}{3}(p^3 - p) & (6) = \frac{1}{6}(p^6 - p^3 - pp + p) & \text{usw.} \end{array}$$

344–346.

Aus diesem Anfang der Folge erkennt man, dass der höchste Term des Ausdrucks (n) gleich $\frac{1}{n}p^n$ ist. Ist n eine Primzahl, so kommt $-\frac{1}{n}p$ hinzu; ist n dagegen zusammengesetzt, so tritt das Gesetz weniger deutlich hervor. Betrachtet man die Sache aber genauer, so sieht man, dass

$$\begin{array}{ll} p = (1) & p^5 = 5(5) + (1) \\ pp = 2(2) + (1) & p^6 = 6(6) + 3(3) + 2(2) + (1) \\ p^3 = 3(3) + (1) & p^7 = 7(7) + (1) \\ p^4 = 4(4) + 2(2) + (1) & p^8 = 8(8) + 4(4) + 2(2) + (1) \text{ usw.} \end{array}$$

wobei das Bildungsgesetz offensichtlich ist. Hat nämlich die Zahl n sämtliche Teiler $\alpha, \beta, \gamma, \delta$ usw., so gilt

$$p^n = \alpha(\alpha) + \beta(\beta) + \gamma(\gamma) + \delta(\delta) + \text{usw.}$$

Wir gehen nun daran, die Allgemeingültigkeit dieser Beobachtung zu beweisen.

Wir haben gezeigt, dass die Summe aller solchen Ausdrücke $(1^\alpha)(2^\beta)(3^\gamma)\ldots$, wenn stets $\alpha + 2\beta + 3\gamma + \ldots = n$ gilt, alle Funktionen des Grades n erschöpft und somit $= p^n$ ist. Hieraus folgt, — — —. Entwickelt man

$$\left(\frac{1}{1-x}\right)^{(1)}\left(\frac{1}{1-xx}\right)^{(2)}\left(\frac{1}{1-x^3}\right)^{(3)}\ldots$$

in die Reihe $1 + Ax + Bx^2 \ldots = P$, so ist

$$A = p, \quad B = p^2, \quad C = p^3 \text{ usw.}$$

$$\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x} = \frac{(1)x}{1-x} + \frac{2(2)x^3}{1-x^2} + \frac{3(3)x^3}{1-x^3}\ldots$$

— — — —

[Hieraus ergibt sich, wenn man $\frac{px}{1-px}$ für $\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x}$ einsetzt und die einzelnen Brüche in unendliche Reihen entwickelt, die Richtigkeit des Satzes von selbst.]

347.

Dieser Satz lässt sich auch anders ausdrücken. Sind sämtliche Teiler der Zahl n gleich $n, 1, \delta, \delta', \delta'', \delta'''$ usw., so besagt der Satz, dass

$$p^n = n(n) + (1) + \delta(\delta) + \delta'(\delta') + \text{usw.}$$

Offenbar hat nun das Produkt aus den (n) Primfunktionen des Grades n den Grad $n(n)$. Entsprechendes gilt für die übrigen. Daher gilt

Das Produkt aus allen Primfunktionen ersten Grades und der Grade n, δ, δ' usw. hat den Grad p^n.

Aus diesem Satz lässt sich nun leicht der Wert des Ausdrucks (n) selbst ableiten. Der Kürze halber unterdrücken wir jedoch die Rechnung, die nicht schwierig ist. Es sei also $n = a^\alpha b^\beta c^\gamma$ usw., wobei a, b, c usw. verschiedene Primzahlen seien. Dann gilt

$$n(n) = p^n - \Sigma p^{\frac{n}{a}} + \Sigma p^{\frac{n}{ab}} - \Sigma p^{\frac{n}{abc}} \text{ usw.}$$

Hier bezeichnet $\Sigma p^{\frac{n}{abc..}}$ die Gesamtheit aller zu $p^{\frac{n}{abc..}}$ ähnlichen Ausdrücke, wenn man die Größen $a, b, c..$ auf jede Weise untereinander vertauscht. So ist für $n = 36$ dann $36(36) = p^{36} - p^{18} - p^{12} + p^6$.

Eine weitere Bemerkung sei noch erlaubt. Hat n die Form a^α und ist a prim, so ist $n(n) = p^n - p^{\frac{n}{a}}$. Da (n) notwendig eine ganze Zahl ist, gilt daher für jedes p

$$p^n \equiv p^{\frac{n}{a}} \ (\mathrm{mod.}\, n)$$

Ist also p zu a teilerfremd, so gilt

$$p^{n-\frac{n}{a}} \equiv 1 \ (\mathrm{mod.}\, n)$$

und für $\alpha = 1$

$$p^{a-1} \equiv 1 \ (\mathrm{mod.}\, a)$$

Es ist bemerkenswert, dass sich diese Sätze auf so verschiedene Weise gewinnen lassen.

348.

Aufgabe. *Gegeben sei die Gleichung*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \text{usw.} + M = 0$$

mit den Wurzeln $x = a$, $x = b$, $x = c$ usw. Man finde eine Gleichung mit den Wurzeln $x = a^\tau$, $x = b^\tau$, $x = c^\tau$ usw.

Erste Lösung. Man bestimme mit dem bekannten Satz die Summen der Wurzeln der gegebenen Gleichung, ihrer Quadrate, Kuben usw. bis zur Potenz mit dem Exponenten $m\tau$. Damit erhält man auch die Summen der Wurzeln der gesuchten Gleichung und ihrer Quadrate usw., nämlich Σa^τ, $\Sigma a^{2\tau}$ usw. Hieraus lassen sich mit demselben Satz die Koeffizienten bestimmen.

Für die praktische Rechnung ist diese Lösung zwar einfacher; doch eignet sich die folgende besser für unseren Zweck und auch dazu, zu zeigen, dass die Koeffizienten der gesuchten Gleichung ganze Zahlen sind, wenn die Koeffizienten der gegebenen Gleichung ganze Zahlen sind.

Zweite Lösung. Es sei θ eine primitive Wurzel der Gleichung $x^\tau = 1$. Man bilde das Produkt aus

$$\begin{aligned}
&x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.}\\
&x^m + A\theta x^{m-1} + B\theta\theta x^{m-2} + \text{usw.}\\
&x^m + A\theta\theta x^{m-1} + B\theta^4 x^{m-2} + \text{usw.}\\
&\text{usw.}\\
&x^m + A\theta^{\tau-1} x^{m-1} + B\theta^{2\tau-2} x^{m-2} + \text{usw.}
\end{aligned}$$

Die Wurzeln dieses Produkts sind daher

$$\begin{array}{llll}
a, & \theta a, & \theta\theta a & \text{usw.}\\
b, & \theta b, & \theta\theta b & \text{usw.}\\
c, & \theta c, & \theta\theta c & \text{usw.}
\end{array}$$

d. h. das Produkt ist gleich

$$(x^\tau - a^\tau)(x^\tau - b^\tau)(x^\tau - c^\tau)\dots$$

und hat somit die Form

$$x^{\tau m} + A' x^{\tau(m-1)} + B' x^{\tau(m-2)} + \text{usw.}$$

Schreibt man nun für x^τ die Größe x, so ist

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{usw.} = (x - a^\tau)(x - b^\tau)(x - c^\tau)\dots$$

und damit

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{usw.} = 0$$

die gesuchte Gleichung. Dass hier A', B' usw. nicht nur rationale, sondern auch ganze Zahlen sind, folgt leicht aus der Theorie der Gleichung $x^\tau = 1$.

Da wir diese Operation im Folgenden oft verwenden werden, bezeichnen wir mit (P, ρ^τ) die Funktion, die, gleich null gesetzt, eine Gleichung ergibt, deren Wurzeln die Potenzen mit dem Exponenten τ der Wurzeln der Gleichung $P = 0$ sind.

Ist $P \equiv Q$ nach irgendeinem Modul, so ist auch $(P, \rho^\tau) \equiv (Q, \rho^\tau)$ nach demselben Modul.

349.

Satz. *Der Koeffizient des Terms x^n in (P, ρ^τ) ist nach dem Modul τ dem Koeffizienten des Terms $x^{\tau n}$ in P^τ kongruent, sofern τ eine Primzahl ist* (was für diesen Fall eine dritte Lösung der vorigen Aufgabe ergibt).

Beweis. Aus dem sechsten Kapitel folgt, dass jeder Koeffizient des Produkts

$$(x^m + Ax^{m-1} + \text{usw.})(x^m + A\theta x^{m-1} + \text{usw.})\dots$$

nach dem Ersetzen von θ^τ durch die Einheit die folgende Form hat:

$$E + (1 + \theta + \theta\theta + \text{usw.} + \theta^{\tau-1})F$$

Betrachtet man nun θ als primitive Wurzel der Gleichung $x^\tau = 1$, so geht das ganze Produkt in E über. Setzt man hingegen $\theta = 1$, so geht das ganze Produkt in $P^\tau = E + \tau F$ über. Daher ist der Koeffizient des Terms $x^{n\tau}$ in P^τ nach dem Modul τ dem Koeffizienten des Terms $x^{n\tau}$ in E kongruent, d. h. dem Koeffizienten des Terms x^n in (P, ρ^τ).

350.

Satz. *Ist τ eine Primzahl, so ist*

$$(P, \rho^\tau) \equiv P \ (mod.\, \tau)$$

Beweis. Es sei der Koeffizient des Terms x^n in $(P, \rho^\tau) = N'$, der Koeffizient desselben Terms in P dagegen $= N$. Setzt man dann

$$P = x^m + Ax^{m-1} + \text{usw.} + Nx^n + \text{usw.}$$

so gilt

$$P^\tau \equiv x^{m\tau} + A^\tau x^{(m-1)\tau} + \text{usw.} + N^\tau x^{n\tau} + \text{usw.} \ (\text{mod.}\, \tau)$$

und daher nach dem vorigen Artikel $N' \equiv N^\tau \ (\text{mod.}\, \tau)$. Wegen $N^\tau \equiv N$ ist somit $N' \equiv N$. Q. E. D.

Hieraus ist auch ersichtlich, dass $(P, \rho^{\alpha}) \equiv (P, \rho^{\alpha\tau})$ und $(P, \rho^{\tau}) \equiv (P, \rho^{\tau\tau})$, also allgemein

$$(P, \rho^{\alpha}) \equiv (P, \rho^{\alpha\tau^k}) \,(\mathrm{mod.}\, \tau)$$

351.

Satz. *Es gibt einen Wert der Zahl ν, der kleiner als p^m ist, sodass die Funktion $x^{\nu} - 1$ durch die gegebene Funktion P vom Grad m, deren niedrigster Term die Unbestimmte x nicht enthält, nach dem Modul p teilbar ist.*

Beweis. Man teile durch P die Folge der Funktionen $1, x, xx \ldots$ bis x^{p^m-1}, sobald ihr Grad m übersteigt. Da keine durch P ohne Rest teilbar ist, lassen sich alle Reste auf die Form

$$Ax^{m-1} + Bx^{m-2} + \ldots + N$$

bringen, wobei alle Koeffizienten positiv und $< p$ sind. Da aber niemals alle $= 0$ sein können, gibt es offenbar nur $p^m - 1$ Funktionen, deren einer die einzelnen Reste gleich sein müssen. Da man bis zur Potenz von x mit dem Exponenten $p^m - 1$ insgesamt p^m Reste erhält, müssen notwendig mindestens zwei übereinstimmen. Bei der Division von x^a und $x^{a+\nu}$ durch P möge also derselbe Rest entstehen, wobei $a + \nu < p^m$. Dann ist $x^{a+\nu} - x^a$ durch P teilbar. Da nach Voraussetzung x und damit auch x^a eine zu P teilerfremde Funktion ist, lässt sich daher auch $x^{\nu} - 1$ durch P teilen. Q. E. D.

Folgerung. Ist $x^{\nu} - 1$ durch P teilbar, so ist auch $x^{k\nu} - 1$ durch P teilbar, wobei k eine beliebige ganze Zahl bezeichnet.

352.

Satz. *Bei den Bezeichnungen des vorigen Artikels sei P eine Primfunktion und x^{ν} die niedrigste Potenz, die nach Abzug der Einheit durch P teilbar ist. Dann ist ν entweder $= p^m - 1$ oder ein Teiler dieser Zahl, mit der einzigen Ausnahme $P = x$.*

Beweis. Da P eine Primfunktion vom Grad m ist, gibt es $p^m - 1$ verschiedene Funktionen von kleinerem Grad als m, wenn man die Funktion 0 aus ihrer Gesamtzahl ausschließt. Sie sind alle zu P teilerfremd. Da nun x^ν der Annahme nach die niedrigste Potenz ist, die bei der Division durch P die Einheit als Rest lässt, entstehen offenbar bei der Division aller niedrigeren Potenzen von $1, x, ..$ bis $x^{\nu-1}$ durch P genau ν verschiedene Reste, die allgemein mit A bezeichnet seien. Erschöpfen sie alle möglichen Reste, so ist der Satz bewiesen. Sind aber noch einige nicht darunter, so sei B irgendeiner davon. Offenbar ergibt die Funktion Bx^ν bei der Division durch P den Rest B, und allgemein ist $Bx^{\nu+k} \equiv Bx^k (\mathrm{mod.}\, P)$. Alle Funktionen von B bis $Bx^{\nu-1}$ liefern aber Reste, die untereinander und von den Resten A verschieden sind. Wäre nämlich $Bx^\lambda \equiv Bx^{\lambda+\delta} (\mathrm{mod.}\, P)$, so wäre auch $1 \equiv x^\delta (\mathrm{mod.}\, P)$ und $\delta < \nu$, entgegen der Voraussetzung. Wäre dagegen $Bx^\lambda \equiv x^\mu (\mathrm{mod.}\, P)$, so wäre $B \equiv x^{\mu+\nu-\lambda} (\mathrm{mod.}\, P)$ und damit B einer der Reste A, ebenfalls entgegen der Voraussetzung. Man hat somit offenbar noch ν neue Reste. Auf dieselbe Weise kann man weiter fortfahren (ganz wie oben, §. .). Dabei zeigt sich, dass die Anzahl $p^m - 1$ aller möglichen Reste entweder $= \nu$ oder $= 2\nu$ oder $= 3\nu$ oder allgemein ein Vielfaches der Zahl ν ist. Q. E. D.

353.

Aus dem vorigen Satz und der Folgerung zu §. 351 ergibt sich, dass jede Primfunktion vom Grad n die Funktion $x^{p^n-1} - 1$ nach dem Modul p teilt. Daher teilen alle Funktionen ersten Grades mit der einzigen Ausnahme derjenigen, die $\equiv x$ ist, die Funktion $x^{p-1} - 1$. Dies ist der Fermatsche Satz. Alle Primfunktionen zweiten Grades, d. h. von der Form $xx + Ax + B$, teilen die Funktion $x^{pp-1} - 1$ usw. Die Zahl n habe nun sämtliche Teiler $n, \delta, \delta', \delta''$ usw. . 1. Offenbar ist $p^n - 1$ auch durch $p^\delta - 1$, $p^{\delta'} - 1$, $p^{\delta''} - 1$ usw. $p - 1$ teilbar. Deshalb ist die Funktion $x^{p^n-1} - 1$ durch *alle Primfunktionen der Grade* $n, \delta, \delta', \delta''$ *usw. bis zu den Primfunktionen ersten Grades (unter Ausschluss der Funktion* x*)* teilbar und daher auch, da alle diese Funktionen an sich prim und somit untereinander teilerfremd sind, durch *das Produkt aus allen.* Eben dieses Produkt hat aber den Grad $p^n - 1$ (§. 347), da die eine Funktion x fehlt. Somit ist klar, dass *dieses Produkt selbst* $x^{p^n-1} - 1 (\mathrm{mod.}\, p)$ *kongruent sein muss.*

354.

Satz. *Ist die Funktion $x^\nu - 1$ durch die Funktion P teilbar, so gilt*

$$(P, \rho^{k\nu+t}) \equiv (P, \rho^t)$$

wobei k, t beliebige ganze Zahlen bezeichnen.

Beweis. Es sei

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.}$$

Bekanntlich ergibt die Entwicklung von

$$\frac{mx^{m-1} + (m-1)Ax^{m-2} + \text{usw.}}{x^m + Ax^{m-1} + \text{usw.}}$$

in eine unendliche Reihe der Form

$$m\frac{1}{x} + \alpha\frac{1}{xx} + \beta\frac{1}{x^3} + \gamma\frac{1}{x^4} + \text{usw.}$$

für α die Summe der Wurzeln der Gleichung $P = 0$, für β die Summe ihrer Quadrate usw. Hieraus folgt ohne Mühe, dass die Summen der Potenzen mit den Exponenten $\nu + 1$, $\nu + 2$ usw. der Summe der Wurzeln, ihrer Quadrate usw. kongruent sind. Sofern der Modul nicht gleich dem Grad der Funktion P oder kleiner ist, folgt hieraus

$$(P, \rho^{\nu+1}) \equiv P, \quad (P, \rho^{\nu+2}) \equiv (P, \rho^2), \quad (P, \rho^{\nu+3}) \equiv (P, \rho^3) \text{ usw.}$$

Jenen Fall werden wir weiter unten betrachten.

355.

Satz. *Sind in der Folge*

$$(P,\rho^0),\quad (P,\rho)\quad (P,\rho^2),\quad (P,\rho^3) \text{ usw.}$$

die auf das Glied an der Stelle ν folgenden Glieder den ersten der Reihe nach kongruent, so ist $x^\nu - 1$ durch P teilbar, sofern P keinen Faktor mehrfach enthält.

Beweis. Setzt man $\frac{\mathrm{d}P}{\mathrm{d}x} = Q$, so ist Q eine zu P teilerfremde Funktion. Es sei

$$\frac{Q}{P} \equiv \frac{A}{x} + \frac{B}{xx} + \frac{C}{x^3} + \text{usw.}$$

Dann folgt nach Voraussetzung auf das Glied $\frac{N}{x^\nu}$

$$\frac{A}{x^{\nu+1}} + \frac{B}{x^{\nu+2}} + \frac{C}{x^{\nu+3}} + \text{usw.}$$

Daher ist

$$\frac{Q}{P} \equiv \frac{Ax^{\nu-1} + Bx^{\nu-2} + \text{usw.}}{x^\nu - 1}$$

woraus sich ergibt, dass die Funktion $x^\nu - 1$ durch P teilbar ist. Q. E. D.

356.

Satz. *Es sei P eine Primfunktion von x vom Grad m und X eine Funktion von $x, x^p, x^{pp}, x^{p^3} \ldots x^{p^{m-1}}$, in der alle diese Größen auf gleiche Weise vorkommen, d. h. die unverändert bleibt, wie auch immer diese Größen untereinander vertauscht werden. Dann ergibt die Funktion X bei der Division durch P einen Rest, der eine Zahl ist.*

Beweis. Es sei der Rest

$$Ax^{m-1} + Bx^{m-2} + \ldots + N \equiv \xi$$

Alle Koeffizienten $A, B, C \ldots$ bis ausschließlich N sind $\equiv 0$. Dies wird folgendermaßen bewiesen. Da $X - \xi$ durch P teilbar ist, lässt sich auch $X^p - \xi^p$ durch P teilen. Man erkennt aber leicht, dass X^p aus X entsteht, wenn man x durch x^p, x^p durch x^{pp} usw. . und $x^{p^{m-1}}$ durch x^{p^m} oder, was dasselbe ist, durch x ersetzt. Somit ist offenbar $X^p \equiv X \pmod{P}$. Da nun $X^p \equiv \xi^p$ und $X \equiv \xi \pmod{P}$, ist auch $\xi^p \equiv \xi \pmod{P}$, oder

$$\xi^p - \xi \equiv 0 \pmod{P}$$

Doch ist $\xi^p - \xi$ nach dem Modul p dem Produkt aus $\xi, \xi+1, \xi+2, \ldots$ bis $\xi + p - 1$ kongruent. Diese Faktoren sind alle zu P teilerfremd, sofern ξ nicht einfach eine Zahl ist. Daher kann auch $\xi^p - \xi$ auf keine andere Weise durch P teilbar sein. Q. E. D.

Solche Funktionen sind die Summe aller Größen, die Summe ihrer Quadrate, Kuben usw. und die Summen der Produkte aus je zwei, drei usw. Größen. Welche Zahl dies aber ist, werden wir im folgenden Artikel bestimmen:

357.

Satz. *Die Primfunktion des vorigen Artikels sei*

$$P \equiv x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \text{usw.}$$

Dann ist der Rest bei der Division der Summe der Größen x, x^p *usw.* $x^{p^{m-1}}$ *durch* $P \equiv A$*, bei der Summe der Produkte aus je zwei* $\equiv B$*, bei der Summe der Produkte aus je drei* $\equiv C$ *usw.*

Beweis. Jene Funktionen seien X, Y, Z usw. und ihre Reste der Reihe nach die Zahlen A', B', C' usw. Man sieht leicht, dass x, x^p, x^{pp} usw. Wurzeln der Gleichung

$$z^m - Xz^{m-1} + Yz^{m-2} - Zz^{m-3} + \text{usw.} = 0$$

sind. Setzt man daher $z = x$, so ist

$$x^m - Xx^{m-1} + Yx^{m-2} - Zx^{m-3} + \text{usw.} = 0$$

Die Funktionen $X - A'$, $Y - B'$, $Z - C'$ usw. sind aber durch P teilbar und daher auch die Funktion

$$x^m - A'x^{m-1} + B'x^{m-2} - C'x^{m-3} + \text{usw.}$$

Dies ist nur möglich, wenn $A' \equiv A$, $B' \equiv B$, $C' \equiv C$ usw. Q. E. D.

Ferner ist bekannt, dass jede andere Funktion X von x, x^p usw. [in der alle diese Größen auf gleiche Weise vorkommen,] stets aus diesen abgeleitet werden kann. So ist

$$x^2 + x^{2p} + x^{3pp} + \text{usw.} \equiv AA - 2B(\text{mod. } P) \text{ usw. usw.}$$

Beispiel. Es sei $p = 5$ und $P \equiv x^2 + 2x + 3$. Dann ergibt die Funktion $x + x^5$ bei der Division durch P den Rest $\equiv -2$, und es ist $x^6 \equiv 3$ usw. usw.

358. 359.

Satz. *Es sei P eine Primfunktion und x^ν die niedrigste Potenz von x, die bei der Division durch P den Rest 1 ergibt. Ferner sei $P \equiv (P, \rho^n)$. Dann ist n einer Potenz der Zahl p nach dem Modul ν kongruent.*

Beweis. Wir haben oben gezeigt, dass, wenn P

$$= x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.}$$

ist, der Ausdruck

$$z^m + Az^{m-1} + Bz^{m-2} + \text{usw.} \\ - (z-x)(z-x^p)\,..\,(z-x^{p^{m-1}})$$

durch P teilbar ist. Auf dieselbe Weise würde folgen, dass

$$z^m + Az^{m-1} + Bz^{m-3} + \text{usw.} \\ - (z-x^n)(z-x^{np})\,..\,(z-x^{np^{m-1}})$$

durch P teilbar ist. Da diese Faktoren aber untereinander teilerfremd sind, müssen die einzelnen Faktoren notwendig den entsprechenden einzelnen Faktoren nach P, p kongruent sein. Daher muss $z - x^n \equiv z - x^{p^\kappa}$ sein, d. h. $p^\kappa \equiv n (\text{mod.}\, \nu)$. Q. E. D.[*)]

Die Primteiler der Funktion $x^\nu - 1$ nach einem Primzahlmodul bestimmen.

360.

Ist ν durch den Modul p oder eine seiner Potenzen teilbar, so sei $\nu = p^k \lambda$. Dann ist

$$x^\nu - 1 \equiv (x^\lambda - 1)^{p^k} (\text{mod.}\, p)$$

Hieraus ergibt sich, dass nur der Fall betrachtet werden muss, in dem ν nicht durch p teilbar ist.

[*)] Ist $(P, \rho^a) \equiv (P, \rho^b) (\text{mod.}\, p)$, so ist $a \equiv p^\kappa b (\text{mod.}\, \nu)$.

Beweis. Es sei $z^m + Az^{m-1} + Bz^{m-2} + .. = \Pi$. Dann ist $(\Pi, \rho^a) \equiv (\Pi, \rho^b) (\text{mod.}\, P)$; es gilt aber

$$(\Pi, \rho^a) \equiv (z-x^a)(z-x^{ap})(z-x^{app})\,..\,(z-x^{ap^{m-1}}),$$
$$(\Pi, \rho^b) \equiv (z-x^b)(z-x^{bp})(z-x^{bpp})\,..\,(z-x^{bpm-1})$$

woraus die Behauptung folgt.

Das Produkt aus $\Pi, (\Pi, \rho^2), (\Pi, \rho^3)$ usw. (Π, ρ^ν) ist $\equiv (z^\nu - 1)^m (\text{mod.}\, P)$, denn es ist

$$(z-x)(z-x^2)(z-x^3)\ldots(z-x^\nu) \\ \equiv (z-x^p)(z-x^{2p})(z-x^{3p})\,..\,(z-x^{\nu p}) \equiv \text{usw.} \equiv z^\nu - 1$$

In der Folge $P, (P, \rho^2), (P, \rho^3)$ usw. $\ldots . (P, \rho^\nu)$ kommen alle Primteiler der Funktion $x^\nu - 1$ vor, und zwar jeder m Mal. Daraus folgt, dass das Produkt aus allen $\equiv (x^\nu - 1)^m$ ist.

Ist $p^m \equiv 1 (\mathrm{mod.}\, \nu)$, und zwar m so klein wie möglich, so ist offenbar $x^{p^m-1} - 1$ durch $x^\nu - 1$ teilbar. Daher kann $x^\nu - 1$ nur solche Teiler haben wie $x^{p^m-1} - 1$. Dieser Ausdruck hat aber Primteiler vom Grad m und andere, deren Grad ein Teiler der Zahl m ist. Solche Teiler hat daher auch $x^\nu - 1$. Wie viele von jeder Art vorhanden sind, zeigen wir an einem Beispiel, aus dem sich das allgemeine Gesetz leicht ableiten lässt.

Es sei $\nu = 63$ und $p = 13$. Dann ist $m = 6$. Daher hat $x^{63} - 1$ nach dem Modul 13 Primfaktoren der Grade sechs, drei, zwei und eins. Offenbar ist das Produkt aus den Faktoren ersten Grades der gemeinsame Teiler höchsten Grades der Funktionen $x^{63} - 1$ und $x^{12} - 1$, d. h. $x^3 - 1$. Es gibt also drei Primfaktoren ersten Grades. Das Produkt aus allen Primfaktoren zweiten und ersten Grades ist der gemeinsame Teiler der Funktionen $x^{63} - 1$ und $x^{168} - 1$, d. h. $x^{21} - 1$. Daher gibt es $\frac{21-3}{2}$ oder 9 Faktoren zweiten Grades. Das Produkt aus den Primfaktoren dritten und ersten Grades ist der gemeinsame Teiler der Funktionen $x^{63} - 1$ und $x^{2196} - 1$, d. h. $x^9 - 1$. Daher gibt es $\frac{9-3}{3}$, d. h. 2 Teiler dritten Grades. Die übrigen haben schließlich den Grad sechs; ihre Anzahl ist daher $= \frac{63-6-18-3}{6}$, d. h. 6.

Durch genaue Betrachtung dieses Sachverhalts lässt sich leicht die folgende allgemeine Regel herleiten:

Es sei δ ein Teiler von m, und es seien alle Teiler der Zahl δ, die kleiner als δ sind, $\delta', \delta'', \delta'''$ usw. Die größten gemeinsamen Teiler von ν mit $p^\delta - 1$, $p^{\delta'} - 1$, $p^{\delta''} - 1$ usw. seien der Reihe nach μ, μ', μ'' usw. Es sei $\frac{\mu}{\mu'}; \frac{\mu}{\mu''}, \frac{\mu}{\mu'''}$ usw. $= \lambda', \lambda'', \lambda'''$ usw. Dann hat $x^\nu - 1$ $\frac{1}{\delta}$ Mal so viele Primteiler vom Grad δ, wie es unterhalb von μ Zahlen gibt, die durch keine der Zahlen $\lambda', \lambda'', \lambda'''$ usw. teilbar sind.

361.

Satz. *Ist eine Funktion X der Unbestimmten x durch eine andere Funktion ξ teilbar und geht X, wenn man x durch x^k ersetzt, in X' über, so ist X' durch $(\xi, \rho^{\frac{1}{k}})$ teilbar.*

Beweis. Es sei $X \equiv \xi\upsilon$, und ξ, υ mögen in ξ', υ' übergehen, wenn man x durch x^k ersetzt. Offenbar ist dann $X' \equiv \xi'\upsilon'$. Doch ist ξ' durch $(\xi, \rho^{\frac{1}{k}})$ teilbar. Also gilt dies auch für X'. Q. E. D.

362.

Mit diesen Grundlagen können wir die Primteiler der Funktion $x^\nu - 1$ leicht bestimmen. Wir nehmen an, dass alle Teiler, die auch irgendeine Funktion $x^\nu - 1$ teilen, wobei $\nu' < \nu$, bereits gefunden sind, und wollen die übrigen untersuchen. Diese lassen sich alle im Ausdruck (P, ρ^k) erfassen, wenn P einer von ihnen ist und für k alle Zahlen eingesetzt werden, die kleiner als ν und dazu teilerfremd sind.

Im Kapitel VI haben wir gezeigt, wie sich die primitiven Wurzeln der Gleichung $x^\nu = 1$ so in Klassen aufteilen lassen, dass dieselbe Klasseneinteilung entsteht, wenn man alle durch Potenzen einer von ihnen ausdrückt, gleichgültig, welche primitive Wurzel man als Basis nimmt. Solche Zusammenstellungen von Wurzeln haben wir *Perioden* genannt. Offenbar lassen sich die Funktionen $x, x^\alpha, x^\beta, x^\gamma$ usw., wobei α, β, γ usw. alle zu ν teilerfremden Zahlen bezeichnen, auf dieselbe Weise in Perioden zerlegen und jede größere Periode wiederum in kleinere, bis man schließlich zu Perioden der Form $x^k, x^{kp}, x^{kpp} \ldots x^{kp^{m-1}}$ gelangt. Ist dies geschehen, so ist Folgendes klar:

1. Da jede Periode aus kleinsten Perioden der Form $x^k + x^{kp} +$ usw. zusammengesetzt ist, ergibt ihre Division durch irgendeine Primfunktion vom Grad m einen Rest, der eine Zahl ist.

2. Alle Terme einer Periode lassen sich stets auf die Form $x^{\kappa . a^\alpha b^\beta c^\gamma \ldots}$ bringen, wobei $\kappa.\ a, b, c \ldots$ feste Zahlen sind, während für $\alpha, \beta, \gamma \ldots$ alle Werte eingesetzt werden können. Daher geht die Periode in sich selbst über, wenn man x durch x^k ersetzt und k die Form $a^\alpha b^\beta c^\gamma \ldots (\mathrm{mod.}\, \nu)$ hat. Hieraus erkennt man leicht, dass alle Funktionen $P, (P\ \rho^k)$ usw., wobei k eine solche Zahl bezeichnet, bei der Division der Periode durch sie denselben Rest ergeben.

3. Nach Abzug eines solchen Restes lässt sich die Periode somit durch das Produkt aus allen Funktionen (P, ρ^k) teilen.

363.

Die Hauptaufgabe besteht darin, diese Reste zu bestimmen. Zuerst suche man den Rest, den die größte Periode bei der Division durch das Produkt aller zugehörigen Primfunktionen ergibt. Ist dieses Produkt

$$\equiv x^\lambda - Ax^{\lambda-1} + \text{usw.}$$

so ist dieser Rest $\equiv A$. Die Form dieses Produkts lässt sich leicht finden, und aus Kapitel VI folgt, dass $A = 0$ ist, wenn ν durch ein Quadrat teilbar ist; andernfalls ist A entweder $= +1$ oder $= -1$, je nachdem, ob die Anzahl der Primfaktoren von ν gerade oder ungerade ist.

Nun zerlege man diese größte Periode in kleinere Perioden und stelle die Glieder einer beliebigen Periode durch $x^{kp^\pi u}$ dar, sodass k innerhalb jeder Periode eine feste Zahl ist, zwischen den Perioden aber wechselt, während π und u innerhalb jeder Periode veränderlich sind und die Werte, die sie in

einer Periode annehmen, auch in den übrigen annehmen können. Man nehme vorläufig eine beliebige Primfunktion P als Basis an, und die Perioden $\Sigma x^{p^\pi u}$, $\Sigma x^{k' p^\pi u}$ usw. mögen bei der Division durch sie jeweils die Reste A, A' usw. ergeben. Dann ist $\Sigma x^{p^\pi u} - A$ durch das Produkt aller Funktionen (P, ρ^u) teilbar; $\Sigma x^{k' p^\pi u} - A'$ durch das Produkt aller Funktionen $(P, \rho^{k' u})$; usw., usw. Man sieht leicht, dass die Größen A, A' usw. Wurzeln einer bekannten Kongruenz sind. Sind nämlich die Perioden der Wurzeln der Gleichung $x^\nu = 1$, die den vorigen Perioden entsprechen, Wurzeln der Gleichung $Q = 0$, so sind A, A' usw. Wurzeln der Kongruenz $Q \equiv 0$. Denn es gilt

$$A + A' + \text{usw.} \equiv \text{der Summe der Perioden},$$
$$AA + A'A' + \text{usw.} \equiv \text{der Summe der Quadrate der Perioden}$$

usw., usw. Die Rechnung ist derjenigen völlig ähnlich, die wir in Kapitel VI dargestellt haben, wenn man für ρ nun x setzt, da man auch hier für x^ν die Einheit setzen kann, wie dort für ρ^ν.

Hat man die Wurzeln A, A' usw. gefunden, so wähle man eine als Rest der Periode $\Sigma x^{p^\pi u}$ und ordne danach die Reste der übrigen wie in Kapitel VI. Auch hier bleibt diese Wahl frei, da die Funktion P bisher völlig unbestimmt ist. Die folgende Rechnung ist derjenigen ganz analog, die wir in Kapitel VI behandelt haben; jede Einzelheit darzustellen, würde uns zu weit führen. Ist man schließlich zu Σx^{p^π} gelangt, so ist die Hauptaufgabe erledigt. Denn setzt man

$$P \equiv x^m + ax^{m-1} + bx^{m-2} + \text{usw.}$$

so ist $-a \equiv \Sigma x^{p^\pi}$. Ebenso erhält man den zweiten Koeffizienten der übrigen Funktionen (P, ρ^k), woraus sich die restlichen Koeffizienten von P bestimmen lassen. Es kann häufig vorkommen, dass man zu identischen Kongruenzen gelangt, aus denen sich anscheinend nichts ableiten lässt. Wie man dieser Schwierigkeit begegnen kann, wird weiter unten gezeigt.

364.

Ein Beispiel wird dies alles viel deutlicher machen. Die Funktion $x^{15} - 1$ soll modulo 17 in Faktoren zerlegt werden. Es ist $m = 4$, und da das Produkt aller elementaren Funktionen

$$\equiv \frac{x^{15} - 1 \,.\, x - 1}{x^3 - 1 \,.\, x^5 - 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

ist, gibt es somit nur zwei Primfaktoren vierten Grades, P und P'. Nun verteile man $x, xx, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}$ auf diese beiden Perioden:

$$\Sigma x^{17^\alpha} \equiv x + xx + x^4 + x^8,$$
$$\Sigma x^{7.17^\alpha} \equiv x^7 + x^{11} + x^{13} + x^{14}$$

Modulo einer der Funktionen P, P' sei

$$\Sigma x^{17^\alpha} \equiv A, \quad \Sigma x^{7.17^\alpha} \equiv A'$$

Dann gilt

$$\begin{aligned} A + A' &\equiv 1 \\ AA &\equiv \Sigma x^{2.17^\alpha} + \Sigma x^{3.17^\alpha} + \Sigma x^{5.17^\alpha} + \Sigma x^{9.17^\alpha} \\ A'A' &\equiv \Sigma x^{14.17^\alpha} + \Sigma x^{6.17^\alpha} + \Sigma x^{5.17^\alpha} + \Sigma x^{3.17^\alpha} \end{aligned}$$

also

$$\begin{aligned} AA + A'A' &\equiv \Sigma x^{17^\alpha} + \Sigma x^{7.17^\alpha} + 4\Sigma x^{3.17^\alpha} + 2\Sigma x^{5.17^\alpha} \\ &\equiv 1 - 4 - 4 \equiv -7 \end{aligned}$$

Somit sind A und A' die Wurzeln der Kongruenz

$$xx - x + 4 \equiv 0 \,(\text{mod. } 17)$$

und diese sind $6, 12$. Daher teilt P den Ausdruck

$$x^8 + x^4 + xx + x - 6$$

und ist

$$\equiv x^4 - 6x^3 - 2xx - 12x + 1$$

Weiter ist P' dann $\equiv (P, \rho^7)$ und somit

$$\equiv x^4 - 12x^3 - 2xx - 6x + 1$$

365.

Uns genügt es hier, die Möglichkeit dieser Lösungen gezeigt zu haben. Viele Kunstgriffe, die diese Operationen erleichtern können, übergehen wir der Kürze wegen. Einige sehr wichtige Folgerungen können wir aber nicht auslassen.

Durch das Vorige ist bewiesen, dass alle Hilfsgleichungen zur Lösung der Gleichung $x^\nu = 1$, wenn man sie in Kongruenzen umwandelt, mögliche Wurzeln haben, wenn die Periode

$$x + x^p + x^{pp} + \ldots + x^{p^{m-1}}$$

noch nicht zerlegt ist. Bleiben wir bei dem Fall, dass ν eine Primzahl ist; dann ist m ein Teiler von $\nu - 1$. Hier haben also die Hilfskongruenzen wirkliche Wurzeln, wenn die Anzahl der durch sie gefundenen Perioden ein Teiler von $\frac{\nu-1}{m}$ ist. Ist daher $\frac{\nu-1}{m}$ gerade, ist also m ein Teiler von $\frac{\nu-1}{2}$, oder gilt

gleichbedeutend $p^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$, oder ist gleichbedeutend p ein quadratischer Rest der Primzahl ν, so hat die quadratische Gleichung, durch die die Wurzeln in zwei Perioden geteilt werden, wirkliche Wurzeln modulo p. In Kapitel VI haben wir aber gezeigt, dass diese Gleichung, wenn man $\nu = 4n \pm 1$ setzt, stets $xx + x \mp n = 0$ ist. Somit erhalten wir den bemerkenswerten

SATZ. *Ist die Primzahl p ein quadratischer Rest der Primzahl $4n \pm 1$, so hat die Kongruenz*

$$xx + x \mp n \equiv 0 (\mathrm{mod.}\, p)$$

wirkliche Wurzeln und folglich auch die Kongruenz

$$4xx + 4x \mp 4n \equiv 0 \quad \text{oder} \quad (2x+1)^2 \mp \nu \equiv 0$$

das heißt, $\pm\nu$ ist ein quadratischer Rest von p.

366.

Dies ist also der dritte vollständige Beweis des Fundamentalsatzes aus Kapitel IV. Er verdient umso mehr Aufmerksamkeit, als die Prinzipien, aus denen er gewonnen ist, von denen, die wir für die früheren Beweise verwendet haben, völlig verschieden sind. .Aus derselben Quelle wollen wir nun auf dem entgegengesetzten Weg einen vierten ableiten. Es sei nämlich ν eine Primzahl der Form $4n \pm 1$, p eine beliebige andere Primzahl, und $\pm\nu$ sei ein quadratischer Rest der Primzahl p; wir werden beweisen, dass p ein quadratischer Rest von ν ist.

Es sei p^m die kleinste Potenz von p, die $\equiv 1(\mathrm{mod.}\,\nu)$ ist. Die elementaren Teiler der Funktion $\frac{x^\nu-1}{x-1}$ modulo p haben den Grad m, sodass ihre Gesamtzahl $= \frac{\nu-1}{m}$ ist. Da nun $\pm\nu Rp$ gilt, ist die Kongruenz

$$xx + x \mp n \equiv 0(\mathrm{mod.}\,p)$$

lösbar; ihre Wurzeln seien A, A'. Man verteile die Funktionen $x, xx, .. x^{\nu-1}$ auf zwei Klassen, die mit ξ, ξ' bezeichnet werden. Dann ist

$$\xi + \xi' \equiv A + A' + (1 + x + xx + .. + x^{\nu-1})$$
$$\xi\xi' \equiv AA' + \lambda(1 + x + xx + .. + x^{\nu-1})$$

also ist

$$(z - \xi)(z - \xi') - (z - A)(z - A')$$

durch jeden elementaren Teiler der Funktion $\frac{x^\nu-1}{x-1}$ teilbar. Daher teilt jeder dieser elementaren Teiler entweder $\xi - A$ und $\xi' - A'$ oder $\xi - A'$ und $\xi' - A$. Hieraus folgt (da A nicht $\equiv A'$ ist): Setzt man für x nun x^p, so ändern sich ξ und ξ' nicht. Ginge nämlich ξ in ξ' über und umgekehrt, so wären $\xi - A$ und $\xi - A'$ durch dieselbe Primfunktion teilbar. Q. E. A. Schließlich folgt daraus, dass $\frac{\nu-1}{2}$ durch m teilbar ist oder gleichbedeutend $p^{\frac{\nu-1}{2}} - 1$ durch ν. Also ist p ein quadratischer Rest von ν. Q. E. D.

Alle Fälle des Fundamentalsatzes lassen sich leicht aus den beiden Sätzen ableiten.

367.

Obwohl wir uns hier auf den Fall beschränkt haben, dass ν eine Primzahl ist, lassen sich auch für zusammengesetztes ν ohne große Mühe analoge Sätze bestimmen; der Kürze wegen können wir dies jetzt nicht ausführlicher darstellen.

Es ist offensichtlich, dass sich ähnliche Beobachtungen auch über eine größere Anzahl von Perioden anstellen lassen. Ist also $\frac{\nu-1}{m}$ durch 3 teilbar, ist also p ein kubischer Rest der Primzahl ν, so ist die Gleichung, durch die die Wurzeln der Gleichung $x^\nu = 1$ auf drei Perioden verteilt werden und deren Bestimmung a priori wir in Kapitel VI gelehrt haben, modulo p lösbar und umgekehrt. So lässt sich zum Beispiel die Kongruenz $x^3 + xx - 2x - 1 \equiv 0$ modulo jeder Primzahl der Form $7n \pm 1$ lösen, nicht aber, wenn sie eine andere Form hat.

Es würde uns nicht schwerfallen, dieses Kapitel mit vielen anderen Beobachtungen zu bereichern, wenn die Grenzen, innerhalb deren wir bleiben müssen, es nicht verhinderten. Denjenigen, die weitergehen möchten, können diese Prinzipien wenigstens den Weg weisen.

368.

Wir sagen, eine Kongruenz $S \equiv 0$ habe *gleiche* Wurzeln oder allgemeiner gleiche Teiler, wenn sie durch eine Potenz irgendeiner Funktion teilbar ist.

Ob eine gegebene Kongruenz gleiche Teiler hat, entscheidet man ebenso wie in der Theorie der Gleichungen. Setzen wir

$$X \equiv \xi^m P$$

so ist offensichtlich

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv \xi^{m-1}\left(mP\frac{\mathrm{d}\xi}{\mathrm{d}x} + \xi\frac{\mathrm{d}P}{\mathrm{d}x}\right)$$

also ist $\frac{\mathrm{d}X}{\mathrm{d}x}$ durch ξ^{m-1} teilbar. Allgemeiner sei

$$X \equiv A^a B^b C^c \text{ usw.}$$

wobei A, B, C usw. verschiedene Primfunktionen bezeichnen. Dann ist

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv X\left(\frac{a\,\mathrm{d}A}{A\,\mathrm{d}x} + \frac{b\,\mathrm{d}B}{B\,\mathrm{d}x} + \frac{c\,\mathrm{d}C}{C\,\mathrm{d}x} + \text{usw.}\right)$$

Daraus folgt, dass, sofern nicht eine der Zahlen a, b, c usw. durch den Modul teilbar ist, $\frac{\mathrm{d}X}{\mathrm{d}x}$ durch $A^{a-1}B^{b-1}C^{c-1}$ usw., nicht aber durch A^a, B^b, C^c usw. teilbar ist. Hieraus folgt der

Satz. *Ist der gemeinsame Teiler höchsten Grades der Funktionen X und $\frac{\mathrm{d}X}{\mathrm{d}x}$ gleich ξ, so kommen alle Primfaktoren von ξ auch in X vor, und zwar jeweils mit einer um $+1$ größeren Vielfachheit als in ξ. Sind also X und $\frac{\mathrm{d}X}{\mathrm{d}x}$ teilerfremde Funktionen, so hat X keine gleichen Faktoren.*

369.

Beispiel I. Gesucht ist, ob die Funktion

$$x^5 + 3x^4 - 6x^3 + 3x - 4 \ldots (X)$$

modulo 17 gleiche Teiler hat. Es ist

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 5x^3 - xx + 3$$

Hieraus findet man, dass die Funktionen X und $\frac{\mathrm{d}X}{\mathrm{d}x}$ teilerfremd sind, sodass X keine gleichen Teiler hat.

Beispiel II. Es sei

$$X \equiv x^5 + 6x^4 - 3x^3 - 4xx + 2x - 3 (\text{mod. } 13)$$

Dann ist

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 2x^3 + 4xx + 5x + 2$$

Der größte gemeinsame Teiler der Funktionen X, $\frac{\mathrm{d}X}{\mathrm{d}x}$ ist $\equiv 5xx + 7x + 7$ oder, mit 8 multipliziert: $xx+4x+4$. Da dieser Teiler $\equiv (x+2)^2$ ist, ist die Funktion X durch $(x+2)^3$ teilbar, und der Quotient (der $xx + 11$ ist) enthält keinen weiteren doppelten Teiler.

370. 371.

Ist die Funktion X nach den vorigen Abschnitten als $A^a B^b C^c$ usw. dargestellt, wobei A, B, C usw. teilerfremd und die Zahlen a, b, c usw. ungleich sind, so lässt sich die Zerlegung weiter fortsetzen. Es sei also X eine Funktion, die keine gleichen Teiler mehr enthält. Wir haben oben gesehen, dass $x^p - x$ das Produkt aller Primfunktionen ersten Grades ist. Es sei ξ der gemeinsame Teiler höchsten Grades der Funktionen X und $x^p - x$; dann ist ξ das Produkt aller Teiler von X ersten Grades, und $\frac{X}{\xi}$ hat keine solchen Teiler mehr. Findet man dagegen, dass die Funktionen X und $x^p - x$ teilerfremd sind, so hat X keinen Teiler ersten Grades, und daher hat die Kongruenz $X \equiv 0$ keine wirklichen Wurzeln. Da ferner $x^{pp} - x$ das Produkt aller Primfunktionen zweiten und ersten Grades ist, enthält der gemeinsame Teiler höchsten Grades der Funktionen $x^{pp} - x$ und $\frac{X}{\xi}$, nämlich ξ', alle Teiler von X zweiten Grades. Setzt man dies fort, so erkennt man, dass X auf diese Weise in Faktoren ξ, ξ', ξ'' usw. zerlegt wird, die jeweils alle Teiler ersten, zweiten, dritten usw. Grades enthalten.

372.

Ist aber das Produkt mehrerer Primfunktionen gleichen Grades gegeben, so müssen die einzelnen Funktionen durch Probieren gefunden werden. Diese Aufgabe hat große Ähnlichkeit mit derjenigen, die Faktoren zusammengesetzter Zahlen zu finden. Hier ist jedoch schon a priori bestimmt, ob sich die gegebene Funktion noch in Faktoren zerlegen lässt. Da auch hier die Anzahl aller möglichen Faktoren endlich ist, können wir ein ähnliches Hilfsmittel wie oben verwenden. Doch wollen wir uns damit nicht aufhalten, denn ein geübter Rechner, der die Prinzipien gründlich erfasst hat, wird bei Bedarf leicht besondere Kunstgriffe finden.

Wir gehen zu einem anderen Thema über, nämlich zur Betrachtung von Kongruenzen, deren Modul keine Primzahl ist, wie wir es bisher stets vorausgesetzt haben. Besonders verdient hier der Fall Aufmerksamkeit, dass der Modul eine Potenz einer Primzahl ist, sowohl an sich als auch deshalb, weil er zur Beseitigung einiger Zweifel (§.§. . .) nötig ist.

373.

Aufgabe. *Ist die Funktion X modulo p in teilerfremde Faktoren ξ, ξ', ξ'' usw. zerlegt, so zerlege man X modulo pp in ähnliche Faktoren Ξ, Ξ', Ξ'' usw., sodass*

$$\xi \equiv \Xi, \quad \xi' \equiv \Xi', \quad \xi'' \equiv \Xi'', \text{ usw. } (\mathrm{mod.}\, p)$$

Lösung. Es sei $X \equiv \xi\psi (\mathrm{mod.}\, p)$ oder gleichbedeutend $X = \xi\psi + p\Sigma$. Setzt man

$$\Xi = \xi + p\varphi, \quad \Psi = \psi + p\omega$$

so ist

$$\Xi\Psi = X - p\Sigma + (\varphi\psi + \xi\omega)p + pp\varphi\omega$$

Soll also $\Xi\Psi$ nun $\equiv X (\mathrm{mod.}\, pp)$ sein, so muss $\varphi\psi + \xi\omega - \Sigma$ notwendig durch p teilbar sein. Da aber ψ und ξ modulo p teilerfremde Funktionen sind, lassen sich φ und ω so bestimmen, dass diese Bedingung erfüllt ist (§. 336), und zwar außerdem so, dass die Grade von φ und ω jeweils um eins kleiner sind als die Grade der Funktionen ξ, ψ. Daher ist $X \equiv \Xi\Psi (\mathrm{mod.}\, pp)$. Offenbar lässt sich Ψ auf ähnliche Weise wieder in Faktoren $\Xi'\Omega$ zerlegen, wobei der Faktor Ξ' dann $\equiv \xi' (\mathrm{mod.}\, p)$ ist, und so fort, bis schließlich

$$X \equiv \Xi\,\Xi'\,\Xi'' \text{ usw. } (\mathrm{mod.}\, pp). \quad \text{Q. E. Fac.}$$

374.

Hieraus lässt sich leicht beweisen, dass die Funktion X auch modulo p^3, p^4 usw. in Faktoren zerlegt werden kann. Allgemeiner sei

$$X \equiv PQ (\mathrm{mod.}\, p^m) \quad \text{oder} \quad X = PQ + p^m R$$

und die Funktion P sei zu Q modulo p teilerfremd. Setzt man

$$P' = P + Ap^m, \quad Q' = Q + Bp^m$$

so ist

$$P'Q' = X - p^m R + (AQ + BP)p^m + ABp^{2m}$$

Hieraus folgt für jeden Modul p^ν (wobei ν dann $> m$ und $< 2m + 1$ ist)

$$P'Q' \equiv X, \quad \text{wenn} \quad R \equiv AQ + BP (\mathrm{mod.}\, p^{\nu - m})$$

Daraus erkennt man: Hat die Funktion X modulo p keine gleichen Teiler, so lässt sie sich modulo p^k auf ähnliche Weise in Faktoren zerlegen wie modulo p. Hat aber X gleiche Teiler, so wird die Sache viel komplizierter und lässt sich durch die vorigen Prinzipien nicht einmal vollständig behandeln. Da wir nicht alles hierzu Gehörige mitteilen können, wollen wir nur einen einzigen Fall betrachten, der sehr häufig vorkommt und dessen Auflösung nötig ist, um

gewisse Zweifel im Vorigen zu beseitigen. Dies ist der Fall, dass nur gleiche Faktoren ersten Grades betrachtet werden. Er lässt sich auch unmittelbar zur Bestimmung der Wurzeln von Kongruenzen verwenden. Allgemein werden wir diesen Gegenstand bei anderer Gelegenheit behandeln.

375.

Es sei also $X \equiv X'(x-a)^m (\mathrm{mod.}\, p)$, und die Funktion X' sei zu $x-a$ teilerfremd: Gesucht sind alle Teiler ersten Grades, die $x-a$ modulo p kongruent sind und X modulo pp, p^3 usw. teilen. (Wir setzen voraus, dass die Funktion X ohne einen Modul nicht durch $x-a$ teilbar ist; andernfalls würde $x-a$ die Funktion X nach jedem Modul teilen.) Setzt man $z+a$ für x ein, so erhält man

$$Z \equiv Z' z^m (\mathrm{mod.}\, p) \quad \text{oder} \quad Z = Z' z^m + pA$$

Ist nun Z modulo pp durch einen Teiler der Form $z+\alpha p$ teilbar, so muss A notwendig die Form $zZ'' + pB$ haben. Ist dies nicht der Fall, so ist die Untersuchung bereits beendet. Setzen wir also

$$Z \equiv Z' z^m + pZ'' z (\mathrm{mod.}\, pp)$$
$$\text{oder} \quad Z = Z' z^m + pZ'' z + ppB$$

so ist offenbar Z durch z und jeden anderen diesem modulo p kongruenten Teiler teilbar.

Um die Aufmerksamkeit auf einen bestimmten Fall zu richten, setzen wir $m = 4$; man sieht leicht, dass jeder andere Fall auf ähnliche Weise behandelt werden kann. Ist nun Z modulo p^3 durch einen Teiler der Form $z+\alpha p$ teilbar, so ist

$$0 \equiv -\alpha pp Z'' + ppB (\mathrm{modd.}\, z+\alpha p, p^3)$$
$$\text{oder} \quad \alpha Z'' \equiv B (\mathrm{modd.}\, z, p)$$

Nun können drei Fälle eintreten

1) Ist $Z'' \equiv 0 (\mathrm{modd.}\, z, p)$ und B nicht $\equiv 0$, so erfüllt offenbar kein Wert von α die Kongruenz, sodass Z modulo p^3 keinen Teiler der Form $z+\alpha p$ hat. Die Untersuchung ist somit beendet

2) Ist weder Z'' noch $B \equiv 0 (\mathrm{modd.}\, z, p)$, so hat α einen einzigen Wert, nämlich

$$\alpha \equiv \frac{B}{Z''} (\mathrm{modd.}\, z, p).$$

Daher gibt es einen einzigen Teiler $\equiv z+\alpha p (\mathrm{mod.}\, pp)$ von Z modulo p^3, und es ist

$$Z \equiv V(z+\alpha p) + p^3 W$$

Setzt man nun als Teiler von $Z (\mathrm{mod.}\, p^4)$ den Ausdruck $z+\alpha p+\beta pp$ an, so ist

$$0 \equiv$$

BEMERKUNGEN ZUR ANALYSIS RESIDUORUM.

Die beiden vorstehenden Abhandlungen sind einem umfangreichen Manuskript mit dem Titel Analysis Residuorum entnommen, das vermutlich aus dem Jahr 1797 oder 1798 stammt; durch eine vollständige Umarbeitung entstanden daraus später die Disquisitiones Arithmeticae. Der vollständige Titel des sechsten Kapitels lautet:

Lösung der Kongruenz $x^m - 1 \equiv 0$ und der Gleichung $x^m - 1 = 0$; mit Erläuterungen zur Theorie der regelmäßigen Vielecke.

Der wesentliche Inhalt seines zweiten Teils (§§. 253–278) ging in den siebten Abschnitt der Disqq. Arithm. über.

Außerdem ist das siebte Kapitel teilweise erhalten: Verschiedene Anwendungen einiger vorangehender Untersuchungen (§§. 279–302). Es gliedert sich in folgende Unterabschnitte:

Über Umformungen gewöhnlicher Brüche (§§. 279–281).

Über die Umwandlung gewöhnlicher Brüche in Dezimalbrüche (§§. 282–292).

Über die Lösung der unbestimmten Gleichung $xx = a + by$ (§§. 293–297).

Über die Lösung der unbestimmten Gleichung $axx + byy = c$ (§§. 298–301).

Über die Bestimmung der Teiler von Zahlen (§. 302; die folgenden Bogen fehlen).

Dies alles ist fast wörtlich in den sechsten Abschnitt der Disqq. Arithm. aufgenommen.

Die beiden hier mitgeteilten Abschnitte behandeln die Gegenstände, die, wie aus der Vorrede und den Artikeln 11, 44, 61, 62, 65, 84 der Disqq. Arithm. hervorgeht, den Inhalt des achten Abschnitts dieses Werks bilden sollten. Es ist jedoch zu bemerken, dass dieser Plan später wieder geändert wurde; unter den Manuskripten findet sich nämlich ein Fragment mit der Überschrift Achter Abschnitt: Ausführlichere Betrachtung einiger Untersuchungen zur Kreisteilung. Dieses beginnt mit Art. 367 und sollte somit die Fortsetzung der Disqq. Arithm. bilden; der Inhalt der wenigen noch vorhandenen Artikel ging aber später in die Abhandlung Summatio quarundam serierum singularium über, und deshalb wird dieses Fragment von der gegenwärtigen Ausgabe ausgeschlossen.

Im vorstehenden Abdruck der beiden Teile der Analysis Residuorum ist der Text des Originals im Wesentlichen treu beibehalten, obwohl es seiner Form nach nicht als druckfertig gelten kann; die folgenden Bemerkungen geben die wichtigsten Abänderungen an und fügen zugleich einige Erläuterungen hinzu.

§. 237. Vgl. Disqq. Arithm. artt. 61, 62.

§. 239. Vgl. Disqq. Arithm. artt. 53, 54, 65.

§. 241. Ist $n = 2^\nu$ und $\nu \geqq 3$, so gibt es zwar keine Zahl ρ der angegebenen Art, aber die gesamte Untersuchung wird dadurch nicht wesentlich geändert.

§. 251. Vermutlich sollte die hier erwähnte Schwierigkeit durch die Einführung höherer Potenzen von p als Moduln beseitigt werden. Vgl. §§. 363, 372, 373.

§. 332. Die Voraussetzung, dass der Modul eine Primzahl ist, wird bis einschließlich §. 372 beibehalten.

§. 338. Das unvollständige Zitat kann sich auf Disqq. Arithm. art. 44 beziehen.

§§. 344–346. Von den beiden im Manuskript vorhandenen Beweisen ist hier der erste, der mit den Worten »wir gehen nun daran zu beweisen« eingeleitet wird und auf einer näheren Untersuchung der Ausdrücke $(1^\alpha 2^\beta 3^\gamma \ldots)$ beruht, nach der eigenen Anweisung des Verfassers vollständig unterdrückt (»Der gesamte vorangehende Beweis muss zusammen mit einem anderen Beweis des vorigen Satzes, den wir hinzufügen wollten, unterdrückt werden, da wir einen anderen, unendlich einfacheren entdeckt haben. Er beruht auf dieser Grundlage«); im obigen Abdruck ist ferner der zweite Beweis dadurch verkürzt, dass die Entwicklung von $\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x}$ statt derjenigen von $\frac{x\,\mathrm{d}P}{\mathrm{d}x}$ betrachtet wird, wodurch zugleich ein im Original enthaltener Bezug auf den unterdrückten ersten Beweis vermieden wird.

§. 348. Der Ausdruck radix prima ist hier in derselben Bedeutung zu verstehen wie radix propria in der Abhandlung Summatio quarundam serierum singularum, art. 11. — Bei der Behauptung, dass die Koeffizienten $A'.B'\ldots$ des ausmultiplizierten Produkts ganze rationale Zahlen sind, wird auf das sechste Kapitel verwiesen, in dem aber die Theorie der Gleichung $x^\tau - 1 = 0$ nur für den Fall behandelt wird, dass τ eine Primzahl ist; die Form des Beweises in §. 349 führt zunächst zu folgender Ergänzung. Bringt man das ausmultiplizierte Produkt in die (für alle Wurzeln der Gleichung $\theta^\tau = 1$ geltende) Form

$$S = E + F\theta + \ldots + N\theta^{\tau-1}$$

so sind die Koeffizienten $E, F \ldots N$ Polynome in x mit ganzzahligen rationalen Koeffizienten. Da ferner das Produkt unverändert bleibt, wenn θ durch θ^k ersetzt wird, wobei k eine beliebige zu τ teilerfremde Zahl bedeutet, gilt dasselbe für den Ausdruck S. Daraus folgt ohne Schwierigkeit, dass alle in S enthaltenen Potenzen von θ, deren Exponenten s denselben größten gemeinsamen Teiler mit τ haben, auch identische Koeffizienten haben müssen. Da schließlich jede Summe solcher Potenzen θ^s stets eine ganze Zahl ist, ist offensichtlich, dass der Ausdruck S und folglich auch das fragliche Produkt ein Polynom in x mit ganzzahligen Koeffizienten ist, was zu zeigen war. Aus dieser Betrachtung ergibt sich zugleich die Richtigkeit der Bemerkung am Schluss

des Paragraphen. Andere Gründe lassen jedoch vermuten, dass dem Verfasser schon damals der allgemeine Satz über die Transformation symmetrischer Funktionen (Demonstratio nova altera theorematis omnem functionem etc. art. 4) bekannt war, aus dem die obigen Sätze unmittelbar folgen.

§. 352. Das Zeichen $R \equiv S(\mathrm{mod.}\, P)$ oder auch $R \equiv S(\mathrm{mod.}\, P, p)$ bedeutet hier und im Folgenden, dass die Differenz $R - S$ modulo p den Teiler P hat. — Das unvollständige Zitat kann sich auf Disqq. Arithm. art. 49 beziehen.

§. 354. Durch Multiplikation mit $x^\nu - 1$ ergibt sich, dass die Summen gleich hoher Potenzen der Wurzeln der beiden Gleichungen $(P, \rho^{k\nu+t}) = 0$, $(P, \rho^t) = 0$ einander kongruent sind $(\mathrm{mod.}\, p)$, und daraus folgt die Kongruenz $(P, \rho^{k\nu+t}) \equiv (P, \rho^t)(\mathrm{mod.}\, p)$, sobald $m < p$ gilt (vgl. §. 244). Ist aber $m \geqq p$, so lässt sich der Koeffizient der Potenz x^{m-p} in einer Gleichung nicht mehr modulo p aus den gegebenen Potenzsummen ihrer Wurzeln bestimmen, weil er in den dazu dienenden Formeln von Newton mit dem Faktor p auftritt. Tatsächlich darf man aus der Kongruenz je zweier gleich hoher Potenzsummen der Wurzeln der Gleichungen $A = 0$, $B = 0$ allgemein nur folgern, dass $A \equiv \mathfrak{A}^p\mathfrak{C}$, $B = \mathfrak{B}^p\mathfrak{C}(\mathrm{mod.}\, p)$ gilt, wobei $\mathfrak{C}$ den größten gemeinsamen Teiler der beiden Funktionen A, B nach dem Primzahlmodul p bezeichnet, während $\mathfrak{A}$ und $\mathfrak{B}$ völlig unbestimmte Funktionen sind. Es ist zu vermuten, dass der Verfasser die Allgemeingültigkeit des Satzes aus der Theorie der Transformation symmetrischer Funktionen und insbesondere aus dem folgenden Satz abgeleitet hat: Ist in Bezug auf einen beliebigen Modul p die Differenz $R(x) - S(x)$ durch die Funktion $P(x)$ teilbar, und sind $a, b, c \ldots$ die Wurzeln der Gleichung $P(x) = 0$, so sind die Funktionen

$$(x - R(a))(x - R(b))(x - R(c)) \ldots \quad \text{und}$$
$$(x - S(a))(x - S(b))(x - S(c)) \ldots$$

einander modulo p kongruent.

§. 355. In §. 368 wird gezeigt, dass P und $\frac{\mathrm{d}P}{\mathrm{d}x}$ keinen gemeinsamen Teiler haben, wenn P keinen Faktor mehr als einmal enthält.

§§. 358, 359. Die unter den Text gesetzte Note ist einem einzelnen Blatt entnommen, das wahrscheinlich den bereits in der Handschrift gestrichenen §. 359 ersetzen sollte.

§. 360. In der Formulierung des Satzes ist eine Ungenauigkeit der Handschrift berichtigt.

§. 361. Hier bedeutet der Exponent $\frac{1}{k}$ im Zeichen $(\xi, \rho^{\frac{1}{k}})$ jede positive ganze Zahl k', für die $kk' \equiv 1(\mathrm{mod.}\, \nu)$ gilt, wobei ν die kleinste positive ganze Zahl ist, für die $x^\nu - 1$ durch ξ modulo p teilbar wird; dabei ist vorauszusetzen, dass ξ nicht durch x modulo p teilbar ist, und außerdem, dass k zu ν teilerfremd ist. Die Richtigkeit der Behauptung, dass ξ' durch $(\xi, \rho^{\frac{1}{k}})$ teilbar ist $(\mathrm{mod.}\, p)$, ergibt sich aus §. 354.

§. 363. Die Schlussbemerkung bezieht sich vermutlich auf die Einführung von Moduln, die Potenzen der Primzahl p sind; vgl. §§. 251, 372, 373.

§. 367. Die Wurzeln der Gleichung $x^3 + xx - 2x - 1 = 0$ sind die zweigliedrigen Perioden, in die die Wurzeln der Gleichung $\frac{x^7-1}{x-1} = 0$ zerfallen. Dasselbe Beispiel findet sich auch auf einem einzelnen Blatt, auf dem das Hauptresultat der §§. 362, 363 unter dem Titel »der goldene Lehrsatz« ausgesprochen ist.

§. 371. Dieser Paragraph sollte ein Beispiel enthalten; es ist jedoch nicht ausgeführt.

R. Dedekind.

WEITERE ENTWICKLUNG DER UNTERSUCHUNGEN ÜBER REINE GLEICHUNGEN.

1.

Das Verfahren, mit dem wir in Artikel 360 der *Disquiss. Arithm.* gezeigt haben, wie die Gleichung $x^n - 1 = 0$ zu lösen ist, bildet eine überaus fruchtbare und bedeutende Theorie, von der wir in jenem Werk nur die ersten Grundlagen berühren konnten. Wir hoffen daher, dass es den Mathematikern willkommen sein wird, wenn wir diesen Gegenstand hier erneut aufnehmen, das nur kurz und zum Teil unter Auslassung der Beweise Skizzierte ausführlicher behandeln und die seit jener Zeit hinzugekommenen Entwicklungen eingehender verfolgen.

Der Exponent n wird als Primzahl vorausgesetzt und die Zahl $n - 1$ als in die Faktoren $\alpha \times \beta \times \gamma$ zerlegt; ferner bezeichnen wir mit g irgendeine primitive Wurzel zum Modul n. Es bezeichne r eine beliebige Wurzel der Gleichung $x^n - 1 = 0$ und R eine beliebige Wurzel der Gleichung $x^\beta - 1 = 0$. Bezeichnen wir also den Umfang des Kreises, dessen Radius $= 1$ ist, mit P und die imaginäre Größe $\sqrt{-1}$ mit i, so werden sämtliche Wurzeln der Gleichung $x^\beta - 1 = 0$ oder sämtliche Werte von R durch die Formel

$$\cos \frac{kP}{\theta} + i \sin \frac{kP}{\theta}$$

dargestellt, wobei k die ganzen Zahlen $0, 1, 2, 3 \ldots \beta - 1$ durchläuft. Ferner sind offenbar sämtliche Potenzen jeder Wurzel R selbst ebenfalls Wurzeln; ist R die Wurzel, die einem Wert von k entspricht, der zu β teilerfremd ist, so sind alle Potenzen $R^0, R, R^2, R^3 \ldots R^{\beta-1}$ voneinander verschieden und erschöpfen daher die gesamte Menge der Wurzeln. In diesem Fall nennen wir R eine *eigentliche* Wurzel der Gleichung $x^\beta - 1 = 0$; dagegen heißt eine Wurzel R, die einem Wert von k entspricht, der zu β nicht teilerfremd ist, *uneigentlich*. Ist δ der größte gemeinsame Teiler der Zahlen k und β, so gilt, wie man leicht sieht, $R^{\frac{\beta}{\delta}\cdot} = 1$, während alle Potenzen $R^0, R, R^2, R^3 \ldots R^{\frac{\beta}{\delta}-1}$ voneinander verschieden sind; daher ist R eine eigentliche Wurzel der Gleichung $x^{\frac{\beta}{\delta}} - 1 = 0$. Dasselbe gilt für die Gleichung $x^n - 1 = 0$, doch sind deren Wurzeln mit Ausnahme der Wurzel 1 notwendigerweise sämtlich eigentlich.

2.

Nach diesen Vorbemerkungen soll sich unsere Untersuchung vor allem mit Funktionen der folgenden Form befassen, die aus $\beta\gamma$ Gliedern bestehen:

$$r + Rr^{g^\alpha} + R^2 r^{g^{2\alpha}} + R^3 r^{g^{3\alpha}} \ldots + R^{\beta\gamma-1} r^{g^{\alpha\beta\gamma-\alpha}}$$

Der Kürze halber bezeichnen wir sie mit dem Zeichen $[r, R]$. Die einzelnen Glieder eines solchen Ausdrucks sind Produkte aus Potenzen von r und Potenzen von R; die Exponenten der ersteren bilden eine geometrische, die der letzteren eine arithmetische Folge. Die Exponenten

$$1, \quad g^\alpha, \quad g^{2\alpha}, \quad g^{3\alpha} \ldots\ldots g^{\alpha\beta\gamma-\alpha}$$

sind sämtlich zum Modul n inkongruent zueinander, also jene Potenzen von r voneinander verschieden; weiter fortgesetzt würden sie jedoch dieselbe Reihe erneut beginnen, da $g^{\alpha\beta\gamma} \equiv 1 (\mathrm{mod.}\, n)$ und daher $r^{g^{\alpha\beta\gamma}} = r$ ist. Die anderen Faktoren

$$1, \quad R, \quad R^2, \quad R^3 \ldots . R^{\beta\gamma-1}$$

bilden γ gleiche Perioden, da $R^\beta = 1$, $R^{\beta-1} = R$ usw. ist. Daraus folgt, dass sich die Funktion $[r, R]$ auch so darstellen lässt:

$$\begin{aligned}
&r + r^{g^{\alpha\beta}} + r^{g^{2\alpha\beta}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta}} \\
&+ R\big(r^{g^\alpha} + r^{g^{\alpha\beta+\alpha}} + r^{g^{2\alpha\beta+\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta+\alpha}}\big) \\
&+ R^2\big(r^{g^{2\alpha}} + r^{g^{\alpha\beta+2\alpha}} + r^{g^{2\alpha\beta+2\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta+2\alpha}}\big) \\
&+ \text{usw.} \\
&+ R^{\beta-1}\big(r^{g^{\alpha\beta-\alpha}} + r^{g^{2\alpha\beta-\alpha}} + r^{g^{3\alpha\beta-\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha}}\big).
\end{aligned}$$

oder, wenn wir das Zeichen aus Artikel 343 der Disq. Ar. einführen,

$$[r, R] = (\gamma, 1) + R(\gamma, g^\alpha) + R^2(\gamma, g^{2\alpha}) \ldots + R^{\beta-1}(\gamma, g^{\alpha\beta-\alpha})$$

3.

Nehmen wir für die Wurzel r die Einheit, so erhalten wir

$$[1, R] = 1 + R + R^2 + R^3 \ldots + R^{\beta\gamma-1} = \gamma(1 + R + R^2 + R^3 \ldots + R^{\beta-1})$$

mit dem Wert $= \beta\gamma$, wenn wir auch für R die Wurzel 1 nehmen, dagegen $= 0$ für jeden anderen Wert von R. Bleibt hingegen r unbestimmt und setzen wir $R = 1$, so ist $[r, 1] = r + r^{g^\alpha} + r^{g^{2\alpha}} + r^{g^{3\alpha}} \ldots + r^{g^{\alpha\beta\gamma-\alpha}}$ oder, mit dem in den Disq. Ar. eingeführten Zeichen, $[r, 1] = (\beta\gamma, 1)$; das heißt, der Ausdruck besteht aus einer Periode von $\beta\gamma$ Wurzeln, von denen eine r selbst ist. Ist $\alpha = 1$, so umfasst diese Periode sämtliche Wurzeln $r, r^2, r^3 \ldots r^{n-1}$, nur in anderer Reihenfolge.

Man beachte noch die folgenden Beziehungen, deren Grund unmittelbar ersichtlich ist:

$$[r, R] = R[r^{g^\alpha}, R] = R^2[r^{g^{2\alpha}}, R] \quad \text{oder allgemein} \quad = R^k[r^{g^{\alpha k}}, R]$$

wobei k eine beliebige positive ganze Zahl bezeichnet. Daraus folgt, dass die Funktion $[r^m, R]$ entweder $= [1, R]$ ist, nämlich wenn m durch n teilbar ist, oder sich in den übrigen Fällen auf die Form $R^\mu[r^{g^\nu}, R]$ mit $\nu < \alpha$ bringen lässt. Ist nämlich m nicht durch n teilbar, so ist es zum Modul n irgendeiner Potenz von g kongruent, deren Exponent sich wie in den Disq. Ar. zweckmäßig durch ind. m ausdrücken lässt; setzen wir also ind. $m = \lambda\alpha + \nu$, was offenbar so geschehen kann, dass $\nu < \alpha$ ist, so erhalten wir $[r^m, R] = [r^{g^{\lambda\alpha+\nu}}, R] = R^{-\lambda}[r^{g^\nu}, R]$. Daher ist $\mu = -\lambda$ zu setzen oder, wenn du einen positiven Exponenten wünschst, $\mu \equiv -\lambda (\mathrm{mod.}\ \beta)$.

4.

Satz. *Bezeichnet r' ebenso wie r eine beliebige Wurzel der Gleichung $x^n - 1 = 0$ und R' ebenso wie R eine beliebige Wurzel der Gleichung $x^\beta - 1 = 0$, so ist das Produkt*

$$\begin{aligned}&[r, R] \times [r', R'] = \\ &\quad [rr', RR'] + R[r^{g^\alpha} r', RR'] + R^2[r^{g^{2\alpha}} r', RR'] \\ &\quad + R^3[r^{g^{3\alpha}} r', RR'] \ldots + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}} r', RR']\end{aligned}$$

Beweis. Multipliziert man $[r, R]$ mit den einzelnen Gliedern von $[r', R']$, so lässt sich das Produkt in folgender Form darstellen:

$$\begin{aligned}&[r, R]r' + RR'[r^{g^\alpha}, R]r'^{g^\alpha} + R^2R'^2[r^{g^{2\alpha}}, R]r'^{g^{2\alpha}} \\ &+ R^3R'^3[r^{g^{3\alpha}}, R]r'^{g^{3\alpha}} \ldots \\ &+ R^{\beta\gamma-1}R'^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}}, R]r'^{g^{\alpha\beta\gamma-\alpha}}\end{aligned}$$

Fasst man dann die ersten Glieder der einzelnen, ordnungsgemäß entwickelten Teile zusammen, so ergibt sich $[rr', RR']$; sammelt man ebenso die zweiten Glieder, so entsteht $R[r^{g^\alpha} r', RR']$, und so weiter. Auf diese Weise erhält man schließlich die angegebene Form des Produkts. Q. E. D.

Ferner zeigt schon die Vertauschung von r, R mit r', R', dass sich dasselbe Produkt auch in folgende Form bringen lässt:

$$[rr', RR'] + R'[rr'^{g^\alpha}, RR'] + R'^2[rr'^{g^{2\alpha}}, RR']$$
$$+ R'^3[rr'^{g^{3\alpha}}, RR'] \ldots . + R'^{\beta\gamma-1}[rr'^{g^{\alpha\beta\gamma-\alpha}}, RR']$$

Daraus folgt weiter: Bezeichnen auch r'', r''' usw. beliebige Wurzeln der Gleichung $x^n - 1 = 0$ sowie R'', R''' usw. beliebige Wurzeln der Gleichung $x^\beta - 1 = 0$, so ist das Produkt der Funktionen $[r, R], [r', R'], [r'', R''], [r''', R''']$ usw., wie groß auch ihre Anzahl sein mag, gleich der Summe

$$\Sigma R'^{k'} R''^{k''} R'''^{k'''} \text{ usw.}$$

$$[rr'^{g^{\alpha k'}} r''^{g^{\alpha k''}} r'''^{g^{\alpha k'''}} \text{ usw.},\ RR'R''R''' \text{ usw.}]$$

wobei für k', k'', k''' usw. sämtliche Zahlen $0, 1, 2, 3 \ldots \beta\gamma - 1$ eingesetzt werden, die auf alle möglichen verschiedenen Arten miteinander kombiniert werden. Dadurch ergeben sich insgesamt $\beta^{\mu-1}\gamma^{\mu-1}$ Glieder, wenn μ die Anzahl jener miteinander multiplizierten Funktionen bezeichnet.

5.

Die Formel, mit der wir im vorigen Artikel das Produkt beliebig vieler Funktionen ausgedrückt haben, ist allgemein und setzt keinen Zusammenhang zwischen den Wurzeln r, r', r'', r''' usw. oder zwischen R, R', R'', R''' usw. voraus. Daraus lässt sich leicht ableiten: Dürfen die Wurzeln r', r'', r''' usw. als Potenzen von r und die Wurzeln R', R'', R''' usw. als Potenzen von R betrachtet werden, so hat jedes Glied des Produkts die Form $R^M[r^m, R^\lambda]$, wobei der Exponent λ für alle Glieder derselbe ist, nämlich $R^\lambda = RR'R''R'''$ usw. Nach dem, was wir in Artikel 3 bemerkt haben, lässt sich daher ein solches Produkt auf die folgende Form bringen:

$$A[1, R^\lambda] + B[r, R^\lambda] + B'[r^g, R^\lambda] + B''[r^{g^2}, R^\lambda] + B'''[r^{g^3}, R^\lambda] + \text{usw.}$$
$$+ B^{(\alpha-1)}[r^{g^{\alpha-1}}, R^\lambda]$$

Dabei haben die einzelnen Koeffizienten A, B, B', B'', B''' usw. die Form

$$h + h'R + h''R^2 + h'''R^3 + \text{usw.} + h^{(\beta-1)}R^{\beta-1}$$

und h, h', h'', h''' usw. bezeichnen bestimmte ganze Zahlen.

Der einfachste Fall ist der, in dem $r = r' = r'' = r'''$ usw. und auch $R = R' = R'' = R'''$ usw. gesetzt wird; dann geht unser Produkt in die Potenz $[r, R]^\lambda$ über, die sich daher stets auf die oben angegebene Form bringen lässt.

6.

Setzen wir also $\lambda = \beta$, so erhält die Potenz $[r, R]^\beta$ die Form

$$\begin{aligned} &A[1,1] + B[r,1] + B'[r^g,1] + \text{usw.} + B^{\alpha-1)}[r^{g^{\alpha-1}},1] \\ &= \beta\gamma A + B(\beta\gamma,1) + B'(\beta\gamma,g) + B''(\beta\gamma,g^2) + \text{usw.} \\ &\quad + B^{(\alpha-1)}(\beta\gamma,g^{\alpha-1}) = \theta' \end{aligned}$$

Werden also nicht nur der Wert der Wurzel R (und damit auch die Werte der Koeffizienten A, B, B' usw.), sondern auch die Werte der einzelnen Summen von $\beta\gamma$ Gliedern $(\beta\gamma,1), (\beta\gamma,g)$ usw. als bekannt vorausgesetzt, so ist der Wert von θ' unmittelbar bekannt, und daraus lässt sich $[r, R]$ durch die Formel $\sqrt[\beta]{\theta'}$ ermitteln. Dieser Ausdruck lässt β verschiedene Werte zu; daher könnte zweifelhaft erscheinen, welchen man nehmen soll. Man zeigt jedoch leicht, dass diese Wahl völlig beliebig ist, sofern R eine *eigentliche* Wurzel der Gleichung $x^\beta - 1 = 0$ ist. In diesem Fall sind nämlich jene β Werte des Wurzelausdrucks $\sqrt[\beta]{\theta'}$ offenbar

$$[r, R], \quad [r^{g^\alpha}, R], \quad [r^{g^{2\alpha}}, R] \ldots . [r^{g^{\alpha\beta-\alpha}}, R]$$

denn die Potenzen dieser Funktionen mit dem Exponenten β sind nach Artikel 3 einander gleich, während die Funktionen selbst zu den β verschiedenen Wurzeln der Gleichung $x^\beta - 1 = 0$ proportional sind. Solange aber nur die Summen von $\beta\gamma$ Gliedern $(\beta\gamma,1), (\beta\gamma,g)$ usw. bekannt sind, ist die Wurzel r selbst nur insofern bestimmt, als sie in der Menge $(\beta\gamma,1)$ enthalten sein muss; es bleibt beliebig, welche Wurzel aus dieser Menge wir für r nehmen. Diese Wurzeln sind $r, r^{g^\alpha}, r^{g^{2\alpha}}$ usw., und daher können wir auch von den Funktionen $[r, R], [r^{g^\alpha}, R], [r^{g^{2\alpha}}, R]$ usw. eine beliebige für $[r, R]$ nehmen.

Diese Schlüsse würden nicht gelten, wenn R keine eigentliche Wurzel der Gleichung $x^\beta - 1 = 0$ wäre. Nimmt man nämlich an, dass R eine eigentliche Wurzel der Gleichung $x^{\beta'} - 1 = 0$ und β' ein Teiler von β ist, so ergibt sich leicht

$$[r, R] = [r^{g^{\alpha\beta'}}, R], \quad [r^{g^\alpha}, R] = [r^{g^{\alpha\beta'+\alpha}}, R] \text{ usw.}$$

Daher kommen in der Menge der β Funktionen $[r, R], [r^{g^\alpha}, R] \ldots [r^{g^{\alpha\beta-\alpha}}, R]$ nur β' verschiedene vor; folglich sind auch von den Werten des Ausdrucks $\sqrt[\beta]{\theta'}$ nicht mehr als β' zulässig, die übrigen $\beta - \beta'$ dagegen unzulässig. Man sieht aber leicht, dass man in diesem Fall nicht bis zur Potenz mit dem Exponenten β der Funktion $[r, R]$ aufsteigen muss, sondern dass sich bereits die Potenz $[r, R]^{\beta'}$ auf unsere Form

$$\beta\gamma A + B(\beta\gamma,1) + B'(\beta\gamma,g) + B''(\beta\gamma,g^2) \text{ usw.}$$

bringen lässt. Wir erhalten somit $[r, R]$ durch einen Ausdruck wie $\sqrt[\beta']{\theta}$, und es ist gleichgültig, welchen Wert dieses Ausdrucks wir nehmen.

7.

Ebenso wie $[r, R]$ lassen sich auch die Funktionen $[r, R^2]$, $[r, R^3]$ usw. oder allgemein $[r, R^k]$ bestimmen. Nimmt man nämlich an, dass in θ' anstelle von R die Potenzen R^2, R^3 usw. R^k eingesetzt werden und dadurch die Funktionen θ'', θ''' usw. $\theta^{(k)}$ entstehen, so ist offenbar $[r, R^2]^\beta = \theta''$, $[r, R^3]^\beta = \theta'''$ usw. und allgemein $[r, R^k]^\beta = \theta^{(k)}$; daher können auch diese Funktionen durch Wurzelausdrücke dargestellt werden, $[r, R^2] = \sqrt[\beta]{\theta''}$ usw. Es ist jedoch nicht zweckmäßig, diese Wurzelausdrücke zu verwenden, wenn eine Größe durch eine Funktion von $[r, R]$, $[r, R^2]$ usw. ausgedrückt werden soll. Da nämlich ihre einzelnen Werte nicht vollständig bestimmt sind, bliebe zweifelhaft, welche man miteinander kombinieren dürfte; offenbar ist dies aber keineswegs beliebig. Man sieht leicht, dass, sobald für $[r, R]$ ein bestimmter Wert genommen wird, auch sämtliche $[r, R^2]$, $[r, R^3]$ usw. vollständig bestimmte Werte erhalten müssen, die jedoch durch die Wurzelausdrücke nicht angegeben werden. Diese sind daher beiseitezusetzen und andere Ausdrücke zu suchen, mit deren Hilfe $[r, R^2]$, $[r, R^3]$ usw. *rational* durch $[r, R]$ und bekannte Größen dargestellt werden. Dies erreichen wir leicht auf folgende Weise.

Nach dem Satz aus Artikel 4 und dem, was wir in Artikel 5 gezeigt haben, lässt sich auch das Produkt $[r, R^k] \times [r, R]^{\beta-k}$ auf eine Form wie

$$\begin{aligned}&\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \text{usw.}\\ &\quad + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1})\end{aligned}$$

bringen, wobei A, B, B', B'' usw. rationale Funktionen von R sind. Setzen wir also die Produkte

$$\begin{aligned}[r, R^2] \times [r, R]^{\beta-2} &= \vartheta''\\ [r, R^3] \times [r, R]^{\beta-3} &= \vartheta'''\\ [r, R^4] \times [r, R]^{\beta-4} &= \beta''''\\ &\text{usw.}\end{aligned}$$

so sind auch $\vartheta'', \vartheta''', \vartheta''''$ usw. rational bestimmbare Größen, und es gilt

$$\begin{aligned}[r, R^2] &= \frac{\vartheta''}{\theta'}[r, R]^2\\ [r, R^3] &= \frac{\vartheta'''}{\theta'}[r, R]^3\\ [r, R^4] &= \frac{\vartheta''''}{\theta'}[r, R]^4\\ &\text{usw.}\end{aligned}$$

Diese Ausdrücke stellen somit die Werte der Funktionen $[r, R^2]$, $[r, R^3]$ usw. rational dar, sofern nicht $[r.R] = 0$ ist; gälte diese Gleichheit, so würden sie unbestimmt. Wir können aber streng beweisen, dass $[r, R] = 0$ niemals eintreten kann, sofern r eine von 1 verschiedene Wurzel bezeichnet, auch wenn wir uns die Darlegung dieses Beweises für eine andere Gelegenheit vorbehalten müssen, um hier nicht zu ausführlich zu werden.

8.

Was wir in den vorigen Artikeln dargelegt haben, ist nützlich, wenn wir von Perioden mit $\beta\gamma$ Gliedern zu Perioden mit γ Gliedern absteigen wollen. Man sieht nämlich leicht, dass, wenn R eine eigentliche Wurzel bezeichnet, gilt:

$$\begin{aligned}
\beta(\gamma, 1) &= (\beta\gamma, 1) + [r, R] + [r, R^2] + [r, R^3] + \text{usw.} + [r, R^{\beta-1}] \\
\beta(\gamma, g^\alpha) &= (\beta\gamma, 1) + R^{\beta-1}[r, R] + R^{\beta-2}[r, R^2] \\
&\qquad + R^{\beta-3}[r, R^3] + \text{usw.} + R[r, R^{\beta-1}] \\
\beta(\gamma, g^{2\alpha}) &= (\beta\gamma, 1) + R^{2\beta-2}[r, R] + R^{2\beta-4}[r, R^2] \\
&\qquad + R^{2\beta-6}[r, R^3] + \text{usw.} + R^2[r, R^{\beta-1}] \\
&\text{usw.}
\end{aligned}$$

Nähme man hier für die einzelnen $[r, R]$, $[r, R^2]$ usw. die Wurzelausdrücke $\sqrt[\beta]{\theta'}$, $\sqrt[\beta]{\theta''}$ usw., so wäre der Wert jeder Reihe unter $\beta^{\beta-1}$ Werten zweifelhaft. Nimmt man dagegen für $[r, R^2]$ usw. die rationalen Ausdrücke, so ist er keiner anderen Mehrdeutigkeit unterworfen als derjenigen, die der Natur der Sache nach unvermeidlich ist. Diese Bemerkung scheint der Aufmerksamkeit des berühmten LAGRANGE entgangen zu sein, der glaubte, unsere in den Disquis. arithm. Artikel 360 angegebene Methode *vereinfacht* zu haben, indem er jene Wurzelausdrücke anstelle der rationalen Ausdrücke einsetzte; dabei hatten wir dort die Wurzelausdrücke mit Bedacht übergangen und nur rationale Ausdrücke angegeben (Traité de la résolution numérique des équations; Ausgabe 2, S. 311).

Ferner muss hier kaum darauf hingewiesen werden, dass, sobald die Werte der Perioden $(\gamma, 1)$, (γ, g^α) usw. oder auch nur einer von ihnen ermittelt sind, die Werte aller übrigen Perioden mit γ Gliedern rational daraus abgeleitet werden können. Der Abstieg von Perioden mit $\beta\gamma$ Gliedern zu Perioden mit γ Gliedern erfordert somit die Lösung der Gleichungen $x^\beta = 1$, $x^\beta = \theta'$; die übrigen Operationen werden rational ausgeführt.

9.

All dies war bereits in den Disquis. Ar. auf nahezu dieselbe Weise behandelt worden; einiges war dort jedoch ohne Beweis hinzugefügt worden, den wir hier nachzutragen für zweckmäßig halten. Wir haben dort angekündigt, dass die Bestimmung des Wertes der Wurzelgröße $\sqrt[\beta]{\theta'}$, die, da θ' eine imaginäre Größe ist, die Teilung sowohl eines Verhältnisses als auch eines Winkels in β Teile zu erfordern scheint, nur von der letzteren abhängt und dass die erstere stets auf das Ziehen einer einzigen Quadratwurzel zurückgeführt werden kann. Dies beweisen wir wie folgt.

Bezeichnen wir wie oben die imaginäre Größe $\sqrt{-1}$ mit i und schreiben $\theta' = P + iQ$ sowie $\sqrt[\beta]{\theta'} = p + iq$, wobei für die Wurzelgröße ein beliebiger Wert gewählt ist und P, Q, p, q reell sind, so ist bekannt: Werden die positiven Größen E, e und die Winkel F, f so bestimmt, dass $P = E\cos F$, $Q = E\sin F$, $p = e\cos f$, $q = e\sin f$ ist, so gilt $e = \sqrt[\beta]{E}$, und f ist gleich einem der Winkel

$$\frac{1}{\beta}F, \quad \frac{1}{\beta}(F + 360^0), \quad \frac{1}{\beta}(F + 720^0) \ldots . \frac{1}{\beta}(F + (\beta - 1)360^0)$$

Somit wird f· ger durch Teilung des Winkels F in β Teile bestimmt; das Ziehen der Wurzel $\sqrt[\beta]{E}$ können wir jedoch auf folgende Weise vermeiden. Jedes Produkt $r^k R^K$ hat denselben reellen Teil wie $r^{-k}R^{-K}$, während die imaginären, den Faktor i enthaltenden Teile in diesen Produkten gleich, aber entgegengesetzt sind. Daraus folgt unmittelbar $[r^{-1}, R^{-1}] = p - iq = e(\cos f - i\sin f)$ und daher

$$[r, R] \times [r^{-1}, R^{-1}] = e^2$$

Nach dem Satz aus Artikel 4 wird jenes Produkt jedoch

$$\begin{aligned} &= [1,1] + R[r^{g^\alpha - 1}, 1] + R^2[r^{g^{2\alpha}-1}, 1] + \text{usw.} \\ &\quad + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}-1}, 1] \\ &= \beta\gamma + R(\beta\gamma, g^\alpha - 1) + R^2(\beta\gamma, g^{2\alpha} - 1) + \text{usw.} \\ &\quad + R^{\beta\gamma-1}(\beta\gamma, g^{\alpha\beta\gamma-\alpha} - 1) \end{aligned}$$

Diese Größe lässt sich bestimmen, wenn R und sämtliche Perioden mit $\beta\gamma$ Gliedern als bekannt vorausgesetzt werden. Die Bestimmung von e verlangt somit nur das Ziehen einer Quadratwurzel.

Im besonderen Fall $\alpha = 1$ sind die einzelnen Perioden $(\beta\gamma, g^\alpha - 1)$, $(\beta\gamma, g^{2\alpha} - 1)$ usw. offenbar $= r + r^2 + r^3 + r^4 + \text{usw.} + r^{n-1}$, und daher

$$\begin{aligned} ee &= \beta\gamma + (R + R^2 + R^3 + \text{usw.} + R^{\beta\gamma-1})(r + r^2 + r^3 + \text{usw.} + r^{n-1}) \\ &= \beta\gamma + 1 = n \end{aligned}$$

sofern r und R als von 1 verschiedene Wurzeln vorausgesetzt werden; folglich gilt stets $e = \sqrt{n}$ (Disq. arithm., Artikel 360 am Ende).

10.

Bisher haben wir unsere Untersuchung in größter Allgemeinheit geführt, sodass sie beliebige Werte der Zahlen α, β, γ umfasst; von nun an gehen wir jedoch zu dem eingeschränkteren Fall $\alpha = 1$ über, der uns den Weg zu überaus fruchtbaren und eleganten Untersuchungen eröffnen wird. Das Zeichen $[r, R]$ bezeichne also die Funktion

$$r + Rr^g + R^2 r^{g^2} + R^3 r^{g^3} + \text{usw.} + R^{n-2} r^{g^{n-2}}$$

Dabei ist n eine Primzahl, r eine beliebige Wurzel der Gleichung $x^n - 1 = 0$ (die Wurzel 1 nicht ausgenommen), R eine beliebige Wurzel der Gleichung $x^\beta - 1 = 0$, wobei β einen gegebenen Teiler von $n-1$ bezeichnet, und schließlich g eine ganze Zahl, die eine fest gewählte primitive Wurzel zum Modul n ist. Ferner schreiben wir der Kürze halber

$$1 + r + r^2 + r^3 + \text{usw.} + r^{n-1} = s$$
$$1 + R + R^2 + R^3 + \text{usw.} + R^{n-2} = S$$

Daraus folgt offenbar, dass s den Wert $= n$ für $r = 1$ annimmt, dagegen $s = 0$ für jeden anderen Wert von r; ebenso gilt $S = n - 1$ für $R = 1$, dagegen $S = 0$ für jeden anderen Wert von R.

Nach Artikel 3 haben wir daher $[1, R] = S$, $[r, 1] = s - 1$; ferner gilt für jeden ganzzahligen Wert von m, der nicht durch n teilbar ist, $[r^m, R] = R^{-\operatorname{ind} m}[r, R]$ oder allgemeiner $[r^m, R^M] = R^{-M \operatorname{ind} m}[r, R^M]$, wobei $\operatorname{ind} m$ der Exponent der Potenz der Zahl g ist, die zum Modul n der Zahl m kongruent ist. Wenden wir diese Transformation auf das an, was wir in Artikel 5 gezeigt haben, so folgt, dass sich das Produkt zweier oder mehrerer solcher Funktionen $[r^h, R^H]$ auf die Form

$$A[1, R^\lambda] + B[r, R^\lambda]$$

bringen lässt. Dabei sind A und B rationale Funktionen von R mit ganzzahligen Koeffizienten, und λ ist die Summe aller Werte von H. Es wird von großer Bedeutung sein, solche Transformationen auf einen handlichen Algorithmus zurückzuführen; dazu müssen wir vor allem die Beschaffenheit des Produkts zweier Funktionen näher betrachten.

11.

Das Produkt $[r, R^\mu] \times [r, R^\nu]$ wird nach dem Satz aus Artikel 4 =

$$[r^2, R^{\mu+\nu}] + R^\mu[r^{g+1}, R^{\mu+\nu}] + R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] + R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] + \text{usw.} + R^{(n-2)\mu}[r^{g^{n-2}+1}, R^{\mu+\nu}]$$

Unter den $n-1$ Exponenten $2, g+1, g^2+1, g^3+1$ usw. $g^{n-2}+1$ ist nur einer durch n teilbar, nämlich $g^{\frac{1}{2}(n-1)}+1$; das entsprechende Glied unserer Summe ist daher $R^{\frac{1}{2}(n-1)\mu}[1, R^{\mu+\nu}]$. Dieses Glied ist $= 0$, sofern nicht $R^{\mu+\nu} = 1$ ist, und $= (n-1)R^{\frac{1}{2}(n-1)\mu} = \pm(n-1)$ für $R^{\mu+\nu} = 1$. Die übrigen Teile unserer Summe, deren Summe wir $= \Omega$ setzen, werden auf folgende Weise umgeformt:

$$\begin{aligned}
[r^2, R^{\mu+\nu}] &= R^{-(\mu+\nu)\operatorname{ind} 2}[r, R^{\mu+\nu}] \\
R^\mu[r^{g+1}, R^{\mu+\nu}] &= R^{\mu-(\mu+\nu)\operatorname{ind}(g+1)}[r, R^{\mu+\nu}] \\
R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] &= R^{2\mu-(\mu+\nu)\operatorname{ind}(g^2+1)}[r, R^{\mu+\nu}] \\
R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] &= R^{3\mu-(\mu+\nu)\operatorname{ind}(g^3+1)}[r.R^{\mu+\nu}] \\
&\text{usw.}
\end{aligned}$$

Daraus erhalten wir

$$\text{I.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind} x-(\mu+\nu)\operatorname{ind}(x+1)}$$

wenn für x der Reihe nach die Werte $1, g, g^2, g^3 \ldots . g^{n-2}$ mit Ausnahme von $g^{\frac{1}{2}(n-1)}$ eingesetzt werden oder, was offenbar auf dasselbe hinausläuft, wenn wir für x die Werte $1, 2, 3, 4 \ldots . n-2$ einsetzen, da diese Werte jenen zum Modul n, wenn auch in anderer Reihenfolge, kongruent sind.

Nehmen wir die ganze Zahl y zu x invers zum Modul n, also so bestimmt, dass $xy \equiv 1 \pmod{n}$ gilt, so ist $\operatorname{ind} x \equiv -\operatorname{ind} y \pmod{n-1}$ und $\operatorname{ind}(x+1) + \operatorname{ind} y \equiv \operatorname{ind}(xy+y) \equiv \operatorname{ind}(1+y) \pmod{n-1}$; daraus ergibt sich

$$\begin{aligned}
\mu \operatorname{ind} x - (\mu+\nu)\operatorname{ind}(x+1) &\equiv -\mu \operatorname{ind} y - (\mu+\nu)\{\operatorname{ind}(y+1) - \operatorname{ind} y\} \\
&\equiv \nu \operatorname{ind} y - (\mu+\nu)\operatorname{ind}(y+1)
\end{aligned}$$

Da nun die zu $1, 2, 3 \ldots n-2$ inversen Zahlen mit diesen selbst übereinstimmen und nur ihre Reihenfolge geändert ist, gilt auch

$$\text{II.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\nu \operatorname{ind} y-(\mu+\nu)\operatorname{ind}(y+1)}$$

wobei für y der Reihe nach die Zahlen $1, 2, 3 \ldots n-2$ eingesetzt werden. Dieselbe Formel folgt unmittelbar aus I, da sich die Zahlen μ, ν offenbar miteinander vertauschen lassen.

Nehmen wir schließlich die ganze Zahl z zu $x+1$ invers zum Modul n, also $xz+z \equiv 1 \pmod{n}$, so gilt $\operatorname{ind}(1-z) \equiv \operatorname{ind} x + \operatorname{ind} z \pmod{n-1}$, $\operatorname{ind}(x+1) \equiv -\operatorname{ind} z \pmod{n-1}$ und daher

$$\begin{aligned}\mu \operatorname{ind} x - (\mu+\nu)\operatorname{ind}(x+1) &\equiv \mu(\operatorname{ind}(1-z) - \operatorname{ind} z) + (\mu+\nu)\operatorname{ind} z \\ &\equiv \mu \operatorname{ind}(1-z) + \nu \operatorname{ind} z\end{aligned}$$

Da folglich, wenn x die Werte $1, 2, 3 \ldots n-2$ durchläuft, die Zahl z die Werte $2, 3, 4 \ldots n-1$, wenn auch in anderer Reihenfolge, durchlaufen muss, erhalten wir den dritten Ausdruck

$$\text{III.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(1-z)+\nu \operatorname{ind} z}$$

wobei für z der Reihe nach die Werte $2, 3, 4 \ldots n-1$ eingesetzt werden, oder, wenn du es vorziehst,

$$\begin{aligned}\text{IV.} \qquad \Omega &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(n+1-z)+\nu \operatorname{ind} z} \\ &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind} z+\nu \operatorname{ind}(n+1-z)}\end{aligned}$$

Da $\operatorname{ind}(1-z) = \frac{1}{2}(n-1) + \operatorname{ind}(z-1)$ gilt, lässt sich unser Produkt auch so darstellen:

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] &= R^{\frac{1}{2}(n-1)\mu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(z-1)+\nu \operatorname{ind} z}\} \\ &= R^{\frac{1}{2}(n-1)\nu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind} z+\nu \operatorname{ind}(z-1)}\}\end{aligned}$$

Dabei sind für z stets die Werte $2, 3, 4 \ldots . n-1$ einzusetzen.

Ferner können in allen diesen Formeln die Zahlen

$$\mu \operatorname{ind} x - (\mu+\nu)\operatorname{ind}(x+1), \quad \nu \operatorname{ind} y - (\mu+\nu)\operatorname{ind}(y+1), \quad \mu \operatorname{ind}(1-z) + \nu \operatorname{ind} z$$

usw. offenbar durch ihre kleinsten Reste zum Modul β ersetzt werden.

Ist $\mu+\nu \equiv 0 \pmod{\beta}$, so gilt

$$\begin{aligned}[r, R^{\mu}][r, R^{\nu}] = (n-1)&R^{\frac{1}{2}(n-1)\mu} \\ &+ (r + r^2 + r^3 + \cdots + r^{n-1}) \\ &\times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(n-2)\mu} - R^{\frac{1}{2}(n-1)\mu})\end{aligned}$$

12.

Das Produkt $[1, R^\mu] \times [r, R^\nu]$ wird nach dem Satz aus Artikel 4

$$= [r, R^{\mu+\nu}] + R^\mu [r, R^{\mu+\nu}] + R^{2\mu} [r, R^{\mu+\nu}] + \text{usw.} + R^{(n-2)\mu} [r, R^{\mu+\nu}]$$
$$= [r, R^{\mu+\nu}] \times (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{usw.} + R^{(n-2)\mu})$$
$$= [r, R^{\mu+\nu}] \times \frac{n-1}{\beta} (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{usw.} + R^{(\beta-1)\mu})$$

Daraus entwickelt sich das Produkt $[1, R^\mu] \times [1, R^\nu]$ zu

$$\frac{n-1}{\beta} [1, R^{\mu+\nu}] \times (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{usw.} + R^{(\beta-1)\mu})$$

Nun lässt sich das Produkt $[r^m, R^\mu] \,.\, [r^{m'}, R^{\mu'}]$ allgemein ohne Schwierigkeit ermitteln. Denn es ist $[r^m, R^\mu] = R^{-\mu \operatorname{ind} m} [r, R^\mu]$ für einen Wert von m, der nicht durch n teilbar ist, und $= [1, R^\mu]$ für einen teilbaren Wert; und da eine ähnliche Transformation für den anderen Faktor $[n^{m'}, R^{\mu'}]$ gilt, führt die Multiplikation entweder auf die Aufgabe des vorigen Artikels oder auf die Fälle zurück, die wir in diesem Artikel betrachtet haben.

13.

Da wir nun gezeigt haben, wie sich ein Produkt aus zwei Faktoren entwickeln lässt, wird die Entwicklung eines Produkts aus mehr Faktoren keine Schwierigkeit bereiten. Ist das Produkt $[r, R^\mu] \times [r, R^\nu]$ auf die Form $A[1, R^{\mu+\nu}] + B[r, R^{\mu+\nu}]$ gebracht, so wird beim Hinzufügen eines dritten Faktors $[r, R^\pi]$ das Produkt offenbar $= C[1, R^{\mu+\nu+\pi}] + D[r, R^{\mu+\nu+\pi}]$, wenn wir

$$[r, R^{\mu+\nu}][r, R^\pi] = c[1, R^{\mu+\nu+\pi}] + d[r, R^{\mu+\nu+\pi}]$$

und

$$C = Bc$$
$$D = Bd + A\{1 + R^{\mu+\nu} + R^{2\mu+2\nu} + \text{usw.} + R^{(n-2)(\mu+\nu)}\}$$

setzen. Somit lässt sich $[r, R]^\lambda$ leicht auf die Form $A[1, R^\lambda] + B[r, R^\lambda]$ bringen.

Als Beispiel wollen wir die Potenzen der Funktion $[r, R]$ für $n = 11$, $\beta = 5$ entwickeln und dabei $g = 2$ setzen. Den Zahlen entsprechen dann die folgenden Indizes:

Zahlen	1.2.3.4.5.6.7.8.9.10
Indizes	0.1.8.2.4.9.7.3.6. 5

Zur Entwicklung des Quadrats $[r, R]^2$ nach Formel I aus Artikel 11 haben wir also

$$\mu = 1, \quad \nu = 1$$

Werte von x ...	1. 2.3.4. 5. 6.7. 8. 9
$\operatorname{ind} x$ ...	0. 1.8.2. 4. 9.7. 3. 6
$2 \operatorname{ind}(x+1)$ ...	2.16.4.8.18.14.6.12.10
Kleinste Reste von $\operatorname{ind} x - 2 \operatorname{ind}(x+1)$ zum Modul 5 ...	3. 0.4.4. 1. 0.1. 1. 1

woraus wir

$$\Omega = [r, R^2] \times \{2 + 4R + R^3 + 2R^4\}$$

und

$$1^0. \qquad [r, R]^2 = [1, R^2] + [r, R^2] \times \{2 + 4R + R^3 + 2R^4\}$$

herleiten. Derselbe Ausdruck ergibt sich aus Formel III aus Artikel 11, nämlich

Werte von z ...	2.3.4.5.6.7.8.9. 10
$\operatorname{ind} z$ ...	1.8.2.4.9.7.3.6. 5
$\operatorname{ind}(n+1-z)$ ...	5.6.3.7.9.4.2.8. 1
kleinste Reste von $\operatorname{ind} z + \operatorname{ind}(n+1-z)$ zum Modul 5 ...	1.4.0.1.3.1.0.4. 1

Auf ganz dieselbe Weise finden wir

$$2^0. \qquad [r, R^2] \,.\, [r, R] = [1, R^3] + [r, R^3] \times \{2 + R + 4R^2 + 2R^3\}$$
$$3^0. \qquad [r, R^3] \,.\, [r, R] = [1, R^4] + [r, R^4] \times \{2 + 4R + R^3 + 2R^4\}$$

Schließlich wird

$$4^0. \qquad [r, R^4] \,.\, [r, R] = [1, 1] + [r, 1] \times \{1 + 2R + 2R^2 + 2R^3 + 2R^4\}$$

Multiplizieren wir Gleichung 1^0 mit $[r, R]$ und setzen für $[r, R^2] \,.\, [r, R]$ seinen Wert aus 2^0 ein und verwenden außerdem

$$[1, R^2] \,.\, [r, R] = [r, R^3] \,.\, \{2 + 2R + 2R^2 + 2R^3 + 2R^4\}$$

so erhalten wir

$$\begin{aligned}[r, R]^3 = {} & [1, R^3] \times \{2 + 4R + R^3 + 2R^4\} \\ & + [r, R^3] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\}\end{aligned}$$

und ebenso

$$\begin{aligned}[r, R]^4 = {} & [1, R^4] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\} \\ & + [r, R^4] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ [r, R]^5 = {} & [1, 1] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ & + [r, 1] \times \{1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4\} \\ = {} & 1640 + 1700R + 2050R^2 + 1800R^3 + 1900R^4 \\ & + (1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4)(s - 1) \\ = {} & 918Ss - 98S - (6R + 41R^2 + 16R^3 + 26R^4)s \\ & + 66R + 451R^2 + 176R^3 + 286R^4\end{aligned}$$

14.

Die Rechnung in den vorhergehenden Artikeln' ist so durchgeführt, dass sie sich auf sämtliche Werte von r und R erstrecken lässt. Sie wird erheblich kürzer, wenn wir R von Anfang an als eigentliche Wurzel der Gleichung $x^\beta - 1 = 0$ betrachten. Unter dieser Voraussetzung lässt sich das Produkt $[r, R^\mu] \times [r, R^\nu]$ auf die Form $B[r, R^{\mu+\nu}]$ bringen, sofern $\mu + \nu$ nicht durch β teilbar ist; ist dagegen $\mu + \nu$ durch β teilbar, so wird jenes Produkt $= (n-1)R^{\frac{1}{2}(n-1)\mu} + [r, 1]\Sigma R^{\mu \operatorname{ind} x}$, wenn wir für $\operatorname{ind} x$ alle Zahlen $0, 1, 2, 3 \ldots . n-2$ mit Ausnahme von $\frac{1}{2}(n-1)$ einsetzen. Daraus folgt leicht, dass in diesem Fall, sofern μ und damit auch ν nicht durch β teilbar sind,

$$[r, R^\mu] \,.\, [r, R^\nu] = R^{\frac{1}{2}(n-1)\mu}\{n - 1 - [r, 1]\}$$

gilt, also $= 0$ für $r = 1$ und $= nR^{\frac{1}{2}(n-1)\mu}$ für jeden anderen Wert von r. Da ferner $R^{\frac{1}{2}(n-1)\mu}$ den Wert $= +1$ oder $= -1$ annimmt, je nachdem, ob $\frac{n-1}{\beta} \,.\, \mu$ gerade oder ungerade ist, wird unser Produkt im ersten Fall $= n$, im zweiten $= -n$.

Daraus folgt weiter, dass wir

$$\begin{aligned}[r,R]^2 &= A'[r,R^2]\\ [r,R^2]\,.\,[r,R] &= A''[r,R^3]\\ [r,R^3]\,.\,[r,R] &= A'''[r,R^4]\end{aligned}$$

setzen können, und so fort bis

$$[r,R^{\beta-2}]\,.\,[r,R] = A^{(\beta-2)}[r,R^{\beta-1}]$$

woraus sich

$$\begin{aligned}[r,R]^2 &= A'[r,R^2]\\ [r,R]^3 &= A'A''[r,R^3]\\ [r,R]^4 &= A'A''A'''[r,R^4]\end{aligned}$$

ergibt, und so fort. Schließlich gilt

$$[r,R]^\beta = \pm nA'A''A'''\ldots A^{(\beta-2)}$$

Dabei ist das obere oder das untere Vorzeichen zu wählen, je nachdem, ob $\frac{n-1}{\beta}$ gerade oder ungerade ist.

Ist der Wert von $[r,R]$ gefunden, so können die übrigen Funktionen

$$[r,R^2] = \frac{[r,R]^2}{A'}, \quad [r,R^3] = \frac{[r,R]^3}{A'A''} \quad \text{usw.}$$

hier also offenbar viel leichter bestimmt werden als in den Fällen, in denen die Bedingung $\alpha = 1$ nicht erfüllt ist, wie wir bereits in den *Disq. Ar.* (Artikel 360, III) angemerkt haben. Eine eingehendere Betrachtung der Natur der Funktionen A', A'' usw. erleichtert diese Operationen noch mehr.

15.

In Artikel 9 haben wir gezeigt, dass sich der Wert der Funktion $[r,R]$ auf die Form $\sqrt{n}(\cos f + i\sin f)$ bringen lässt; ebenso lassen sich die Funktionen $[r,R^2]$, $[r,R^3]$ usw. bis $[r,R^{\beta-1}]$ auf eine ähnliche Form bringen. Setzen wir

$$\begin{aligned}[r,R] &= \sqrt{n}(\cos f' + i\sin f')\\ [r,R^2] &= \sqrt{n}(\cos f'' + i\sin f'')\\ [r,R^3] &= \sqrt{n}(\cos f''' + i\sin f''')\\ &\text{usw.}\end{aligned}$$

so wird

$$\begin{aligned}A' &= \sqrt{n}(\cos(2f' - f'') + i\sin(2f' - f''))\\ A'' &= \sqrt{n}(\cos(f' + f'' - f''') + i\sin(f' + f'' - f'''))\\ A''' &= \sqrt{n}(\cos(f' + f''' - f'''') + i\sin(f' + f''' - f''''))\\ &\text{usw.}\end{aligned}$$

Daraus ist ersichtlich: Werden die Funktionen A', A'', A''' usw. auf die Formen

$$\begin{aligned} A' &= a'(\cos b' + i \sin b') \\ A'' &= a''(\cos b'' + i \sin b'') \\ A''' &= a'''(\cos b''' + i \sin b''') \\ &\text{usw.} \end{aligned}$$

gebracht, und zwar so, dass alle a', a'', a''' usw. positiv sind, so gilt

$$\begin{aligned} a' = a'' = a''' \text{ usw.} &= \sqrt{n} \\ f' &= \frac{1}{\beta}(b' + b'' + b''' + \text{usw.} + b^{(\beta-2)}) \end{aligned}$$

wenn $\frac{n-1}{\beta}$ gerade ist, oder

$$f' = \frac{1}{\beta}(180^0 + b' + b'' + \text{usw.} + b^{(\beta-2)})$$

wenn $\frac{n-1}{\beta}$ ungerade ist, und dann

$$\begin{aligned} [r, R] &= \sqrt{n}(\cos f' + i \sin f') \\ [r, R^2] &= \sqrt{n}(\cos(2f' - b') + i \sin(2f' - b')) \\ [r, R^3] &= \sqrt{n}(\cos(3f' - b' - b'') + i \sin(3f' - b' - b'')) \\ &\text{usw.} \end{aligned}$$

Schließlich gilt nach den Formeln aus Artikel 8

$$\begin{aligned} \left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&\cos f'' + \cos(2f' - b') + \cos(3f' - b' - b'') + \text{usw.} \\ &+ \cos((\beta-1)f' - b' - b'' - b''' - \text{usw.} - b^{(\beta-2)})\} \\ + \frac{i\sqrt{n}}{\beta}\{&\sin f' + \sin(2f' - b') + \sin(3f' - b' - b'') + \text{usw.}\} \end{aligned}$$

Ebenso ergeben sich die Werte der Funktionen $\left(\frac{n-1}{\beta}, g\right), \left(\frac{n-1}{\beta}, g^2\right), \left(\frac{n-1}{\beta}, g^3\right)$ usw., wenn wir in dieser Formel für f' der Reihe nach $f' - \frac{360^0 k}{\beta}$, $f' - 2\frac{360^0 k}{\beta}$, $f' - 3\frac{360^0 k}{\beta}$ usw. einsetzen und dabei $R = \cos\frac{360^0 k}{\beta} + i \sin\frac{360^0 k}{\beta}$ voraussetzen.

16.

Eine weitere Vereinfachung ergibt sich aus der folgenden Beobachtung. Da nach Artikel 14

$$\pm[r,R][r,R^{\beta-1}] = [r,R^2][r,R^{\beta-2}] = \pm[r,R^3][r,R^{\beta-3}] \text{ usw.} = n$$

gilt, wobei [im ersten, dritten usw. Produkt] das obere oder untere Vorzeichen zu wählen ist, je nachdem, ob $\frac{n-1}{\beta}$ gerade oder ungerade ist, muss im ersten Fall

$$\cos(f' + f^{(\beta-1)}) = \cos(f'' + f^{(\beta-2)}) = \cos(f''' + f^{(\beta-3)}) \text{ usw.} = 1$$

im zweiten

$$-\cos(f' + f^{(\beta-1)}) = \cos(f'' + f^{(\beta-2)}) = -\cos(f''' + f^{(\beta-3)}) \text{ usw.} = 1$$

und in beiden Fällen

$$\sin(f' + f^{(\beta-1)}) = \sin(f'' + f^{(\beta-2)}) = \sin(f''' + f^{(\beta-3)}) \text{ usw.} = 0$$

gelten. Daher dürfen wir im ersten Fall

$$f^{(\beta-1)} = -f', \quad f^{(\beta-2)} = -f'', \quad f^{(\beta-3)} = -f''' \quad \text{usw.}$$

im zweiten

$$f^{(\beta-1)} = 180^0 - f', \quad f^{(\beta-2)} = -f'', \quad f^{(\beta-3)} = 180^0 - f''' \quad \text{usw.}$$

setzen. Daraus folgt aber, dass im ersten Fall

$$b^{(\beta-2)} = b', \quad b^{(\beta-3)} = b'', \quad b^{(\beta-4)} = b''' \quad \text{usw.}$$
$$A^{(\beta-2)} = A', \quad A^{(\beta-3)} = A'', \quad A^{(\beta-4)} = A''' \quad \text{usw.}$$

im zweiten dagegen

$$b^{(\beta-2)} = b' - 180^0, \quad b^{(\beta-3)} = b'' + 180^0, \quad b^{(\beta-4)} = b''' - 180^0 \quad \text{usw.}$$
$$A^{(\beta-2)} = -A', \qquad A^{(\beta-3)} = -A'', \qquad A^{(\beta-4)} = -A''' \quad \text{usw.}$$

gilt, sodass sich die Anzahl der Funktionen A', A'', A''' usw. auf die Hälfte verringert. Daraus ergibt sich weiter im ersten Fall

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{usw.} + 2b^{(\frac{1}{2}\beta-1)})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos f' + 2\cos(2f' - b') \\ &+ 2\cos(3f' - b' - b'') + \text{usw.} \\ &+ 2\cos((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{8}\beta-2)}) \\ &+ \cos(\tfrac{1}{2}\beta f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-1)})\}\end{aligned}$$

(wobei das letzte Glied offenbar $= \cos 0 = 1$ ist) oder

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{usw.} + 2b^{(\frac{1}{2}(\beta-3))} + b^{(\frac{1}{2}(\beta-1))})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos f' + 2\cos(2f' - b') \\ &+ 2\cos(3f' - b' - b'') + \text{usw.} \\ &+ 2\cos(\tfrac{1}{2}(\beta - 1)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}(\beta-3))})\}\end{aligned}$$

je nachdem, ob β gerade oder ungerade ist; und im zweiten Fall

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{usw.} + 2b^{(\frac{1}{2}\beta-1)})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \text{usw.} \\ &+ 2\cos((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-3)}) \\ &+ \cos(\tfrac{1}{2}\beta f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-1)})\} \\ + i\frac{\sqrt{n}}{\beta}\{&2\sin f' + 2\sin(3f' - b' - b'') + \text{usw.} \\ &+ 2\sin((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-2)})\}\end{aligned}$$

oder

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{usw.} + 2b^{(\frac{1}{2}\beta-1)} + 180^0)$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \text{usw.}\\ &+ 2\cos((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-2)})\}\\ + i\frac{\sqrt{n}}{\beta}\{&2\sin f' + 2\sin(3f' - b' - b'') + \text{usw.}\\ &+ 2\sin((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-3)})\\ &+ \sin(\tfrac{1}{2}\beta f' - b' - b'' - \text{usw.} - b^{(\frac{1}{2}\beta-1)})\}\end{aligned}$$

je nachdem, ob $\frac{1}{2}\beta$ gerade oder ungerade ist. Für die übrigen Perioden mit $\frac{n-1}{\beta}$ Gliedern gilt dasselbe, was wir oben angemerkt haben. Allgemein folgt daraus also, dass zur Bestimmung dieser Perioden die Teilung des ganzen Kreises in β Teile erforderlich ist, von der die Konstruktion der Winkel b', b'', b''' usw. rational abhängt; ferner die Teilung des Winkels $b' + b'' + b''' + \text{usw.}$ in β Teile; schließlich die Quadratwurzel $\sqrt{n}$. Setzen wir sogleich $\beta = \frac{1}{2}(n-1)$, so stimmen jene Perioden offenbar mit den doppelten Kosinus der Winkel $\frac{360^0}{n}$, $2\frac{360^0}{n}$, $3\frac{360^0}{n}$ usw. bis $\frac{1}{2}(n-1)\frac{360^0}{n}$ überein. Daher hängt die Teilung des Kreises in n Teile von der Teilung des ganzen Kreises in $\frac{1}{2}(n-1)$ Teile ab, von der Teilung eines nach Ausführung jener Teilung konstruierbaren Winkels in $\frac{1}{2}(n-1)$ Teile und von der Wurzelgröße $\sqrt{n}$. Wollen wir bis zu den Sinus der Winkel $\frac{360^0}{n}$ usw. fortgehen, so ist eine weitere Operation nötig.

17.

Zur weiteren Verdeutlichung greifen wir das Beispiel aus Artikel 13 wieder auf, in dem wir

$$A' = A''' = 2 + 4R + R^3 + 2R^4 = 2R - 2R^2 - R^3$$
$$A'' = 2 + R + 4R^2 + 2R^3 = -R + 2R^2 - 2R^4$$

gefunden haben. Nehmen wir für R den Wert $\cos 72^0 + i \sin 72^0$, so wird

$$A' = A''' = 2\cos 72^0 - 3\cos 144^0 + i(2\sin 72^0 - \sin 144^0)$$
$$A'' = -3\cos 72^0 + 2\cos 144^0 + i(\sin 72^0 + 2\sin 144^0)$$

Die Winkel b', b'' werden daher durch die Gleichungen

$$1) \qquad \sin b' = \frac{2\sin 72^0 - \sin 144^0}{\sqrt{11}}$$
$$2) \qquad \cos b' = \frac{2\cos 72^0 - 3\cos 144^0}{\sqrt{11}}$$
$$3) \qquad \operatorname{tang} b' = \frac{2\sin 72^0 - \sin 144^0}{2\cos 72^0 - 3\cos 144^0}$$
$$4) \qquad \sin b'' = \frac{\sin 72^0 + 2\sin 144^0}{\sqrt{11}}$$
$$5) \qquad \cos b'' = \frac{-3\cos 72^0 + 2\cos 144^0}{\sqrt{11}}$$
$$6) \qquad \operatorname{tang} b'' = \frac{\sin 72^0 + 2\sin 144^0}{-3\cos 72^0 + 2\cos 144^0}$$

bestimmt. Jede der Gleichungen $1, 2, 3$ genügt, um den Winkel b' zu bestimmen, sofern der Quadrant bekannt ist, in dem er zu nehmen ist; dieser muss anhand der Vorzeichen der Größen $2\sin 72^0 - \sin 144^0$, $2\cos 72^0 - 3\cos 144^0$ bestimmt werden. Dasselbe gilt für den Winkel b''. In unserem Fall ist b' zwischen 0 und 90^0, b'' zwischen 90^0 und 180^0 zu nehmen. Multiplizieren wir Zähler und Nenner von Gleichung 3 mit $-3\cos 72^0 + 2\cos 144^0$, so geht sie in

$$\operatorname{tang} b' = \frac{2}{31}\{-\sin 72^0 + 13\sin 144^0\}$$

über. Ebenso ergibt sich aus Gleichung 6, wenn Zähler und Nenner mit $2\cos 72^0 - 3\cos 144^0$ multipliziert werden,

$$\operatorname{tang} b'' = \frac{2}{31}\{-13\sin 72^0 - \sin 144^0\}$$

In Zahlen erhalten wir daraus

$$\begin{aligned}\operatorname{tang} b' &= +0{,}4316226944, \quad \log\operatorname{tang} b' = 9{,}6351042715\\ b' &= 23^0 20' 46'' 04603\\ \operatorname{tang} b'' &= -0{,}8355819332, \quad \log\operatorname{tang} b'' = 9{,}9219890411\mathrm{n}\\ b'' &= 140^0 7' 6'' 52441\end{aligned}$$

woraus sich

$$5f' = 186^0 48' 38'' 61647, \qquad f' = 37^0 21' 43'' 723294$$

ergibt.

.Wir haben also

$$\begin{aligned}(2,1) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 37^0 21' 43'' 723294 + 2\cos 51^0 22' 41'' 400558\}\\ (2,2) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 325^0 21' 43'' 723294 + 2\cos 267^0 22' 41'' 400558\}\\ (2,4) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 253^0 21' 43'' 723294 + 2\cos 123^0 22' 41'' 400558\}\\ (2,8) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 181^0 21' 43'' 723294 + 2\cos 339^0 22' 41'' 400558\}\\ (2,5) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 109^0 21' 43'' 723294 + 2\cos 195^0 22' 41'' 400558\}\end{aligned}$$

woraus wir

$$\begin{array}{lcll}(2,1) & = & +1{,}6825070652 & = 2\cos\frac{360^0}{11}\\ (2,2) & = & +0{,}8308299 & = 2\cos\frac{720^0}{11}\\ (2,4) & = & & = 2\cos\frac{1440^0}{11}\\ (2,8) & = & & = 2\cos\frac{2880^0}{11}\\ (2,5) & = & & = 2\cos\frac{1800^0}{11}\end{array}$$

finden.

18.

Ein weiteres Beispiel liefert uns die Gleichung $x^{17} - 1 = 0$, die wir in den *Disquis. Arithm.* schon nach einer anderen Methode behandelt haben. Setzen wir also $n = 17$, $\beta = 8$, $g = 3$; dann entsprechen den Zahlen die folgenden Indizes:

Zahlen	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16
Indizes	0.	14.	1.	12.	5.	15.	11.	10.	2.	3.	7.	13.	4.	9.	6.	8

Daraus finden wir

$$A' = A''''' = 2R + 2R^2 + 3R^4 + 4R^5 + 2R^6 + 2R^7$$
$$A'' = A'''' = 2 + 3R + R^3 + R^4 + 3R^5 + 4R^6 + R^7$$
$$A''' = A'''' = 3 + 3R + 2R^2 + 3R^3 + R^5 + 2R^6 + R^7$$

oder, da in diesem Fall $R^4 + 1 = 0$ gilt,

$$A' = A''''' = -3 - 2R - 2R^3$$
$$A'' = A'''' = 1 - 4R^2$$
$$A''' = A'''' = 3 + 2R + 2R^3$$

Setzen wir also $R = \cos 45^0 + i \sin 45^0$, so wird

$$A' = A''''' = -3 - 2i\sqrt{2},$$
$$A'' = A'''' = 1 - 4i,$$
$$A''' = A'''' = 3 + 2i\sqrt{2}$$

Somit finden wir b', b'', b''' aus den Gleichungen

$$\sin b' = -\sqrt{\tfrac{8}{17}} \qquad \sin b'' = -\sqrt{\tfrac{16}{17}} \qquad \sin b''' = +\sqrt{\tfrac{8}{17}}$$
$$\cos b' = -\sqrt{\tfrac{9}{17}} \qquad \cos b'' = +\sqrt{\tfrac{1}{17}} \qquad \cos b''' = +\sqrt{\tfrac{9}{17}}$$
$$\operatorname{tang} b' = +\sqrt{\tfrac{8}{9}} \qquad \operatorname{tang} b'' = -4 \qquad \operatorname{tang} b''' = +\sqrt{\tfrac{8}{9}}$$

woraus wir

$$b' = 223^0 18' 49'', \quad b'' = 284^0 2' 10, \quad b''' = 43^0 18' 49'' = b' - 180^0$$
$$4f' = 550^0 39' 48'', \qquad f' = 137^0 39' 57''$$

$$(2,1) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 137^0 39'57'' + 2\cos 52^0 1'5'' + 2\cos 265^0 38'52'' + 1\}$$
$$(2,4) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 92^0 39'57'' + 2\cos 322^0 1'5'' + 2\cos 130^0 38'52'' - 1\}$$
$$(2,9) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 47^0 39'57'' + 2\cos 232^0 1'5'' + 2\cos 355^0 38'52'' + 1\}$$
$$(2,10) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 2^0 39'57'' + 2\cos 142^0 1'5'' + 2\cos 220^0 38'52'' - 1\}$$
$$(2,13) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 317^0 39'57'' + 2\cos 52^0 1'5'' + 2\cos 85^0 38'52'' + 1\}$$
$$(2,5) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 272^0 39'57'' + 2\cos 322^0 1'5'' + 2\cos 310^0 38'52'' - 1\}$$
$$(2,15) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 227^0 39'57'' + 2\cos 232^0 1'5'' + 2\cos 175^0 38'52'' + 1\}$$
$$(2,11) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 182^0 39'57'' + 2\cos 142^0 1'5'' + 2\cos 40^0 38'52'' - 1\}$$

herleiten.

$$\begin{array}{rcccl}
\frac{1}{2}(2,1) & = & +0{,}092268 & = & \cos\frac{4}{17}360^0 \\
\frac{1}{2}(2,3) & = & & = & \cos\frac{5}{17}360^0 \\
\frac{1}{2}(2,9) & = & & = & \cos\frac{2}{17}360^0 \\
\frac{1}{2}(2,10) & = & & = & \cos\frac{6}{17}360^0 \\
\frac{1}{2}(2,13) & = & +0{,}93247 & = & \cos\frac{1}{17}360^0 \\
\frac{1}{2}(2,5) & = & & = & \cos\frac{3}{17}360^0 \\
\frac{1}{2}(2,15) & = & & = & \cos\frac{8}{17}360^0 \\
\frac{1}{2}(2,11) & = & & = & \cos\frac{7}{17}360^0
\end{array}$$

* *

Von diesen allgemeineren Untersuchungen über die Funktionen $[r, R]$, welche die in Artikel 360 der *Disquiss. Ar.* begonnene zweite Theorie der reinen Gleichungen weiter verdeutlichen und erweitern, gehen wir zu einer genaueren Betrachtung gewisser besonderer Fälle über, nämlich solcher, in denen für β bestimmte Werte genommen werden. Daraus werden mehrere ebenso fruchtbare wie elegante Untersuchungen hervorgehen; einige davon waren zwar schon in den *Disq. Ar.* (Artikel . . .), jedoch nach einer anderen Methode, behandelt worden, andere sind dagegen als völlig neu anzusehen. Den bemerkenswerten Zusammenhang dieser Untersuchungen mit der höheren Arithmetik, die dadurch sehr große und bisher unerwartete Fortschritte macht, wollen wir in einer anderen, bald zu veröffentlichenden Abhandlung darlegen. — Ferner setzen wir in der gesamten folgenden Untersuchung voraus, dass für r eine *eigentliche* Wurzel der Gleichung $x^n - 1 = 0$ und für R eine eigentliche Wurzel der Gleichung $R^\beta - 1 = 0$ genommen wird.

19.

Wir beginnen mit dem Wert $\beta = 2$, wobei also für R der Wert -1 zu nehmen ist. Unsere Funktion $[r, R]$ wird daher

$$= r - r^g + r^{g^2} - r^{g^3} \ldots . - r^{g^{n-2}}$$

und es gilt

$$[r, R] = -[r^g, R] = +[r^{g^2}, R] = -[r^{g^3}, R] \quad \text{usw.}$$

Allgemein gilt, wenn λ eine beliebige, nicht durch n teilbare ganze Zahl bezeichnet,

$$[r^\lambda, R] = +[r, R] \quad \text{wenn } \lambda \text{ quadratischer Rest von } n \text{ ist,}$$
$$[r^\lambda, R] = -[r, R] \quad \text{wenn } \lambda \text{ quadratischer Nichtrest von } n \text{ ist.}$$

Bezeichnen wir ferner die quadratischen Reste von n, die unter $1, 2, 3 \ldots n-1$ enthalten sind, unbestimmt mit a und die Nichtreste von n innerhalb derselben Grenzen mit b, so sind offenbar die Zahlen

$$1, g^2, g^4 \ldots . g^{n-3}$$

ohne Rücksicht auf ihre Reihenfolge zum Modul n den Zahlen a kongruent, und ebenso die Zahlen

$$g, g^3, g^5 \ldots . g^{n-2}$$

den Zahlen b, sodass $[r, R] = \Sigma r^a - \Sigma r^b$ wird.

Setzen wir also $\frac{360^0}{n} = \omega$ und $r = \cos k\omega + i \sin k\omega$, so wird $[r, R] = \Sigma \cos ak\omega - \Sigma \cos bk\omega + i\Sigma \sin ak\omega - i\Sigma \sin bk\omega$. Nach Artikel 14 ist das Quadrat der Funktion $[r, R]$ gleich $= +n$ oder $= -n$, je nachdem, ob n von der Form $4z+1$ oder $4z-1$ ist; somit gilt im ersten Fall $[r, R] = \pm\sqrt{n}$, im zweiten $[r.R] = \pm i\sqrt{n}$. Das der Wurzelgröße vorangestellte Vorzeichen bleibt jedoch mehrdeutig. Daraus ergeben sich die folgenden Summen:

I. Ist n von der Form $4z + 1$, so gilt

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = \pm\sqrt{n}$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = 0$$

II. Ist n von der Form $4z - 1$, so gilt

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = 0$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = \pm\sqrt{n}$$

Da ferner die Gesamtheit der Zahlen a, b offenbar mit $1, 2, 3 \ldots n-1$ übereinstimmt, gilt $\Sigma r^a + \Sigma r^b = r + r^2 + r^3 + \text{usw.} + r^{n-1} = -1$, und damit $\Sigma \cos ak\omega + \Sigma \cos bk\omega = -1$, $\Sigma \sin ak\omega + \Sigma \sin bk\omega = 0$. Aus diesen und den vorigen Summen folgen die nachstehenden:

I. Für den ersten Fall

$$\Sigma \cos ak\omega = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin ak\omega = \Sigma \sin bk\omega = 0$$

II. Für den zweiten Fall

$$\Sigma \cos ak\omega = \Sigma \cos bk\omega = -\tfrac{1}{2}$$
$$\Sigma \sin ak\omega = \pm\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin bk\omega = \mp\tfrac{1}{2}\sqrt{n}$$

Diese Summen wurden bereits in den *Disquiss. Arr.*, Artikel 356, nach einer nicht sehr verschiedenen Methode hergeleitet; keine der beiden Methoden kann jedoch die Mehrdeutigkeit des der Wurzelgröße voranzustellenden Vorzeichens beseitigen. Diesen Mangel haben wir aber vor Kurzem in einer besonderen Abhandlung behoben, in der bewiesen wurde, dass für den Wert $k = 1$ in allen angeführten Formeln die oberen Vorzeichen zu nehmen sind.

Bemerkungen.

Aus der ursprünglichen Fortsetzung dieser Abhandlung von Artikel 19 an, die der Behandlung besonderer Fälle gewidmet war, sind nur noch einige Artikel erhalten. Sie befassen sich mit der quadratischen Gleichung, deren Wurzeln die beiden Perioden mit $\frac{n-1}{2}$ Gliedern sind; das Manuskript bricht zu Beginn der Untersuchung ab, durch die das Vorzeichen der bei ihrer Lösung auftretenden Quadratwurzel bestimmt werden sollte. Die Übereinstimmung dieses noch erhaltenen Anfangs mit der Abhandlung Summatio quarumdam serierum singularium zeigt, dass der Verfasser seinen Plan änderte, um die eben genannte Bestimmung des Vorzeichens zum Gegenstand einer besonderen Abhandlung zu machen. Vergleicht man damit das Zitat in Artikel 8, wo im Manuskript versehentlich die dritte statt der zweiten Ausgabe des Werkes von Lagrange angegeben war, so ergibt sich, dass diese Handschrift aus dem Jahr 1808 stammt. Dass die Veröffentlichung des Vorangehenden nicht aufgegeben worden war, zeigt ein bei Artikel 19 offenbar später eingefügtes Blatt, auf dem eine andere Fortsetzung beginnt und hinsichtlich der Bestimmung des Vorzeichens bereits auf die Abhandlung Summatio usw. verwiesen wird. Diese zweite Fortsetzung, die aber ebenfalls bald abbricht, ist hier wiedergegeben. Der Text des durchweg druckfertigen Manuskripts wurde bei der Herausgabe getreu beibehalten; nur in Artikel 16 mussten die Formeln für den zweiten Fall hinzugefügt werden.

R. Dedekind.

BEWEIS EINIGER SÄTZE ÜBER DIE PERIODEN DER KLASSEN BINÄRER QUADRATISCHER FORMEN.

Satz. I. *Die Anzahl der (eigentlich primitiven) Klassen derselben Determinante, die, zur P-ten Potenz erhoben, wobei P entweder eine Primzahl oder eine Primzahlpotenz $= p^\pi$ ist, die Hauptklasse K ergeben, ist entweder gleich* 1 *oder gleich einer Potenz derselben Primzahl p.*

Beweis. Es sei $(\mathfrak{Q})$ die ganze Gruppe aller in Betracht kommenden Klassen und n ihre Anzahl. Da die Hauptklasse K notwendig in $(\mathfrak{Q})$ enthalten ist, ist der Satz evident, wenn sie die einzige darin ist. Gibt es aber noch andere, so wird die Anzahl der in der Periode jeder von ihnen enthaltenen Klassen eine Potenz von p sein; es sei eine von ihnen A, und wir nehmen an, ihre Periode $(\mathfrak{A})$ enthalte p^α Klassen, die sämtlich in $(\mathfrak{Q})$ enthalten sein werden. Erschöpfen nun die Klassen dieser Periode $(\mathfrak{A})$ die Gruppe $(\mathfrak{Q})$, so gilt $p^\alpha = n$, und der Satz ist bewiesen; andernfalls sei B eine beliebige Klasse von $(\mathfrak{Q})$, die nicht in $(\mathfrak{A})$ enthalten ist, und wir nehmen an, ihre Periode werde so weit entwickelt, bis wir zu einer Klasse bB gelangen, die zugleich unter den Klassen von $(\mathfrak{A})$ vorkommt. Dies muss notwendig eintreten, weil zumindest die Hauptklasse dieser Periode und $(\mathfrak{A})$ gemeinsam ist. Nehmen wir nun an, bB sei die *erste* Klasse in der Periode von B, die $(\mathfrak{A})$ gemeinsam ist, oder b sei so klein wie möglich, so behaupte ich

1^0. Dass b eine Potenz von p sein wird. Denn offenbar erhalten wir, wenn wir $b = p^\beta h$, $bB = iA$ und $hk \equiv 1 \pmod{p^\pi}$ setzen (was möglich sein wird), $kbB = p^\beta hkB = p^\beta B = ikA$, das heißt, auch $p^\beta B$ wird unter den Klassen von $(\mathfrak{A})$ vorkommen, woraus folgt, dass $h = 1$ und $b = p^\beta$ gilt.

2^0. Dass, wenn wir die Klassen $K, B, 2B \ldots (b-1)B$ mit $(\mathfrak{B})$ bezeichnen, sämtliche Kompositionen einer Klasse von $(\mathfrak{A})$ mit einer Klasse von $(\mathfrak{B})$ zusammen $p^{\alpha+\beta}$ verschiedene Klassen ergeben. Denn nehmen wir $mA + nB = m'A + n'B$ und $n = n'$ an, so gilt notwendig $m = m'$; ist $n > n'$, so gilt $(n - n')B = (m' - m)A$, was unmöglich ist, wenn nicht $n = n'$ gilt.

3^0. Dass diese $p^{\alpha+\beta}$ verschiedenen Klassen in $(\mathfrak{Q})$ enthalten sein werden, was evident ist.

Erschöpfen nun diese $p^{\alpha+\beta}$ Klassen die Gruppe $(\mathfrak{Q})$, so ist der Satz bewiesen; andernfalls wählen wir eine weitere Klasse von $(\mathfrak{Q})$, die nicht unter ihnen enthalten ist, nämlich C; wir setzen ihre Periode so weit fort, bis wir zu einer Klasse gelangen, die bereits unter den aus $(\mathfrak{A})$ und $(\mathfrak{B})$ zusammengesetzten Klassen enthalten ist. Durch eine ähnliche Schlussweise wie zuvor werden wir beweisen, dass der Exponent dieser Klasse eine Potenz von p, $= p^\gamma$, sein muss und dass die Komposition der ersten p^γ Klassen der Periode von C mit den bereits gefundenen $p^{\alpha+\beta}$ Klassen $p^{\alpha+\beta+\gamma}$ verschiedene Klassen

ergibt, die sämtlich in $(\mathfrak{Q})$ enthalten sind. Erschöpfen diese Klassen die Gruppe $(\mathfrak{Q})$ noch nicht, so behandeln wir in derselben Weise eine vierte Klasse D usw.; und es ist evident, dass, da $(\mathfrak{Q})$ aus endlich vielen Klassen besteht, auch diese Operationen enden werden und n gleich einer Potenz von p sein wird. Q. E. D.

Satz. II. *Wird die Anzahl aller Klassen des Hauptgeschlechts durch* $a^\alpha b^\beta c^\gamma$ *usw. ausgedrückt, wobei* a, b, c *verschiedene Primzahlen bezeichnen, so gibt es in diesem Geschlecht* $a^\alpha, b^\beta, c^\gamma$ *usw. Klassen, die, jeweils zur Potenz* $a^\alpha, b^\beta, c^\gamma$ *usw. erhoben, die Hauptklasse ergeben.*

Beweis Es seien A, A', A'' usw. sämtliche Klassen, die, zur Potenz a^α erhoben, K ergeben, und $(\mathfrak{A})$ ihre Gesamtheit; ebenso B, B', B'' usw. $(\mathfrak{B})$, C, C', C'', $(\mathfrak{C})$ usw. usw. Ich behaupte, dass aus der Komposition aller Klassen von $(\mathfrak{A})$ mit allen Klassen von $(\mathfrak{B})$ mit allen Klassen von $(\mathfrak{C})$ usw. Klassen hervorgehen, die voneinander verschieden sind. Denn ist $A + B + C \cdots = A' + B' + C' \ldots$ usw., so erhalten wir, wenn wir $A - A' = A''$, $B - B' = B''$ usw. setzen,

$$A'' + B'' + C'' \text{ usw.} = K$$

also, wenn wir zur Potenz $b^\beta c^\gamma$ usw. erheben, $(b^\beta c^\gamma \ldots)A'' = K$, woraus leicht $A'' = K$ und $A = A'$ folgt, und ebenso gilt $B = B'$, $C = C'$ usw. Es sei die Gesamtheit dieser Klassen $= (S)$. Ferner ist klar, dass alle diese Klassen zum Hauptgeschlecht gehören werden. Schließlich kann es im Hauptgeschlecht keine Klasse geben, die nicht in (S) enthalten ist. Es sei . . .

Bemerkung.

Dieses 1801 geschriebene Fragment bezieht sich auf Disq. Arithm., Artikel 306, ix. Das Wort *dignité* wird hier in einem sonst nicht üblichen Sinn gebraucht.

Stern.

[I.]

ÜBER DEN ZUSAMMENHANG ZWISCHEN DER ANZAHL DER KLASSEN, IN DIE BINÄRE QUADRATISCHE FORMEN ZERFALLEN, UND IHRER DETERMINANTE.

ERSTE ABHANDLUNG

DER KÖNIGLICHEN GESELLSCHAFT VORGELEGT 1834 . . . .

1.

Dreiunddreißig Jahre sind nun vergangen, seit wir die Prinzipien des bemerkenswerten Zusammenhangs entdeckten, dem diese Abhandlung gewidmet ist, wie schon am Schluss der *Untersuchungen über höhere Arithmetik* angekündigt wurde. Andere Beschäftigungen hatten uns jedoch lange von dieser Untersuchung abgehalten, bis wir in jüngerer Zeit zu ihr zurückkehren und sie durch neue Bemühungen erweitern konnten. Da aber dieser neue Teil der höheren Arithmetik den Umfang einer einzigen Abhandlung übersteigt, soll diese erste den Formen mit negativen Determinanten gewidmet sein; die Formen mit positiven Determinanten, die eine ganz eigene Behandlung erfordern, müssen einer anderen Abhandlung vorbehalten bleiben.

2.

Die Grundlage des ganzen Gegenstands bildet eine besondere Untersuchung über die Anzahl aller Kombinationen ganzzahliger Werte, die zwei unbestimmte ganze Zahlen x, y innerhalb eines vorgeschriebenen Bereichs annehmen. Offenbar lässt sich diese Aufgabe auch geometrisch darstellen, indem man die Anzahl der *komplexen Zahlen* ermittelt, deren Darstellung in eine vorgeschriebene Figur fällt. Die Beschaffenheit der Figur hängt von der Beschaffenheit der sie umgebenden Linie ab und somit entweder von einer einzigen Gleichung zwischen den Koordinaten x, y (wenn der Rand eine in sich zurückkehrende Kurve ist) oder von mehreren solchen Gleichungen (wenn er .aus mehreren gekrümmten oder geraden Teilen besteht); dabei bleibt es unserer Wahl überlassen, ob wir Punkte, die komplexen ganzen Zahlen entsprechen und etwa auf dem Rand selbst liegen, mitzählen oder ausschließen wollen.

Bei der analytischen Darstellung der Aufgabe lassen sich diese Begrenzungsbedingungen stets so ausdrücken, dass eine oder mehrere gegebene Funktionen der Variablen x, y, nämlich P, Q, R usw., positive oder nichtnegative Werte annehmen müssen (je nachdem, ob der Wert 0 ausgeschlossen oder zugelassen wird).

Ist beispielsweise die vorgeschriebene Figur ein Kreis mit dem Radius $= \sqrt{A}$, und liegt sein Mittelpunkt in einem Punkt, der einer komplexen ganzen Zahl entspricht, so lautet die analytische Bedingung, dass $A - xx - yy$ nicht negativ ist, sofern wir, was wir immer voraussetzen werden, die auf dem Rand selbst liegenden Punkte beibehalten wollen. Ist die Figur ein Dreieck, so müssen die drei linearen Funktionen $ax+by+c$, $a'x+b'y+c'$, $a''x+b''y+c''$ nichtnegative Werte haben, und ebenso in anderen Fällen.

3.

Eine *exakte* Lösung der Aufgabe muss im Allgemeinen so vorgehen, dass zunächst aus der Beschaffenheit der Bedingungen die eine Variable, beispielsweise x, auf Grenzen beschränkt wird, zwischen denen die einzelnen ganzzahligen Werte nacheinander durchlaufen werden. Es ist zu ermitteln, wie viele ganzzahlige Werte der anderen Variablen y jedem davon entsprechen; diese Anzahlen sind dann zusammenzuzählen. In besonderen Fällen wird es meist besondere Verfahren geben, um die Arbeit abzukürzen.

Ist die Figur beispielsweise wie oben ein Kreis mit dem Radius $= \sqrt{A}$, so sei r die nächstkleinere ganze Zahl unterhalb von $\sqrt{A}$ oder $\sqrt{A}$ selbst, falls A ein Quadrat ist. Ebenso seien r', r'', r''' usw. $r^{(r)}$ die nächstkleineren ganzen Zahlen unterhalb von $\sqrt{(A-1)}$, $\sqrt{(A-4)}$, $\sqrt{(A-9)}$ usw. bis zu $\sqrt{(A-rr)}$. Dann ist die gesuchte Anzahl

$$\begin{aligned} &= 2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \text{usw.} \\ &= 1 + 4r + 4r' + 4r'' + 4r''' + \text{usw.} + 4r^{(r)} \end{aligned}$$

In diesem Beispiel ist die folgende Methode kürzer. Es sei q die nächstkleinere ganze Zahl unterhalb von $\sqrt{\frac{1}{2}A}$ (oder dieser gleich, falls sie ganzzahlig ist); ferner seien $r^{(q+1)}$, $r^{(q+2)}$, $r^{(q+3)}$ usw. die nächstkleineren ganzen Zahlen unterhalb von $\sqrt{(A-(q+1)^2)}$, $\sqrt{(A-(q+2)^2)}$, $\sqrt{(A-(q+3)^2)}$ usw. bis zu $\sqrt{(A-rr)}$. Dann ist die gesuchte Anzahl

$$= 4qq + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \text{usw.} + r^{(r)})$$

Nach dieser Formel wurden die folgenden Anzahlen ermittelt:

A		A		A	
100	317	1000	3149	10000	31417
200	633	2000	6293	20000	62845
300	949	3000	9425	30000	94237
400	1257	4000	12581	40000	125629
500	1581	5000	15705	50000	157093
600	1885	6000	18853	60000	188453
700	2209	7000	21993	70000	219901
800	2521	8000	25137	80000	251305
900	2821	9000	28269	90000	282697
1000	3149	10000	31417	100000	314197

4.

Für unser Vorhaben ist keine exakte Bestimmung erforderlich, sondern die Suche nach einem Ausdruck, der sich der genauen Anzahl beliebig weit nähern kann, während die Grenzen ins Unendliche erweitert werden. Da dies aber etwas Unbestimmtes enthält, müssen wir die Sache zunächst genauer darlegen.

Wir nehmen also an, dass die Funktionen P, Q, R usw. außer den Variablen x, y ein konstantes Element k enthalten, sodass die einzelnen P, Q, R usw. homogene Funktionen der drei Größen x, y, k sind. Die durch die Gleichungen $P = 0, Q = 0, R = 0$ usw. bestimmte Figur hängt damit von k ab, und zwar entsprechen verschiedenen Werten von k ähnliche und bezüglich des Koordinatenursprungs ähnlich gelegene Figuren; entsprechende lineare Abmessungen sind den Werten von k, die Flächeninhalte den Werten von kk proportional. Bezeichnen wir nun die Anzahl der Punkte innerhalb der Figur mit M, ihren Flächeninhalt mit V, so müssen offenbar M und V mit wachsendem k wachsen; wächst k ins Unendliche, so nähern sich M und V dem Verhältnis der Gleichheit beliebig weit. Oder, wenn du elementare Klarheit verlangst: Ist eine Größe λ gegeben, wie klein sie auch sei, so lässt sich stets eine solche Grenze angeben, dass für jeden Wert von k, der diese Grenze übersteigt, $\frac{M}{V}$ sicher zwischen $1-\lambda$ und $1+\lambda$ liegen muss. Nach der üblichen Ausdrucksweise darf man dies so angeben: Es wird $M = V$ für einen unendlichen Wert von k.

In unserem Beispiel gilt die erforderliche Bedingung, wenn wir $k = \sqrt{A}$ setzen, und die Kurve wird ein Kreis, dessen Flächeninhalt $= \pi A$, wobei π den halben Umfang eines Kreises mit dem Radius $= 1$ bezeichnet. Die oben angegebenen Zahlen lassen die Konvergenz deutlich erkennen.

Wenn es übrigens der Mühe wert wäre, könnten wir den Beweis dieses Satzes leicht mit der Strenge der Alten durchführen; an dieser Stelle haben wir ihn jedoch lieber unterdrückt und eilen zu schwierigeren Dingen weiter.

5.

In dieser Abhandlung wird der Rand durch eine *einzige* Gleichung der Form $axx + 2bxy + cyy = A$ ausgedrückt, wobei a, b, c ganze Zahlen sind und $bb - ac$ eine negative Zahl ist, die wir $= -D$ setzen. Offenbar ist die die Figur begrenzende Kurve eine Ellipse, und es ist leicht zu sehen, dass die Quadrate der Halbachsen die Wurzeln der Gleichung

$$(ac - bb)qq - (a + c)Aq + AA = 0 \quad \text{oder} \quad = A\left(\frac{a + c \pm \sqrt{(4bb + (a - c)^2)}}{2(ac - bb)}\right)$$

sind.

Das Produkt dieser Wurzeln ist $\frac{AA}{ac-bb} = \frac{AA}{D}$, also der Flächeninhalt der Ellipse $= \frac{\pi A}{\sqrt{D}}$. Daraus folgt, dass die Anzahl aller Kombinationen ganzzahliger Werte von x, y, für die $axx + 2bxy + cyy$ den Wert A nicht übersteigt, mit wachsendem A dem Wert $\frac{\pi A}{\sqrt{D}}$ immer näher kommt und für unendliches A diesem Wert gleichgesetzt werden muss. Dabei ist offenbar gleichgültig, ob die Kombination $x = 0, y = 0$ zu den übrigen mitgezählt oder ausgeschlossen wird. Somit ist die gesuchte Anzahl (im letzteren Sinn) nichts anderes als die Summe der Anzahlen der Darstellungen der einzelnen Zahlen $1, 2, 3 \ldots A$ durch die binäre quadratische Form $axx + 2bxy + cyy$; und da einige dieser Zahlen durch diese Form überhaupt nicht dargestellt werden können, andere mehr, andere weniger Darstellungen zulassen, ist die Größe $\frac{\pi}{\sqrt{D}}$ als mittlerer Wert der Anzahl der Darstellungen einer unbestimmten positiven Zahl durch eine beliebige Form zu betrachten, deren Determinante $= -D$.

6.

Bevor wir die Folgerungen hieraus allgemein untersuchen, erschien es uns zweckmäßig, einige besondere Fälle auszuarbeiten, damit sich die Art der Argumentation leichter verstehen lässt. Greifen wir also zunächst die Form $xx + yy$ wieder auf, für die die Anzahl der Darstellungen einer unbestimmten Zahl den mittleren Wert $= \pi$ erhält. Die Anzahl der tatsächlichen Darstellungen einer gegebenen Zahl lässt sich ohne Schwierigkeit aus den in den Untersuchungen über höhere Arithmetik aufgestellten allgemeinen Prinzipien bestimmen. Bezeichnen wir mit fA die Anzahl der Darstellungen der Zahl A, so ist diese $= 4$, wenn $A = 1$ oder 2 oder eine Potenz von zwei ist; $= 8$, wenn A eine Primzahl der Form $4n + 1$ oder das Produkt einer solchen Primzahl mit einer Potenz von zwei ist; $= 0$, wenn A eine Primzahl der Form $4n + 3$ oder durch eine solche Primzahl, jedoch nicht durch deren Quadrat teilbar ist; schließlich *allgemein*

$$\begin{aligned} \text{entweder} \quad &= 4(\alpha + 1)(\beta + 1)(\gamma + 1)\ldots \\ \text{oder} \quad &= 0 \end{aligned}$$

Dabei wird die Zahl A auf die Form $2^\mu S a^\alpha b^\beta c^\gamma \ldots$ gebracht; a, b, c usw. bezeichnen verschiedene Primzahlen der Form $4n+1$ und S das Produkt der Primzahlen der Form $4n+3$, die ein- oder mehrmals unter den Faktoren der Zahl A vorkommen, falls es solche gibt. Es gilt der erste oder zweite Wert, je nachdem, ob die Zahl S ein Quadrat oder kein Quadrat ist. Somit hängt fA offenbar allein davon ab, wie die Primzahlen $3, 5, 7, 11, 13$ usw. unter den Faktoren der Zahl A vorkommen, sodass allgemein

$$fA = 4(3) \,.\, (5) \,.\, (7) \,.\, (11) \,.\, (13) \ldots .$$

zu setzen ist, wenn wir annehmen, dass die Werte der Zeichen $(3), (5), (7)$ usw. so gewählt werden, dass für eine Primzahl p gilt:

erstens $(p) = 1$, wenn p die Zahl A nicht teilt

zweitens $(p) = \alpha + 1$, wenn p die Form $4n+1$ hat und p^α die höchste Potenz ist, die A teilt

drittens $(p) = 0$, wenn p die Form $4n+3$ hat und der Exponent der höchsten Potenz von p, die A teilt, ungerade ist; schließlich

viertens $(p) = 1$, wenn p die Form $4n+3$ hat und der Exponent der höchsten Potenz von p, die A teilt, gerade ist.

Offenbar ist der erste Fall im zweiten und vierten enthalten.

Auf diese Weise verlaufen die Glieder der Folge $f1, f2, f3, f4$ usw. sehr unregelmäßig, obwohl sich der mittlere Wert $= \pi$ umso genauer ergeben muss, je mehr Glieder genommen werden. Die Summe $f1 + f2 + f3 + \ldots + fA$ bezeichnen wir mit FA.

7.

Setzen wir nun allgemein $fm + f3m = f'm$, so erkennt man leicht, dass

$$f'A = 4(5) \,.\, (7) \,.\, (11) \,.\, (13) \ldots$$

gilt, das heißt, $f'A$ wird von der Beziehung von A zum Teiler 3 unabhängig sein, sodass die Unregelmäßigkeit der Folge $f'1, f'2, f'3, f'4, f'5, f'6$ usw. sowohl später beginnt als auch viel geringer ist. Setzen wir ferner

$$f'1 + f'2 + f'3 + f'4 + \text{usw.} + f'm = F'm$$

so gilt

$$\begin{aligned} F'3A &= F3A + f3 + f6 + f9 + \ldots + f9A \\ &= F3A + FA \end{aligned}$$

Daraus folgt leicht, dass für ins Unendliche wachsendes A

$$F'3A = 4\pi A$$

zu setzen ist, oder dass der mittlere Wert der Glieder der Folge
$f'1, f'2, f'3, f'4$ usw.

$$= \tfrac{4}{3}\pi$$

ist.

Ebenso ergibt sich, wenn wir allgemein $-f'm + f'5m = f''m$ setzen,

$$f''A = 4(7)(11)(13)\ldots$$

das heißt, aus der neuen Folge $f''1, f''2$ usw. verschwinden die Schwankungen, die von der Beziehung zur Zahl 5 abhängen. Setzen wir die Summe

$$f''1 + f''2 + f''3 + \ldots + f''m = F''m$$

so gilt

$$F''5m = -F'm + F'5m$$

woraus folgt, dass für ins Unendliche wachsendes m

$$F''5m = \tfrac{4}{3}\pi \,.\, 4m$$

zu setzen ist, oder dass der mittlere Wert der Glieder der Folge $= \frac{4}{3} \,.\, \frac{4}{5}\pi$ ist.

Gehen wir in derselben Weise weiter, indem wir neue Folgen bilden und dabei nacheinander die Faktoren $(7), (11), (13), (17)$ usw. entfernen, so nähern sich diese immer mehr der Unveränderlichkeit, und ihre mittleren Werte erhalten nacheinander die neuen Faktoren $\frac{8}{7}, \frac{12}{11}, \frac{12}{13}, \frac{16}{17}, \frac{20}{19}$ usw. Die Nenner sind dabei die Primzahlen in ihrer natürlichen Reihenfolge, die Zähler dagegen um eins größer oder kleiner, je nachdem, ob jene die Form $4n-1$ oder $\cdot 4n+1$ haben. Da nun bei Fortsetzung dieses Verfahrens ins Unendliche der konstante Wert 4 dem mittleren Wert immer näher kommen muss, erhalten wir

$$4 = \pi \,.\, \tfrac{4}{3} \cdot \tfrac{4}{5} \cdot \tfrac{8}{7} \cdot \tfrac{12}{11} \cdot \tfrac{12}{13} \ldots \text{ bis ins Unendliche}$$

oder

$$\pi = 4 \,.\, \frac{3}{3+1} \cdot \frac{5}{5-1} \cdot \frac{7}{7+1} \cdot \frac{11}{11+1} \cdot \frac{13}{13-1} \cdots$$

Entwickelt man die einzelnen Brüche in unendliche Reihen,

$$\frac{3}{3+1} = 1 - \frac{1}{3} + \frac{1}{9} - \frac{1}{27} + \dots$$
$$\frac{5}{5-1} = 1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \dots$$
$$\frac{7}{7+1} = 1 - \frac{1}{7} + \frac{1}{49} - \frac{1}{343} + \dots$$
usw.

so lässt sich das Produkt leicht in

$$1 - \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{7} + \tfrac{1}{9} - \tfrac{1}{11} + \tfrac{1}{13} \dots .$$

entwickeln; die Summe dieser Reihe ist bekanntlich $= \frac{1}{4}\pi$. Tatsächlich hatte der berühmte Euler schon vor langer Zeit auf umgekehrtem Weg hieraus die Gleichheit zwischen $\frac{1}{4}\pi$ und dem unendlichen Produkt $\frac{4}{3} \cdot \frac{4}{5} \cdot \frac{8}{7} \cdot .$ hergeleitet (*Introd. in analys. inf.*, Bd. I, Kap. xv, Artikel 285).

8.

Betrachten wir an zweiter Stelle die Form $xx + 2yy$, für die die Anzahl der Darstellungen einer unbestimmten Zahl den mittleren Wert $= \frac{\pi}{\sqrt{2}}$ haben wird. Bezeichnen wir mit fA die Anzahl der Darstellungen einer gegebenen Zahl A durch diese Form, so ist diese $= 2$ für $A = 1$ oder $A = 2$ oder immer dann, wenn A eine Potenz von zwei ist; ferner $fA = 4$, wenn A eine der Primzahlen ist, deren quadratischer Rest -2 ist, also eine der Formen $8k + 1, 8k + 3$, etwa $A = 3, 11, 17, 19, 41, 43$ usw.; schließlich $fA = 0$, wenn A eine Primzahl ist, deren quadratischer Nichtrest -2 ist, etwa aus der Folge $5, 7, 13, 23, 29, 31$ usw., also entweder der Form $8k + 5$ oder der Form $8k + 7$. Allgemein ist jedoch

$$\begin{aligned} \text{entweder} \quad & fA = 2(\alpha+1)(\beta+1)(\gamma+1)\ldots \\ \text{oder} \quad & fA = 0 \end{aligned}$$

zu setzen. Dabei wird die Zahl A auf die Form $2^\mu S a^\alpha b^\beta c^\gamma \ldots$ gebracht; a, b, c usw. bezeichnen verschiedene Primzahlen der Formen $8k+1, 8k+3$, dagegen S das Produkt der übrigen Zahlen (der Formen $8k + 5, 8k + 7$), falls solche unter den Faktoren der Zahl A vorkommen. Es gilt der erste oder zweite Wert, je nachdem, ob S ein Quadrat oder kein Quadrat ist. Durch ganz ähnliche Schlussfolgerungen wie im vorigen Artikel gehen wir nun von der Folge $f1, f2, f3, f4, f5$ usw., also $2, 2, 4, 2, 0, 2$ usw., nacheinander zu anderen über, die immer länger *konstant* bleiben. Ihre *mittleren* Werte sind nacheinander $\frac{\pi}{\sqrt{2}}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5} \cdot \frac{8}{7}$ usw.; wir gehen dabei so vor, dass wir zu der Gleichung

$$2 = \frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{10}{11} \cdot \frac{14}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} \cdots$$

gelangen, in der die Nenner die natürliche Folge der Primzahlen bilden, die Zähler dagegen um eins kleiner sind, wenn die Nenner die Form $8k + 1$ oder $8k + 3$ haben, und um eins größer, wenn die Nenner die Form $8k + 5$ oder $8k + 7$ haben.

[II.]

ÜBER DEN ZUSAMMENHANG ZWISCHEN DER ANZAHL DER KLASSEN, IN DIE BINÄRE QUADRATISCHE FORMEN ZERFALLEN, UND IHRER DETERMINANTE.

ERSTE ABHANDLUNG

DER KÖNIGLICHEN GESELLSCHAFT VORGELEGT 1837 . . .

1.

Sechsunddreißig Jahre sind vergangen, seit die Prinzipien des bemerkenswerten Zusammenhangs entdeckt wurden, der in dieser Abhandlung behandelt werden soll, wie schon am Schluss der *Untersuchungen über höhere Arithmetik* angekündigt wurde. Andere Beschäftigungen hatten die Aufmerksamkeit jedoch lange von dieser Untersuchung abgelenkt, bis es in jüngerer Zeit gelang, zu ihr zurückzukehren und sie durch neue Bemühungen zu erweitern. Da aber dieser neue Teil der höheren Arithmetik den Umfang einer einzigen Abhandlung übersteigt, soll diese erste den Formen mit negativen Determinanten gewidmet sein; die Formen mit positiven Determinanten, die eine ganz eigene Behandlung erfordern, bleiben einer anderen Abhandlung vorbehalten.

2.

Für unser Vorhaben wird ein Satz benötigt, der an sich zwar arithmetisch ist, dessen Wesen sich jedoch bequemer und deutlicher durch Überlegungen in geometrischer Form vor Augen führen lässt.

Ist in einer unbegrenzten Ebene eine durch eine beliebige Linie begrenzte Figur gegeben, so lässt sich ihr Flächeninhalt näherungsweise bestimmen, indem man die Ebene in Quadrate teilt und sowohl diejenigen zählt, die ganz innerhalb der Figur liegen, als auch diejenigen, die von ihrem Rand geschnitten werden. Offenbar ergibt sich ein kleinerer oder größerer Flächeninhalt als der wahre, je nachdem, ob die letzteren Quadrate weggelassen oder zu den ersteren hinzugezählt werden. Will man aber die letzteren, auf dem Rand liegenden Quadrate nach irgendeiner Regel teils ausschließen, teils mitzählen, so kann der Fehler positiv oder negativ sein; er muss jedoch kleiner sein als der gesamte Flächeninhalt aller Randquadrate. Je kleiner man die Quadrate wählt, desto genauer wird der Flächeninhalt auf diese Weise bestimmt. Man kann eine solche Annäherung unbegrenzt fortsetzen oder die Quadrate so klein wählen, dass der Fehler kleiner als jede gegebene Größe wird. Obwohl dies schon an sich einleuchtend erscheinen mag, werden wir es dennoch nicht verschmähen, es durch einen strengen Beweis abzusichern.

Zwei Quadrate können entweder einen Eckpunkt, zwei oder keinen gemeinsam haben; im ersten und zweiten Fall sollen sie benachbart, im dritten disjunkt heißen. Offenbar können höchstens vier Quadrate sämtlich einander benachbart sein; daher müssen sich unter je fünf verschiedenen Quadraten mindestens zwei disjunkte finden. Da nun der Abstand zwischen zwei Punkten in disjunkten Quadraten nicht kleiner sein kann als die Seitenlänge der Quadrate, die wir mit a bezeichnen wollen, ist klar: Geht ein Punkt von einer beliebigen Stelle eines Quadrats aus, durchquert dann ein zweites, drittes und viertes und gelangt schließlich zu einem fünften, so ist die Länge seines Weges sicher nicht kleiner als a. Aus demselben Grund kann, wenn die Linie immer weitere Quadrate durchläuft, der Teil zwischen dem fünften und neunten sowie zwischen dem neunten und dreizehnten usw. nicht kleiner als a sein. Wir schließen daher leicht, dass eine beliebige in sich zurückkehrende Linie, die insgesamt n verschiedene Quadrate berührt hat, sicher nicht kürzer als $\frac{(n-4)a}{4}$ sein kann. Umgekehrt kann also eine geschlossene Linie der Länge $= l$ sicher nicht mehr als $4 + \frac{4l}{a}$ verschiedene Quadrate berührt haben. Da deren Flächeninhalt $= 4aa + 4al$ bei unbegrenzt abnehmendem a kleiner als jede gegebene Größe werden kann, gilt dies umso mehr für den Fehler der oben besprochenen Flächenbestimmung.

3.

Die Regel für die Zulassung oder den Ausschluss der auf dem Rand der Figur liegenden Quadrate ließe sich auf viele verschiedene Arten festlegen. Am einfachsten scheint es jedoch, nur die Lage des Mittelpunkts jedes Quadrats zu beachten: Quadrate, deren Mittelpunkte innerhalb der Figur liegen, werden zugelassen, diejenigen, deren Mittelpunkte außerhalb liegen, ausgeschlossen. Schließlich bleibt es unserer Wahl überlassen, ob Mittelpunkte, die etwa auf dem Rand selbst liegen, den inneren oder den äußeren zugerechnet werden sollen. Anstelle der Mittelpunkte könnten wir auch beliebige andere Punkte nehmen, die in den einzelnen Quadraten jeweils dieselbe relative Lage haben.

Damit kommt es darauf an, sich in der Ebene Punkte in gleichen Abständen auf ebenfalls gleich weit voneinander entfernten Geraden so verteilt zu denken, dass sie Quadrate bilden. Nach dem Satz des vorigen Artikels können wir dann behaupten, dass die Anzahl der in der Figur enthaltenen Punkte, multipliziert mit dem Quadrat des Abstands zweier nächster Punkte, dem Flächeninhalt der Figur beliebig nahe kommt, sofern jener Abstand nur hinreichend klein gewählt wird; oder, nach der gewöhnlichen Ausdrucksweise, dass dieses Produkt den Flächeninhalt angibt, wenn der Abstand unendlich klein ist.

4.

Die durch die folgende Gleichung zwischen den rechtwinkligen Koordinaten p, q ausgedrückte Kurve,

$$app + 2bpq + cqq = 1$$

ist ein Kegelschnitt, und zwar eine Ellipse, wenn a, c sowie $ac - bb$ positive Größen sind. Der von dieser Ellipse eingeschlossene Flächeninhalt ergibt sich zu . $= \frac{\pi}{\sqrt{(ac-bb)}}$. Der Wert von $app + 2bpq + cqq$ ist außerhalb der Ellipse überall größer als 1, innerhalb kleiner als 1 und nirgends negativ.

Man denke sich ein .System von Punkten in der Ebene der Ellipse so verteilt, dass sie Quadrate bilden, deren Seiten $= \lambda$ den Koordinatenachsen parallel sind. Dabei ist es gleichgültig, ob der Koordinatenursprung, also der Mittelpunkt der Ellipse, mit einem dieser Punkte zusammenfällt oder nicht. Die Anzahl der Punkte innerhalb der Ellipse, einschließlich etwa auf dem Rand selbst liegender Punkte, sei $= m$. Dann ist nach dem Satz des vorigen Artikels $\frac{\pi}{\sqrt{(ac-bb)}}$ der Grenzwert von $m\lambda\lambda$, dem diese Größe bei unbegrenzt abnehmendem λ beliebig nahe kommt.

Nehmen wir an, dass der Koordinatenursprung mit einem Punkt des Systems zusammenfällt, so sind, wenn wir $p = \lambda x, q = \lambda y$ setzen, offenbar für die einzelnen Punkte des Systems x und y ganze Zahlen; umgekehrt entspricht jede Kombination ganzzahliger Werte der Größen x, y einem Punkt des Systems. Die Zahl m ist daher nichts anderes als die Anzahl aller Kombinationen ganzzahliger Werte von x, y, für die F nicht größer als M wird, wenn wir der Kürze wegen die Funktion oder quadratische Form $axx + 2bxy + cyy$ mit F und die Größe $\frac{1}{\lambda\lambda}$ mit M bezeichnen. Die Determinante dieser Form ist $bb-ac$; dafür schreiben wir $-D$. Unser Satz ist nun folgendermaßen auszusprechen.

Satz I. *Die Anzahl m aller Kombinationen ganzzahliger Werte der Unbestimmten x, y, für die der Wert einer Form mit negativer Determinante $-D$ die Grenze M nicht überschreitet, wird $= \frac{\pi M}{\sqrt{D}}$, zwar näherungsweise, doch mit unbegrenzt zunehmender Annäherung, während M ins Unendliche wächst. Es braucht kaum darauf hingewiesen zu werden, dass die unbegrenzte Annäherung hier, und ebenso im Folgenden, nicht so zu verstehen ist, als ob die Differenz zwischen $\frac{\pi M}{\sqrt{D}}$ und m selbst unbegrenzt abnähme. Vielmehr nähert sich das Verhältnis dieser Größen unbegrenzt der Gleichheit; das heißt, $\frac{\pi M}{m\sqrt{D}} - 1$ nimmt unbegrenzt ab.*

5.

Um die Auszählung tatsächlich auszuführen, kann man für die einzelnen ganzzahligen Werte von x zwischen den Grenzen $-\sqrt{\frac{cM}{D}}$ und $+\sqrt{\frac{cM}{D}}$ die beiden Werte von y berechnen, die $F = M$ entsprechen; daraus ergibt sich unmittelbar die Anzahl der dazwischenliegenden ganzen Zahlen. Da diese Anzahl für entgegengesetzte Werte von x dieselbe ist, ersparen wir uns nahezu die Hälfte der Arbeit. Man kann auch die Werte von x zählen, die den einzelnen Werten von y zwischen den Grenzen $-\sqrt{\frac{aM}{D}}$ und $+\sqrt{\frac{aM}{D}}$ entsprechen. Durch eine geeignete Verbindung beider Methoden lässt sich die Arbeit weiter verringern; wir führen dies hier jedoch nicht ausführlicher aus. Es möge genügen, einiges zum einfachsten Fall hinzuzufügen.

Die Form sei $F = xx + yy$, also die Kurve ein Kreis; ferner seien $r, r', r'', r''' \dots r^{(r)}$ die nächstkleineren ganzen Zahlen unterhalb von

$$\sqrt{M}, \quad \sqrt{(M-1)}, \quad \sqrt{(M-4)}, \quad \sqrt{(M-9)} \dots \sqrt{(M-rr)}$$

oder diese Größen selbst, falls sich unter ihnen ganze Zahlen befinden. Dann ist die gesuchte Anzahl

$$\begin{aligned} m &= 2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \text{usw.} + 2(2r^{(r)} + 1) \\ &= 1 + 4r + 4r' + 4r'' + 4r''' + \text{usw.} + 4r^{(r)} \end{aligned}$$

Dasselbe erreichen wir jedoch schneller, indem wir mit q die nächstkleinere ganze Zahl unterhalb von $\sqrt{\frac{1}{2}M}$ bezeichnen (oder diese Größe selbst, wenn sie ganzzahlig ist) und die Formel

$$m = 4qq + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \text{usw.} + r^{(r)})$$

verwenden. Auf diese Weise wurden die folgenden Anzahlen ermittelt.

M	m	M	m	M	m
100	317	1000	3149	10000	31417
200	633	2000	6293	20000	62845
300	949	3000	9425	30000	94237
400	1257	4000	12581	40000	125629
500	1581	5000	15705	50000	157093
600	1885	6000	18853	60000	188453
700	2209	7000	21993	70000	219901
800	2521	8000	25137	80000	251305
900	2821	9000	28269	90000	282697
1000	3149	10000	31417	100000	314197

6.

Dem Satz des Artikels 4 geben wir auf folgende Weise größere Allgemeinheit.

Satz II. *Sollen nicht alle Kombinationen ganzzahliger Werte von x, y, für die F den Wert M nicht überschreitet, gesammelt werden, sondern nur diejenigen in bestimmten Abständen, nämlich diejenigen, bei denen x einer gegebenen Zahl G zu einem gegebenen Modul g und y einer gegebenen Zahl H zu einem gegebenen Modul h kongruent ist, so wird die Anzahl m' dieser Kombinationen näherungsweise durch $\frac{\pi M}{gh\sqrt{D}}$ ausgedrückt, mit unbegrenzt zunehmender Annäherung, während M ins Unendliche wächst.*

Setzen wir nämlich $x = gx' + G, y = hy' + H$, so ist klar, dass m' die Anzahl aller Kombinationen ganzzahliger Werte von x', y' ist, für die

$$agg(x' + \tfrac{G}{g})^2 + 2bgh(x' + \tfrac{G}{g})(y' + \tfrac{H}{h}) + chh(y' + \tfrac{H}{h})^2$$

den Wert M nicht überschreitet. Denken wir uns also ein Punktesystem in der Ebene wie in Artikel 4 verteilt, jedoch so, dass nicht der Koordinatenursprung, sondern der Punkt mit den Koordinaten $p = \frac{G\lambda}{g}, q = \frac{H\lambda}{h}$ mit einem Punkt des Systems zusammenfällt, so drückt m' die Anzahl der Punkte innerhalb der Ellipse aus, deren Gleichung

$$aggpp + 2bghpq + chhqq = 1$$

ist, wobei etwa auf dem Rand selbst liegende Punkte stets mitgezählt werden. Der Flächeninhalt dieser Ellipse $= \frac{\pi}{gh\sqrt{(ac-bb)}} = \frac{\pi}{gh\sqrt{D}}$ ist der Grenzwert, dem sich das Produkt $m'\lambda\lambda = \frac{m'}{M}$ unbegrenzt nähert, wenn λ unbegrenzt abnimmt oder M ins Unendliche wächst.

Offenbar umfasst unser Satz auch den Fall, dass nur eine der Unbestimmten x, y in bestimmten Abständen fortschreiten soll, während der Wert der anderen keiner Bedingung unterliegt. Denn dies ist offenbar dasselbe, als wenn entweder h oder $g = 1$ gesetzt wird.

7.

Die bisherigen Ausführungen sind von der Beschaffenheit der Koeffizienten der Form $axx + 2bxy + cyy$ unabhängig; von nun an werden wir aber voraussetzen, dass diese Koeffizienten ganzzahlig sind. Damit gibt jede Kombination ganzzahliger Werte von x, y der Form selbst einen ganzzahligen Wert oder entspricht einer Darstellung irgendeiner ganzen Zahl durch diese Form. Daher ist die Gesamtheit aller Kombinationen ganzzahliger Werte von x, y, durch die die Form $F = axx + 2bxy + cyy$ einen Wert nicht größer als die Grenze M erhält, dieselbe wie die Gesamtheit aller Darstellungen ganzer Zahlen, die die Grenze M nicht überschreiten, also bis zu dieser Grenze einschließlich, falls sie selbst ganzzahlig ist. Bezeichnen wir daher

der Kürze wegen die Anzahl der verschiedenen Darstellungen einer bestimmten ganzen Zahl n durch die Form F mit $F(n)$ oder, wenn keine Mehrdeutigkeit zu befürchten ist, einfach mit Fn, so ist die oben durch m ausgedrückte Zahl $= F0 + F1 + F2 + F3 +$ usw. $+ FM$, und der erste Satz nimmt die folgende Gestalt an.

Satz III. *Die Summe $F0 + F1 + F2 +$ usw. $+ FM$ wird näherungsweise durch $\frac{\pi M}{\sqrt{D}}$ ausgedrückt, mit unbegrenzt zunehmender Annäherung, während M ins Unendliche wächst.*

8.

Es bietet sich an, dem dritten Satz, der die Darstellungen *aller* Zahlen betrifft, einen anderen hinzuzufügen, der nur ungerade Zahlen betrifft. Offenbar können durch die Form F keine ungeraden Zahlen dargestellt werden, wenn a und c beide gerade Zahlen sind; die Untersuchung wird daher auf die drei übrigen Fälle beschränkt.

I. Ist a ungerade und c gerade, so wird eine ungerade Zahl dargestellt, indem man x einen ungeraden Wert gibt, während der Wert von y beliebig bleibt. Satz II zeigt daher, wenn man $g = 2, G = 1, h = 1$ setzt, dass die Anzahl aller Kombinationen solcher Werte von x, y, die der Form einen ungeraden Wert nicht größer als die Grenze M geben, mit unbegrenzter Annäherung durch $\frac{\pi M}{2\sqrt{D}}$ ausgedrückt wird, während M ins Unendliche wächst.

II. Ist a gerade und c ungerade, so muss zur Darstellung einer ungeraden Zahl y ungerade sein. Setzen wir daher $g = 1, h = 2, H = 1$, so gelangen wir zum selben Schluss.

III. Sind sowohl a als auch c ungerade, so muss entweder ein ungerader Wert von x mit einem geraden Wert von y oder ein gerader Wert von x mit einem ungeraden Wert von y kombiniert werden, damit sich ein ungerader Wert der Formel ergibt. Für jede der beiden Arten wird die Anzahl aller Kombinationen, für die der Wert der Form die Grenze M nicht überschreitet, mit unbegrenzter Annäherung durch $\frac{\pi M}{4\sqrt{D}}$ ausgedrückt. Daher wird die Anzahl aller Kombinationen, die der Form ungerade Werte nicht größer als die Grenze M geben, auch hier mit unbegrenzter Annäherung durch $\frac{\pi M}{2\sqrt{D}}$ ausgedrückt.

Da nun die Gesamtheit aller solchen Kombinationen nichts anderes ist als die Gesamtheit aller Darstellungen aller Zahlen $1, 3, 5, 7 \ldots M$, wenn M eine ungerade ganze Zahl ist, oder $1, 3, 5, 7 \ldots . M - 1$, wenn M gerade ist, haben wir

Satz IV. *Die Summe*

$$F1 + F3 + F5 + F7 .. + FM \quad \text{oder} \quad F1 + F3 + F5 + F7 .. + F(M-1)$$

(je nachdem, ob M ungerade oder gerade ist) wird mit unbegrenzter Annäherung durch $\frac{\pi M}{2\sqrt{D}}$ ausgedrückt, sofern F eine Form ist, in der einer der Koeffizienten a, c oder beide ungerade sind.

[III.]

Es sei C die Gesamtheit der Repräsentanten sämtlicher Klassen der eigentlich primitiven Formen für die Determinante $-D$. Wir bezeichnen mit (n) die Anzahl aller Darstellungen der Zahl n durch Formen aus der Gesamtheit C. Es sei p eine ungerade Primzahl. Dann ist

$$\begin{array}{ll} 1. & (pn) = (n) \quad \text{wenn } p \text{ ein Divisor von } D \\ \left.\begin{array}{ll} 2. & (pn) = (n) + (h) \\ 3. & (pn) = -(n) + (h) \end{array}\right\} & \text{wenn } p \text{ Nichtdivisor von } D \end{array}$$

$$\begin{cases} \text{Divisor von } xx + D \\ \text{Nichtdivisor von } xx + D \end{cases}$$

wobei $n = hp^\mu$, μ beliebig und h nicht durch p teilbar ist.

Im Fall 1. ist $(h) = (ph) = (pph) = (p^3h)$ usw.

2. $(ph) = 2(h),\ (pph) = 3(h),\ (p^3h) = 4(h)$ usw.

3. $(ph) = 0,\ (pph) = (h),\ (p^3h) = 0,\ (p^4h) = (h)$ usw.

* *
*

Aus jeder eigentlich primitiven Klasse für die Determinante $= -D$, deren Anzahl $= \lambda$ ist, sei eine Form ausgewählt; die Gesamtheit dieser Formen sei L.

Man bezeichne mit fA die Anzahl sämtlicher Darstellungen der Zahl A durch Formen aus L.

Es sei ferner $f(A;p) = f\frac{A}{p^\alpha}$, wenn p^α die höchste Potenz der Primzahl p ist, die A teilt; ferner $f(A;p,q) = f\frac{A}{p^\alpha q^\beta}$, wenn q eine andere Primzahl ist, deren höchste A teilende Potenz $= q^\beta$ ist; ebenso $f(A;p,q,r) = f\frac{A}{p^\alpha q^\beta r^\gamma}$, wenn r eine dritte Primzahl ist, deren höchste A teilende Potenz r^γ ist, und so weiter.

[IV.]

Man bezeichne mit (n) die Anzahl der Werte x aus der Gesamtheit

$$0, 1, 2, 3, 4 \ldots . p^n - 1$$

für die $xx - D = xx - ap^\mu$ durch p^n teilbar ist.

1) μ ungerade z. B. $= 7$.	2) μ gerade z. B. $= 6$	
	aNp	aRp
$(1) = 1$	$(1) = 1$	$(1) = 1$
$(2) = p$	$(2) = p$	$(2) = p$
$(3) = p$	$(3) = p$	$(3) = p$
$(4) = pp$	$(4) = pp$	$(4) = pp$
$(5) = pp$		

$(6) = p^3$	$(5) = pp$	$(5) = pp$
$(7) = p^3$	$(6) = p^3$	$(6) = p^3$
$(8) = 0$	$(7) = 0$	$(7) = 2p^3$
$(9) = 0$	$(8) = 0$	$(8) = 2p^3$
usw.	usw.	usw.

Man mache nun	Dann ist
$(1) - \frac{(2)}{p} = (1)'$	$fp = (1)'$
$(2) - \frac{(3)}{p} = (2)'$	$fpp = 1 + (2)'$
$(3) - \frac{(4)}{p} = (3)'$	$fp^3 = (1)' + (3)'$
$(4) - \frac{(5)}{p} = (4)'$	$fp^4 = 1 + (2)' + (4)'$
usw.	usw.

Setzt man also $\frac{p-1}{p}(1 + \frac{fp}{p} + \frac{fpp}{pp} + \frac{fp^3}{p^3} + \text{usw.}) = T$, so ist

$$\frac{p+1}{p}T = 1 + \frac{(1)'}{p} + \frac{(2)'}{pp} + \frac{(3)'}{p^3} + \frac{(4)'}{p^4} + \text{usw.}$$
$$= 1 + \frac{(1)}{p} = 1 + \frac{1}{p}$$

Also $T = 1$

[V.]

Die durchschnittliche Anzahl der Klassen*) in der Nähe der negativen Determinante $-D$ ist näherungsweise

$$= \frac{\pi\sqrt{D}}{4(1 + \frac{1}{27} + \frac{1}{125} + \text{usw.})}$$

Die tatsächliche Anzahl wird durch die folgenden Formeln ausgedrückt. Der Kürze wegen steht dabei m für die durchschnittliche, M für die tatsächliche Anzahl; p, q bezeichnen alle ungeraden Primzahlen, die D nicht teilen, und zwar ersteres die Teiler, letzteres die Nichtteiler von $\square + D$; r die Primzahlen**), die D teilen:

*)[Vgl. *Disquiss. Arithm.*, Artikel 302; die dortige Formel weicht um eine Konstante δ von der hier im Text vorkommenden ab.]

**)[ungerade.]

$$\text{I.} \quad M = m \text{ Produkt aus } \frac{p^3+p^2}{p^3-1} \cdot \frac{q^3-q^2}{q^3-1} \cdot \frac{r^3-r}{r^3-1}$$

$$\text{II.} \quad M = \frac{\pi\sqrt{D}}{4} \text{ Produkt aus } \frac{p+1}{p} \cdot \frac{q-1}{q} \cdot \frac{rr-1}{rr}$$

$$\text{III. NB.} \quad M = \frac{2\sqrt{D}}{\pi} \text{ Produkt aus } \frac{p}{p-1} \cdot \frac{q}{q+1}$$

$$\text{IV.} \quad M = \sqrt{\left\{ \frac{D}{2} \cdot \text{Produkt aus } \frac{p+1}{p-1} \cdot \frac{q-1}{q+1} \cdot \frac{rr-1}{rr} \right\}}$$

$$\text{V.} \quad M = \frac{2\sqrt{D}}{\pi}\{1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \pm \tfrac{1}{7} \pm \tfrac{1}{9} \text{ usw.}\}$$

NB. Die Formel III wird unmittelbar aus dem Vergleich der beiden Arten abgeleitet, die darstellbaren Zahlen bis zu einer gewissen Grenze zu zählen.

[VI.]

Satz. Die Anzahl der Klassen, in die alle eigentlich primitiven binären Formen mit der negativen Determinante $-D$[*], ist gleich

$$\frac{\pi}{4} \times \sqrt{D} \times \text{Produkt aus } \frac{p-1}{p}\frac{q+1}{q} \times \frac{rr-1}{rr}$$

wobei bezeichnet:

p alle Primzahlen[**], für die $-D$ ein Nichtrest ist,

q alle Primzahlen[**], für die $-D$ ein Rest ist,

r alle Primzahlen[**], die D teilen;

$$= \frac{\frac{\pi}{4}\sqrt{D} \text{ Produkt aus } \frac{rr-1}{rr}}{1 \pm \frac{1}{3} \pm \frac{1}{5} \text{ usw.}}$$

Im Nenner steht das positive Vorzeichen vor den Brüchen, deren Nenner die Form von Nichtteilern haben, das negative vor denen, deren Nenner die Form von Teilern von $xx + D$ haben; die Brüche, deren Nenner nicht zu D teilerfremd sind, werden ganz weggelassen[***].

---

[*] [eingeteilt werden.]

[**] [ungerade.]

[***] [Bezeichnet man mit m alle positiven ganzen Zahlen, die zu $2D$ teilerfremd sind, und verwendet das von Jacobi verallgemeinerte Symbol von Legendre, so ist die obige Regel für die Vorzeichen folgendermaßen zu berichtigen: In der vorhergehenden Formel ist der Nenner

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \text{ usw.} = \Sigma \pm \left(\frac{-D}{m}\right)\frac{1}{m}$$

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \ldots)}{\pi}$$
$$= \frac{\operatorname{cotg}\theta \pm \operatorname{cotg} 3\theta \pm \operatorname{cotg} 5\theta \ldots \pm \operatorname{cotg} n\theta}{N : \sqrt{D}}$$

wobei $\theta = \frac{\pi}{N}$, $N = \{\frac{1}{4}\} D$ gesetzt und für n alle zu D teilerfremden Zahlen genommen werden, mit dem wie oben bestimmten Vorzeichen*).

Für eine positive Determinante ist die Anzahl der Klassen**)

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \ldots)}{\log .T + U\sqrt{D}}$$

Dabei bezeichnen T, U die kleinsten Werte der Größen t, u, die der Gleichung $tt - Duu = 1$ genügen

$$= \frac{\log \sin \frac{1}{2}\theta \pm \log \sin \frac{3}{2}\theta \pm \log \sin \frac{5}{2}\theta \text{ usw.}}{\log T + U\sqrt{D}}$$

[VII.]

Bei einer negativen Determinante $-p$, die***) eine Primzahl der Form $4n+1$ ist, ist die Anzahl der Klassen†) $= (\alpha - \beta)$, wobei α die Anzahl der quadratischen Reste im ersten Viertel

$$1 \,.\, 2 \,.\, 3 \ldots . \tfrac{1}{4}(p-1)$$

und β die Anzahl der Nichtreste ist.

---

wobei das obere oder untere Vorzeichen zu nehmen ist, je nachdem die Zahl m ein Produkt aus einer geraden oder ungeraden Anzahl (gleicher oder ungleicher) Primzahlen ist; dagegen ist im Zähler der nachfolgenden Formel

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \ldots = \Sigma \left(\frac{-D}{m}\right) \frac{1}{m}$$

]

*) [Siehe die weiter unten folgende Anmerkung zu diesem Fragment.]

**) [In der nachfolgenden Formel bezeichnet D die positive Determinante, und es ist

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \ldots = \Sigma \left(\frac{D}{m}\right) \frac{1}{m}$$

]

***) [d. h. wenn p eine positive Primzahl der Form $4n+1$ ist.]

†) [die Anzahl der Klassen ist $= 2(\alpha - \beta)$.]

[VIII.]

$$b \equiv 2m + a - 1 \pmod 8$$

wobei m die [halbe] Anzahl der Klassen für die Determinante $-p$ ist

p	m	a	b	f	$\frac{2m+a-1-b}{8}$	α	β
17	2	+1	−4	−4	+1	3	2
41	4	+5	+4	+9	+1	3	4
73	2	−3	−8	+27	+1	1	6
89	6	+5	−8	+34	+3	9	2
97	2	+9	+4	+22	+1	5	6
113	4	−7	+8	+15	−1	9	4
137	4	−11	+4	+37	−1	3	8
193	2	−7	+12	+81	−2	11	6
233	6	+13	+8	+144	+2	15	2
241	6	+15	+4	+64	−1	13	6
257	8	+1	+16	+16	0	15	4
281	10	+5	−16	+53	+5	9	10
313	4	+13	−12	−25	+1	5	12
337	4	+9	+16	−148	0	7	12
353	8	+17	+8	+42	+3	15	8
5	.1	+1	+2	+2	0		
13	1	−3	−2	+5	0		
29	3	+5	+2	+12	+1		
37	1	+1	−6	−6	+1		
53	3	−7	−2	+23	0		
61	3	+5	−6	+11	+2		
101	7	+1	−10	−10	+3		
109	3	−3	+10	+33	−1		
149	7	−7	−10	+44	+2		
157	3	−11	−6	−28	0		
173	7	+13	+2	+80	+3		
181	5	+9	+10	−19	+1		
197	5	+1	−14	−14	+3		
229	5	−15	+2	−107	−1		
269	11	+13	+10	−82	+3		
277	3	+9	+14	−60	0		
293	9	+17	+2	+138	+4		
317	5	−11	+14	+114	−2		
349	7	+5	+18	−136	0		
373	5	−7	+18	+104	−2		
389	11	+17	−10	−115	+6		
397	3	−19	−6	+63	−1		

[IX.]

Verteilung der quadratischen Reste auf Achtel.

p eine Primzahl; (r) die Anzahl der quadratischen Reste von p, die zwischen $(r-1)\frac{p}{8}$ und $r\frac{p}{8}$ liegen.

Erster Fall; $p = 8n + 1$.

$2t$ Anzahl der Klassen für die Determinante $-p$;

$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = (8) = \tfrac{1}{4}(2n + t + u)$$
$$(2) = (4) = (5) = (7) = \tfrac{1}{4}(2n + t - u)$$
$$(3) = (6) = \tfrac{1}{4}(2n - 3t + u)$$

p	$2n$	t	u	(1)	(2)	(3)
17	4	2	2	2	1	0
41	10	4	2	4	3	0
73	18	2	8	7	3	5
89	22	6	4	8	6	2
97	24	2	10	9	4	7
113	28	4	4	9	7	5
137	34	4	6	11	8	7
193	48	2	10	15	10	13
233	58	6	4	17	15	11
241	60	6	10	19	14	13
257	64	8	8	20	16	12
281	70	10	4	21	19	11
313	78	4	18	25	16	21
337	84	4	12	25	19	21
353	88	8	12	27	21	19
401	100	10	6	29	26	19

Zweiter Fall; $p = 8n + 5$.

$2t$ Anzahl der Klassen für die Determinante $-p$;
$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = (3) = (6) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(2) = (7) = \tfrac{1}{4}(2n + 3t - u + 2)$$
$$(4) = (5) = \tfrac{1}{4}(2n - t - u + 2)$$

p	$2n$	t	u	(1)	(2)	(4)
5	0	1	1	0	1	0
13	2	1	3	1	1	0
29	6	3	1	1	4	1
37	8	1	5	3	2	1
53	12	3	3	3	5	2
61	14	3	5	4	5	2
101	24	7	3	5	11	4
109	26	3	5	7	8	5
149	36	7	3	8	14	7
157	38	3	13	12	9	6
173	42	7	5	10	15	8
181	44	5	9	12	13	8
197	58	5	5	12	15	10
229	56	5	13	16	15	10
269	66	11	5	15	24	13
277	68	3	11	19	17	14
293	72	9	9	18	23	14
317	78	5	7	20	22	17
349	86	7	13	23	24	17
373	92	5	13	25	24	19
389	96	11	7	23	31	20
397	98	3	21	29	22	19

Dritter Fall; $p = 8n + 3$.

t Anzahl der Klassen für die Determinante $-p$

$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = (4) = (7) = \tfrac{1}{4}(2n + t - u)$$
$$(2) = (5) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(3) = \tfrac{1}{4}(2n + t + u + 2)$$
$$(6) = \tfrac{1}{4}(2n - t - u + 2)$$

p	$2n$	t	u	(1)	(2)	(3)	(6)
3	0	1	1	0	0	1	0
11	2	3	1	1	0	2	0
19	4	3	3	1	1	3	0
43	10	3	5	2	3	5	1
59	14	9	3	5	2	7	1
67	16	3	7	3	5	7	2
83	20	9	5	6	4	9	2
107	26	9	3	8	5	10	4
131	32	15	3	11	5	13	4
139	34	9	7	9	8	13	5
163	40	3	11	8	12	14	7
179	44	15	3	14	8	16	7
211	52	9	5	14	12	17	10
227	56	15	7	16	12	20	9
251	62	21	7	19	12	23	9
283	70	9	15	16	19	24	12
307	76	9	17	17	21	26	13
331	82	9	11	20	21	26	16
347	86	15	5	24	19	27	17
379	94	9	11	23	24	29	19

Vierter Fall; $p = 8n + 7$.

t Anzahl der Klassen für die Determinante $-p$;
$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = \tfrac{1}{4}(2n + 2t - u)$$
$$(2) = (3) = (5) = \tfrac{1}{4}(2n + u + 2)$$
$$(4) = (6) = (7) = \tfrac{1}{4}(2n - u + 2)$$
$$(8) = \tfrac{1}{4}(2n - 2t + u)$$

p	$2n$	t	u	(1)	(2)	(4)	(8)
7	0	1	2	0	1	0	0
23	4	3	2	2	2	1	0
31	6	3	4	2	3	1	1
47	10	5	4	4	4	2	1
71	16	7	2	7	5	4	1
79	18	5	4	6	6	4	3
103	24	5	10	6	9	4	6
127	30	5	8	8	10	6	7
151	36	7	6	11	11	8	7
167	40	11	6	14	12	9	6
191	46	13	4	17	13	11	6
199	48	9	10	14	15	10	10
223	54	7	16	13	18	10	14
239	58	15	4	21	16	14	8
263	64	13	6	21	18	15	11
271	66	11	12	19	20	14	14
311	76	19	6	27	21	18	11
359	88	19	6	30	24	21	14
367	90	9	20	22	28	18	23
383	94	17	12	29	27	21	18

[X.]

Verteilung der quadratischen Reste auf Zwölftel.

p eine Primzahl; (r) die Anzahl der quadratischen Reste von p, die zwischen $\frac{r-1}{12}p$ und $\frac{r}{12}p$ liegen.

Erster Fall; $p = 24n + 1$.

$2t$ Anzahl der Klassen für die Determinante $-p$

$4u$ Anzahl der Klassen für die Determinante $-3p$

$$(1) = (12) = \tfrac{1}{6}(6n + 3t + 2u)$$
$$(2) = (4) = (6) = (7) = (9) = (11) = \tfrac{1}{6}(6n - 3t + 2u)$$
$$(3) = (5) = (8) = (10) = \tfrac{1}{6}(6n + 3t - 4u)$$

p	n	t	u	(1)	(2)	(3)
73	3	2	3	5	3	2
97	4	2	3	6	4	3
193	8	2	6	11	9	5
241	10	6	3	14	8	11

Zweiter Fall; $p = 24n + 13$.

$2t$ Anzahl der Klassen für die Determinante $-p$;

$4u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (3) = (10) = (12) = \tfrac{1}{2}(2n + 1 + t)$$
$$(2) = (6) = (7) = (1.1) = \tfrac{1}{2}(2n + 1 - t)$$
$$(4) = (9) = \tfrac{1}{2}(2n + 1 - t + 2u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 + t - 2u)$$

p	n	t	u	(1)	(2)	(4)	(5)
13	0	1	1	1	0	1	0
37	1	1	2	2	1	3	0
61	2	3	2	4	1	3	2
109	4	3	3	6	3	6	3
157	6	3	4	8	5	9	4
181	7	5	3	10	5	8	7
229	9	5	3	12	7	10	9

Dritter Fall; $p = 24n + 5$.

$2t$ Anzahl der Klassen für die Determinante $-p$;
$2u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (2) = (6) = (7) = (11) = (12) = n$$
$$(3) = (10) = \tfrac{1}{2}(2n + 1 + t)$$
$$(4) = (9) = \tfrac{1}{2}(2n - t + u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 - u)$$

p	n	t	u	(1)	(3)	(4)	(5)
5	0	1	1	0	1	0	0
29	1	3	3	1	3	1	0
53	2	3	5	2	4	3	0
101	4	7	5	4	8	3	2
149	6	7	7	6	10	6	3
173	7	7	9	7	11	8	3
197	8	5	11	8	11	11	3
269	11	11	7	11	17	9	8

Vierter Fall; $p = 24n + 17$.

$2t$ Anzahl der Klassen für die Determinante $-p$;
$2u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (2) = (6) = (7) = (11) = (12) = \tfrac{1}{6}(6n + 3 + u)$$
$$(3) = (10) = \tfrac{1}{6}(6n + 6 + 3t - 2u)$$
$$(4) = (9) = \tfrac{1}{6}(6n + 3 - 3t + u)$$
$$(5) = (8) = \tfrac{1}{6}(6n + 6 - 2u)$$

p	n	t	u	(1)	(3)	(4)	(5)
17	0	2	3	1	1	0	0
41	1	4	3	2	3	0	1
89	3	6	3	4	6	1	3
113	4	4	9	6	4	4	2
137	5	4	9	7	5	5	3
233	9	6	15	12	8	9	5
257	10	8	9	12	12	8	8

Bemerkungen zur Abhandlung

Über den Zusammenhang zwischen der Anzahl der Klassen, in die binäre quadratische Formen zerfallen, und ihrer Determinante.

Zu I. und II.

Die zweite Formel für die Anzahl der Punkte innerhalb des Kreises (I, Artikel 3, und II, Artikel 5) ergibt sich aus der Betrachtung des in den Kreis eingeschriebenen Quadrats, dessen Seiten parallel zu den Koordinatenachsen sind; der Vergleich beider Formeln führt zu dem auch arithmetisch leicht zu beweisenden Satz

$$r' + r'' + \ldots + r^{(q)} = qq + r^{(q+1)} + r^{(q+2)} + \ldots + r^{(r)}$$

aus dem sich wiederum die Richtigkeit der ersten der beiden folgenden Regeln ergibt, die sich auf einem besonderen Blatt vorfanden:

„Auflösungen der Gleichung $xx + yy \leqq A$; Formel

$$1 + 4\sqrt{A} + 4\sqrt{\tfrac{1}{2}A} + 8\Sigma(\sqrt{(A - nn)} - n)$$

wobei bei jeder Wurzel der Bruchteil weggelassen und von $n = 1$ bis $n = \sqrt{A}$ „(soll heißen $\sqrt{\frac{1}{2}A}$)“ summiert wird.

Andere Formel

$$1 + 4\{A - \tfrac{A}{3} + \tfrac{A}{5} - \tfrac{A}{7} + \tfrac{A}{9} - \tfrac{A}{11} \ldots\}$$

wobei bei jedem Glied der Bruchteil weggelassen wird.“

Diese letztere Formel folgt aus dem später (I, Artikel 6) angewandten Satz über die Anzahl aller verschiedenen Darstellungen einer bestimmten Zahl durch die Form $xx + yy$ (vgl. Disqq. Arithm., Artikel 182, Anmerkung). Er lässt sich leicht folgendermaßen umformen: Die Anzahl der verschiedenen Darstellungen einer positiven ganzen Zahl m durch die Form $xx+yy$ ist $= 4(a-b)$, wobei a, b die Anzahlen der Teiler von m bezeichnen, die jeweils die Form $4n + 1$, $4n + 3$ haben. Aus dem Vergleich dieser arithmetischen Formel mit der (in I, Artikel 5, oder II, Artikel 4) durch geometrische Betrachtungen gewonnenen mittleren Darstellungsanzahl erhält man leicht und in aller Strenge das bekannte Ergebnis

$$\frac{\pi}{4} = 1 - \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{7} + \ldots$$

das in der Abhandlung (I, Artikel 7) durch einen ähnlichen Vergleich, aber mithilfe unendlicher Produkte hergeleitet wird.

Zu III und IV.

Ist C die Gesamtheit aller positiven, nicht eigentlich äquivalenten, eigentlich primitiven Formen mit negativem Determinanten $-D$, und weist man den Variablen jeder dieser Formen zwei zueinander teilerfremde Werte zu, so ist die Anzahl aller Darstellungen einer positiven ganzen Zahl m gleich $\epsilon\psi(m)$. Dabei bezeichnet ϵ die Anzahl der Lösungen der Gleichung $tt + Duu = 1$ und $\psi(m)$ die Anzahl derjenigen Wurzeln n der Kongruenz $nn + D \equiv 0 \pmod{m}$, für die die drei Zahlen $m,\ 2n$ und $\frac{nn+D}{m}$ keinen gemeinsamen Teiler haben (Disqq. Arithm., Art. 180). Für den Faktor gilt $\epsilon = 4$ für $D = 1$, in allen anderen Fällen $= 2$. Ist ferner $m = p^\pi p'^{\pi'} p''^{\pi''} \ldots$, wobei $p, p', p'' \ldots$ verschiedene Primzahlen sind, so ist $\psi(m) = \psi(p^\pi)\psi(p'^{\pi'})\psi(p''^{\pi''})\ldots$; bezeichnet $\mathfrak{A}(m)$ die Anzahl der Wurzeln n der Kongruenz $nn + D \equiv 0 \pmod{m}$, und verwendet man das von Legendre eingeführte und von Jacobi verallgemeinerte Zeichen, so ist $\psi(p^\pi) = \mathfrak{A}(p^\pi) = 1 + \left(\frac{-D}{p}\right)$, wenn p kein Teiler von $2D$ ist, andernfalls aber $= \mathfrak{A}(p^\pi - \frac{1}{p}\mathfrak{A}(p^{\pi+1})$; die Anzahl $\mathfrak{A}(p^\pi)$ lässt sich stets leicht bestimmen (Disqq. Arithm., Art. 104). Für das Folgende genügt jedoch die Bemerkung, dass $\mathfrak{A}(p^\pi)$ stets von π unabhängig wird, sobald π eine gewisse Größe überschreitet.

Weist man den Variablen der in der Gesamtheit C enthaltenen Formen ausnahmslos alle ganzzahligen Werte zu (Disqq. Arithm., Art. 181), so wird die Anzahl (m) aller Darstellungen der Zahl m gleich $\epsilon f(m)$, wobei $f(m) = \Sigma\psi\left(\frac{m}{\mu\mu}\right)$ ist und die Summe über alle quadratischen Teiler $\mu\mu$ der Zahl m zu bilden ist. Daraus folgt unmittelbar

$$f(m) = f(p^\pi p'^{\pi'} p''^{\pi''} \ldots) = f(p^\pi) f(p'^{\pi'}) f(p''^{\pi''}) \ldots$$

und

$$f(p^\pi) = \psi(p^\pi) + \psi(p^{\pi-2}) + \psi(p^{\pi-4}) + \ldots$$

wobei die Reihe so lange fortzusetzen ist, wie die Exponenten $\pi,\ \pi-2,\ \pi-4\ldots$ nicht negativ werden. Wenn p kein Teiler von $2D$ ist, folgt daraus

$$f(p^\pi) = 1 + \left(\frac{-D}{p}\right) + \left(\frac{-D}{pp}\right) + \ldots + \left(\frac{-D}{p^\pi}\right)$$

und allgemein, wenn m zu $2D$ teilerfremd ist,

$$f(m) = \Sigma\left(\frac{-D}{n}\right)$$

wobei die Summe über alle Teiler n der Zahl m zu bilden ist.

Aus diesen Bemerkungen ergibt sich unmittelbar die Richtigkeit der im Text (III, 1, 2, 3) aufgestellten Sätze über die Anzahl (m), wenn man beim ersten noch die Bedingung hinzufügt, dass D nicht durch pp teilbar sein darf (die Bestimmung der Klassenanzahl ist schon in den Disqq. Arithm., Art. 256, auf den Fall zurückgeführt, in dem D durch kein Quadrat teilbar ist). Zugleich findet man auch ohne diese Einschränkung, dass die unendliche Reihe

$$1 + \frac{f(p)}{p} + \frac{f(pp)}{pp} + \frac{f(p^3)}{p^3} + \dots$$

den Wert

$$\frac{1}{1 - \frac{1}{p}} \quad \text{oder} \quad \frac{1}{1 - .\frac{1}{p}} \cdot \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

hat, je nachdem, ob $2D$ durch die Primzahl p teilbar oder nicht teilbar ist.

Zu V.

Die Bemerkung zu Formel III zeigt, auf welchem Weg der Verfasser die Anzahl k der in der Gesamtheit C enthaltenen Formen bestimmt hat. Aus geometrischen Betrachtungen (vgl. I, Art. 5, und II, Art. 4) ergibt sich, dass der Grenzwert, dem sich der Quotient

$$\frac{(1) + (2) + (3) + \dots + (m)}{m}$$

bei unbegrenzt wachsendem m nähert, also die mittlere Anzahl der Darstellungen einer unbestimmten positiven ganzen Zahl,

$$= k\frac{\pi}{\sqrt{D}}$$

ist. Ein zweiter Ausdruck für denselben Grenzwert lässt sich auf verschiedene Arten aus der Beschaffenheit der zuvor bestimmten Anzahl $(m) = \epsilon f(m)$ der Darstellungen der Zahl m ableiten. Nach den erhaltenen Bruchstücken (I, Art. 7, 8; III und IV) scheint der Verfasser dabei zunächst den folgenden Weg eingeschlagen zu haben.

Ist $\theta(m)$ eine beliebige Funktion der positiven ganzen Zahl m und p eine beliebige Primzahl, so lässt sich aus $\theta(m)$ stets eine neue Funktion $\theta'(m)$ ableiten, deren Wert unabhängig davon ist, ob und wie oft p als Faktor in m enthalten ist, und die für alle nicht durch p teilbaren Zahlen m mit $\theta(m)$ übereinstimmt. Man erhält eine solche Funktion, indem man $\theta'(m) = \theta\left(\frac{m}{p^\pi}\right)$ setzt, wobei p^π die höchste in m aufgehende Potenz von p bezeichnet; man kann sagen, dass die Funktion $\theta'(m)$ aus $\theta(m)$ durch Elimination der Primzahl p entsteht. Bildet man auf diese Weise aus $f(m)$ eine neue Funktion $f'(m)$ durch

Elimination der Primzahl 2, daraus die Funktion $f''(m)$ durch Elimination von 3 und so weiter, so verläuft jede folgende Funktion regelmäßiger als die vorhergehenden. Eliminiert man die Primzahlen nacheinander in aufsteigender Reihenfolge, so hat eine solche Funktion $\theta(m)$ für unendlich viele Werte von m den Wert $f(1) = 1$, insbesondere für alle Werte von m, die kleiner als die zuletzt eliminierte Primzahl sind. Durch unendliche Fortsetzung dieses Verfahrens nähert man sich immer mehr der Funktion $f^{\infty}(m)$, die für alle Werte von m den Wert 1 hat und deren mittlerer Wert folglich ebenfalls $= 1$ ist. Gelingt es nun, den mittleren Wert einer Funktion $\theta(m)$ durch denjenigen der nächstfolgenden $\theta'(m)$ auszudrücken, so lässt sich auch der mittlere Wert der Funktion $f(m)$ durch eine unendliche Kette von Operationen finden.

Ist p die Primzahl, durch deren Elimination $\theta'(m)$ aus $\theta(m)$ entsteht, so ist $\theta(m) = \theta'(m)f(p^{\pi})$, wobei p^{π} wieder die höchste in m aufgehende Potenz von p bezeichnet. Wenn p kein Teiler von $2D$ ist, findet man daraus leicht

$$\theta'(m) = \theta(mp) - \left(\frac{-D}{p}\right)\theta(m)$$

Setzt man zur Abkürzung

$$\Theta(m) = \theta(1) + \theta(2) + \ldots + \theta(m)$$
$$\Theta'(m) = \theta'(1) + \theta'(2) + \ldots + \theta(m)$$

so ergibt sich

$$\Theta'(mp) = \Theta(mp) - \left(\frac{-D}{p}\right)\Theta(m)$$

und daraus, wenn ω, ω' die jeweiligen mittleren Werte der Funktionen $\theta(m), \theta'(m)$ bezeichnen,

$$\omega = \frac{\omega'}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

Wenn dagegen die Primzahl p ein Teiler von $2D$ ist, besteht zwischen den Funktionen $\theta(m)$ und $\theta'(m)$ im Allgemeinen keine so einfache Beziehung mehr; auf ähnliche Weise ergibt sich jedoch leicht, dass in diesem Fall $\omega = \omega'$ ist. Die Beziehung zwischen ω und ω' lässt sich in beiden Fällen auch auf folgendem Weg ableiten. Setzt man

$$\vartheta(m) = \Sigma\theta(\mu)$$

wobei die Summe über alle Zahlen μ zu bilden ist, die nicht durch p teilbar und zudem nicht größer als m sind, und bezeichnet man mit $m', m'', m''' \ldots$ die jeweiligen größten in $\frac{m}{p}, \frac{m'}{p}, \frac{m''}{p} \ldots$ enthaltenen ganzen Zahlen, so ist

$$\Theta(m) = \vartheta(m) + \vartheta(m')f(p) + \vartheta(m'')f(pp) + \vartheta(m''')f(p^3) + \ldots$$
$$\Theta'(m) = \vartheta(m) + \vartheta(m') + \vartheta(m'') + \vartheta(m''') + \ldots$$

und daraus folgt

$$\frac{\omega}{\omega'} = (1 - \tfrac{1}{p})\{1 + \frac{f(p)}{p} + \frac{f(pp)}{pp} + \frac{f(p^3)}{p^8} + \ldots\}$$

in Übereinstimmung mit dem oben gefundenen Ergebnis (vgl. die Note zu III und IV).

Der mittlere Wert der Funktion $f(m)$ ist daher gleich dem unendlichen Produkt

$$\Pi \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

in dem p alle Primzahlen durchlaufen muss, die keine Teiler von $2D$ sind; daraus folgt

$$k = \frac{\epsilon\sqrt{D}}{\pi} \Pi \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

Hinsichtlich der Strenge dieser Herleitung bleibt jedoch ein Bedenken gegen die Methode, den mittleren Wert der Funktion $f(m)$ durch schrittweise Elimination aller Primzahlen zu bestimmen. Zwar ist ersichtlich, dass die durch Elimination der ersten n Primzahlen erhaltene Funktion $f^{(n)}(m)$ im Wert mit der Funktion $f^{\infty}(m) = 1$ übereinstimmt, solange m kleiner als die zuletzt eliminierte Primzahl bleibt. Durch hinreichend große Wahl von n lässt sich diese Übereinstimmung somit bis zu jeder vorgegebenen Größe der Zahl m erreichen. Damit allein ist aber keineswegs bewiesen, dass sich bei unbegrenzt wachsendem n der mittlere Wert von $f^{(n)}(m)$ dem mittleren Wert von $f^{\infty}(m)$, also dem Wert 1, unbegrenzt nähert. Wie der Verfasser diese Lücke ausfüllen wollte, lässt sich aus den erhaltenen Papieren nicht mit Sicherheit erkennen. Doch führt die schon oben (in der Note zu I) mitgeteilte Formel

$$1 + 4\{A - \frac{A}{3} + \frac{A}{5} - \frac{A}{7} + \frac{A}{9} - \frac{A}{11} \ldots\}$$

für die Anzahl der Zahlenpaare, deren Quadratsumme den Wert A nicht übersteigt, zu der Vermutung, dass der Verfasser unter Umgehung des unendlichen Produkts für den mittleren Wert der Funktion $f(m)$ unmittelbar die unendliche Reihe

$$\Sigma \left(\frac{-D}{n}\right)\frac{1}{n}$$

gefunden hat. Dabei muss n der Größe nach alle positiven ganzen Zahlen durchlaufen, die zu $2D$ teilerfremd sind. Die einfachste Art, diesen Übergang anzudeuten, scheint die folgende zu sein.

Ist μ der größte unter den Teilern einer Zahl m, die zu $2D$ teilerfremd sind, und setzt man $\theta(m) = f(\mu)$, so ist $\theta(m)$ die Funktion, die durch Elimination aller in $2D$ aufgehenden Primzahlen aus $f(m)$ entsteht und deren mittlerer Wert nach dem Obigen mit demjenigen von $f(m)$ übereinstimmt. Da nun $\theta(m) = \Sigma\left(\frac{-D}{n}\right)$ ist, wobei n alle Teiler von μ, also alle Teiler von m, die zu $2D$ teilerfremd sind, durchläuft, ergibt sich die zur obigen analoge Formel

$$\Theta(m) = \theta(1) + \theta(2) + \ldots + \theta(m) = \Sigma\left(\frac{-D}{n}\right)\frac{m}{n}$$

wobei in der rechten Summe der Buchstabe n alle zu $2D$ teilerfremden Zahlen durchläuft und vom Quotienten $\frac{m}{n}$ stets nur die größte in ihm enthaltene ganze Zahl zu nehmen ist. Ordnet man die Glieder dieser Reihe nach wachsenden Zahlen n, so nimmt der Faktor $\frac{m}{n}$ fortwährend ab oder zumindest nie zu, und die Reihe bricht ab, sobald $n > m$ wird. Außerdem folgt aus dem Fundamentaltheorem der Theorie der quadratischen Reste und seiner Verallgemeinerung, dass die Summe von jeweils $\varphi(4D)$ aufeinanderfolgenden Werten des Faktors $\left(\frac{-D}{n}\right)$ verschwindet. Daraus ergibt sich, dass die Summe beliebig vieler aufeinanderfolgender Werte dieses Faktors ihrem absoluten Wert nach niemals die endliche, nur vom Determinanten D abhängige Größe $\Delta = \varphi(2D)$ übersteigt. Verbindet man diese beiden Bemerkungen, so findet man leicht, dass die Summe aller auf das Glied $\left(\frac{-D}{n}\right)\frac{m}{n}$ folgenden Glieder dem absoluten Wert nach kleiner als $\Delta\frac{m}{n}$ ist und folglich der Quotient $\Theta(m) : m$ bei unendlich wachsendem m die in der angegebenen Weise geordnete, konvergierende unendliche Reihe

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$$

zum Grenzwert hat. Nachdem so der gemeinsame mittlere Wert der Funktionen $\theta(m)$ und $f(m)$ gefunden ist, erhält man unmittelbar

$$k = \frac{\epsilon\sqrt{D}}{\pi}\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$$

Ferner ist zu bemerken, dass die Artikel 6 und 8 der Abhandlung II auf eine in mancher Hinsicht einfachere und auch leicht durchführbare Behandlung des Problems hinweisen, bei der nur Darstellungen ungerader Zahlen oder sogar nur solcher Zahlen betrachtet werden, die zu $2D$ teilerfremd sind.

Zu VI und VII.

Wie der Verfasser die Reihe $\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$ summiert hat, geht aus einigen besonderen Beispielen hervor, die sich auf einzelnen Blättern finden.

Ist $D \equiv 3 \pmod 4$, so folgt aus dem Fundamentaltheorem der Theorie der quadratischen Reste unter Verwendung der Reihe

$$\operatorname{cotang} u = \frac{1}{u} + \frac{1}{u-\pi} + \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} + \dots$$

dass

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \Sigma\left(\frac{n}{D}\right)\frac{1}{n} = \frac{\pi}{2D}\Sigma\left(\frac{\nu}{D}\right)\operatorname{cotang}\frac{\nu\pi}{2D}$$

ist, wobei ν alle zu $2D$ teilerfremden Zahlen durchläuft, die kleiner als D sind. Setzt man

$$\sqrt{-1} = i, \quad \cos\frac{2\pi}{D} + i\sin\frac{2\pi}{D} = r$$

und bezeichnet mit μ alle zu D teilerfremden Zahlen, die nicht größer als D sind, so lässt sich die vorstehende Summe leicht umformen zu

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\Sigma\left(\frac{\mu}{D}\right)\frac{r^\mu - 1}{r^\mu + 1}$$

Wendet man nun die für jede Wurzel ω der Gleichung $\omega^D = 1$ gültige Formel

$$\frac{\omega - 1}{\omega + 1} = \Sigma(-1)^{\alpha-1}\omega^\alpha$$

an, in der α die Zahlen $1, 2, 3 \dots (D-1)$ durchlaufen muss, so erhält man durch Umkehrung der Summationsreihenfolge

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\Sigma(-1)^{\alpha-1}\Sigma\left(\frac{\mu}{D}\right)r^{\alpha\mu}$$

Die Summation über μ lässt sich bekanntlich mithilfe der in der Abhandlung *Summatio quarundam serierum singularium* bewiesenen Sätze ausführen.

Beschränkt man sich auf den Fall, in dem D durch kein Quadrat teilbar ist, so findet man allgemein

$$\Sigma\left(\frac{\mu}{D}\right) r^{\alpha\mu} = \left(\frac{\alpha}{D}\right) i^{\left(\frac{D-1}{2}\right)^2} \sqrt{D}$$

wobei $\left(\frac{\alpha}{D}\right) = 0$ zu setzen ist, wenn α nicht zu D teilerfremd ist. Im Fall $D \equiv 3 \pmod 4$ erhält man daher

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{4\sqrt{D}}\left(\frac{2}{D}\right)\Sigma(-1)^{\alpha}\left(\frac{\alpha}{D}\right) = \frac{\pi}{2\sqrt{D}}\Sigma\left(\frac{\alpha'}{D}\right)$$

wobei α' alle zu D teilerfremden Zahlen durchläuft, die kleiner als $\frac{1}{2}D$ sind. Da schließlich $\epsilon = 2$ ist, wird die Klassenanzahl

$$k = \Sigma\left(\frac{\alpha'}{D}\right)$$

Ist dagegen $D \equiv 1 \pmod 4$, so erhält man unter Verwendung der Reihe

$$\operatorname{cosec} u = \frac{1}{u} - \frac{1}{u-\pi} - \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} - \dots$$

auf ähnliche Weise

$$\begin{aligned}\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} &= \Sigma(-1)^{\frac{n-1}{2}}\left(\frac{n}{D}\right)\frac{1}{n} = \frac{\pi}{2D}\Sigma(-1)^{\frac{\nu-1}{2}}\left(\frac{\nu}{D}\right)\operatorname{cosec}\frac{\nu\pi}{2D} \\ &= \frac{\pi}{2D}\Sigma\left(\frac{\mu}{D}\right)\frac{r^{\mu}}{r^{2\mu}+1}\end{aligned}$$

wobei die Buchstaben ν und μ ihre frühere Bedeutung haben. Schließt man den offensichtlichen Fall $D = 1$ aus und wendet die für jede Wurzel ω der Gleichung $\omega^D = 1$ (außer $\omega = 1$) gültige Formel

$$\frac{\omega}{\omega\omega + 1} = 1 + \Sigma\omega^{4\alpha''} + \Sigma\omega^{D-4\alpha''}$$

an, in der α'' die Zahlen $1, 2, 3 \dots \frac{1}{4}(D-1)$ durchlaufen muss, so ergibt sich, wieder unter der Einschränkung, dass D durch kein Quadrat teilbar ist,

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{\sqrt{D}}\Sigma\left(\frac{\alpha''}{D}\right)$$

und daraus, da $\epsilon = 2$ ist,

$$k = 2\Sigma\left(\frac{\alpha''}{D}\right)$$

Die Fälle, in denen D gerade ist, ließen sich ganz ähnlich behandeln. —

Zur Bestimmung der Klassenanzahl für *positive* Determinanten D finden sich außer der im Text mitgeteilten Schlussformel nur einzelne geometrische Figuren. Sie stellen Hyperbelsektoren endlicher Ausdehnung dar; daneben stehen Ungleichungen, die die Punkte, deren Koordinaten die Variablen der quadratischen Formen sind, auf das Innere eines solchen Hyperbelsektors beschränken. Diese Hyperbelsektoren treten an die Stelle der Ellipsen, die den quadratischen Formen mit negativen Determinanten entsprechen. Durch die Bestimmung ihrer Flächeninhalte ergibt sich wiederum die mittlere Darstellungsanzahl, sofern nur Darstellungen zugelassen werden, deren Variablen die erwähnten Ungleichungen erfüllen. Andererseits dienen diese Ungleichungen dazu, aus den unendlich vielen Darstellungen einer Zahl m, die alle zu ein und derselben Wurzel n der Kongruenz $nn - D \equiv 0 \pmod{\frac{m}{\mu\mu}}$ gehören und sämtlichen Lösungen der Gleichung $tt - Duu = 1$ entsprechen (vgl. Disqq. Arithm., Art. 205), eine einzige herauszugreifen und alle anderen auszuschließen. Die Anzahl aller zugelassenen Darstellungen der Zahl m durch die Gesamtheit aller nicht eigentlich äquivalenten, eigentlich primitiven Formen ist dann gleich dem Wert der Funktion $f(m)$, in der nur $-D$ durch D zu ersetzen ist. Aus ihren Eigenschaften ergibt sich wie zuvor bei negativen Determinanten ein zweiter Ausdruck für die mittlere Darstellungsanzahl; der Vergleich mit dem zuvor geometrisch abgeleiteten Wert führt dann unmittelbar zur Bestimmung der Klassenanzahl.

Zu VIII.

Hier bezeichnet p eine positive Primzahl der Form $4n+1$; die Bezeichnung stimmt mit der in der Abhandlung *Theoria residuorum biquadraticorum* I, Art. 23, verwendeten überein. Es gilt also

$$f \equiv 1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, \tfrac{1}{2}(p-3) \,.\, \tfrac{1}{2}(p-1) \pmod{p}$$
$$p = aa + bb; \quad a \equiv 1 \pmod{4}; \quad b \equiv af \pmod{p}$$

Die mit α, β bezeichneten Zahlen sind durch die Zerlegung $p = \alpha\alpha + 2\beta\beta$ bestimmt. Die Spalte f ist den beiden vorgefundenen Tabellen hinzugefügt worden; außerdem wurden einige Lücken darin ausgefüllt.

Der im Text aufgestellte Satz hängt mit dem biquadratischen Charakter der Zahl 2 zusammen. Da nämlich (vgl. *Theoria resid. biqu.* I, Art. 21)

$$2^{\frac{p-1}{4}} \equiv f^{\frac{1}{2}b} \pmod{p}$$

gilt, folgt aus der Kongruenz

$$b \equiv 2m + a - 1 \pmod{8}$$

die andere Kongruenz

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}$$

und umgekehrt die erste aus der zweiten. Die zweite Kongruenz lässt sich leicht folgendermaßen beweisen. Ist μ die Anzahl der quadratischen Reste α_1 zwischen 0 und $\frac{1}{4}p$, so ist nach VII

$$m = 2\mu - \tfrac{1}{4}(p-1)$$

und die Anzahl der quadratischen Reste α_2 zwischen $\frac{1}{4}p$ und $\frac{1}{2}p$ ist $= \frac{1}{4}(p-1) - \mu$. Ist nun $p \equiv 1 \pmod{8}$, also die Zahl 2 ein quadratischer Rest, so bilden die Zahlen $2\alpha_1$ und $p - 2\alpha_2$ zusammen dieselbe Gesamtheit wie die Zahlen α_1 und α_2. Bezeichnet man das Produkt dieser Zahlen mit A, ergibt sich

$$2^{\frac{p-1}{4}} A \equiv (-1)^{\frac{1}{4}(p-1)-\mu} A \pmod{p}$$

und folglich

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu} \equiv f^{2\mu} \equiv f^{m+\frac{1}{4}(p-1)} \pmod{p}$$

Da ferner in diesem Fall $b \equiv 0 \pmod{4}$ und somit

$$\frac{p-1}{4} = (a+1)\frac{a-1}{4} + \frac{bb}{4} \equiv 2\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod{4}$$

gilt, erhält man die zu beweisende Kongruenz

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}$$

Ist dagegen $p \equiv 5 \pmod 8$, also die Zahl 2 ein quadratischer Nichtrest, so stimmen die Zahlen $2\alpha_1$ und $p-2\alpha_2$ mit sämtlichen quadratischen Nichtresten zwischen 0 und $\frac{1}{2}p$ überein. Bezeichnet man ihr Produkt mit B und das Produkt der Zahlen α_1 und α_2 wieder mit A, so ist

$$f \equiv AB, \quad (-1)^{\frac{p-1}{4}-\mu} 2^{\frac{p-1}{4}} A \equiv B \pmod p$$

Quadriert man diese beiden Kongruenzen und berücksichtigt dabei, dass

$$ff \equiv -1, \quad 2^{\frac{p-1}{2}} \equiv -1 \pmod p$$

ist, erhält man

$$-1 \equiv AABB, \quad -AA \equiv BB$$

und daraus $A^4 \equiv +1$. Da nun A ein Produkt quadratischer Reste ist, ist AA ein Produkt biquadratischer Reste und somit selbst ein biquadratischer Rest. Daher muss $AA \equiv +1$ sein, weil -1 ein biquadratischer Nichtrest ist. Daraus folgt

$$(-1)^{\frac{p-1}{4}-\mu} 2^{\frac{p-1}{4}} \equiv AB \equiv f \pmod p$$

und

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu-1} f \equiv f^{2\mu-1} \equiv f^{m+\frac{p-5}{4}} \pmod p$$

Da schließlich in diesem Fall $b \equiv 2 \pmod 4$ und folglich

$$\frac{p-5}{4} = (a+1)\frac{a-1}{4} + \frac{bb-4}{4} \equiv 2\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod 4$$

gilt, erhält man wiederum die zu beweisende Kongruenz

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod p$$

Zu IX.

Es sei p eine positive ungerade Zahl, die durch kein Quadrat teilbar ist, und

$$S_r = \Sigma\left(\frac{s_r}{p}\right)$$

wobei s_r alle zu p teilerfremden Zahlen durchlaufen muss, die zwischen $(r-1)\frac{p}{8}$ und $r\frac{p}{8}$ liegen. Bezeichnet man die Anzahlen der nicht eigentlich äquivalenten, eigentlich primitiven Formen für die Determinanten $-p$ und $-2p$ mit C_1 beziehungsweise C_2, so ist (vgl. DIRICHLET, Recherches sur diverses applications etc., § 11, in CRELLE's Journal XXI)

$$C_1 = 2(S_1 + S_2), \quad C_2 = 2(S_1 - S_4)$$

oder

$$C_1 = S_1 + S_2 + S_3 + S_4, \quad C_2 = 2(S_2 + S_3)$$

je nachdem, ob $p \equiv 1$ oder $\equiv 3 \pmod 4$ ist. Ferner bilden die Zahlen s_1 und s_2 zusammen dieselbe Gesamtheit wie die Zahlen $2s_1$ und $p - 2s_4$, ebenso die Zahlen s_3 und s_4 dieselbe Gesamtheit wie die Zahlen $2s_2$ und $p - 2s_3$. Im Fall $p \equiv 1 \pmod 4$ ist die Summe $S_1 + S_2 + S_3 + S_4 = 0$. Daraus ergeben sich in beiden Fällen zwei weitere Beziehungen zwischen den vier Summen S_1, S_2, S_3, S_4, sodass jede durch C_1 und C_2 ausgedrückt werden kann. Auf diese Weise erhält man, wenn $p \equiv 1 \pmod 4$ ist,

$$S_1 = S_8 = \tfrac{1}{4}\left(\frac{2}{p}\right) C_1 + \tfrac{1}{4}C_2$$

$$S_2 = S_7 = \tfrac{1}{4}\left(2 - \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

$$S_3 = S_6 = -\tfrac{1}{4}\left(2 + \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_4 = S_5 = \tfrac{1}{4}\left(\frac{2}{p}\right) C_1 - \tfrac{1}{4}C_2$$

und, wenn $p \equiv 3 \pmod 4$ ist,

$$S_1 = -S_8 = \tfrac{1}{4}\left(3 + \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

$$S_2 = -S_7 = -\tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_3 = -S_6 = \tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_4 = -S_5 = \tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

Ist p eine Primzahl, so folgen daraus unmittelbar die im Text angegebenen Formeln für die Anzahl der quadratischen Reste in den einzelnen Achteln.

Zu X.

Es sei p eine positive Zahl der Form $6n \pm 1$, die durch kein Quadrat teilbar ist, und

$$S_r = \Sigma \left(\frac{s_r}{p} \right)$$

wobei s_r alle zu p teilerfremden Zahlen durchlaufen muss, die zwischen $(r-1)\frac{p}{12}$ und $r\frac{p}{12}$ liegen. Bezeichnet man die Anzahlen der nicht eigentlich äquivalenten, eigentlich primitiven Formen für die Determinanten $-p$ und $-3p$ mit C_1, C_3, so findet man leicht (vgl. DIRICHLET, Recherches etc., § 11, oder die Note zu VI und VII)

$$C_1 = 2(S_1 + S_2 + S_3), \quad C_3 = 2(S_1 + S_2 - S_5 - S_6)$$

oder

$$C_1 = S_1 + S_2 + S_3 + S_4 + S_5 + S_6, \quad C_3 = 2(S_2 + S_3 + S_4 + S_5)$$

je nachdem, ob $p \equiv 1$ oder $\equiv 3 \pmod 4$ ist. Berücksichtigt man außerdem, dass

die	Zahlen	s_1 und s_2	mit	den	Zahlen	$2s_1$ und $p - 2s_6$
„	„	s_3 und s_4	„	„	„	$2s_2$ und $p - 2s_5$
„	„	s_5 und s_6	„	„	„	$2s_3$ und $p - 2s_4$

und ebenso

die	Zahlen	s_1, s_2, s_3	mit	den	Zahlen	$3s_1,\ 3s_5 - p,\ p - 3s_4$
„	„	s_4, s_5, s_6	„	„	„	$3s_2,\ 3s_6 - p,\ p - 3s_3$

übereinstimmen und dass im Fall $p \equiv 1 \pmod 4$ die Summe $S_1 + S_2 + S_3 + S_4 + S_5 + S_6 = 0$ ist, so erhält man neben den beiden obigen vier weitere Beziehungen zwischen den sechs Summen $S_1, S_2 \ldots S_6$, sodass alle aus C_1 und C_3 bestimmt werden können. Auf diese Weise erhält man, wenn $p \equiv 1 \pmod 4$ ist,

$$S_1 = S_{12} = \tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_2 = S_{11} = -\tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_3 = S_{10} = \tfrac{1}{2} C_1 - \tfrac{1}{6}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_4 = S_9 = -\tfrac{1}{2} C_1 - \tfrac{1}{6}\left(2 - \left(\frac{2}{p}\right)\right) C_3$$

$$S_5 = S_8 = \tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 - \tfrac{1}{12}\left(5 - \left(\frac{2}{p}\right)\right) C_3$$

$$S_6 = S_7 = -\tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

und, wenn $p \equiv 3 \pmod 4$ ist,

$$
\begin{aligned}
S_1 = -S_{12} &= \tfrac{1}{12}\left(9 + 3\left(\frac{2}{p}\right) - \left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1 - \tfrac{1}{4} C_3 \\
S_2 = -S_{11} &= \tfrac{1}{4}\left(-1 + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1 + \tfrac{1}{4} C_3 \\
S_3 = -S_{10} &= \tfrac{1}{6}\left(-\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1 \\
S_4 = -S_9 &= \tfrac{1}{6}\left(3 - 2\left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1 \\
S_5 = -S_8 &= \tfrac{1}{4}\left(-1 - \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1 + \tfrac{1}{4} C_3 \\
S_6 = -S_7 &= \tfrac{1}{12}\left(3 - 3\left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1 - \tfrac{1}{4} C_3
\end{aligned}
$$

Ist p eine Primzahl, so folgen aus dem ersten System die im Text angegebenen Formeln; für die anderen Fälle erhält man ähnliche Formeln aus dem zweiten System.

R. Dedekind.

GEOMETRISCHE SEITE DER TERNÄREN FORMEN.

Ein Punkt im Raum (0) werde als Anfangspunkt gewählt. Der Übergang von da zu drei anderen Punkten P, P', P'', die mit jenem nicht in einer Ebene liegen, sei jeweils t, t', t''; wobei, wenn keine Verwechslung möglich ist, die Punkte P, P', P'' selbst durch (t). (t'), (t'') bezeichnet werden können.

Ferner sei allgemein (t, t') das Produkt der Längen der beiden Linien t, t' mit dem Kosinus ihres Neigungswinkels usw.

Man hat allgemein $(\alpha t + \alpha' t' + \alpha'' t'' + \ldots \quad \beta u + \beta' u' + \beta'' u'' + \ldots)$ wenn man die Multiplikation

$$(\alpha t + \alpha' t' + \alpha'' t'' + \ldots) \times (\beta u + \beta' u' + \beta'' u'' + \ldots)$$

ausführt und statt $tu, tu', tu'', t'u', t'u'' \ldots$ usw. $(t, u), (t, u'), (t, u''), (t', u')$, (t', u'') usw. schreibt.

Jeder Punkt im Raum kann durch ein Trinom

$$(xt + x't' + x''t'')$$

dargestellt werden.

Für alle Punkte, die in einer bestimmten Ebene liegen, wird dann eine Gleichung

$$\lambda x + \lambda' x' + \lambda'' x'' = L$$

gelten, wo $\lambda, \lambda', \lambda'', L$ feste Zahlen bezeichnen. Für eine Ebene durch die drei Punkte $\mu t, \mu' t', \mu'' t''$ ist

$$\lambda\mu = \lambda'\mu' = \lambda''\mu'' = L$$

Schreibt man

$$(t,t) = a, \quad (t',t') = a', \quad (t'',t'') = a'',$$
$$(t',t'') = b, \quad (t,t'') = b', \quad (t,t') = b''$$

und

$$a'a'' - bb = A, \quad aa'' - b'b' = A', \quad aa' - b''b'' = A''$$
$$b'b'' - ab = B, \quad bb'' - a'b' = B', \quad bb' - a''b'' = B''$$
$$D = aa'a'' + 2bb'b'' - abb - a'b'b' - a''b''b''$$

so ist

$$\begin{array}{rcll} T & = & At + B''t' + B't'' & \text{senkrecht zu } t' \text{ und } t'' \\ T' & = & B''t + A't' + Bt'' & t \text{ und } t'' \\ T'' & = & B't + Bt' + A''t'' & t \text{ und } t' \end{array}$$

und allgemein, wenn

$$\lambda x + \lambda' x' + \lambda'' x'' = L$$

die Gleichung einer Ebene ist, so wird die Linie

$$\lambda T + \lambda' T' + \lambda'' T''$$

zu ihr senkrecht sein.

Ferner gilt

$$\begin{aligned} aT + b''T' + b'T'' &= Dt \\ b''T + a'T' + bT'' &= Dt' \\ b'T + bT' + a''T'' &= Dt'' \end{aligned}$$

und die Linien t, t', t'' sind senkrecht zu den Ebenen, deren Gleichungen

$$\begin{aligned} ax + b''x' + b'x'' &= \text{Const} \\ b''x + a'x' + bx'' &= \text{Const} \\ b'x + bx' + a''x'' &= \text{Const} \end{aligned}$$

Der doppelte Flächeninhalt des Dreiecks durch die Punkte $mt, m't', m''t''$ ist gleich der Quadratwurzel aus dem Wert der Form

$$F \ldots \begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$$

wenn man einsetzt: $X = m'm'', X' = mm'', X'' = mm'$, während das sechsfache Volumen der Pyramide, die sich dadurch mit dem Punkt 0 bildet, $= mm'm''\sqrt{D}$ wird, also ist das Lot

$$= \sqrt{\frac{D}{F(\frac{1}{m}, \frac{1}{m'}, \frac{1}{m''})}}$$

T, T', T'' beziehen sich ebenso auf die Form $\begin{pmatrix} AD, & A'D, & A''D \\ BD, & B'D, & B''D \end{pmatrix}$ wie t, t', t'' auf $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$

Die drei Wurzeln der Gleichung

$$0 = p^3 - pp(a + a' + a'') + p(A + A' + A'') - D$$

geben die Quadrate der drei Hauptachsen eines Ellipsoids an, das in dasjenige Parallelepiped eingeschrieben ist, auf welches sich die positive ternäre Form

$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ mit adjungierter Form $\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$ und Determinante $= -D$

bezieht.

Beziehung der Raumverhältnisse auf ein gegebenes Tetraeder.

Es bezeichnen $(0), (1), (2), (3)$ die vier Ecken, gegenüberliegenden Flächen und Lote. Jeder Punkt des Raums P hat dann bezüglich eines beliebigen Anfangspunkts M vier Koordinaten x, x', x'', x''', zwischen denen jedoch die Beziehung

$$x + x' + x'' + x''' = 0$$

gilt. Dabei bezeichnet x den Quotienten, den man erhält, wenn man den Abstand des Punktes P von einer durch M zur Ebene (0) gelegten parallelen Ebene durch das Lot (0) dividiert usw.

Allgemein ist dann

$$\begin{aligned} -(PM)^2 = {} & xx'(01)^2 + xx''(02)^2 + xx'''(03)^2 \\ & + x'x''(12)^2 + x'x'''(13)^2 + x''x'''(23)^2 \end{aligned}$$

Das Grundgesetz der Kristallisation lässt sich am kürzesten so aussprechen: Zwischen je fünf dabei vorkommenden Ebenen besteht folgende Beziehung:

Sind ihre Normalen auf der Kugeloberfläche $(0), (1), (2), (3), (4)$, so sind stets die Produkte $\sin 102 \,.\, \sin 304$, $\sin 103 \,.\, \sin 204$, $\sin 203 \,.\, \sin 104$ in einem rationalen Verhältnis; ist dies wie $\alpha : \beta : \gamma$, so ist $\beta = \alpha + \gamma$.

Sind die Koordinaten der 5 Punkte auf der Kugeloberfläche

$$\left.\begin{array}{ccc} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \\ a''' & b''' & c''' \\ 0 & 0 & 1 \end{array}\right\} \quad \text{so müssen} \quad \begin{array}{l} (ab' - ba') \,.\, (a''b''' - b''a''') \\ (ab'' - ba'') \,.\, (a'''b' - b'''a') \\ (ab''' - ba''') \,.\, (a'b'' - b'a'') \end{array}$$

in rationalem Verhältnis stehen.

Allgemein seien $1, 2, 3, 4, 5$ die 5 Punkte auf der Kugeloberfläche, 0 der Mittelpunkt; dann stehen, wenn 12 das Volumen des Tetraeders 0345 bedeutet

$$\left.\begin{array}{l} 23 \,.\, 45 \\ 24 \,.\, 53 \\ 25 \,.\, 34 \end{array}\right\} \quad \text{in rationalem Verhältnis}$$

ebenso

$$\left.\begin{array}{l} 12 \,.\, 34 \\ 13 \,.\, 42 \\ 14 \,.\, 23 \end{array}\right\} \quad \text{usw.}$$

Transformationen der Form $\left(\begin{smallmatrix}5, & 5, & 5\\ -1, & -1, & -1\end{smallmatrix}\right)$ Det. $= 108$

					Chaux carbonatée
$\left\{\begin{smallmatrix}+1 & +1 & -1\\ -1 & +1 & +1\\ +1 & -1 & +1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}17 & 17 & 17\\ -7 & -7 & -7\end{smallmatrix}\right)$		$\left(\begin{smallmatrix}240 & 240 & 240\\ +168 & +168 & +168\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10 & 10 & 10\\ +7 & +7 & +7\end{smallmatrix}\right)$	equiaxe
	$36 \,.\, 108$		$256 \,.\, 11664$	216	
$\left\{\begin{smallmatrix}+1 & +1 & 0\\ 0 & +1 & +1\\ +1 & 0 & +1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}8 & 8 & 8\\ +2 & +2 & +2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4 & 4 & 4\\ +1 & +1 & +1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}15 & 15 & 15\\ -3 & -3 & -3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5 & 5 & 5\\ -1 & -1 & -1\end{smallmatrix}\right)$	inverse
	$4 \,.\, 108$	54	$27 \,.\, 108$	54	
$\left\{\begin{smallmatrix}+2 & +1 & +1\\ +1 & +2 & +1\\ +1 & +1 & +2\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}20 & 20 & 20\\ +14 & +14 & +14\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10 & 10 & 10\\ +7 & +7 & +7\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}51 & 51 & 51\\ -21 & -21 & -21\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}17 & 17 & 17\\ -7 & -7 & -7\end{smallmatrix}\right)$	contrastante
	$16 \,.\, 108$	216	$432 \,.\, 108$	$16 \,.\, 108$	
$\left\{\begin{smallmatrix}+1 & +2 & +2\\ +2 & +1 & +2\\ +2 & +2 & +1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}29 & 29 & 29\\ +23 & +23 & +23\end{smallmatrix}\right)$		$\left(\begin{smallmatrix}312 & 312 & 312\\ -138 & -138 & -138\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}52 & 52 & 52\\ -23 & -23 & -23\end{smallmatrix}\right)$	mixte
	$25 \,.\, 108$		$67500 \,.\, 108$	33750	

Schreibt man die ursprüngliche Form allgemein als $\left(\begin{smallmatrix}t, & t, & t\\ u, & u, & u\end{smallmatrix}\right)$ und eine abgeleitete als $\left(\begin{smallmatrix}T, & T, & T\\ U, & U, & U\end{smallmatrix}\right)$ so gilt

$$\begin{aligned}
&1, \quad T = 3t - 2u \quad U = -t + 2u\\
&2, \quad T = 2t + 2u \quad U = t + 3u\\
&3, \quad T = 6t + 10u \quad U = 5t + 11u\\
&4, \quad T = 9t + 16u \quad U = 8t + 17u
\end{aligned}$$

Die Form $\left(\begin{smallmatrix}1, & 3, & k\\ 0, & 0, & 0\end{smallmatrix}\right)$ geht durch die Substitution

$$\begin{aligned}
x &= u + u' - 2u'' \quad \text{umgekehrt} \quad 6u = x + 3y + 2z\\
y &= u - u' \qquad\qquad\quad\;\; 6u' = x - 3y + 2z\\
z &= u + u' + u'' \qquad\quad\;\; 6u'' = -2x + 2z
\end{aligned}$$

$$x \equiv z' \pmod 3, \quad x \equiv y \pmod 2$$

über in $\left(\begin{smallmatrix}4{+}k, & 4{+}k, & 4{+}k\\ k{-}2, & k{-}2, & k{-}2\end{smallmatrix}\right)$

Um Kalkspat zu erhalten, ist $k = 0{,}973103$ zu setzen.

Hind die komplexen Werte der orthographischen Projektion von drei gleich langen und zueinander senkrechten Geraden a, b, c, so gilt $aa + bb + cc = 0$, allgemein kann man, mit beliebigen komplexen Zahlen p und q, setzen

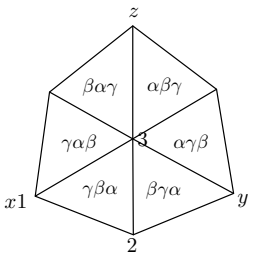
$$a = (p - q)(q - pii), \quad b = (q - qi)(pii - pi),$$
$$c = (qi - p)(pi - q)$$

Hexakisoktaeder.



Gleichung: $px + qy + rz = 1$

Koordinaten.



1.	$\frac{1}{\gamma}$	0	0
2.	$\frac{1}{\beta+\gamma}$	$\frac{1}{\beta+\gamma}$	0
3.	$\frac{1}{\alpha+\beta+\gamma}$	$\frac{1}{\alpha+\beta+\gamma}$	$\frac{1}{\alpha+\beta+\gamma}$

$\alpha < \beta < \gamma$

Sechsfaches Volumen einer Elementarpyramide

$$= \frac{1}{\gamma \,.\, (\beta+\gamma)(\alpha+\beta+\gamma)}$$

Alle [Flächen] sind um eine Kugel beschrieben, deren Radius

$$= \frac{1}{\sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}$$

Doppelter Flächeninhalt eines Dreiecks

$$= \frac{\sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}{\gamma(\beta+\gamma)(\alpha+\beta+\gamma)}$$

Kante

$$1\,.\,2 = \frac{\sqrt{(\beta\beta+\gamma\gamma)}}{\gamma(\beta+\gamma)},$$

$$1\,.\,3 = \frac{\sqrt{((\alpha+\beta)^2+2\gamma\gamma)}}{\gamma(\alpha+\beta+\gamma)},$$

$$2\,.\,3 = \frac{\sqrt{(2\alpha\alpha+(\beta+\gamma)^2)}}{(\beta+\gamma)(\alpha+\beta+\gamma)}$$

Kosinus des Winkels zwischen den Kanten 3 . 1 . 2

$$= \frac{\alpha\beta+\beta\beta+\gamma\gamma}{\sqrt{(\beta\beta+\gamma\gamma)((\alpha+\beta)^3+2\gamma\gamma)}}$$

Sinus

$$= \frac{\gamma \,.\, \sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}{\sqrt{(\beta\beta+\gamma\gamma)((\alpha+\beta)^2+2\gamma\gamma)}}$$

Vorkommende Werte.

	α	β	γ	
7.	0.	0.	1	Hexaeder
3.	0.	1.	1	Rhombendodekaeder
6.	0.	1.	2	Tetrakishexaeder
	0.	1.	3	
	0.	2.	3	
1.	1.	1.	1	Oktaeder
5.	1.	1.	2	Trapezikositetraeder
	1.	1.	3	

	α	β	γ	
2.	1.	2.	2.	Triakisoktaeder
4.	1.	2.	3.	Hexakisoktaeder
	1.	2.	4.	
2.	1.	3.	3.	Triakisoktaeder
4.	1.	3.	5.	Hexakisoktaeder
2.	2.	3.	3	Triakisoktaeder
	2.	3.	4?	
	3.	5.	11	

BEMERKUNGEN.

Neben den vorstehenden Notizen, die die in der Besprechung von SEEBERS Untersuchungen der ternären Formen dargestellten Gesichtspunkte teilweise weiterentwickeln, sind in der Handschrift mehrere eigene Kristallmessungen mit einem achtzölligen REICHENBACHschen Theodoliten aufgezeichnet. Die einzelnen Protokolle enthalten jeweils das Beobachtungsdatum, aus dem hervorgeht, dass diese Untersuchung dem Juli 1831 angehört.

Aus der Theorie der indefiniten ternären quadratischen Formen findet sich im handschriftlichen Nachlass nur der folgende, wahrscheinlich während der Ausarbeitung der Disqu. Arr. aufgezeichnete Satz

„Alle Transformationen der ternären Form

$$\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

in sich selbst werden durch die Formel

$$\begin{array}{lll} \alpha\delta+\beta\gamma & \alpha\beta-\gamma\delta & \alpha\beta+\gamma\delta \\ \alpha\gamma-\beta\delta & \frac{1}{2}(\alpha\alpha+\delta\delta-\beta\beta-\gamma\gamma) & \frac{1}{2}(\alpha\alpha+\gamma\gamma-\beta\beta-\delta\delta) \\ \alpha\gamma+\beta\delta & \frac{1}{2}(\alpha\alpha+\beta\beta-\gamma\gamma-\delta\delta) & \frac{1}{2}(\alpha\alpha+\beta\beta+\gamma\gamma+\delta\delta) \end{array}$$

dargestellt, wobei $\alpha, \beta, \gamma, \delta$ so gewählt werden, dass $\alpha\delta - \beta\gamma = 1$ gilt."

Es entstehen nämlich alle Transformationen, in denen die neun Koeffizienten ganze Zahlen sind, wenn für $\alpha, \beta, \gamma, \delta$ sowohl alle die der Bedingungsgleichung genügenden ganzen Zahlen und zwar zwei gerade und zwei ungerade gesetzt werden, als auch alle die ungeraden Vielfachen von $\sqrt{\frac{1}{2}}$, die dieselbe Bedingungsgleichung $\alpha\delta - \beta\gamma = 1$ erfüllen.

Zu Seite 309. Chaux carbonatée équiaxe, inverse, contrastante und mixte sind die von HAUY (Traité de Minéralogie 1801 Band II, S. 132, 137) gebrauchten Benennungen.

Die Tafel der Transformationen der Form $\begin{pmatrix} 5, & 5, & 5 \\ 1, & 1, & 1 \end{pmatrix}$ enthält in der ersten vertikalen Spalte die Koeffizienten der Substitution, in der zweiten die dadurch entstandene neue Form, in der dritten die der letzteren Form entsprechende primitive, wenn diese nicht bereits selbst primitiv ist, und in der vierten deren adjungierte Form.

SCHERING.

ZUR THEORIE DER BIQUADRATISCHEN RESTE.

[I.]

1.

Wir erweitern das Gebiet der höheren Arithmetik, indem wir darin auch die komplexen Größen aufnehmen. In dieser Untersuchung nennen wir jede Größe $x + iy$ eine komplexe ganze Zahl, wenn x, y reelle ganze Zahlen sind.

2.

Die unendlich vielen komplexen ganzen Zahlen lassen sich am bequemsten durch Punkte in einer unbegrenzten Ebene anschaulich darstellen; wir nennen den Punkt mit der Abszisse x und der Ordinate y den Punkt $x + iy$; alle Punkte, die ganze Zahlen darstellen, sollen ganzzahlige Punkte heißen.

3.

Um eine bestimmte Festlegung zu treffen, sollen die Abszissen stets nach links positiv und die Ordinaten nach oben positiv sein.

4.

Die vom Punkt $x + iy$ zum Punkt $x' + iy'$ gezogene gerade Linie soll die gerade Linie $(x + iy, x' + iy')$ heißen; dabei berücksichtigen wir, wo es darauf ankommt, zugleich die Richtung und unterscheiden daher die gerade Linie $x + iy, x' + iy'$ von $x' + iy', x + iy$.

5.

Der Kürze halber wollen wir komplexe Größen wie $x + iy$ auch durch einen einzigen Buchstaben bezeichnen, etwa z.

6.

Die von den geraden Linien $zz', z'z'', z''z''' \dots z^{n-1}z^n, z^nz$ begrenzte Figur nennen wir die Figur $zz'z''z''' \dots z^n$. Wir schließen den Fall nicht aus, dass einige dieser Linien einander schneiden.

7.

Mit $S(z, z', z'' \dots z^n)$ bezeichnen wir allgemein die Summe von so vielen reellen ganzen Zahlen, wie ganzzahlige Punkte innerhalb der Figur liegen. Dabei setzen wir für jeden Punkt, den die Grenzlinie der Figur einmal, zweimal, dreimal usw. umläuft, die Zahl ± 1, ± 2, ± 3 usw.; die oberen Zeichen gelten, wenn die Grenzlinie den Punkt so umgibt, dass er auf der rechten Seite der Figur liegt, die unteren im entgegengesetzten Fall. Schneiden sich also keine Seiten der Figur, so ist $S(z, z', z'' \dots)$ die Anzahl der Punkte innerhalb der Figur, positiv oder negativ genommen.

8.

Offenbar gilt stets

$$\begin{aligned} S(z, z', z'' \dots z^n) &= S(z', z'', z''' \dots z^n, z) \\ &= S(z'', z''' \dots z') \text{ usw.} \\ &= -S(z^n, z^{n-1} \dots z'', z', z) \\ &= -S(z^{n-1} \,.\, z^{n-2} \dots z', z, z^n) \text{ usw.} \end{aligned}$$

9.

Wie die auf der Grenzlinie selbst liegenden Punkte zu behandeln sind, muss noch genauer festgelegt werden. In vielen Fällen können auf der Grenzlinie überhaupt keine ganzzahligen Punkte liegen; dann ist keine Festlegung nötig. Liegen aber auf der Grenzlinie zz' solche Punkte, so zeigen wir durch ein zwischen z und z' eingefügtes $+$ an, dass diese Punkte so zu behandeln sind, als lägen sie rechts von der Grenzlinie, und durch ein $-$, als lägen sie links. Wir werden auch gelegentlich ein 0 oder $\frac{1}{2}$ einfügen, um anzuzeigen, dass sie auf jeder Seite gar nicht oder nur mit ihrem halben Wert zu berücksichtigen sind. Ist einer der Punkte z, z', z'' usw. selbst ein ganzzahliger Punkt, so wird er, sofern nicht ausdrücklich das Gegenteil gesagt wird, überhaupt nicht mitgezählt, außer soweit er zugleich auch als Punkt, der kein Eckpunkt ist, in Betracht kommt.

10.

Sätze. Werden alle z, z', z'' usw. um dieselbe ganze Zahl vermehrt, so bleibt S unverändert.

Wird i durch $-i$ und jedes Verbindungszeichen durch sein entgegengesetztes ersetzt, so ändert S nur sein Vorzeichen.

$$\begin{aligned} S(z, z', z'' \ldots z^n) &= S(z, u, u' \,..\, u^n, z', z'', z^n) \\ &\quad - S(z, u, u' \,..\, u^n, z') \\ &= S(z, u, u', u'' \,..\, u^n, z^m, z^{m+1} \,..\, z^n) \\ &\quad - S(z, u, u', u'' \,..\, u^n, z^m, z^{m-1} \,..\, z', z) \end{aligned}$$

Dabei müssen die Verbindungszeichen einander entsprechen, zwischen den rückwärts laufenden Gliedern jedoch umgekehrt werden.

Ist ζ eine ganze Zahl $= a + bi$, so gilt, wenn die gegenüberliegenden Verbindungszeichen entgegengesetzt sind,

$$S(z, z', z' + \zeta, z + \zeta) = [bx' - ay'] - [bx - ay]$$

Ist hierbei $bx' - ay'$ selbst eine ganze Zahl, so ist diese für $[bx' - ay']$ zu nehmen, wenn das Verbindungszeichen zwischen z' und $z' + \zeta$ + ist, dagegen 1 oder $\frac{1}{2}$ weniger, wenn dieses Zeichen − oder $\frac{1}{2}$ ist; für $bx - ay$ gilt das Umgekehrte.

Die Formel gilt nur, wenn a und b keinen gemeinsamen Teiler haben; ist ihr größter gemeinsamer Teiler $= h$, so ist stattdessen

$$h\left[\frac{bx' - ay'}{h}\right] - h\left[\frac{bx - ay}{h}\right]$$

zu nehmen.

11.

Wenden wir uns nun unserem eigentlichen Gegenstand näher zu. Sind für den Modul $m = a + bi$ die Zahlen f, f', f'' usw. so beschaffen, dass sie erstens alle modulo m paarweise inkongruent sind und zweitens jede ganze Zahl notwendig einer von ihnen kongruent sein muss, so nennen wir die Gesamtheit der Zahlen f, f', f'' usw. das System der Primitivreste von m. Ihre Anzahl ist stets $= aa + bb$.

12.

Das System der Primitivreste kann auf viele Arten gebildet werden. Am einfachsten wählt man die Punkte innerhalb des Quadrats $0, m, (1 + i)m, im$; hinzuzufügen sind jedoch noch

I. der Punkt oder die Größe 0;

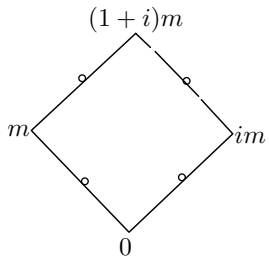
II. alle Punkte auf zwei einander nicht gegenüberliegenden Grenzlinien.

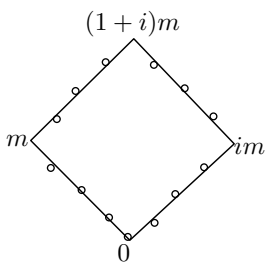
Statt auf einer der 4 Grenzlinien alle Punkte zu nehmen, kann man sie auch auf mehreren zugleich nehmen.

Die Auswahl dieser Punkte auf den Grenzlinien, falls dort welche liegen, kann auf mehrere Arten geschehen, die den obigen Bedingungen genügen. Die einfachste ist die folgende.

Man nehme auf der Grenzlinie $0, m$ alle Punkte zwischen 0 und $\frac{1}{2}m$, inklusive, und auf der Grenzlinie $0, im$ alle Punkte von $\frac{1}{2}im$ bis im, exklusive, und verfahre bei den beiden anderen ähnlich.

Diese beiden Verfahren lassen sich so veranschaulichen:





13.

Schließt man von den Primitivpunkten aus:

I. nur den Punkt 0, wenn a gerade und b ungerade ist, oder umgekehrt;

II. die Punkte 0 und $\frac{1}{2}(1+i)m$, wenn a und b beide ungerade sind;

III. die vier Punkte $0, \frac{1}{2}m, \frac{1}{2}(1+i)m, \frac{1}{2}im$, wenn a und b beide gerade sind,

so nennen wir die verbleibenden eigentliche Primitivpunkte und die ausgeschlossenen uneigentliche. Die Anzahl der ersteren ist also

$$\begin{array}{rrcl} \text{im Fall} & \text{I} & = & aa + bb - 1 \\ & \text{II} & = & aa + bb - 2 \\ & \text{III} & = & aa + bb - 4 \end{array}$$

und damit stets durch 4 teilbar.

14.

Diese eigentlichen Primitivpunkte lassen sich in 4 Klassen F, F', F'', F''' aufteilen, sodass

$$\begin{array}{llll} iF \equiv F' & iF' \equiv F'' & iF'' \equiv F''' & iF''' \equiv F \\ -F \equiv F'' & -F' \equiv F''' & -F'' \equiv F & -F''' \equiv F' \\ -iF \equiv F''' & -iF' \equiv F & -iF'' \equiv F' & -iF''' \equiv F'' \end{array}$$

Dabei gilt nun der folgende äußerst wichtige Satz.

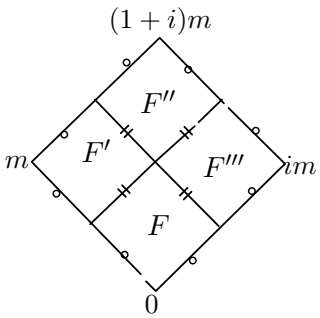
Es sei M eine Zahl, die mit m keinen Faktor gemeinsam hat. Von den Zahlen MF gehören zur Klasse F eine Anzahl von n,

$$\begin{array}{cc} F' & n' \\ F'' & n'' \\ F''' & n''' \end{array}$$

und der kleinste Rest von $n' + 2n'' + 3n''$ modulo 4 sei $= N$, also N gleich einer der 4 Zahlen $0, 1, 2, 3$. Unter dieser Voraussetzung ist N *unabhängig* von der Aufteilung der Primitivreste in Klassen. Wir nennen ihn den Dezidenten des biquadratischen Verhältnisses der Zahl M zu m.

15.

Die einfachste Art der Aufteilung ist allerdings die folgende:



In besonderen Fällen kann jedoch eine andere Aufteilung vorteilhafter sein.

16.

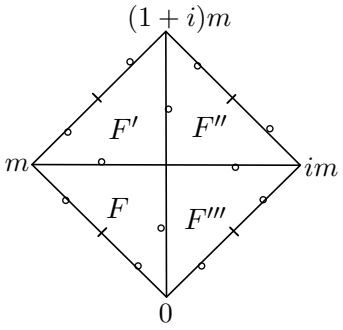
Sind f, f', f'' usw. sämtliche Primitivreste des Moduls m, so gilt

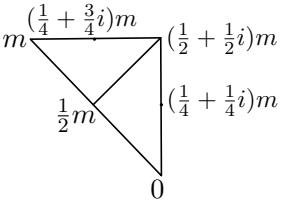
$$\begin{aligned} & S(z + \tfrac{f}{m},\ z' + \tfrac{f}{m},\ z'' + \tfrac{f}{m},\ \text{usw.}) \\ & + S(z + \tfrac{f'}{m},\ z' + \tfrac{f'}{m},\ z'' + \tfrac{f'}{m},\ \text{usw.}) \\ & + S(z + \tfrac{f''}{m},\ z' + \tfrac{f''}{m},\ z'' + \tfrac{f''}{m},\ \text{usw.}) \\ & + \text{usw.} \\ & = S(mz, mz', mz'',\ \text{usw.} \end{aligned}$$

17.

Theorie des biquadratischen Restes $1+i$.

Der Modul soll mit dem Rest keinen Teiler gemeinsam haben. Wir nehmen daher an, dass von den Zahlen a und b die eine gerade und die andere ungerade ist. Das folgende Schema zeigt die Aufteilung der eigentlichen Primitivreste in die vier Klassen:





Zu n sind alle Zahlen zu rechnen auf

$$\text{der Linie } 0 \ldots \tfrac{1}{2}m \qquad \text{Anzahl } = g$$

Zu n' alle Zahlen auf

$$\text{der Linie } 0 \ldots (\tfrac{1}{4}+\tfrac{1}{4}i)m \qquad \text{Anzahl } = g'$$

Zu n'' alle Zahlen innerhalb

$$\text{des Dreiecks } \tfrac{1}{2}m, m, (\tfrac{1}{2}+\tfrac{1}{2}i)m \qquad \text{Anzahl } = h$$

Zu n''' alle Zahlen innerhalb

$$\text{des Dreiecks } 0, \tfrac{1}{2}m, (\tfrac{1}{2}+\tfrac{1}{2}i)m \qquad \text{Anzahl } = h'$$

und außerdem alle Zahlen auf

$$\text{der Linie } (\tfrac{1}{4}+\tfrac{1}{4}i)m \,..\, (\tfrac{1}{2}+\tfrac{1}{2}i)m \qquad \text{Anzahl } = g''$$

Es gilt stets $g'+g''=g$, $aa+bb=p$, $\frac{1}{4}(p-1)=g+g'+g''+h+h'$. Der Dezident ist also

$$D = S(0_{(+)}, \tfrac{1}{2}m, (\tfrac{1}{2}+\tfrac{1}{2}i)m_{(-)}) + \tfrac{1}{2}(p-1) + 2g''$$

Man nehme nun für den Modul $m+1+i$ die folgenden Übergänge an:

g	geht über in	G
g'		G'
g''		G''
h		H
h'		H'

so gilt

$$\begin{aligned}\Delta S(0_{(+)}, \tfrac{1}{2}m, (\tfrac{1}{2}+\tfrac{1}{2}i)m_{(-)}) \\ = +S(0_{(+)}, (\tfrac{1}{2}+\tfrac{1}{2}i)m, (\tfrac{1}{2}+\tfrac{1}{2}i)m+i_{(-)}) \\ - S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)}) \\ - S(\tfrac{1}{2}m, (\tfrac{1}{2}+\tfrac{1}{2}i)m, (\tfrac{1}{2}+\tfrac{1}{2}i)m+i,\ \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i)\end{aligned}$$

Das letzte dieser S ist

$$= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] - S((\tfrac{1}{2}+\tfrac{1}{2}i)m, \tfrac{1}{2}m, \tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i)$$

wenn a ungerade oder gerade ist

$$\begin{aligned}&= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] - S(-\tfrac{1}{2}+\tfrac{1}{2}i, \tfrac{1}{2}m-\tfrac{1}{2}+\tfrac{1}{2}i, \tfrac{1}{2}m+i) \\ &= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] + S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)}) \\ &\quad - S(0_{(+)}, (\tfrac{1}{2}+\tfrac{1}{2}i)m, (\tfrac{1}{2}+\tfrac{1}{2}i)m+i_{(-)})\end{aligned}$$

Also

$$\begin{aligned}\Delta D = &- \left[\tfrac{1}{2}(a-b)\right] + \left[\tfrac{1}{2}a\right] \\ &+ 2S(0_{(+)}, (\tfrac{1}{2}+\tfrac{1}{2}i)m, (\tfrac{1}{2}+\tfrac{1}{2}i)m+i_{(-)}) + a + b + 1 \\ &- 2S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)}) - 2g'' + 2G''\end{aligned}$$

Die Verbindungszeichen gelten alle für den Fall, dass $a-b$ positiv ist; sonst nimmt man die entgegengesetzten.

Wir zerlegen ferner $S(0_{(+)}, (\tfrac{1}{2}+\tfrac{1}{2}i)m, (\tfrac{1}{2}+\tfrac{1}{2}i)m+i_{(-)})$ in

$$\begin{aligned}&S(0_{(+)}, (\tfrac{1}{4}+\tfrac{1}{4}i)m, (\tfrac{1}{4}+\tfrac{1}{4}m)+\tfrac{1}{2}i_{(-)}) \\ &+ \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{4}(a-b)\right] \\ &- S((\tfrac{1}{2}+\tfrac{1}{2}i)m_{(-)}, (\tfrac{1}{4}+\tfrac{1}{4}i)m, (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}i_{(-)})\end{aligned}$$

Der letzte Teil

$$\begin{aligned}&= -S(\tfrac{1}{2}+\tfrac{1}{2}i_{(-)}, (-\tfrac{1}{4}-\tfrac{1}{4}i)m+\tfrac{1}{2}+\tfrac{1}{2}i,\ (-\tfrac{1}{4}-\tfrac{1}{4}i)m+\tfrac{1}{2}{}_{(+)}) \\ &= -S(-\tfrac{1}{2}-\tfrac{1}{2}i_{(-)}, (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}{}_{(+)}) \\ &= -S(-\tfrac{1}{2}-\tfrac{1}{2}i_{(+)}, (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}{}_{(-)}) + g'' - G'' \\ &= S(0_{(+)}, (\tfrac{1}{4}+\tfrac{1}{4}i)m, (\tfrac{1}{4}+\tfrac{1}{4}i)m+\tfrac{1}{2}i_{(-)}) \\ &\quad - S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)}) + g'' - G''\end{aligned}$$

Damit ergibt sich also

$$\begin{aligned}\Delta D = &+ \left[\tfrac{1}{2}(a-b)\right] + \left[\tfrac{1}{2}a\right] \\ &- 4S(-\tfrac{1}{2} - \tfrac{1}{2}i_{(+)}, \tfrac{1}{4} + \tfrac{1}{4}im - \tfrac{1}{2} - \tfrac{1}{2}i,\ (\tfrac{1}{4} + \tfrac{1}{4}i)m - \tfrac{1}{2}{}_{(-)}) \\ &- 2\left[\tfrac{1}{4}(a-b)\right] + a + b + 1\end{aligned}$$

Für die Vermehrung des Moduls um $1-i, -1+i, -1-i$ ist keine besondere Untersuchung nötig, weil die Moduln $m, im, -m, -im$ offenbar gleiche Dezidenten haben. Wir haben also die folgenden Sätze:

Sind der Modul und sein Dezident $a+bi, = D$, so haben die folgenden Moduln die angegebenen Dezidenten:

$a+1+(b+1)i$	$D + a + b + 1 + [\frac{1}{2}a] + [\frac{1}{2}(a-b)] - 2[\frac{1}{4}(a-b)]$
$a+1+(b-1)i$	$D + a - b + 1 + [-\frac{1}{2}b] + [-\frac{1}{2}(a+b)] - 2[-\frac{1}{4}(a+b)]$
$a-1+(b+1)i$	$D - a + b + 1 + [\frac{1}{2}b] + [\frac{1}{2}(a+b)] - 2[\frac{1}{4}(a+b)]$
$a-1+(b-1)i$	$D - a - b + 1 + [-\frac{1}{2}a] + [\frac{1}{2}(b-a)] - 2[\frac{1}{4}(b-a)]$

Daraus ferner

		oder wenn a ungerade ist
$a+2+bi$	$D - \frac{a-b-3}{2} + 2[\frac{1}{2}a] - 2[\frac{a-b}{4}] - 2[\frac{-a-b-2}{4}]$	$D + \frac{b-a-1}{2}$
$a-2+bi$	$D + \frac{a-b+3}{2} + 2[-\frac{1}{2}a] - 2[\frac{b-a}{4}] - 2[\frac{a+b-2}{4}]$	D
$a+(b+2)i$	$D - \frac{a+b-3}{2} + 2[\frac{1}{2}b] - 2[\frac{a+b}{4}] - 2[\frac{a-b-2}{4}]$	$D + \frac{a+b-3}{2}$
$a+(b-2)i$	$D + \frac{a+b+3}{2} + 2[-\frac{1}{2}b] - 2[\frac{-a-b}{4}] - 2[\frac{b-a-2}{4}]$	

$a+2+(b+2)i$	$2a - b + 1 + D$	oder $D + b - 1$
$a+2+(b-2)i$	$-a - 2b + 1 + D$	$D + a - 1$
$a-2+(b+2)i$	$a + 2b + 1 + D$	$D - a - 1$
$a-2+(b-2)i$	$-2a + b + 1 + D$	$D - b - 1$

$a+4+bi$	$D + a + b$	$a+8+bi$	$D+2$
$a+(b+4)i$	$D - a + b$		
$a-4+bi$	$D - a - b$		
$a+(b-4)i$	$D + a - b$		

$a+4+(b+4)i$	$D + 2b$
$a+4+(b-4)i$	$D + 2a$
$a-4+(b+4)i$	$D + 2a$
$a-4+(b-4)i$	$D + 2b$

Das Ergebnis der vorhergehenden Untersuchungen ist also folgendes: Für den Modul $m = a + bi$, wobei a ungerade und b gerade ist, gilt

$$D\frac{1+i}{m} = \tfrac{1}{8}(-aa + 2ab + bb - 8b + 1)$$
$$\text{(und wenn } a + bi = 1 + (2+2i)(\alpha + \beta i)\text{)}$$
$$\text{oder } \tfrac{1}{8}(-aa + 2ab - 3bb + 1) \equiv -(\alpha - \beta)^2 - \beta$$

$$D\frac{1-i}{m} = \tfrac{1}{8}(+aa + 2ab - bb - 8b - 1)$$
$$\text{oder } \tfrac{1}{8}(+aa + 2ab + 3bb - 1)$$

$$D\frac{-1-i}{m} = \tfrac{1}{8}(-aa + 2ab + bb + 1)$$
$$= \beta + \alpha\alpha + 2\alpha\beta - \beta\beta \equiv -\beta + (\alpha + \beta)^2$$

$$D\frac{-1+i}{m} = \tfrac{1}{8}(+aa + 2ab - bb - 1)$$
$$= \alpha + \alpha\alpha - 2\alpha\beta - \beta\beta \equiv -\alpha - (\alpha + \beta)^2$$

$$D\frac{2}{m} = \tfrac{1}{2}ab$$
$$D\frac{i}{m} = \tfrac{1}{4}(aa + bb - 1)$$
$$D\frac{-1}{m} = \tfrac{1}{2}(aa + bb - 1)$$

Allgemeiner Satz über die Dezidenten.

Es seien A, B, C usw. verschiedene (ungerade komplexe) Primzahlen, von denen keine die Zahl M teilt; dann gilt

$$D\frac{M}{A^\alpha B^\beta C^\gamma D^\delta} = \alpha D\frac{M}{A} + \beta D\frac{M}{B} + \gamma D\frac{M}{C} + \text{usw.}$$

$$M^{\frac{1}{4}(aa+bb-1)} \equiv i^{D\frac{M}{a+bi}} \pmod{(a+bi)} \quad \text{wenn } a + bi \text{ eine Primzahl}$$

$$D\frac{1+i}{m} = \tfrac{1}{8}(-aa + 2ab - 3bb + 1)$$
$$= -\tfrac{1}{8}(3(a-b) \mp 1)(a - b \mp 1) \quad \text{wenn } a \equiv \tfrac{1}{3}$$
$$D\frac{1-i}{m} = \tfrac{1}{8}(+aa + 2ab + 3bb - 1)$$
$$D\frac{-1-i}{m} = \tfrac{1}{8}(-aa + 2ab + bb + 1)$$
$$= \tfrac{1}{8}(a - b \mp 1)(a - b \mp 3) \quad \text{wenn } a \equiv \pm 1$$
$$D\frac{-1+i}{m} = \tfrac{1}{8}(+aa + 2ab - bb - 1)$$

Allgemein $m \equiv 1 \bmod.(1+i)$

$$D\frac{1+i}{m} = -\text{Realteil } \frac{(1+i)(m^4-1)}{16} = \text{Imaginärkoeff. } \frac{m^4-1}{8+8i}$$
$$D\frac{1-i}{m} = +\text{Realteil } \frac{(1-i)(m^4-1)}{16} = \text{Imaginärkoeff. } \frac{m^4-1}{8-8i}$$

$1+i \pmod{16}$

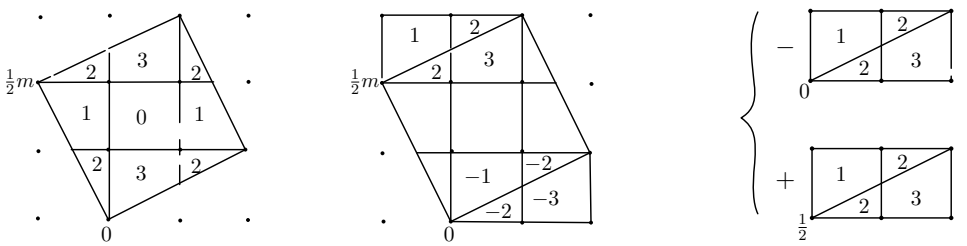
a	b							
	0	2	4	6	8	10	12	14
1	0	3	3	0	2	1	1	2
3	3	3	0	2	1	1	2	0
5	1	2	0	3	3	0	2	1
7	2	0	3	3	0	2	1	1
9	2	1	1	2	0	3	3	0
11	1	1	2	0	3	3	0	2
13	3	0	2	1	1	2	0	3
15	0	2	1	1	2	0	3	3

18.

Theorie des biquadratischen Restes $-1-2i$.

Der Modul $= m = a + bi$ sei so beschaffen, dass a ungerade und b gerade ist; außerdem setzen wir voraus, dass er eine Primzahl ist.

Die folgenden Schemata stellen den Dezidenten dar; von ihrer Identität überzeugt man sich leicht:



Der Kürze halber bezeichnen wir $S(x, x+\alpha, x+\alpha+\beta, x+\beta)$ mit $[x, \alpha, \beta]$, sodass

$$\begin{aligned}[x,\alpha,\beta] &= -[x,\beta,\alpha] = [x+\alpha,\beta,-\alpha] \\ &= -[x+\alpha,-\alpha,\beta] \\ &= [x+\alpha+\beta,-\alpha,-\beta] \\ &= -[x+\alpha+\beta,-\beta,-\alpha]\end{aligned}$$

Setzt man ferner

$$\frac{m}{-2-4i} = \frac{-a-2b}{10} + \frac{-b+2a}{10}i = Q$$

so besteht der Dezident aus den folgenden acht Teilen:

$$\begin{aligned}
\mathrm{I} &= [0, \tfrac{1}{2}, -iQ] \\
-2\mathrm{II} &= -2[0, \tfrac{1}{2}, Q] \\
\mathrm{III} &= +[Q, \tfrac{1}{2}, -iQ] \\
\mathrm{IV} &= +[-iQ, \tfrac{1}{2}, Q] \\
-3\mathrm{V} &= -3[Q, \tfrac{1}{2}, Q] \\
-3\mathrm{VI} &= -3[2Q, \tfrac{1}{2}, -iQ] \\
+2\mathrm{VII} &= +2[(1-i)Q, \tfrac{1}{2}, Q] \\
+\mathrm{VIII} &= +[0, \tfrac{1}{2}, \tfrac{1}{2}im]
\end{aligned}$$

Bezeichne F einen beliebigen Elementarrest des Moduls $-1-2i$, so gilt

$$\Sigma[2FQ, \tfrac{1}{2}, iQ] = [0, -\tfrac{1}{2} - i, \tfrac{1}{2}im]$$

Setzt man also für F die Werte $0, 1, i, -1, -i$ ein, so gilt

$$\begin{aligned}
0 = \quad & [0, \tfrac{1}{2}, iQ] && = \mathrm{IX} \\
& +[2Q, \tfrac{1}{2}, iQ] && = \mathrm{X}. \\
& +[2iQ, \tfrac{1}{2}, iQ] && = \mathrm{XI} \\
& +[-2Q, \tfrac{1}{2}, iQ] && = \mathrm{XII} \\
& +[-2iQ, \tfrac{1}{2}, iQ] && = \mathrm{XIII} \\
& -[0, -\tfrac{1}{2} - i, \tfrac{1}{2}im] && = -\mathrm{XIV}
\end{aligned}$$

Man addiere dies zum vorigen Wert des Dezidenten. Aus dieser Verbindung ergeben sich die folgenden Resultate:

(1) Da $(1+2i)Q + \frac{1}{2}$ eine ganze Zahl ist, gilt

$$\begin{aligned}
\mathrm{XI} &= [-Q - \tfrac{1}{2}, \tfrac{1}{2}, iQ] = -[-Q, -\tfrac{1}{2}, iQ] \\
&= -[Q, \tfrac{1}{2}, -iQ]
\end{aligned}$$

also

$$\mathrm{III} + \mathrm{XI} = 0$$

(2) Wir fassen $\mathrm{IV}, -3\mathrm{V}, \mathrm{X}, \mathrm{XIII}$ auf folgende Weise zusammen:

$$\begin{aligned}
\mathrm{IV} &= +[-2Q + \tfrac{1}{2}i, \tfrac{1}{2}, Q] = [-2iQ - \tfrac{1}{2}, \tfrac{1}{2}i, iQ] \\
\mathrm{V}' &= -[2Q, +\tfrac{1}{2}, -Q] = -[-2iQ, -\tfrac{1}{2}i, iQ] \\
\mathrm{X} &= [+iQ - \tfrac{1}{2}i, \tfrac{1}{2}, iQ] \\
&= [-iQ + \tfrac{1}{2}i, -\tfrac{1}{2}, -iQ] = [-2iQ - \tfrac{1}{2} + \tfrac{1}{2}i, \tfrac{1}{2}, iQ] \\
\mathrm{XIII} &= [-2iQ, \tfrac{1}{2}, iQ]
\end{aligned}$$

Das gesamte Ergebnis aus diesen Teilen ist also

$$\begin{aligned}&-4\mathrm{V}\\&+R(-2iQ)-R(-iQ)-I(-2iQ)+I(-iQ)\\&-\text{Quadr. }[-2iQ-\tfrac{1}{4}+\tfrac{1}{4}i]\\&+\text{Quadr. }[-2iQ+\tfrac{1}{4}-\tfrac{1}{4}i]\end{aligned}$$

(3) Fasst man I, -2II, -3VI, $+2$VII, $+$IX, $+$XII zusammen, so ergibt sich

$$\begin{aligned}\mathrm{I}&=[0,\tfrac{1}{2},-iQ]\\\mathrm{II}&=[0,-\tfrac{1}{2}i,-iQ]\\\mathrm{VI}&=[iQ-\tfrac{1}{2}i,\tfrac{1}{2},-iQ]=[\tfrac{1}{2}-\tfrac{1}{2}i,-\tfrac{1}{2},iQ]\\&=[-\tfrac{1}{2}+\tfrac{1}{2}i,\tfrac{1}{2},-iQ]\\\mathrm{VII}&=[-Q-\tfrac{1}{2}i,\tfrac{1}{2},Q]=[-\tfrac{1}{2}+\tfrac{1}{2}i,-\tfrac{1}{2},-Q]\\&=[+\tfrac{1}{2}+\tfrac{1}{2}i,-\tfrac{1}{2}i,-iQ]\\\mathrm{IX}&=[0,-\tfrac{1}{2},-iQ]\\\mathrm{XII}&=[-iQ+\tfrac{1}{2}i,\tfrac{1}{2},iQ]=[\tfrac{1}{2}+\tfrac{1}{2}i,-\tfrac{1}{2},-iQ]\end{aligned}$$

$$\begin{aligned}=\;&+4\mathrm{I}-4\mathrm{II}-4\mathrm{VI}+4\mathrm{XII}\\&-I(\tfrac{1}{2}i)+I(-iQ+\tfrac{1}{2}i)+I0-I(-iQ)-2R0+2R(-iQ)\\&+2\text{Quadr. }(-iQ+\tfrac{1}{4}+\tfrac{1}{4}i)\\=\;&4\mathrm{I}-4\mathrm{II}-4\mathrm{VI}+4\mathrm{XII}\\&+R(-1-2i)Q-R(-2iQ)-I(-iQ)+2R(-iQ)\\&+2\text{Quadr. }(-2iQ+\tfrac{1}{4}+\tfrac{1}{4}i)\end{aligned}$$

Dies alles zusammen ergibt folglich

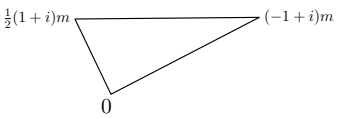
$$\begin{aligned}&+4\mathrm{I}-4\mathrm{II}-4\mathrm{V}-4\mathrm{VI}+4\mathrm{XII}+\tfrac{1}{2}(a-1)-\tfrac{1}{2}b\\&+\text{Quadr. }(-2iQ+\tfrac{1}{4}-\tfrac{1}{4}i)\\&+2\text{Quadr. }(-2iQ+\tfrac{1}{4}+\tfrac{1}{4}i)\\&-\text{Quadr. }(-2iQ-\tfrac{1}{4}+\tfrac{1}{4}i)\end{aligned}$$

Schließlich ergibt sich $\mathrm{VIII}-\mathrm{XIV}=\frac{1}{2}(a-1)+\frac{1}{2}b$. Da die drei Quadratteile dem Dezidenten von $\frac{m}{-1-2i}$ gleich sind, gilt also

$$\text{Dez. }\frac{-1-2i}{m}\equiv a-1+\text{Dez. }\frac{m}{-1-2i}\quad\text{Was zu beweisen war.}$$

Wahrscheinlich lässt sich der Beweis noch erheblich dadurch vereinfachen, dass

$$\text{Dez. }\frac{1+2i}{m}=$$



19.

Durch Induktion wurde Folgendes gefunden:

$$\text{Dez.}\ \frac{a-bi}{a+bi} \equiv \frac{aa+2ab-1}{4}, \qquad a \equiv 1 \ (\text{mod. } 4)$$
$$\equiv \frac{aa+2ab+2bb-1}{4}, \quad a+bi \equiv 1 \ (\text{mod. } 2+2i)$$

Damit hängt Folgendes zusammen: Es sei $aa+bb=p$ (Primzahl), $a \equiv 1$ (mod. 4)

$$1 \,.\, 2 \,.\, 3 \ldots\ldots\ldots\ldots \tfrac{1}{4}(p-1) \equiv \alpha \ \text{mod.} p$$
$$\tfrac{1}{4}(p+3) \,.\, \tfrac{1}{4}(p+7) \ldots \tfrac{1}{2}(p-1) \equiv \beta$$
$$\tfrac{1}{2}(p+1) \,.\, \tfrac{1}{2}(p+3) \ldots \tfrac{3}{4}(p-1) \equiv \gamma$$
$$\tfrac{1}{4}(3p+1) \ldots\ldots\ldots\ldots\ p-1 \equiv \delta$$

so gilt

$$\alpha \equiv \delta, \quad \beta \equiv \gamma \qquad \text{wenn } \tfrac{1}{2}b \text{ gerade}$$
$$\alpha \equiv -\delta, \quad \beta \equiv -\gamma \quad \text{wenn } \tfrac{1}{2}b \text{ ungerade}$$

$$\pm\alpha\beta \equiv i, \quad \pm\beta\beta \equiv 2b, \quad \frac{\beta}{\alpha} \equiv 2a,$$
$$\frac{\beta}{1+\alpha\beta} \equiv \sqrt{a}, \quad \tfrac{1}{2}\beta(1-\alpha\beta) \equiv \sqrt{a}$$

Es kommt demnach nur noch darauf an, die Dezidenten bei reellen Resten zu bestimmen.

$$a^{\frac{1}{4}bb} \,.\, b^{\frac{1}{4}(aa-1)} \equiv 1 \ (\text{mod. } (aa+bb))$$
$$\text{wenn } a \equiv 1)(\text{mod. } 4) \quad b \text{ gerade} \quad aa+bb \text{ Primzahl}$$

Will man nur mit reellen Zahlen arbeiten, so kommt es auf den folgenden Hauptsatz an. Es sei $a-1$ durch 4 und b durch 2 teilbar; a und b seien ohne gemeinsamen Teiler, und k bezeichne die Zahlen $1, 2, 3 \ldots aa+bb-1$. Es sei

α die Anzahl aller Werte von k, für die die kleinsten Reste von $ak, bk, aak, \quad abk$ alle zwischen 0 und $\frac{1}{2}(aa+bb)$ liegen

β $ak, bk, \quad aak, -abk$

γ $ak, bk, -aak, -abk$

δ $ak, bk, -aak, \quad abk$

Dann ist $\beta + 2\gamma + 3\delta - \frac{1}{4}(aa-1)$ durch 4 teilbar.

[II.]

VORBEREITUNGEN ZUR ALLGEMEINEN THEORIE DER BIQUADRATISCHEN RESTE.

(1.)

Es sei $P = x+iy$, wobei weder x noch y eine ganze Zahl ist. Wir bezeichnen die Zahl $+1$ mit $LP, L'P, L''P, L'''P$, je nachdem P im ersten, zweiten, dritten oder vierten Quadranten liegt (im ersten und zweiten Quadranten ist $[y]$ gerade, im dritten und vierten ungerade; im ersten und vierten ist $[x]$ gerade, im zweiten und dritten ungerade). In allen Fällen, in denen diese Zeichen nicht $= 1$ sind, werden sie als $= 0$ vorausgesetzt. Dann gelten die folgenden 24 Relationen:

$$\begin{array}{lll} L(P\pm 1) = L'P & L(P\pm i) = L'''P & L(P\pm 1\pm i) = L''P \\ L'(P\pm 1) = LP & L'(P\pm i) = L''P & L'(P\pm 1\pm i) = L'''P \\ L''(P\pm 1) = L'''P & L''(P\pm i) = L'P & L''(P\pm 1\pm i) = LP \\ L'''(P\pm 1) = L''P & L'''(P\pm i) = LP & L'''(P\pm 1\pm i) = L'P \end{array}$$

$$\begin{array}{lll} LiP = L'''P & L(-P) = L''P & L(-iP) = L'P \\ L'iP = LP & L'(-P) = L'''P & L'(-iP) = L''P \\ L''iP = L'P & L''(-P) = LP & L''(-iP) = L'''P \\ L'''iP = L''P & L'''(-P) = L'P & L'''(-iP) = LP \end{array}$$

(2.)

Mit PP' oder z bezeichnen wir eine Linie, die bei P beginnt und bei P' endet. Sie muss nicht gerade sein. Wir geben allen von $2x + 2iy$ nach $2x + (2y + 1)i$ gezogenen geraden Linien (wobei x, y sämtliche ganzen Zahlen durchlaufen) eine positive und eine negative Seite; als positive wählen wir die rechte, als negative die linke. Mit Tz bezeichnen wir die Anzahl aller Schnitte

der Linie z mit den eben beschriebenen Linien, wobei diejenigen positiv gezählt werden, bei denen z von der negativen auf die positive Seite übergeht, und die anderen negativ. Ferner setzen wir

$$Tz - T(z-1) = Sz$$

($z-1$ ist eine zu z parallele Linie, die vom Punkt $P-1$ nach $P'-1$ geht). Offenbar brauchen wir dem obigen Liniensystem nur noch die von $2x+1+2yi$ nach $2x+1+(2y+1)i$ gezogenen Linien hinzuzufügen und deren linke Seiten als positiv und die rechten als negativ zu betrachten, um in Sz die Anzahl aller Schnitte von z mit diesem doppelten System gerader Linien zu erkennen. Ferner gilt

$$\begin{aligned} T(-z) &= -T(z+i) \\ T(z)+T(z+i) &= [\tfrac{1}{2}x]-[\tfrac{1}{2}x'] \\ S(z+1) &= -Sz \\ S(z+i) &= -Sz+LP+L'''P-LP'-L'''P' \\ S(z+1+i) &= Sz-LP+L'''P+LP'+L'''P' \\ Siz &= Sz-LP+LP' \\ S(-z) &= Sz-LP-L'''P+LP'+L'''P' \\ S(-iz) &= Sz+L'P-L'P' \end{aligned}$$

1.

Wir betrachten in der Ebene zwei Arten von Punkten: erstens diejenigen, denen ganze Zahlen entsprechen; zweitens diejenigen, die durch Produkte ganzer Zahlen mit der Größe $Q=\frac{m}{2M}$ bestimmt sind. Wir können sie als Punkte erster und Punkte zweiter Ordnung unterscheiden.

2.

Verbindet man jeden Punkt zweiter Ordnung mit seinen vier Nachbarn durch gerade Linien, die wir *Ligaturen* nennen werden, so wird die ganze Ebene in unendlich viele Quadrate geteilt. Die Punkte erster Ordnung liegen teils innerhalb dieser Quadrate, teils auf den Ligaturen innerhalb ihrer

Grenzen und teils auf den Grenzen der Ligaturen; Letzteres gilt, wenn sie zugleich Punkte zweiter Ordnung sind. Ist kQ ein solcher Punkt, so muss, sofern m, M ohne gemeinsamen Teiler und beide ungerade sind, k durch M teilbar sein.

3.

Bei den Ligaturen können wir auch zwischen Anfangs- und Endpunkt unterscheiden, also PQ von QP, oder diese Unterscheidung in einigen Fällen beiseitelassen. Zwei solche Ligaturen nennen wir entgegengesetzte. Im Allgemeinen lassen sich die Ligaturen am bequemsten durch ihren Anfangs- und Endpunkt bezeichnen, die man gegebenenfalls in eine Klammer einschließen kann. Die zu einer Ligatur entgegengesetzte soll durch doppeltes Überstreichen angezeigt werden: $QP=\overline{\overline{PQ}}$.

4.

Jedes der betrachteten Quadrate wird von vier solchen Ligaturen eingeschlossen

$$\{kQ, (k+1)Q\},\ \{(k+1)Q, (k+1+i)Q\},$$
$$\{(k+1+i)Q, (k+i)Q\},\ \{(k+i)Q, kQ\} \ldots . \Omega$$

denen es zur Rechten liegt. Dabei ist es wichtig, auf die Form der Zahl k zu achten. Wir unterscheiden vier Arten von Quadraten, je nachdem $k \equiv 0, 1, 1+i, i \pmod 2$ gilt, und verwenden die Zahlen $0, 1, 2, 3$, die wir die jeweiligen Intensoren der Quadrate nennen.

5.

Den Ligaturen geben wir dieselben Intensoren wie den Quadraten, die ihnen zur Rechten liegen.

6.

Nun haben wir ein anderes, größeres Quadrat Ω' zu betrachten, nämlich dasjenige, das entsteht, wenn das in 4 für $k = 0$ angegebene mit M multipliziert wird. Es wird also von den geraden Linien μ, μ', μ'', μ''' begrenzt

$$\{0, \tfrac{1}{2}m\},\ \{\tfrac{1}{2}m, \tfrac{1}{2}(1+i)m\},\ \{\tfrac{1}{2}(1+i)m, \tfrac{1}{2}im\},\ \{\tfrac{1}{2}im, 0\}$$

Es besteht aus ganzen Quadraten Ω und Teilen solcher Quadrate. Man zähle

alle Punkte erster Ordnung in seinem Innern zusammen, indem man für jeden Punkt den Intensor des Quadrats Ω nimmt, in dem er liegt. Diese Summe oder ihr kleinster Rest modulo 4 heißt der Dezident von M für den Modul m und bestimmt die biquadratische Modalität von M bezüglich dieses Moduls.

7.

Wir zerlegen das Quadrat Ω' auf folgende Weise in 5 Teile. Man verbinde den Punkt 0 mit $\frac{1}{4}(1+i)(m-1)$ durch die Linie λ, die ausschließlich entlang Ligaturen innerhalb von Ω' verläuft. Es sei

$$\tfrac{1}{2}m + i\lambda = \lambda', \quad \tfrac{1}{2}(1+i)m - \lambda = \lambda'', \quad \tfrac{1}{2}im - i\lambda = \lambda'''$$

Diese 4 Linien gehen also von den Ecken des Quadrats Ω' ins Innere und enden an den vier Ecken des innersten Quadrats. Dessen Intensor ist 0, wenn $m \equiv 1 \pmod{2+2i}$; die Ligaturen dieses Quadrats seien ν, ν', ν'', ν'''.

Die 5 Teile werden also begrenzt sein durch

I. $\ldots$ $\mu,\ \lambda',\ \overline{\overline{\nu}},\ \overline{\overline{\lambda}}$
II. $\ldots$ $\mu',\ \lambda'',\ \overline{\overline{\nu'}},\ \overline{\overline{\lambda'}}$
III. $\ldots$ $\mu'',\ \lambda''',\ \overline{\overline{\nu''}},\ \overline{\overline{\lambda''}}$
IV. $\ldots$ $\mu''',\ \lambda,\ \overline{\overline{\nu'''}},\ \overline{\overline{\lambda'''}}$
V. das innere Quadrat $\nu,\ \nu',\ \nu'',\ \nu'''$

Der Dezident ist also die Aufzählung aller Punkte erster Ordnung in I. II. III. IV.

8.

Der Kürze halber soll der Intensor eines beliebigen Punktes der Intensor des Quadrats sein, in dem er liegt, und durch ein vorangestelltes Υ bezeichnet werden.

9.

Der Dezident ist also

$$\Sigma\Upsilon P + \Sigma\Upsilon P' + \Sigma\Upsilon P'' + \Sigma\Upsilon P'''$$

wobei P alle Punkte in I. usw. bezeichnet.

10.

Wir betrachten nun noch den Bereich VI $= -i$IV, der außerhalb von Ω' liegt, sich aber entlang μ an I anschließt und mit ihm zusammen den Bereich ω bildet, der aus $AA + BB$ vollständigen Quadraten besteht. Bezeichnet Π alle ganzen und Π' alle um $\frac{1}{2}i$ vermehrten ganzen Punkte dieses Bereichs, so lässt sich leicht beweisen, dass der Dezident

$$\begin{aligned} &= \Sigma\Upsilon\Pi - \Sigma\Upsilon\Pi' + \text{Anzahl aller ganzen Punkte innerhalb VI} \\ &\quad - \text{Anzahl aller halben Punkte innerhalb VI.} \end{aligned}$$

11.

Man stelle sich von jedem ganzen Punkt k nach $k + \frac{1}{2}i$ gerade Linien gezogen vor, deren rechte Seite als positiv und deren linke als negativ gilt. Es sei l eine Linie, und Sl bezeichne die Summe aller Schnitte von l mit diesem Liniensystem, wobei diejenigen positiv gezählt werden, bei denen l von der negativen auf die positive Seite übergeht, und die entgegengesetzten Schnitte negativ. Für den Dezidenten gilt dann der folgende Ausdruck:

$$\Sigma(\Upsilon l \,.\, Sl) + \Sigma Sl' - S\mu$$

Dabei bezeichnet l alle Ligaturen der Quadrate in ω (stets so genommen, dass die Quadrate ihnen zur Rechten liegen), und l' diejenigen Ligaturen, die auf dem Umfang der Figur ω zwischen 0 und $\frac{1}{2}m$ liegen, also außerhalb von Ω'.

Alle Ligaturen l bestehen aus

1) l';

2) l'', den innerhalb von Ω' liegenden Grenzligaturen, also $\lambda', \overline{\overline{\nu}}, \overline{\overline{\lambda}}$;

3) l''', die im Innern von ω liegen.

Verstünde man unter l unbestimmt alle Ligaturen, die innerhalb von ω oder auf den Grenzen dieser Figur liegen, sofern sie von Punkten $\frac{km}{2M}$ ausgehen, wobei k durch $1+i$ teilbar ist, so wäre der Dezident

$$= \Sigma\alpha \,.\, Sl - S\mu$$

wobei $\alpha = 1$ für alle Ligaturen im Innern von ω;

$\alpha = \Upsilon l + 1$ für alle Grenzligaturen außerhalb von Ω', deren Richtung entlang der von 0 nach $\frac{1}{2}m$ gehenden Grenze verläuft;

$\alpha = -(\Upsilon\overline{\overline{\lambda}} + 1) = -\Upsilon l$ für alle auf dieser Grenze, die in entgegengesetzter Richtung verlaufen;

$\alpha = \Upsilon l$ für alle Grenzligaturen innerhalb von Ω', deren Richtung auf 0 zugeht;

$\alpha = -\Upsilon l + 1$ für alle Grenzligaturen innerhalb von Ω', deren Richtung von 0 wegführt.

12.

Wir können nun sämtliche vorkommenden l (nach dem letzten Verfahren) paarweise zusammenfassen, nämlich l mit $\overline{\overline{\frac{1}{2}m - l}}$, die wir verbundene Ligaturen nennen wollen. Eine einzige ist davon ausgenommen, die isoliert steht oder mit ihrer verbundenen Ligatur identisch ist, nämlich diejenige, die von

$$\tfrac{1}{2}(M-1) \,.\, \frac{m}{2M} \quad \text{nach} \quad \tfrac{1}{2}(M+1)\frac{m}{2M} \quad \text{läuft}$$

Für verbundene Ligaturen ist α stets gleich.

[III.]

Theorie der biquadratischen Reste.

1.

Die kleinsten Reste zum Modul $m = a + bi$ sind die ganzen Zahlen $\mu = \alpha + \beta i$, für die bei $\frac{\mu}{m} = x + yi$ die Größen x und y positiv und kleiner als 1 sind. Hinzu kommt der Rest 0[*]. Ihre Anzahl ist $= aa + bb$.

2.

Ist $aa+bb$ ungerade, so hat $aa+bb$ die Form $4n+1$. Lässt man den kleinsten Rest 0 weg, so zerfallen die übrigen in vier Klassen. Zur ersten Klasse f zählen wir diejenigen, bei denen x und y kleiner als $\frac{1}{2}$ sind,

die zweite	f'	bei denen $x > \frac{1}{2}$,	$y < \frac{1}{2}$
dritte	f''	$x > \frac{1}{2}$,	$y > \frac{1}{2}$
vierte	f'''	$x < \frac{1}{2}$,	$y > \frac{1}{2}$

Man erhält alle Reste

$$\begin{array}{lll} f' & \text{aus} & if + m \\ f'' & \text{aus} & -f + (1+i)m \\ f''' & \text{aus} & -if + im \end{array}$$

[*] und, falls a und b einen gemeinsamen Teiler e haben, die Zahlen $\frac{m}{e}, \frac{2m}{e}, \frac{3m}{e} \ldots \frac{(e-1)m}{e}$. Diesen Fall wollen wir jedoch vorerst aus der Untersuchung ausschließen.

3.

Es sei M eine andere Zahl, die mit m keinen Faktor gemeinsam hat. Dann gilt

$$M^{aa+bb-1} \equiv 1 \text{ (mod. } m)$$

folglich ist $M^{\frac{1}{4}(aa+bb-1)}$ entweder $\equiv 1$, oder $\equiv i$, oder $\equiv -1$, oder $\equiv -i$, das heißt $\equiv i^{\varepsilon}$, wobei ε eine der vier Zahlen $0, 1, 2, 3$ bezeichnet. Im ersten Fall ist M ein biquadratischer Rest von m, also auch ein quadratischer. Im dritten Fall ist M ein quadratischer, aber kein biquadratischer Rest; im zweiten und vierten Fall sowohl ein quadratischer als auch ein biquadratischer Nichtrest. Wir nennen dieses ε, von dem der biquadratische Charakter der Zahl M bezüglich des Moduls m abhängt, den Dezidenten von M zum Modul m. Durch Induktion erhält man den folgenden schönen Satz. „Sind M und m ungerade Primzahlen der Form $1 + (2 + 2i)\mu$, wobei μ eine ganze Zahl ist, so ist die Differenz der beiden Dezidenten, von M zum Modul m und von m zum Modul M, entweder $= 0$ oder $= 2$; das Erste gilt, wenn wenigstens eine der Zahlen m, M die Form $1 + 4N$ hat, das Andere, wenn beide die Form $1 + 2i + 4N$ haben." Dieser Reziprozitätssatz ist dem für quadratische Reste bei ausschließlich reellen Zahlen analog.

4.

Man multipliziere alle Zahlen f mit M und bestimme ihre kleinsten Reste zum Modul m. Befinden sich darunter

α	zu f	gehörig
β	f'	
γ	f''	
δ	f'''	

so ist $\varepsilon \equiv \beta + 2\gamma + 3\delta$ (mod. 4).

Beweis. Die Gesamtheit derjenigen Zahlen aus f, deren Produkte mit M Reste aus f ergeben, sei g; die Gesamtheit derjenigen, deren Produkte Reste aus f' ergeben, sei g', und ebenso $g'' \,.\, g'''$. Dann sind die kleinsten Reste von

$$-ig'M, \quad -g''M, \quad ig'''M$$

sämtlich in f enthalten und sowohl voneinander als auch von den kleinsten Resten der Produkte gM verschieden. Folglich ist das Produkt aller

$$gM, \quad -ig'M, \quad -g''M, \quad +ig'''M$$

zum Produkt aller f kongruent, also auch zum Produkt aller g, g', g'', g'''. Jenes Produkt ist aber gleich dem Produkt aller g, g', g'', g''' multipliziert mit

$$M^\alpha \,.\, (-iM)^\beta \,.\, (-M)^\gamma \,.\, (iM)^\delta$$

also ist dieses letzte Produkt $\equiv 1$

$$\begin{aligned} \text{folglich} \qquad & M^{\alpha+\beta+\gamma+\delta}(-i)^\beta(-1)^\gamma i^\delta \equiv 1 \\ \text{oder} \qquad & M^{\alpha+\beta+\gamma+\delta} \equiv i^\beta(-1)^\gamma(-i)^\delta \equiv i^{\beta+2\gamma+3\delta} \end{aligned}$$

woraus der Satz unmittelbar folgt.

5.

Ob der kleinste Rest einer Zahl N zum Modul m zur Klasse f, f', f'' oder f''' gehört, lässt sich leicht entscheiden. Ist nämlich ω die in $\frac{N}{m}$ enthaltene ganze Zahl, so ist jener Rest $= N - \omega m$ und gehört somit zu f, f', f'', je nachdem nach dem Ansatz

$$\frac{N}{m} - \omega = x + iy$$

die folgenden Bedingungen gelten:

$$\begin{array}{ll} x < \frac{1}{2}, & y < \frac{1}{2} \\ x > \frac{1}{2}, & y < \frac{1}{2} \\ x > \frac{1}{2}, & y > \frac{1}{2} \\ x < \frac{1}{2}, & y > \frac{1}{2} \end{array}$$

In diesen 4 Fällen ist die in $\frac{2N}{m}$ enthaltene ganze Zahl der Reihe nach die folgende:

$$\begin{array}{l} 2\omega \\ 2\omega + 1 \\ 2\omega + 1 + i \\ 2\omega + i \end{array}$$

Daraus ist ersichtlich, dass der kleinste Rest von N zum Modul m zu f, f', f'', f''' gehört, je nachdem die folgenden Bedingungen gelten, wenn man die in $\frac{2N}{m}$ enthaltene ganze Zahl $= \xi + \eta i$ setzt:

ξ gerade	η gerade
ξ ungerade	η gerade
ξ ungerade	η ungerade
ξ gerade	η ungerade

6.

Danach erhält man den Dezidenten von M zum Modul m wie folgt. Man bestimme die ganzen Zahlen, die in den einzelnen $\frac{2fM}{m}$ enthalten sind. Bezeichnet man diese allgemein mit $x + yi$, so lasse man diejenigen ganz außer Acht, bei denen x und y beide gerade sind; man rechne für jede derjenigen, bei denen x ungerade und y gerade ist, eins, nehme für jede derjenigen, bei denen x und y beide ungerade sind, zwei und für jede derjenigen, bei denen x gerade und y ungerade ist, drei. Von der Summe aller dieser Zahlen nehme man den kleinsten Rest modulo 4; dies ist der gesuchte Dezident. Wir drücken dies so aus:

$$\text{Dec.}\frac{M}{m} = \Sigma n$$

wobei $[\frac{2fM}{m}] = x + yi$ und $n = 0$ zu setzen ist, wenn x gerade und y gerade ist

1	x ungerade	y gerade
2	x ungerade	y ungerade
3	x gerade	y ungerade

Der Kürze halber wollen wir n mit der Charakteristik Θ bezeichnen, $n = \Theta\frac{2fM}{m}$*).

*) Um zu entscheiden, zu welcher Klasse M bezüglich m gehört, wählt man diejenigen Werte von k (unter den Zahlen $1, 2, 3 \ldots p-1$) aus, für die $[\frac{2km'M}{p}]$ gerade wird, und addiert $-\Sigma[\frac{2km'}{p}]^2$. Nimmt man k nur bis $\frac{1}{2}p$, so ist zu summieren

$$-\Sigma\{[\frac{2km'M}{p}]^2 + [\frac{2km'}{p}]^2\}$$

für diejenigen Werte von $[\frac{2km'M}{p}]$, die durch $1 + i$ teilbar sind.

7. 8.

Diese Regel ist allgemein, welche Zahl M auch bezeichnet. Für den Fall, der zunächst Gegenstand unserer Untersuchung sein soll, in dem M als ungerade und von der Form $1+(2+2i)N$ vorausgesetzt wird, ist eine etwas abgeänderte Regel zweckmäßiger.

Man denke sich die Zahlen f erneut in 4 Klassen zerlegt. In die erste setzt man die (h), deren Doppeltes ebenfalls in f liegt; zur zweiten, h', zählen wir diejenigen, deren Doppeltes $2h'$ zu f' gehört. Ebenso bezeichnen h'' und h''' diejenigen, deren Doppeltes zu f'' und f''' gehört. Der Dezident ε ist also

$$\varepsilon = \Sigma\Theta\frac{2hM}{m} + \Sigma\Theta\frac{2h'M}{m} + \Sigma\Theta\frac{2h''M}{m} + \Sigma\Theta\frac{2h'''M}{m}$$

Die Gesamtheit aller $2h$ und $-2h'' + (1+i)m$ nennen wir H

die aller $-i(2h' - m)$ und $i(2h''' - im)$ nennen wir H'

H und H' umfassen somit alle f; jene sind die geraden, diese die ungeraden.

Ferner sind die folgenden Beziehungen anzuwenden

$$\begin{aligned}
\Theta iN &= 1 + \Theta N \\
\Theta(-N) &= 2 + \Theta N \\
\Theta(-iN) &= 3 + \Theta N \\
\Theta(N+1) &= 1 - \Theta N \\
\Theta(N+1+i) &= 2 + \Theta N \\
\Theta(N+i) &= 3 - \Theta N
\end{aligned}$$

folglich

$$\begin{aligned}
\Theta\frac{(-2h'i + mi)M}{m} &= 3 - \Theta\frac{-2h'iM}{m} = -\Theta\frac{2h'M}{m} \\
\Theta\frac{(-2h'' + m(1+i))M}{m} &= 2 + \Theta\frac{-2h''M}{m} = \Theta\frac{2h''M}{m} \\
\Theta\frac{(2h'''i + m)M}{m} &= 1 - \Theta\frac{2h'''iM}{m} = -\Theta\frac{2h'''M}{m}
\end{aligned}$$

und

$$\begin{aligned}
\varepsilon &= \Sigma\Theta\frac{2hM}{m} - \Theta\frac{(-2h'i + mi)M}{m} \\
&\quad + \Theta\frac{(-2h'' + m(1+i))M}{m} - \Theta\frac{(2h'''i + m)M}{m} \\
&= \Sigma\Theta\frac{HM}{m} - \Sigma\Theta\frac{H'M}{m}
\end{aligned}$$

oder

$$\varepsilon = \Sigma \pm \Theta\frac{fM}{m}$$

wobei das obere Zeichen für gerade f, das untere für ungerade zu nehmen ist.

9.

Es sei nun allgemein $f = \xi + \eta i$. Die Zahlen ξ, η sind durch die Bedingung, dass f ein kleinster Rest von m ist, oder dass nach dem Ansatz $\frac{f}{m} = x + yi$ die Größen x und y zwischen den Grenzen 0 und $\frac{1}{2}$ liegen müssen, auf bestimmte Bereiche beschränkt. Durch Unterscheidung der verschiedenen Fälle ließen sich dafür leicht bestimmte Regeln angeben. Geben wir η einen bestimmten Wert, so hat wiederum ξ seine bestimmten Grenzen. Nehmen wir zum Beispiel an, dass a negativ und b positiv ist, so müssen wegen

$$x = \frac{a\xi + b\eta}{aa + bb}$$
$$y = \frac{a\eta - b\xi}{aa + bb}$$

die folgenden Bedingungen gelten:

I.	damit x positiv werde	$\xi < -\frac{b}{a}\eta$
II.	damit y positiv werde	$\xi < \frac{a}{b}\eta$
III.	damit $x < \frac{1}{2}$ werde	$\xi > \frac{aa+bb-2b\eta}{2a}$
IV.	damit $y < \frac{1}{2}$ werde	$\xi > \frac{2a\eta-aa-bb}{2b}$

Für positives η schließt die zweite Bedingung bereits die erste ein, für negatives η ist es umgekehrt. Ebenso ist die dritte Bedingung bereits in der vierten enthalten,

wenn	$\eta < \frac{1}{2}(a+b)$
und umgekehrt, wenn	$\eta > \frac{1}{2}(a+b)$

Wir brauchen jedoch nicht alle acht Fälle, die hier auftreten können, einzeln zu betrachten. Für einen bestimmten Wert von η bezeichnen wir lediglich die kleinere Grenze von ξ mit ξ^0, die größere mit ξ^{00}, und bemerken nur, dass an diesen Grenzwerten stets entweder $x = 0, y = 0, x = \frac{1}{2}, y = \frac{1}{2}$ gilt, und zwar muss Folgendes gelten:

wenn	in der *oberen* Grenze	in der *unteren* Grenze
a pos. b positiv	$x = \frac{1}{2}$ oder $y = 0$	$x = 0$ oder $y = \frac{1}{2}$
a neg. b positiv	$x = 0$ oder $y = 0$	$x = \frac{1}{2}$ oder $y = \frac{1}{2}$
a neg. b negativ	$x = 0$ oder $y = \frac{1}{2}$	$x = \frac{1}{2}$ oder $y = 0$
a pos. b negativ	$x = \frac{1}{2}$ oder $y = \frac{1}{2}$	$x = 0$ oder $y = 0$

Der Kürze halber unterscheiden wir diese vier Fälle, indem wir sagen, dass im ersten m zum ersten Quadranten gehört, im zweiten zum zweiten usw.

10.

Wir wollen nun die Summe aller $\pm\Theta\frac{fM}{m}$ näher betrachten, bei denen η einen bestimmten Wert hat. Wenn ξ nach und nach stetig vom kleinsten Wert ξ^0 zum größten ξ^{00} wächst, ändert sich auch

$$\frac{(\xi+\eta i)M}{m} = X + Yi$$

nach dem Gesetz der Stetigkeit. Liegt $\frac{M}{m}$ im ersten Quadranten, so wachsen sowohl X als auch Y fortwährend; liegt $\frac{M}{m}$ im zweiten Quadranten, so nimmt X fortwährend ab und Y zu. Im dritten Quadranten tritt das Umgekehrte des ersten, im vierten das Umgekehrte des zweiten Falls ein. Die in $X + iY$ enthaltene ganze Zahl ändert sich jedoch sprunghaft, indem sich entweder $[X]$ oder $[Y]$ um eine Einheit ändert. Die Werte von ξ, bei denen ein solcher Übergang stattfindet, das heißt, bei denen entweder X oder Y eine ganze Zahl wird, seien der Reihe nach

$$\xi',\ \xi'',\ \xi'''\ldots.\xi^n$$

Hier ist zu bemerken, dass weder diese Werte noch ξ^0 und ξ^{00} ganze Zahlen sein können, außer für $\eta = 0$, wo entweder ξ^0 oder $\xi^{00} = 0$ wird. Es sei nun

$$\begin{aligned}
\Theta\frac{(\xi'+\eta i)M}{m} - \Theta\frac{(\xi^0+\eta i)M}{m} &= \delta' \quad \text{(anders auszudrücken)}\\
\Theta\frac{(\xi''+\eta i)M}{m} - \Theta\frac{(\xi'+\eta i)M}{m} &= \delta''\\
&\text{usw.}\\
\Theta\frac{(\xi^{00}+\eta i)M}{m} - \Theta\frac{(\xi^{n-1}+\eta i)M}{m} &= \delta^n
\end{aligned}$$

Dann sieht man leicht, da zwischen ξ^0 und ξ' $[\frac{1}{2}\xi'] - [\frac{1}{2}\xi^0]$ gerade und $[\frac{1}{2}\xi' + \frac{1}{2}] - [\frac{1}{2}\xi^0 + \frac{1}{2}]$ ungerade ganze Zahlen liegen usw., dass bei Betrachtung allein des bestimmten Wertes von η gilt:

$$\begin{aligned}(\pm 1)\Sigma\Theta\frac{fM}{m} = \{&[\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi^0] - [\tfrac{1}{2}\xi' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi^0 + \tfrac{1}{2}]\}\\ &\quad .\,\Theta\frac{(\xi^0 + \eta i)M}{m}\\ &+ \{[\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi'' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi' + \tfrac{1}{2}]\}\\ &\quad .\,\{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta'\}\\ &+ \{[\tfrac{1}{2}\xi'''] - [\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi''' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi'' + \tfrac{1}{2}]\}\\ &\quad .\,\{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta' + \delta''\}\\ &+ \text{usw.}\\ &+ \{[\tfrac{1}{2}\xi^{00}] - [\tfrac{1}{2}\xi^n] - [\tfrac{1}{2}\xi^{00} + \tfrac{1}{2}] + [\tfrac{1}{2}\xi^n + \tfrac{1}{2}]\}\\ &\quad .\,\{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta' + \delta'' + \ldots + \delta^n\}\end{aligned}$$

$$\begin{aligned}= &- ([\tfrac{1}{2}\xi^0] - [\tfrac{1}{2}\xi^0 + \tfrac{1}{2}]) \,.\, \Theta\frac{(\xi^0 + \eta i)M}{m}\\ &- ([\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi' + \tfrac{1}{2}]) \,.\, \delta'\\ &- ([\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi'' + \tfrac{1}{2}]) \,.\, \delta''\\ &- \text{usw.}\\ &- ([\tfrac{1}{2}\xi^n] - [\tfrac{1}{2}\xi^n + \tfrac{1}{2}]) \,.\, \delta^n\\ &+ ([\tfrac{1}{2}\xi^{00}] - [\tfrac{1}{2}\xi^{00} + \tfrac{1}{2}]) \,.\, \Theta\frac{(\xi^{00} + \eta i)M}{m}\end{aligned}$$

(Dabei gilt das obere Zeichen für gerades η, das untere für ungerades.)

Die Zahlen $\delta', \delta'', \delta'''$ usw. können keine anderen Werte als $+1$ und -1 haben. Den Wert $+1$ erhält δ' unter den folgenden Bedingungen, wobei die Werte von X, Y, die zu ξ' gehören, mit X', Y' bezeichnet sind:

$\frac{M}{m}$ im 1. Quadr.	$\frac{M}{m}$ im 2. Quadr.
X' ganze gerade Zahl und $[Y]$ ungerade	X' ganze gerade Zahl $[Y]$ gerade
Y' ganze gerade Zahl und $[X]$ gerade	Y' ganze gerade Zahl $[X]$ gerade

$\frac{M}{m}$ im 3. Quadr.	$\frac{M}{m}$ im 4. Quadr.
X' ganze gerade Zahl und $[Y]$ gerade	X' ganze gerade Zahl $[Y]$ ungerade
Y' ganze gerade Zahl und $[X]$ ungerade	Y' ganze gerade Zahl $[X]$ ungerade

Sobald sich eine dieser Bedingungen in die entgegengesetzte ändert, wird $\delta = -1$; ändern sich beide, so bleibt $\delta = +1$.

11.

Die folgenden Formeln dienen der bequemeren Übersicht dieser Rechnungen:

$$\text{es ist } m = a + bi, \qquad aa + bb = d$$
$$M = A + Bi, \qquad AA + BB = D$$
$$\frac{dM}{m} = \alpha + \beta i, \qquad \alpha = aA + bB, \quad \beta = aB - bA$$
$$\frac{\xi + i\eta}{m} = x + iy, \qquad M(x + iy) = X + iY$$

Sind η und X gegeben, so gilt

1. $\xi = \frac{\beta\eta}{\alpha} + \frac{dX}{\alpha}$
2. $Y = \frac{D\eta}{\alpha} + \frac{\beta X}{\alpha}$

Sind η und Y gegeben, so gilt

3. $\xi = -\frac{\alpha\eta}{\beta} + \frac{dY}{\beta}$
4. $X = -\frac{D\eta}{\beta} + \frac{\alpha Y}{\beta}$

Sind η und x gegeben, so gilt

5. $\xi = -\frac{b\eta}{a} + \frac{dx}{a}$
6. $X = -\frac{B\eta}{a} + \frac{\alpha x}{a}$
7. $Y = \frac{A\eta}{a} + \frac{\beta x}{a}$

Sind η und y gegeben, so gilt

$$8.\quad \xi = \frac{a\eta}{b} - \frac{dy}{b}$$
$$9.\quad X = \frac{A\eta}{b} - \frac{\alpha y}{b}$$
$$10.\quad Y = \frac{B\eta}{b} - \frac{\beta y}{b}$$

12.

Die Regel des Artikels 10 lässt sich nun so ausdrücken. Erhält η einen bestimmten Wert, so ist

$$\Sigma \pm \Theta\frac{fM}{m} = k^0\Theta(X^0 + Y^0 i) - k^{00}\Theta(X^{00} + Y^{00}i) + \Sigma k$$

Hier ist $k^0 = 0$, wenn $[\xi^0]$ gerade ist; $k^0 = +1$, wenn $[\xi^0]$ ungerade und η gerade ist; $k^0 = -1$, wenn $[\xi^0]$ ungerade und η ungerade ist. k^{00} wird ebenso durch $[\xi^{00}]$ und η bestimmt. Schließlich ist Σk eine Summe aus so vielen Zahlen, wie es zwischen $\xi = \xi^0$ und $\xi = \xi^{00}$ ganze Werte von X oder Y gibt. Jedes Mal ist $k = 0$, wenn das entsprechende $[\xi]$ gerade ist, hingegen $= \pm 1$, wenn $[\xi]$ ungerade ist. Das Zeichen wird wie folgt bestimmt. Ist X eine ganze Zahl, so wird $k = 1$, wenn zugleich gilt:

η	gerade
X	gerade
$[Y]$	gerade
$\frac{M}{m}$	im zweiten oder dritten Quadranten d. h. α negativ

Ist eine oder sind drei dieser Bedingungen nicht erfüllt, so wird $k = -1$; fehlen zwei oder alle vier, so bleibt $k = 1$. Ist hingegen Y eine ganze Zahl, so wird $k = 1$, wenn von den 4 Bedingungen

η	gerade
Y	gerade
$[X]$	gerade
$\frac{M}{m}$	im ersten oder zweiten Quadranten d. h. β positiv

alle, zwei oder keine erfüllt sind.

13.

Jetzt müssen wir noch die Fälle einzeln betrachten, in denen ξ^0 oder ξ^{00} (oder X^0, Y^0, X^{00}, Y^{00}) eine ganze Zahl ist. Hier sind vier Fälle zu unterscheiden, wobei wir a und A als ungerade voraussetzen.

I. Liegt m im ersten Quadranten, so ist für $x = \frac{1}{2}, y = 0$ die Größe $\eta = \frac{1}{2}b$ eine ganze Zahl. Dann ist $Y^{00} = \frac{1}{2}B$ eine ganze Zahl, und $\Theta(X^{00} + Y^{00}i)$ wird nur dann $= \Theta(\frac{1}{2}A + \frac{1}{2}Bi)$ sein, wenn β negativ ist. Bei positivem β wird hingegen $\Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i)$ dafür genommen.

II. Liegt m im zweiten Quadranten, so ergibt sich für $x = 0, y = 0$ der Wert $\eta = 0$. Hier gilt für diesen Wert von η: $X^{00} = 0, Y^{00} = 0$. Man hat dann

$$\Theta(X^{00} + Y^{00}i) = \begin{array}{ll} 2, & \text{je nachdem } \frac{M}{m} \text{ im 1.} \\ 3, & \qquad\qquad\qquad\quad 2. \\ 0 & \qquad\qquad\qquad\quad 3. \\ 1 & \text{4. Quadr. liegt, und } k^{00} = 1 \end{array}$$

III. Liegt m im dritten Quadranten, so ist für $x = \frac{1}{2}, y = 0$ die Größe $\eta = \frac{1}{2}b$ eine ganze Zahl, wofür $X^0 + Y^0 i = \frac{1}{2}A + \frac{1}{2}Bi$ gilt. Man setzt dann

$$\Theta(X^0 + Y^0 i) = \Theta(\tfrac{1}{2}A + (\tfrac{1}{2}B - 1)i)$$

sooft β negativ ist.

IV. Liegt m im vierten Quadranten, so ist für $\eta = 0$ $\Theta(X^0 + Y^0 i = 0, 1, 2, 3$ zu setzen, je nachdem $\frac{M}{m}$ im 1. 2. 3. 4. Quadranten liegt; $k^0 = 0$.

14.

Aus den vorhergehenden Untersuchungen folgt nun die folgende Bestimmung des Dezidenten.

Man sammle alle Werte von x und y, die *innerhalb* der Grenzen 0 und $\frac{1}{2}$ liegen und für die entweder η und X oder η und Y ganze Zahlen sind, und bestimme für jedes $x + iy$ nach den Regeln des Artikels 12 den Wert von k.

Man sammle ferner alle Werte auf den Grenzen, das heißt, wo entweder $x = 0$ oder $\frac{1}{2}$, während y *zwischen* 0 und $\frac{1}{2}$ liegt, oder $y = 0$ oder $= \frac{1}{2}$, während x *zwischen* 0 und $\frac{1}{2}$ liegt, und die so beschaffen sind, dass η eine ganze Zahl und $[\xi]$ ungerade ist. Das zugehörige l bestimme man wie folgt. Es sei $\Theta M(x + yi) = \pm\theta$, das obere Zeichen für gerades, das untere für ungerades η

	so ist für m im			
für	1. Quadr.	2. Quadr.	3. Quadr.	4. Quadr.
$y = 0$	$l = -\theta$	$l = -\theta$	$l = +\theta$	$l = +\theta$
$x = \frac{1}{2}$	$l = -\theta$	$l = +\theta$	$l = +\theta$	$l = -\theta$
$y = \frac{1}{2}$	$l = +\theta$	$l = +\theta$	$l = -\theta$	$l = -\theta$
$x = 0$	$l = +\theta$	$l = -\theta$	$l = -\theta$	$l = +\theta$

Kürzer so:

$$l = \pm\theta,$$

das Zeichen ist dasselbe wie das von a	wenn $x = 0$
das entgegengesetzte	wenn $x = \frac{1}{2}$
dasselbe wie das von b	wenn $y = \frac{1}{2}$
das entgegengesetzte	wenn $y = 0$

Zu $\Sigma k + \Sigma l$ kommt dann noch hinzu

wenn m im zweiten Quadranten liegt: $2, 1, 0, 3$
wenn m im vierten Quadranten liegt: $0,$
} je nachdem $\frac{M}{m}$ im 1. 2. 3. 4. Quadr.

wenn m im ersten Quadranten liegt und $\frac{1}{2}(a-1)$ ungerade ist,

$$\begin{array}{ll} \Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i) & \text{wenn } \beta \text{ positiv} \\ \Theta(\frac{1}{2}A + \frac{1}{2}Bi) & \text{wenn } \beta \text{ negativ} \end{array}$$

wenn m im dritten Quadranten liegt und $\frac{1}{2}(a-1)$ ungerade ist,

$$\begin{array}{ll} -\Theta(\frac{1}{2}A + \frac{1}{2}Bi) & \text{wenn } \beta \text{ positiv} \\ -\Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i) & \text{wenn } \beta \text{ negativ.} \end{array}$$

[IV.]

1.

$$\begin{array}{ll} \text{Biquadratischer Rest?} & m = a + bi; \qquad aa + bb = d \\ \text{Modulus} & M = A + Bi, \quad AA + BB = D \end{array}$$

$$\frac{mD}{M} = \mu \qquad \mu = \alpha + \beta i, \quad \alpha = aA + bB, \quad \beta = Ab - Ba$$

$$\xi + \eta i = \pi; \quad \pi m = x + yi = p; \quad \pi M = X + Yi = P$$

Beziehungen

$$\begin{array}{lll} x = a\xi - b\eta & d\xi = ax + by & D\xi = AX + BY \\ y = b\xi + a\eta & d\eta = -bx + ay & D\eta = -BX + AY \\ X = A\xi - B\eta & dX = \alpha x + \beta y & Dx = \alpha X - \beta Y \\ Y = B\xi + A\eta & dY = -\beta x + \alpha y & Dy = \beta X + \alpha Y \end{array}$$

$$\begin{aligned} \beta\xi &= -Bx + bX = Ay - aY \\ \beta\eta &= -Ax + aX = -By + bY \\ \alpha\xi &= Ax + aY = By + aX \\ \alpha\eta &= -Bx + aY = Ay - bX \end{aligned}$$

Diejenigen π, bei denen ξ und η zwischen 0 und $\frac{1}{2}$ liegen, sollen mit π^0 bezeichnet werden, die entsprechenden p und P mit p^0 und P^0; diejenigen π, bei denen $\eta = 0$ und ξ zwischen 0 und $\frac{1}{2}$ liegt, mit π'; diejenigen, bei denen $\xi = \frac{1}{2}$ und η zwischen 0 und $\frac{1}{2}$ liegt, mit π''; diejenigen π, bei denen $\eta = \frac{1}{2}$ und ξ zwischen 0 und $\frac{1}{2}$ liegt, mit π'''; schließlich diejenigen, bei denen $\xi = 0$ und η zwischen 0 und $\frac{1}{2}$ liegt, mit π''''.

Den Dezidenten von $\frac{m}{M}$ findet man wie folgt:

Man sammle alle *ganzen* P^0, für die somit x^0 und y^0 gebrochen sind. Die jeweiligen Intensoren von p^0 seien t^0, das heißt die Zahlen $0, 1.\ 2, 3$, je nachdem

$$\begin{array}{lllll} [x^0] & \text{gerade}, & \text{ungerade}, & \text{ungerade}, & \text{gerade} \\ [y^0] & \text{gerade}, & \text{gerade}, & \text{ungerade}, & \text{ungerade} \end{array}$$

Dann ist der gesuchte Dezident $= \Sigma \pm t^0$, wobei das obere Zeichen für gerade P^0, das untere für die ungeraden zu nehmen ist.

Dies ist die *erste* Methode.

2.

Wir wollen nun die einzelnen P^0 nach den Werten von Y^0 zusammenordnen. Beschränken wir uns auf den Fall, dass a, b, A, B positiv sind, so ist der kleinste Wert durch $Y^0 \ldots +1$ angegeben, der größte durch $\frac{1}{2}(A+B-1)$. Für jeden bestimmten Wert von Y^0 müssen die Werte von X^0 zwischen bestimmten Grenzen liegen, nämlich

I. wenn $A - B$ positiv ist

wenn	zwischen	und
$Y < \frac{1}{2}B$	$-\frac{BY^0}{A}$	$\frac{AY^0}{B}$
$Y = \frac{1}{2}B$	$-\frac{BB}{2A}$	$\frac{1}{2}A$
$Y > \frac{1}{2}B$ und $< \frac{1}{2}A$	$-\frac{BY^0}{A}$	$-\frac{BY^0}{A} + \frac{D}{2A}$
$Y > \frac{1}{2}A$	$\frac{AY^0}{B} - \frac{D}{2B^0}$	$-\frac{BY^0}{A} + \frac{D}{2A}$

II. Wenn $A - B$ negativ ist,

wenn	zwischen	und
$Y < \frac{1}{2}A$	$-\frac{BY^0}{A}$	$\frac{AY^0}{B}$
$Y > \frac{1}{2}A$ und $< \frac{1}{2}B$	$\frac{AY^0}{B} - \frac{D}{2B}$	$\frac{AY^0}{B}$
$Y = \frac{1}{2}B$	$\frac{AB-D}{2B}$	$\frac{1}{2}A$
$Y > \frac{1}{2}B$	$\frac{AY^0}{B} - \frac{D}{2B}$	$-\frac{BY^0}{A} + \frac{D}{2A}$

An den kleineren Grenzen gilt entweder $\xi = 0$ oder $\eta = \frac{1}{2}$, an den größeren hingegen entweder $\eta = 0$ oder $\xi = \frac{1}{2}$. Es lässt sich leicht beweisen, dass die Grenzen von x nie ganze Zahlen sind.

3.

Wir wollen nun die Partialsummen für jedes bestimmte Y^0 anders darstellen. An den Grenzen hat p bestimmte Werte, die mit p^*, p^{**} bezeichnet seien. Während sich X stetig von der einen Grenze zur anderen ändert, geht p stetig von p^* zu p^{**} über. Die in $[p]$ enthaltene ganze Zahl ändert sich dabei jedoch sprunghaft, indem sich stets entweder der reelle oder der imaginäre Teil um eine Einheit ändert. Die Änderungen treten bei den Werten von X

$$X',\ X'',\ X'''\ldots X^\mu$$

ein, die bereits nach ihrer Größe geordnet sind und denen die Werte von p

$$p',\ p''.\ p'''\ldots$$

entsprechen.

Das letzte X^μ kann auch mit X^{**} identisch sein, wenn β positiv ist, oder X' mit X^* identisch sein usw.

Die x nehmen hier zu; wenn also x^{**} eine ganze Zahl ist, wird sie als x^μ gezählt.

Die y nehmen bei positivem β zu; dann wird y^{**} ganz mitgezählt;

bei negativem β nehmen sie ab; dann wird y^* mitgezählt.

Die Intensoren von p^*, p^{**} seien λ^* und λ^{**}

$$\begin{array}{lllll} \text{der Intensor von } p' & \text{an bis } p''\ldots & \lambda^* + \delta' \\ p'' & \text{bis } p'''\ldots & \lambda^* + \delta' + \delta'' \\ p^\mu & \text{bis } p^{**}\ldots & \lambda^* + \delta' + \delta''\ldots + \delta^\mu = \lambda^{**} \end{array}$$

Dann wird die Partialsumme, sofern Y^0 gerade ist,

$$\begin{aligned} &= \lambda^*(g-h) + (\lambda^* + \delta')(g'-h') \\ &\quad + (\lambda^* + \delta' + \delta'')(g''-h'') + \text{usw.} + \lambda^{**}(g^\mu - h^\mu) \end{aligned}$$

wobei g die Anzahl der geraden X^0 von X^* bis X' und h die der ungeraden bezeichnet.

4.

Diese Formel lässt sich auch so darstellen:

$$\begin{aligned}&\lambda^*\{[\tfrac{1}{2}X^* - \tfrac{1}{2}] - [\tfrac{1}{2}X^*]\}\\ &+ \delta'\{[\tfrac{1}{2}X' - \tfrac{1}{2}] - [\tfrac{1}{2}X']\}\\ &+ \delta''\{[\tfrac{1}{2}X'' - \tfrac{1}{2}] - [\tfrac{1}{2}X'']\}\\ &+ \text{usw.}\\ &+ \delta^\mu\{[\tfrac{1}{2}X^\mu - \tfrac{1}{2}] - [\tfrac{1}{2}X^\mu]\}\\ &- \lambda^{**}\{[\tfrac{1}{2}X^{**} - \tfrac{1}{2}] - [\tfrac{1}{2}X^{**}]\}\end{aligned}$$

oder durch

$$\lambda^*\varepsilon^* + \delta'\varepsilon' + \delta''\varepsilon'' + \text{usw.} + \delta^\mu\varepsilon^\mu - \lambda^{**}\varepsilon^{**}$$

wo allgemein $\varepsilon = 0$ wenn $[X]$ ungerade
und $= -1$ wenn $[X]$ gerade ist und Y gerade
$+1$ wenn $[X]$ gerade und Y ungerade.

Für δ hat man hingegen die Werte

		β	
		positiv	negativ
wenn x eine ganze gerade Zahl,	$[y]$ gerade	-1	-1
	$[y]$ ungerade	$+1$	$+1$
x eine ganze ungerade Zahl,	$[y]$ gerade	$+1$	$+1$
	$[y]$ ungerade	-1	-1
y eine ganze gerade Zahl,	$[x]$ gerade	-3	$+3$
	$[x]$ ungerade	-1	$+1$
y eine ganze ungerade Zahl,	$[x]$ gerade	$+3$	-3
	$[x]$ ungerade	$+1$	-1

5.

Hieraus leiten wir die folgende zweite Methode zur Bestimmung des Dezidenten ab.

I. Man sammle alle Kombinationen ganzer Werte von Y und x, die folgende Eigenschaften haben:

1. dass $\xi = \frac{Ax+bY}{\alpha}$ zwischen 0 und $\frac{1}{2}$ liegt, wobei die zweite Grenze eingeschlossen ist;

2. dass $\eta = \frac{-Bx+aY}{\alpha}$ zwischen 0 und $\frac{1}{2}$ liegt, wobei die erste Grenze eingeschlossen ist.

II. Dafür berechne man

$$X = \frac{Dx + \beta Y}{\alpha}$$
$$y = \frac{\beta x + dY}{\alpha}$$

III. Man lasse alle diejenigen weg, bei denen $[X]$ ungerade ist, und teile die übrigen, bei denen $[X]$ gerade ist, in zwei Klassen;
in die erste Klasse setze man diejenigen, bei denen zugleich gilt:

Y gerade, x gerade, $[y]$ gerade
oder wo eine dieser Bedingungen gilt;

in die zweite diejenigen, bei denen zwei dieser Bedingungen oder gar keine erfüllt sind,

oder in I. wo $[Y + x + y]$ gerade
II. wo $[Y + x + y]$ ungerade

und nenne den Überschuss der Anzahl in der ersten Klasse über die in der zweiten c.

IV. Man sammle alle Kombinationen ganzer Werte von Y und y, die folgende Eigenschaften haben:

1. dass $\xi = \frac{Ay-aY}{\beta}$ zwischen 0 und $\frac{1}{2}$ liegt, die erste Grenze eingeschlossen bei negativem β, die zweite bei positivem β;

2. dass $\eta = \frac{-By+bY}{\beta}$ zwischen 0 und $\frac{1}{2}$ liegt, die erste Grenze eingeschlossen bei positivem β, die zweite bei negativem.

[V.]

[1.]

Modulus	$M = A + Bi$	$AA + BB = D$
Rest	$m = a + bi,$	$aa + bb = d$

$$\frac{mD}{M} = \mu = \alpha + \beta i = aA + bB + (Ab - Ba)i$$

$$\xi + \eta i = \pi, \quad \pi m = p = x + yi; \quad \pi M = P = X + Yi$$

ω ist eine unbestimmte unendlich kleine reelle positive Größe.

[2.]

Vorbereitung.

I. Man sammle alle π, für die gilt:

ξ nicht negativ und nicht größer als $\frac{1}{2}$
η positiv und kleiner als $\frac{1}{2}$
Entweder x oder y eine ganze Zahl
Entweder X oder Y eine ganze Zahl

und bestimme für jedes π die Größe ε nach folgender Regel:

Es sei p^0	die nächste durch $1 + i$ teilbare ganze Zahl bei p
P^0	die nächste durch $1 + i$ teilbare ganze Zahl bei P

und setze $\varepsilon = \pm 1$, wobei das Zeichen stets dasselbe ist wie das Zeichen des imaginären Teils der Größe

$$\frac{p - p^0}{P - P^0}(\alpha - \beta i)$$

Es gelten die folgenden besonderen Regeln. Erste Klasse, x und X ganze Zahlen

$$\beta\xi = -Bx + bX$$
$$\beta\eta = -Ax + aX$$
$$\beta y = -\alpha x + dX$$
$$\beta Y = -Dx + \alpha X$$

$\varepsilon = -1$, wenn β positiv, x gerade, $[y]$ gerade, X gerade, $[Y]$ gerade ist oder wenn nur eine ungerade Anzahl dieser Bedingungen gilt.

$\varepsilon = +1$, wenn keine oder eine gerade Anzahl dieser Bedingungen gilt.

Zweite Klasse, y und Y ganze Zahlen

$$\begin{aligned}\beta\xi &= +Ay - aY\\ \beta\eta &= -By + bY\\ \beta x &= +\alpha y - dY\\ \beta X &= +Dy - \alpha Y\end{aligned}$$

$\varepsilon = -1$, wenn β positiv, $[x]$ gerade, y gerade, $[X]$ gerade, Y gerade ist oder wenn eine ungerade Anzahl dieser Bedingungen gilt.

$\varepsilon = +1$, wenn keine oder eine gerade Anzahl gilt.

Dritte Klasse, y und X ganze Zahlen

$$\begin{aligned}\alpha\xi &= +By + aX\\ \alpha\eta &= +Ay - bX\\ \alpha x &= -\beta y + dX\\ \alpha Y &= +Dy - \beta X\end{aligned}$$

$\varepsilon = -1$, wenn α positiv ist und $[x], y, X, [Y]$ alle gerade sind oder wenn eine ungerade Anzahl dieser Bedingungen gilt.

$\varepsilon = +1$, wenn keine oder eine gerade Anzahl erfüllt ist.

Vierte Klasse, x und Y ganze Zahlen

$$\begin{aligned}\alpha\xi &= +Ax + bY\\ \alpha\eta &= -Bx + aY\\ \alpha y &= +\beta x + dY\\ \alpha X &= +Dx + \beta Y\end{aligned}$$

$\varepsilon = +1$, wenn α positiv ist und $x, [y], [X], Y$ alle gerade sind oder wenn eine ungerade Anzahl dieser Bedingungen gilt.

$\varepsilon = -1$, wenn keine oder eine gerade Anzahl davon gilt.

[3.]

II. Man sammle alle π, für die gilt:

ξ positiv und kleiner als $\frac{1}{2}$
$\eta = \omega$
und entweder X oder Y eine ganze Zahl,

und setze $\varepsilon = \pm 1$, wobei das Zeichen des imaginären Teils von

$$\frac{M}{P - P^0}$$

zu nehmen ist.

Besondere Regel: erste Klasse, X ganz

$$\begin{aligned} A\xi &= +X + B\omega \\ Ax &= +aX - \beta\omega \\ Ay &= +bX - \alpha\omega \\ AY &= +BX + D\omega \end{aligned}$$

$\varepsilon = -1$, wenn A positiv ist und X und $[Y]$ gerade sind oder wenn nur eine Bedingung gilt.

$\varepsilon = +1$, wenn keine oder zwei gelten.

Zweite Klasse, Y ganz

$$\begin{aligned} B\xi &= +Y - A\omega \\ Bx &= +aY - \alpha\omega \\ By &= +bY - \beta\omega \\ BX &= +AY - D\omega \end{aligned}$$

$\varepsilon = +1$, wenn B positiv ist und $[X]$ und Y gerade sind oder wenn nur eine Bedingung gilt.

$\varepsilon = -1$, wenn keine oder zwei gelten.

[4.]

III. Man sammle alle π, für die gilt:

ξ und η unterliegen denselben Bedingungen wie in II;

entweder x oder y ist ganz,

und setze $\varepsilon = \pm 1$ mit dem Zeichen des imaginären Teils von

$$\frac{m}{p - p^0}$$

Besondere Regeln: erste Klasse, x ganz

$$\begin{aligned} a\xi &= +x + b\omega \\ ay &= +bx + d\omega \\ aX &= +Ax + \beta\omega \\ aY &= +Bx + \alpha\omega \end{aligned}$$

$\varepsilon = -1$, wenn a positiv ist und $x, [y]$ beide gerade sind oder wenn nur eine Bedingung gilt.

$\varepsilon = +1$, wenn keine oder zwei gelten.

Zweite Klasse, y ganz

$$\begin{aligned} b\xi &= +y - a\omega \\ bx &= +ay - d\omega \\ bX &= +Ay - \alpha\omega \\ bY &= +By + \beta\omega \end{aligned}$$

$\varepsilon = +1$, wenn b positiv ist und $[x]$ und y gerade sind oder wenn nur eine Bedingung gilt.

$\varepsilon = -1$, wenn keine gilt.

[5.]

IV. Man sammle alle π, für die gilt:

$$\begin{array}{l}\xi = \frac{1}{2} + \frac{1}{2}\omega \\ \eta \text{ positiv und kleiner als } \frac{1}{2} \\ X \text{ oder } Y \text{ ganz,}\end{array}$$

und setze $\varepsilon = \pm 1$ mit dem Zeichen des imaginären Teils von

$$\frac{iM}{P - P^0}$$

Besondere Regeln: erste Klasse, X eine ganze Zahl,

$$\begin{aligned} 2B\eta &= +A - 2X + A\omega \\ 2Bx &= -\beta + 2bX - \beta\omega \\ 2By &= +\alpha - 2aX + \alpha\omega \\ 2BY &= +D - 2AX + D\omega \end{aligned}$$

$\varepsilon = +1$, wenn B positiv ist und $X, [Y]$ gerade sind oder wenn eine Bedingung gilt,

$\varepsilon = -1$, wenn keine oder zwei Bedingungen gelten.

Zweite Klasse, Y eine ganze Zahl

$$\begin{aligned} 2A\eta &= -B + 2Y - B\omega \\ 2Ax &= +\alpha - 2bY + \alpha\omega \\ 2Ay &= +\beta + 2aY + \beta\omega \\ 2AX &= +D - 2BY + D\omega \end{aligned}$$

$\varepsilon = +1$, wenn A positiv ist und $[X], Y$ gerade sind oder wenn eine Bedingung gilt;
$\varepsilon = -1$, wenn keine oder zwei Bedingungen gelten.

[6.]

V. Man sammle alle π, für die gilt:

$$\xi, \eta \text{ denselben Bedingungen unterworfen sind wie in IV,}$$
$$\text{und wo } x \text{ oder } y \text{ eine ganze Zahl,}$$

und setze $\varepsilon = \pm 1$ mit dem Zeichen des imaginären Teils von

$$\frac{im}{p - p^0}$$

Besondere Regeln: erste Klasse, x eine ganze Zahl

$$\begin{aligned} 2b\eta &= +a - 2x + a\omega \\ 2by &= +d - 2ax + d\omega \\ 2bX &= +\beta + 2Bx + \beta\omega \\ 2bY &= +\alpha - 2Ax + \alpha\omega \end{aligned}$$

$\varepsilon = +1$, wenn b positiv ist und $x, [y]$ gerade sind oder wenn eine Bedingung gilt;
$\varepsilon = -1$, wenn keine oder zwei Bedingungen gelten.

Zweite Klasse, y eine ganze Zahl

$$\begin{aligned} 2a\eta &= -b + 2y - b\omega \\ 2ax &= +d - 2by + d\omega \\ 2aX &= +\alpha - 2By + \alpha\omega \\ 2aY &= -\beta + 2Ay - \beta\omega \end{aligned}$$

$\varepsilon = +1$, wenn a positiv ist und $[x], y$ gerade sind oder wenn eine Bedingung gilt;
$\varepsilon = -1$, wenn keine oder zwei Bedingungen gelten.

[7.]

Die erste Methode ergibt nun folgendes Resultat:

$$\begin{aligned} 4\,\text{Dezident} = \text{I}\quad & \Sigma\varepsilon \text{ von allen} \\ & -4\Sigma\varepsilon \text{ von denen, wo } y \text{ ganz } [x] \text{ gerade} \\ \text{II.}\quad & -\Sigma\varepsilon \text{ von allen} \\ & +4\Sigma\varepsilon \text{ von denen, wo } [x] \text{ gerade } [y] \text{ ungerade} \\ \text{IV.}\quad & +4\Sigma\varepsilon \text{ von denen, wo nicht zugleich} \\ & \qquad\qquad [x] \text{ und } [y] \text{ gerade} \\ & +Q \end{aligned}$$

Hier ist

für A	B	$Q =$
$+$	$+$	$-\text{Intens.}\ +\mu\omega i + \text{Int.}\ \frac{1}{2}m - \mu\omega$
$+$	$-$	$-\text{Intens.}\ +\mu\omega + \text{Int.}\ \frac{1}{2}mi - \mu\omega i$
$-$	$-$	$-\text{Intens.}\ -\mu\omega i - \text{Int.}\ \frac{1}{2}m + \mu\omega$
$-$	$+$	$-\text{Intens.}\ -\mu\omega - \text{Int.}\ \frac{1}{2}mi + \mu\omega i$

Die folgende Tabelle stellt dies dar:

α	β	A	B	A	B	A	B	A	B
		$+$	$+$	$+$	$-$	$-$	$-$	$-$	$+$
$+$	$+$	$+2$	0	0	$+2$	-3	-5	-3	-5
$+$	$-$	0	$+2$	-2	0	-5	-3	-1	-3
$-$	$-$	-3	-1	-1	$+1$	-4	-2	0	-2
$-$	$+$	$+1$	-1	-1	$+1$	0	-2	-4	-6
$\frac{m-1}{2}$		gerade,	ungerade						

Der erste Teil von

$$2Q \ldots -3 - (\alpha\beta AB) + (A\alpha) + (A\beta) + (B\alpha) - (B\beta)$$

Das ganze $2Q$ für

$$\begin{aligned} \tfrac{m-1}{2} \text{ ungerade}\quad & -3 + 4(A) - (B) - (\beta) + (\alpha A) + (\alpha B) \\ & + (\beta A) - (\beta B) - (\alpha\beta AB) \\ \tfrac{m-1}{2} \text{ gerade}\quad & -3 + 2(A) + (B) + (\beta) + (\alpha A) + (\alpha B) \\ & + (\beta A) - (\beta B) + 2(\beta AB) - (\alpha\beta AB) \end{aligned}$$

Beispiel

$$\begin{array}{r|l} m = +3-2i & 13 \\ M = -1-6i & 37 \end{array} \qquad \begin{array}{c} (1+i)M + (-2+i)m = 1 \\ mM = -15-16i \end{array}$$

$$\mu = +9+20i$$

$+4+13i$	$+38+31i$	$+1$	-1
$+5+7i$	$+29+11i$	0	$+0$
$+6+i$	$+20-9i$	$0-i$	-3
$+10+14i$	$+58+22i$	$+1$	$+1$
$+11+8i$	$+49+2i$	$+1$	-1
$+12+2i$	$+40-18i$	$+1-i$	$+2$
$+16+15i$	$+78+13i$	$+2$	-0
$+17+9i$	$+69-7i$	$+1-i$	$+2$
$+18+3i$	$+60-27i$	$+1-i$	-2
			Dezident $= -2$

I..	$+1$	0
II..	0	-4
IV..		0
$Q =$	-5	
	-8	

Gut.

I

x	X	20ξ	20η	$20y$	$20Y$	ε
$+1$	0	6	1	-9	-37	-1
	$+1$	4	4	$+4$	-28	-1
	$+2$	2	7	$+17$	-19	-1
$+2$	$+1$	10	5	-5	-65	-1
	$+2$	8	8	$+8$	-56	$+1$
						-3

y	Y	20ξ	20η	$20x$	$20X$	ε
0	-1	3	2	$+13$	$+9$	$+1^*$
	-2	6	4	$+26$	$+18$	$+1$
	-3	9	6	$+39$	$+27$	$+1$
$+1$	-1	2	8	$+22$	$+46$	$+1$
						$+4$
						$(+1)$

y	X	9ξ	9η	$9x$	$9Y$	ε
0	$+1$	3	2	$+13$	-20	$+1$
-2	$+2$	0	3	$+6$	-3	-1^*
						$0(-1)$

x	Y	9ξ	9η	$9y$	$9X$	ε
$+1$	-1	1	3	$+7$	$+17$	-1
$+2$	-3	4	3	$+1$	$+14$	$+1$
						0

I . . . $+1(0)$

II

Y	6ξ	$6x$	$6y$	$6X$	ε
-1	$+1$	$+3+9\omega$	-2	-1	-1^*
-2	$+2$	$+6+9\omega$	-4	-2	$+1$
					$0(-1)$

III

x	3ξ	$3y$	$3X$	$3Y$	ε
$+1$	1	-2	-1	$-6+9\omega$	-1

IV

X	12η	$12x$	$12y$	$12Y$	ε
0	$+1$	$+20+20\omega$	-9	-37	-1^*
$+1$	$+3$	$+24+20\omega$	-3	-39	$+1^*$
$+2$	$+5$	$+28+20\omega$	$+3$	-41	-1
					$-1(0)$

V

x	4η	$4y$	$4X$	$4Y$	ε
$+2$	$+1$	-1	$+4-20\omega$	-13	$+1$

y	6η	$6x$	$6X$	$6Y$	ε
0	$+2$	$+13$	$+9$	-20	$+1$

[8.]

Wir wollen nun das Resultat von I näher betrachten. Es gibt vier Kombinationen:
1^0, wenn x und X ganze Zahlen sind. Hier gilt

$$\begin{aligned}\beta\xi &= -Bx + bX\\ \beta\eta &= -Ax + aX\\ \beta y &= -\alpha x + dX\\ \beta Y &= -Dx + \alpha X\end{aligned}$$

Es seien y^0 und Y^0 die absolut kleinsten Reste von $-\alpha x + dX$, $-Dx + \alpha X$ modulo β und $\beta y = \beta y' + y^0$, $\beta Y = \beta Y' + Y^0$, und man setze

$$\begin{aligned} \beta u &= -By^0 + bY^0 \qquad & y^0 &= +au - bt \\ \beta t &= -Ay^0 + aY^0 \qquad & Y^0 &= +Au - Bt \end{aligned}$$

Dann werden t, u ganze Zahlen sein, nämlich

$$\begin{aligned} -u + ti &= M(x + y'i) - m(X + Y'i)\ ^* \\ i(t + ui) &= Mi(y' - y) - mi(Y' - Y) \end{aligned}$$

und es gilt dann $\varepsilon = -1$, wenn
$t + u$ gerade und β, y^0, Y^0 positiv sind oder wenn zwei oder keine Bedingung gilt; sonst $\varepsilon = +1$.

Wir setzen

$$\begin{aligned} t + ui = +\theta &\quad \text{wenn } y^0 \text{ und } Y^0 \text{ beide positiv} \\ -\theta &\quad y^0 \text{ und } Y^0 \text{ beide negativ} \\ +\theta' &\quad y^0 \text{ positiv } Y^0 \text{ negativ} \\ -\theta' &\quad y^0 \text{ negativ } Y^0 \text{ positiv} \end{aligned}$$

jedem durch $1+i$ teilbaren	θ	entspricht dann ein	$\varepsilon = -1$
jedem durch $1+i$ teilbaren	θ'		$\varepsilon = +1$
jedem durch $1+i$ nicht teilbaren	θ		$\varepsilon = +1$
jedem durch $1+i$ nicht teilbaren	θ'		$\varepsilon = -1$

sofern β positiv ist.

Für negatives β ist die Regel umgekehrt.

x	X	y^0	Y^0	$t+ui$	θ	θ'	ε
$+1$	0	-9	$+3$	$0-3i$		$0+3i$	-1
	$+1$	$+4$	-8	$-1+2i$		$-1+2i$	-1
	$+2$	-3	$+1$	$0-i$		$0+i$	-1
$+2$	$+1$	-5	-5	$-1-i$	$+1+i$		-1
	$+2$	$+8$	$+4$	$+1+2i$	$+1+2i$		$+1$

[9.]

2^0, wenn y und Y ganze Zahlen sind. Hier seien x', X' die nächsten ganzen Zahlen bei x und X, und

$$x - x' = \frac{x^0}{\beta}, \quad X - X' = \frac{X^0}{\beta}$$

und man setze

$$\begin{aligned} \beta(t + ui) &= -Mx^0 + mX^0 = -Mp^0 + mP^0, \\ t + ui &= Mp' - mP' \end{aligned}$$

das heißt,

$$\beta t = -Ax^0 + aX^0 \qquad x^0 = -bt + au$$
$$\beta u = -Bx^0 + bX^0 \qquad X^0 = -Bt + Au$$

Es gilt dann

$\varepsilon = -1$, wenn β positiv, x^0 positiv, X^0 positiv, $t+u$ gerade
usw.

Wir setzen

		besser
$t+ui = +\theta$	wenn x^0 und X^0 positiv	$+\theta''$
$= -\theta$	wenn beide negativ	$-\theta''$
$= +\theta'$	wenn x^0 positiv, X^0 negativ	$-\theta$
$= -\theta'$	wenn x^0 negativ, X^0 positiv	$+\theta$

wobei für ε dieselbe Regel wie oben gelten wird.

y	Y	x^0	X^0	$t+ui$	θ	θ'	ε
0	-1	-7	$+9$	$+1-3i$		$-1+3i$	$+1$
	-2	$+6$	-2	$0+2i$		$0+2i$	$+1$
	-3	-1	$+7$	$+1-i$		$-1+i$	$+1$
$+1$	-1	$+2$	$+6$	$+1$	$+1$		$+1$

Man kann nun beweisen:

1) Dass alle θ, die aus (1) und aus (2) hervorgegangen sind, voneinander verschieden sind. Ihre Gesamtheit heiße Θ.

2) Dass alle $\theta = T + Ui$ die Eigenschaft haben, dass

$$-bT + aU$$
$$-BT + AU$$

positive Zahlen kleiner als $\frac{1}{2}\beta$ sind.

3) Dass, wenn T, U zwei ganze Zahlen sind, die den eben genannten Bedingungen unterliegen, $T + Ui$ gewiss in Θ liegt.

(Wie denn? Es wird auf die obige Gleichung * gegründet.)

4) Ähnlich verhält es sich mit θ', deren Gesamtheit Θ' aus denjenigen Zahlen $T' + U'i$ bestehen wird, für die

$$-bT' + aU'$$
$$-(-BT' + AU')$$

positive Zahlen kleiner als $\frac{1}{2}\beta$ sind.

In unserem Fall gilt

θ	ε	θ'	ε	θ''	ε	θ'''	ε
$+1$	$+1$	$0+i$	-1	$+2-i$	$+1$	$+1$	-1
$+1+i$	-1	$0+2i$	$+1$	$+3-i$	-1	$+2$	$+1$
$+1+2i$	$+1$	$0+3i$	-1				
		$-1+i$	$+1$				
		$-1+2i$	-1				
		$-1+3i$	$+1$				

Hier ist

$$\theta = -_*M + {}_*m$$
$$\theta' = -_*M - {}_*m$$
$$\theta'' = +_*Mi + {}_*m$$
$$\theta''' = +_*Mi - {}_*m$$

[10.]

3^0. y und X ganze Zahlen. Es seien x', Y' die nächsten ganzen Zahlen bei x und Y, und

$$x' + yi = p', \quad X + Y'i = P'; \quad p - p' = \frac{p^0}{\alpha}, \quad P - P' = \frac{P^0}{\alpha}$$

und man setze

$$i(t+ui) = Mp' - mP' = -\frac{Mp^0}{\alpha} + \frac{mP^0}{\alpha}$$
$$= -\frac{Mx^0}{\alpha} + \frac{miY^0}{\alpha} \quad \text{d. h.}$$

$$\alpha t = -Bx^0 + aY^0 \quad \text{so ist} \quad x^0 = -bt + au$$
$$\alpha u = +Ax^0 + bY^0 \qquad\qquad Y^0 = +At + Bu$$

Es gilt dann

$\varepsilon = -1$, wenn α positiv, x^0 positiv, Y^0 positiv, $t+u$ gerade usw.

Wir setzen

		besser
$t+ui = +\theta''$	wenn x^0 positiv, Y^0 positiv	$+\theta'$
$= +\theta'''$	wenn x^0 positiv, Y^0 negativ	$-\theta'''$
$-\theta''$	wenn x^0 negativ, Y^0 negativ	$-\theta'$
$-\theta'''$	wenn x^0 negativ, Y^0 positiv	$+\theta'''$

Es wird also für jedes $\theta'' \ldots \varepsilon = -1$
$\theta''' \ldots \varepsilon = +1$

sofern θ'' oder θ''' durch $1+i$ teilbar und α positiv ist.

y	X	x^0	X^0	$t+ui$	θ''	θ'''	ε
0	+1	+4	−2	+2		+2	+1
+1	+2	−3	−3	$-3+i$	$+3-i$		−1

[11.]

Klasse 4, x und Y ganze Zahlen. Unter ähnlichen Voraussetzungen wie in 3 setze man

$$-(t+ui) = Mp' - mP' = -\frac{Mp^0}{\alpha} + \frac{mP^0}{\alpha}$$
$$= -\frac{Miy^0}{\alpha} + \frac{mX^0}{\alpha}$$
$$\alpha t = -By^0 - aX^0 \qquad y^0 = -bt + au$$
$$\alpha u = +Ay^0 - bX^0 \qquad X^0 = -At - Bu$$

Es gilt dann

$\varepsilon = +1$ wenn α positiv, y^0 positiv, X^0 positiv, $t+u$ gerade usw.

Wir setzen

$$\begin{array}{rl} t+ui = +\theta'' & \text{wenn } y^0 \text{ positiv } X^0 \text{ negativ} \\ +\theta''' & \text{wenn } y^0 \text{ positiv } X^0 \text{ positiv} \\ -\theta'' & \text{wenn } y^0 \text{ negativ } X^0 \text{ positiv} \\ -\theta''' & \text{wenn } y^0 \text{ negativ } X^0 \text{ negativ} \end{array}$$

Für ε gilt dann die Regel (wie oben in 3), sofern α positiv ist:

$$\varepsilon = -1 \text{ für jedes durch } 1+i \left\{ \begin{array}{ll} \text{teilbare} & \theta'' \\ \text{nicht teilbare} & \theta''' \end{array} \right.$$

$$\varepsilon = +1 \text{ für jedes durch } 1-i \left\{ \begin{array}{ll} \text{teilbare} & \theta''' \\ \text{nicht teilbare} & \theta'' \end{array} \right.$$

x	Y	y^0	X^0	$t+ui$	θ''	θ'''	ε
$+1$	-1	-2	-1	-1		$+1$	-1
$+2$	-3	$+1$	-4	$+2-i$	$+2-i$		$+1$

Die Gesamtheit aller θ'' aus 3 und 4, die wir mit Θ'' bezeichnen, besteht also aus allen Zahlen $T+Ui$, für die

$$\left.\begin{array}{r} -bT+aU \\ \text{und } +AT+BU \end{array}\right\} \text{ positiv und kleiner als } \frac{1}{2}\alpha$$

die Gesamtheit aller $\theta''' \ldots$ (Θ''') aus denen, für die

$$\left.\begin{array}{r} -bT+aU \\ -AT-BU \end{array}\right\} \text{ positiv und kleiner als } \frac{1}{2}\alpha$$

[12.]

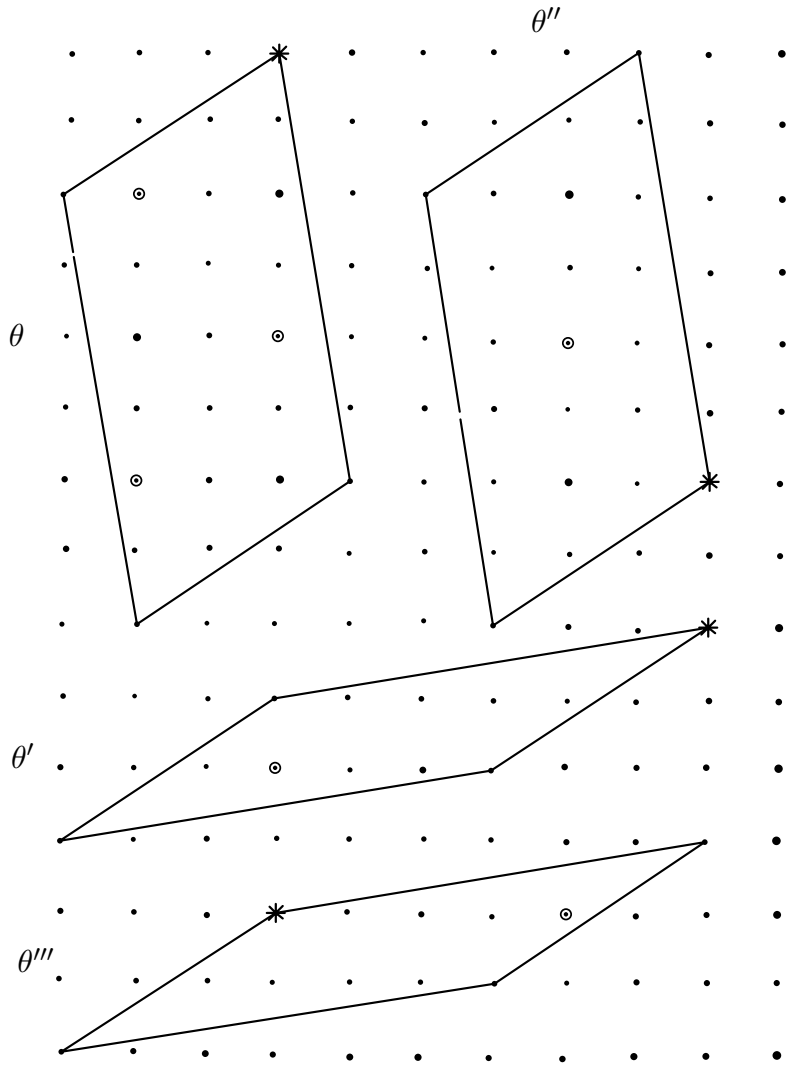
Nach der obigen Verbesserung lautet die Regel also so:
Es enthalte

$$\begin{aligned}
\Theta &\quad \text{alle Zahlen } T+Ui, \text{ wo } +bT-aU \text{ positiv} \\
&\qquad -BT+AU \text{ positiv und } < \tfrac{1}{2}\beta \\
\Theta' &\quad \text{alle Zahlen } T+Ui, \text{ wo } -bT+aU \text{ positiv} \\
&\qquad +AT+BU \text{ positiv und } < \tfrac{1}{2}\alpha \\
\Theta'' &\quad \text{alle Zahlen } T+Ui, \text{ wo } -bT+aU \text{ positiv} \\
&\qquad -BT+AU \text{ positiv und } < \tfrac{1}{2}\beta \\
\Theta''' &\quad \text{alle Zahlen } T+Ui, \text{ wo } +bT-aU \text{ positiv} \\
&\qquad +AT+BU \text{ positiv und } < \tfrac{1}{2}\alpha
\end{aligned}$$

sofern jeweils β oder α positiv ist.

Für alle durch $1+i$ teilbaren	ist dann $\varepsilon =$	wenn
θ	$+1$	β positiv
θ'	-1	α positiv
θ''	-1	β positiv
θ'''	$+1$	α positiv

Θ		Θ'		Θ''		Θ'''	
$0-i$	-1	$+2-i$	$+1$	$+1$	$+1$	-1	-1
$0-2i$	$+1$	$+3-i$	-1	$+1+i$	-1	-2	$+1$
$0-3i$	-1			$+1+2i$	$+1$		
$+1-i$	$+1$						
$+1-2i$	-1						
$+1-3i$	$+1$						



[13.]

Daraus folgt die folgende Regel. Es seien die Resultate aus den Vorschriften

$$\text{II}\ldots\ G,\quad \text{III}\ldots\ g,\quad \text{IV}\ldots\ H,\quad \text{V}\ldots\ h$$

Dann gilt

$$\begin{aligned} 4\Theta &= R = 0 \\ 4\Theta' &= -g + G - h - H + R' \\ 4\Theta'' &= -2g + 2G + R'' \\ 4\Theta''' &= -g + G + h + H + R''' \end{aligned}$$

In unserem Beispiel gilt

$$\begin{gathered} G = 0, \quad g = -1, \quad H = -1, \quad h = +2, \\ R' = 0, \quad R'' = +2, \quad R''' = -2 \\ 4\Theta = 0, \quad 4\Theta' = +1 - 1 + 0 = 0, \\ 4\Theta'' = +2 + 2 = +4, \quad 4\Theta''' = +1 + 1 - 2 = 0 \end{gathered}$$

und die Korrekturen R, R' usw. werden folgendermaßen bestimmt:

$$R = \begin{cases} -(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) - \frac{1}{2}(B) \\ +(\beta) - \frac{1}{2}(\alpha\beta) - \frac{1}{2}(\alpha\beta abAB) \\ +\frac{1}{2}(b) + \frac{1}{2}(B) \end{cases}$$

$$R' = \begin{cases} +(\alpha) - \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) - \frac{1}{2}(A) \\ 0 \\ -\frac{1}{2}(a) + \frac{1}{2}(B) \end{cases}$$

$$R'' = \begin{cases} +(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(B) \\ +(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(B) \end{cases}$$

$$R''' = \begin{cases} -(\alpha) - \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(A) \\ 0 \\ +\frac{1}{2}(a) + \frac{1}{2}(B) \end{cases}$$

wobei die Größen in Klammern nur die Zeichen angeben.

Es gilt also

$$R + R' + R'' + R''' = 2(\alpha\beta abAB) - 2(b) + 2(B) + 2(\beta)$$

folglich

$$\begin{aligned} \Theta + \Theta' + \Theta'' + \Theta''' = & -g + G + \tfrac{1}{2}(\alpha\beta abAB) \\ & + \tfrac{1}{2}(\beta) - \tfrac{1}{2}(b) + \tfrac{1}{2}(B) \\ = & -g + G + S \end{aligned}$$

ab		+	+		−	+		−	−		+	−	
A	B	α	β	S	α	β	S	α	β	S	α	β	S
+	+	+	+	+1	−	+	+1	−	−	+1	+	−	+1
		+	−	−1	+	+	0	−	+	+1	−	−	0
−	+	+	−	0	+	+	+1	−	+	+2	−	−	+1
		−	−	−1	+	−	−1	+	+	+1	−	+	+1
−	−	−	−	−1	+	−	−1	+	+	+1	−	+	+1
		−	+	−1	−	−	−2	+	−	−1	+	+	0
+	−	−	+	0	−	−	−1	+	−	0	+	+	+1
		+	+	−1	−	+	−1	−	−	−1	+	−	−1

[14.]

Danach erhält die erste Regel nun folgende Gestalt:

$4\,\text{Dez.} =$ I. $-4\Sigma\varepsilon$ von denen, für die y ganz, $[x]$ gerade
II. $+4\Sigma\varepsilon$ von denen, für die $[x]$ gerade, $[y]$ ungerade
III. $-\Sigma\varepsilon$ von allen
IV. $+4\Sigma\varepsilon$ von denen, für die nicht zugleich $[x]$ und $[y]$ gerade
$+Q+S$

In unserem Beispiel

I....	0
II....	−4
III	+1
IV	0
Q	−5
S	0
	−8

Man denke sich nun in III diejenigen besonders markiert, für die y ganz und $[x]$ gerade ist. Dann gilt

$$\left.\begin{array}{l}\text{III. } \Sigma\varepsilon \text{ von allen}\\ \qquad -4\Sigma\varepsilon \text{ der besonders markierten}\end{array}\right\} = \text{Intensor } (\tfrac{1}{2}-\omega)m - \text{Intens. } \omega m = -W$$

Hier ist

	a	b		
	+	+	−3	−1
	−	+	−2	0
$W=$	−	−	+2	0
	−	+	+3	+1
			$\frac{m-1}{2}$ gerade	$\frac{m-1}{2}$ ungerade

Also

$$
\begin{aligned}
4\,\text{Dezident} = {} & \text{I. } -4\Sigma\varepsilon \quad y \text{ ganz, } [x] \text{ gerade} \\
& \text{II. } +4\Sigma\varepsilon \quad [x] \text{ gerade, } [y] \text{ ungerade} \\
& \text{III. } -4\Sigma\varepsilon \quad y \text{ ganz, } [x] \text{ gerade} \\
& \text{IV. } +4\Sigma\varepsilon \quad \text{alle, für die nicht zugleich } [x], [y] \text{ gerade} \\
& +Q+S+W
\end{aligned}
$$

Tabelle für $\frac{1}{4}(Q+S+W)$

a	b	A	B	α	β			a	b	A	B	α	β		
+	+	+	+	+	+	0	0	−	−	+	+	−	−	0	0
				+	−	−1	0					−	+	+1	0
		−	+	+	−	−1	−1			−	+	−	+	0	−1
				−	−	−1	−1					+	+	0	−1
		−	−	−	−	−2	−1			−	−	+	+	0	−1
				−	+	−1	−1					+	−	−1	−1
		+	−	−	+	−1	0			+	−	+	−	0	0
				+	+	−1	0					−	−	0	0
−	+	+	+	−	+	0	0	+	−	+	+	+	−	+1	+1
				+	+	0	0					−	−	0	0
		−	+	+	+	−1	−1			−	+	−	−	+1	0
				+	−	−1	−1					−	+	0	−1
		−	−	+	−	−2	−1			−	−	−	+	+1	0
				−	−	−2	−1					+	+	0	−1
		+	−	−	−	−1	0			+	−	+	+	+1	+1
				−	+	−1	0					+	−	0	0

[15.]

Die zweite Methode ist folgende:

Dezident = I. $+\Sigma\varepsilon$, für die Y ganz, $[X]$ gerade
$-4\Sigma\varepsilon$, unter diesen, für die auch y ganz, $[x]$ gerade
II. $+\Sigma\lambda\varepsilon$, für die Y ganz, $[X]$ gerade;
λ ist der Intensor von p
II. $-\Sigma\lambda'\varepsilon$, für die X ganz, $[Y]$ ungerade
λ' der Intensor von $ip = 1, 2, 3, 0$
wenn $\lambda = 0, 1, 2, 3$
IV. $+\Sigma\lambda\varepsilon$, für die Y ganz, $[X]$ gerade,
λ der Intensor von p
IV. $+\Sigma\lambda'\varepsilon$, für die X ganz, $[Y]$ gerade
λ' der Intensor von $im - ip = 0 \quad 3 \quad 2 \quad 1$
wenn Int. $p = 0 \quad 1 \quad 2 \quad 3$
$+ q$

Hier ist $q = 0$, wenn $\frac{M-1}{2}$ ungerade, das heißt nur durch $1+i$, nicht durch 2 teilbar ist und nicht zugleich $AB\ +\ -$ gilt; sonst hingegen

A	B		α	β	α	β	α	β	α	β
$+$	$+$	Int. $\frac{1}{2}(m-\omega\mu)$	$+3$	$+1$	$+3$	$+1$	$+0$	$+2$	$+0$	$+2$
$-$	$+$	0		0		0		0		
$-$	$-$	$-$Int. $\frac{1}{2}(m+\omega\mu)$	-0	-2	-0	-2	-3	-1	-3	-1
$+$	$-$	$-$Int. $\omega\mu$		-0		-1		-2		-3

Wo zwei Zahlen stehen, gilt die erste für gerades $\frac{m-1}{2}$, die andere für ungerades.

In unserem Beispiel:

I.	y	Y	$20x$	$20Y$	ε	
	0	-1	$+13$	$+9$	$+1^*$	$+3$
	0	-2	$+26$	$+18$	$+1$	-4
	$+1$	-1	$+22$	$+46$	$+1$	-1
					$+3(+1)$	Dez. $= -2$

II. Fehlen.

IV.	X	$12x$	$12y$	$12Y$	ε	λ	λ'	$\lambda'\varepsilon$
	0	$+20+20\omega$	-9	-37	-1	2	2	-2
	$+1$	$+24+20\omega$	-3	-39	$+1$	3	1	$+1$
	$+2$	$+28+20\omega$	$+3$	-41	-1	0	0	0
								-1

Die Beiträge aus II vereinigen sich zu folgendem Resultat:

$$\begin{aligned}
\text{II. } &-\Sigma\varepsilon, \text{ für die } Y \text{ ganz, } [X] \text{ gerade}\\
&+4\Sigma\varepsilon, \text{ von eben diesen, wenn zugleich } [x] \text{ gerade,}\\
&\quad [y] \text{ ungerade}\\
\text{II. } &+\Sigma\lambda'\varepsilon, \text{ für die } Y \text{ ganz, } [X] \text{ gerade}\\
&-\Sigma\lambda'\varepsilon, \text{ für die } X \text{ ganz, } [Y] \text{ ungerade,}\\
&\quad \lambda' \text{ der Intensor von } ip
\end{aligned}$$

Die letzten beiden Teile vereinigen sich wiederum zu

$$\begin{aligned}
\text{III. } &+\Sigma\varepsilon, \text{ für die } [X] \text{ gerade, } [Y] \text{ ungerade}\\
&-4\Sigma\varepsilon, \text{ wenn zugleich } x \text{ eine ganze Zahl, } [y] \text{ ungerade}\\
&+r+s
\end{aligned}$$

wobei $r=0$, wenn $AB\ldots\ldots\left\{\begin{array}{cc}+&+\\-&+\\-&-\end{array}\right.$

und $r = \text{Int. } \omega mi$, wenn $AB\ldots+\ -$

$$s = -\text{Int. } (\tfrac{1}{2}-\omega)mi, \quad \text{wenn } \frac{M-1}{2} \text{ gerade und } B \text{ positiv,}$$
$$\text{in allen anderen Fällen } = 0$$

In unserem Beispiel

$$\text{III. Fällt aus.} \quad r=0,\ s=0$$

Die Beiträge aus IV vereinigen sich zu folgendem Resultat:

$$\begin{aligned}
\text{IV. } &+4\Sigma\varepsilon, \text{ für die } Y \text{ ganz, } [X] \text{ gerade und nicht zugleich}\\
&\quad [x] \text{ gerade, } [y] \text{ gerade}\\
&-\Sigma\lambda'\varepsilon, \text{ für die } Y \text{ ganz, } [X] \text{ gerade}\\
&+\Sigma\lambda'\varepsilon, \text{ für die } X \text{ ganz, } [Y] \text{ gerade}\\
&\quad \text{für die } \lambda' \text{ Int. von } im-ip
\end{aligned}$$

Die letzten beiden Teile vereinigen sich wiederum zu

$$\begin{aligned}
\text{V. } &+\Sigma\varepsilon, \text{ wo nicht zugleich } [X] \text{ und } [Y] \text{ gerade}\\
&-4\Sigma\varepsilon, \text{ wo zugleich } x \text{ eine ganze Zahl, } [y] \text{ gerade}\\
&+w
\end{aligned}$$

Hier ist $w=0$, wenn $\frac{M-1}{2}$ gerade und A positiv ist; in allen übrigen Fällen

$$= -\text{Intensor } (\tfrac{1}{2}i+\omega)m$$

In unserem Beispiel

V.

y	$6x$	$6X$	$6Y$	ε
0	+13	+9	−20	+1

$$w = -2$$

Tafel für q, r, s, w und deren Summe.

a	b	A	B	α	β	$\frac{M-1}{2}$ ger. $\frac{m-1}{2}$ ger.	$\frac{M-1}{2}$ ung. $\frac{m-1}{2}$ ger.	$\frac{M-1}{2}$ ger. $\frac{m-1}{2}$ ung.	$\frac{M-1}{2}$ ung. $\frac{m-1}{2}$ ung.
+	+	+	+	+	+	+3 0 0 0 +3	0 0 0 0 0	+1 0 −2 0 −1	0 0 0 −2 −2
				+	−	0 0 0 0 0	0 0 0 0 0	+2 0 −2 0 0	0 0 0 −2 −2
			−	+	+	0 0 0 0 0	0 0 0 0 0	0 0 −2 −2 −4	0 0 0 −2 −2
				−	−	0 0 0 0 0	0 0 0 0 0	0 0 −2 −2 −4	0 0 0 −2 −2
			−	−	−	−3 0 0 0 −3	0 0 0 0 0	−1 0 0 −2 −3	0 0 0 −2 −2
				−	+	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
		+	−	−	+	−1 +1 0 0 0	−1 +1 0 0 0	−1 +1 0 0 0	−1 +1 0 −2 −2
				+	+	0 +1 0 0 +1	0 +1 0 0 +1	0 +1 0 0 +1	0 +1 0 −2 −1
	−	+	+	−	+	+3 0 0 0 +3	0 0 0 −1 −1	+1 0 −2 0 −1	0 0 0 −3 −3
				+	+	+3 0 0 0 +3	0 0 0 −1 −1	+1 0 −2 0 −1	0 0 0 −3 −3
			−	+	+	0 0 0 −1 −1	0 0 0 −1 −1	0 0 −2 −3 −5	0 0 0 −3 −3
				+	−	0 0 0 −1 −1	0 0 0 −1 −1	0 0 −2 −3 −5	0 0 0 −3 −3
			−	−	+	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
				−	−	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
		+	−	−	−	−2 +2 0 0 0	−2 +2 0 −1 −1	−2 +2 0 0 0	−2 +2 0 −3 −3
				−	+	−1 +2 0 0 +1	−1 +2 0 −1 0	−1 +2 0 0 +1	−1 +2 0 −3 −2
	−	−	+	−	−	0 0 −1 0 −1	0 0 0 −1 −1	+2 0 −3 0 −1	0 0 0 −3 −3
				−	+	+3 0 −1 0 +2	0 0 0 −1 −1	+1 0 −3 0 −2	0 0 0 −3 −3
			−	+	−	0 0 −1 −1 −2	0 0 0 −1 −1	0 0 −3 −3 −6	0 0 0 −3 −3
				+	+	0 0 −1 −1 −2	0 0 0 −1 −1	0 0 −3 −3 −6	0 0 0 −3 −3
			−	−	+	0 0 0 −1 −1	0 0 0 −1 −1	−2 0 0 −3 −5	0 0 0 −3 −3
				+	−	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
		+	−	+	−	−3 +3 0 0 0	−3 +3 0 −1 −1	−3 +3 0 0 0	−3 +3 0 −3 −3
				−	−	−2 +3 0 0 +1	−2 +3 0 −1 0	−2 +3 0 0 +1	−2 +3 0 −3 −2
	+	−	+	+	−	0 0 −1 0 −1	0 0 0 0 0	+2 0 −3 0 −1	0 0 0 −2 −2
				−	−	0 0 −1 0 −1	0 0 0 0 0	+2 0 −3 0 −1	0 0 0 −2 −2
			−	+	−	0 0 −1 0 −1	0 0 0 0 0	0 0 −3 −2 −5	0 0 0 −2 −2
				−	+	0 0 −1 0 −1	0 0 0 0 0	0 0 −3 −2 −5	0 0 0 −2 −2
			−	−	−	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
				+	+	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
		+	−	+	+	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 −2 −2
				+	−	−3 0 0 0 −3	−3 0 0 0 −3	−3 0 0 0 −3	−3 0 0 −2 −5

[16.]

Es gilt folglich

$$\text{Dez. } \frac{m}{M} - \text{Dez. } \frac{M}{m} =$$

I. $-4\Sigma\varepsilon$, für die y, Y ganz, $[x], [X]$ gerade

II. $+4\Sigma\varepsilon$, Y ganz, $[X]$ gerade, $[x]$ gerade, $[y]$ ungerade

III. $-4\Sigma\varepsilon$, x ganz, $[X]$ gerade, $[Y]$ ungerade, $[y]$ ungerade

IV. $+4\Sigma\varepsilon$, Y ganz, $[X]$ gerade, und nicht zugleich $[x], [y]$ gerade

V. $-4\Sigma\varepsilon$, x ganz, $[y]$ gerade und nicht zugleich $[X], [Y]$ gerade

$+\psi$

Hier ist ψ in folgender Tabelle dargestellt:

a	b	A	B	α	β	ψ	a	b	A	B	α	β	ψ
+	+	+	+	+	+	+4 0 0 −2	−	−	+	+	−	−	0 0 0 −2
		+	+	+	−	0 0 0 −2			+	+	−	+	+4 0 0 −2
		−	+	+	−	0 −4 0 −2			−	+	−	+	0 −4 0 −2
		−	+	−	−	0 −4 0 −2			−	+	+	+	0 −4 0 −2
		−	−	−	−	−4 −4 0 −2			−	−	+	+	0 −4 0 −2
		−	−	−	+	0 −4 0 −2			−	−	+	−	−4 −4 0 −2
		+	−	−	+	0 0 0 −2			+	−	+	−	0 0 0 −2
		+	−	+	+	0 0 0 −2			+	−	−	−	0 0 0 −2
−	+	+	+	−	+	+4 0 0 −2	+	−	+	+	+	−	0 0 0 −2
		+	+	+	+	+4 0 0 −2			+	+	−	−	0 0 0 −2
		−	+	+	+	0 −4 0 −2			−	+	−	−	0 −4 0 −2
		−	+	+	−	0 −4 0 −2			−	+	−	+	0 −4 0 −2
		−	−	+	−	−4 −4 0 −2			−	−	−	+	0 −4 0 −2
		−	−	−	−	−4 −4 0 −2			−	−	+	+	0 −4 0 −2
		+	−	−	−	0 0 0 −2			+	−	+	+	0 0 0 −2
		+	−	−	+	0 0 0 −2			+	−	+	−	−4 −4 −4 −6

Hier gelten die ersten beiden Spalten	für $\frac{1}{2}(M-1)$ gerade
die letzten beiden	für $\frac{1}{2}(M-1)$ ungerade
die erste und dritte	für $\frac{1}{2}(m-1)$ gerade
die zweite und vierte	für $\frac{1}{2}(m-1)$ ungerade

[17.]

Die 128 Fälle, die in der obigen Tafel bei der Bestimmung von ψ unterschieden werden, lassen sich viel kürzer folgendermaßen zusammenfassen:

$$\psi = k + l$$

$k = -4$, wenn $a, A, \alpha, b, B, \beta$ gleichzeitig die Zeichen $+\ +\ +\ -\ -\ -$ haben, sonst stets

$$k = 0$$

$\frac{1}{2}(M-1)$ gerade	$\frac{1}{2}(m-1)$ gerade	$l = +4,$	wenn $AB\beta$ positiv
		$-4,$	wenn $AB\beta$ negativ
		$0,$	in allen übrigen Fällen
$\frac{1}{2}(M-1)$ gerade	$\frac{1}{2}(m-1)$ ungerade	$l = -4,$	wenn A negativ
		$0,$	wenn A positiv
$\frac{1}{2}(M-1)$ ungerade	$\frac{1}{2}(m-1)$ gerade	$l = 0$	
$\frac{1}{2}(M-1)$ ungerade	$\frac{1}{2}(m-1)$ ungerade	$l = -2$	

Es ist noch zu versuchen, ob es vorteilhafter ist, A und a positiv, dagegen aber $m \equiv 1$, $M \equiv 1$ nur modulo 2 (nicht modulo $2 + 2i$) zu nehmen. Das Endresultat muss sein

$$\text{Dez.}\ \frac{m}{M} - \text{Dez.}\ \frac{M}{m} \equiv$$

	$M \equiv$			
$m \equiv$	1	$1+2i$	3	$3+2i$
1	0	0	0	0
$1+2i$	0	2	2	0
3	0	2	0	2
$3+2i$	0	0	2	2

Alles modulo 4.

[VI.]

Theorie der biquadratischen Reste.

1.

Eine Folge komplexer ganzer Zahlen $\varphi, \varphi', \varphi''$ usw. sei so beschaffen, dass sie erstens modulo $\mu = \alpha + \beta i$ alle paarweise inkongruent sind, wobei α und β ganze reelle Zahlen bezeichnen, und dass zweitens jede komplexe ganze Zahl modulo μ einer von ihnen kongruent ist. Unter dieser Voraussetzung heißt die Gesamtheit der Zahlen $\varphi, \varphi', \varphi''$ usw. ein vollständiges Restsystem für den Modul μ. Es ist bewiesen, dass die Anzahl seiner Zahlen gleich der Norm von μ ist, also der Zahl $\alpha\alpha + \beta\beta$, die mit ν bezeichnet werden soll.

2.

Unter den Zahlen $\varphi, \varphi', \varphi''$ usw. ist eine durch μ teilbar. Wird sie ausgeschlossen und die Gesamtheit der übrigen mit χ bezeichnet, so bildet χ ein vollständiges System der durch den Modul nicht teilbaren Reste, deren Anzahl $= \nu - 1$ ist. Beschränken wir die Untersuchung auf ungerade Moduln, so ist $\nu - 1$ durch 4 teilbar. Dann sind ferner $f, if, -f, -if$ untereinander inkongruent; folglich sind diejenigen Zahlen in χ, die jeweils $if, -f, -if$ kongruent sind, voneinander und von f verschieden. (Assoziierte und zusammengesetzte Zahlen.)

Daraus ergibt sich eine Zerlegung von χ in vier Gruppen oder Teilsysteme $\kappa, \kappa', \kappa'', \kappa'''$. Man setzt eine beliebige Zahl aus χ, zum Beispiel φ, in die Gruppe κ und die drei den Zahlen $i\varphi, -\varphi, -i\varphi$ kongruenten Glieder von χ der Reihe nach in die Gruppen $\kappa', \kappa'', \kappa'''$. Nachdem diese vier Zahlen aus χ gestrichen sind, setzt man wieder eine beliebige der übrigen in κ und die drei auf dieselbe Weise von ihr abhängigen in $\kappa', \kappa'', \kappa'''$. So fährt man fort, bis das ganze System χ verteilt ist. Die Gruppen $\kappa, \kappa', \kappa'', \kappa'''$ sollen zusammengehörige Viertelsysteme heißen. Offenbar haben sie folgende Eigenschaften:

1) Jedes Viertelsystem besteht aus $\frac{1}{4}(\nu - 1) = \frac{1}{4}(\alpha\alpha + \beta\beta - 1)$ Zahlen.

2) Kennzeichnend für ein Viertelsystem ist, dass keine seiner Zahlen, weder selbst noch mit $i, -1$ oder $-i$ multipliziert, einer anderen Zahl aus demselben Viertelsystem kongruent ist, dass aber jede durch μ nicht teilbare Zahl, entweder selbst oder mit $i, -1$ oder $-i$ multipliziert, darin vorkommt oder einer seiner Zahlen kongruent ist.

3) So wie die Multiplikation der Zahlen in κ mit $i, -1$ und $-i$ jeweils die Zahlen in $\kappa', \kappa'', \kappa'''$ oder ihnen kongruente Zahlen ergibt, erzeugt die

Multiplikation der Zahlen in κ' mit jenen Faktoren jeweils wieder die Zahlen in $\kappa'', \kappa''', \kappa$; die Multiplikation der Zahlen in κ'' erzeugt auf ähnliche Weise die Zahlen in $\kappa''', \kappa, \kappa'$; schließlich erzeugt die Multiplikation der Zahlen in κ''' wieder $\kappa, \kappa', \kappa''$.

Der Kürze halber lässt sich diese wechselseitige Abhängigkeit der vier Viertelsysteme so ausdrücken:

$$\begin{aligned}\kappa' &\equiv i\kappa,\\ \kappa'' &\equiv -\kappa \equiv i\kappa',\\ \kappa''' &\equiv i\kappa'' \equiv -\kappa' \equiv -i\kappa.\end{aligned}$$

3.

Wenn m eine komplexe ganze Zahl bezeichnet, die mit μ keinen gemeinsamen Teiler hat, und sämtliche Zahlen eines Viertelsystems κ mit m multipliziert werden, so bilden die Produkte oder beliebige ihnen kongruente Zahlen ihrerseits ein Viertelsystem. Ebenso entstehen durch Multiplikation der Zahlen der Systeme $\kappa', \kappa'', \kappa'''$ drei weitere Viertelsysteme, die mit dem ersten zusammengehören. Der Beweis lässt sich leicht führen. Diese vier neuen Systeme mögen mit $m\kappa, m\kappa', m\kappa'', m\kappa'''$ bezeichnet werden, unabhängig davon, ob die Produkte selbst oder ihnen kongruente Zahlen gewählt werden. Im letzteren Fall kann man stets Zahlen wählen, die in einem der Systeme $\kappa, \kappa', \kappa'', \kappa'''$ liegen. So ist das System χ, wenigstens im Allgemeinen gesprochen, auf zwei verschiedene Arten in Viertelsysteme zerlegt. Nehmen wir an, dass $m\kappa$ gemeinsam hat

$$\begin{aligned}\text{mit } \kappa \ldots\ldots &\quad \lambda \text{ Zahlen}\\ \kappa' \ldots\ldots &\quad \lambda' \text{ Zahlen}\\ \kappa'' \ldots\ldots &\quad \lambda'' \text{ Zahlen}\\ \kappa''' \ldots\ldots &\quad \lambda''' \text{ Zahlen}\end{aligned}$$

Dann haben auch κ' mit $m\kappa'$, κ'' mit $m\kappa''$ und κ''' mit $m\kappa'''$ jeweils λ Glieder gemeinsam; κ'' mit $m\kappa'$, κ''' mit $m\kappa''$, κ mit $m\kappa'''$ jeweils λ' Glieder usw. Es sei ε der kleinste Rest von $\lambda' + 2\lambda'' + 3\lambda'''$ modulo 4, oder ε eine der vier Zahlen $0, 1, 2, 3$, je nachdem $\lambda' + 2\lambda'' + 3\lambda'''$ die Form $4n, 4n+1, 4n+2, 4n+3$ hat. Ich behaupte nun, dass ε von der Anordnung des Viertelsystems κ unabhängig ist.

Um die Beweisführung zu erleichtern, verwende ich folgende Bezeichnung. $\Pi\psi$ soll die Zahl $0, 1, 2, 3$ bezeichnen, je nachdem die durch μ nicht teilbare Zahl ψ (selbst oder durch Kongruenzrepräsentation) in der Gruppe $\kappa, \kappa', \kappa'', \kappa'''$ liegt. Daraus ergeben sich unmittelbar folgende Aussagen:

I. $\Pi(i\psi) \equiv 1 + \Pi\psi \pmod 4$.

II. Die Zahl $i^{-\Pi\psi} \,.\, \psi$ liegt selbst oder durch Kongruenzrepräsentation in der Gruppe κ.

III. $\Sigma\Pi m\varphi \equiv \varepsilon, \pmod 4$, wenn die Summation über alle in κ liegenden Glieder φ erstreckt wird.

Es sei nun k ein anderes Viertelsystem aus f, f', f'' usw., während κ aus $\varphi, \varphi', \varphi''$ usw. besteht. Ich setze voraus, was erlaubt ist, da die *Reihenfolge* der Glieder in κ beliebig ist, dass f mit φ identisch ist oder zusammengehört, f' mit φ', f'' mit φ'' usw. Die mit k zusammengehörigen Viertelsgruppen seien $k'(\equiv ik)$, $k''(\equiv -k)$, $k'''(\equiv -ik)$. Ferner habe die Charakteristik P für die Gruppen k, k', k'', k''' dieselbe Bedeutung wie Π für $\kappa, \kappa', \kappa'', \kappa'''$, sodass $\mathrm{P}\psi = 0, 1, 2, 3$, je nachdem ψ zu k, k', k'', k''' gehört.

Geht man also von der Zerlegung von χ in die Viertelsysteme k, k', k'', k''' anstelle von $\kappa, \kappa', \kappa'', \kappa'''$ aus, so tritt an die Stelle von ε der kleinste Rest von $\mathrm{P}mf + \mathrm{P}mf' + \mathrm{P}mf'' + \mathrm{P}mf'''$ usw. usw. oder von $\Sigma\mathrm{P}mf$ modulo 4, und es ist zu beweisen, dass $\Sigma\mathrm{P}mf - \Sigma\Pi m\varphi$ durch 4 teilbar ist.

Wir schreiben diese Größe so:

$$\begin{array}{r} \mathrm{P}mf + \mathrm{P}mf' + \mathrm{P}mf'' + \mathrm{P}mf''' + \text{usw.} \\ -\mathrm{P}m\varphi - \mathrm{P}m\varphi' - \mathrm{P}m\varphi'' - \mathrm{P}m\varphi'''- \\ +\mathrm{P}m\varphi + \mathrm{P}m\varphi' + \mathrm{P}m\varphi'' + \mathrm{P}m\varphi'''+ \\ -\Pi m\varphi - \Pi m\varphi' - \Pi m\varphi'' - \Pi m\varphi'''- \end{array}$$

Da nach Voraussetzung f und φ kongruent sind oder zusammengehören, gilt dasselbe für mf und $m\psi$, und es ist

$$\left.\begin{array}{r} f \equiv i^{-\mathrm{P}\varphi}\varphi \\ i^{-\mathrm{P}mf}mf \equiv i^{-\mathrm{P}m\varphi}m\varphi \end{array}\right\} \pmod \mu$$

Daraus folgt leicht $\mathrm{P}mf - \mathrm{P}m\varphi \equiv -\mathrm{P}\varphi \pmod 4$, und die Summe der beiden obersten Reihen $\equiv -\Sigma\mathrm{P}\varphi$. Da ferner $\mathrm{P}m\varphi - \Pi m\varphi \equiv \mathrm{P}(i^{-\Pi m\varphi}m\varphi), m\varphi.i^{-\Pi m\varphi}$ zu κ gehört und die Gesamtheit *aller* $m\varphi \,.\, i^{-\Pi m\varphi}$ ohne Rücksicht auf die Reihenfolge mit allen φ übereinstimmt, ist die Summe *aller* $\mathrm{P}(m\varphi \,.\, i^{-\Pi m\varphi})$ gleich der Summe aller $\mathrm{P}\varphi$. Folglich ist die Summe der dritten und vierten Reihe $\equiv \Sigma\mathrm{P}\varphi \pmod 4$, also die Summe aller vier Reihen $\equiv 0 \pmod 4$. Was zu beweisen war.

Da ε also unabhängig von der Wahl der Viertelsysteme nur von m und μ abhängt, nennen wir ε den Charakter der Zahl m in Bezug auf den Modul μ und bezeichnen ihn mit Ch. $m \pmod \mu$. Offenbar ist dies nur eine Verallgemeinerung der Definition, die (Art. …) für den Fall gegeben wurde, dass μ eine Primzahl ist, oder schließt sie ein.

4.

Ich gehe jetzt zu *bestimmten* Anordnungen der Viertelsysteme über und setze den mit m bezeichneten Modul $= ea + ebi$. Dabei bezeichnet die positive ganze Zahl e den größten reellen Divisor, also den größten gemeinsamen Divisor der beiden Bestandteile von m; somit sind a, b teilerfremd. Das am einfachsten angeordnete Viertelsystem ist dasjenige, dessen Glieder $x + iy$ so beschaffen sind, dass $ax + by$ positiv und kleiner als $\frac{1}{2}e(aa + bb)$ ist, während $ay - bx$ nichtnegativ und ebenfalls kleiner als $\frac{1}{2}e(aa + bb)$ ist. Die letzte Bedingung ist absichtlich so ausgedrückt, dass auch die Fälle $ay - bx = 0$ eingeschlossen sind. Man sieht leicht, dass es insgesamt $\frac{1}{2}(e-1)$ solche Fälle gibt, nämlich

$$\begin{array}{llll} x & = a, & y & = b \\ x & = 2a, & y & = 2b \\ x & = 3a, & y & = 3b \\ & & \text{usw. bis} & \\ x & = \frac{1}{2}(e-1)a, & y & = \frac{1}{2}(e-1)b \end{array}$$

also gar keine, wenn die Bestandteile von m keinen gemeinsamen Divisor haben. Nennen wir dieses Viertelsystem k und diejenigen Systeme, die durch Multiplikation der zu k gehörenden Zahlen mit $i, -1, -i$ entstehen, k', k'', k'''; oder man kann auch setzen

$$k' = m + ik, \quad k'' = (1+i)m - k, \quad k''' = im - ik$$

So erhält man die folgende Regel, um zu entscheiden, ob eine beliebige vorgegebene, durch m nicht teilbare ganze Zahl $x+iy$ einem Glied von k, k', k'' oder k''' kongruent ist. Man kann nämlich $2(ax + by)$ in die Form $Pe(aa + bb) + Q$ und $2(ay - bx)$ in die Form $Re(aa + bb) + S$ bringen, wobei P, Q, R, S ganze reelle Zahlen sind und folgende Bedingungen erfüllen:

wenn $x + iy$ einer Zahl aus folgendem System kongruent ist

so dass	k	k'	k''	k'''
P	gerade	ungerade	ungerade	gerade
R	gerade	gerade	ungerade	ungerade
Q	positiv	positiv	positiv	nichtnegativ
$e(aa + bb) - Q$	positiv	nichtnegativ	positiv	positiv
S	nichtnegativ	positiv	positiv	positiv
$e(aa + bb) - S$	positiv	positiv	nichtnegativ	positiv

Die Übersicht wird leichter, wenn man die Fälle, in denen keine der Zahlen $ax + by$, $ay - bx$ durch $e(aa + bb)$ teilbar ist, von den übrigen unterscheidet.

I. Im ersten Fall nimmt man für P einfach die (algebraisch) kleinere der beiden ganzen Zahlen, zwischen denen $\frac{2(ax+by)}{e(aa+bb)}$ ausschließlich liegt, und ebenso für R die kleinere der beiden, zwischen denen $\frac{2(ay-bx)}{e(aa+bb)}$ liegt.

II. Ist $ax+by$ durch $e(aa+bb)$ teilbar, so ist $ay-bx$ zwar durch $aa+bb$, aber nicht durch $e(aa+bb)$ teilbar (weil sonst $x+iy$ durch $ea+ebi$ teilbar wäre). Ist nun R, also die unmittelbar unter $\frac{2(ay-bx)}{e(aa+bb)}$ liegende ganze Zahl, gerade, so ist $x+iy$ modulo $ea+ebi$ einer Zahl aus k' kongruent, dagegen einer aus k''', wenn R ungerade ist.

III. Ist $ay+bx$ durch $e(aa+bb)$ teilbar, nicht aber $ax+by$, so ist $x+iy$ einer Zahl aus k oder aus k'' kongruent, je nachdem die algebraisch unmittelbar unter $\frac{2(ax+by)}{e(aa+bb)}$ liegende ganze Zahl gerade oder ungerade ist.

5.

Aus dem Vorstehenden ergibt sich ohne Mühe die folgende Methode, um den Charakter einer gegebenen ganzen Zahl $M=A+Bi$ bezüglich des ungeraden Moduls $m=ea+ebi$, der sie nicht teilt, zu bestimmen.

Zur Abkürzung verwenden wir folgende Bezeichnung. Ist p eine beliebige nichtganze reelle Zahl, so bezeichnet $[p]$ diejenige ganze Zahl, die sowohl $p-[p]$ als auch $1+[p]-p$ positiv macht. Diese Definition schließt also die Anwendung der Bezeichnung auf ganze Zahlen aus. Würde man verlangen, dass weder $p-[p]$ noch $1+[p]-p$ negativ ist, so wäre das Zeichen $[p]$ für ganzzahliges p zweideutig. Man könnte auch, wie in einer früheren Abhandlung geschehen, verlangen, dass $1+[p]-p$ positiv und $p-[p]$ lediglich nichtnegativ ist. Für unseren Zweck ist es etwas bequemer, bei der ersten Definition zu bleiben.

Das Viertelsystem k besteht demnach aus allen ganzen Zahlen f, für die, wenn man $\frac{2f}{m}=\xi+\eta i$ setzt, ξ ausschließlich zwischen 0 und 1 liegt und η zwischen 0 und 1, mit eingeschlossener 0; oder

$$\begin{aligned} &[\xi]=0, \quad [\eta]=0 \\ \text{oder} \quad &[\xi]=0, \quad \eta=0 \end{aligned}$$

Setzt man nun für jedes f $\frac{2fM}{m}=\xi+i\eta$ und nimmt

$\Psi f = 0$ wenn zugleich $[\xi]$ gerade und entweder $[\eta]$ gerade oder η ganz
1 $[\eta]$ gerade und entweder $[\xi]$ ungerade oder ξ ganz
2 $[\xi]$ ungerade und entweder $[\eta]$ ungerade oder η ganz
3 $[\eta]$ ungerade und entweder $[\xi]$ gerade oder ξ ganz

oder in Tabellenform

	$[\eta]$ gerade	$[\eta]$ ungerade	η ganz
$[\xi]$ gerade	0	3	0
$[\xi]$ ungerade	1	2	2
ξ ganz	1	3	– .

was man mit $\nabla(\xi+i\eta)$ bezeichnen kann, so ist der gesuchte Charakter der Zahl M bezüglich des Moduls m gleich dem kleinsten Rest von $\Sigma\Psi f$ modulo 4.

6.

Die im vorhergehenden Artikel gegebene Vorschrift ist allgemein; für den Fall, dass M ungerade ist, werden wir ihr jedoch eine andere Gestalt geben. Zugleich nehmen wir an, dass die reellen Teile von m und M ungerade und daher die imaginären Teile gerade sind.

Wir ordnen jeder zum Viertelsystem k gehörenden Zahl f eine andere Zahl g zu, die aus f folgendermaßen abgeleitet wird. Setzt man $\frac{2f}{m} = \xi + i\eta$, so unterscheidet man vier Fälle:

I. Wenn $[2\xi] = 0$ und entweder $[2\eta] = 0$ oder $\eta = 0$
II. Wenn $[2\xi] = 1$ und entweder $[2\eta] = 0$ oder $\eta = 0$
III. Wenn $[2\xi] = 0$ und $[2\eta] = 1$
IV. Wenn $[2\xi] = 1$ und $[2\eta] = 1$

Im ersten Fall setzt man $g = 2f$, im zweiten $g = im - 2if$, im dritten $g = m + 2if$, im vierten $g = (1+i)m - 2f$. Man sieht leicht, dass die Gesamtheit aller g ein vollständiges Viertelsystem l bildet. Seine kennzeichnende Eigenschaft ist, dass, wenn man $\frac{g}{m} = \xi + i\eta$ setzt, zugleich folgende Bedingungen gelten:

entweder	$[\xi] = 0,$	$[\eta] = 0$	
oder	$\eta = 0,$	$[\xi] = 0$	und g durch $1+i$ teilbar
oder	$\xi = 0,$	$[\eta] = 0$	und g durch $1+i$ nicht teilbar

Daraus folgt, dass l sich von k nur dadurch unterscheidet, dass diejenigen Zahlen in k, für die $\eta = 0$ und die durch $1+i$ nicht teilbar sind, nämlich

$$a+bi, \quad 3(a+bi), \quad 5(a+bi) \ldots \frac{e-3}{2}(a+bi)$$
$$\text{oder bis } \frac{e-1}{2}(a+bi)$$

je nachdem e die Form $4n+1$ oder $4n+3$ hat, in l fehlen und stattdessen in der letzteren Gesamtheit die Produkte dieser Zahlen mit i auftreten. Zugleich sieht man, dass für $e = 1$, also wenn m durch keine reelle ganze Zahl teilbar ist, k und l völlig gleich sind.

Nun ist Ψf unmittelbar aus dem zu f gehörenden g abzuleiten. Das Ergebnis ist, dass für die obigen 4 Fälle gilt:

I. $\Psi f = \nabla \frac{gM}{m}$

II. $\Psi f = \begin{cases} -\nabla \frac{gM}{m} & \text{wenn weder reeller noch imaginärer Teil von } \frac{gM}{m} \text{ ganz} \\ 1 - \nabla \frac{gM}{m} & \text{wenn einer von beiden ganz ist} \end{cases}$

III. wie II. IV. wie I.

Bemerkungen.

Nach der Stelle zu urteilen, die die betreffenden Handschriften in einem Notizbuch einnehmen, stammen die hier im Druck mit I und II bezeichneten Bruchstücke aus dem Jahr 1811 oder der unmittelbar folgenden Zeit. Von den vorangegangenen Versuchen, das Fundamentaltheorem für biquadratische Reste mit den hier für den Rest $1+i$ angewandten Methoden zu beweisen, ist eine Aufzeichnung erhalten, die den besonderen Fall des Restes $1+2i$ erledigt und von jener Bestimmung des biquadratischen Charakters ausgeht, die Artikel 6 des Bruchstücks III als Anmerkung beigefügt wurde. Im Übrigen lassen sich die historischen Angaben, die Gauss in den Anzeigen seiner arithmetischen Abhandlungen veröffentlicht hat, mithilfe des Nachlasses dahin ergänzen, dass die in den Artikeln 15 bis 20 der *Theoria residuorum biquadrat.* enthaltenen Lehrsätze schon vor der Ausarbeitung der *Theoria motus corporum coel.* niedergeschrieben wurden. Die in den Anzeigen erwähnten Untersuchungen über kubische Reste sind wohl nicht zur Ausarbeitung gelangt; aufgezeichnet sind davon die mit den Hilfsmitteln der Abhandlung *Disquisitionum circa aequationes puras ulterior evolutio* geführten Beweise der Reziprozitätssätze für zwei Primzahlen, von denen eine reell ist.

Die Bruchstücke III bis VI bilden in der Handschrift besondere Hefte. Bei den ersten drei weist die Form der Schriftzüge auf eine Zeit hin, die nicht weit von derjenigen der Bruchstücke I und II entfernt liegt, während für das letzte, Nr. VI, ein erheblich späterer Zeitpunkt anzunehmen ist.

[I.] Art. 10. Die Anzahl der Gitterpunkte in $(z, z', z'+\zeta, z+\zeta)$ ergibt sich aus dem Satz: Sind a und b teilerfremd, so geht die von $\xi+\eta i$ nach $\xi+\eta i+a+bi$ gezogene Gerade durch einen Gitterpunkt, wenn der imaginäre Teil von $(\xi+\eta i)\,.\,(-a+bi)$ eine ganze Zahl ist.

[I.] Art. 17. Die erste Umformung des letzten S im Ausdruck für ΔS erhält man, indem man das betreffende Flächenstück in drei Teile zerlegt, sodass jenes S in

$$\begin{aligned} &S\big(\tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{2}+\tfrac{1}{2}i)m,\\ &\qquad (\tfrac{1}{2}+\tfrac{1}{2}i)m+i,\ \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(+)}\big)\\ &-S\big(\tfrac{1}{2}m,\ \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(+)},\ \tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i\big)\\ &-S\big((\tfrac{1}{2}+\tfrac{1}{2}i)m,\ \tfrac{1}{2}m,\ \tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i\big) \end{aligned}$$

übergeht, dann die Gitterpunkte im ersten Flächenteil mithilfe des Satzes in Artikel 10 auszählt und außerdem berücksichtigt, dass im zweiten Flächenteil kein Gitterpunkt liegt.

Die zweite Umformung erhält man, indem man die den Eckpunkten des dritten Flächenteils entsprechenden Größen mit i multipliziert und um die ganze Zahl $(1-i)\frac{m-1}{2}$ vermehrt; schließlich erhält man die dritte, indem

man die zuletzt entstandene Figur nach der Vorschrift von Artikel 16 mit derjenigen vergleicht, die gegenüber ihr die Ortsverschiebung $\frac{-1}{1+i}$ hat.

[I.] Art. [18.] Eine Erläuterung zum ersten Schema findet sich in den Artikeln 1 bis 6 des später niedergeschriebenen, hier mit [II.] bezeichneten Bruchstücks.

[I.] Art. [18.] (2.) Die geometrische Deutung ergibt mithilfe der beiden Systeme von Gitterpunkten

$$[-2iQ - \tfrac{1}{2}, \tfrac{1}{2}, iQ] = [-2iQ + \tfrac{1}{2}, \tfrac{1}{2}, iQ] = \mathrm{IV}^*$$

und

$$-[-2iQ + \tfrac{1}{2}i, -\tfrac{1}{2}i, iQ] = -[-2iQ - \tfrac{1}{2}i, -\tfrac{1}{2}i, iQ] = \mathrm{X}^*$$

die Gleichungen

$$\begin{aligned} \mathrm{IV} - \mathrm{IV}^* + [-2iQ, \tfrac{1}{2}i, -\tfrac{1}{2}] &= -\mathrm{X} + \mathrm{X}^* + [-iQ, \tfrac{1}{2}i, -\tfrac{1}{2}] \\ \mathrm{XIII} + \mathrm{IV}^* &= [-2iQ, 1, iQ] = -I(-2iQ) + I(-iQ) \\ \mathrm{V} + \mathrm{X}^* &= -[-2iQ, -i, iQ] = R(-2iQ) - R(-iQ) \end{aligned}$$

wobei allgemein Rx und Ix die größten im reellen Teil und im Koeffizienten des imaginären Teils von x enthaltenen ganzen Zahlen bezeichnen.

$[-2iQ, \frac{1}{2}i, -\frac{1}{2}]$ ist aber die Anzahl der Gitterpunkte in dem Quadrat, dessen Mittelpunkt bei $-2iQ - \frac{1}{4} + \frac{1}{4}i$ liegt und zwischen dessen Endpunkten die Ortsverschiebungen $\frac{1}{2}$ und $\frac{1}{2}i$ bestehen.

$[-iQ, \frac{1}{2}i, -\frac{1}{2}]$ oder $[-2iQ, -\frac{1}{2}i, \frac{1}{2}]$ ist die Anzahl der Gitterpunkte in einem gleichen Quadrat mit Mittelpunkt $-2iQ + \frac{1}{4} - \frac{1}{4}i$.

[I.] Art. [18.] (3.) Mithilfe der Gitterpunkte

$$[0, \tfrac{1}{2}i, -iQ] = -[-\tfrac{1}{2}i, -\tfrac{1}{2}i, -iQ] = \mathrm{I}^*$$

erhält man

$$\begin{aligned} \mathrm{VII} - \mathrm{XII} &= \mathrm{I} - \mathrm{I}^* + [-iQ, \tfrac{1}{2}, \tfrac{1}{2}i] - [0, \tfrac{1}{2}, \tfrac{1}{2}i] \\ &= \mathrm{I} - \mathrm{I}^* + [-2iQ, \tfrac{1}{2}, \tfrac{1}{2}i] \\ \mathrm{II} - \mathrm{I}^* &= [0, -i, -iQ] = -R0 + R(-iQ) \\ \mathrm{IX} - \mathrm{I} &= [0, -1, -iQ] = I0 - I(-iQ) \\ \mathrm{VI} - \mathrm{XII} &= -[\tfrac{1}{2}i, -1, -iQ] = -I(\tfrac{1}{2}i) + I(-iQ + \tfrac{1}{2}i) \\ \mathrm{VIII} - \mathrm{XIV} &= -[\tfrac{1}{2}, -1 - i, \tfrac{1}{2}im_{(-)}] = \frac{a-1}{2} + \frac{b}{2} \end{aligned}$$

[II.] Art. 10. Es gilt

$$\begin{aligned} \Upsilon P' &\equiv -\Upsilon(-iP' + \tfrac{1}{2}im), \\ \Upsilon P'' &\equiv -1 - \Upsilon(P'' - \tfrac{1}{2}im), \\ \Upsilon P''' &\equiv 1 + \Upsilon(-iP''') \pmod 4 \end{aligned}$$

und $-iP' + \frac{1}{2}im$, $P'' - \frac{1}{2}im$ sind die jeweils um $\frac{1}{2}i$ vermehrten Gitterpunkte in I und VI.

[III.] Art. 6. Die in der Anmerkung angegebenen Regeln zur Bestimmung von Dec.$\frac{M}{m}$ habe ich der vorliegenden Abhandlung aus einer anderen Stelle der Handschriften beigefügt. Die erste dieser beiden Regeln, die, wie leicht zu sehen ist, mit der zweiten übereinstimmt, folgt aus derjenigen von Artikel 6, weil

$$k \equiv f \,.\, i^{-n} \text{ (mod. } m), \quad n = \Theta\frac{2fM}{m}, \quad p = mm',$$
$$\left[\frac{2km'}{p}\right]^2 \equiv \Theta\frac{2km'}{p} \text{ (mod. } 2+2i)$$

gilt.

[III.] Art. 8 enthält in der Handschrift ein Beispiel zu Artikel 7, nämlich die Bestimmung des Dezidenten von $-1+2i$ für den Modul $-11+4i$.

[III.] Art. 10. Zur Bemerkung 'anders auszudrücken' kann man Artikel 3 des folgenden Bruchstücks [IV] vergleichen.

[IV.] Die Artikel 1. 2. 4 enthalten in der Handschrift außer dem hier Abgedruckten noch die Anwendung auf die beiden Beispiele für $m = 5+8i$, $M = 9+4i$ und für $m = 9+4i$, $M = 5+8i$. [V.] Art. [7.] Hier bezeichnet Dec.$\frac{m}{M}$, wie in Artikel 1 des vorhergehenden Bruchstücks [IV], den Wert von

$$\Sigma(-1)^X \Sigma(-1)^Y \text{Int.}\, p$$

wobei die Summation über alle ganzen Zahlen X und Y erstreckt wird, für die die zugehörigen ξ und η innerhalb der Grenzen 0 und $\frac{1}{2}$ liegen.

Nach der Angabe im Text wurden die Formeln für den Dezidenten in den Artikeln 7 und 15 auf zwei besonderen Wegen gefunden. Um diese Erläuterungen jedoch nicht zu sehr auszudehnen, werden sie hier aus einer gemeinsamen Quelle abgeleitet.

Nimmt X einen beliebigen bestimmten ganzzahligen Wert an, so sei Y^* der kleinere und Y^{**} der größere der beiden Werte von Y, die den Grenzwerten von ξ, η entsprechen. Die zu Y^* und Y^{**} gehörenden Werte von p seien p^* und p^{**}. Ebenso wie Y^* und Y^{**} können sie nicht gleich sein, weil die Summe Σ sich nicht über die Grenzwerte von ξ und η erstreckt.

Führt man wie in den beiden vorhergehenden Aufsätzen [III] und [IV] die Summation über alle beim selben X auftretenden Werte von Y aus, setzt dabei für die Anzahl der zwischen Y' und Y'' liegenden ungeraden Zahlen $[\frac{1}{2}Y'' - \frac{1}{2}] - [\frac{1}{2}Y' - \frac{1}{2}]$ und fügt die auf die Grenzen $\xi = 0$ und $= \frac{1}{2}$ bezogenen Intensoren zweimal mit entgegengesetzten Zeichen hinzu, so erhält man für $\Sigma(-1)^Y \text{Int.}\, p$ den aus sieben Teilen bestehenden Ausdruck

$$-\Sigma[-\text{Int.}(p - \mu\omega i) + \text{Int.}(p + \mu\omega i)]$$

wobei alle p aufzunehmen sind, für die $[Y]$ gerade,

x oder y ganz, einschl. $\xi = 0$ und $\frac{1}{2}$, ausschl. $\eta = 0$ und $\frac{1}{2}$

$$\left.\begin{array}{l} -\,\mathrm{Int.}(p^* - \mu\omega i) \text{ wenn } [Y^*] \text{ gerade} \\ +\,\mathrm{Int.}(p^{**} + \mu\omega i) \text{ wenn } [Y^{**}] \text{ gerade} \end{array}\right\} \xi = 0 \text{ oder } \tfrac{1}{2}, \quad 0 < \eta < \tfrac{1}{2}$$

$$\left.\begin{array}{l} -\,\mathrm{Int.}(p^* + \mu\omega i) \text{ wenn } [Y^*] \text{ gerade} \\ +\,\mathrm{Int.}(p^{**} - \mu\omega i) \text{ wenn } [Y^{**}] \text{ gerade} \end{array}\right\} 0 < \xi < \tfrac{1}{2}, \quad \eta = 0 \text{ oder } \tfrac{1}{2}$$

$$\left.\begin{array}{l} -\,\mathrm{Int.}(p^* + \mu\omega i) \text{ wenn } [Y^*] \text{ gerade} \\ +\,\mathrm{Int.}(p^{**} - \mu\omega i) \text{ wenn } [Y^{**} - \omega] \text{ gerade} \end{array}\right\} \xi = 0 \text{ oder } \tfrac{1}{2}, \quad \eta = 0 \text{ oder } \tfrac{1}{2}$$

der, mit $(-1)^X$ multipliziert und über alle ganzzahligen X summiert, den Dezidenten $\frac{m}{M}$ ergibt.

Aus dem ersten Teil des Ausdrucks entsteht so für die nach Artikel 2, Vorschrift I gebildeten ε

$$\begin{array}{l} \Sigma\varepsilon \text{ wobei } X \text{ ganz, } [Y] \text{ gerade} \\ -\,\Sigma\varepsilon \text{ wobei außerdem } y \text{ ganz, } [x] \text{ gerade} \end{array}$$

Für die folgenden Teile kann man

$$\left.\begin{array}{l} -\,(B)\mathrm{Int.}(p - B\mu\omega i) \text{ wenn } \xi = 0 \\ +\,(B)\mathrm{Int.}(p + B\mu\omega i) \text{ wenn } \xi = \frac{1}{2} \end{array}\right\} X \text{ ganz, } [Y] \text{ gerade, } 0 < \eta < \tfrac{1}{2}$$

$$\left.\begin{array}{l} -\,(A)\mathrm{Int.}(p + A\mu\omega i) \text{ wenn } \eta = 0 \\ +\,(A)\mathrm{Int.}(p - A\mu\omega i) \text{ wenn } \eta = \frac{1}{2} \end{array}\right\} X \text{ ganz, } [Y] \text{ gerade, } 0 < \xi < \tfrac{1}{2}$$

$$-\tfrac{1}{2}[(A') + (B')]\mathrm{Int.}(p + A'\mu\omega i)$$
$$\text{wenn } X \text{ ganz, } [Y + A'\omega] \text{ gerade, } \xi \text{ und } \eta = 0 \text{ oder } \tfrac{1}{2}$$

setzen. Dabei ist $A' = +A$ oder $-A$, wenn $\eta = 0$ oder $\frac{1}{2}$, und $B' = +B$ oder $-B$, wenn $\xi = 0$ oder $\frac{1}{2}$; zum Beispiel verwendet man die Bezeichnung $(A) : +1$ oder -1, je nachdem A positiv oder negativ ist.

Multipliziert man mit $(-1)^X$, führt die Summation über X aus und lässt dabei in diesen Ausdrücken, und zwar im

$$\begin{array}{rl} \text{ersten} & p - B\mu\omega i,\ P - BD\omega i,\ \pi - AB\omega i - BB\omega,\ X,\ [Y] \\ & \text{jeweils in } ip,\ iP,\ i\pi,\ -Y,\ [X] \\ \text{zweiten} & p + B\mu\omega i,\ P + BD\omega i,\ \pi + AB\omega i + BB\omega,\ X,\ [Y] \\ & \ldots \quad p,\ P,\ \pi \quad X,\ [Y] \\ \text{dritten} & p + A\mu\omega i,\ P + AD\omega i,\ \pi + AA\omega i + AB\omega,\ X,\ [Y] \\ & \ldots \quad p,\ P,\ \pi \quad X,\ [Y] \\ \text{vierten} & p - A\mu\omega i,\ P - AD\omega i,\ \pi - AA\omega i - AB\omega,\ X,\ [Y] \\ & \ldots \text{ in } im - ip,\ iM - iP,\ i - i\pi,\ Y - B,\ A - 1 - [X] \end{array}$$

die angegebenen Größen ineinander übergehen und bezeichnet das Ergebnis aus dem fünften Ausdruck mit Q_1, so erhält man

$$\begin{aligned}
&- \Sigma(-1)^Y(B)\text{Int.}\, ip, \\
&\qquad \text{wobei } Y \text{ ganz, } [X] \text{ gerade, } \eta = \omega,\ 0 < \xi < \tfrac{1}{2} \\
&+ \Sigma(-1)^X(B)\text{Int.}\, p, \\
&\qquad \text{wobei } X \text{ ganz, } [Y] \text{ gerade, } \xi = \tfrac{1}{2} + \omega,\ 0 < \eta < \tfrac{1}{2} \\
&- \Sigma(-1)^X(A)\text{Int.}\, p, \\
&\qquad \text{wobei } X \text{ ganz, } [Y] \text{ gerade, } \eta = \omega,\ 0 < \xi < \tfrac{1}{2} \\
&+ \Sigma(-1)^Y(A)\text{Int.}(im - ip), \\
&\qquad \text{wobei } Y \text{ ganz, } [X] \text{ gerade, } \xi = \tfrac{1}{2} + \omega,\ 0 < \eta < \tfrac{1}{2} \\
&+ Q_1
\end{aligned}$$

Die Untersuchung der einzelnen Fälle zeigt, dass unter der Voraussetzung $M \equiv 1 \pmod{2 + 2i}$

$$\begin{aligned}
Q_1 = \ &- \text{Int.}\, \mu\omega i \text{ ist, wenn } M \text{ im 1. Quadranten liegt} \\
&- \text{Int.}(\tfrac{1}{2}mi + \mu\omega i), \quad \text{wenn } M \text{ im 2. Quadr. und } \frac{M-1}{2} \text{ gerade} \\
&+ \text{Int.}(\tfrac{1}{2}mi - \mu\omega i), \quad \text{wenn } M \text{ im 4. Quadr. und } \frac{M-1}{2} \text{ gerade}
\end{aligned}$$

wobei man eine komplexe Zahl gerade oder ungerade nennt, je nachdem sie durch 2 teilbar ist oder nicht.

Bei Anwendung der in den Vorschriften II und IV bestimmten ε ergibt sich somit

$$\begin{aligned}
\text{Dec.}\frac{m}{M} = \text{I}, \quad &\Sigma\varepsilon, \text{ wobei } X \text{ ganz, } [Y] \text{ gerade} \\
&- 4\Sigma\varepsilon, \text{ wobei außerdem } y \text{ ganz, } [x] \text{ gerade} \\
\text{II}, \quad &- \Sigma\varepsilon\text{Int.}\, ip, \text{ wobei } Y \text{ ganz, } [X] \text{ gerade} \\
\text{IV}, \quad &+ \Sigma\varepsilon\text{Int.}\, p, \text{ wobei } X \text{ ganz, } [Y] \text{ gerade} \\
\text{II}, \quad &+ \Sigma\varepsilon\text{Int.}\, p, \text{ wobei } X \text{ ganz, } [Y] \text{ gerade} \\
\text{IV}, \quad &+ \Sigma\varepsilon\text{Int.}(im - ip), \text{ wobei } Y \text{ ganz, } [X] \text{ gerade} \\
&+ Q_1
\end{aligned}$$

Eine andere Form des Ausdrucks für den Dezidenten erhält man, wenn man zuerst über X summiert und die Anzahl der zwischen X' und X'' liegenden ungeraden Zahlen durch $[\frac{1}{2}X'' + \frac{1}{2}] - [\frac{1}{2}X' + \frac{1}{2}]$ darstellt, nämlich

$$\begin{aligned}
\text{Dec.}\frac{m}{M} = \text{I}, \quad & \Sigma\varepsilon, \text{ wobei } Y \text{ ganz, } [X] \text{ ungerade} \\
& -4\Sigma\varepsilon, \text{ wobei außerdem } y \text{ ganz, } [x] \text{ gerade} \\
\text{II}, \quad & -\Sigma\varepsilon\text{Int.}\, ip, \text{ wobei } X \text{ ganz, } [Y] \text{ gerade} \\
\text{IV}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ wobei } Y \text{ ganz, } [X] \text{ ungerade} \\
\text{II}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ wobei } Y \text{ ganz, } [X] \text{ ungerade} \\
\text{IV}, \quad & +\Sigma\varepsilon\text{Int.}(im - ip), \text{ wobei } X \text{ ganz, } [Y] \text{ ungerade} \\
& +Q_2
\end{aligned}$$

$$\begin{aligned}
Q_2 = & -\text{Int.}(-\mu\omega), \quad \text{wenn } M \text{ im 2. Quadr.} \\
& +\text{Int.}(\tfrac{1}{2}m - \mu\omega), \quad \text{wenn } M \text{ im 1. Quadr. und } \frac{M-1}{2} \text{ ungerade} \\
& -\text{Int.}(\tfrac{1}{2}m + \mu\omega), \quad \text{wenn } M \text{ im 3. Quadr. und } \frac{M-1}{2} \text{ ungerade}
\end{aligned}$$

Führt man die Summation über Y zuerst aus, wählt aber die zweite soeben verwendete Methode, um die Anzahl der zwischen zwei Werten liegenden ungeraden Zahlen zu bestimmen, so ergibt sich

$$\begin{aligned}
\text{Dec.}\frac{m}{M} = \text{I}, \quad & \Sigma\varepsilon, \text{ wobei } X \text{ ganz, } [Y] \text{ ungerade} \\
& -4\Sigma\varepsilon, \text{ wobei außerdem } y \text{ ganz, } [x] \text{ gerade} \\
\text{II}, \quad & -\Sigma\varepsilon\text{Int.}\, ip, \text{ wobei } Y \text{ ganz, } [X] \text{ ungerade} \\
\text{IV}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ wobei } X \text{ ganz, } [Y] \text{ ungerade} \\
\text{II}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ wobei } X \text{ ganz, } [Y] \text{ ungerade} \\
\text{IV}, \quad & +\Sigma\varepsilon\text{Int.}(im - ip), \text{ wobei } Y \text{ ganz, } [X] \text{ ungerade} \\
& +Q_3
\end{aligned}$$

$$\begin{aligned}
Q_3 = & -\text{Int.}(-\mu\omega i), \quad \text{wenn } M \text{ im 3. Quadr.} \\
& -\text{Int.}(\tfrac{1}{2}mi + \mu\omega i), \quad \text{wenn } M \text{ im 2. Quadr. und } \frac{M-1}{2} \text{ ungerade} \\
& +\text{Int.}(\tfrac{1}{2}mi - \mu\omega i), \quad \text{wenn } M \text{ im 4. Quadr. und } \frac{M-1}{2} \text{ ungerade}
\end{aligned}$$

Summiert man auch zuerst über X und verwendet die erste Darstellung der Anzahl der zwischen zwei Werten liegenden ungeraden Zahlen, so erhält

man die in [V], Artikel 15 angegebene Form für den Dezidenten. Dabei kann die Größe q auch durch folgende Gleichung definiert werden:

$$\begin{aligned} q = & -\text{Int.}\,\mu\omega, \quad \text{wenn } M \text{ im 4. Quadr.} \\ & +\text{Int.}(\tfrac{1}{2}m - \mu\omega), \quad \text{wenn } M \text{ im 1. Quadr. und } \frac{M-1}{2} \text{ gerade} \\ & -\text{Int.}(\tfrac{1}{2}m + \mu\omega), \quad \text{wenn } M \text{ im 3. Quadr. und } \frac{M-1}{2} \text{ gerade} \end{aligned}$$

Die Vereinigung dieser vier Ausdrücke für den Dezidenten ergibt das in [V], Artikel 7 aufgestellte Resultat. Denn $\text{Int.}\,ip - \text{Int.}\,p$ ist gleich 3 für gerades $[x]$ und ungerades $[y]$, sonst aber gleich 1; ferner ist $\text{Int.}(im - ip) + \text{Int.}\,p$ gleich 0, wenn $[x]$ und $[y]$ gerade sind, in allen übrigen Fällen aber gleich 4.

[V.] Art. [7.] Die erste Tafel zum Beispiel gibt in der ersten Spalte die zu jedem ganzzahligen P gehörenden Werte von $\frac{37.P}{M}$ oder $37(\xi + \eta i)$, wenn $0 < \xi < \frac{1}{2}$, $0 < \eta < \frac{1}{2}$; in der zweiten $\frac{37.Pm}{M}$ oder $37\,.\,p$; in der dritten die größte in p enthaltene ganze Zahl; und in der vierten $\pm\text{Int.}\,p$, wobei das obere Zeichen gilt, wenn P durch $1 + i$ teilbar ist, das untere, wenn P nicht durch $1 + i$ teilbar ist.

[V.] Art. [9.]. [12.] Die verbesserte Bezeichnung der θ ist nur bei der zweiten und dritten Klasse, Artikel 9. 10, angedeutet, aber auch auf die erste und vierte, Artikel 8. 11, auszudehnen. Demnach hat ein $\theta^\lambda = T + Ui$ denjenigen Index $\lambda, = 0, 1, 2$ oder 3, für den die durch die Gleichungen

$$\begin{aligned} i^\lambda M &= \mathfrak{A} + \mathfrak{B}i, \quad i^{-\lambda}\mu = \rho + \sigma i \\ \sigma\varphi^0 &= -\text{Koeff. Imag. } \theta^\lambda(a - bi) = +bT - aU \\ \sigma\Phi^0 &= +\text{Koeff. Imag. } \theta^\lambda(\mathfrak{A} - \mathfrak{B}i) = -\mathfrak{B}T + \mathfrak{A}U \end{aligned}$$

bestimmten Größen φ^0 und Φ^0 zwischen 0 und $\frac{1}{2}$ liegen.

Um nach den Andeutungen in Artikel 9 (3) zu beweisen, dass, wenn T, U zwei ganze reelle Zahlen sind, die die soeben aufgestellten Bedingungen erfüllen, $T + Ui$ auch in der bei einer der vier Kombinationen, Artikel 8. 11, bestimmten Gesamtheit θ^λ liegt, bezeichne man mit φ', Φ' diejenigen komplexen ganzen Zahlen, für die die Gleichung

$$T + Ui = \varphi' i^\lambda M + \Phi' m$$

gilt und für die eine der vier Größen $\pm\frac{\varphi' - \varphi^0}{m}$, $\pm i\frac{\varphi' - \varphi^0}{m}$ so beschaffen ist, dass ihr reeller Teil und der Koeffizient ihres imaginären Teils zwischen 0 und $\frac{1}{2}$ liegen (*Theoria residuorum biquadr. artt.* 45, 46). Die betreffende Größe ist dann, wie man aus der Untersuchung der sechzehn einzelnen Fälle in den vier Kombinationen leicht erkennt, $\frac{p}{m}$, und die ihr entsprechende Größe unter $\pm\frac{\Phi' - \Phi^0}{m}$, $\pm i\frac{\Phi' - \Phi^0}{M}$ ist $\frac{P}{M}$, weil $\frac{\Phi' - \Phi^0}{M} = -\frac{\varphi' - \varphi^0}{m} i^\lambda$.

Aus dieser Darstellung der Größen $\frac{p}{m}$ oder $\frac{P}{M}$ folgt auch, dass I, $\Sigma\varepsilon$ von allen aus $\Theta+\Theta'+\Theta''+\Theta'''$ besteht. Dabei bezeichnet Θ^λ die Summe derjenigen ε, die für jeden Gitterpunkt θ innerhalb des Parallelogramms $0,\ \frac{1}{2}m,\ \frac{1}{2}m+\frac{1}{2}i^\lambda M,\ \frac{1}{2}i^\lambda M,$

$= +1$ zu setzen sind, wenn θ durch $1+i$ teilbar und Koeff. Imag. $\mu i^{-\lambda}$ positiv ist oder wenn keine Bedingung gilt; dagegen

$= -1$, wenn nur eine gilt.

[V.] Art. 13. Die Bestimmung von Θ^λ kann entweder mit den vier oben für Dec. $\frac{m}{M}$ verwendeten Summationsarten oder, was im Wesentlichen dasselbe ist, mit den in [II], Artikel 11 angedeuteten Methoden ausgeführt werden. Dabei sind die vier Konstruktionen zugrunde zu legen, die entstehen, wenn man die Punkte, deren θ ein Vielfaches von $1+i$ ist, jeweils mit den Punkten $\theta+1$, $\theta+i$, $\theta-1$ und $\theta-i$ verbindet.

Ordnet man auf der Begrenzung des zuvor genannten Parallelogramms allen Punkten ein θ zu, für die der reelle oder imaginäre Teil von θ eine ganze Zahl ist, bezeichnet mit θ^0 die nächste durch $1+i$ teilbare ganze Zahl bei θ und mit l die Ortsverschiebung von einem Punkt des geraden Begrenzungsstücks, das θ enthält, zu einem beliebigen nachfolgenden Punkt derselben Geraden, also zum Beispiel bei diesem Parallelogramm der Reihe nach die Größen $m,\ Mi^\lambda,\ -m,\ -Mi^\lambda$, und setzt

$$\varepsilon = \pm 1 \text{ mit dem Zeichen des imaginären Teils von } \frac{l}{\theta-\theta^0}$$

so ergibt die Vereinigung der auf die eine oder andere Weise erhaltenen vier Resultate $4\Theta^\lambda = -\Sigma\varepsilon$.

Die gesonderte Bestimmung der zu den Eckpunkten gehörenden θ und ε wird vermieden, wenn man dieses Parallelogramm durch ein anderes ersetzt, dessen Begrenzungen denjenigen des ersten unendlich nahe sind und das die beiden Punkte 0 und $\frac{1}{2}m+\frac{1}{2}i^\lambda M$ nicht einschließt. Die Begrenzung eines solchen Parallelogramms erhält man, indem man sie auf die positiven Seiten der Linien

$$0\ldots.\tfrac{1}{2}m, \quad \tfrac{1}{2}m+\tfrac{1}{2}i^\lambda M\ldots.\tfrac{1}{2}m,$$
$$\tfrac{1}{2}m+\tfrac{1}{2}i^\lambda M\ldots.\tfrac{1}{2}i^\lambda M, \quad 0\ldots.\tfrac{1}{2}i^\lambda M$$

legt. Ordnet man den vier so entstandenen Geraden der Reihe nach die unendlich kleinen positiven Größen $\omega_1,\omega_2,\omega_3,\omega_4$ zu, so kann man für die auf ihnen liegenden Punkte θ

$$\begin{aligned}
\theta = p &= m(\xi+\omega_1 i),\\
-\theta i^\lambda + \tfrac{1}{2}mi^\lambda + \tfrac{1}{2}M = P &= M(\xi+\omega_2 i),\\
-\theta + \tfrac{1}{2}m + \tfrac{1}{2}Mi^\lambda = p &= m(\xi+\omega_3 i),\\
\theta i^{-\lambda} = P &= M(\xi+\omega_4 i) \quad \text{wenn } \lambda \text{ gerade}
\end{aligned}$$

$$\begin{aligned}
\theta = p &= m(\xi + \omega_1 i),\\
\theta i^{1-\lambda} - \tfrac{1}{2}mi^{1-\lambda} + \tfrac{1}{2}M = P &= M(\tfrac{1}{2} + \omega_2 + \eta i),\\
\theta i + \tfrac{1}{2}m - \tfrac{1}{2}Mi^{1+\lambda} = p &= m(\tfrac{1}{2} + \omega_3 + \eta i),\\
\theta i^{-\lambda} = P &= M(\xi + \omega_4 i) \quad \text{wenn } \lambda \text{ ungerade}
\end{aligned}$$

setzen. Dabei überschreiten ξ und η zur Schließung der Figur teilweise auch den Bereich der reellen Werte von 0 bis $\frac{1}{2}$ um unendlich kleine Größen.

Bezeichnen G, g, H, h die Summen der jeweils nach den Vorschriften II, III, IV, V (in den Artikeln 3 bis 6) gebildeten ε, umfassen G' oder $G_{\prime}$ und g' oder $g_{\prime}$ diejenigen ε, die für die beim zweiten Parallelogramm gegebenenfalls auftretenden unendlich kleinen Werte von ξ gelten, im Übrigen aber jeweils nach den Vorschriften II und III gebildet sind, beziehen sich ferner G'' oder $G_{\prime\prime}$ und g'' oder $g_{\prime\prime}$ ebenso auf dieselben Vorschriften, jedoch auf die unendlich kleinen Werte von $\frac{1}{2}-\xi$, und schließlich $H', h_{\prime}, H'', h_{\prime\prime}$ jeweils auf die Vorschriften IV, V, IV, V und die unendlich kleinen Werte von $\frac{1}{2}-\eta, \frac{1}{2}-\eta, \eta, \eta$, so gilt

$$\begin{aligned}
4\Theta^{\lambda} = {} & -(g+g'+g'') - i^{\lambda}(G+G'+G'')\\
& + i^{\lambda}(g+g_{\prime}+g_{\prime\prime}) + (G+G_{\prime}+G_{\prime\prime}) \quad \text{wenn } \lambda \text{ gerade}\\
4\Theta^{\lambda} = {} & -(g+g'+g'') - i^{1-\lambda}(H+H'+H'')\\
& - i^{\lambda-1}(h+h_{\prime}+h_{\prime\prime}) + (G+G_{\prime}+G_{\prime\prime}) \quad \text{wenn } \lambda \text{ ungerade}
\end{aligned}$$

Für den Eckpunkt θ des Parallelogramms, der dem Punkt 0 am nächsten liegt, bezeichne ξ_1 den zugehörigen Wert des ξ der ersten Seite und ξ_4 den zugehörigen Wert des ξ der vierten Seite, sodass

$$\theta = m(\xi_1 + \omega_1 i) = i^{\lambda} M(\xi_4 + \omega_4 i)$$

Dann ergibt sich dasjenige ξ, dem auf der ersten Seite oder ihrer Verlängerung ein Punkt p mit reellem Teil gleich 0 entspricht, aus der Gleichung

$$(\text{Real. } p = 0), \quad \xi - \xi_1 = \sigma a \mathfrak{A}\omega_1 - \sigma\omega_4$$

wobei die positiven Faktoren der unendlich kleinen positiven Größen durch die Einheit ersetzt sind und σ, $\mathfrak{A}$ die durch

$$\rho + \sigma i = i^{-\lambda}(\alpha + \beta i), \quad \mathfrak{A} + \mathfrak{B}i = i^{\lambda}(A + Bi)$$

bestimmten reellen Größen bezeichnen. Dieser Punkt p liegt auf der ersten Seite selbst, wenn $\xi - \xi_1$ positiv ist, also, wenn man ω_1 unendlich klein gegenüber ω_4 annimmt, wenn σ negativ ist. Der dem Punkt p nächste Punkt p^0, dessen darstellende Zahl durch $1+i$ geteilt wird, ist der Punkt 0; daher

hat Imag.$\frac{m}{p-p^0}$ oder Imag.$\frac{1}{\xi+\omega_1 i}$ das Minuszeichen. Für Real.$\,p=0$ erhält man somit

$$\varepsilon=-1 \text{ wenn } (\sigma)=-1, \quad \varepsilon=0 \text{ wenn } (\sigma)=+1, \quad \text{d. h. } \varepsilon=-\tfrac{1}{2}+\tfrac{1}{2}(\sigma)$$

und ebenso für Imag.$\,p=0$

$$\xi-\xi_1=\sigma b\mathfrak{B}\omega_1-\sigma\omega_4, \quad \text{Imag.}\frac{m}{p-p^0}=\text{Imag.}\frac{1}{\xi+\omega_1 i},$$
$$\varepsilon=-\tfrac{1}{2}+\tfrac{1}{2}(\sigma) \quad \text{also } g'=-1+(\sigma)$$

Bezüglich der vierten Seite gilt $P^0=0$, Imag.$\frac{M}{P-P^0}=$ Imag.$\frac{1}{\xi+\omega_4 i}$,

$$\begin{aligned}&\text{also für Real.}(i^\lambda P)=0; \quad \xi-\xi_4=-\sigma a\mathfrak{A}\omega_4+\sigma\omega_1,\\ &\qquad\qquad\qquad\qquad\quad \varepsilon=-\tfrac{1}{2}+\tfrac{1}{2}(\sigma a\mathfrak{A})\\ &\text{und für Imag.}(i^\lambda P)=0; \quad \xi-\xi_4=-\sigma b\mathfrak{B}\omega_4+\sigma\omega_1,\\ &\qquad\qquad\qquad\qquad\quad \varepsilon=-\tfrac{1}{2}+\tfrac{1}{2}(\sigma b\mathfrak{B})\end{aligned}$$

also $G_\prime=-1+\frac{1}{2}(\sigma a\mathfrak{A})+\frac{1}{2}(\sigma b\mathfrak{B})$ oder, weil $\rho=a\mathfrak{A}+b\mathfrak{B}$, $G_\prime=-1+\frac{1}{2}(\rho\sigma)+\frac{1}{2}(\rho\sigma ab\mathfrak{A}\mathfrak{B})$.

Der Teil R_1^λ von $4\Theta^\lambda$, der aus dem unendlich nahe beim Punkt 0 liegenden Stück der Begrenzung entsteht, ist somit

$$R_1^\lambda=+G_\prime-g'=-(\sigma)+\tfrac{1}{2}(\rho\sigma)+\tfrac{1}{2}(\rho\sigma ab\mathfrak{A}\mathfrak{B})$$

Durch ähnliche Überlegungen findet man für die Teile R_2^λ, R_3^λ, R_4^λ, die jeweils dieselbe Beziehung zu den Punkten $\frac{1}{2}m$, $\frac{1}{2}m+\frac{1}{2}Mi^\lambda$, $\frac{1}{2}Mi^\lambda$ haben wie R_1^λ zum Punkt 0, bei geradem λ

$$\begin{aligned}R_2^\lambda&=-g''-i^\lambda G''=-\tfrac{1}{2}(b)-\tfrac{1}{2}(\mathfrak{B}),\\ R_3^\lambda&=-i^\lambda G'+i^\lambda g_\prime=i^\lambda(\sigma)-\tfrac{1}{2}i^\lambda(\rho\sigma)-\tfrac{1}{2}i^\lambda(\rho\sigma ab\mathfrak{A}\mathfrak{B})\\ R_4^\lambda&=+i^\lambda g_{\prime\prime}+G_{\prime\prime}=\tfrac{1}{2}i^\lambda(b)+\tfrac{1}{2}i^\lambda(\mathfrak{B})\end{aligned}$$

und bei ungeradem λ

$$\begin{aligned}R_2^\lambda&=-g''-i^{1-\lambda}H''=-\tfrac{1}{2}(b)-\tfrac{1}{2}(\mathfrak{B}),\\ R_3^\lambda&=-i^{1-\lambda}H'-i^{\lambda-1}h_\prime=0,\\ R_4^\lambda&=-i^{\lambda-1}h_{\prime\prime}+G_{\prime\prime}=\tfrac{1}{2}i^{\lambda+1}(a)+\tfrac{1}{2}i^{\lambda+1}(\mathfrak{A})\end{aligned}$$

[V.] Art. [14.] Die Auswertung der Summen der nach Vorschrift III gebildeten ε ergibt sich aus der Gleichung

$$\begin{aligned}&\text{III}, \quad \Sigma\varepsilon \text{ von allen } -4\Sigma\varepsilon \text{ von denen, für die } y \text{ ganz, } [x] \text{ gerade}\\ &=\text{III}, \quad \Sigma[-\text{Int.}(p-m\omega)+\text{Int.}(p+m\omega)]\end{aligned}$$

die anhand der Definition der ε leicht zu überprüfen ist. Dabei nimmt p alle Werte an, die die unter Vorschrift III angegebenen Bedingungen erfüllen. Mit Ausnahme der beiden Intensoren, die dem kleinsten (ξ^*) und dem größten zulässigen Wert (ξ^{**}) von ξ entsprechen und jeweils gleich

$$-\mathrm{Int.}(p^* - m\omega) \text{ und } +\mathrm{Int.}(p^{**} + m\omega) \text{ oder}$$
$$-\mathrm{Int.}(\omega m) \text{ und } +\mathrm{Int.}(\tfrac{1}{2} - \omega)m$$

sind, lassen sich diese Intensoren stets paarweise als $+\mathrm{Int.}(p' + m\omega)$ und $-\mathrm{Int.}(p'' - m\omega)$ so zusammenstellen, dass zwischen ξ' und ξ'', die den Größen p' und p'' entsprechen, kein Wert von ξ liegt, der den reellen oder imaginären Teil von p zu einer ganzen Zahl macht. Die beiden Intensoren heben sich daher immer gegenseitig auf.

[V.] Art. [15.] Es gilt

$$\begin{aligned}
\text{II,}\quad & +\Sigma\varepsilon\mathrm{Int.}\, ip \text{ wobei } Y \text{ ganz } [X] \text{ gerade,}\\
& -\Sigma\varepsilon\mathrm{Int.}\, ip \text{ wobei } X \text{ ganz } [Y] \text{ ungerade}\\
&= \Sigma[-\mathrm{Int.}\, i(p - m\omega) + \mathrm{Int.}\, i(p + m\omega)]\\
&\quad \text{für diejenigen } p, \text{ für die } x \text{ oder } y \text{ ganz, } [X] \text{ gerade}\\
&\quad Y \text{ ungerade, } 0 < \xi < \tfrac{1}{2}, \quad \eta = \omega\\
&\quad +\mathrm{Int.}\, i(p^* - m\omega) \text{ wenn } [X^*] \text{ gerade } [Y^*] \text{ ungerade}\\
&\quad -\mathrm{Int.}\, i(p^{**} + m\omega) \text{ wenn } [X^{**}] \text{ gerade } [Y^{**}] \text{ ungerade}
\end{aligned}$$

wie man leicht erkennt, wenn man auf der zweiten Seite der Gleichung nach dem Verfahren der vorhergehenden Anmerkung über jedes Intervall von $\xi_\prime$ bis $\xi_{\prime\prime}$ summiert, das so klein ist, dass zwischen $\xi_\prime$ und $\xi_{\prime\prime}$ kein ξ liegt, das im zugehörigen P den reellen oder imaginären Teil zu einer ganzen Zahl macht. Die Anwendung der nach Vorschrift III gebildeten ε bringt die zweite Seite dieser Gleichung in die in Artikel 15 angegebene Form.

[V.] Art. [15.] Die Umformung der Summen der nach Vorschrift IV gebildeten $\lambda'\varepsilon$ in die Summen der ε aus V ergibt sich durch dieselben Überlegungen wie in der letzten Anmerkung, wenn man außerdem die Gleichung

$$\begin{aligned}
\text{V,}\quad & \Sigma\varepsilon \text{ von allen, } -4\Sigma\varepsilon \text{ wobei } x \text{ ganz } [y] \text{ gerade,}\\
&= +\mathrm{Int.}(\tfrac{1}{2}im + m\omega) - \mathrm{Int.}(\tfrac{1}{2}im + \tfrac{1}{2} - \omega m)
\end{aligned}$$

verwendet, die der zuvor ermittelten Auswertung der Summe der ε in Vorschrift III entspricht.

[V.] Art. [17.] Bestimmt man die Hilfsgrößen U, T, L, V durch die Gleichungen

$$\begin{aligned}
U &= 1 - 2(B) - (AB) + (\alpha a) + (\beta b) + (\alpha b) - (\beta a)\\
&\quad + (\alpha\beta ab) - (\alpha\beta abAB) \quad \text{oder}\\
U &= (1 + (A))(1 - (B))(1 - (a\beta) + (b\beta) + (\alpha\beta))
\end{aligned}$$

$$\text{weil } (\alpha a)+(\beta b)=(A)+(A\alpha\beta ab),$$
$$(\alpha b)-(\beta a)=(B)-(B\alpha\beta ab) \text{ ist,}$$
$$T=-2+(a)+(b)-(\beta)-2(B)-(\alpha ab) \quad \text{oder}$$
$$T=-2+(a)+(b)-(\beta)-2(B)-(aA)+(bB)-(\beta AB)$$
$$L=(1+(A))(1+(B))(1+(\beta))-(1-(A))(1-(B))(1-(\beta))$$
$$V=(1+(A))(1-(B))(-2(a)+2(\beta)+(ab)+(\alpha\beta)) \quad \text{oder}$$
$$V=(1+(A))(1-(B))(-(a)+(b)+(\beta)+(ab)-(\beta ab)+(\alpha\beta))$$
$$\text{weil } (a)+(b)=(\beta)+(\beta ab) \text{ wenn } A \text{ positiv } B \text{ negativ}$$

und bezeichnet mit W', S', Q' die Größen, in die W, S, Q im Ausdruck für Dec.$\frac{m}{M}$ in Artikel 14 übergehen, wenn man darin m mit M, also $\alpha+\beta i$ mit $\alpha-\beta i$, vertauscht, so gilt

$$2W'=-5(B)-(AB) \quad \text{wenn } \frac{M-1}{2} \text{ gerade}$$
$$2W'=-(B)-(AB) \quad \text{wenn } \frac{M-1}{2} \text{ ungerade}$$
$$2S'=-(\alpha\beta abAB)-(\beta)-(B)+(b)$$
$$2Q'+2S'+2W'=2T+U \quad \text{wenn } \frac{M-1}{2} \text{ gerade}$$
$$2Q'+2S'+2W'=-4+4(a)+U \quad \text{wenn } \frac{M-1}{2} \text{ ungerade}$$
$$8\psi=8(q+r+s+w)-(2Q'+2S'+2W')$$

Ersetzt man hier $8(q+r+s+w)$ durch den in Artikel 15 angegebenen Wert, bringt ihn jedoch in die Form

$2T+4L+V$	wenn $\frac{M-1}{2}$ gerade	$\frac{m-1}{2}$ gerade
$2T-16+16(A)+V$	wenn $\frac{M-1}{2}$ gerade	$\frac{m-1}{2}$ ungerade
$-4+4(a)+V$	wenn $\frac{M-1}{2}$ ungerade	$\frac{m-1}{2}$ gerade
$-20+4(a)+V$	wenn $\frac{M-1}{2}$ ungerade	$\frac{m-1}{2}$ ungerade

und beachtet, dass

$$V-U=-\tfrac{1}{2}(1+(a))(1+(A))(1+(\alpha))(1-(b))(1-(B))(1-(\beta))$$

gilt, so erhält man für ψ die in Artikel 17 angegebene Bestimmung.

[VI.] Art. 3. Das unvollständige Zitat kann auf Artikel 4 des Bruchstücks III bezogen werden.

Schering.

ZUR THEORIE DER KOMPLEXEN ZAHLEN.

[I.]

NEUE THEORIE DER ZERLEGUNG DER KUBEN.

I. Wir nehmen an, die Gleichung $x^3 + y^3 + z^3 = 0$ habe eine Lösung, nämlich $x = a,\ y = b,\ z = c$, wobei a, b, c keinen gemeinsamen Teiler haben und folglich auch paarweise teilerfremd sind. Wir setzen

$$\begin{aligned} b + c &= \alpha \\ c + a &= \beta \\ a + b &= \gamma \end{aligned}$$

wobei auch α, β, γ notwendig paarweise teilerfremd sind. Hätten nämlich α und β einen gemeinsamen Teiler, so würde dieser auch a^3 und b^3 teilen; daher müssten auch a und b einen gemeinsamen Teiler haben.

Wir haben nun

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = 0$$

Es gilt aber die Identität

$$\begin{aligned} &(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 \\ &= (\alpha + \beta + \gamma)^3 - 24\alpha\beta\gamma \end{aligned}$$

Folglich ist

$$(\alpha + \beta + \gamma)^3 = 24\alpha\beta\gamma$$

Sind α, β, γ reelle Zahlen, so ist $\alpha + \beta + \gamma$ durch 3 teilbar, also $\alpha + \beta + \gamma)^3$ durch 27 und folglich $\alpha\beta\gamma$ durch 9. Daher muss eine der Zahlen α, β, γ, zum Beispiel γ, durch 9 teilbar sein, also auch c^3 und folglich c durch 3.

Sind dagegen α, β, γ imaginäre Zahlen, so schließen wir, dass $\alpha + \beta + \gamma$ durch $1 - \varepsilon$, folglich $24\alpha\beta\gamma$ durch $(1 - \varepsilon)^3$ und somit $\alpha\beta\gamma$ durch $1 - \varepsilon$ teilbar sein muss. Also ist eine der Zahlen α, β, γ durch $1 - \varepsilon$ teilbar und folglich auch eine der Zahlen a, b, c.

II. Allgemein gilt die Identität

$$\begin{aligned} &(p + q + r)^3 + (p + q\varepsilon + r\varepsilon\varepsilon)^8 + (p + q\varepsilon\varepsilon + r\varepsilon)^3 \\ &= 27pqr + 3(p + q + r)(p + q\varepsilon + r\varepsilon\varepsilon)(p + q\varepsilon\varepsilon + r\varepsilon) \end{aligned}$$

Ist also $p + q + r = 0$, so ist

$$(p + q\varepsilon + r\varepsilon\varepsilon)^3 + (p + q\varepsilon\varepsilon + r\varepsilon)^3 - 27pqr = 0$$

Sind hier p, q, r, selbst Kuben, nämlich der Reihe nach $= a^3, b^3, c^3$, das heißt, gibt es eine Lösung der Gleichung $x^3 + y^3 + z^3 = 0$, so setzen wir

$$\begin{aligned} a^3 + b^3\varepsilon + c^3\varepsilon\varepsilon &= a' \\ a^3 + b^3\varepsilon\varepsilon + c^3\varepsilon &= b' \\ -3abc &= c' \end{aligned}$$

und erhalten ebenfalls $a'^3 + b'^3 + c'^3 = 0$. Aus dieser neuen Lösung lässt sich auf dieselbe Weise eine dritte ableiten und so weiter. Man sieht leicht, dass auch die dritte Lösung aus reellen Zahlen besteht, wenn dies für die erste gilt.

Weiter ist zu bemerken: Haben a, b, c keinen gemeinsamen Faktor, so gilt dies auch für a', b', c', abgesehen vom Faktor $1 - \varepsilon$. Es ist nämlich

$$\begin{aligned} \frac{a'}{1-\varepsilon} &= -\varepsilon\varepsilon a^3 + \varepsilon b^3 = a^2 - \varepsilon c^3 = -b^3 + \varepsilon\varepsilon c^3 \\ \frac{b'}{1-\varepsilon} &= a^3 - \varepsilon b^3 = -\varepsilon\varepsilon a^3 + \varepsilon c^3 = \varepsilon\varepsilon b^3 - c^3 \\ \frac{c'}{1-\varepsilon} &= (\varepsilon\varepsilon - 1)abc \end{aligned}$$

Die ersten beiden Zahlen haben also weder mit a noch mit b noch mit c einen gemeinsamen Faktor und können auch nicht durch $1 - \varepsilon$ teilbar sein, sofern nicht a, b, c alle durch $1 - \varepsilon$ teilbar sind. Daher haben sie auch keinen gemeinsamen Faktor mit der dritten Zahl.

III. Aber auch der umgekehrte Weg steht offen. Wir haben gesehen, dass eine der Größen durch $1 - \varepsilon$ teilbar ist; dies sei c. Da man für a auch $a\varepsilon$ oder $a\varepsilon\varepsilon$ und ebenso für b auch $b\varepsilon$ oder $b\varepsilon\varepsilon$ einsetzen kann, dürfen wir voraussetzen, dass a entweder $\equiv 1$ oder $\equiv -1$ ist. Wir nehmen den ersten Fall an, da im anderen Fall $b \equiv 1$ gelten würde und es nur mit a vertauscht werden müsste. Wir setzen also

$$\begin{aligned} a &= 1 + 3\alpha \\ b &= -1 + 3\beta \end{aligned}$$

und

$$\begin{aligned} \frac{a\varepsilon + b\varepsilon\varepsilon}{\varepsilon - \varepsilon\varepsilon} &= 1 + (\varepsilon\varepsilon - \varepsilon)(\alpha\varepsilon + \beta\varepsilon\varepsilon) = A \\ \frac{a\varepsilon\varepsilon + b\varepsilon}{\varepsilon - \varepsilon\varepsilon} &= -1 + (\varepsilon\varepsilon - \varepsilon)(\alpha\varepsilon\varepsilon + \beta\varepsilon) = B \\ \frac{a + b}{\varepsilon - \varepsilon\varepsilon} &= (\varepsilon\varepsilon - \varepsilon)(\alpha + \beta) = C \end{aligned}$$

wobei $A + B + C = 0$ und $ABC = \frac{a^3+b^3}{(\varepsilon-\varepsilon\varepsilon)^3} = \left(\frac{c}{\varepsilon\varepsilon-\varepsilon}\right)^3$ gilt.

Da hier

$$a = -\varepsilon A + \varepsilon\varepsilon B$$
$$b = \varepsilon\varepsilon A - \varepsilon B$$

gilt, können A und B keinen gemeinsamen Faktor haben, weil dieser sonst auch ein gemeinsamer Faktor von a und b wäre. Wegen $A + B + C = 0$ kann folglich auch C weder mit A noch mit B einen gemeinsamen Faktor haben. Daraus folgt leicht, dass A und B und somit auch C Kuben sind. Denn $\left(\frac{c}{\varepsilon\varepsilon-\varepsilon}\right)^3$ ist durch $\varepsilon - \varepsilon\varepsilon$ und folglich auch durch $(\varepsilon - \varepsilon\varepsilon)^3$ teilbar oder $\alpha + \beta$ durch 3; daher gilt $A \equiv 1$, $B \equiv -1$ (mod. 3).

Setzen wir nun

$$A = a'^3$$
$$B = b'^3$$
$$C = c'^3$$

so haben wir aus der Lösung der Gleichung $x^3 + y^3 + z^3 = 0$

$$x = a$$
$$y = b$$
$$z = c$$

eine andere Lösung abgeleitet,

$$x = a'$$
$$y = b'$$
$$z = c'$$

$$\text{wo } a'^3 b'^3 c'^3 = \frac{c^3}{(\varepsilon\varepsilon - \varepsilon)^3}$$

wobei also c' den Faktor $1 - \varepsilon$ einmal weniger enthält als c. Dies ist aber widersinnig, wenn c nur durch eine bestimmte Potenz von $1-\varepsilon$ teilbar ist, das heißt, wenn c von 0 verschieden ist. Denn durch Fortsetzen dieser Operationen kämen wir sonst schließlich zu einer Lösung, bei der z überhaupt nicht durch $1 - \varepsilon$ teilbar wäre, im Widerspruch zu (I).

Für Potenzen mit dem Exponenten 5 kann man einen ähnlichen Weg einschlagen. Ist nämlich $a^5 + b^5 + c^5 = 0$, so setzen wir $b + c = \alpha$, $c + a = \beta$, $a + b = \gamma$ und erhalten

$$\begin{aligned} 0 &= (2a)^5 + (2b)^5 + (2c)^5 \\ &= (\beta + \gamma - \alpha)^5 + (\gamma + \alpha - \beta)^5 + (\alpha + \beta - \gamma)^5 \\ &= (\alpha + \beta + \gamma)^5 - 80\alpha\beta\gamma(\alpha\alpha + \beta\beta + \gamma\gamma) \end{aligned}$$

Es kann aber nicht $(\alpha+\beta+\gamma)^5 = 80\alpha\beta\gamma(\alpha\alpha+\beta\beta+\gamma\gamma)$ gelten, ohne dass eine der Zahlen α, β, γ durch $1-\varepsilon$ teilbar ist. Wäre nämlich keine davon teilbar, so müssten sowohl $\alpha+\beta+\gamma$ als auch $\alpha\alpha+\beta\beta+\gamma\gamma$ durch $1-\varepsilon$ teilbar sein, folglich auch $2(\alpha\alpha+\beta\beta+\gamma\gamma)+2(\alpha+\beta+\gamma)(\alpha+\beta-\gamma) = (2\alpha+\beta)^2+3\beta\beta$, was unmöglich ist.

Man kann dies auch so darstellen. Ist $a^5+b^5+c^5=0$, so ist

$$\begin{aligned} 4(a+b+c)^5 &= 5(b+c)(c+a)(a+b) \\ &\qquad [(a+2b+3c)^2+3(a+c)^2-8(a+b+c)c] \\ &= 5(b+c)(c+a)(a+b) \\ &\qquad [(b-c)^2+3(b+c)^2+4(a+b+c)a] \end{aligned}$$

$$4(a+b+c)^5+5abc[(b-c)^2+3(b+c)^2] = 5(a+b+c)\{\dots\}$$

Im Übrigen wäre der Beweis dem vorherigen sehr ähnlich.

Versucht man aber dasselbe Vorgehen bei siebenten Potenzen, so gelingt es nicht zu beweisen, dass bei einer gegebenen Lösung

$$a^7+b^7+c^7=0$$

notwendig eine der Größen a, b, c durch 7 teilbar sein muss. Es folgt nämlich nur

$$\begin{aligned} (\alpha+\beta+\gamma)^7 = 5\alpha\beta\gamma\{&3(\alpha^4+\beta^4+\gamma^4) \\ &+10(\alpha\alpha\beta\beta+\alpha\alpha\gamma\gamma+\beta\beta\gamma\gamma)\} \end{aligned}$$

was gelten kann, ohne dass α, β, γ durch $1-\varepsilon$ teilbar sind.

Hoffentlich lässt sich dies jedoch künftig aus der Natur der Determinanten und der Einheiten ableiten.

[II.]

BESTIMMUNG DER NÄCHSTEN GANZEN ZAHL.

Es sei

$$\begin{aligned} \varepsilon^3 = 1, \quad m &= a+b\varepsilon+c\varepsilon\varepsilon \\ 2a-b-c &= A+\alpha \\ 2b-c-a &= B+\beta \\ 2c-a-b &= C+\gamma \end{aligned}$$

wobei A, B, C ganze Zahlen und α, β, γ positive echte Brüche sind. Dann gilt

$$A+B+C+\alpha+\beta+\gamma=0$$

Es sind also drei Fälle zu unterscheiden:

I. $\alpha + \beta + \gamma = 0$, folglich $\alpha = 0$, $\beta = 0$, $\gamma = 0$

1, $A \equiv B \equiv C \pmod 3$. Hier ist m selbst eine ganze Zahl.

2, $A - B \equiv B - C \equiv C - A \equiv \pm 1 \pmod 3$. Hier ist $m \pm \frac{\varepsilon - \varepsilon\varepsilon}{3} \,.\, \varepsilon^n$ eine ganze Zahl.

II. $\alpha + \beta + \gamma = 1$.

Hier ist jede der Zahlen

$$A + B\varepsilon + C\varepsilon\varepsilon + 1$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon\varepsilon$$

durch $1 - \varepsilon$ teilbar und eine davon durch 3. Der Quotient oder

$$m + \frac{\varepsilon^n - \alpha - \beta\varepsilon - \gamma\varepsilon\varepsilon}{3}$$

ist die gesuchte ganze Zahl.

III. $\alpha + \beta + \gamma = 2$

Hier sind

$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon + \varepsilon\varepsilon$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon\varepsilon + 1$$
$$A + B\varepsilon + C\varepsilon\varepsilon + 1 + \varepsilon$$

durch $1 - \varepsilon$ und eine dieser Zahlen durch 3 teilbar. Der Quotient oder

$$m + \frac{\varepsilon^n(\varepsilon + \varepsilon\varepsilon) - \alpha - \beta\varepsilon - \gamma\varepsilon\varepsilon}{3}$$

ist die gesuchte ganze Zahl.

In allen drei Fällen hat der Rest die Form

$$x + y\varepsilon + z\varepsilon\varepsilon$$

sodass x, y, z dem Betrag nach kleiner als $\frac{1}{3}$ sind und $x+y+z = 0$ gilt. Daraus folgt notwendig

$$xx + yy + zz = 2xx - 2yz = 2yy - 2xz = 2zz - 2xy < \tfrac{2}{9}$$

weil zwei der drei Größen x, y, z notwendig dasselbe Vorzeichen haben. Folglich ist die Determinante des Restes

$$= \tfrac{3}{2}(xx + yy + zz) < \tfrac{1}{3} \qquad \text{Q. E. D.}$$

Die nächste ganze Zahl lässt sich *bequemer* auf folgende Weise bestimmen. Gegeben sei $a + b\varepsilon + c\varepsilon\varepsilon = m$; man setze

$$b - a = C + \gamma$$
$$c - b = A + \alpha$$
$$a - c = B + \beta$$

wobei A, B, C die nächstkleineren ganzen Zahlen und α, β, γ positive Brüche sind. Hier sind drei Fälle zu unterscheiden:

I. $\alpha + \beta + \gamma = 0$; dann ist m selbst eine ganze Zahl

II. $\alpha + \beta + \gamma = 1$; dann ist die nächste ganze Zahl

$$\begin{array}{lll} B + (B+C)\varepsilon & & \text{wenn } \alpha \text{ der größte Bruch ist.} \\ \quad C\varepsilon + (A+C)\varepsilon\varepsilon & \beta & \\ A + B \quad . \quad +A\varepsilon\varepsilon & \gamma & \end{array}$$

II. $\alpha + \beta + \gamma = 2$; dann ist die nächste ganze Zahl

$$\begin{array}{lll} B + 1 + (B + C + 2)\varepsilon & & \text{wenn } \alpha \text{ der kleinste Bruch ist.} \\ \quad (C+1)\varepsilon + (A + C + 2)\varepsilon\varepsilon & \beta & \\ A + B + 2 \quad . \quad +(A+1)\varepsilon\varepsilon & \gamma & \end{array}$$

In II, 1 ist der Rest $\beta + (\beta + \gamma)\varepsilon$, dessen Determinante

$$\begin{aligned} &= \beta\beta + \beta\gamma + \gamma\gamma \\ &= \tfrac{1}{3} - \tfrac{1}{6}[(\alpha - \beta)(1 + 3\beta) + (\alpha - \gamma)(1 + 3\gamma)] \end{aligned}$$

ist.

Noch einfacher so:

Man ordne die Brüche $a - [a], b - [b], c - [c]$ nach ihrer Größe und bezeichne sie der Reihe nach mit p, q, r. Sind alle drei gleich groß, so ist m eine ganze Zahl. Sind sie aber ungleich, so sei t ein beliebiger Bruch zwischen

$$\begin{array}{llll} p \text{ und } q, & \text{jenachdem} & q - p & \text{am größten ist} \\ q \text{ und } r & & r - q & \\ r \text{ und } 1 + p & & 1 + p - r & \end{array}$$

Dann ist

$$[a - t] + [b - t]\varepsilon + [c - t]\varepsilon\varepsilon$$

die nächste ganze Zahl.

[III.]

Es sei $\varepsilon^5 = 1$

$$a + b\varepsilon + c\varepsilon\varepsilon + d\varepsilon^2 + e\varepsilon^4 = q'$$

$$a + b\varepsilon^{-1} + c\varepsilon^{-2} + d\varepsilon^{-3} + e\varepsilon^{-4} = q''''$$

$$(a-b)^2 + (b-c)^2 + (c-d)^2 + (d-e)^2 + (e-a)^2 = 2p'$$

$$(a-c)^2 + (b-d)^2 + (c-e)^2 + (d-a)^2 + (e-b)^2 = 2p''$$

$$q'q'''' = -p'\varepsilon - p''\varepsilon\varepsilon - p''\varepsilon^3 - p'\varepsilon^4 = P'$$
$$q''q''' = -p'\varepsilon\varepsilon - p''\varepsilon^4 - p''\varepsilon - p'\varepsilon^3 = P''$$

$$\text{Determinante} = P'P'' = -p'p' + 3p'p'' - p''p''$$
$$\begin{aligned}\text{Mensura} &= 2p' + 2p'' = 2P' + 2P'' \\ &= 5(aa + bb + cc + dd + ee) - (a + b + c + d + e)^2\end{aligned}$$

Multiplikation mit $1 - \varepsilon$ ergibt die neue Mensur $= 8p'$

$$\text{Höchste Mensur} = 2\left(\frac{\sin 72^\circ}{\sin 36^\circ} + \frac{\sin 36^\circ}{\sin 72^\circ}\right)\sqrt{D} = 4{,}472\sqrt{D}$$

Modul $= 1 - \varepsilon$

$$\begin{aligned}1 - \varepsilon &= x \\ \varepsilon &= 1 - x \\ \varepsilon\varepsilon &= 1 - 2x + xx \\ \varepsilon^3 &= 1 - 3x + 3xx - x^3 \\ \varepsilon^4 &= 1 - 4x + 6xx - 4x^3 + x^4 \\ &= -4 + 6x - 4xx + x^3\end{aligned}$$

Also

$$\begin{aligned}\frac{1 - \varepsilon^n}{1 - \varepsilon} &\equiv n \text{ mod. } (1 - \varepsilon) \\ \varepsilon^n &\equiv 1 - nx \text{ mod. } (1 - \varepsilon)^2 \\ \left(\frac{\varepsilon + \varepsilon^4}{\varepsilon\varepsilon + \varepsilon^3}\right)^n &\equiv 1 + nxx \text{ mod. } (1 - \varepsilon)^3\end{aligned}$$

Eine Zahl, die $\equiv 1$ mod. $(1 - \varepsilon)^3$ ist, kann also *nur* dann eine Einheit sein, wenn sie zugleich $\equiv 1$ (mod. 5) ist.

[IV.]

EINIGES ÜBER DIE MENSUR DER ZAHLEN.

Es sei $\varepsilon^n = 1$, wobei n eine Primzahl ist,

$$\begin{aligned} m &= a + a'\varepsilon + a''\varepsilon\varepsilon + a'''\varepsilon^3 + \ldots + a^{(n-1)}\varepsilon^{n-1} = f\varepsilon \\ D &= f\varepsilon \,.\, f\varepsilon\varepsilon \,.\, f\varepsilon^3 \ldots f\varepsilon^{n-1} \\ f\varepsilon \,.\, f\varepsilon^{n-1} &= -b'(\varepsilon + \varepsilon^{n-1}) - b''(\varepsilon^2 + \varepsilon^{-2}) \\ &\quad - b'''(\varepsilon^3 + \varepsilon^{-3}) \ldots \end{aligned}$$

dann ist

$$\begin{aligned} 2b' &= (a - a')^2 + (a' - a'')^2 + (a'' - a''')^2 + \text{usw.} \\ 2b'' &= (a - a'')^2 + (a' - a''')^2 + (a'' - a'''')^2 + \text{usw.} \\ &\text{usw.} \end{aligned}$$

Hier sind also $b', b'', b''' \ldots$ ausschließlich positive Größen; sie heißen *Partialmensuren* von m, ihre Summe

$$\begin{aligned} b' + b'' + b''' + \text{usw.} &= n(aa + a'a' + a''a'' + \ldots) \\ &\quad - (a + a' + a'' + \text{usw.})^2 \end{aligned}$$

die *Generalmensur*. Setzt man

$$f\varepsilon \,.\, f\varepsilon^{n-1} = c', \quad f\varepsilon\varepsilon \,.\, f\varepsilon^{n-2} = c'' \quad \text{usw.}$$

so ist

$$\begin{aligned} c' + c'' + c''' + \text{usw.} + c^{\frac{1}{2}(n-1)} \\ = b' + b'' + b''' + \text{usw.} + b^{\frac{1}{2}(n-1)} \\ c'(\varepsilon + \varepsilon^{n-1}) + c''(\varepsilon\varepsilon + \varepsilon^{n-2}) + c'''(\varepsilon^3 + \varepsilon^{n-3}) + \text{usw.} \\ = 2(b' + b'' + b''' + \text{usw.} + b^{\frac{1}{2}(n-1)}) - nb' \\ c'(2 - \varepsilon - \varepsilon^{n-1}) + c''(2 - \varepsilon\varepsilon - \varepsilon^{n-2}) \\ + c'''(2 - \varepsilon^3 - \varepsilon^{n-3}) + \text{usw.} = nb' \end{aligned}$$

$$b' > \frac{n-1}{2n}(nD)^{\frac{2}{n-1}}, \quad b' + b'' + b''' + \text{usw.} > \frac{n-1}{2} \,.\, D^{\frac{2}{n-1}}$$

Gilt allgemein

$$f\varepsilon \,.\, f\varepsilon^{n-1} = A + A'\varepsilon + A''\varepsilon\varepsilon + A'''\varepsilon^3 + \ldots$$

so ist die Generalmensur $\triangle = -A - A' - A'' - \text{usw.} + nA$

Mensur von $(1+\varepsilon)f\varepsilon\ldots$

$$\triangle' = 4\triangle - 2n(A - A') = 4\triangle - 2nb'$$

Ist $a + a' + a'' + \ldots = 0$, so ist $\triangle = n(aa + a'a' + a''a'' + \text{usw.})$

und ist $A + A' + A'' + \ldots = 0$, so ist $\triangle = nA$, $\triangle' = n(2A + 2A')$

Ist also einer der Koeffizienten A', A'' usw. negativ und dem Betrag nach größer als $\frac{1}{2}A$, so lässt sich die Mensur verringern, ohne die Determinante zu ändern.

[V.]

Sollte sich bestätigen, dass jede Einheit nur aus Faktoren der Form

$$\frac{\varepsilon^\alpha - \varepsilon^\beta}{\varepsilon^\gamma - \varepsilon^\delta}$$

zusammengesetzt ist, so wäre folgender Satz bewiesen:

Ist $f(\varepsilon)$ eine Einheit, so ist

$$\frac{f(\varepsilon)}{f(\varepsilon^{-1})} = \varepsilon^n$$

Auch ohne *jenen* Satz *vorauszusetzen*, lässt sich der Schlusssatz leicht beweisen. Es sei

$$\frac{f\varepsilon}{f\varepsilon^{-1}} = F\varepsilon$$

dann ist

$$F\varepsilon \,.\, F\varepsilon^{-1} = 1$$

woraus sich mithilfe der Lehre von der Mensur leicht ergibt, dass

$$F\varepsilon = \pm\varepsilon^n$$

Das untere Zeichen ist jedoch unmöglich, weil sonst $f\varepsilon$ durch $1 - \varepsilon$ teilbar sein müsste.

Dass die Determinante einer von 0 verschiedenen Zahl nicht $= 0$ sein kann, lässt sich leicht beweisen. Ist die Determinante durch m teilbar, so ist die Zahl selbst durch $1 - \varepsilon$ teilbar. Ist also die Determinante durch m^{m-1} teilbar, so muss die Zahl selbst durch m teilbar sein. Dies ist widersinnig, denn bei der Determinante 0 könnte man die Zahl zunächst so oft durch m teilen, ohne die Determinante zu ändern, bis sie nicht mehr teilbar wäre. Der erste Satz wird so ersichtlich. Es sei die gegebene Zahl

$$a + b\varepsilon + c\varepsilon\varepsilon + \text{usw.} \equiv a + b + c\,..\ \text{mod. } 1 - \varepsilon$$

also ihre Determinante $\equiv (a + b + c\,..)^{m-1}$ mod. $1 - \varepsilon$.

[VI.]

Es sei $\varepsilon^n = 1$

$$\begin{aligned} f\varepsilon &= a + b\varepsilon + c\varepsilon\varepsilon + d\varepsilon^3 + \text{usw.} \\ m &= \text{Determinante dieser Zahl} \\ \frac{m}{f\varepsilon} &= f\varepsilon\varepsilon \,.\, f\varepsilon^3 \ldots f\varepsilon^{n-1} \\ &= A + B\varepsilon + C\varepsilon\varepsilon + \text{usw.} = F\varepsilon \end{aligned}$$

Der Zahl $f\varepsilon$ entspricht eine Wurzel der Kongruenz $x^n \equiv 1$ (mod. m.) Sie sei r. Es gilt

$$\begin{aligned} nA &= F1 + F\varepsilon + F\varepsilon\varepsilon + .. \\ nB &= F1 + \varepsilon^{-1}F\varepsilon + \varepsilon^{-2}F\varepsilon\varepsilon + .. \\ nC &= F1 + \varepsilon^{-2}F\varepsilon + \varepsilon^{-4}F\varepsilon\varepsilon + .. \\ &\text{usw.} \end{aligned}$$

Da $F\varepsilon\varepsilon, F\varepsilon^3, F\varepsilon^4$ usw. durch $f\varepsilon$ teilbar sind, sind also

$$\begin{gathered} nA - F1 - \varepsilon(nB - F1) \\ nA - F1 - \varepsilon\varepsilon(nC - F1) \\ nA - F1 - \varepsilon^3(nD - F1) \\ \text{usw.} \end{gathered}$$

alle durch $f\varepsilon$ teilbar oder auch

$$\begin{gathered} n(A - B) - \varepsilon n(B - C) \\ n(B - C) - \varepsilon n(C - D) \\ \text{usw.} \end{gathered}$$

durch $f\varepsilon$ teilbar; folglich [wenn $f\varepsilon$ durch $1 - \varepsilon$ und $F\varepsilon$ durch eine reelle ganze Zahl nicht teilbar ist]

$$\varepsilon \equiv \frac{A - B}{B - C} \equiv \frac{B - C}{C - D} \equiv \frac{C - D}{D - E} \text{ usw. (mod. } f\varepsilon)$$

BEMERKUNGEN.

Die hier unter der gemeinsamen Überschrift Zur Theorie der komplexen Zahlen zusammengestellten Untersuchungen sind verstreute Notizen in der Handschrift. Sie enthalten die wesentlichen Schritte des Beweises des FERMATschen Satzes für die dritte und fünfte Potenz. Die aus dritten Einheitswurzeln zusammengesetzten Zahlen sind in unvollständigen, hier nicht abgedruckten Aufzeichnungen sowohl mithilfe der Theorie der binären quadratischen Formen als auch der Kreisteilung untersucht. Bei der Anwendung der letzteren, und zwar während der Ausarbeitung der Abhandlung *Disquisitionum circa aequationes puras ulterior evolutio*, wurde auch die ternäre kubische Form aufgestellt, in die $27\frac{x^n-1}{x-1}$ für eine Primzahl $n \equiv 1 \bmod. 3$ umgewandelt werden kann. Zugleich wurde die Theorie der Komposition der damit verwandten Form $X^3 + mY^3 + mmZ^3 - 3mXYZ$ entwickelt.

Die in den Untersuchungen des Bruchstücks [I] vorausgesetzte Eigenschaft der aus dritten Einheitswurzeln gebildeten ganzen Zahlen, dass jede nur auf eine Weise in Primfaktoren zerlegt werden kann, ergibt sich aus dem EUKLIDischen Verfahren zur Bestimmung der gemeinsamen Teiler zweier Zahlen, wenn man dabei den unter [II] hergeleiteten Satz über die nächste ganze Zahl zu einem beliebig vorgegebenen Bruch anwendet.

Dass dieselbe grundlegende Eigenschaft auch den aus fünften Einheitswurzeln zusammengesetzten Zahlen zukommt, folgt daraus, dass der nach einer ganz entsprechenden Regel wie in [II] gebildete Bruchrest entweder von m oder aber von m multipliziert mit einer geeigneten Einheit E so beschaffen ist, dass er durch Subtraktion von der gegebenen Zahl mE eine ganze Zahl ergibt und dass seine Determinante die Einheit nicht übersteigt. Die Einheiten lassen sich aber, wie in [III] angedeutet, aus der Theorie der binären quadratischen Formen der Determinante 5 in Verbindung mit der Zerlegung irgendeiner reellen Primzahl in vier Faktoren (zum Beispiel $11 = \text{Det. } (2+\varepsilon)$) ableiten, nämlich als Produkte der Potenzen von ε und $1 + \varepsilon$.

SCHERING.

TAFEL

DES QUADRATISCHEN CHARAKTERS

DER PRIMZAHLEN VON 2 BIS 997 ALS RESTE

IN BEZUG

AUF DIE PRIMZAHLEN VON 3 BIS 503 ALS TEILER.

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	
3		−		−		−		−			−	−		−				3
5			−		−			−		−	−		−				−	5
7	−			−	−				−	−		−		−		−		7
11		−	−		−				−		−	−			−	−	−	11
13		−				−	−		−	−				−		−		13
17	−					−	−	−						−	−	−	−	17
19			−	−	−		−	−	−					−	−			19
23	−	−				−			−	−	−		−		−		−	23
29			−	−		−			−	−						−	−	29
31	−		−	−				−			−		−		−		−	31
37		−		−	−							−	−		−	−		37
41	−		−						−		−	−	−	−			−	41
43					−	−	−		−		−		−	−	−	−	−	43
47	−	−		−			−					−			−	−	−	47
53				−	−	−	−			−		−		−	−	−	−	53
59		−	−	−			−	−		−			−			−	−	59
61		−	−			−		−					−		−			61
67							−	−	−	−		−			−		−	67
71	−	−	−					−		−		−		−				71
73	−	−						−	−			−	−					73
79	−		−		−	−		−	−		−							79
83		−		−	−		−		−	−	−	−	−				−	83
89	−		−		−		−								−	−		89
97	−	−			−						−			−	−	−		97
101			−			−	−	−	−		−	−		−	−			101
103	−			−		−	−	−	−	−			−				−	103
107		−			−	−		−	−	−		−	−		−	−		107
109		−	−	−						−	−			−				109
113	−			−	−	−					−		−			−		113
127	−				−	−	−	−			−	−	−		−			127
131		−	−	−	−	−							−	−		−	−	131
137	−			−	−		−	−				−					−	137
139			−	−	−	−				−	−	−	−		−			139
149			−	−			−	−		−	−	−			−	−		149
151	−		−		−		−	−		−	−	−		−	−		−	151
157		−			−	−	−	−			−	−			−			157
163													−	−	−	−		163
167	−	−		−	−			−		−	−				−			167
173						−			−	−	−	−	−	−	−			173
179		−	−			−	−	−		−	−			−	−		−	179
181		−	−		−	−				−		−		−			−	181
191	−	−	−			−	−		−					−			−	191
193	−	−		−					−		−			−			−	193
197				−				−	−	−		−	−	−	−	−	−	197
199	−		−	−		−			−	−	−			−	−	−		199
211			−		−	−		−				−		−	−	−	−	211
223	−			−			−	−		−	−	−	−	−	−	−		223
227		−		−	−			−	−	−				−	−	−	−	227
	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	

	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	
3	−	−		−	−			−		−		−		−			−	3
5	−		−		−		−		−			−			−		−	5
7		−	−		−						−	−	−	−		−		7
11		−	−				−	−		−			−			−		11
13	−				−				−	−	−		−	−	−		−	13
17		−				−	−		−	−				−		−		17
19	−			−		−			−						−	−	−	19
23			−	−					−					−	−		−	23
29		−	−			−				−	−	−					−	29
31		−	−					−	−	−	−	−	−		−			31
37		−	−	−		−			−		−			−		−	−	37
41	−			−		−				−	−		−	−	−		−	41
43		−			−	−		−	−	−	−	−		−			−	43
47	−		−		−	−	−	−	−	−					−			47
53							−	−			−		−		−			53
59			−		−						−			−		−	−	59
61	−			−		−		−		−	−	−	−	−	−	−		61
67		−	−	−		−	−			−	−			−	−			67
71			−	−	−	−	−		−	−	−	−			−			71
73	−	−	−	−	−		−	−				−		−		−		73
79		−		−	−	−	−	−	−						−			79
83	−					−						−	−	−	−			83
89		−	−	−	−		−	−			−	−			−		−	89
97	−			−	−		−	−	−	−		−	−					97
101			−		−			−	−		−				−	−		101
103	−				−	−		−		−	−				−	−	−	103
107	−				−	−	−		−		−					−		107
109	−		−	−		−	−	−				−	−		−	−		109
113	−					−		−				−	−	−	−		−	113
127	−		−	−	−					−	−		−	−	−			127
131	−						−		−		−	−	−		−			131
137	−			−					−	−	−	−				−	−	137
139		−	−		−	−	−				−		−	−	−	−	−	139
149	−	−		−						−	−		−	−				149
151								−		−				−		−	−	151
157		−	−				−		−			−	−	−				157
163	−		−			−		−					−		−			163
167	−						−	−			−			−		−		167
173		−		−		−	−					−	−			−	−	173
179	−	−				−	−		−		−						−	179
181		−		−	−				−							−	−	181
191		−			−			−		−	−	−						191
193		−				−		−	−		−	−			−	−	−	193
197	−					−		−	−		−	−		−		−		197
199	−				−		−			−					−		−	199
211			−	−	−	−			−	−	−	−	−			−	−	211
223				−		−	−		−			−		−	−		−	223
227			−	−	−		−	−	−	−		−	−		−		−	227
	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	
229		−	−		−		−	−				−		−		−		229
233	−			−		−		−	−	−	−	−						233
239	−	−	−		−		−			−	−							239
241	−	−	−							−			−		−	−	−	241
251		−	−	−		−	−		−		−		−					251
257	−				−	−	−		−	−	−						−	257
263	−	−			−	−	−		−		−	−		−				263
269			−		−	−			−			−	−	−	−	−		269
271	−		−	−	−		−				−	−	−			−		271
277		−		−		−		−	−	−			−		−		−	277
281	−		−	−			−			−	−			−		−	−	281
283				−	−	−			−	−			−				−	283
293							−				−	−		−		−	−	293
307				−	−		−	−				−	−			−		307
311	−	−	−	−		−									−	−		311
313	−	−			−	−		−		−								313
317				−	−				−		−	−		−		−	−	317
331			−				−	−			−			−		−		331
337	−	−		−		−						−	−	−	−			337
347		−			−	−				−	−			−		−	−	347
349		−	−				−	−	−	−	−	−	−					349
353	−				−		−	−	−	−			−	−	−			353
359	−	−	−		−		−		−			−	−		−			359
367	−			−		−			−		−	−	−		−	−	−	367
373		−		−		−	−			−	−	−	−				−	373
379			−					−	−			−	−					379
383	−	−		−			−	−	−	−	−			−				383
389			−	−	−	−	−	−					−				−	389
397		−			−			−	−	−	−	−		−	−			397
401	−		−	−	−					−			−	−	−			401
409	−	−	−				−		−				−			−		409
419		−	−	−		−			−	−		−	−	−	−		−	419
421		−	−	−	−		−				−							421
431	−	−	−		−			−	−	−			−			−	−	431
433	−	−			−	−	−					−	−			−	−	433
439	−		−	−	−	−		−		−						−		439
443		−				−	−					−	−		−		−	443
449	−		−	−	−				−				−			−	−	449
457	−	−		−			−	−		−					−			457
461			−				−	−	−				−	−		−	−	461
463	−						−			−	−			−	−		−	463
467		−		−		−	−		−				−	−	−	−	−	467
479	−	−	−	−	−				−									479
487	−							−		−	−		−			−		487
491		−	−		−	−	−				−	−	−	−				491
499			−							−	−			−	−			499
503	−	−		−	−	−			−					−	−		−	503
	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	

	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	
229	–		–			–		–		–								229
233			–				–		–		–	–	–		–			233
239	–	–	–			–			–			–	–	–				239
241	–	–			–	–		–			–		–					241
251		–		–	–	–	–		–	–			–		–			251
257	–	–		–	–		–						–			–	–	257
263	–					–	–			–		–				–		263
269	–	–		–	–		–	–		–				–	–			269
271	–	–			–	–	–			–							–	271
277		–	–		–	–	–						–		–			277
281					–				–			–				–		281
283	–		–	–		–	–	–	–	–			–	–		–		283
293	–	–	–	–		–		–			–	–				–		293
307			–		–	–	–	–	–	–	–	–	–	–				307
311		–		–	–	–	–				–	–	–	–		–	–	311
313			–		–	–		–		–	–		–			–	–	313
317	–	–		–	–	–	–		–	–			–		–			317
331		–	–		–	–	–			–		–	–	–	–		–	331
337					–					–	–		–		–	–		337
347	–	–	–	–		–	–				–	–	–	–	–	–		347
349		–		–		–						–					–	349
353	–			–		–		–				–	–	–	–			353
359				–	–				–		–			–	–			359
367	–	–		–		–	–		–		–		–			–		367
373			–	–		–	–		–	–	–	–				–		373
379	–	–			–	–		–	–	–	–			–		–	–	379
383		–	–	–					–	–			–			–	–	383
389		–		–	–			–					–	–		–		389
397		–		–	–	–		–			–			–	–	–		397
401				–		–	–			–		–	–					401
409			–			–	–		–	–		–			–	–	–	409
419				–	–			–			–				–	–	–	419
421		–			–			–	–	–	–	–	–		–		–	421
431	–							–				–					–	431
433					–							–		–		–	–	433
439	–		–	–		–				–		–	–	–		–	–	439
443	–	–	–		–		–			–	–	–	–		–	–	–	443
449	–	–					–	–	–					–		–		449
457		–		–	–						–	–		–	–			457
461	–	–		–			–			–	–	–	–			–	–	461
463	–	–		–	–		–	–		–		–	–		–			463
467			–			–	–	–				–	–	–		–	–	467
479	–		–	–			–	–		–	–	–			–	–	–	479
487	–	–	–	–		–	–	–		–	–			–		–	–	487
491	–		–		–	–		–	–		–			–	–		–	491
499		–		–					–	–	–	–		–	–	–	–	499
503	–	–		–	–	–		–					–		–			503
	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	

	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	
3		–	–	–				–		–		–	–	–		–		3
5	–	–					–	–	–			–	–			–		5
7	–	–		–			–		–	–	–		–				–	7
11			–	–			–	–	–			–		–		–		11
13			–			–	–	–	–			–	–				–	13
17	–	–	–				–		–					–		–		17
19	–		–	–					–		–	–				–	–	19
23		–		–	–	–	–			–	–		–	–			–	23
29	–	–			–	–	–	–			–	–		–	–		–	29
31	–		–	–		–			–	–			–		–		–	31
37	–	–	–			–		–			–		–	–		–	–	37
41				–		–					–			–				41
43					–	–		–		–	–					–		43
47	–		–			–			–		–							47
53	–			–							–	–	–	–	–	–		53
59				–	–			–		–	–	–		–				59
61	–			–	–		–				–	–				–		61
67	–	–	–	–	–	–		–		–		–	–	–	–			67
71		–	–		–		–		–			–		–		–	–	71
73	–					–		–					–	–	–			73
79		–		–	–		–	–						–				79
83		–			–	–			–	–	–	–			–	–		83
89			–		–	–	–					–		–	–		–	89
97		–		–	–				–	–	–				–	–		97
101			–				–	–		–	–		–	–	–		–	101
103	–			–	–		–							–		–		103
107	–	–		–						–	–	–		–	–		–	107
109			–			–			–	–	–		–	–	–		–	109
113	–		–	–		–							–		–		–	113
127	–		–	–			–		–		–	–	–		–			127
131		–			–		–		–	–			–				–	131
137		–			–	–		–		–	–		–					137
139				–	–	–		–	–	–								139
149	–					–	–		–							–		149
151		–			–	–			–	–				–	–	–		151
157			–		–	–				–	–	–					–	157
163		–		–	–	–	–				–	–		–	–			163
167			–		–	–	–	–	–			–	–	–		–	–	167
173	–	–	–	–	–	–	–				–		–		–	–	–	173
179	–	–				–	–		–	–		–			–			179
181					–			–		–	–			–	–	–	–	181
191	–			–					–	–	–	–	–	–	–			191
193		–	–				–	–	–	–	–	–	–			–		193
197			–	–		–		–	–	–	–			–			–	197
199		–	–							–		–			–			199
211		–		–		–	–			–		–	–		–			211
223							–	–			–	–	–	–	–			223
227					–	–		–							–			227
	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	

	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	
3		–					–	–		–		–		–		–	–	3
5	–	–	–			–	–		–				–			–		5
7	–				–			–	–						–	–	–	7
11			–	–		–							–	–	–	–		11
13			–	–	–	–		–		–			–	–			–	13
17	–		–	–	–		–		–		–	–				–		17
19	–		–		–		–	–		–			–	–				19
23	–			–		–	–	–				–	–		–	–		23
29	–	–		–				–	–	–				–				29
31				–					–	–	–	–	–		–			31
37					–	–	–				–	–			–		–	37
41		–	–			–	–	–		–		–					–	41
43	–		–			–	–		–	–	–	–	–		–		–	43
47	–	–	–		–	–	–	–		–		–				–	–	47
53		–				–	–		–		–	–	–		–	–		53
59	–	–	–	–	–		–	–	–		–	–	–		–	–		59
61	–	–		–	–	–	–			–	–				–			61
67		–		–	–	–		–		–	–	–			–			67
71			–		–		–	–			–		–	–				71
73			–	–		–				–	–		–		–			73
79	–	–		–	–	–		–	–	–				–	–		–	79
83		–						–			–			–	–			83
89			–	–	–	–	–	–		–		–	–		–	–		89
97		–				–				–	–	–		–				97
101	–		–						–	–		–			–			101
103	–					–							–	–	–		–	103
107	–	–	–		–		–			–	–			–		–	–	107
109	–				–				–		–	–	–			–		109
113	–	–	–	–				–		–		–	–	–	–	–	–	113
127			–		–	–	–											127
131	–				–	–	–	–		–		–	–		–		–	131
137				–	–				–	–	–		–	–			–	137
139	–		–	–	–					–		–		–				139
149			–		–	–			–		–	–			–	–	–	149
151	–	–	–			–						–	–	–		–		151
157	–			–	–			–	–	–			–	–	–	–		157
163			–		–				–			–		–				163
167	–		–		–				–	–	–		–		–		–	167
173			–	–	–	–							–	–	–	–	–	173
179	–														–		–	179
181		–	–		–				–	–		–		–	–		–	181
191	–	–	–		–	–	–	–	–	–	–		–					191
193	–	–		–				–			–		–		–	–	–	193
197	–		–	–							–		–	–		–		197
199	–		–	–	–	–	–				–		–	–		–		199
211		–		–	–	–		–	–		–	–	–			–	–	211
223	–	–	–	–					–	–					–			223
227	–			–	–		–						–		–	–	–	227
	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	

	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	
229	–	–			–	–		–		–						–	–	229
233			–		–	–		–			–					–	–	233
239			–	–						–	–		–					239
241		–						–	–	–			–	–		–	–	241
251	–					–	–	–			–		–		–		–	251
257			–			–				–	–	–	–	–	–			257
263	–	–	–			–	–	–						–			–	263
269	–	–				–			–			–	–				–	269
271		–		–	–		–						–	–		–	–	271
277			–						–	–			–			–		277
281	–		–	–	–			–	–				–	–				281
283		–	–	–			–	–				–	–		–		–	283
293	–				–				–	–	–	–	–			–	–	293
307	–				–		–	–	–			–		–	–	–	–	307
311			–	–		–	–			–	–			–		–		311
313		–	–	–		–		–			–	–						313
317	–		–		–	–	–	–		–				–	–			317
331	–		–	–	–	–	–		–	–	–			–			–	331
337	–				–	–	–	–		–			–		–	–	–	337
347	–		–		–	–		–			–	–				–		347
349		–	–					–	–					–	–		–	349
353			–		–			–	–		–			–			–	353
359	–	–				–		–	–	–						–	–	359
367	–	–				–		–	–			–	–		–	–		367
373				–			–	–								–		373
379	–	–			–	–	–		–	–	–		–		–			379
383	–					–				–				–	–	–		383
389			–			–	–	–		–			–	–				389
397		–		–	–	–	–		–							–		397
401	–	–				–	–	–			–			–		–		401
409				–	–		–		–	–	–				–	–		409
419	–	–	–			–			–		–	–						419
421	–			–	–			–	–			–				–		421
431	–	–	–	–		–	–				–			–	–	–		431
433					–		–		–		–	–	–	–		–	–	433
439					–				–			–	–	–		–		439
443	–	–		–	–			–	–		–				–	–	–	443
449					–			–	–	–	–	–			–	–		449
457		–	–	–					–		–				–	–	–	457
461		–	–	–	–			–	–	–		–		–	–	–		461
463	–			–	–	–	–	–					–			–		463
467	–	–	–	–		–	–			–		–		–	–	–	–	467
479		–		–	–	–		–		–	–		–				–	479
487			–		–			–	–	–	–							487
491				–			–	–			–	–		–	–	–	–	491
499		–			–			–			–	–	–		–		–	499
503						–					–	–		–		–	–	503
	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	

	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	
229		–					–	–			–	–	–				–	229
233		–	–		–	–	–			–	–	–				–	–	233
239	–	–	–	–	–	–	–			–	–	–	–				–	239
241	–	–	–	–			–	–	–					–		–	–	241
251		–	–		–		–						–		–	–	–	251
257	–	–		–						–	–	–			–			257
263					–	–	–		–			–	–	–	–	–	–	263
269	–				–	–				–	–	–		–		–		269
271		–					–		–		–	–	–					271
277		–						–	–		–	–	–	–	–			277
281		–			–		–	–	–	–				–	–	–	–	281
283			–	–	–	–	–		–	–	–	–	–		–		–	283
293	–			–		–	–	–		–	–	–			–	–		293
307			–	–		–		–			–	–	–	–	–	–		307
311								–					–	–	–	–	–	311
313		–			–	–		–	–			–	–	–	–	–	–	313
317			–	–	–			–	–	–	–	–	–	–	–			317
331	–	–				–	–		–	–	–			–		–	–	331
337	–	–	–		–				–	–			–	–		–	–	337
347		–	–		–	–	–	–	–		–							347
349	–	–		–	–	–	–		–	–	–	–		–			–	349
353						–	–	–	–	–	–	–	–		–	–	–	353
359		–							–	–		–			–	–		359
367			–				–	–	–	–				–				367
373	–		–	–						–		–					–	373
379	–		–	–	–		–	–	–			–	–	–		–	–	379
383			–		–			–			–			–	–	–		383
389	–					–		–		–	–		–	–		–	–	389
397				–			–	–	–		–	–						397
401	–	–		–	–							–	–	–		–	–	401
409	–						–		–			–	–	–	–		–	409
419			–	–		–			–		–						–	419
421	–	–				–		–	–	–		–		–	–		–	421
431					–			–		–		–					–	431
433		–		–		–	–	–		–	–					–	–	433
439			–			–	–		–	–		–				–		439
443					–		–		–		–	–	–			–		443
449			–		–	–	–				–					–	–	449
457	–	–		–		–				–		–	–	–		–		457
461					–				–				–		–	–		461
463	–		–				–	–		–	–		–	–			–	463
467	–	–	–					–		–					–	–		467
479		–	–	–			–	–			–	–		–		–		479
487		–	–		–	–	–	–				–	–	–			–	487
491	–	–		–	–	–		–			–					–		491
499	–		–	–	–			–	–		–	–			–	–	–	499
503				–	–		–		–	–	–				–			503
	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	

	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	
3		–			–	–	–			–		–		–		–	–	3
5		–		–			–		–		–	–	–	–	–		–	5
7	–			–		–	–		–		–			–	–			7
11			–		–		–	–	–	–	–		–	–		–		11
13	–				–	–			–				–			–	–	13
17		–	–	–		–		–	–			–		–		–		17
19	–	–	–	–	–				–	–			–					19
23	–	–	–							–		–					–	23
29	–	–	–			–		–		–	–		–		–		–	29
31		–		–		–	–			–			–	–	–		–	31
37		–		–	–	–	–			–			–			–		37
41		–	–	–	–	–	–		–		–	–	–		–	–		41
43			–	–	–		–			–	–				–		–	43
47	–		–				–	–		–	–				–		–	47
53	–				–							–			–	–	–	53
59				–		–	–	–	–							–	–	59
61	–		–		–		–								–		–	61
67		–		–					–	–			–	–	–		–	67
71				–	–	–	–					–	–		–			71
73	–	–	–	–	–	–		–	–	–	–		–				–	73
79	–				–			–	–	–				–	–	–	–	79
83		–	–	–		–		–		–	–	–	–		–			83
89	–				–	–					–	–						89
97			–				–		–	–			–	–	–			97
101				–	–	–	–	–				–		–				101
103	–			–	–	–					–	–	–	–	–			103
107						–		–		–				–	–		–	107
109	–	–	–			–					–	–		–	–	–	–	109
113	–		–		–			–	–		–			–			–	113
127			–		–			–	–	–			–		–	–		127
131			–		–		–	–		–		–		–	–		–	131
137	–				–	–	–	–	–	–		–	–			–	–	137
139	–	–		–	–							–		–		–		139
149	–			–	–		–	–			–		–	–	–			149
151	–	–						–		–	–						–	151
157	–	–	–						–				–		–			157
163	–			–	–	–	–	–		–		–	–	–			–	163
167			–	–	–			–		–		–	–	–	–	–		167
173	–			–	–		–	–	–	–	–		–		–			173
179	–			–	–	–		–	–	–	–	–	–			–	–	179
181	–	–	–	–	–	–			–		–			–				181
191	–	–	–					–		–		–		–	–	–		191
193				–			–	–	–			–						193
197	–		–				–				–	–	–		–	–		197
199				–			–	–						–	–	–		199
211	–			–				–	–				–		–	–		211
223	–	–	–	–	–		–		–		–		–			–		223
227	–	–		–								–	–				–	227
	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	

	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	
3			–		–			–		–				–	–	–		3
5		–		–			–		–	–		–	–		–			5
7	–	–	–		–			–	–	–					–	–	–	7
11	–	–			–	–		–		–		–	–					11
13	–					–			–		–		–	–		–		13
17	–		–	–	–	–			–			–		–			–	17
19	–		–	–	–	–	–		–	–	–				–		–	19
23	–	–		–	–			–	–	–		–			–	–		23
29			–		–			–		–		–	–	–		–	–	29
31	–					–	–				–		–		–	–		31
37	–								–			–	–					37
41	–	–		–		–		–	–					–	–			41
43	–			–			–	–				–			–	–	–	43
47			–				–	–	–				–	–	–			47
53		–		–		–		–					–	–	–	–		53
59		–		–			–	–	–	–			–	–		–	–	59
61	–	–		–	–		–	–	–		–							61
67		–	–	–		–	–		–			–		–			–	67
71					–					–	–	–	–			–	–	71
73			–	–	–		–	–		–	–	–		–		–	–	73
79			–			–	–	–		–				–	–	–	–	79
83	–						–			–		–	–	–		–	–	83
89	–	–		–	–	–	–	–				–		–				89
97		–		–	–	–	–	–	–		–	–	–			–	–	97
101		–							–	–		–	–		–		–	101
103				–		–			–		–	–		–	–	–		103
107			–	–	–	–					–	–				–		107
109	–		–	–	–	–	–			–		–		–	–		–	109
113	–			–	–	–					–	–	–			–	–	113
127	–	–	–		–		–				–	–	–	–			–	127
131			–			–		–									–	131
137	–	–		–		–	–	–		–		–		–	–	–	–	137
139				–	–						–			–	–		–	139
149	–				–	–								–		–	–	149
151			–	–	–			–	–		–		–		–	–		151
157			–	–		–		–						–		–	–	157
163			–	–				–		–	–			–		–		163
167		–		–		–			–		–	–		–			–	167
173					–	–	–				–	–		–	–		–	173
179	–						–	–		–	–	–			–		–	179
181	–	–		–	–		–	–	–	–		–		–		–	–	181
191		–	–	–	–	–	–		–	–	–							191
193		–		–		–	–	–						–		–		193
197	–	–	–				–	–	–	–	–		–				–	197
199	–	–		–	–		–	–				–	–	–				199
211	–					–		–	–		–	–	–	–	–	–		211
223	–			–	–		–	–		–		–				–		223
227		–	–	–	–		–	–			–			–	–		–	227
	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	

	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	
229	–			–	–	–		–		–	–	–		–	–	–	–	229
233		–	–	–												–		233
239	–	–		–	–	–		–	–		–	–	–	–	–		–	239
241	–	–		–							–			–		–		241
251				–		–									–			251
257		–				–	–			–	–		–			–		257
263		–		–	–						–		–				–	263
269	–	–	–						–				–	–		–	–	269
271		–	–	–				–		–		–	–		–	–		271
277	–		–		–		–	–	–	–				–	–	–		277
281	–	–	–	–	–		–			–		–	–	–			–	281
283	–	–	–			–	–	–	–				–	–		–		283
293	–	–	–					–	–	–			–			–		293
307	–	–	–		–	–		–		–	–	–	–	–				307
311	–		–	–	–			–	–		–	–	–		–		–	311
313		–			–		–	–	–		–	–		–				313
317			–	–				–				–		–				317
331	–		–		–				–		–		–		–	–		331
337		–	–			–	–		–		–	–	–	–	–	–		337
347	–			–				–	–					–				347
349		–	–							–		–	–					349
353		–	–					–	–	–				–	–		–	353
359				–	–		–	–	–			–	–		–	–	–	359
367	–				–			–		–			–		–	–	–	367
373						–		–	–		–	–	–	–			–	373
379	–				–		–	–			–	–				–		379
383			–			–		–	–	–	–		–	–	–	–	–	383
389	–		–	–		–		–	–			–	–		–	–		389
397		–	–		–			–		–	–	–			–	–	–	397
401						–	–	–		–	–	–	–	–		–		401
409		–		–		–	–		–	–	–	–	–	–		–	–	409
419	–	–				–	–		–		–	–	–		–		–	419
421	–		–			–		–			–	–		–		–		421
431	–		–				–		–	–					–	–	–	431
433				–	–		–	–	–	–	–	–		–	–	–	–	433
439	–		–			–	–			–		–				–	–	439
443	–	–		–	–	–		–	–			–	–					443
449	–	–		–	–		–					–		–	–	–	–	449
457	–	–		–		–			–		–	–	–	–		–	–	457
461	–			–	–	–				–					–		–	461
463				–	–	–		–	–			–	–				–	463
467		–				–			–					–		–		467
479		–				–				–	–			–				479
487						–	–	–		–	–		–		–	–	–	487
491		–					–		–		–	–	–					491
499			–	–						–	–	–		–	–	–	–	499
503					–	–	–	–	–	–	–			–		–		503
	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	

	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	
229	–	–	–	–	–	–			–		–	–			–		–	229
233	–		–			–	–		–	–	–		–			–	–	233
239	–		–				–	–			–	–		–				239
241			–			–	–	–	–			–		–	–		–	241
251	–	–							–		–	–		–	–	–		251
257			–				–		–	–	–			–				257
263		–		–	–	–	–						–				–	263
269		–	–					–	–							–		269
271		–				–			–	–		–	–	–		–		271
277					–	–	–	–	–	–					–	–	–	277
281	–			–						–	–	–		–			–	281
283	–		–				–	–	–	–			–	–		–		283
293	–	–			–		–		–	–	–	–	–			–		293
307			–		–	–			–		–			–	–	–	–	307
311			–	–		–	–		–	–	–		–	–				311
313			–		–		–	–				–	–	–	–	–		313
317				–		–				–	–		–			–	–	317
331		–	–	–	–			–			–					–		331
337		–			–			–		–		–					–	337
347		–	–	–	–	–	–	–	–	–	–			–	–			347
349	–	–	–			–	–		–						–	–		349
353										–		–	–		–	–		353
359		–	–	–		–	–	–	–		–	–	–	–	–	–	–	359
367		–		–		–	–	–	–	–					–		–	367
373	–		–	–	–	–	–	–			–		–				–	373
379	–	–			–	–	–			–		–	–	–			–	379
383						–	–		–	–		–	–				–	383
389	–		–		–	–			–		–	–					–	389
397				–			–	–		–	–		–	–	–		–	397
401			–				–	–	–	–	–				–	–	–	401
409	–	–	–		–				–	–		–				–		409
419			–			–	–			–	–		–		–			419
421		–	–			–	–			–	–		–					421
431	–	–		–	–	–	–		–		–		–	–	–	–		431
433		–	–			–		–		–	–		–		–			433
439	–	–	–	–		–	–		–		–	–			–			439
443	–		–				–		–	–		–					–	443
449		–	–		–	–				–			–		–	–		449
457	–	–	–	–	–				–	–			–		–		–	457
461			–	–		–		–	–					–	–		–	461
463	–	–	–		–	–	–			–			–	–	–	–	–	463
467	–	–		–		–	–				–				–		–	467
479							–	–	–	–	–	–	–	–				479
487	–			–	–	–		–	–		–			–		–	–	487
491			–	–	–	–			–		–					–		491
499		–	–			–		–	–	–	–		–	–				499
503	–				–						–	–	–			–	–	503
	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	

	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	
3			–	–				–	–	–		–	–		–			3
5		–	–				–	–				–	–	–				5
7		–	–				–			–	–		–	–			–	7
11				–	–		–				–	–	–	–	–	–	–	11
13	–	–	–				–	–	–					–		–	–	13
17	–	–		–	–	–	–			–			–			–		17
19			–	–	–	–				–	–	–	–		–	–	–	19
23				–	–	–	–	–	–							–	–	23
29			–		–	–				–			–		–	–		29
31	–			–		–	–		–		–						–	31
37			–			–	–	–		–	–	–		–				37
41		–					–		–	–	–	–	–			–		41
43	–	–					–			–	–	–			–			43
47			–					–		–	–	–			–	–	–	47
53				–	–	–	–		–			–			–	–	–	53
59				–		–	–		–		–	–	–	–	–	–	–	59
61	–	–	–					–	–	–		–						61
67		–	–					–	–	–	–	–			–			67
71		–	–	–	–	–				–	–			–	–	–		71
73					–	–			–			–		–			–	73
79	–	–	–			–	–				–			–	–		–	79
83	–					–			–		–	–						83
89					–			–	–	–		–	–	–	–			89
97			–			–			–	–	–		–		–	–		97
101	–	–			–	–		–	–			–	–		–		–	101
103			–		–				–	–		–	–	–	–	–		103
107		–	–	–	–		–								–		–	107
109			–			–						–				–	–	109
113	–	–			–	–		–			–					–	–	113
127		–		–	–				–						–		–	127
131	–	–		–	–		–	–		–			–	–		–	–	131
137	–				–				–	–	–			–		–	–	137
139	–	–			–	–		–	–	–		–				–		139
149	–		–	–	–			–		–			–	–	–			149
151	–	–	–	–				–		–				–	–	–	–	151
157			–	–		–		–			–	–	–	–		–	–	157
163	–			–		–			–					–		–	–	163
167	–			–			–	–		–	–		–					–	167
173			–						–			–		–	–			173
179						–		–	–	–	–	–			–	–	–	179
181	–			–	–		–		–	–					–			181
191				–		–	–		–	–		–		–			–	191
193	–		–	–	–	–			–					–	–			193
197	–	–			–			–	–	–	–	–	–				–	197
199	–						–	–	–	–	–				–	–	–	199
211						–		–	–				–			–	–	211
223				–			–				–				–	–		223
227	–				–	–		–		–			–		–			227
	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	

	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	
3		–	–			–		–		–	–	–		–	–		3
5	–	–				–	–	–	–			–		–		–	5
7	–		–		–		–	–				–	–	–	–		7
11		–			–	–		–	–	–				–	–		11
13	–		–	–			–		–	–				–	–		13
17	–	–					–			–	–	–			–	–	17
19						–	–	–	–	–	–	–			–	–	19
23			–		–	–			–			–				–	23
29		–	–		–	–	–	–	–							–	29
31	–	–			–	–	–			–	–			–			31
37	–		–	–		–			–		–	–	–	–		–	37
41		–		–			–				–	–	–			–	41
43	–	–			–		–	–	–								43
47	–	–			–			–	–		–	–				–	47
53		–	–		–					–	–		–	–	–		53
59		–		–				–		–	–		–		–	–	59
61	–				–	–			–	–	–			–	–		61
67	–					–		–	–				–	–		–	67
71	–			–					–			–					71
73	–	–	–							–	–	–			–		73
79				–	–				–	–	–		–	–	–	–	79
83	–		–			–	–			–	–	–		–	–		83
89	–		–			–	–				–			–	–	–	89
97		–	–	–	–	–	–			–	–		–	–			97
101				–	–	–	–			–			–			–	101
103	–		–	–			–	–				–		–	–		103
107		–		–	–	–				–			–			–	107
109	–	–			–					–			–	–			109
113				–		–		–	–	–		–				–	113
127		–	–	–				–	–		–	–			–		127
131	–				–	–	–		–			–			–		131
137				–	–		–		–						–	–	137
139			–	–	–		–		–		–	–				–	139
149	–			–		–		–	–			–		–		–	149
151	–		–				–	–		–			–		–		151
157	–	–		–				–		–	–	–	–				157
163		–	–	–		–	–	–			–	–	–				163
167				–			–				–		–		–	–	167
173	–	–		–	–	–	–			–	–	–	–				173
179		–			–			–	–		–		–			–	179
181	–					–		–	–	–	–	–		–	–	–	181
191	–		–	–		–	–	–		–	–		–		–		191
193				–		–		–						–			193
197		–			–	–				–	–	–		–			197
199	–	–		–	–	–	–	–	–	–					–		199
211				–		–		–			–						211
223	–		–	–	–		–		–	–	–		–	–			223
227	–	–	–			–		–					–	–	–		227
	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	

	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	
229		–			–	–			–		–	–	–	–	–			229
233			–		–		–	–	–					–	–	–	–	233
239	–	–	–	–	–		–			–			–	–	–	–		239
241	–	–						–	–		–			–	–			241
251		–	–	–	–	–			–		–	–						251
257	–		–		–	–				–			–		–	–	–	257
263	–	–		–	–			–	–			–	–		–	–		263
269	–				–	–	–				–	–	–	–	–		–	269
271				–	–		–					–	–	–				271
277	–			–		–		–		–	–			–	–			277
281	–	–	–		–	–		–	–			–	–	–	–	–		281
283	–			–					–		–				–	–		283
293		–	–	–	–			–	–		–	–		–	–	–	–	293
307	–	–	–		–	–		–					–				–	307
311	–		–			–	–						–		–	–		311
313		–		–	–	–	–	–	–	–	–						–	313
317		–	–	–								–		–	–			317
331	–	–			–		–	–	–							–		331
337	–		–			–	–					–	–			–	–	337
347		–	–			–					–		–		–	–	–	347
349	–			–	–				–	–	–		–	–		–	–	349
353			–			–			–	–				–				353
359	–						–	–		–			–	–		–	–	359
367	–	–	–	–	–	–		–	–			–	–	–				367
373		–	–	–		–	–						–		–		–	373
379				–				–		–				–		–		379
383		–			–		–		–				–	–	–			383
389		–					–		–			–		–			–	389
397		–			–	–	–						–		–	–	–	397
401	–			–	–		–	–	–			–			–		–	401
409	–	–	–		–	–		–		–								409
419	–		–				–		–		–							419
421	–				–		–	–		–	–			–	–		–	421
431	–	–				–			–	–			–		–	–		431
433		–		–									–	–	–			433
439		–		–		–	–	–				–			–	–		439
443	–	–			–		–		–	–	–		–	–		–		443
449	–		–	–		–				–					–	–	–	449
457		–	–		–	–		–	–			–	–				–	457
461	–		–		–	–	–				–	–		–				461
463	–			–	–	–	–	–	–		–	–	–	–			–	463
467					–			–		–		–	–	–			–	467
479	–	–	–	–	–		–	–	–		–	–		–		–		479
487	–	–	–		–	–			–		–	–	–	–	–		–	487
491			–				–				–				–	–		491
499	–	–			–		–				–	–	–	–	–			499
503		–			–		–	–	–				–	–		–	–	503
	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	

	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	
229		–	–		–	–	–				–		–	–	–		229
233		–	–		–	–	–			–				–	–	–	233
239		–				–			–	–	–	–		–	–	–	239
241	–		–		–	–			–	–	–	–	–				241
251				–	–	–		–	–	–		–	–	–	–		251
257			–		–		–	–	–	–		–					257
263	–		–	–	–			–			–			–		–	263
269	–									–			–	–			269
271		–			–			–	–	–						–	271
277				–			–	–	–			–	–		–	–	277
281			–		–				–	–			–		–		281
283	–	–		–	–		–	–		–				–		–	283
293	–		–	–	–		–	–	–	–		–					293
307				–	–	–	–		–	–	–		–				307
311		–					–			–		–	–		–	–	311
313	–	–			–		–	–			–	–	–				313
317	–		–	–	–	–	–		–		–	–			–		317
331	–				–		–				–	–	–	–	–		331
337		–	–	–	–		–										337
347			–	–					–	–	–		–			–	347
349		–	–		–		–			–		–	–				349
353	–			–	–	–				–							353
359	–	–			–				–	–	–		–	–			359
367	–					–							–		–		367
373	–		–		–	–		–	–		–	–	–				373
379	–		–		–		–			–			–	–			379
383	–	–		–	–				–	–	–			–		–	383
389	–	–			–	–	–	–	–		–		–			–	389
397			–		–		–	–	–	–				–	–	–	397
401				–		–		–	–		–	–		–	–	–	401
409	–				–			–		–	–		–				409
419	–		–		–				–			–	–			–	419
421		–	–	–							–	–	–		–	–	421
431	–	–	–	–			–	–	–		–			–	–	–	431
433									–	–	–	–	–	–	–	–	433
439	–	–	–		–	–			–	–			–				439
443						–	–			–			–	–	–	–	443
449		–	–	–		–	–								–	–	449
457		–	–	–				–	–			–	–	–	–	–	457
461	–		–	–				–	–	–	–			–	–		461
463	–				–	–		–	–	–	–	–	–	–		–	463
467	–		–	–					–		–	–	–	–			467
479	–		–	–				–	–				–		–		479
487					–	–	–	–	–	–			–	–	–	–	487
491	–		–		–		–	–						–			491
499			–	–	–					–	–				–		499
503	–	–	–			–	–		–	–		–				–	503
	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	

	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	
3	–		–			–		–		–		–		–		–		3
5	–				–	–	–			–	–			–			–	5
7					–		–	–	–						–	–		7
11		–		–				–		–	–			–	–		–	11
13				–	–			–		–			–	–			–	13
17	–	–		–						–				–	–			17
19	–				–		–	–				–		–			–	19
23					–	–	–	–		–		–	–	–	–	–		23
29			–			–	–						–		–	–		29
31	–					–					–	–	–			–		31
37		–	–			–	–	–			–				–	–	–	37
41	–		–	–		–	–			–		–	–	–	–	–	–	41
43	–		–	–	–		–	–	–			–	–			–	–	43
47	–	–				–		–	–			–			–			47
53						–		–			–		–	–	–	–		53
59			–						–	–		–				–		59
61		–		–	–				–	–	–	–	–	–	–		–	61
67		–		–			–	–	–	–	–	–		–	–	–	–	67
71			–	–		–	–			–	–	–	–			–	–	71
73			–	–	–	–	–		–		–	–	–			–		73
79		–	–		–	–	–				–		–		–	–		79
83		–	–			–					–	–	–	–	–		–	83
89	–			–	–	–	–	–									–	89
97		–	–		–	–		–		–			–			–	–	97
101			–		–		–		–	–	–	–	–					101
103		–	–	–			–				–	–	–					103
107				–		–					–		–	–			–	107
109				–	–	–		–	–	–			–		–	–	–	109
113	–	–	–		–		–	–	–			–			–			113
127		–	–	–	–	–		–								–		127
131	–		–	–		–	–		–	–	–				–	–		131
137		–		–		–	–	–		–	–			–			–	137
139		–				–					–			–	–		–	139
149	–	–	–		–		–		–				–	–	–	–		149
151		–	–	–				–	–	–	–	–						151
157	–	–		–			–		–	–		–						157
163		–	–	–			–			–	–	–				–		163
167					–						–	–	–	–	–	–		167
173	–	–	–		–	–			–	–				–			–	173
179		–		–	–	–		–					–		–	–		179
181	–	–		–		–		–				–	–	–	–			181
191	–	–	–		–			–		–	–						–	191
193	–	–		–			–		–		–	–	–				–	193
197	–	–	–	–		–	–		–	–	–	–					–	197
199	–			–	–		–		–	–	–	–	–	–		–		199
211	–		–		–	–	–		–	–		–	–		–		–	211
223	–			–			–						–				–	223
227		–		–								–	–		–	–		227
	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	

	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	
3	–		–		–		–				–				–	–	3
5				–	–	–		–				–			–		5
7	–		–	–	–				–	–	–		–		–		7
11	–		–	–		–			–			–	–	–	–		11
13	–	–	–	–	–		–			–		–			–	–	13
17	–				–		–			–	–	–	–				17
19	–				–	–	–		–		–					–	19
23	–	–				–			–		–				–	–	23
29	–				–	–	–	–		–			–		–		29
31		–	–		–		–					–	–			–	31
37		–				–	–	–		–		–		–			37
41			–	–				–	–	–				–			41
43	–		–		–			–	–		–	–	–				43
47	–		–	–		–		–	–		–		–		–		47
53			–	–		–	–	–	–	–	–	–		–	–	–	53
59	–		–	–					–	–		–				–	59
61				–	–	–	–				–	–	–		–		61
67		–	–	–					–	–	–	–	–			–	67
71						–		–	–	–		–	–	–		–	71
73				–			–	–	–	–	–					–	73
79		–	–	–	–			–		–	–	–				–	79
83			–	–		–		–		–			–	–	–	–	83
89			–	–		–	–		–			–	–	–		–	89
97							–				–	–				–	97
101		–				–					–		–		–	–	101
103	–	–	–			–		–		–			–	–	–		103
107	–						–	–			–		–			–	107
109		–	–						–	–			–			–	109
113				–	–	–				–	–				–		113
127	–		–	–	–			–		–		–	–	–			127
131		–	–	–		–	–			–			–		–	–	131
137	–	–				–	–	–			–		–		–	–	137
139	–			–				–	–			–	–			–	139
149		–		–	–	–		–	–		–					–	149
151	–		–	–			–			–					–	–	151
157			–	–		–		–		–	–		–		–		157
163				–	–			–	–		–	–					163
167	–		–	–	–	–			–		–					–	167
173		–			–	–				–		–		–	–	–	173
179		–	–	–			–	–	–			–	–	–			179
181					–			–	–	–	–						181
191				–				–			–	–			–		191
193				–	–	–	–	–	–	–	–	–	–	–		–	193
197															–		197
199		–	–	–	–			–	–	–		–		–		–	199
211		–					–		–	–	–			–			211
223		–	–	–		–		–	–							–	223
227				–	–	–	–	–			–	–	–	–		–	227
	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	

	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	
229	–		–				–							–	–			229
233		–		–	–	–		–	–							–	–	233
239				–					–		–	–		–		–		239
241		–	–				–	–		–	–		–			–	–	241
251	–	–				–	–		–		–	–		–	–	–		251
257	–	–	–	–			–	–		–	–			–	–			257
263	–			–		–	–	–			–	–	–	–	–	–	–	263
269	–	–	–			–	–	–	–					–	–	–		269
271			–				–	–	–	–		–	–		–	–	–	271
277	–			–	–		–		–			–		–				277
281		–	–		–	–		–	–	–	–	–	–	–	–	–		281
283	–	–						–	–	–		–		–		–		283
293				–		–	–	–			–	–	–		–			293
307	–			–				–		–	–							307
311	–			–	–	–		–					–	–				311
313	–	–	–	–		–		–			–				–		–	313
317	–				–				–		–		–	–			–	317
331		–	–			–		–	–	–	–	–	–	–		–	–	331
337	–		–	–		–	–	–		–	–	–			–			337
347	–		–		–	–	–	–	–			–			–	–		347
349		–			–		–	–				–						349
353			–	–					–					–	–	–		353
359	–	–	–	–	–					–	–	–		–				359
367			–	–			–	–		–	–				–			367
373		–	–	–	–		–		–	–	–	–	–		–			373
379				–	–						–	–		–	–	–		379
383	–	–	–	–	–		–	–		–	–	–		–				383
389	–	–	–	–				–	–				–	–	–	–		389
397	–			–			–	–	–	–				–	–	–	–	397
401		–		–	–	–			–			–	–	–				401
409	–	–			–		–	–	–					–	–			409
419			–				–		–		–	–		–	–	–	–	419
421			–	–	–	–	–		–		–	–	–	–	–	–		421
431	–	–		–		–		–	–						–	–	–	431
433			–						–	–	–	–	–		–	–		433
439		–				–	–				–		–		–			439
443			–				–	–		–		–	–		–		–	443
449	–	–	–	–	–	–	–				–	–	–	–	–			449
457		–	–						–		–		–	–	–			457
461	–			–	–	–			–	–					–	–	–	461
463	–		–	–	–		–		–		–				–		–	463
467					–			–	–	–			–			–		467
479		–	–		–					–	–		–		–			479
487	–	–			–	–	–	–	–	–			–				–	487
491		–			–	–		–							–	–		491
499	–			–				–	–				–		–		–	499
503				–		–			–		–	–	–				–	503
	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	

	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	
229	–		–	–	–			–		–	–	–	–		–	–	229
233	–		–		–			–	–					–			233
239	–	–			–		–				–	–		–			239
241	–	–		–	–		–				–				–		241
251			–						–		–	–					251
257		–	–	–		–			–		–	–				–	257
263		–		–		–	–				–					–	263
269		–	–									–	–	–		–	269
271	–	–		–	–		–	–	–	–	–	–	–	–	–		271
277	–		–		–		–		–	–	–		–		–		277
281	–		–	–		–		–			–	–		–			281
283	–	–		–	–			–						–			283
293	–				–		–		–		–			–			293
307	–	–	–		–		–		–		–			–	–	–	307
311		–		–			–	–	–	–				–		–	311
313		–	–				–	–	–			–	–	–	–	–	313
317		–	–	–				–	–		–		–		–		317
331		–	–					–		–					–	–	331
337	–		–	–		–	–		–					–		–	337
347			–		–	–	–			–		–		–	–		347
349	–					–	–	–	–	–	–	–	–	–	–		349
353	–	–	–		–	–	–				–	–	–	–	–		353
359	–	–		–			–		–	–		–			–		359
367	–		–			–		–	–			–					367
373	–			–							–	–				–	373
379	–	–	–			–	–		–	–		–	–	–		–	379
383		–			–		–	–			–	–		–	–		383
389			–	–	–		–		–	–		–		–	–		389
397		–						–			–						397
401	–			–					–	–		–	–	–		–	401
409		–	–		–			–		–		–	–			–	409
419	–	–	–	–	–	–				–	–		–	–			419
421		–			–			–	–		–		–		–	–	421
431		–	–	–	–		–			–		–	–	–		–	431
433	–		–		–			–	–			–	–	–			433
439	–	–	–			–		–	–			–	–		–		439
443		–		–			–	–	–	–	–				–	–	443
449		–	–				–		–	–					–	–	449
457		–	–	–				–				–	–				457
461	–							–	–		–	–		–			461
463			–		–			–	–					–	–		463
467					–	–	–	–	–				–	–		–	467
479			–	–	–	–		–			–			–	–		479
487		–		–		–	–		–		–	–		–			487
491		–			–	–			–	–				–	–	–	491
499	–			–	–		–					–		–	–		499
503	–	–			–			–		–		–	–		–		503
	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	

T A F E L

ZUR UMWANDLUNG

GEWÖHNLICHER BRÜCHE MIT NENNERN AUS DEM ERSTEN TAUSEND

IN DEZIMALBRÜCHE.

3 (1)..6; (0)..3

7 (0)..428571

9 (1)..2; (2)..4; (3)..8; (4)..7; (5)..5; (0)..1

11 (1)..81; (2)..63; (3)..27; (4)..54; (0)..90

13 (1)..615384; (0)..769230

17 (0)..5882352941 176470

19 (0)..5263157894 73684210

23 (0)..4347826086 9565217391 30

27 (1)..740; (2)..481; (3)..962; (4)..925; (5)..851; (0)..370

29 (0)..3448275862 0689655172 41379310

31 (1)..4838709677 41935; (0)..3225806451 61290

37 (1)..351; (2)..756; (3)..783; (4)..918; (5)..594; (6)..972; (7)..864; (8)..324; (9)..621; (10)..108; (11)..540; (0)..270

41 (1)..46341; (2)..78048; (3)..68292; (4)..09756; (5)..58536; (6)..51219; (7)..07317; (0)..24390

43 (1)..5116279069 7674418604 6; (0)..2325581395 3488372093 0

47 (1)..2127659574 4680851063 8297872340 4255319148 936170

49 (0)..2040816326 5306122448 9795918367 3469387755 10

53 (1)..9056603773 584; (2)..5471698113 207; (3)..2264150943 396; (0)..1886792452 830

59 (0)..1694915254 2472881355 9322033898 3050847457 6271186440 67796610

61 (0)..1639344262 2950819672 1311475409 8360655737 7049180327 8688524590

67 (1)..7910447761 1940298507 4626865671 641; (0)..1492537313 4328358208 9552238805 970

71 (1)..7323943661 9718309859 1549295774 64788; (0)..1408450704 2253521126 7605633802 81690

73 (1)..68493150; (2)..42465753; (3)..12328767; (4)..61643835; (5)..08219178; (6)..41095890 (7)..05479452; (8)..27397260; (0)..13698630

79 (1)..6708860759 493; (2)..4556962025 316; (3)..2151898734 177; (4)..2405063291 139; (5)..9746835443 037; (0)..1265822784 810

81 (1)..358024691; (2)..938271604; (3)..320987654; (4)..530864197; (5)..839506172; (0)..123456790

83 (1)..0240963855 4216867469 8795180722 8915662650 6; (0)..1204819277 1084337349 3975903614 4578313253 0

89 (1)..3707865168 5393258426 9662921348 3146067415 7303;
(0)..1123595505 6179775280 8988764044 9438202247 1910

97 (0)..1030927835 0515463917 5257731958 7628865979 3814432989
6907216494 8453608247 4226804123 7113402061 855670

101 (1)..1980; (2)..3960; (3)..7920; (4)..5841; (5)..1683; (6)..3366;
(7)..6732; (8)..3465; (9)..6930; (10)..3861; (11)..7722;
(12)..5445; (13)..0891; (14)..1782; (15)..3564; (16)..7128;
(17)..4257; (18)..8514; (19)..7029; (20)..4059; (21)..8118;
(22)..6237; (23)..2475; (24)..4950; (0)..0990

103 (1)..5825242718 4466019417 4757281553 3980; (2)..4951456310
6796116504 8543689320 3883 (0)..0970873786 4077669902
9126213592 2330

107 (1)..8878504672 8971962616 8224299065 4205607476 6355140186 915
(0)..0934579439 2523364485 9813084112 1495327102 8037383177 570

109 (0)..0917431192 6605504587 1559633027 5229357798 1651376146
7889908256 8807339449 5412844036 6972477064 2201834862 38532110

113 (0)..0884955752 2123893805 3097345132 7433628318 5840707964
6017699115 0442477876 1061946902 6548672566 3716814159
2920353982 30

121 (1)..8925619834 7107438016 52; (2)..2396694214 8760330578 51;
(3)..3884297520 6611570247 93; (4)..5950413223 1404958677 68;
(0)..0826446280 9917355371 90;

127 (1)..3464566929 1338582677 1653543307 0866141732 28;
(2)..7244094488 1889763779 5275590551 1811023622 04;
(0)..0787401574 8031496062 9921259842 5196850393 70

131 (0)..0763358778 6259541984 7328244274 8091603053 4351145038
1679389312 9770992366 4122137404 5801526717 5572519083
9694656488 5496183206 1068702290

137 (1)..87591240; (2)..51094890; (3)..13138686; (4)..57664233;
(5)..91970802; (6)..03649635; (7)..43795620; (8)..25547445;
(9)..06569343; (10)..78832116; (11)..45985401; (12)..51824817;
(13)..21897810; (14)..62773722; (15)..53284671; (16)..39416058;
(0)..07299270

139 (1)..6187050359 7122302158 2733812949 6402877697 841726;
(2)..9208633093 5251798561 1510791366 9064748201 438848;
(0)..0719424460 4316546762 5899280575 5395683453 237410

149 (0)..0671140939 5973154362 4161073825 5033557046 9798657718
1208053691 2751677852 3489932885 9060402684 5637583892
6174496644 2953020134 2281879194 6308724832 21476510

151 (1) . . 5496688741 7218543046 3576158940 3973509933 7748344370
8609271523 1788079470 19867 (0) . . 0662251655 6291390728
4768211920 5298013245 0331125827 8145695364 2384105960 26490

157 (1) . . 1464968152 8662420382 1656050955 4140127388 5350318471
3375796178 3439490445 85987261 (0) . . 0636942675 1592356687
8980891719 7452229299 3630573248 4076433121 0191082802 54777070

163 (1) . . 2944785276 0736196319 0184049079 7546012269 9386503067
4846625766 8711656441 7177914110 4 (0) . . 0613496932 5153374233
1288343558 2822085889 5705521472 3926380368 0981595092
0245398773 0

167 (0) . . 0598802395 2095808383 2335329341 3173652694 6107784431
1377245508 9820359281 4371257485 0299401197 6047904191
6167664670 6586826347 3053892215 5688622754 4910179640
7185628742 514970

169 (1) . . 1065088757 3964497041 4201183431 9526627218 9349112426
0355029585 7988165680 47337278 (0) . . 0591715976 3313609467
4556213017 7514792899 4082840236 6863905325 4437869822 48520710

173 (1) . . 7398843930 6358381502 8901734104 0462427745 664;
(2) . . 6705202312 1387283236 9942196531 7919075144 508;
(3) . . 9826589595 3757225433 5260115606 9364161849 710;
(0) . . 0578034682 0809248554 9132947976 8786127167 630

179 (0) . . 0558659217 8770949720 6703910614 5251396648 0446927374
3016759776 5363128491 6201117318 4357541899 4413407821
2290502793 2960893854 7486033519 5530726256 9832402234
6368715083 7988826815 64245810

181 (0) . . 0552486187 8453038674 0331491712 7071823204 4198895027
6243093922 6519337016 5745856353 5911602209 9447513812
1546961325 9668508287 2928176795 5801104972 3756906077
3480662983 4254143646 4088397790

191 (1) . . 2198952879 5811518324 6073298429 3193717277 4869109947
6439790575 9162303664 9214659685 8638743455 49738;
(0) . . 0523560209 4240837696 3350785340 3141361256 5445026178
0104712041 8848167539 2670157068 0628272251 30890

193 (0) . . 0518134715 0259067357 5129533678 7564766839 3782383419
6891191709 8445595854 9222797927 4611398963 7305699481
8652849740 9326424870 4663212435 2331606217 6165803108
8082901554 4041450777 2020725388 6010362694 30

197 (1) . . 7055837563 4517766497 4619289340 1015228426 3959390862
9441624365 4822335025 3807106598 9847715736 04060913;
(0) . . 0507614213 1979695431 4720812182 7411167512 6903553299
4923857868 0203045685 2791878172 5888324873 09644670

199 (1) . . 3819095477 3869346733 6683417085 4271356783 9195979899 4974874371 8592964824 1206030150 7537688442 211055276; (0) . . 0502512562 8140703517 5879396984 9246231155 7788944723 6180904522 6130653266 3316582914 5728643216 080402010

211 (1) . . 3317535545 0236966824 6445497630; (2) . . 3222748815 1658767772 5118483412; (3) . . 2559241706 1611374407 5829383886; (4) . . 7914691943 1279620853 0805687203; (5) . . 5402843601 8957345971 5639810426; (6) . . 7819905213 2701421800 9478672985; (0) . . 0473933649 2890995260 6635071090

223 (0) . . 0448430493 2735426008 9686098654 7085201793 7219730941 7040358744 3946188340 8071748878 9237668161 4349775784 7533632286 9955156950 6726457399 1031390134 5291479820 6278026905 8295964125 5605381165 9192825112 1076233183 8565022421 5246636771 30

227 (1) . . 1806167400 8810572687 2246696035 2422907488 9867841409 6916299559 4713656387 6651982378 8546255506 6079295154 1850220264 317; (0) . . 0440528634 3612334801 7621145374 4493392070 4845814977 9735682819 3832599118 9427312775 3303964757 7092511013 2158590308 370

229 (0) . . 0436681222 7074235807 8602620087 3362445414 8471615720 5240174672 4890829694 3231441048 0349344978 1659388646 2882096069 8689956331 8777292576 4192139737 9912663755 4585152838 4279475982 5327510917 0305676855 8951965065 5021834061 1353711790 39301310

233 (0) . . 0429184549 3562231759 6566523605 1502145922 7467811158 7982832618 0257510729 6137339055 7959914163 0901287553 6480686695 2789799570 8154506437 7682403433 4763948497 8540772532 1888412017 1673819742 4892703862 6609442060 0858369098 7124463519 3133047210 30

239 (1) . . 4644351; (2) . . 2552301; (3) . . 9330543; (4) . . 6569037; (5) . . 9916317; (6) . . 7071129; (7) . . 7489539; (8) . . 2133891; (9) . . 4686192; (10) . . 4016736; (11) . . 0585774; (12) . . 0502092; (13) . . 7573221; (14) . . 5062761; (15) . . 7196652; (16) . . 1882845; (17) . . 5899581; (18) . . 6485355; (19) . . 6987447; (20) . . 4560669; (21) . . 9623430; (22) . . 6820083; (23) . . 8702928; (24) . . 4602510; (25) . . 1087866; (26) . . 8075313; (27) . . 2635983; (28) . . 2259414; (29) . . 9079497; (30) . . 7782426; (31) . . 2384937; (32) . . 3472803; (33) . . 1548117; (0) . . 0418410

241 (1) . . 5809128630 7053941908 7136929460; (2) . . 1327800829 8755186721 9917012448; (3) . . 8589211618 2572614107 8838174273; (4) . . 0248962655 6016597510 3734439834; (5) . . 3485477178 4232365145 2282157676; (6) . . 8796680497 9253112033 1950207468; (7) . . 3153526970 9543568464 7302904564; (0) . . 0414937759 3360995850 6224066390

243 (1) . . 6748971193 4156378600 8230452; (3) . . 8683127572 0164609053 4979423; (3) . . 4403292181 0699588477 3662551; (4) . . 6213991769 5473251028 8065843; (5) . . 3909465020 5761316872 4279835; (0) . . 0411522633 7448559670 7818930

251 (1) . . 4223107569 7211155378 4860557768 9243027888 4462151394; (2) . . 8764940239 0438247011 9521912350 5976095617 5298804780; (3) . . 2908366533 8645418326 6932270916 3346613545 8167330677; (4) . . 2828685258 9641434262 9482071713 1474103585 6573705179; (0) . . 0398406374 5019920318 7250996015 9362549800 7968127490

257 (0) . . 0389105058 3657587548 6381322957 1984435797 6653696498 0544747081 7120622568 0933852140 0778210116 7315175097 2762645914 3968871595 3307392996 1089494163 4241245136 1867704280 1556420233 4630350194 5525291828 7937743190 6614785992 2178988326 8482490272 3735408560 3112840466 926070

263 (0) . . 0380228136 8821292775 6653992395 4372623574 1444866920 1520912547 5285171102 6615969581 7490494296 5779467680 6083650190 1140684410 6463878326 9961977186 3117870722 4334600760 4562737642 5855513307 9847908745 2471482889 7338403041 8250950570 3422053231 9391634980 9885931558 9353612167 30

269 (0) . . 0371747211 8959107806 6914498141 2639405204 4609665427 5092936802 9739776951 6728624535 3159851301 1152416356 8773234200 7434944237 9182156133 8289962825 2788104089 2193308550 1858736059 4795539033 4572490706 3197026022 3048327137 5464684014 8698884758 3643122676 5799256505 5762081784 38661710

271 (1) . . 22140; (2) . . 32841; (3) . . 97047; (4) . . 82287; (5) . . 93726;
(6) . . 62361; (7) . . 74169; (8) . . 45018; (9) . . 70110; (10) . . 20664;
(11) . . 23985; (12) . . 43911; (13) . . 63468; (14) . . 80811; (15) . . 84870;
(16) . . 09225; (17) . . 55350; (18) . . 32103; (19) . . 92619; (20) . . 55719;
(21) . . 34317; (22) . . 05904; (23) . . 35424; (24) . . 12546; (25) . . 75276;
(26) . . 51660; (27) . . 09963; (28) . . 59778; (29) . . 58671; (30) . . 52029;
(31) . . 12177; (32) . . 73062; (33) . . 38376; (34) . . 30258; (35) . . 81549;
(36) . . 89298; (37) . . 35793; (38) . . 14760; (39) . . 88560; (40) . . 31365;
(41) . . 88191; (42) . . 29151; (43) . . 74907; (44) . . 49446; (45) . . 96678;
(46) . . 80073; (47) . . 80442; (48) . . 82656; (49) . . 95940; (50) . . 75645;
(51) . . 53874; (52) . . 23447; (53) . . 39483; (0) . . 03690

277 (1) . . 8880866425 9927797833 9350180505 4151624548 7364620938
6281588447 653429602 (2) . . 0469314079 4223826714 8014440433
2129963898 9169675090 2527075812 274368231 (3) . . 7545126353
7906137184 1155234657 0397111913 3574007220 2166064981
949458483 (0) . . 0361010830 3249097472 9241877256 3176895306
8592057761 7328519855 595667870

281 (1) . . 9217081850 5338078291 81494661; (2) . . 7722419928 8256227758
00711743; (3) . . 7010676156 5836298932 38434163; (4) . . 8576512455
5160142348 75444839; (5) . . 3131672597 8647686832 74021352;
(6) . . 9110320284 6975088967 97153024; (7) . . 1957295373 6654804270
46263345; (8) . . 5693950177 9359430604 98220640; (9) . . 7473309608
5409252669 03914590; (0) . . 0355871886 1209964412 81138790

283 (1) . . 1519434628 9752650176 6784452296 8197879858 6572438162
5441696113 0742049469 9646643109 5406360424 0282685512
3674911660 7773851590 1060070671 3780918727 9 (0) . . 0353356890
4593639575 9717314487 6325088339 2226148409 8939929328
6219081272 0848056537 1024734982 3321554770 3180212014
1342756183 7455830388 6925795053 0

289 (0) . . 0346020761 2456747404 8442906574 3944636678 2006920415
2249134948 0968858131 4878892733 5640138408 3044982698
9619377162 6297577854 6712802768 1660899653 9792387543
2525951557 0934256055 3633217993 0795847750 8650519031
1418685121 1072664359 8615916955 0173010380 6228373702
4221453287 1972318339 10

293 (1) . . 0375426621 1604095563 1399317406 1433447098 9761092150
1706484641 6382252559 7269624573 3788395904 4368600682
5938566552 9010238907 8498293515 3583617747 440273
(0) . . 0341296928 3276450511 9453924914 6757679180 8873720136
5187713310 5802047781 5699658703 0716723549 4880546075
0853242320 8191126279 8634812286 6894197952 218430

307 (1) . . 4951140065 1465798045 6026058631 9218241042 3452768729 6416938110 7491856677 5244299674 2671009771 9869706840 3908794788 2736156351 7915309446 2540716612 3778501628 664 (0) . . 0325732899 0228013029 3159609120 5211726384 3648208469 0553745928 3387622149 8371335504 8859934853 4201954397 3941368078 1758957654 7231270358 3061889250 8143322475 570

311 (1) . . 2958199356 9131832797 4276527331 1897106109 3247588424 4372990353 6977491961 4147909967 8456591639 8713826366 5594855305 4662379421 2218649517 6848874598 0707395498 39228 (0) . . 0321543408 3601286173 6334405144 6945337620 5787781350 4823151125 4019292604 5016077170 4180064308 6816720257 2347266881 0289389067 5241157556 2700964630 2250803858 52090

313 (0) . . 0319488817 8913738019 1693290734 8242811501 5974440894 5686900958 4664536741 2140575079 8722044728 4345047923 3226837060 7028753993 6102236421 7252396166 1341853035 1437699680 5111821086 2619808306 7092651757 1884984025 5591054313 0990415335 4632587859 4249201277 9552715654 9520766773 1629392971 2460063897 7635782747 6038338658 1469648562 30

317 (1) . . 2397476340 6940063091 4826498422 7129337539 4321766561 5141955835 9621451104 100946372 (2) . . 0220820189 2744479495 2681388012 6182965299 6845425867 5078864353 3123028391 167192429 (3) . . 5678233438 4858044164 0378548895 8990536277 6025236593 0599369085 1735015772 870662460 (0) . . 0315457413 2492113564 6687697160 8832807570 9779179810 7255520504 7318611987 381703470

331 (1) . . 1178247734 1389728096 6767371601 2084592145 0151057401 8126888217 5226586102 7190332326 2839879154 0785498489 4259818731 (2) . . 3595166163 1419939577 0392749244 7129909365 5589123867 0694864048 3383685800 6042296072 5075528700 9063444108 7613293051 (0) . . 0302114803 6253776435 0453172205 4380664652 5679758308 1570996978 8519637462 2356495468 2779466193 3534743202 4169184290

337 (0) . . 0296735905 0445103857 5667655786 3501483679 5252225519 2878338278 9317507418 3976261127 5964391691 3946587537 0919881305 6379821958 4569732937 6854599406 5281899109 7922848664 6884272997 0326409495 5489614243 3234421364 9851632047 4777448071 2166172106 8249258160 2373887240 3560830860 5341246290 8011869436 2017804154 3026706231 4540059347 1810089020 7715133531 157270

343. (0) . . 0291545189 5043731778 4256559766 7638483965 0145772594 7521865889 2128279883 3819241982 5072886297 3760932944 6064139941 6909620991 2536443148 6880466472 3032069970 8454810495 6268221574 3440233236 1516034985 4227405247 8134110787 1720116618 0758017492 7113702623 9067055393 5860058309 0379008746 3556851311 9533527696 7930

347 (1) . . 6023054755 0432276657 0605187319 8847262247 8386167146 9740634005 7636887608 0691642651 2968299711 8155619596 5417867435 1585014409 2219020172 9106628242 0749279538 9048991354 4668587896 253 (0) . . 0288184438 0403458213 2564841498 5590778097 9827089337 1757925072 0461095100 8645533141 2103746397 6945244956 7723342939 4812680115 2737752161 3832853025 9365994236 3112391930 8357348703 170

.349 (1) . . 3037249283 6676217765 0429799426 9340974212 0343839541 5472779369 6275071633 2378223495 7020057306 5902578796 5616045845 272206 (2) . . 8194842406 8767908309 4555873925 5014326647 5644699140 4011461318 0515759312 3209169054 4412607449 8567335243 5530085959 885386 (0) . . 0286532951 2893982808 0229226361 0315186246 4183381088 8252148997 1346704871 0601719197 7077363896 8481375358 1661891117 478510

353 (1) . . 7932011331 4447592067 9886685552 40; (2) . . 2096317280 4532577903 6827195467 42; (3) . . 8696883852 6912181303 1161473087 81; (4) . . 3512747875 3541076487 2521246458 92; (5) . . 8356940509 9150141643 0594900849 85; (6) . . 3994334277 6203966005 6657223796 03; (7) . . 1841359773 3711048158 6402266288 95; (8) . . 1558073654 3909348441 9263456090 65; (9) . . 3626062322 9461756373 9376770538 24; (10) . . 1529745042 4929178470 2549575070 82; (0) . . 0283286118 9801699716 7138810198 30;

359 (1) . . 3286908077 9944289693 5933147632 3119777158 7743732590 5292479108 6350974930 3621169916 4345403899 7214484679 6657381615 5988857938 7186629526 4623955431 7548746518 1058485821 7270194986 072423398 (0) . . 0278551532 0334261838 4401114206 1281337047 3537604456 8245125348 1894150417 8272980501 3927576601 6713091922 0055710306 4066852367 6880222841 2256267409 4707520891 3649025069 6378830083 565459610

361 (0)..0277008310 2493074792 2437673130 1939058171 7451523545
7063711911 3573407202 2160664819 9445983379 5013850415
5124653739 6121883656 5096952908 5872576177 2853185595
5678670360 1108033240 9972299168 9750692520 7756232686
9806094182 8254847645 4293628808 8642659279 7783933518
0055401662 0498614958 4487534626 0387811634 3490304709
1412742382 2714681440 4432132963 9889196675 90

367 (0)..0272479564 0326975476 8392370572 2070844686 6485013623
9782016348 7738419618 5286103542 2343324250 6811989100
8174386920 9809264305 1771117166 2125340599 4550408719
3460490463 2152588555 8583106267 0299727520 4359673024
5231607629 4277929155 3133514986 3760217983 6512261580
3814713896 4577656675 7493188010 8991825613 0790190735
6948228882 8337874659 4005449591 2806539509 5367847411
4441416893 732970

373 (1)..1983914209 1152815013 4048257372 6541554959 7855227882
0375335120 6434316353 8873994638 0697050938 3378016085
7908847184 9865951742 6273458445 0402144772 1179624664
8793565683 6461126005 3619302949 061662 (0)..0268096514
7453083109 9195710455 7640750670 2412868632 7077747989
2761394101 8766756032 1715817694 3699731903 4852546916
8900804289 5442359249 3297587131 3672922252 0107238605
8981233243 9678284182 305630

379 (0)..0263852242 7440633245 3825857519 7889182058 0474934036
9393139841 6886543535 6200527704 4854881266 4907651715
0395778364 1160949868 0738786279 6833773087 0712401055
4089709762 5329815303 4300791556 7282321899 7361477572
5593667546 1741424802 1108179419 5250659630 6068601583
1134564643 7794722955 1451187335 0923482849 6042216358
8390501319 2612137203 1662269129 2875989445 9102902374
6701846965 6992084432 71767810

383 (0)..0261096605 7441253263 7075718015 6657963446 4751958224
5430809399 4778067885 1174934725 8485639686 6840731070
4960835509 1383812010 4438642297 6501305483 0287206266
3185378590 0783289817 2323759791 1227154046 9973890339
4255874673 6292428198 4334203655 3524804177 5456919060
0522193211 4882506527 4151436031 3315926892 9503916449
0861618798 9556135770 2349869451 6971279373 3681462140
9921671018 2767624020 8877284595 30

389 (0) . . 0257069408 7403598971 7223650385 6041131105 3984575835
4755784061 6966580976 8637532133 6760925449 8714652956
2982005141 3881748071 9794344473 0077120822 6221079691
5167095115 6812339331 6195372750 6426735218 5089974293
0591259640 1028277634 9614395886 8894601542 4164524421
5938303341 9023136246 7866323907 4550128534 7043701799
4858611825 1928020565 5526992287 9177377892 0308483290
4884318766 0668380462 7249357326 47814910

397 (1) . . 3501259445 8438287153 6523929471 0327455919 3954659949
6221662468 5138539042 8211586901 7632241813 602015113;
(2) . . 5667506297 2292191435 7682619647 3551637279 5969773299
7481108312 3425692695 2141057934 5088161209 068010075;
(3) . . 3778337531 4861460957 1788413098 2367758186 3979848866
4987405541 5617128463 4760705289 6725440806 045340050;
(0) . . 0251889168 7657430730 4785894206 5491183879 0931989924
4332493702 7707808564 2317380352 6448362720 303022670

401 (1) . . 7381546134 6633416458 8528678304 2394014962 5935162094
7630922693 2668329177 0573566084 7880299251 8703241895
2618453865 3366583541 1471321695 7605985037 4064837905
2369077306 7331670822 9426433915 2119700748 1296758104
(0) . . 0249376558 6034912718 2044887780 5486284289 2768079800
4987531172 0698254364 0897755610 9725685785 5361596009
9750623441 3965087281 7955112219 4513715710 7231920199
5012468827 9301745635 9102244389 0274314214 4638403990

409 (1) . . 2542787286 0635696821 5158924205 3789731051 3447432762
8361858190 7090464547 6772616136 9193154034 2298288508
5574572127 1393643031 7848410757 9462102689 4865525672
3716381418 0929095354 5232273838 6308068459 6577017114 9144
(0) . . 0244498777 5061124694 3765281173 5941320293 3985330073
3496332518 3374083129 5843520782 3960880195 5990220048
8997555012 2249388753 0562347188 2640586797 0660146699
2665036674 8166259168 7041564792 1760391198 0440097799 5110

419 (0) . . 0238663484 4868735083 5322195704 0572792362 7684964200
4773269689 7374701670 6443914081 1455847255 3699284009
5465393794 7494033412 8878281622 9116945107 3985680190
9307875894 9880668257 7565632458 2338902147 9713603818
6157517899 7613365155 1312649164 6778042959 4272076372
3150357995 2267303102 6252983293 5560859188 5441527446
3007159904 5346062052 5059665871 1217183770 8830548926
0143198090 6921241050 1183317422 4343675417 6610978520
2863961813 84248210

421 (1)..2826603325 4156769596 1995249406 1757719714 .9643705463 1828978622 3277909738 7173396674 5843230403 8004750593 8242280285 0356294536 8171021377 6722090261 (2)..2636579572 4465558194 7743467933 4916864608 0760095011 8764845605 7007125890 7363420427 5534441805 2256532066 5083135391 9239904988 1235154394 2992874109 (0)..0237529691 2114014251 7814726840 8551068883 6104513064 1330166270 7838479809 9762470308 7885985748 2185273159 1448931116 3895486935 8669833729 2161520190

431 (1)..4872389791 1832946635 7308584686 7749419953 5962877030 1624129930 3944315545 2436194895 5916473317 8654292343 3874709976 7981438515 0812064965 1972197772 6218097447 7958236658 9327146171 6937354988 3990719257 5406032482 5986078886 31090 (0)..0232018561 4849187935 0348027842 2273781902 5522041763 3410672853 8283062645 0116009280 7424593967 5174013921 1136890951 2761020881 6705336426 9141531322 5058004640 3712296983 7587006960 5568445475 6380510440 8352668213 4570765661 25290

433 (0)..0230946882 2170900692 8406466512 7020785219 3995381062 3556581986 1431870669 7459584295 6120092378 7528868360 2771362586 6050808314 0877598152 4249422632 7944572748 2678983833 7182448036 9515011547 3441108545 0346420323 3256351039 2609699769 0531177829 0993071593 5334872979 2147806004 6189376443 4180138568 1293302540 4157043879 9076212471 1316397228 6374133949 1916859122 4018475750 5773672055 4272517321 0161662817 5519630484 9884526558 8914549653 5796766743 6489607390 30

439 (1)..4920273348 5193621867 8815489749 4305239179 9544419134 3963553530 7517084282 4601366742 5968109339 4077448747 1526195899 7722095671 9817767653 7585421412 3006833712 9840546697 0387243735 7630979498 8610478359 9088838268 7927107061 503416856 (0)..0227790432 8018223234 6241457858 7699316628 7015945330 2961275626 4236902050 1138952164 0091116173 1207289293 8496583143 5079726651 4806378132 1184510250 5694760820 0455580865 6036446469 2482915717 5398633257 4031890660 5922551252 847380410

443 (1) . . 4176072234 7629796839 7291196388 2618510158 0135440180 5869574492 0993227990 9706546275 3950338600 4514672686 2302483069 9774266365 6884875846 5011286681 7155756207 6749435665 9142212189 6162528216 7042889390 5191873589 1647855530 4740406320 5 (0) . . 0225733634 3115124153 4988713318 2844243792 3250564334 0857787810 3837471783 2957110609 4808126410 8352144469 5259593679 4582392776 5237020316 0270880361 1738148984 1986455981 9413092550 7900677200 9029345372 4604966139 9548532731 3769751693 0

449 (1) . . 7572383073 4966592427 6169265033 40; (2) . . 7461024498 8864142538 9755011135 85; (3) . . 3674832962 1380846325 1670378619 15; (4) . . 4944320712 6948775055 6792873051 22; (5) . . 8106904231 6258351893 0957683741 64; (6) . . 5634743875 2783964365 2561247216 03; (7) . . 1581291759 4654788418 7082405345 21; (8) . . 3763919821 8262806236 0801781737 19; (9) . . 7973273942 0935412026 7260579064 58; (10) . . 1091314031 1804008908 6859688195 99; (11) . . 7104677060 1336302895 3229398663 69; (12) . . 1559020044 5434298440 9799554565 70; (13) . . 3006681514 4766146993 3184855233 85; (0) . . 0222717149 2204899777 2828507795 10

457 (1) . . 7768052516 4113785557 9868708971 5536105032 8227571115 9737417943 1072210065 6455142231 9474835886 2144420131 2910284463 8949671772 4288840262 5820568927 7899343544 85 (2) . . 0765864332 6039387308 5339168490 1531728665 2078774617 0678336980 3063457330 4157549234 1356673960 6126914660 8315098468 2713347921 2253829321 6630196936 5426695842 45 (0) . . 0218818380 7439824945 2954048140 0437636761 4879649890 5908096280 0875273522 9759299781 1816192560 1750547045 9518599562 3632385120 3501094091 9037199124 7264770240 70

461 (0) . . 0216919739 6963123644 2516268980 .4772234273 3188720173 5357917570 4989154013 0151843817 7874186550 9761388286 3340563991 3232104121 4750542299 3492407809 1106290672 4511930585 6832971800 4338394793 9262472885 0325379609 5444685466 3774403470 7158351409 9783080260 3036876355 7483731019 5227765726 6811279826 4642082429 5010845986 9848156182 2125813449 0238611713 6659436008 6767895878 5249457700 6507592190 8893709327 5488069414 3167028199 5661605206 0737527114 9674620390 4555314533 6225596529 2841648590

463 (1) . . 7580993520 5183585313 1749460043 1965442764 5788336933
0453563714 9028077753 7796976241 9006479481 6414686825
0539956803 4557235421 1663066954 6436285097 1922246220 3023
(2) . . 9092872570 1943844492 4406047516 1987041036 7170626349
8920086393 0885529157 6673866090 7127429805 6155507559
3952483801 2958963282 9373650107 9913606911 4470842332 6133
(0) . . 0215982721 3822894168 4665226781 8574514038 8768898488
1209503239 7408207343 4125269978 4017278617 7105831533
4773218142 5485961123 1101511879 0496760259 1792656587 4730

Teiler	3	9	11	13	27	31	37	41	43	53	67	71	73	79	81	83	89	101
Primitive Wurzel . .	2	2	2	6	2	17	5	6	28	26	12	62	5	29	11	50	30	2

Teiler	103	107	121	127	137	139	151	157	163	169	173	191	197	199	211
Primitive Wurzel . .	6	63	35	106	12	92	114	18	70	137	82	157	73	127	7

Teiler	227	239	241	243	251	271	277	281	283	293	307	311	317	331	347
Primitive Wurzel . .	163	35	14	65	111	6	80	54	259	89	138	258	71	37	125

Teiler	349	353	359	373	397	401	409	421	431	439	443	449	457	463	
Primitive Wurzel . .	220	28	299	82	133	190	174	54	21	285	240	34	264	174	

467 2141327623 1263383297 6445396145 6102783725 9100642398
2869379014 9892933618 8436830835 1177730192 7194860813
7044967880 0856531049 2505353319 0578158458 2441113490
3640256959 3147751605 9957173447 5374732334 0471092077
0877944325 4817987152 0342612419 700<u>2141327</u> . . . . .

479 2087682672 2338204592 9018789144 0501043841 3361169102
2964509394 5720250521 9206680584 5511482254 6972860125
2609603340 2922755741 1273486430 0626304801 6701461377
8705636743 2150313152 4008350730 6889352818 3716075156
5762004175 3653444676 4091858037 578288100<u>2</u> . . . . .

487 2053388090 3490759753 5934291581 1088295687 8850102669
4045174537 9876796714 5790554414 7843942505 1334702258
7268993839 8357289527 7207392197 1252566735 1129363449
6919917864 4763860369 6098562628 3367556468 1724845995
8932238193 0184804928 1314163377 8234086242 2997946611
9096509240 2464065708 4188911704 3121149897 3305954825
4620123203 2854209445 5852156057 4948665297 7412731006
1601642710 4722792607 8028747433 2648870636 5503080082
1355236139 6303901437 3716632443 5318275154 0041067761
8069815195 0718685831 6221765913 757700<u>2053</u> . . .

491 2036659877 8004073319 7556008146 6395112016 2932790224
0325865580 4480651731 1608961303 4623217922 6069246435
8452138492 8716904276 9857433808 5539714867 6171079429
7352342158 8594704684 3177189409 3686354378 8187372708
7576374745 4175152749 4908350305 4989816700 6109979633
4012219959 2668024439 9185336048 8798370672 0977596741
3441955193 4826883910 3869653767 8207739307 5356415478
6150712830 9572301425 6619144602 8513238289 2057026476
5784114052 9531568228 1059063136 4562118126 2729124236
2525458248 4725050916 4969450101 8329938900 ...

499 2004008016 0320641282 5651302605 2104208416 8336673346
6933867735 4709418837 6753507014 0280561122 2444889779
5591182364 7294589178 3567134268 5370741482 9659318637
2745490981 9639278557 1142284569 1382765531 0621242484
9699398797 5951903807 6152304609 2184368737 4749498997
9959919839 6793587174 3486973947 8957915831 6633266533
0661322645 2905811623 2464929859 7194388777 5551102204
4088176352 7054108216 4328657314 6292585170 3406813627
2545090180 3607214428 8577154308 6172344689 3787575150
3006012024 0480961923 8476953907 8156312625 2505010020 ....

503 1988071570 5765407554 6719681908 5487077534 7912524850
8946322067 5944333996 0238568588 4691848906 5606361829
0258449304 1749502982 1073558648 1113320079 5228628230
6163021868 7872763419 4831013916 5009940357 8528827037
7733598409 5427435387 6739562624 2544731610 3379721669
9801192842 9423459244 5328031809 1451292246 5208747514
9105367793 2405566600 3976143141 1530815109 3439363817
0974155069 5825049701 7892644135 1888667992 0477137176
9383697813 1212723658 0516898608 3499005964 2147117296
2226640159 0457256461 2326043737 5745526838 9662027833
00<u>19880715</u> .....

509 1964636542 2396856581 5324165029 4695481335 9528487229
8624754420 4322200392 9273084479 3713163064 8330058939
0962671905 6974459724 9508840864 4400785854 6168958742
6326129666 0117878192 5343811394 8919449901 7681728880
1571709233 7917485265 2259332023 5756385068 7622789783
8899803536 3457760314 3418467583 4970530451 8664047151
2770137524 5579567779 9607072691 5520628683 6935166994
1060903732 8094302554 0275049115 9135559921 4145383104
1257367387 0333988212 1807465618 8605108055 0098231827
1119842829 0766208251 4734774066 7976424361 4931237721
021611001<u>9</u> .....

521 1919385796 5451055662 1880998080 6142034548 9443378119
00191938 57 ....

523 1912045889 1013384321 2237093690 2485659655 8317399617
5908221797 3231357552 5812619502 8680688336 5200764818
3556405353 7284894837 4760994263 8623326959 8470363288
7189292543 0210325047 8011472275 3346080305 9273422562
1414913957 9349904397 7055449330 7839388145 3154875717
0172084130 0191204588 .....

529 1890359168 2419659735 3497164461 2476370510 3969754253
3081285444 2344045368 6200378071 8336483931 9470699432
8922495274 1020793950 8506616257 0888468809 0737240075
6143667296 7863894139 8865784499 0548204158 7901701323
2514177693 7618147448 0151228733 4593572778 8279773156
8998109640 8317580340 2646502835 5387523629 4896030245
7466918714 5557655954 6313799621 9281663516 0680529300
5671077504 7258979206 0491493383 7429111531 1909262759
9243856332 7032136105 8601134215 5009451795 8412098298
6767485822 3062381852 5519848771 2665406427 2211720226
8431001890 ....

541 1848428835 4898336414 0480591497 2273567467 6524953789
2791127541 5896487985 2125693160 8133086876 1552680221
8114602587 8003696857 6709796672 8280961182 9944547134
9353049907 5785582255 0831792975 9704251386 3216266173
7523105360 4436229205 1756007393 7153419593 3456561922
3659889094 2698706099 8151571164 5101663385 9519408502
7726432532 3475046210 7208872458 4103512014 7874306839
1866913123 8447319778 1885397412 1996303142 3290203327
1719038817 0055452865 0646950092 4214417744 9168207024
0295748613 6783733826 2476894639 5563770794 8243992606
2846580406 6543438077 6340110905 7301293900 1848428835 ....

547 1828153564 8994515539 3053016453 3820840950 6398537477
1480804387 5685557586 8372943327 2394881170 0182815356 ....

557 1795332136 4452423698 3842010771 9928186714 5421903052
0646319569 1202872531 4183123877 9174147217 2351885098
7432675044 8833034111 3105924596 0502692998 2046678635
5475763016 1579892280 0718132854 5780969479 3536804308
7971274685 8168761220 8258527827 6481149012 5673249551
1669658886 8940754039 4973070017 ....

563 1776198934 2806394316 1634103019 5381882770 8703374777
9751332149 2007104795 7371225577 2646536412 0781527531
0834813499 1119005328 5968028419 1829484902 3090586145
6483126110 1243339253 9964476021 3143872113 6767317939
6092362344 5825932504 4404973357 0159857904 0852575488
4547069271 7584369449 3783303730 01̲77619893̲ .....

569 1757469244 2882249560 6326889279 4376098418 2776801405
9753954305 7996485061 5114235500 8787346221 4411247803
1634446397 1880492091 3884007029 8769771528 9982425307
5571177504 3936731107 2056239015 8172231985 9402460456
9420035149 3848857644 9912126537 7855887521 9683655536
0281195079 0861159929 7012302284 7100175746̲ ....

571 1751313485 1138353765 3239929947 4605954465 8493870402
8021015761 8213660245 1838879159 3695271453 5901926444
8336252189 1418563922 9422066549 9124343257 4430823117
3380035026 2697022767 0753064798 5989492119 0893169877
4080560420 3152364273 2049036777 5831873905 4290718038
5288966725 0437828371 2784588441 3309982486 8651488616
4623467600 7005253940 4553415061 2959719789 8423817863
3975481611 2084063047 2854640980 7355516637 4781085814
3607705779 3345008756 5674255691 7688266199 6497373029
7723292469 3520140105 0788091068 3012259194 3957968476
3572679509 6322241681 2609457092 8196147110 3327495621
7162872154 1155866900 1̲751313485 ....

577 1733102253 0329289428 0762564991 3344887348 3535528596
1871750433 2755632582 3223570190 6412478336 2218370883
8821490467 9376083188 9081455805 8925476603 1195840554
5927209705 3726169844 0207972270 3639514731 3691507798
9601386481 8024263431 5424610051 9930675909 8786828422
8769497400 3466204506 0658578856 1525129982 6689774696
7071057192 3743500866 5511265164 6447140381 2824956672
4436741767 7642980935 8752166377 8162911611 7850953206
2391681109 1854419410 7452339688 0415944540 7279029462
7383015597 9202772963 6048526863 0849220103 9861351819
7573656845 7538994800 6932409012 1317157712 3050259965
3379549393 4142114384 7487001̲733 ....

587 1703577512 7768313458 2623509369 1763202725 7240204429
3015332197 6149914821 1243611584 3270868824 5315161839
8637137989 7785349233 3901192504 2589437819 4207836456
5587734241 9080068143 1005110732 5383304940 3747870528
1090289608 1771720613 2879045996 5928449744 4633730834
7529812606 4735945485 5195911413 9693356047 7001703577 ....

593 1686340640 8094435075 8853288364 2495784148 3979763912
3102866779 0893760539 6290050590 2192242833 0522765598
6509274873 5244519392 9173693086 0033726812 8161888701
5177065767 2849915682 9679595278 2462057335 5817875210
7925801011 8043844856 6610455311 9730185497 4704890387
8583473861 7200674536 2563237774 0303541315 3456998313
6593591905 5649241146 7116357504 2158516020 2360876897
1332209106 2394603709 9494097807 7571669477 2344013490
7251264755 4806070826 3069139966 2731871838 1112984822
9342327150 0843170320 4047217537 9426644182 1247892074
1989881956 1551433389 5446880269 8145025295 1096121416
5261382799 3254637436 7622259696 4586846543 0016863406 ....

599 1669449081 8030050083 4724540901 5025041736 2270450751
2520868113 5225375626 0434056761 2687813021 7028380634
3906510851 4190317195 3255425709 5158597662 7712854757
9298831385 6427378964 9415692821 3689482470 7846410684
4741235392 3205342237 0617696160 2671118530 8848080133
5559265442 4040066777 9632721202 0033388981 6360601001 ....

601 1663893510 8153078202 9950083194 6755407653 9101497504
1597337770 3826955074 8752079866 8885191347 7537437603
9933444259 5673876871 8801996672 2129783693 8435940099
8336106489 1846921797 0049916805 3244592346 0898502495
8402662229 6173044925 1247920133 1114808652 2462562396
0066555740 4326123128 1198003327 7870216306 1564059900
1663893510 ...

607 1647446457 9901153212 5205930807 2487644151 5650741350
9060955518 9456342668 8632619439 8682042833 6079077429
9835255354 2009884678 7479406919 2751235584 8434925864
9093904448 1054365733 1136738056 0131795716 6392092257
0016474464 ....

613 1631321370 3099510603 5889070146 8189233278 9559543230
0163132137 ....

617 1620745542 9497568881 6855753646 6774716369 5299837925
4457050243 1118314424 6353322528 3630470016 ....

619 1615508885 2988691437 8029079159 9353796445 8804523424
8788368336 0258481421 6478190630 0484652665 5896607431
3408723747 9806138933 7641357027 4636510500 8077544426
4943457189 0145395799 6768982229 4022617124 3941841680
1292407108 2390953150 2423263327 9483037156 7043618739
9030694668 8206785137 3182552504 0387722132 4717235945
0726978998 3844911147 0113085621 9709208400 6462035541
1954765751 2116316639 7415185783 5218093699 5153473344
1033925686 5912762520 1938610662 3586429725 3634894991
9224555735 0565428109 8546042003 2310177705 9773828756
0581583198 7075928917 6090468497 5767366720 5169628432
9563812600 9693053311 7932148626 8174474959 6122778675
2827140549 2730210016 ....

631 1584786053 8827258320 1267828843 1061806656 1014263074
4849445324 8811410459 5879556259 9049128367 6703645007
9239302694 1362916006 3391442155 3090332805 0713153724
2472266244 0570522979 3977812995 2456418383 5182250396
1965134706 8145800316 9572107765 4516640253 5657686212
3613312202 8526148969 8890649762 2820919175 9112519809
8256735340 7290015847 ....

641 1560062402 4960998439 9375975039 0015600624 ..

643 1555209953 3437013996 8895800933 1259720062 2083981337
4805598755 8320373250 3888024883 3592534992 2239502332
8149300155 ....

647 1545595054 0958268933 5394126738 7944358578 0525502318
3925811437 4034003091 1901081916 5378670788 2534775888
7171561051 0046367851 6228748068 0061823802 1638330757
3415765069 5517774343 1221020092 7357032457 4961360123
6476043276 6615146831 5301391035 5486862442 0401854714
0649149922 7202472952 0865533230 2936630602 7820710973
7248840803 7094281298 2998454404 9459041731 0664605873
2612055641 4219474497 6816074188 5625965996 9088098918
0834621329 2117465224 1112828438 9489953632 1483771251
9319938176 1978361669 2426584234 9304482225 6568778979
9072642967 5425038639 8763523956 7233384853 1684698608
9644513137 5579598145 2859350850 0772797527 0479134466
7697063369 3972179289 0262751159 1962905718 7017001545 ....

653 1531393568 1470137825 4211322312 4042879019 9081163859
1117917304 7473200612 5574272588 0551301684 5329249617
1516079632 4655436447 1669218989 2802450229 7090352220
5206738131 6998468606 4318529862 1745788667 6875957120
9800918836 1408882082 6952526799 3874425727 4119448698
3154670750 3828483920 3675344563 5528330781 0107197549
7702909647 7794793261 868300$\underline{1531}$ ....

659 1517450682 · 8528072837 6327769347 4962063732 9286798179
0591805766 3125948406 6767830045 5235204855 8421851289
8330804248 8619119878 6039453717 7541729893 7784522003
0349013657 0561456752 6555386949 9241274658 5735963581
1836115326 2518968133 5356600910 4704097116 8437025796
6616084977 2382397572 0789074355 0834597875 5690440060
6980273141 1229135053 1107738998 4825493171 4719271623
6722306525 0379362670 7132018209 4081942336 8740515933
2321699544 7647951441 5781487101 6691957511 3808801213
9605462822 4582701062 2154779969 6509863429 4385432473
4446130500 7587253414 2640364188 1638846737 4810318664
6433990895 2959028831 5629742033 3839150227 6176024279
2109256449 1654021244 3095599393 0197268588 7708649468
892261001$\underline{5}$ ....

661 1512859304 0847201210 2874432677 7609682299 5461422087
7458396369 1376701966 7170953101 3615733736 7624810892
5869894099 8487140695 9152798789 7125567322 2390317700
4538577912 2541603630 8623298033 2829046898 6384266263
2375189107 4130105900 $\underline{15}$12859304 ....

673 1485884101 0401188707 2808320950 9658246656 7607726597
3254086181 2778603268 9450222882 6151560178 3060921248
1426448736 9985141158 9895988112 9271916790 4903417533
4323922734 0267459138 1872213967 3105497771 1738484398
2169390787 5185735512 6300148588 ....

677 1477104874 4460856720 8271787296 8980797636 6322008862
6292466765 1403249630 7237813884 7858197932 0531757754
8005908419 4977843426 8833087149 1875923190 5465288035
4505169867 0605612998 5228951255 5391432791 7282127031
0192023633 6779911373 7075332348 5967503692 7621861152
1418020679 4682422451 9940915805 0221565731 1669128508
1240768094 5347119645 4948301329 394387001$\underline{4}$ ....

683 1464128843 3382137628 1112737920 9370424597 3645680819
9121522693 9970717423 1332357247 4377745241 5812591508
0527086383 6017569546 1200585651 5373352855 0512445095
1683748169 8389458272 3279648609 0775988286 9692532942
8989751098 0966325036 6032210834 5534407027 8184480234
2606149341 1420204978 0380673499 2679355783 3089311859
4436310395 3147877013 1771595900 4392386530 0146412884 ....

691 1447178002 8943560057 8871201157 7424023154 8480463096
9609261939 2185238784 3704775687 4095513748 1910274963
8205499276 4109985528 2199710564 3994211287 9884225759
7684515195 3690303907 3806078147 6121562952 2431259044
8625180897 2503617945 0072358900 1447178022 ....

701 1426533523 5378031383 7375178316 6904422253 9229671897
2895863052 7817403708 9871611982 8815977175 4636233951
4978601997 1469329529 2439372325 2496433666 1911554921
5406562054 2082738944 3651925820 2567760342 3680456490
7275320970 0427960057 0613409415 1212553495 0071326676
1768901569 1868758915 8345221112 6961483594 8644793152
6390870185 4493580599 1440798858 7731811697 5748930099
8573466476 4621968616 2624821683 3095577746 0770328102
7104136947 2182596291 0128388017 1184022824 5363766048
5021398002 8530670470 7560627674 7503566333 8088445078
4593437945 7917261055 6348074179 7432239657 6319543509
2724679029 9572039942 9386590584 8787446504 9928673323
8231098430 8131241084 1654778887 3038516405 1355206847
3609129814 5506419400 8559201141 2268188302 4251069900 ....

709 1410437235 5430183356 8406205923 8363892806 7700987306
0648801128 3497884344 1466854724 9647390691 1142454160
7898448519 0409026798 3074753173 4837799717 9125528913
9633286318 7588152327 2214386459 8025387870 2397743300
4231311706 6290550070 5218617771 5091678420 3102961918
1946403385 0493653032 4400564174 8942172073 3427362482
3695345557 1227080394 9224259520 4513399153 7376586741
8899858956 2764456981 6643159379 4076163610 7193229901
2693935119 8871650211 5655853314 5275035260 9308885754
5839210155 1480959097 3201692524 6826516220 0282087447
1086036671 3681241184 7672778561 3540197461 2129760225
6699576868 8293370944 9929478138 2228490832 1579689703
8081805359 6614950634 6967559943 5825105782 7926657263
7517630465 4442877291 9605077574 0479548660 0846262341
3258110014 ....

719 1390320584 1446453407 5104311543 8108484005 5632823365
7858136300 4172461752 4339360222 5312934631 4325452016
6898470097 3574408901 2517385257 3018080667 5938803894
2976356050 0695410292 0723226703 7552155771 9054242002
7816411682 8929068150 2086230876 2169680111 2656467315
7162726008 3449235048 6787204450 6258692628 6509040333
7969401947 1488178025 0347705146 0361613351 8776077885
9527121001 ....

727 1375515818 4319119669 8762035763 4112792297 1114167812
9298486932 5997248968 3631361760 6602475928 4731774415
4057771664 3741403026 1348005502 0632737276 4786795048
1430536451 1691884456 6712517193 9477303988 9958734525
4470426409 9037138927 0976616231 0866574965 6121045392
0220082530 9491059147 1801925722 1458046767 5378266850
0687757909 2159559834 9381017881 7056396148 5557083906
4649243466 2998624484 1815680880 3301237964 2365887207
7028885832 1870701513 0674002751 0316368638 2393397524
0715268225 5845942228 3356258596 9738651994 4979367262
7235213204 9518569463 5488308115 5433287482 8060522696
0110041265 4745529573 5900962861 0729023383 7689133425
0343878954 6079779917 4690508940 8528198074 2778541953
2324621733 1499312242 0907840440 1650618982 1182943603
8514442916 0935350756 5337001375 ....

729 1371742112 4828532235 9396433470 5075445816 1865569272
9766803840 8779149519 8902606310 0137174211

733 1364256480 2182810368 3492496589 3587994542 9740791268
7585266030 0136425648 ....

739 1353179972 9364005412 7198917456 0216508795 6698240866
0351826792 9634641407 3071718538 5656292286 8741542625
1691474966 1705006765 8998646820 0270635994 5872801082
5439783491 2043301759 1339648173 2070365358 5926928281
4614343707 7131258457 3748308525 0338294993 2341001353 ....

743 1345895020 1884253028 2637954239 5693135935 3970390309
5558546433 3781965006 7294751009 4212651413 1897711978
4656796769 8519515477 7927321668 9098250336 4737550471
0632570659 4885598923 2839838492 5975773889 6366083445
4912516823 6877523553 1628532974 4279946164 1991924629
8788694481 8304172274 5625841184 3876177658 1426648721
3997308209 9596231493 9434724091 5208613728 1292059219
3808882907 1332436069 9865410497 9811574697 1736204576
0430686406 4602960969 0444145356 6621803499 3270524899
0578734858 6810228802 1534320323 0148048452 2207267833
1090174966 3526244952 8936742934 0511440107 6716016150
7402422611 0363391655 4508748317 6312247644 6837146702
5572005383 5800807537 0121130551 8169582772 5437415881
5612382234 1857335127 8600269179 0040376850 6056527590
8479138627 1870794078 0619111709 2866756393 00<u>13458</u>950 ....

751 1331557922 7696404793 6085219707 0572569906 7909454061
2516644474 0346205059 9201065246 3382157123 8348868175
7656458055 9254327563 249<u>0013315</u> ....

757 1321003963 0118890356 671070<u>0132</u> ....

761 1314060446 7805519053 8764783180 0262812089 3561103810
7752956636 0052562417 8712220762 1550591327 2010512483
5742444152 4310118265 4402102496 7148488830 4862023653
0880420499 3429697766 0972404730 6176084099 8685939553
2194480946 1235216819 9737187910 6438896189 2247043363
9947437582 1287779237 8449408672 7989487516 4257555847
5689881734 5597897503 2851511169 5137976346 9119579500
6570302233 9027595269 3823915900 <u>13</u>1<u>4060446</u> ....

769 1300390117 0351105331 5994798439 5318595578 6736020806
2418725617 6853055916 7750325097 5292587776 3328998699
6098829648 8946684005 2015604681 4044213263 9791937581
2743823146 9440832249 6749024707 4122236671 00<u>1300</u>390<u>1</u> ....

773 1293661060 8020698576 9728331177 2315653298 8357050452
7813712807 2445019404 9159120310 4786545924 9676584734
7994825355 7567917205 6921096675 2910737386 8046571798
1888745148 7710219922 3803363518 7580853816 300<u>1293661</u> ....

787 1270648030 4955527318 9326556543 8373570520 9656925031
7662007623 8881829733 1639135959 3392630241 4231257941
5501905972 0457433290 9783989834 8157560355 7814485387
5476493011 4358322744 5997458703 9390088945 3621346886
9123252858 9580686149 9364675984 7522236340 5336721728
0813214739 5171537484 1168996188 0559085133 4180432020
3303684879 2884371029 2249047013 9771283354 5108005082
5921219822 1092757306 2261753494 2820838627 700$\underline{12}$70648 ....

797 1254705144 2910915934 7553324968 6323713927 2271016311
1668757841 9071518193 2245922208 2810539523 2120451693
8519447929 7365119196 9887076537 0138017565 8720200752
8230865746 5495608531 9949811794 2283563362 6097867001 ....

809 1236093943 1396786155 7478368355 9950556242 2744128553
7700865265 7601977750 3090234857 8491965389 3695920889
9876390605 6860321384 4252163164 4004944375 7725587144
6229913473 4239802224 9690976514 2150803461 0630407911
00$\underline{12360939}$ ....

811 1233045622 6880394574 5992601726 2638717632 5524044389
6424167694 2046855733 6621454993 8347718865 5980271270
0369913686 8064118372 3797780517 8791615289 7657213316
8927250308 2614056720 0986436498 1504315659 6794081381
0110974106 0419235511 7139334155 3637484586 9297163995
0678175092 4784217016 0295930949 4451294697 9038224414
3033292231 8125770653 5141800246 6091245376 0789149198
5203452527 7435265104 8088779284 8335388409 3711467324
2909987669 5437731196 0542540073 9827373612 8236744759
5561035758 3230579531 4426633785 4500616522 8113440197
2872996300 8631319358 8162762022 1948212083 8471023427
8668310727 4969173859 4327990135 6350184956 8434032059
1861898890 2589395807 6448828606 6584463625 1541307028
3600493218 2490752157 8298397040 6905055487 0530209617
7558569667 0776818742 2934648581 9975339087 5462392108
5080147965 4747225647 3489519112 2071516646 1159062885
3267570900 123$\underline{3045}$$\underline{662}$ ....

821 1218026796 5895249695 4933008526 1875761266 7478684531
0596833130 3288672350 7917174177 8319123020 7064555420
2192448233 8611449451 8879415347 1376370280 1461632155
9074299634 5919610231 4250913520 0974421437 2716199756
3946406820 9500609013 3982947624 8477466504 2630937880
6333739342 2655298416 5651644336 1753958587 0889159561
5103532277 7101096224 1169305724 7259439707 6735688185
1400730816 0779537149 8172959805 1157125456 7600487210
7186358099 8781973203 4104750304 5066991473 8124238733
2521315468 9403166869 6711327649 2082825822 1680876979
2935444579 7807551766 1388550548 1120584652 8623629719
8538367844 0925700365 4080389768 5749086479 9025578562
7283800243 6053593179 0499390986$\dot{}$ 6017052375 1522533495
7369062119 3666260657 7344701583 4348355663 8246041412
9110840438 4896467722 2898903775 8830694275 2740560292
3264311814 8599269183 9220462850 1827040194 8842874543
2399512789 2813641900 $\underline{1218026796}$ ....

823 1215066828 6755771567 4362089914 9453219927 0959902794
6537059538 2746051032 8068043742 4058323207 7764277035
2369380315 9173754556 5006075334 1433778857 8371810449
5747266099 6354799513 9732685297 6913730255 1640340218
7120291616 0388821385 1761846901 5795868772 7825030376
6707168894 2891859052 2478736330 4981773997 5698663426
4884568651 2758201701 0935601458 0801944106 9258809234
5078979343 8639125151 8833535844 4714459295 2612393681
6524908869 9878493317 1324422843 2563791008 5054678007
2904009720 5346294046 1725394896 7193195625 7594167679
2223572296 4763061968 4082624544 3499392466 5856622114
2162818955 0425273390 0364520048 6026731470 2308626974
4835965978 1287970838 3961117861 4823815309 8420413122
7217496962 3329283110 5710814094 7752126366 9501822600
2430133657 3511543134 8724179829 8906439854 1919805589
3074119076 5492102065 6136087484 8116646415 5528554070
4738760631 8347509113 00$\underline{12150668}$ ....

827 1209189842 8053204353 0834340991 5356711003 6275695284
1596130592 5030229746 0701330108 8270858524 7883917775
0906892382 1039903264 8125755743 6517533252 7206771463
1197097944 3772672309 5525997581 6203143893 5912938331
3180169286 5779927448 6094316807 7388149939 5405078597
3397823458 2829504232 1644498186 2152357920 1934703748
4885126964 9334945586 4570737605 8041112454 6553808948
0048367593 7122128174 1233373639 6614268440 1451027811
3663845223 700<u>1209189</u> . . . .

829 1206272617 6115802171 2907117008 4439083232 8106151990
3498190591 0735826296 7430639324 4873341375 1507840772
0144752714 1133896260 5548854041 0132689987 9372738238
8419782870 9288299155 6091676718 9384800965 0180940892
6417370325 6936067551 2665862484 9215922798 5524728588
6610373944 5114595898 673100<u>1206</u> . . . .

839 1191895113 2300357568 5339690107 2705601907 0321811680
5721096543 5041716328 9630512514 8986889153 7544696066
7461263408 8200238379 0226460071 5137067938 0214541120
3814064362 3361144219 3087008343 2657926102 5029797377
8307508939 2133492252 6817640047 6758045292 0143027413
5876042908 2240762812 8724672228 8438617401 6686531585
2205005959 4755661501 7878426698 4505363528 0095351609
0584028605 4827175208 5816448152 5625744934 4457687723
4803337306 317044100<u>1</u> . . . .

841 1189060642 0927467300 8323424494 6492271105 8263971462
5445897740 7847800237 8121284185 4934601664 6848989298
4542211652 7942925089 1795481569 5600475624 2568370986
9203329369 7978596908 4423305588 5850178359 0963139120
0951248513 6741973840 6658739595 7193816884 6611177170
0356718192 6278240190 2497027348 3947681331 7479191438
7633769322 2354340071 3436385255 6480380499 4054696789
5362663495 8382877526 7538644470 8680142687 2770511296
0760998810 9393579072 5326991676 5755053507 7288941736
0285374554 1022592152 1997621878 7158145065 3983353151
0107015457 7883472057 0749108204 5184304399 5243757431
6290130796 6706302021 4030915576 6944114149 8216409036
8608799048 7514863258 0261593341 2604042806 1831153388
8228299643 2818073721 7598097502 9726516052 3186682520
8085612366 2306777645 6599286563 6147443519 6195005945
3032104637 3365041617 1224732461 3555291319 8573127229
4887039239 00<u>11890606</u> . . . .

853 1172332942 5556858147 7139507620 1641266119 5779601406
7995310668 2297772567 4091441969 5193434935 5216881594
3728018757 3270808909 7303634232 1219226260 2579132473
6225087924 9706916764 3610785463 0715123094 9589683470
1055099648 300$\underline{1172}$33$\underline{2}$ ....

857 1166861143 5239206534 4224037339 5565927654 6091015169
1948658109 6849474912 4854142357 0595099183 1971995332
5554259043 1738623103 8506417736 2893815635 9393232205
3675612602 1003500583 4305717619 6032672112 0186697782
9638273045 5075845974 3290548424 7374562427 0711785297
5495915985 9976662777 1295215869 3115519253 2088681446
9078179696 6161026837 8063010501 7502917152 8588098016
3360560093 3488914819 1365227537 9229871645 2742123687
2812135355 8926487747 9579929988 3313885647 6079346557
7596266044 3407234539 0898483080 5134189031 5052508751
4585764294 0490081680 2800466744 4574095682 6137689614
9358226371 0618436406 0676779463 2438739789 9649941656
9428238039 6732788798 1330221703 6172695449 2415402567
0945157526 2543757292 8821470245 0408401400 2333722287
0478413068 8448074679 1131855309 2182030338 3897316219
3698949824 9708284714 1190198366 3943990665 1108518086
3477246207 7012835472 5787631271 8786464410 7351225204
200700$\underline{1166}$ ....

859 1164144353 8998835855 6461001$\underline{1164}$ ....

863 1158748551 5643105446 1181923522 5955967555 0405561993
0475086906 1413673232 9084588644 2641946697 5666280417
1494785631 5179606025 4924681344 1483198146 0023174971
0312862108 9223638470 4519119351 1008111239 8609501738
1228273464 6581691772 8852838933 9513325608 3429895712
6303592120 5098493626 8829663962 9200463499 4206257242
1784472769 4090382387 0220162224 7972190034 7624565469
2931633835 4577056778 6790266512 1668597914 2526071842
4101969872 5376593279 2584009269 9884125144 8435689455
3881807647 7404403244 4959443800 6952491309 3858632676
7091541135 5735805330 2433371958 2850521436 8482039397
4507531865 5851680185 3997682502 8968713789 1077636152
9548088064 8899188876 0139049826 1877172653 5341830822
7114716106 6048667439 1657010438 7369640787 9490150637
3117033603 7079953650 0579374275 7821552723 0590961761
2977983777 5202780996 5237543453 0706836616 4542294322
1320973348 7833140208 5747392815 7589803012 7462340672
0741599073 00$\underline{11587485}$ ....

877 1140250855 1881413911 0604332953 2497149372 8620296465
2223489167 6168757126 5678449258 8369441277 0809578107
1835803876 8529076396 8072976054 7320410490 3078677309
0079817559 8631698973 7742303306 7274800456 1003420752
5655644241 7331812998 8597491448 1185860889 3956670467
5028506271 3797035347 7765108323 8312428734 3215507411
6305587229 1904218928 1641961231 4709236031 9270239452
6795895096 9213226909 9201824401 3683010262 2576966932
7251995438 9965792474 3443557582 668187011 ....

881 1135073779 7956867196 3677639046 5380249716 2315550510
7832009080 5902383654 9375709421 1123723041 9977298524
4040862656 0726447219 0692395005 6753688989 7843359818
3881952326 9012485811 5777525539 1600454029 5119182746
8785471055 6186152099 8864926220 2043132803 6322360953
4619750283 7684449489 2167990919 4097616345 0624290578
8876276958 0022701475 5959137343 9273552780 9307604994
3246311010 2156640181 6118047673 0987514188 4222474460
8399545970 4880817253 1214528944 3813847900 1135073779 ....

883 1132502831 2570781426 9535673839 1845979614 9490373725
9343148357 8708946772 3669309173 2729331823 3295583238
9580973952 4348810872 0271800679 5016987542 4688561721
4043035107 5877689694 2242355605 8890147225 3680634201
5855039637 5990939977 3499433748 5843714609 2865232163
0804077010 1925754813 1370328425 8210645526 6138165345
4133635334 0883352208 3805209513 0237825594 5639864099
6602441506 2287655719 1392978482 4462061155 1528878822
1970554926 3873159682 8992072480 1812004530 01132502 83 ....

887 1127395715 8962795941 3754227733 9346110484 7801578354
0022547914 3179255918 8275084554 6786922209 6956031567
0800450958 2863585118 3765501691 0935738444 1939120631
3416009019 1657271702 3675310033 8218714768 8838782412
6268320180 3833145434 0473506200 6764374295 3776775648
2525366403 6076662908 6809470124 0135287485 9075535512
9650507328 0721533258 1736189402 4802705749 7181510710
2593010146 5614430665 1634723788 0496054114 9943630214
2051860202 9312288613 3032694475 7609921082 2998872604
2841037204 0586245772 2660653889 5152198421 6459977452
0856820744 0811724915 4453213077 7903043968 4329199549
0417136414 8816234498 3089064261 5558060879 3686583990
9808342728 2976324689 9661781285 2311161217 5873731679
8196166854 5659526493 7993235625 7046223224 3517474633
5963923337 0913190529 8759864712 5140924464 4870349492
6719278466 7418263810 5975197294 2502818489 2897406989
8534385569 3348365276 2119503945 8850056369 7857948139
7970687711 3866967305 5242390078 9177001127 ....

907 1102535832 4145534729 8787210584 3439911797 1334068357
2216097023 1532524807 0562293274 5314222712 2381477398
0154355016 5380374862 1830209481 8081587651 5986769570
0110253583 ....

911 1097694840 8342480790 3402854006 5861690450 0548847420
4171240395 1701427003 2930845225 0274423710 2085620197
5850713501 6465422612 5137211855 1042810098 7925356750
8232711306 2568605927 5521405049 3962678375 4116355653
1284302963 7760702524 6981339187 7058177826 5642151481
8880351262 3490669593 8529088913 2821075740 9440175631
1745334796 9264544456 6410537870 4720087815 5872667398
4632272228 3205268935 2360043907 7936333699 2316136114
1602634467 6180021953 8968166849 6158068057 0801317233
8090010976 ....

919 1088139281 8280739934 7116430903 1556039173 0141458106
6376496191 5125136017 4102285092 4918389553 8628944504
8966267682 2633297062 0239390642 0021762785 6365614798
6942328618 0631120783 4602829162 1327529923 8302502720
3482045701 8498367791 0772578890 0979325353 6452665941
2404787812 8400435255 7127312295 9738846572 3612622415
6692056583 2426550598 4766050054 4069640914 0369967355
8215451577 8019586507 0729053318 8248095756 2568008705
1142546245 9194776931 4472252448 3133841131 6648531011
9695321001 ....

929 1076426264 8008611410 1184068891 2809472551 1302475780
4090419806 2432723358 4499461786 8675995694 2949407965
5543595263 7244348762 1097954790 0968783638 3207750269
1065662002 1528525296 0172228202 3681377825 6189451022
6049515608 1808396124 8654467168 9989235737 3519913885
8988159311 0871905274 4886975242 1959095801 9375672766
4155005382 1313240043 0570505920 3444564047 3627556512
3789020452 0990312163 6167922497 3089343379 9784714747
0398277717 9763186221 7438105489 7739504843 9181916038
7513455328 3100107642 ....

937 1067235859 1248665955 1760939167 5560298826 0405549626
4674493062 9669156883 6712913553 8954108858 0576307363
9274279615 7950907150 4802561366 0618996798 2924226254
0021344717 1824973319 1035218783 3511205976 5208110992
5293489861 2593383137 6734258271 0779082177 1611526147
2785485592 3159018143 0096051227 3212379935 9658484525
0800426894 3436499466 3820704375 6670224119 5304162219
8505869797 2251867662 7534685165 4215581643 5432230522
9455709711 8463180362 8601921024 5464247598 7193169690
5016008537 8868729989 3276414087 5133404482 3906083244
3970117395 9445037353 2550693703 3084311632 8708644610
4589114194 2369263607 2572038420 4909284951 9743863393
8100320170 7577374599 7865528281 7502668089 6478121664
8879402347 9188900747 0651013874 0661686232 6574172892
2091782283 8847385272 1451440768 4098185699 0394877267
8762006403 4151547491 9957310565 6350053361 7929562433
2977588046 9583778014 9413020277 4813233724 6531483457
8441835645 6776947705 4429028815 3681963713 9807897545
3575240128 0683030949 8399146211 3127001067 ....

941 1062699256 1105207226 3549415515 4091392136 0255047821
4665249734 3251859723 6981934112 6461211477 1519659936
2380446333 6875664187 0350690754 5164718384 6971307120
0850159404 8884165781 0839532412 3273113708 8204038257
1732199787 4601487778 9585547290 1168969181 7215727948
9904357066 9500531349 6280552603 6131774707 7577045696
0680127523 9107332624 8671625929 8618490967 0563230605
7385759829 9681190223 1668437832 0935175345 3772582359
1923485653 5600425079 7024442082 8905419766 2061636556
8544102019 1285866099 8937300743 8894792773 6450584484
5908607863 9744952178 5334750265 6748140276 3018065887
3538788522 8480340063 7619553666 3124335812 9649309245
4835281615 3028692879 9149840595 1115834218 9160467587
6726886291 1795961742 8267800212 5398512221 0414452709
8831030818 2784272051 0095642933 0499468650 3719447396
3868225292 2422954303 9319872476 0892667375 1328374070
1381509032 9436769394 2614240170 0318809776 8331562167
9064824654 6227417640 8076514346 4399574920 2975557917
1094580233 7938363443 1455897980 8714133900 1062699256 ....

947 1055966209 0813093980 9926082365 3643083421 3305174234
4244984160 5068637803 5902851108 7645195353 7486800422
3864836325 2375923970 4329461457 2333685322 0696937697
9936642027 4551214361 1404435058 0781414994 7201689545
9345300950 3695881731 7845828933 4741288278 7750791974
6568109820 4857444561 7740232312 5659978880 6758183738
1203801478 3526927138 3315733896 5153115100 3167898627
2439281942 9778247096 0929250263 9915522703 2734952481
5205913410 7708553326 2935586061 2460401267 1594508975
7127771911 2988384371 7001055966 ....

953 1049317943 3368310598 1112277019 9370409233 9979013641
1332633788 0377754459 6012591815 3200419727 1773347324
2392444910 8079748163 6935991605 4564533053 5152151101
7838405036 7261280167 8908709338 9296956977 9643231899
2654774396 6421825813 2214060860 4407135362 0146904512
0671563483 7355718782 7911857292 7597061909 7586568730
3252885624 3441762854 1448058761 8048268625 3934942287
5131164742 9171038824 .7639034627 4921301154 2497376705
1416579223 5047219307 4501573976 9150052465 8971668415
5299055613 8509968520 4616998950 6820566631 6894018887
7229800629 5907660020 9863588667 3662119622 2455403987
4081846799 5802728226 6526757607 5550891920 2518363064
0083945435 4669464847 8488982161 5949632738 7198321091
2906610703 0430220356 7681007345 2256033578 1741867785
9391395592 8646379853 0954879328 4365162644 2812172088
1427072402 9380902413 4312696747 1143756558 2371458551
9412381951 7313746065 0577124868 8352570828 9611752360
9653725078 6988457502 6232948583 4207764952 7806925498
4260230849 9475341028 3315844700 9443861490 0314795383
00<u>10493179</u> ....

961 1040582726 3267429760 6659729448 4911550468 2622268470
3433922996 8782518210 1977107180 0208116545 2653485952
1331945889 6982310093 6524453694 0686784599 3756503642
0395421436 0041623309 0530697190 4266389177 9396462018
7304890738 8137356919 8751300728 4079084287 2008324661
8106139438 0853277835 5879292403 7460978147 7627471383
9750260145 6815816857 4401664932 3621227887 6170655567
1175858480 7492195629 5525494276 7950052029 1363163371
4880332986 4724245577 5234131113 4235171696 1498439125
9105098855 3590<u>10405</u> ....

967 1034126163 3919338159 2554291623 5780765253 3609100310
2378490175 8014477766 2874870734 2295760082 7300930713
5470527404 3433298862 4612202688 7280248190 2792140641
1582213029 9896587383 6608066184 0744570837 6421923474
6639089968 9762150982 4198552223 3712512926 5770423991
7269966928 6452947259 5656670113 7538779731 1271975180
9720785935 8841778697 00<u>10341261</u> ....

971 1029866117 4047373841 4006179196 7044284243 0484037075
1802265705 4582904222 4510813594 2327497425 3347064881
5653964984 5520082389 2893923789 9073120494 3357363542
7394438722 9660144181 2564366632 3377960865 0875386199
7940267765 1905252317 1987641606 5911431513 9031925849
6395468589 0834191555 0978372811 5345005149 3305870236
8692070030 8959835221 4212152420 1853759011 3285272914
5211122554 0679711637 4871266735 3244078269 8249227600
4119464469 6189495365 6024716786 8177136972 1936148300
7209062821 8331616889 8043254376 9309989701 3388259526
2615859938 2080329557 1575695159 6292481977 3429454170
9577754891 8640576725 0257466529 3511843460 3501544799
1761071060 7621009268 7950566426 3645726055 6127703398
5581874356 3336766220 3913491246 1380020597 3223480947
4768280123 5839340885 6848609680 7415036045 3141091658
0844490216 2718846549 9485066941 2976313079 2996910401
6477857878 4757981462 4098867147 2708547888 7744593202
8836251287 3326467559 2173017507 7239958805 3553038105
0463439752 8321318228 6302780638 5169927909 3717816683
8311019567 4562306900 1029866117 ....

977 1023541453 4288638689 8669396110 5424769703 1729785056
2947799385 8751279426 8167860798 3623336745 1381780962
1289662231 3203684749 2323439099 2835209825 9979529178
9314227226 2026612077 7891504605 9365404298 8741044012
2824974411 4636642784 0327533265 0972364380 7574206755
3735926305 0153531218 0143295803 4800409416 5813715455
4759467758 4442169907 8812691914 0225179119 7543500511
7707267144 3193449334 6980552712 3848515864 8925281473
8996929375 6397134083 9303991811 6683725690 8904810644
8311156601 8423746161 7195496417 6049129989 7645854657
1136131013 3060388945 7523029682 7021494370 5220061412
4872057318 3213920163 7666325486 1821903787 1033776867
9631525076 7656090071 6479017400 2047082906 8577277379
7338792221 0849539406 3459570112 5895598771 7502558853
6335721596 7246673490 2763561924 2579324462 6407369498
4646878198 5670419651 9959058341 8628454452 4053224155
5783009211 8730808597 7482088024 5649948822 9273285568
0655066530 1944728761 5148413510 7471852610 0307062436
0286591606 9600818833 1627430910 9518935516 8884339815
7625383828 0450358239 5087001023 ....

983 1017293997 9654120040 6917599186 1648016276 7039674465
9206510681 5869786368 2604272634 7914547304 1709053916
5818921668 3621566632 7568667344 8626653102 7466937945
0661241098 6775178026 4496439471 0071210579 8575788402
8484231943 0315361159 3692777212 6144455747 7110885045
7782299084 4354018311 2919633774 1607324516 7853509664
2929806714 1403865717 1922685656 1546286876 9074262461
8514750762 9704984740 5900305188 1993896236 0122075279
7558494404 8830111902 3397761953 2044760935 9104781281
7904374364 1912512716 1749745676 5005086469 9898270600
2034587995 9308240081 3835198372 3296032553 4079348931
8413021363 1739572736 5208545269 5829094608 3418107833
1637843336 7243133265 5137334689 7253306205 4933875890
1322482197 3550556052 8992878942 0142421159 7151576805
6968463886 0630722278 7385554425 2288911495 4221770091
5564598168 8708036622 5839267548 3214649033 5707019328
5859613428 2807731434 3845371312 3092573753 8148524923
7029501525 9409969481 1800610376 3987792472 0244150559
5116988809 7660223804 6795523906 4089521871 8209562563
5808748728 3825025432 3499491353 00<u>10172939</u> ....

991 1009081735 6205852674 0665993945 5095862764 8839556004 0363269424
8234106962 6639757820 3834510595 3582240161 4530776992 9364278506
5590312815 3380423814 3289606458 1231079717 4571140262 3612512613
5216952573 1584258324 9243188698 9845610494 4500504540 8678102926
3370332996 9727547931 3824419778 0020181634 7124117053 4813319878
9101917255 2976791120 0807265388 4964682139 2532795156 4076690211
9071644803 2290615539 8587285570 1311806256 3067608476 2865792129
1624621594 3491422805 2472250252 2704339051 4631685166 4984863773
9656912209 8890<u>10090</u> ....

997 1003009027 0812437311 9358074222 6680040120 3610832497 4924774322
9689067201 6048144433 2998996990 9729187562 6880641925 7773319959
8796389167 5025075225 6770310932 7983951855 566700<u>1003</u> ....

TAFEL DER HÄUFIGKEIT DER PRIMZAHLEN.

1	168	51	89	101	81	151	85	201	77	251	71	301	85	351	74	401	70	451	92
2	135	52	97	102	93	152	90	202	87	252	88	302	83	352	80	402	71	452	76
3	127	53	89	103	87	153	88	203	78	253	78	303	72	353	82	403	76	453	63
4	120	54	92	104	80	154	77	204	78	254	81	304	84	354	79	404	75	454	72
5	119	55	90	105	91	155	84	205	77	255	76	305	88	355	87	405	70	455	74
6	114	56	93	106	82	156	85	206	85	256	87	306	80	356	79	406	83	456	82
7	117	57	99	107	92	157	76	207	83	257	72	307	82	357	67	407	67	457	73
8	107	58	91	108	76	158	88	208	87	258	78	308	73	358	80	408	81	458	77
9	110	59	90	109	91	159	87	209	85	259	86	309	76	359	83	409	79	459	75
10	112	60	94	110	88	160	85	210	88	260	76	310	80	360	71	410	82	460	68
11	106	61	88	111	83	161	85	211	84	261	77	311	79	361	68	411	73	461	77
12	103	62	87	112	84	162	84	212	86	262	73	312	69	362	79	412	81	462	69
13	109	63	88	113	81	163	81	213	69	263	79	313	86	363	76	413	74	463	74
14	105	64	93	114	88	164	83	214	81	264	84	314	86	364	84	414	69	464	77
15	102	65	80	115	82	165	77	215	86	265	80	315	76	265	77	415	90	465	85
16	108	66	98	116	93	166	80	216	74	266	78	316	77	366	77	416	80	466	74
17	98	67	84	117	81	167	81	217	76	267	87	317	84	367	85	417	67	467	69
18	104	68	99	118	90	168	83	218	80	268	94	318	84	368	79	418	82	468	83
19	94	69	80	119	79	169	73	219	84	269	75	319	81	369	72	419	85	469	85
20	102	70	81	120	87	170	87	220	91	270	78	320	86	370	68	420	75	470	72
21	98	71	98	121	88	171	87	221	78	271	84	321	79	371	70	421	75	471	87
22	104	72	95	122	86	172	81	222	80	272	78	322	80	372	76	422	73	472	78
23	100	73	90	123	88	173	89	223	81	273	83	323	81	373	81	423	77	473	73
24	104	74	83	124	88	174	79	224	80	274	71	324	71	374	73	424	83	474	78
25	94	75	92	125	83	175	83	225	83	275	80	325	87	375	82	425	81	475	80
26	98	76	91	126	84	176	75	226	84	276	83	326	85	376	85	426	74	476	86
27	101	77	83	127	83	177	95	227	76	277	83	327	73	377	80	427	71	477	75
28	94	78	95	128	86	178	73	228	80	278	74	328	86	378	71	428	78	478	69
29	98	79	84	129	89	179	89	229	89	279	81	329	73	379	77	429	71	479	85
30	92	80	91	130	83	180	94	230	88	280	73	330	81	380	83	430	89	480	71
31	95	81	88	131	85	181	71	231	84	281	87	331	80	381	72	431	76	481	77
32	92	82	92	132	83	182	79	232	78	282	85	332	82	382	76	432	79	482	78
33	106	83	89	133	87	183	91	233	76	283	77	333	72	383	74	433	84	483	82
34	100	84	84	134	82	184	79	234	71	284	72	334	80	384	81	434	80	484	75
35	94	85	87	135	80	185	83	235	87	285	90	335	77	385	78	435	85	485	65
36	92	86	85	136	89	186	91	236	73	286	77	336	77	386	80	436	82	486	63
37	99	87	88	137	96	187	79	237	76	287	71	337	84	387	78	437	73	487	82
38	94	88	93	138	80	188	87	238	73	288	71	338	80	388	69	438	70	488	78
39	90	89	76	139	85	189	80	239	87	289	85	339	77	389	75	439	75	489	83
40	96	90	94	140	84	190	88	240	79	290	84	340	68	390	84	440	75	490	78
41	88	91	89	141	87	191	75	241	80	291	84	341	84	391	81	441	79	491	78
42	101	92	85	142	87	192	81	242	91	292	77	342	77	392	79	442	72	492	76
43	102	93	97	143	82	193	89	243	76	293	78	343	77	393	86	443	85	493	67
44	85	94	86	144	77	194	84	244	77	294	68	344	80	394	87	444	88	494	82
45	96	95	87	145	79	195	74	245	78	295	85	345	80	395	75	445	82	495	80
46	86	96	95	146	85	196	85	246	80	296	75	346	76	396	72	446	68	496	87
47	90	97	84	147	84	197	76	247	84	297	82	347	80	397	75	447	68	497	68
48	95	98	82	148	83	198	87	248	79	298	73	348	82	398	75	448	73	498	81
49	89	99	87	149	83	199	96	249	88	299	73	349	77	399	82	449	70	499	72
50	98	100	87	150	91	200	77	250	80	300	78	350	82	400	81	450	80	500	81

501 78	551 79	601 75	651 61	701 75	751 68	801 85	851 70	901 74	951 76
502 74	552 75	602 73	652 74	702 71	752 85	802 66	852 77	902 73	952 70
503 67	553 71	603 83	653 85	703 81	753 73	803 70	853 74	903 70	953 78
504 76	554 80	604 76	654 69	704 71	754 71	804 69	854 66	904 63	954 65
505 76	555 77	605 73	655 78	705 87	755 83	805 78	855 71	905 81	955 73
506 83	556 61	606 74	656 73	706 68	756 70	806 79	856 73	906 70	956 76
507 76	557 88	607 72	657 71	707 82	757 66	807 68	857 78	907 80	957 58
508 71	558 68	608 78	658 70	708 74	758 68	808 70	858 76	908 80	958 69
509 76	559 74	609 78	659 79	709 77	759 79	809 69	859 69	909 79	959 77
510 75	560 77	610 80	660 73	710 77	760 77	810 78	860 71	910 82	960 69
511 72	561 86	611 73	661 83	711 78	761 77	811 78	861 77	911 62	961 68
512 82	562 61	612 71	662 70	712 76	762 80	812 72	862 74	912 81	962 88
513 70	563 83	613 76	663 74	713 72	763 68	813 69	863 83	913 71	963 71
514 77	564 67	614 79	664 77	714 73	764 79	814 72	864 60	914 54	964 74
515 81	565 77	615 71	665 77	715 66	765 72	815 78	865 80	915 73	965 74
516 66	566 78	616 75	666 77	716 83	766 82	816 69	866 80	916 70	966 70
517 85	567 72	617 85	667 73	717 69	767 78	817 75	867 68	917 72	967 73
518 83	568 72	618 81	668 73	718 65	768 68	818 75	868 78	918 79	968 66
519 76	569 71	619 67	669 66	719 67	769 77	819 62	869 80	919 75	969 75
520 78	570 80	620 73	670 74	720 74	770 74	820 83	870 73	920 71	970 73
521 73	571 85	621 77	671 75	721 78	771 77	821 75	871 79	921 72	971 76
522 83	572 72	622 70	672 76	722 77	772 75	822 72	872 58	922 72	972 78
523 79	573 85	623 74	673 76	723 73	773 70	823 84	873 76	923 72	973 74
524 69	574 72	624 75	674 77	724 86	774 76	824 78	874 65	924 81	974 63
525 77	575 70	625 68	675 69	725 75	775 72	825 71	875 75	925 76	975 85
526 79	576 77	626 69	676 75	726 69	776 67	826 81	876 80	926 80	976 70
527 84	577 78	627 70	677 74	727 76	777 70	827 78	877 75	927 74	977 66
528 72	578 77	628 70	678 63	728 75	778 76	828 69	878 67	928 63	978 60
529 70	579 76	629 71	679 82	729 76	779 81	829 69	879 68	929 70	979 80
530 78	580 77	630 75	680 83	730 75	780 71	830 68	880 75	930 80	980 65
531 80	581 73	631 67	681 75	731 69	781 70	831 76	881 80	931 69	981 67
532 68	582 79	632 81	682 78	732 76	782 82	832 79	882 69	932 69	982 75
533 79	583 73	633 77	683 66	733 71	783 68	833 82	883 72	933 76	983 70
534 74	584 78	634 70	684 78	734 75	784 74	834 68	884 73	934 68	984 70
535 72	585 72	635 82	685 72	735 74	785 75	835 67	885 69	935 81	985 74
536 71	586 81	636 78	686 74	736 79	786 77	836 73	886 77	936 68	986 76
537 87	587 79	637 73	687 74	737 69	787 70	837 71	887 76	937 71	987 76
538 67	588 87	638 74	688 82	738 78	788 73	838 64	888 71	938 71	988 63
539 78	589 73	639 59	689 74	739 70	789 80	839 80	889 77	939 72	989 71
540 71	590 68	640 72	690 79	740 81	790 68	840 69	890 68	940 68	990 72
541 73	591 71	641 77	691 60	741 67	791 78	841 70	891 68	941 74	991 71
542 77	592 67	642 71	692 79	742 74	792 71	842 69	892 80	942 79	992 79
543 78	593 80	643 68	693 77	743 73	793 82	843 83	893 69	943 72	993 65
544 81	594 77	644 70	694 73	744 67	794 71	844 68	894 72	944 76	994 68
545 68	595 78	645 86	695 76	745 64	795 73	845 78	895 74	945 73	995 78
546 68	596 77	646 75	696 77	746 67	796 79	846 70	896 80	946 66	996 69
547 73	597 79	647 74	697 73	747 76	797 77	847 69	897 64	947 72	997 69
548 76	598 73	648 79	698 79	748 71	798 72	848 77	898 75	948 66	998 83
549 77	599 72	649 73	699 62	749 76	799 71	849 75	899 76	949 67	999 74
550 78	600 73	650 84	700 72	750 72	800 81	850 68	900 61	950 75	1000 65

1000000 . . . 1100000

	0	1	2	3	4	5	6	7	8	9	
1	1										1
2		1				1		1	1		4
3		4	2	2	3	1	2	3	3	1	21
4	2	8	5	4	3	6	9	4	5	8	54
5	11	10	8	18	12	10	10	12	15	8	114
6	14	14	18	21	16	22	19	15	17	15	171
7	26	17	23	23	24	24	17	22	20	21	217
8	19	19	21	7	14	15	20	17	15	17	164
9	11	13	9	13	14	14	12	13	11	16	126
10	8	6	8	5	9	5	5	9	7	9	71
11	6	6	4	6	3	1	3	1	4	5	39
12	1	1	2	1	1	1	2	2	1		12
13	1	1			1		1	1	1		6
14											
15											
16											
	752	719	732	700	731	698	713	722	706	737	7210

$$\int \frac{\mathrm{d}x}{\log x} = 7212{,}99$$

1100000 . . . 1200000

	0	1	2	3	4	5	6	7	8	9	
0											0
1					1						1
2			1				1	1		2	5
3	4	3	3	3	3	3	3	2		1	25
4	5	6	7	5	9	4	4	5	6	6	57
5	8	13	10	12	11	11	9	12	12	9	107
6	14	20	17	20	17	17	18	16	17	14	170
7	21	19	22	19	21	21	20	18	29	27	217
8	22	13	10	12	18	20	17	19	9	20	160
9	13	14	16	17	7	11	16	14	12	11	131
10	9	6	10	10	8	9	6	8	3	8	77
11	1	4	2	2	2	1	4	5	9	2	32
12	1	1	1		2	3	1		2		11
13	1	1	1				1		1		5
14	1				1						2
	736	710	716	713	697	725	729	723	735	710	7194

$$\int \frac{\mathrm{d}x}{\log x} = 7165{,}911$$

1200000 . . . 1300000

	0	1	2	3	4	5	6	7	8	9	
0											
1								1	1		2
2	2		2	1						1	6
3	3	2	4	5	4	3	1	4	3	3	32
4	7	7	7	3	5	7	12	2	3	10	63
5	15	12	12	15	10	14	9	15	6	12	120
6	16	14	13	19	17	16	16	15	20	14	160
7	24	15	25	24	21	20	15	22	24	24	214
8	17	19	16	11	17	15	22	18	19	14	168
9	8	12	7	10	12	13	14	13	13	9	111
10	3	11	10	8	10	4	5	3	9	10	73
11	3	6	3	2	3	5	3	6	1	3	35
12	1	1	1			1	3	1	1		9
13	1	1		1		2					5
14				1							1
16					1						1
	676	744	693	693	724	713	718	709	722	689	7081

$$\int \frac{\mathrm{d}x}{\log x} = 7123{,}35$$

1300000 . . . 1400000

	0	1	2	3	4	5	6	7	8	9	
1						1					1
2		1	1		1	1	1	2	1	1	9
3	3	1	1	3	2	2	2		5		19
4	3	10	7	11	6	8	7	6	6	5	69
5	17	13	11	11	15	12	8	8	14	10	119
6	15	14	17	14	20	18	23	17	16	19	173
7	22	18	26	18	21	16	16	28	19	23	207
8	14	22	14	16	14	13	21	17	15	15	161
9	17	11	12	14	12	9	12	7	13	13	120
10	5	6	2	11	5	15	5	8	6	7	70
11	4	2	7	1	1	3	3	6	3	3	33
12		1	2	1	2	2	2	1	1	3	15
13		1			1				1		3
14										1	1
	709	702	713	705	692	713	709	723	695	737	7098

$$\int \frac{\mathrm{d}x}{\log x} = 7084{,}48$$

1400000 . . . 1500000

	141	142	143	144	145	146	147	148	149	150	
0											0
1			1		1	1	1			1	5
2		1	1		2				2	1	7
3	3	3	0	2	1	2	2	4	2	0	19
4	8	8	8	4	6	7	9	9	5	8	72
5	17	9	7	14	13	11	14	15	16	13	129
6	21	23	20	18	20	19	11	16	16	19	183
7	17	23	18	18	13	24	18	11	15	22	179
8	12	16	28	17	24	14	17	18	23	14	183
9	12	11	4	15	6	10	13	12	7	8	98
10	7	2	7	7	9	7	8	9	8	9	73
11	2	2	2	4	2	3	6	5	4	4	34
12	1	2	3	1	2	2	1	1	2	1	16
13			1		1						2
	679	680	717	723	703	701	716	705	706	698	7028

$$\int \frac{\mathrm{d}x}{\log x} = 7048{,}78186$$

1500000 . . . 1600000

	151	152	153	154	155	156	157	158	159	160	
0											0
1						1	1				2
2			1	1	2		2		1	3	10
3	2		4	2	2	3	5	3	6	1.	28
4	8	5	5	7	9	13	6	10	7	7	77
5	8	19	9	13	11	9	12	15	11	17	124
6	16	20	25	21	20	12	26	14	23	22	199
7	19	21	18	19	18	15	12	19	11	20	172
8	19	12	15	18	15	17	10	17	15	11	149
9	16	14	16	12	8	17	15	6	11	9	124
10	8	3	5	4	9	7	5	10	10	2	63
11		5	2	2	3	3	3	2	4	5	29
12	4			1	3	1	1	4	1	2	17
13		1				2	2			1	6
	731	702	691	686	698	714	680	701	693	675	6971

$$\int \frac{\mathrm{d}x}{\log x} = 7015{,}78776$$

1600000 . . . 1700000

	161	162	163	164	165	166	167	168	169	170	
0								1			1
1						2					2
2	1	3	1		1	1	2			2	11
3	3	3	3	4	4	2	2	4	4		29
4	7	4	9	7	7	10	4	4	10	6	68
5	10	11	8	12	11	11	13	12	18	14	120
6	18	22	15	19	15	11	14	19	10	16	159
7	22	15	14	21	25	18	22	24	24	18	203
8	14	23	25	15	17	16	17	15	13	19	174
9	8	12	18	12	12	21	12	8	14	13	130
10	7	2	5	8	4	6	11	7	4	9	63
11	7	3	1	1	3	1	3	2	2	3	26
12	2	1	1	1				4			9
13	1				1				1		3
14		1									1
15						1					1
	719	694	710	692	692	700	716	702	675	712	7012

$$\int \frac{\mathrm{d}x}{\log x} = 6985{,}13714$$

1700000 . . . 1800000

	171	172	173	174	175	176	177	178	179	180	
0											0
1				1							1
2	1					2	1			1	5
3	3	4		3	3	4	3	5	3	2	30
4	7	9	6	6	5	8	6	6	10	7	70
5	13	15	19	16	12	15	21	13	13	15	152
6	17	16	22	22	20	14	15	13	18	17	174
7	23	21	22	15	22	19	19	21	17	15	194
8	11	16	11	15	16	15	13	18	19	13	147
9	18	11	8	11	15	10	12	14	10	15	124
10	3	1	8	7	2	9	6	9	5	11	61
11	1	3	3	1	3	4	4	1	4	2	26
12	2	3		1	1				1	2	10
13	1	1	1	2							5
14											
15											1
	695	685	691	689	706	684	679	700	689	713	6931

$$\int \frac{\mathrm{d}x}{\log x} = 6956{,}53562$$

1800000 . . . 1900000

	181	182	183	184	185	186	187	188	189	190	
0											
1											
2	1	1	2	1		2				3	10
3	3	2	1	5	1	1	1	2	3	3	22
4	6	5	10	12	7	6	5	5	8	7	71
5	14	15	10	11	11	12	19	17	12	14	135
6	13	20	14	15	21	19	16	19	23	15	175
7	25	26	18	17	21	21	20	22	19	17	206
8	15	19	13	18	22	15	19	15	11	14	161
9	10	7	19	13	9	8	10	12	10	15	113
10	9	4	8	6	6	13	4	6	8	10	74
11	2		4			3	5	2	5	2	23
12	2	1	1	2	2		1		1		10
13											
14											
	704	672	718	674	700	707	703	689	697	691	6955

$$\int \frac{\mathrm{d}x}{\log x} = 6929{,}73917$$

1900000 . . . 2000000

	191	192	193	194	195	196	197	198	199	200	
0											
1	1										1
2			1			1	2		1		5
3	4	3	1	2	10	1	3	4	4	2	34
4	5	4	4	6	4	9	7	10	11	7	67
5	12	18	15	18	11	12	11	16	11	12	136
6	19	20	18	16	17	24	20	20	18	10	182
7	21	20	23	27	20	16	25	17	21	31	221
8	16	10	16	14	14	18	17	15	8	20	148
9	15	14	8	8	9	12	8	8	15	6	103
10	5	6	8	6	11	4	5	5	6	6	62
11	2	4	6	2	3	2	1	3	2	5	30
12		1		1				2	1		5
13					1		1		1		3
14						1			1	1	3
	689	697	711	683	692	685	673	670	688	714	6902

$$\int \frac{\mathrm{d}x}{\log x} = 6904{,}54424$$

2000000 . . . 2100000

	201	202	203	204	205	206	207	208	209	210	
0											
1					2	1					3
2			2	2	1			2	2	1	10
3	3	3	5	2	2	3	4	5	2	3	32
4	7	8	9	4	8	5	6	7	9	6	69
5	13	10	9	15	13	10	12	13	9	15	119
6	25	20	13	16	26	23	25	14	17	18	197
7	10	22	23	25	13	23	18	23	25	22	204
8	13	17	15	22	12	13	12	16	18	19	157
9	16	15	11	4	11	12	11	14	11	10	115
10	10	2	8	6	11	7	7	3	3	6	63
11	2	1	5	3		1	3	3	3		21
12		2			1	2	2		1		8
13	1			1							2
	705	691	693	690	671	696	694	674	686	674	6874

$$\int \frac{\mathrm{d}x}{\log x} = 6880{,}780$$

2100000 . . . 2200000

	211	212	213	214	215	216	217	218	219	220	
0											
1		1					1				2
2	1	1	1			1	1	1	1	2	9
3	5	3	3	1	4		2	3	2	4	27
4	7	7	2	13	5	3	9	6	9	8	69
5	12	14	20	16	16	12	17	13	12	14	146
6	12	20	17	14	16	25	16	23	21	19	183
7	19	14	18	23	26	22	18	22	22	17	201
8	22	21	20	20	12	16	20	10	12	15	168
9	12	10	8	7	9	10	7	13	16	17	109
10	6	5	6	2	7	7	8·	5	2	4	52
11	3	2	3	1	4	2	1		2		18
12	1	1	1	1	1	2		2			9
13		1	1	1					1		4
14				1				2			3
	699	683	697	673	693	712	666	691	679	664	6857

$$\int \frac{\mathrm{d}x}{\log x} = 6858{,}292$$

2200000 . . . 2300000

	221	222	223	224	225	226	227	228	229	230	
1					1				1		2
2			1	1		2			3	2	9
3	5	2	4	7	2	1	2	2	2	2	29
4	8	9	5	5	10	7	7	7	6	9	73
5	12	24	16	13	11	10	14	14	15	9	138
6	17	18	12	18	18	20	16	17	21	22	179
7	19	17	25	21	18	20	23	25	19	18	205
8	12	12	19	15	18	24	13	17	16	22	168
9	14	9	6	9	19	11	16	9	13	7	113
10	7	6	6	6	1	3	7	5		3	44
11	5	2	4	4	2	2	2	2	2	5	30
12	1	1	2	1				2	2	1	10
	701	660	695	680	683	688	701	694	662	685	6849

$$\int \frac{\mathrm{d}x}{\log x} = 6836{,}977$$

2300000 . . . 2400000

	231	232	233	234	235	236	237	238	239	240	
1	1	1	1		1						4
2			1		2	2	1	2	1	2	11
3	4	1	2	3	4	3	2	6	4	3	32
4	8	12	10	9	8	7	3	13	7	9	86
5	13	18	13	14	17	12	10	13	10	16	136
6	15	16	21	20	16	21	26	11	14	16	176
7	22	25	20	20	13	16	26	18	19	15	194
8	13	9	16	21	17	15	15	15	21	16	158
9	13	9	6	7	14	14	8	13	14	14	112
10	7	5	3	2	5	5	8	7	8	5	55
11	3	3	4	3	3	5	1	2	2	2	28
12	1		3	1·						2	7
13		1									1
	690	662	672	671	666	690	691	660	705	680	6787

$$\int \frac{\mathrm{d}x}{\log x} = 6816{,}706$$

2400000 . . . 2500000

	241	242	243	244	245	246	247	248	249	250	
1									1		1
2	2						1	1	2	3	9
3	4	6	4	4	1	5	3	5	3	2	37
4	12	8	7	7	9	7	10	8	6	4	78
5	13	14	17	19	15	12	18	11	11	17	147
6	18	16	21	20	18	22	18	18	20	22	193
7	21	16	19	20	17	17	21	22	19	17	189
8	10	16	14	14	21	17	10	17	16	16	151
9	8	13	9	11	7	12	6	11	12	13	102
10	9	6	5	4	6	4	8	6	7	3	58
11	2	4	3	1	4	1	4	1	2	1	23
12	1		1		1	1	1			2	7
13		1			1	2			1		5
	660	690	672	657	701	687	666	672	687	674	6766

$$\int \frac{\mathrm{d}x}{\log x} = 6797{,}394$$

2500000 . . . 2600000

	251	252	253	254	255	256	257	258	259	260	
1		1	1							1	3
2	1	2		1	1						5
3	4		6	6	2	2	1	2	8	4	35
4	7	18	9	7	8	6	10	7	8	8	88
5	10	11	7	15	15	23	16	16	10	13	136
6	22	14	20	21	20	15	18	19	20	25	194
7	24	17	12	20	22	22	23	15	13	12	180
8	18	15	20	9	16	18	16	20	19	19	170
9	8	10	13	7	9	7	6	12	6	10	88
10	2	5	8	10	5	4	7	4	9	4	58
11	1	5	3	2	2	1	2	3	5		24
12	1	1	1	2		2	1	2	1	2	13
13	2	1							1	2	6
	677	675	696	670	670	671	678	698	693	676	6804

$$\int \frac{\mathrm{d}x}{\log x} = 6778{,}960$$

2600000 . . . 2700000

	261	262	263	264	265	266	267	268	269	270	
0				1							1
1			2					2			4
2	1	2	1		2		1	2	1		10
3	3	6	2	2	4		3	3	3	2	28
4	9	6	6	12	3	7	7	8	6	7	71
5	11	15	14	11	13	17	22	16	18	21	158
6	26	17	14	18	23	19	20	24	19	15	195
7	23	11	27	20	21	21	21	14	22	21	201
8	14	23	16	13	15	16	12	8	12	13	142
9	9	10	13	16	10	10	5	10	5	8	96
10	3	6	5	4	2	8	2	5	8	10	53
11	1	1		1	3	1	4	4	5	2	22
12		3		2	4	1	1	4	1	1	17
13							1				1
14							1				1
	653	681	672	680	689	695	660	665	681	686	6762

$$\int \frac{\mathrm{d}x}{\log x} = 6761{,}332$$

2700000 . . . 2800000

	271	272	273	274	275	276	277	278	279	280	
1						1			1		2
2	2		2			2			1		7
3	4	5	6	5	4	4	4	3	3	5	43
4	9	7	16	7	8	9	8	8	12	11	95
5	10	14	13	14	13	12	13	17	11	18	135
6	24	18	15	28	19	20	15	21	18	17	195
7	18	22	15	20	24	16	23	19	22	9	188
8	13	10	13	12	15	13	20	19	15	15	145
9	9	9	10	4	11	12	9	7	8	8	87
10	6	9	6	7	5	8	7	2	7	10	67
11	3	3	4	2		2		3	1	6	24
12	1	3		1	1	1			1	1	9
13							1	1			2
14											
15											
16											
17	1										1
	679	695	644	657	672	671	684	666	662	684	6714

$$\int \frac{\mathrm{d}x}{\log x} = 6744{,}430$$

2800000 . . . 2900000

	281	282	283	284	285	286	287	288	289	290	
1					1		1				2
2		2	4		5	2		1	1		15
3	2	4	4	3	4	3	1	3	2	4	30
4	9	7	6	9	7	8	10	11	10	8	85
5	14	7	14	14	7	16	19	16	18	15	140
6	18	17	20	13	23	18	16	18	15	21	179
7	24	22	21	20	20	27	22	23	21	22	222
8	13	18	9	20	13	12	9	12	12	14	132
9	10	17	12	12	8	6	14	9	10	11	109
10	7	4	6	3	5	7	5	5	8	3	53
11		1	3	3	5		1	2	1	2	18
12	2	1				1	2		2		8
13			1	2	2						5
14	1			1							2
	690	695	667	704	671	654	672	653	676	662	6744

$$\int \frac{\mathrm{d}x}{\log x} = 6728{,}220$$

2900000 . . . 3000000

	291	292	293	294	295	296	297	298	299	300	
1		1							1		2
2		1	2	1	2	2		1	1	3	13
3	3	3	5	2	8	6	4	4	5	4	44
4	7	7	6	6	7	9	6	6	6	4	64
5	20	11	14	18	12	15	17	19	16	11	153
6	17	21	22	18	18	16	11	26	21	17	187
7	19	30	18	22	22	25	27	13	15	23	214
8	14	11	12	12	17	11	13	11	14	19	134
9	10	9	12	13	9	6	12	12	9	11	103
10	6	4	5	6	3	6	8	7	9	4	58
11	2	1	3	1		2	1		1	4	15
12	2	1		1	2	2		1	2		11
13			1								1
14											
15							1				1
	680	663	671	680	649	652	694	658	671	687	6705

$$\int \frac{\mathrm{d}x}{\log x} = 6712{,}64$$

1000000 . . . 2000000

	110	120	130	140	150	160	170	180	190	200	
0							1				1
1	1	1	2	1	5	2	2	1		1	16
2	4	5	6	9	7	10	11	5	10	5	72
3	21	25	32	19	19	28	29	30	22	34	259
4	54	57	63	69	72	77	68	70	71	67	668
5	114	107	120	119	129	124	120	152	135	136	1256
6	171	170	160	173	183	199	159	174	175	182	1746
7	217	217	214	207	179	172	203	194	206	221	2030
8	164	160	168	161	183	149	174	147	161	148	1615
9	126	131	111	120	98	124	130	124	113	103	1180
10	71	77	73	70	73	63	63	61	74	62	687
11	39	32	35	33	34	29	26	26	23	30	307
12	12	11	9	15	16	17	9	10	10	5	114
13	6	5	5	3	2	6	3	5		3	38
14		2	1	1			1			3	8
15							1	1			2
16			1								1
	7210	7194	7081	7098	7028	6971	7012	6931	6955	6902	70382

$$\int \frac{\mathrm{d}x}{\log x} = 70427{,}78$$

2000000 . . . 3000000

	210	220	230	240	250	260	270	280	290	300	
0							1				1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	11	9	5	10	7	15	13	98
3	32	27	29	32	37	35	28	43	30	44	337
4	69	69	73	86	78	88	71	95	85	64	778
5	119	146	138	136	147	136	158	135	140	153	1408
6	197	183	179	176	193	194	195	195	179	187	1878
7	204	201	205	194	189	180	201	188	222	214	1998
8	157	168	168	158	151	170	142	145	132	134	1525
9	115	109	113	112	102	88	96	87	109	103	1034
10	63	52	44	55	58	58	53	67	53	58	561
11	21	18	30	28	23	24	22	24	18	15	223
12	8	9	10	7	7	13	17	9	8	11	99
13	2	4		1	5	6	1	2	5	1	27
14		3					1		2		6
15										1	1
16											
17								1			1
	6874	6857	6849	6787	6766	6804	6762	6714	6744	6705	67862

Die Hundertergruppe an Position 26379 enthält keine Primzahl
Die Hundertergruppe an Position 27050 enthält 17 Primzahlen.

$$\int \frac{\mathrm{d}x}{\log x} = 67915{,}733$$

GAUSS AN ENKE.

Hochverehrter Freund!

— — Ihre freundlich mitgeteilten Bemerkungen über die Häufigkeit der Primzahlen waren für mich in mehr als einer Hinsicht interessant. Sie haben mich an meine eigenen Arbeiten zu diesem Gegenstand erinnert, deren erste Anfänge weit zurückliegen, im Jahr 1792 oder 1793, als ich mir Lamberts Supplemente zu den Logarithmentafeln angeschafft hatte. Noch bevor ich mich mit feineren Untersuchungen der höheren Arithmetik beschäftigt hatte, gehörte es zu meinen ersten Aufgaben, meine Aufmerksamkeit auf die abnehmende Häufigkeit der Primzahlen zu richten. Dazu zählte ich sie in den einzelnen Tausendergruppen und verzeichnete die Ergebnisse auf einem der angehefteten weißen Blätter. Ich erkannte bald, dass diese Häufigkeit trotz aller Schwankungen im Durchschnitt annähernd umgekehrt proportional zum Logarithmus sei, sodass die Anzahl aller Primzahlen unter einer gegebenen Grenze n annähernd durch das Integral

$$\int \frac{\mathrm{d}n}{\log n}$$

ausgedrückt werde, wobei der natürliche Logarithmus gemeint ist. Als ich später die in Vegas Tafeln (von 1796) abgedruckte Liste bis 400031 kennenlernte, dehnte ich meine Zählung weiter aus, was dieses Verhältnis bestätigte. Große Freude bereitete mir 1811 das Erscheinen von Chernacs cribrum, und ich verwendete sehr oft einzelne freie Viertelstunden darauf, bald hier, bald dort eine Tausendergruppe abzuzählen (da ich zu einer anhaltenden Zählung der Reihe nach keine Geduld hatte); schließlich ließ ich es jedoch ganz liegen, ohne mit der Million ganz fertig zu werden. Erst später machte ich mir Goldschmidts Fleiß zunutze, teils um die verbliebenen Lücken in der ersten Million zu füllen, teils um die Zählung nach Burckhardts Tafeln fortzusetzen So sind (nun schon seit vielen Jahren) die ersten drei Millionen abgezählt und mit dem Integralwert verglichen. Ich gebe hier nur einen kleinen Auszug:

Unter	gibt es Primzahlen	Integral $\int \frac{\mathrm{d}n}{\log n}$	Abweich.	Ihre Formel	Abweich.
500000	41556	41606,4	+50,4	41596,9	+40,9
1000000	78501	79627,5	+126,5	78672,7	+171,7
1500000	114112	114263,1	+151,1	114374,0	+264,0
2000000	148883	149054,8	+171,8	149233,0	+350,0
2500000	183016	183245,0	+229,0	183495,1	+479,1
3000000	216745	216970,6	+225,6	217308,5	+563,5

Dass sich auch Legendre mit diesem Gegenstand beschäftigt hatte, war mir nicht bekannt. Ihr Brief veranlasste mich, in seiner *Théorie des Nombres* nachzusehen, und ich fand in der zweiten Ausgabe einige darauf bezogene Seiten, die ich früher übersehen (oder seitdem vergessen) haben muss. Legendre verwendet die Formel

$$\frac{n}{\log n - A}$$

wobei A eine Konstante sein soll, für die er 1,08366 setzt. Nach einer flüchtigen Rechnung finde ich damit in den obigen Fällen die Abweichungen

$$\begin{array}{r} -23{,}3 \\ +42{,}2 \\ +68{,}1 \\ +92{,}8 \\ +159{,}1 \\ +167{,}6 \end{array}$$

Diese Differenzen sind noch kleiner als die mit dem Integral, scheinen aber bei zunehmendem n schneller zu wachsen als diese, sodass es durchaus möglich wäre, dass jene bei einer viel weiteren Fortsetzung die letzteren überträfen. Um Zählung und Formel in Übereinstimmung zu bringen, müsste man jeweils statt $A = 1{,}08366$ setzen

$$\begin{array}{c} 1{,}09040 \\ 1{,}07682 \\ 1{,}07582 \\ 1{,}07529 \\ 1{,}07179 \\ 1{,}07297 \end{array}$$

Es scheint, dass bei wachsendem n der (Durchschnitts-)Wert von A abnimmt. Ob aber der Grenzwert, wenn n ins Unendliche wächst, 1 oder eine von 1 verschiedene Größe sein wird, darüber wage ich keine Vermutung. Ich kann nicht sagen, dass es einen Grund gibt, einen ganz einfachen Grenzwert zu erwarten; andererseits könnte der Überschuss von A über 1 durchaus eine Größe der Ordnung $\frac{1}{\log n}$ sein. Ich wäre geneigt zu glauben, dass das Differential der betreffenden Funktion einfacher sein muss als die Funktion selbst.

Während ich dafür $\frac{\mathrm{d}n}{\log n}$ angenommen habe, würde Legendres Formel eine Differentialfunktion voraussetzen, die etwa $\frac{\mathrm{d}n}{\log n-(A-1)}$ wäre. Ihre Formel könnte übrigens für ein sehr großes n als übereinstimmend mit

$$\frac{n}{\log n - \frac{1}{2k}}$$

betrachtet werden, wobei k der Modul der Briggsschen Logarithmen ist, also mit Legendres Formel, wenn

$$A = \tfrac{1}{2k} = 1{,}1513 \text{ gesetzt wird.}$$

Schließlich will ich noch bemerken, dass ich zwischen Ihren Zählungen und meinen ein paar Unterschiede bemerkt habe.

Zwischen	59000	und	60000	haben Sie	95	ich	94
	101000		102000		94		93

Der erste Unterschied liegt vielleicht daran, dass in Lamberts Supplementen die Primzahl 59023 zweimal aufgeführt ist. Die Tausendergruppe von 101000—102000 wimmelt in Lamberts Supplementen von Fehlern; in meinem Exemplar habe ich 7 Zahlen markiert, die keine Primzahlen sind, und hingegen 2 fehlende eingefügt. Könnten Sie nicht den jungen Dase dazu veranlassen, die Primzahlen in den folgenden Millionen aus den Tafeln bei der Akademie abzuzählen, die, wie ich fürchte, das Publikum nicht besitzen soll? Für diesen Fall bemerke ich, dass die Zählung in der 2. und 3. Million auf meine Anweisung nach einem besonderen Schema vorgenommen wurde, das ich selbst auch schon bei einem Teil der ersten Million angewandt hatte. Die Zählungen für jeweils 100000 stehen auf einer (kleinen) Oktavseite in 10 Spalten, von denen sich jede auf eine Zehntausendergruppe bezieht; dazu kommt noch eine Spalte davor (links) und eine dahinter rechts. Als Beispiel folgt hier eine senkrechte Spalte mit den beiden Zusatzspalten aus dem Intervall 1000000 . . . 1100000 — — —

Zur Erläuterung diene zum Beispiel die 1. senkrechte Spalte. In der Zehntausendergruppe von 1000000 bis 1010000 liegen 100 Hundertergruppen; darunter ist 1, die nur eine Primzahl enthält; gar keine mit 2 oder 3; 2 mit je 4 Primzahlen; 11 mit je 5 usw. Alle zusammen ergeben $752 = 1.1+4.2+5.11+6.14+..$ Die letzte Spalte enthält die Summen aus den 10 einzelnen Spalten. Die Zahlen 14. 15. 16 in der ersten senkrechten Spalte sind hier überflüssig, da keine Hundertergruppen mit so vielen Primzahlen vorkommen; auf den folgenden Blättern kommen sie aber zur Anwendung. Zuletzt werden die 10 Seiten wieder zu 1 vereinigt und umfassen so die ganze 2. Million.

Doch es ist Zeit abzubrechen. — — — Mit herzlichen Wünschen für Ihr Wohlbefinden

Stets der Ihrige

Göttingen, 24. Dezember 1849. C. F. Gauss.

TAFEL
DER ANZAHL DER KLASSEN
BINÄRER QUADRATISCHER FORMEN.

Hundertergruppe 1.
G. I. . . .(17). .(61)
1. 1. 2. 3.
4. 7
3 11. 19. 23.
27. 31. 43.
67
5 47. 79
7 71
9 59. 83
G. II. .(58). .(280)
1 5. 6. 8.
9. 10. 12.
13. 15. 16.
18. 22. 25.
28. 37. 58.
2 14. 17. 20.
32. 34. 36.
39. 46. 49.
52. 55. 63.
64. 73. 82.
97. 100
3 26. 29. 35.
38. 44. 50.
51. 53. 54.
61. 75. 76.
81. 87. 91.
92. 99
4 41. 62. 68.
94. 95. 98
5 74. 86
6 89
G. IV. .(25). .(136)
1 21. 24. 30.
33. 40. 42.
45. 48. 57.
60. 70. 72.
78. 85. 88.
93
2 56. 65. 66.
69. 77. 80.
84. 90. 96

Summe 233. . .477
Irreg. 0 Impr. 74

Hundertergruppe 2.
G. I. . . . .(11). .(101)
3 163
5 103. 127
7 151
9 107. 139. 199
11 167
13 191
15 131. 179
G. II. . . . .(46). .(406)
2 142. 148. 193
3 106. 108. 109.
115. 118. 121.
123. 124. 135.
147. 157. 162.
169. 172. 175.
187
4 111. 113. 128.
137. 158. 178.
183. 196
5 119. 122. 125.
143. 159. 166.
181. 188. 197
6 116. 155. 171
7 101. 134. 149.
173
8 146. 164
10 194
G. IV. . . .(39). .(356)
1 102. 112. 130.
133. 177. 190
2 114. 117. 126.
132. 136. 138.
141. 144. 145.
150. 153. 154.
156. 160. 180.
184. 192. 198
3 104. 110. 129.
140. 152. 170.
174. 176. 182.
186. 189. 195.
200
4 161. 185
G. VIII. . .(4). . .(32)
1 105. 120. 165.
168

Summe 291. . .895
Irreg. 0

Hundertergruppe 3.
G. I. . . . . (9). . . . . (109)
7 223
9 211. 243(*3*). 283
11 271
13 263
15 227. 239
21 251
G. II. . . . . (42). . . . . (482)
3 202. 207. 214. 235. 247. 262. 267. 268. 277. 298
4 226. 256. 289. 292. 295
5 218. 229. 242. 250
6 203. 212. 219. 233. 241. 244. 259. 274. 275. 279. 291
7 215. 278. 284. 287
8 254. 257
9 236. 293
10 206. 281
11 269
12 299
G. IV. . . . . (43). . . . . (512)
1 232. 253
2 205. 208. 213. 217. 220. 225. 228. 238. 252. 258. 265. 282. 288
3 201. 204. 216. 222. 231. 234. 237. 245. 246. 249. 255. 261. 270. 286. 294. 297. 300
4 221. 224. 248. 260. 272. 276
5 209. 230. 266. 290. 296
G. VIII. . . . (6). . . . . (64)
1 210. 240. 273. 280.
2 264. 285

Summe 313. 1167
Irreg. 1 Impr. 183.

Hundertergruppe 4.
G. I. . . . . (9). . . . . (113)
7 343
9 307(*3*). 331. 367. 379
15 347
17 383
19 311. 359
G. II. . . . . (40). . . . . (554)
3 358. 397
4 313. 337. 382. 388
5 303. 316. 317. 319. 346. 361. 373. 375. 394
6 302. 323. 324. 327. 334. 351. 355. 363. 387
7 338. 349. 391
8 353
9 332. 335. 339(*3*). 362
10 386. 398
11 326. 389
12 356. 371. 395
13 314
G. IV. . . . . (43). . . . . (608)
2 301. 310. 322. 328. 333. 340. 352. 372. 400
3 304. 309. 315. 318. 325. 342. 348. 364. 366. 368. 370. 378. 393. 396
4 305. 306. 308. 320. 350. 354. 369. 376. 377. 380. 384. 392. 399
5 321. 344. 365. 381.
6 329
7 341. 374
G. VIII. . . . (8). . . . . (88)
1 312. 330. 345. 357. 385
2 336. 360. 390

Summe 325. 1363
Irreg. 2 Impr. 229

NEGATIVE DETERMINANTEN.

Hundertergruppe 5.
G. I. . . . .(10). .(174)
7 463. 487
9 499
15 439. 443
21 431. 467
25 479
27 419. 491
G. II. . . .(33). .(512)
3 403. 427
4 457. 466. 478
5 412. 415. 421. 422. 423
6 433. 436. 475. 484
7 447. 454
8 407. 409. 452. 471
9 411. 428. 451. 459(*). 486
10 401. 449. 482. 500
13 458
14 404
15 461
16 446
G. IV. . . .(49). .(760)
2 418. 438. 442. 445. 448. 498
3 405. 417. 424. 430. 432. 435. 450. 453. 460. 472. 473. 477. 483. 490. 492. 493. 496
4 402. 406. 410. 414. 441. 444. 468. 469. 481. 485. 495
5 413. 437. 455. 470. 474. 476. 488. 489
6 416. 425. 426. 434. 464. 497
7 494
G. VIII. . .(8). .(120)
1 408. 462
2 420. 429. 456. 465. 480
3 440

Summe 336. . .1566
Irreg. 1

Hundertergruppe 6.
G. I. . . . . .(7). .(133)
9 547
15 523. 571
21 503. 587
25 599
27 563
G. II. . . .(40). .(724)
4 562. 577. 583
5 508. 538. 541
6 507. 526. 529. 543. 567
7 502. 511. 535
8 512. 514. 548. 559. 578
9 515. 519. 527. 531. 556. 557. 575. 586
11 551. 554. 591
12 539. 542. 579. 593
14 596
15 509. 524. 566
16 521. 569
G. IV. . . .(41). .(672)
2 505. 522. 532. 553. 568. 592. 598
3 513. 517. 533. 537. 540. 550. 555. 565. 588. 595. 597
4 501. 518. 544. 558. 564. 573. 574. 576(*2*). 580(*2*). 582. 589
5 534. 572. 590
6 516. 549. 594
7 506. 530. 536. 581
8. . . 545. 584
G. VIII. .(12). .(200)
1 520
2 504. 510. 525. 528. 552. 561. 570. 585. 600
3 546. 560

Summe 347. . .1729
Irreg. 2

Hundertergruppe 7.
G. I. . . . .(8). . .(138)
9 643
13 607. 631
15 619. 683. 691
25 647
33 659
G. II. . . .(37). .(718)
3 652
5 613. 625. 694
6 603. 617. 622. 628. 655. 667. 673. 676. 687
7 604. 634. 639. 653
9 661. 675(*3*). 679
10 601
11 623. 662. 668
12 674. 695
13 698
14 641. 686. 692
16 611. 635. 671. 677. 699
17 614
18 626
G. IV. . . .(43). .(812)
2 658. 697
3 606. 610. 618. 627. 637. 648. 669. 670. 682. 685. 688. 700
4 612. 632. 640. 642. 646. 657. 663
5 615. 633. 636. 638. 649. 664. 666. 678. 681
6 602. 605. 608. 620. 621. 650. 651. 684
7 654
8 644. 656
9 629
10 689
G. VIII. .(12). .(216)
2 609. 616. 624. 630. 645. 660. 672. 690. 693.
3 665. 680. 696.

Summe 350. .1884
Irreg. 1

Hundertergruppe 8.
G. I. . . . . .(6). . .(110)
13 727
15 739. 751. 787
21 743
31 719
G. II. . . . . .(39). . .(860)
4 772
5 709. 757
6 718. 723. 763. 775
7 703. 733. 778
8 799
9 707. 722. 729. 747. 771. 783. 796
10 711. 724. 769. 788
11 758. 767
12 706. 766
13 746. 764. 773
15 716. 779. 797
16 791
17 701
18 731. 755(*3*)
20 734. 761
21 794
G. IV. . . . . .(42). . .(792)
2 708. 742. 793
3 702. 715. 730. 748. 753. 762. 795
4 712. 717. 721. 732. 735. 736. 738. 745. 768. 784. 785. 786. 790
5 726. 737. 750. 752. 754. 774. 781
6 704. 713. 725. 756. 759. 782. 800
8 710. 740. 749. 789
10 776
G. VIII. . . . .(13). . .(264)
1 760
2 720. 765. 777. 792. 798
3 705. 714. 728. 741. 744. 780
4 770

Summe 356. . .2026
Irreg. 1

Hundertergruppe 9.
G. I. . . . . (8). . . . (164)
9 823. 883
21 811. 827. 859. 863.
29 887
33 839
G. II. . . . . (34). . . . (750)
4 862
5 847. 853. 877
6 802. 898
7 807. 838. 841. 892.
8 895
9 835. 843. 844. 867. 886. 891(*3*)
10 878
11 829. 871. 879
13 842
14 818. 831
15 803. 815. 821. 851. 875
16 809. 857
20 881
21 899
22 866
G. IV. . . . (47). . . (1024)
3 808. 813. 814. 817. 826. 828. 837. 856
4 820(*2*). 832. 834. 850. 852. 855. 865. 868. 873. 882. 889. 900(*2*)
5 822. 830. 872. 874
6 801. 804. 810. 812. 819. 833. 848. 864. 876. 890. 894
7 806. 845. 849. 860. 893
8 846. 869. 884(*2*). 896
10 824. 836
11 854
G. VIII. . . (10). . . . (200)
2 805. 858. 870. 880. 897
3 816. 825. 861. 885. 888
G. XVI. . . . (1). . . . (16)
1 840

Summe 360. 2154
Irreg. 4

Hundertergruppe 10.
G. I. . . . . (8). . . . (174)
9 907
11 967
15 947
17 991
19 919
27 983
31 911
45 971
G. II. . . . . (33). . . (810)
5 982
6 955
7 997
8 943. 958. 961
9 922. 931. 963. 972
10 916. 927. 937. 977
12 932. 939. 964. 979. 995. 999
13 934. 951. 998
15 908. 923. 956
16 953
18 914. 929. 959. 974(*3*)
20 926
23 941
G. IV. . . . (45). . . . (976)
2 928
3 913. 918. 925. 933. 940. 942. 949. 970. 973. 988
4 903. 904. 993. 938. 946. 975. 994
5 917. 921. 968. 1000
6 901. 905. 915. 948. 954. 976. 978. 980. 981. 985. 987. 996
7 902. 906. 909. 935. 962
8 992
9 944. 950. 989
11 965. 986
G. VIII. . . (14). . . . (312)
2 910. 912. 952. 957. 960
3 924. 930. 936. 945. 966. 969. 984. 990
5 920

Summe 366. 2272
Irreg. 1

Hundertergruppe 11.
G. I. . . . . (7). . . . . (191)
9 1087
15 1051
19 1063
23 1039
35 1031
39 1019
51 1091
G. II. . . . . (35). . . . (880)
5 1093
6 1003. 1027. 1033. 1042
8 1024. 1047
9 1018. 1059. 1075(*3*). 1083. 1099
10 1006. 1009
11 1021. 1082. 1084
12 1043. 1058
13 1013. 1052. 1061. 1094.
15 1007. 1069
16 1028
17 1079
18 1011. 1055. 1067. 1097
21 1004. 1046
22 1049. 1076
G. IV. . . . . (44). . . . . (984)
2 1012
3 1030. 1038. 1048. 1068 1072. 1090
4 1002. 1015. 1017. 1023. 1054. 1057. 1060. 1078. 1081
5 1037. 1066. 1071. 1098
6 1026. 1035. 1036. 1044. 1053. 1062. 1073. 1077. 1089. 1096. 1100
7 1010. 1014. 1029. 1086. 1095
8 1016. 1022. 1025. 1074. 1088(*2*)
9 1041. 1070
11. . . 1034
G. VIII. . . . . (14). . . . (344)
2 1005. 1008. 1032. 1045. 1065. 1092
3 1020. 1050. 1080
4 1040. 1056. 1085
5 1001. 1064

Summe 365. 2399
Irreg. 2

Hundertergruppe 12.
G. I. . . . . (6). . . . . (148)
15 1123
21 1163. 1171
23 1103
27 1187(*3*)
41 1151
G. II. . . . . (36). . . . (924)
6 1108. 1138. 1198
7 1117. 1183
8 1129. 1153. 1156. 1159
9 1107(*3*). 1132. 1135. 1142. 1147
10 1143
11 1111. 1114. 1126. 1167
12 1127. 1186. 1191. 1195
15 1115. 1174. 1175. 1179
16 1119
18 1172. 1193
19 1199
20 1124
23 1181
24 1139
25 1109
28 1154
G. IV. . . . . (40). . . . (1064)
3 1162. 1177. 1192
4 1149. 1150. 1152. 1168. 1178. 1180
5 1102. 1125. 1137. 1165. 1182. 1189
6 1131. 1134. 1141. 1145. 1158. 1164. 1188
7 1101. 1112. 1133. 1136. 1148. 1157. 1194
8 1146
9 1116. 1118. 1161. 1166
10 1184
11 1121. 1130
12 1106. 1169. 1196
G. VIII. . . . . (18). . . . . (408)
2 1105. 1110. 1113. 1120. 1122. 1128. 1170. 1185. 1197
3 1144. 1155. 1173. 1176 1200
4 1104. 1140
5 1160. 1190

Summe 382. 2544
Irreg. 2

Hundertergruppe 13.
G. I. . . . . .(6). . . . . .(190)
23 1279
27 1231. 1291
33 1283
35 1223
45 1259(*3*)
G. II. . . . . .(38). . . . . .(986)
5 1213
6 1227. 1243. 1255. 1282. 1297
7 1237
8 1201. 1252
9 1203. 1207. 1215. 1219. 1228(*3*). 1267(*3*)
10 1261. 1263. 1268.
12 1202. 1234. 1299
13 1247
14 1294
15 1250
16 1217. 1249
17 1277
18 1251. 1262. 1289
19 1229. 1244
20 1214. 1271
21 1211. 1226. 1238
29 1286
G. IV. . . . . .(40). . . . .(1008)
3 1222. 1258. 1285
4 1204. 1225. 1233. 1246. 1278
5 1210. 1212. 1257. 1264. 1270. 1273. 1276. 1287
6 1208. 1216. 1236. 1242. 1269. 1275. 1292. 1293. 1296. 1300
7 1206
8 1220(*2*). 1239. 1241. 1253. 1266. 1280. 1298
9 1235. 1274. 1295
10 1205. 1284
13 1256
VIII. . . . .(16). . . . . .(416)
2 1240. 1248. 1288. 1290
3 1218. 1230. 1254. 1260. 1272. 1281
4 1221. 1224. 1232. 1245
5 1209. 1265

Summe 370. 2600
Irreg. 4

Hundertergruppe 14.
G. I. . . . . .(7). . . . . .(191)
11 1303
15 1327
27 1367. 1399
33 1307. 1331
45 1319
G. II. . . . . .(32). . . . . .(846)
5 1318
6 1387
7 1372
8 1348
9 1306. 1315(*3*). 1323(*3*). 1324. 1347. 1363. 1366. 1369. 1373. 1383
10 1375
11 1354
12 1321. 1339. 1351
13 1381
14 1346. 1359
15 1388
17 1343
18 1355. 1371
19 1382
21 1322
22 1391
24 1379
25 1301
30 1361
G. IV. . . . . .(46). . . . . .(1340)
4 1312(*2*). 1332(*2*). 1345. 1357. 1393
5 1317. 1333. 1338. 1342. 1378. 1384. 1390. 1398
6 1308. 1313. 1336. 1337. 1350. 1358. 1362. 1377. 1395. 1397
7 1311. 1335. 1341. 1352. 1374. 1389. 1396
8 1314. 1334
9 1310. 1325. 1328. 1329. 1340. 1356(*3*)
10 1376
11 1304. 1370
12 1316. 1385. 1394
14 1349. 1364
G. VIII. . . . . .(13). . . . . .(328)
2 1302. 1353. 1360. 1380
3 1309. 1330. 1368. 1392
4 1305. 1344. 1386. 1400
5 1326
G. XVI. . . . . .(2). . . . . .(32)
1 1320. 1365

Summe 391. 2737
Irreg. 5 Progr. 3192

Hundertergruppe 15.
G. I. . . . . .(10). . . . . .(308)
9 1423
21 1483
23 1447. 1471
33 1459
37 1487
39 1439. 1451. 1499
45 1427
G. II. . . . . .(26). . . . . .(746)
6 1411. 1467
7 1402. 1453
8 1438
9 1458. 1468
10 1444. 1486. 1489. 1492.
11 1429. 1493
15 1431. 1478
16 1412
17 1415. 1418
18 1409. 1433. 1475
19 1436
21 1403
26 1481
29 1466
30 1454
G. IV. . . . . .(49). . . . . .(1348)
3 1432. 1435. 1450
4 1408. 1417. 1422. 1462. 1465. 1474. 1477. 1498
5 1495. 1497. 1500
6 1404. 1405. 1407. 1413. 1420. 1437. 1442. 1443. 1452. 1457. 1472
7 1401. 1414. 1441. 1455. 1461. 1473. 1479
8 1426. 1434. 1446. 1463. 1476
9 1419. 1445. 1448. 1490. 1491
10 1460. 1494
11 1406
12 1421. 1424. 1484
14 1469
G. VIII. . . . .(15). . . . . .(424)
2 1428. 1488
3 1425. 1456. 1464. 1480. 1482. 1485
4 1410. 1416. 1430. 1440(*2*). 1449. 1470
7 1496

Summe 378. 2826
Irreg. 1 Propr. 3282

Hundertergruppe 16.
G. I. . . . . .(9). . . . . .(299)
15 1567
19 1543
21 1523
27 1579
33 1531. 1583
49 1511
51 1559. 1571
G. II. . . . . .(24). . . . . .(656)
6 1507. 1555. 1588
7 1527. 1597
9 1516. 1519. 1549. 1563
10 1522
11 1503. 1591
12 1502. 1587
17 1532. 1546. 1594
18 1539(*3*)
19 1535
20 1553
22 1538. 1556
25 1514
27 1574
G. IV. . . . . .(53). . . . . .(1564)
3 1558. 1593
4 1510. 1513(*2*). 1528. 1537. 1552. 1578. 1582(*2*). 1600(*2*)
5 1534, 1542. 1570. 1573. 1576
6 1501. 1506. 1521. 1525. 1548. 1572. 1575. 1585
7 1557. 1562. 1564. 1565. 1569. 1577
8 1504. 1508. 1536. 1551. 1561. 1568(*2*). 1598
9 1515. 1541. 1547. 1566. 1599
10 1509. 1524. 1544. 1592
11 1586
12 1517. 1526. 1550. 1580. 1595
13 1529. 1589
G. VIII. . . . .(13). . . . . .(360)
2 1540
3 1512. 1518. 1530. 1533. 1545. 1554. 1584
4 1520. 1590(*2*). 1596
5 1505. 1581
G. XVI. . . . . .(1). . . . . .(32)
2 1560

Summe 389. 2911
Irreg. 6 Propr. 3416

Hundertergruppe 17.
G. I. . . . . (6). . . . . (182)
17 1663
21 1627
27 1607
33 1699
39 1667
45 1619
G. II. . . . . (37). . . . (1116)
6 1618
7 1642
8 1657
9 1603. 1621. 1675(*). 1683. 1687
10 1678. 1681. 1684
11 1639. 1654. 1693
12 1647. 1651
13 1669
14 1609. 1623. 1697
15 1611. 1622. 1643. 1682
16 1636
19 1637. 1671
20 1604
21 1613. 1658
22 1631. 1646. 1655
26 1679
27 1676. 1691
28 1601
G. IV. . . . . (41). . . . . (1312)
3 1612
4 1633. 1660. 1698
5 1626. 1648. 1660. 1662. 1688. 1692. 1695
6 1615. 1620. 1635. 1659. 1666. 1668. 1690. 1696
7 1606. 1614. 1630. 1670
8 1602. 1628. 1673
9 1644. 1674. 1689
10 1625. 1629. 1652
11 1641. 1686
12 1649. 1661. 1664. 1694
13 1685
14 1616
16 1634
G. VIII. . . . (15). . . . . (368)
2 1605. 1632. 1645. 1653 1672. 1677
3 1617. 1638
4 1608. 1610. 1624. 1640. 1650. 1656. 1665
G. XVI. . . . . (1). . . . . (32)
2 1680

Summe 380. 3010
Irreg. 1 Impr. 513

Hundertergruppe 18.
G. I. . . . . (5). . . . . (95)
15 1723. 1747
17 1783
21 1787
27 1759
G. II. . . . . (35). . . . . (1182)
10 1714. 1753. 1774
12 1726. 1731. 1732. 1762. 1777. 1795
13 1719. 1735. 1741. 1789
14 1703. 1711. 1775
15 1707. 1756. 1772. 1779
17 1733
18 1727. 1763(*3*). 1791
19 1754
21 1709. 1715. 1724
23 1718
24 1751
25 1766. 1799
26 1721
29 1706
30 1739
G. IV. . . . . (41). . . . . (1260)
3 1708
4 1717. 1737. 1738. 1780. 1792
5 1702. 1750. 1758. 1761. 1765. 1773. 1786. 1798
6 1728. 1743. 1744. 1771. 1782. 1797
7 1757. 1788
8 1764(*2*). 1767
9 1701. 1712. 1713. 1730. 1734. 1755(*). 1793
10 1745. 1746. 1748. 1778. 1796
11 1742
13 1790
16 1769. 1784
17 1781
G. VIII. . . . . (18). . . . . (536)
2 1705. 1710. 1752. 1768
3 1720. 1722. 1729. 1740. 1800
4 1716. 1725. 1776. 1794
5 1749. 1770
6 1704. 1736. 1760
G. XVI. . . . . (1). . . . . (32)
2 1785

Summe 399. 3105
Irreg. 3 Impr. 525

Hundertergruppe 19.
G. I. . . . . (7) . . . . . (263)
15 1867
19 1831
27 1879
43 1847
45 1823. 1871
69 1811
G. II. . . . . (31) . . . . . (994)
6 1807. 1873
7 1852
8 1822. 1828
9 1843. 1863. 1882
10 1858
11 1849
12 1803
14 1801. 1838
15 1819. 1835. 1875. 1891. 1894
17 1877
18 1899
19 1861
20 1839
21 1851. 1859. 1868. 1883
23 1814
24 1895
28 1874
30 1844
36 1889
G. IV. . . . . (45) . . . . . (1416)
4 1813. 1842. 1864. 1897
5 1810. 1857. 1887. 1893
6 1812. 1815. 1818. 1825. 1827. 1837. 1878. 1888. 1892. 1900
7 1816. 1846. 1855. 1898
8 1802. 1808. 1866. 1876. 1884
9 1804. 1809. 1821. 1834. 1836. 1853. 1862
10 1805. 1817. 1829. 1841. 1850. 1854
12 1856. 1865
13 1832
14 1826
16 1886(*2*)
G. VIII. . . . . (16) . . . . . (496)
2 1870. 1885
3 1830. 1833. 1840. 1890
4 1824. 1845. 1860. 1872
5 1806. 1820. 1869. 1880. 1881. 1896
G. XVI. . . . . (1) . . . . . (16)
1 1848

Summe 393. 3185
Irreg. 1 Impr. 513

Hundertergruppe 20.
G. I. . . . . (6) . . . . . (252)
21 1987
27 1999
33 1951.
39 1907
63 1931(*3*)
69 1979
G. II. . . . . (33) . . . . . (1090)
7 1948
8 1983
9 1915. 1927. 1933. 1963. 1996
10 1906. 1975
11 1903. 1942
12 1939. 1982. 1993
14 1954
15 1923
16 ·1922. 1943
18 1913. 1966. 1967. 1971(*3*)
21 1901. 1959. 1973. 1997
22 1919
25 1916
26 1934
27 1964. 1994
28 1991
35 1949
G. IV. . . . . (43) . . . . . (1356)
3 1978
4 1912. 1918(*2*). 1945. 1957
5 1930. 1962. 1969. 1981
6 1908. 1917. 1926. 1936. 1941. 1947. 1972. 1984. 1990
7 1909. 1929. 1935
8 1911. 1924. 1940. 1958. 1961
9 1902. 1944. 1955. 1977. 1998
10 1921. 1928. 1952. 1956. 1985. 2000
12 1982. 1986. 1988
13 1970
14 1910
17 1946
G. VIII. . . . . (18) . . . . . (584)
2 1992
3 1905. 1932. 1950. 1960. 1968. 1995
4 1920. 1938. 1953. 1974. 1980. 1989
5 1904. 1965,
6 1914. 1925
7 1976

Summe 388. 3282
Irreg. 3 Impr. 556

Hundertergruppe 21.
G. I. . . . . .(8). . . . . .(284)
21 2011. 2083
27 2003
33 2027
35 2087
45 2039. 2063
57 2099
G. II. . . . . .(30). . . . . .(1054)
6 2017. 2062
8 2095
9 2023. 2038. 2047. 2053
12 2059. 2098
14 2007. 2018
15 2043. 2071. 2092
16 2048
17 2026. 2029
19 2031. 2069
20 2078
21 2012
22 2089
24 2019
25 2042
27 2051. 2075(*3*)
28 2066
30 2036. 2081
32 2084
G. IV. . . . . .(42). . . . . .(1376).
4 2020. 2077
5 2032. 2073. 2074
6 2022. 2025. 2028. 2035. 2050. 2052. 2067. 2068. 2082. 2086. 2096
7 2008. 2033. 2044. 2055. 2058. 2094
8 2004. 2005. 2034. 2041. 2056
9 2014. 2049. 2060. 2076. 2079. 2091
10 2057. 2061
12 2006. 2009. 2045
13 2015
15 2096
17 2021
18 2054
G. VIII. . . . . .(19). . . . . .(632)
2 2002. 2013. 2080. 2088
3 2037. 2065
4 2010. 2016. 2046. 2072. 2100.
5 2030. 2070. 2085. 2093
6 2001. 2064. 2090
7 2024
G. XVI. . . . . .(1). . . . . .(32)
2 2040

Summe 404. 3378
Irreg. 1 Impr. 560

Hundertergruppe 2
G. I. . .(5). .(149)
13 2143
21 2179
27 2187(*3*)
39 2131
49 2111
G. II. . .(33).(1174)
8 2113. 2137
9 2122. 2167. 2188
10 2164
11 2182
12 2107. 2116
13 2102. 2197
14 2127
15 2151. 2191
16 2153. 2194
17 2103. 2119
18 2155. 2161. 2199
21 2123. 2138. 2147. 2171. 2183. 2186
24 2195
28 2129
30 2126. 2159
32 2174
39 2141
G. IV.(46).(1592)
5 2101. 2118. 2125. 2152. 2158. 2173. 2178
6 2104. 2115. 2132. 2139. 2148. 2157. 2163. 2172.
7 2110. 2140. 2146. 2149. 2165
8 2134. 2176(*2*) 2192
9 2106. 2108. 2117. 2124. 2133(*3*). 2175. 2181. 2198
10 2150. 2154. 2166. 2177
11 2135
12 2105. 2156. 2168. 2169. 2196
14 2114. 2144. 2162
15 2189
16 2180
G. VIII.(14).(424)
2 2128. 2170
3 2160. 2185. 2190. 2193. 2200
4 2112(*2*). 2130. 2142
5 2109. 2121. 2136
7 2120
G. XVI.(2). . .(80)
2 2145
3 2184

Summe 399. . .3419
Irreg. 4 Impr. 585

Hundertergruppe 23.
G. I. . . .(7). .(217)
15 2203
21 2251
29 2287
33 2267
35 2239
39 2207
45 .2243(*3*)
G. II. .(29).(1084)
7 2293
9 2221. 2227. 2283
10 2281
11 2215. 2263
12 2209
13 2218
14 2258
15 2237. 2269. 2284. 2299
16 2206
17 2234
18 2228
20 2297
21 2213. 2259
22 2271
24 2273
27 2252. 2291
28 2279
29 2231
32 2276
36 2219(*3*)
39 2246
G. IV.(46).(1612)
4 2212. 2242. 2248. 2272
5 2202. 2230. 2247. 2290
6 2223. 2257. 2260. 2268. 2275. 2278
7 2217. 2238. 2270
8 2236. 2245. 2254(*2*). 2286. 2292. 2298
9 2214. 2221. 2235(*3*). 2241. 2253. 2266. 2295. 2300.
10 2249. 2250. 2255. 2282
11 2204. 2216
12 2211. 2225. 2229
13 2222
14 2274
15 2264. 2285
16 2201
19 2294
G. VIII.(17).(584)
2 2233. 2277
3 2205. 2220. 2262
4 2208. 2232. 2244. 2256. 2265. 2289. 2296

5 2226. 2288
6 2240
7 2210
9 2261
G. XVI.(1)..(32)
2 2280

Summe 401...3529
Irreg. 4 Impr. 571

Hundertergruppe 24
G. I....(7)..(291)
15 2347
29 2311. 2383
39 2371
57 2339
59 2399
63 2351
G. II..(32).(1106)
7 2335
8 2302. 2308. 2377
11 2326. 2374
12 2307. 2323. 2395
13 2362. 2367
14 2359
15 2303. 2319. 2341. 2363
16 2386
17 2333. 2389. 2391
19 2381
20 2375
21 2342. 2348. 2357
24 2327. 2372
25 2396
27 2315(*3*)
30 2393
32 2306
33 2309
G. IV..(40).(1520)
4 2332. 2353. 2368
5 2398
6 2305. 2317. 2322. 2338. 2358. 2388
7 2314. 2382
8 2304. 2312. 2313. 2329(*2*). 2343. 2350. 2356
9 2318. 2344. 2349. 2355. 2361. 2387
11 2334. 2364.
12 2316. 2331. 2376. 2379(*2*). 2390
14 2324. 2354. 2384
15 2321. 2330. 2378
16 2336
18 2369

G. VIII.(20).(648)
2 2392
3 2325. 2346. 2352. 2370. 2373. 2380
4 2320. 2328. 2337. 2340. 2365. 2385(*2*). 2397. 2400(*2*).
5 2360. 2394.
6 2301. 2376
7 2345
G. XVI. .(1). .(32)
2 2310

Summe 407. . .3597
Irreg. 5 Impr. 611

Hundertergruppe 25.
G. I. . .(5). .(217)
21 2467
33 2423
37 2447
57 2459
69 2411
G. II. .(35).(1250)
9 2403(*3*). 2437(*3*).
2443. 2458
10 2407. 2452. 2473. 2487. 2500
12 2419. 2468. 2479
13 2428
14 2401. 2446. 2455
15 2476
16 2434. 2462
17 2463
18 2417. 2491
19 2477
20 2402. 2404. 2498
21 2427
22 2439
27 2426
28 2495
30 2483
31 2471
33 2435
38 2441
39 2474
G. IV.(38).(1472)
4 2410
5 2422. 2433. 2494
6 2412. 2413. 2425. 2451. 2475.
2482. 2488. 2493
7 2416. 2431. 2438. 2497
8 2454
9 2430(*3*). 2461
10 2449
11 2421. 2489. 2492
12 2420(*2*). 2432. 2450.
2466. 2484. 2499
13 2453. 2469. 2481
14 2429. 2486
15 2406. 2444
17 2456
18 2414
G. VIII.(22).(720)
3 2418. 2424. 2440. 2457. 2472.
2485
4 2436. 2442. 2445. 2448(*2*).
2464. 2465. 2470. 2478. 2490.
2496
5 2405. 2409. 2415. 2460
6 2408. 2480

Summe 403. .3659
Irreg. 5 Impr. 595

Hundertergruppe 26.
G. I. . .(7). .(301)
21 2503
33 2539
35 2543
41 2551
51 2531
57 .2591
63 2579
G. II. .(29).(1028)
8 2578
9 2515. 2557. 2563(*3*).
2566. 2572
10 2527
12 2587. 2593
13 2524
15 2523. 2575. 2518. 2599
16 2521
18 2511. 2547
19 2554
20 2559
21 2507. 2571
22 2567. 2594
25 2582. 2588
28 2564
32 2519. 2558
35 2549
G. IV.(45).(1752)
4 2533. 2542(*2*)
5 2577
6 2512. 2517. 2538. 2545. 2548.
2592. 2598
7 2502. 2509. 2535. 2536. 2556.
2583
8 2506. 2513. 2528. 2560. 2569.
2589
9 2522. 2555. 2581. 2595
10 2514. 2529. 2532. 2596
11 2570. 2573
12 2597
13 2510
14 2501. 2525. 2586
15 2526. 2534. 2537. 2540
16 2546. 2561
18 2504. 2516
G. VIII.(18).(648)
3 2508. 2530. 2550. 2553. 2562.
2590
4 2568. 2580. 2584
5 2505. 2541. 2544. 2552 2585

6 2565. 2574. 2600
8 2576
G. XVI.(1). .(32)
2 2520

Summe 405. .3761
Irreg. 2 Impr. 641

Hundertergruppe 27.
G. I. . .(7). . .(231)
15 2647. 2683
23 2671
39 2659
43 2663
45 2699(*3*)
51 2687
G. II. .(29).(1196)
10 2638
11 2623. 2662. 2677
12 2611. 2689. 2692
14 2612
15 2602. 2643
16 2617. 2633. 2657
18 2619(*3*). 2627. 2644
21 2693
23 2614. 2615
24 2631. 2654
26 2642
27 2675(*3*)
30 2603. 2606
31 2621
33 2636
39 2651
42 2609
G. IV.(46).(1776)
3 2608
4 2605
5 2641
6 2620. 2629. 2650. 2653. 2658. 2667. 2668. 2676. 2682. 2695. 2698
7 2607
8 2601. 2628(*2*). 2655. 2674. 2686
9 2626. 2634. 2635. 2637. 2646(*3*). 2673. 2700(*3*)
10 2656. 2678
11 2645. 2648. 2649. 2672
12 2681. 2691. 2696
13 2679
15 2630. 2684. 2690. 2694
16 2624(*3*). 2639. 2669
17 2666
18 2681
G. VIII.(17).(584)
2 2632
3 2613. 2622. 2680. 2685. 2697
4 2652. 2665. 2688
5 2610. 2618. 2625. 2664. 2670.
6 2604. 2660
7 2616

G. XVI. .(1). .(32)
2 2640

Summe 401. . .3819
Irreg. 7 Impr. 625

Hundertergruppe 28.
G. I. . .(6). .(208)
21 2707 2767
33 2731
39 2791
41 2719
53 2711
G. II.(29).(1190)
9 2787. 2797
10 2722. 2743
12 2713
13 2762
14 2734. 2753
15 2727. 2732. 2764
18 2723. 2763(*3*). 2783
19 2738. 2746. 2799
20 2777
21 2749. 2779
22 2798
27 2747. 2759
29 2741
30 2708.
31 2735
39 2771
40 2729
41 2789
G. IV.(47).(1864)
4 2773. 2788
5 2776
6 2704. 2710. 2715. 2718. 2725. 2740. 2748. 2752. 2755. 2758. 2794
7 2703. 2761. 2766. 2782
8 2733. 2742. 2775. 2785
9 2716. 2770. 2778. 2781. 2795
10 2724. 2751
11 2757
12 2701. 2702(*2*). 2739. 2754 2780
13 2721. 2792
14 2744. 2768. 2774
15 2750. 2796
17 2726
18 2705. 2786
20 2714. 2756(*2*)
G. VIII.(16).(568)
2 2737
3 2728. 2800

4	2706. 2709. 2717. 2745. 2772. 2790. 2793
5	2712. 2769
6	2720. 2736. 2784
7	2765
G. XVI.(2). .(64)	
2	2730. 2760
Summe 412. .3894	
Irreg. 3	Impr. 644

Hundertergruppe 29.
G. I. .(6). .(250)
25 2887
27 2803
33 2851
45 2843
57 2879
63 2819
G. II. .(32).(1298)
8 2878
10 2818. 2836. 2857
11 2815. 2863
12 2827
13 2809. 2823. 2839. 2854
15 2875. 2883. 2899
16 2833
18 2867. 2897
19 2858
20 2866
23 2837
24 2811
26 2807
27 2859. 2891(*3*)
30 2801. 2855
31 2876
33 2861
34 2804. 2831. 2894
36 2846
G. IV.(43).(1680)
4 2842. 2893
5 2830. 2853
6 2802. 2872. 2892
7 2812. 2881
8 2817. 2845. 2847: 2848(*2*).
2868. 2884
9 2806. 2828. 2835(*3*).
2862. 2887. 2888. 2890. 2895
10 2810. 2844. 2869. 2871. 2874.
2896
11 2841
12 2816. 2822. 2824. 2825. 2852.
2873. 2900.
13 2826.
15 2813. 2864. 2889
16 2882
21 2834
G. VIII.(17).(648)
2 2832
3 2808. 2860
4 2821. 2829. 2850(*2*).
2865. 2880. 2898
5 2814. 2838. 2877. 2886
6 2820
7 2870

8 2840. 2849
G. XVI.(2)..(96)
3 2805. 2856

Summe 410..3972
Irreg. 4 Impr. 636

Hundertergruppe 30.
G. I..(6)..(322)
31 2927
33 2971
39 2963
59 2903
73 2999
87 2939
G. II..(33).(1266)
8 2962
9 2902. 2923. 2998
10 2983
11 2917. 2935
12 2947. 2953. 2995
13 2908
14 2932
15 2956. 2986
17 2918
18 2916. 2943. 2979
20 2942. 2959
21 2911. 2931. 2972
24 2974. 2991
26 2969
27 2951. 2957
30 2978. 2987
33 2906
35 2909
43 2966
G. IV.(37).(1588)
5 2965
6 2907. 2914. 2938. 2977. 2997
7 2913. 2930. 2941. 2973
8 2944. 2946. 2949. 2980(*2*)
9 2950. 2955. 2988. 2989
10 2919. 2929. 2948. 2975
11 2922. 2933. 2934. 2967
12 2993(*2*)
13 2901. 2984
16 2921. 2994. 2996.
18 2915. 2924
20 2936. 2954. 2981
G. VIII.(24).(888)
2 2968
3 2905. 2920. 2937. 2970. 2982. 2992
4 2928. 2940. 2952. 2958. 2985
5 2904. 2910. 2926. 2990. 3000

6 2912. 2925. 2961. 2964. 2976
8 2945. 2960

Summe 412. .4064
Irreg. 2 Impr. 714

Hundertergruppe 43.
G. I. . .(7). .(425)
27 4243
45 4219
51 4231
63 4283
65 4271
69 4211
105 4259
G. II.(32).(1592)
12 4222. 4258. 4267. 4273
13 4207. 4282
14 4279
15 4204. 4227
17 4261
18 4201. 4291(*3*). 4297
19 4252
21 4203. 4253
22 4223
24 4239. 4287. 4295
26 4217. 4244
27 4262. 4299
30 4276
31 4247
39 4229
40 4286
42 4274
54 4226. 4241
56 4289
G. IV.(38).(1780)
6 4225. 4237. 4288
7 4210. 4213
8 4228. 4249
9 4236. 4246. 4255. 4263. 4285. 4293. 4294. 4300(*3*)
11 4215. 4238. 4281. 4298
12 4212(*2*). 4232. 4251. 4275(*2*). 4292
13 4202. 4206. 4208. 4234
14 4205
15 4235. 4250. 4266
17 4269
18 4220. 4265. 4268
19 4254
20 4214
G. VIII(22). .(976)
3 4218. 4257. 4272
4 4216. 4240. 4260. 4270. 4278
5 4230. 4233. 4242. 4264. 4284
6 4245. 4248. 4277
7 4209
8 4221. 4224. 4296
9 4280
10 4256

G. XVI.(1)..(48)
3 4290
Summe 415....4821
Irreg. 4

Hundertergruppe 51.
G. I...(8)..(546)
25 5023
45 5003
57 5059
63 5011
69 5087
83 5039
87 5051
117 5099
G. II..(22).(1104)
11 5077. 5098
15 5047. 5062
16 5086
18 5007. 5041. 5042. 5063
21 5027. 5043. 5091
24 5095
25 5071
27 5067. 5078
30 5009
32 5079
39 5021
42 5006
45 5036(*3*)
58 5081
G. IV.(51).(2728)
6 5020. 5065. 5083
7 5038
8 5002. 5008. 5017. 5058. 5089
9 5013. 5014. 5035. 5050. 5055. 5068(*3*). 5097
10 5026. 5028. 5044. 5052. 5053. 5056. 5072. 5092
11 5093
12 5022. 5076
13 5029. 5090
14 5046. 5074
15 5019. 5030. 5094
16 5012. 5031(*2*)
18 5004. 5033. 5034. 5048. 5054. 5069(*3*). 5075(*3*)
19 5001. 5018
20 5057. 5084
22 5015
26 5024. 5045
30 5066
G. VIII(16).(784)
3 5032

4 5037
5 5061. 5080
6 5010. 5025. 5049. 5070. 5073.
5082. 5085. 5088. 5100
8 5064
9 5096
10 5060
G. XVI.(3).(128)
2 5005
3 5016. 5040

Summe 424. . .5290
Irreg. 5

Hundertergruppe 61.
G. I. . .(7). .(353)
27 6007. 6043
45 6067(*3*). 6091(*3*)
57 6079
71 6047
81 6011(*3*)
G. II. .(22).(1440)
12 6073
15 6022
17 6037
18 6087
22 6082. 6092
24 6098
25 6031. 6053
27 6075(*3*)
28 6046
31 6038
33 6019
35 6029
39 6059
41 6023
42 6051
46 6002
48 6071
49 6044
58 6089
63 6074
G. IV.(53).(3012)
7 6013. 6028
8 6001(*2*). 6052(*2*)
9 6015. 6021(*3*). 6055. 6063. 6064. 6070. 6076. 6078. 6085(*3*)
10 6010. 6034. 6049. 6058. 6088.
11 6012
12 6003. 6004. 6008. 6025. 6027. 6057. 6066. 6077. 6084. 6099. 6100(*2*)
13 6033. 6094
14 6062
15 6017. 6039. 6050. 6081. 6093.
16 6016
18 6065. 6083(*3*)
19 6009
20 6036. 6054
21 6035. 6095
24 6014(*2*). 6068. 6086
25 6056
26 6005
28 6026
30 6041
G. VIII.(14).(768)
3 6097

4 6040. 6042
6 6018. 6024. 6030. 6048
8 6032. 6061. 6069. 6080
9 6060
10 6020. 6096
G. XVI.(4).(208)
3 6045. 6072. 6090
4 6006

Summe 439. .5781
Irreg. 11 Impr. 933

Hundertergruppe 62.
G. I. . .(5). .(265)
33 6163
39 6199
41 6143
59 6151
93 6131
G. II. .(28).(1704)
11 6127
14 6103
15 6115. 6147
16 6178
18 6183. 6187. 6196
19 6172·
21 6133
22 6121
27 6122
29 6166
30 6139
33 6124. 6167
34 6113
35 6134. 6197
37 6173
40 6159
41 6119
42. 6155. 6158
45 6107
49 6191
53 6101
60 6179
G. IV.(44).(2568)
6 6157
7 6108. 6142. 6193
8 6112. 6148
9. 6130. 6154. 6175
10 6106. 6117. 6169. 6198
11 6182. 6190
12 6123(*2*). 6181
14 6145. 6174. 6185
15 6102. 6109. 6125. 6126. 6129. 6171
16 6144. 6189

17 6128. 6184
18 6111. 6135. 6156(*3*).
6164
19 6140
20 6114. 6137. 6161. 6176. 6186
22 6152. 6194
25 6170
28 6146
G. VIII(20).(1200)
4 6118
5 6136. 6153. 6162. 6168
6 6132. 6138. 6150. 6165. 6177.
6180. 6192. 6195
7 6141
9 6188
10 6110
12 6104. 6200
13 6116
15 6149
G. XVI(3)..(128)
2 6160
3 6105. 6120

Summe 445...5865
Irreg. 2 Impr. 975

Hundertergruppe 63.
G. I. . .(7). .(447)
43 6247
45 6211
51 6203. 6271. 6287
77 6263
129 6299
G. II. .(28).(1678)
12 6238. 6295
15 6259. 6268
16 6217
18 6267(*3). 6283(*3*)
20 6223. 6241. 6274
23 6218. 6277
25 6207. 6250
27 6227(*3*)
29 6229
30 6212. 6219
33 6243
36 6242
38 6257
42 6275
45 6239. 6291(*3*)
51 6236. 6284
57 6269
63 6221(*3*)
G. IV.(39).(2428)
6 6220. 6262
7 6253
8 6202. 6208(*2*)
9 6235. 6252. 6297.
10 6246. 6292
11 6298
12 6255 6286(*2*)
13 6282
14 6228. 6245. 6260. 6276
15 6214. 6234. 6249
16 6231. 6233. 6244. 6272(*4*)
17 6294
18 6226(*3*). 6251
19 6281. 6289
20 6261
21 6266
22 6224
23 6278
24 6209. 6215
25 6206
27 6296
35 6254
G. VIII(23).(1176)
3 6232
4 6273
5 6205. 6213. 6258. 6280. 6285
6 6210. 6222. 6225. 6237. 6288.

6290. 6300
7 6248. 6256. 6265. 6279. 6293
8 6204
9 6264
10 6201
11 6230
G. XVI(3). .(176)
3 6216
4 6240. 6270

Summe 451. .5905
Irreg. 9

Hundertergruppe 91.
G. I. . .(6). .(386)
27 9067
35 9007
45 9043
63 9091
99 9011
117 9059
G. II. .(26).(1960)
15 9013
18 9003(*3*). 9055
19 9034
21 9004. 9046
26 9079
27 9031. 9094
29 9098
30 9001. 9076
33 9068
36 9049. 9083
40 9023
42 9041
44 9047
45 9019(*3*)
46 9038
48 9092
54 9099(*3*)
57 9029
69 9014. 9071
80 9026
G. IV.(42).(2928)
8 9087. 9088
9 9022. 9037. 9073. 9097
10 9025. 9058
11 9052
12 9018. 9027. 9028
13 9082
14 9017. 9032. 9066
15 9033. 9051. 9063
17 9002. 9057. 9070
18 9012. 9015. 9069(*)..
9075(*3*)

19 9053. 9095
20 9039. 9054. 9062. 9081
21 9036
22 9084
27 9008. 9050. 9074
28 9089
30 9005. 9035. 9056. 9077
G. VIII(23).(1640)
5 9010
6 9040. 9042. 9045. 9072. 9085. 9100
7 9078. 9080. 9090. 9093
8 9016(*2*). 9024. 9060
9 9061. 9074
10 9020
11 9006
12 9021. 9065
14 9096
17 9086
18 9044
G. XVI(3)..(176)
3 9030. 9048
5 9009

Summe 45..7090
Irreg. 6 Impr. 1122

Hundertergruppe 92.
G. I. . .(5). .(295)
51 9199
57 9103. 9127
63 9187
67 9151
G. II. .(30).(2208)
13 9157
14 9172
19 9133
20 9124. 9183
21 9115
23 9181
27 9109. 9123. 9167. 9175
28 9137
29 9148
30 9147
32 9111
34 9122. 9166
36 9143
39 9107. 9171
40 9188
47 9173
54 9134. 9155
56 9182
57 9179
60 9131
62 9119
63 9194
72 9161
G. IV.(36).(2652)
7 9178
8 9118(*2*). 9193
9 9132. 9139. 9162. 9163(*3*)
10 9190
12 9121. 9142. 9153. 9186
13 9117
15 9106. 9136. 9195. 9196
17 9158
18 9154
19 9146
20 9169
21 9126. 9197
22 9138. 9189
24 9113. 9159
25 9101. 9125
27 9164.
28 9116
30 9140
31 9191
32 9104(*2*)
33 9149
34 9110

G. VIII(26).(1752)
4 9108
5 9102. 9160
6 9112. 9130. 9145. 9150
7 9174
8 9135. 9144. 9156. 9168. 9184. 9192. 9198
9 9105. 9114. 9180. 9185. 9200
10 9128. 9152
11 9129. 9170
12 9141
19 9176
G. XVI(3)..(176)
3 9177
4 9120. 9165

Summe 465...7083
Irreg. 3 Impr. 1207

Hundertergruppe 93.
G. I...(4)..(340)
33 9283
75 9227
93 9203
139 9239
G. II..(27).(2092)
13 9277
17 9223
18 9241. 9298
21 9235
25 9293
27 9211. 9247
29 9244
30 9271
31 9263
33 9267
35 9279
36 9259
37 9274
39 9242. 9286. 9287
40 9278
45 9251(*3*)
49 9221
54 9209
60 9257.
63 9206
66 9236
75 9299
80 9281
G. IV.(47).(3216)
7 9262
8 9202. 9208. 9232
10 9238. 9289
11 9237. 9258

12 9207. 9219. 9220(*2*).
9228. 9243(*2*). 9268.
9292. 9259. 9297
13 9249. 9255
14 9217. 9226. 9253
15 9212. 9250. 9276
16 9214(*2*). 9216.
9248(*2*). 9252
17 9254
18 9234
21 9201. 9229. 9261
22 9233. 9245
24 9275. 9291
25 9231. 9294
26 9218. 9290
27 9260(*3*)
29 9215
30 9284
32 9224
36 9266(*2*)

G. VIII(20).(1440)
6 9205. 9213. 9265. 9270. 9288.
9300
7 9256
8 9222. 9225. 9273. 9280(*2*).
9285
9 9272
10 9210
11 9230
12 9204. 9264
14 9269. 9296
15 9246

G. XVI.(1)..(48)
3 9282

G. XXXII(1).(64)
2 9240

Summe 454...7200
Irreg. 9 Ingr. 1145

Hundertergruppe 94.
G. I. . .(6). . .(478)
41 9319
51 9343
55 9391
87 9323
97 9311
147 9371
G. II. .(27).(1894)
15 9307. 9388
18 9355
21 9397
23 9382
25 9375
26 9337
27 9349
28 9327
30 9346. 9358. 9363. 9364
32 9377
34 9326. 9332
36 9347. 9379. 9395
41 9302
46 9351
49 9335
51 9383
52 9359
56 9314
57 9356
69 9341
G. IV.(39).(2848)
7 9340. 9367
9 9342(*3*). 9370
11 9304. 9322
12 9378. 9387
13 9313. 9318
14 9353. 9394
15 9325. 9331. 9339
16 9301. 9316(*2*)
17 9303
18 9315(*3*). 9357. 9362. 9376. 9385(*3*). 9396. 9398
21 9334. 9368. 9392
22 9305. 9317.
23 9365
24 9308. 9399
27 9369. 9374.
30 9386
32 9344(*2)
33 9329. 9389
G. VIII(25).(1752)
4 9310. 9328. 9373
5 9333
6 9352

7 9321. 9361. 9381.
8 9312(*2*). 9348. 9372.
9393. 9394. 9400
9 9390
10 9330. 9338. 9366
11 9306. 9309. 9336
12 9324
14 9350. 9380
13 9320
G. XVI.(3)..(176)
3 9384
4 9345. 9360

Summe 464...7148
Irreg. 6 Impr. 1210

Hundertergruppe 95.
G. I....(8)..(708)
33 9403
45 9463
75 9439
91 9431
101 9479
105 9419
123 9467
135 9491
G. II..(24).(1706)
16 9433
18 9475
19 9466. 9487
20 9442
21 9427
24 9406. 9409. 9423
30 9459
33 9421
34 9458
36 9451. 9497(*3*)
39 9484
40 9473
42 9428
45 9411. 9437
46 9407
51 9413
57 9461
63 9404
71 9446
G. IV.(41).(2988)
8 9412(*2*). 9457(*2*).
9472
9 9493
11 9402. 9447. 9496
12 9445. 9469. 9483. 9498
13 9415. 9418. 9448. 9454. 9468.
9478

14 9436
15 9443. 9452
17 9410
18 9444. 9477. 9482. 9495
20 9500
21 9414. 9481. 9489. 9499
22 9441
24 9422(*2*). 9426. 9474.
9488
28 9494
29 9449
30 9455
35 9470
36 9476
42 9434
G. VIII(25).(1744)
4 9430
5 9417
6 9408. 9432. 9438. 9465. 9492
7 9453. 9462
8 9424. 9460. 9485. 9486. 9490
9 9420. 9450(*3*). 9471
.10 9440
11 9429. 9456
12 9425. 9435. 9464
14 9416
16 9401
G. XVI.(2)..(112)
3 9480
4 9405

Summe 452..7258
Irreg. 5

Hundertergruppe 96.
G. I. . . .(5). .(471)
39 9547
69 9511. 9587
129 9551
165 9539
G. II. .(28).(1964)
16 9508
17 9535
18 9523. 9583
20 9598
24 9502. 9507
25 9559
26 9543
27 9531(*3*). 9563.
9574(*3*)
29 9532
30 9571
33 9527
34 9556. 9586
38 9524. 9567
42 9518
43 9578
48 9566
49 9599
51 9575
59 9596
60 9572
61 9533
64 9521
G. IV.(38).(2700)
8 9538. 9562. 9577
10 9517. 9553. 9573
12 9505. 9522. 9526. 9550. 9580.
9595(*2*)
13 9514. 9549. 9557
14 9501. 9529. 9542
15 9582
16 9544
17 9564
18 9558
19 9565
20 9503(*2*). 9589. 9591.
9593
21 9515. 9561
24 9519. 9579
25 9530. 9584
27 9509
28 9536
30 9506
38 9569
40 9554
G. VIII(26).(1960)
4 9568

5 9592
6 9552. 9585. 9597
7 9528
8 9510(*2*). 9513(*2*).
9537. 9540(*2*). 9588.
9600(*2*).
9 9541. 9548. 9555(*3*)
10 9525. 9534. 9594
12 9504. 9516(*2*). 9560
13 9545. 9594
14 9581
15 9512. 9590
G. XVI.(3).(176)
3 9520. 9570
5 9576

Summe 469. .7271
Irreg. 10

Hundertergruppe 97
G. I. . . .(5). .(333)
33 9643
57 9619
71 9679
77 9631
95 9623
G. II. .(29).(2108)
12 9667
19 9661
20 9697
21 9607. 9613
24 9601
26 9655
27 9627(*3*). 9663.
9683(*3*)
28 9604. 9634. 9649
30 9687. 9691
32 9662
33 9692
36 9668
42 9651
43 9647
44 9602
45 9626
49 9677
52 9689
55 9629
57 9659
63 9671
66 9611
69 9644
G. IV. .(41).(3108)
9 9612(*3*). 9615. 9622.
9678

10 9628
11 9670
12 9652. 9673(*2*). 9676.
9682. 9700
13 9637
14 9642. 9658. 9664
15 9639
16 9610
17 9606
18 9603. 9675(*3*).
9693(*3*).
19 9638. 9694
20 9608. 9616. 9650. 9653
21 9699
22 9654. 9684
23 9695
24 9641. 9666
25 9609
29 9617. 9674. 9698
30 9621
32 9665
33 9635
42 9686
G. VIII(22).(1600)
4 9640
5 9618. 9625. 9685. 9688
6 9648. 9696
7 9633. 9646
8 9645. 9669
9 9630. 9657
10 9620. 9636
11 9681
12 9605. 9632. 9680(*2*)
15 9624
16 9614
18 9656
G. XVI.(3)..(192)
3 9672
4 9690
5 9660

Summe 451..7341
Irreg. 7

Hundertergruppe 98.
G. I. . .(6). .(524)
39 9739. 9787
89 9767
105 9743
119 9791
133 9719
G. II.(24).(1646)
17 9703
18 9748(*3*). 9783
19 9727
21 9733
22 9742
24 9763
25 9781
26 9769. 9778
27 9747(*3*). 9751
30 9755
33 9799
35 9754
37 9788
39 9707. 9771
43 9722
46 9721. 9759
48 9731
76 9764
81 9749
G. IV.(43).(3292)
7 9718
9 9772
10 9732. 9793
11 9738. 9753
12 9706. 9745. 9762
13 9712. 9713
14 9757. 9775. 9784
15 9766. 9777. 9795
16 9736. 9797
17 9711
18 9715. 9723. 9782
19 9773
20 9714. 9796
21 9708. 9710. 9770. 9774
22 9725. 9756
24 9728
26 9794
27 9704. 9726
28 9716. 9734
29 9761
30 9746
33 9740
36 9779
38 9701
G. VIII(24).(1752)
5 9717. 9730

6 9760. 9790
7 9724. 9752
8 9702(*2*). 9729. 9735.
9758. 9780. 9792(*2*)
9 9725. 9709. 9720(*3*)
10 9741. 9750. 9798
11 9737. 9786
12 9800
14 9789
15 9776. 9785
G. XVI(3)..(192)
4 9744. 9765. 9768

Summe 466..7406
Irreg. 5

Hundertergruppe 99.
G. I...(8).(638)
49 9871
51 9883
63 9811(*3*). 9859
75 9887
91 9839
111 9803
135 9851
G. II..(22).(1700)
20 9892
21 9829. 9862. 9868
22 9847
24 9817. 9874
26 9838
28 9886. 9895
30 9857
34 9826
42 9827
45 9899(*3*)
48 9863
49 9818
51 9819
52 9833
57 9836
60 9875
70 9806
77 9866
G. IV.(43).(3164)
6 9823
7 9802
8 9865
9 9832. 9843. 9853. 9898
10 9808. 9837. 9850
11 9813
12 9872. 9835
13 9846
14 9820. 9878

15 9822. 9882
16 9807. 9814. 9848
17 9852. 9893. 9897
18 9801(*3*). 9844. 9873. 9891
19 9815. 9879
21 9855
22 9841
25 9830
26 9812. 9876
27 9831
28 9881(*2*)
31 9884
32 9809(*2*)
34 9824
37 9854
39 9896
41 9869

G. VIII(24).(1712)
5 9877
6 9804. 9810. 9828. 9867. 9888. 9900
7 9805. 9858. 9885
8 9816. 9856. 9860
9 9825(*3*). 9849(*3*). 9889
10 9821. 9834
11 9894
12 9861. 9864
13 9842
16 9845
17 9890

G. XVI(3)..(192)
3 9870
4 9880
5 9840

Summe 464..7406
Irreg. 7

Hundertergruppe 100.
G. I. . .(4). .(228)
39 9967
45 9907(*3*)
69 9931
75 9923
G. II.(28).(2302)
16 9991
18 9934(*3*)
23 9927. 9973
25 9949
27 9963(*3*)
28 9903. 9943
30 9938. 9979
31 9901
32 9986
34 9998
38 9908
39 9914. 9987
42 9939. 9947
46 9983
47 9935. 9946
50 9902
60 9995
63 9971
65 9959
67 9941
76 9929
85 9974
G. IV.(46).(3248)
7 9937
9 9925. 9958. 9997
10 9913. 9942. 9948. 10000
11 9970
12 9916. 9922. 9952. 9955(*2*).
9972(*2*)
13 9993
14 9988
15 9904. 9921. 9969. 9978
16 9961. 9985
17 9919. 9965
18 9910. 9915. 9964
19 9951. 9957. 9977
20 9992
21 9909
22 9953. 9956. 9962. 9999
23 9917. 9994
25 9981
26 9924
27 9989
28 9926. 9980
30 9932. 9950
34 9911

G. VIII(18).(1328)
4 9982
5 9976
6 9928. 9940. 9990
7 9906
8 9930. 9975. 9984
10 9918
11 9968
12 9905. 9920. 9936. 9954. 9996
13 9966
14 9944
G. XVI(4)..(240)
3 9933
4 9912. 9945. 9960

Summe 452..7346
Irreg. 5

Hundertergruppe 117.
G. I...(1)..(147)
147 11699
G. II..(35).(2896)
16 11617
18 11698
19 11677
20 11614
22 11668
26 11647
27 11643. 11683(*3*)
29 11663
30 11602. .11623. 11659
35 11686
36 12603. 11631. 11633. 11667.
11671. 11689. 11691. 11695
37 11642
42 11657
43 11626
45 11611
51 11621
54 11619
56 11678
59 11612
63 11675
67 11639
70 11636
73 11654
81 11651(*3*)
90 11681
G. IV..(35).(2672)
8 11650
9 11608. 11692
11 11638. 11653
12 11635. 11641. 11673
13 11632. 11674

14 11652. 11662
15 11607. 11694
16 11629. 11665
17 11672
18 11601. 11627. 11637. 11664
19 11687
21 11644
23 11618
24 11615
25 11693
26 11604. 11669. 11679
28 11646
29 11630
32 11666. 11684
33 11624
35 11606

G. VIII(27).(2248)
6 11610. 11620. 11628. 11656. 11680. 11697
8 11605. 11622. 11658. 11670. 11682
9 11613. 11655
10 11616. 11625. 11676
11 11688
12 11648. 11661. 11700(*2*)
13 11634. 11645. 11649
14 11690
18 11660. 11696
21 11609

G. XVI.(2).(128)
3 11685
5 11640

Summe 459. . .8091
Irreg. 3 Impr. prim. 1339

Hundertergruppe 118.
G. I. . . .(5). .(319)
39 11743
41 11719
63 11731
81 11779(*3*)
95 11783
G. II. .(28).(2560)
18 11707
21 11767
22 11727. 11758
25 11734
29 11722
30 11755
31 11701. 11708
33 11702. 11763
36 11762
39 11747. 11787
40 11791
49 11789
50 11794
53 11751
54 11723
60 11711. 11771. 11777
61 11735. 11738
65 11759
73 11717
87 11756
98 .11714
G. IV.(40).(3100)
8 11797
9 11782
10 11785
11 11740. 11757
12 11733. 11737. 11788
14 11728. 11746. 11764
15 11710. 11773. 11793
16 11705. 11775. 11776. 11796
17 11761
18 11754. 11772
19 11706
20 11716. 11768
21 11724. 11799
22 11703. 11732. 11749
25 11709. 11769. 11780
27 11795(*3*). 11798.
28 11786
29 11721. 11741.
30 11774
34 11729
40 11744
G. VIII(23).(1744)
4 11713(*3*)
6 11715. 11718. 11748. 11752

7 11720. 11742. 11778
8 11712. 11725(*2*). 11753.
11770. 11784. 11790
9 11800
10 11792
11 11736
12 11739. 11745
15 11766
16 11780
18 11726. 11765
G. XVI.(4)..(320)
4 11760
5 11704. 11730
6 11781

Summe 469...8043
Irreg. 4 Impr. prim. 1369

Hundertergruppe 119.
G. I....(7)..(505)
31 11863
39 11827
47 11887
61 11839
75 11867
113 11807
139 11831
G. II...(23).(1990)
21 11878
24 11806. 11812. 11854
27 11851(*3*). 11881
30 11875
33 11884
39 11852
40 11833. 11897
43 11821
45 11871. 11899(*3*)
49 11813. 11846
52 11876
54 11828. 11843(*.3*)
58 11855
70 11801
72 11819
75 11879
G. IV.(44).(3608)
8 11848
9 11803. 11818. 11893
10 11860. 11862
11 11815
12 11823
13 11838
14 11842. 11892
15 11824. 11853. 11883
16 11857

18 11809. 11811. 11835(*3*).
11873. 11874
19 11841
20 11822(*2*). 11836. 11847.
11858. 11866
21 11859. 11888. 11898
23 11829
24 11826. 11889. 11896
26 11834. 11894
27 11804. 11810. 11861
29 11882
35 11870
36 11849
37 11885
42 11891
43 11864

G. VIII(22).(1688)
4 11872
6 11817. 11845. 11869. 11895
7 11830. 11890
8 11805. 11808(*2*). 11877
9 11802. 11820. 11825
10 11850. 11900
11 11837. 11868
12 11844. 11886
16 11814. 11840
20 11816

G. XVI.(4)..(304)
2 11880
4 11832
6 11856. 11865

Summe 469...8095
Irreg. 6 Impr. 1337

Hundertergruppe 120.
G. I. . .(7). .(547)
39 11923
45 11971(*3*)
81 11903. 11939(*3*)
83 11927
95 11959
123 11987
G. II. .(22).(1912)
20 11953
21 11962
24 11995
27 11907(*9*). 11911. 11967
30 11943. 11947
31 11983
33 11974. 11979
41 11941
48 11963
49 11933. 11999
50 11975
57 11915
66 11906
69 11909
71 11981
73 11996
80 11969
G. IV.(45).(3564)
9 11992
10 11922. 11932. 11938. 11958
11 11902. 11965
12 11905. 11908. 11917. 11929. 11950. 11980. 11988(*2*). 11998
13 11986
15 11944. 11955
17 11982
18 11916. 11956. 11991
19 11918. 11993. 11994
20 11978
21 11901. 11957
23 11989
24 11926. 11964. 11972(*2*)
26 11936. 11945
27 11919. 11930. 11942. 11961(*3*)
29 11951
30 11912. 11948
32 11966(*2*)
33 11931
40 11924
42 11954

G. VIII(22).(1832)
6 11914. 11937. 11968. 11977
7 11973
8 11920(*2*). 11940. 11946
9 11913. 11925. 11935. 11949. 11952
10 11997. 12000
12 11904. 11910
15 11934
16 11976. 11984
17 11990
21 11921
G. XVI.(4)..(288)
3 11928
4 11985
5 11960
6 11970

Summe 471...8143
Irreg. 8 Impr. prim. 1361

Tausendergruppe I.
G. I...(93)..(1277)

1	1. 2. 3. 4. 7 ..	5
3	11. 19. 23. 27. 31. 43. 67. 163 ..	8
5	47. 79. 103. 127 ..	4
7	71. 151. 223. 343. 463. 487 ..	6
9.	59. 83. 107. 139. 199. 211. 243(*3*). 283. 307(*3*). 331. 367. 379. 499. 547. 643. 823. 883. 907	18
11	167. 271. 967	3
13	191. 263. 607. 631. 727	5
15	131. 179. 227. 239. 347. 439. 443. 523. 571. 619. 683. 691. 739. 751. 787. 947 ..	16
17	383. 991 ..	2
19	311. 359. 919	3
21	251. 431. 467. 503. 587. 743. 811. 827. 859. 863 ..	10
25	479. 599. 647	3
27	419. 491. 563. 983 ..	4
29	887	1
31	719. 911 ..	2
33	659. 839 ..	2
45	971	1

Irreg. 2 pr. 2130

G. II.....(402).....(6068)

1	5. 6. 8. 9. 10. 12. 13. 15. 16. 18. 22. 25. 28. 37. 58 ..	15

2	14. 17. 20. 32. 34. 36. 39. 46. 49. 52. 55. 63. 64. 73. 82. 97. 100. 142. 148. 193 . .	20
3	26. 29. 35. 38. 44. 50. 51. 53. 54. 61. 75. 76. 81. 87. 91. 92. 99. 106. 108. 109. 115. 118. 121. 123. 124. 135. 147. 157. 162. 169. 172. 175. 187. 202. 207. 214. 235. 247. 262. 267. 268. 277. 298. 358. 397. 403. 427. 541. 652	49
4	41. 62. 68. 94. 95. 98. 111. 113. 128. 137. 158. 178. 183. 196. 226. 256. 289. 292. 295. 313. 337. 382. 388. 415. 457. 466. 478. 562. 577. 583. 772. 862	32
5	74. 86. 119. 122. 125. 143. 159. 166. 181. 188. 197. 218. 229. 242. 250. 303. 316. 317. 319. 346. 361. 373. 375. 394. 412. 421. 422. 423. 508. 538. 613. 625. 694. 709. 757. 847. 853. 877. 982	39
6	89. 116. 155. 171. 203. 212. 219. 233. 241. 244. 259. 274. 275. 279. 291. 302. 323. 324. 327. 334. 351. 355. 363. 387. 433. 436. 475. 484. 507. 526. 529. 543. 567. 603. 617. 622. 628. 655. 667. 673. 676. 687. 718. 723. 763. 775. 802. 898. 955	49
7	101. 134. 149. 173. 215. 278. 284. 287. 338. 349. 391. 447. 454. 502. 511. 535. 604. 634. 639. 653. 703. 733. 778. 807. 838. 841. 892. 997	28
8	146. 164. 254. 257. 353. 407. 409. 452. 471. 512. 514. 527. 548. 559. 578. 722. 799. 895. 943. 958. 961	22
9	194. 236. 293. 332. 335. 339(*3*). 362. 411. 428. 451. 459. 486. 515. 519. 531. 556. 557. 575. 586. 661. 675(*3*). 679. 707. 729. 747. 771. 783. 796. 835. 843. 844. 867. 886. 891(*3*). 922. 931. 963. 972	37
10	206. 281. 386. 398. 401. 449. 482. 500. 601. 711. 724. 769. 788. 878. 916. 927. 937. 977	18
11	269. 326. 389. 551. 554. 591. 623. 662. 668. 758. 767. 829. 842. 871. 879 .	15
12	299. 356. 371. 395. 539. 542. 579. 593. 674. 695. 706. 766. 932. 939. 964. 979. 995. 999	18
13	314. 458. 698. 746. 764. 773. 934. 951. 998	9
14	404. 596. 641. 686. 692. 818. 831	7
15	461. 509. 524. 566. 611. 635. 671. 677. 699. 716. 779. 797. 803. 815. 821. 851. 875. 908. 923. 956 .	20
16	446. 521. 569. 791. 809. 857. 953	7
17	614. 701	2
18	626. 731. 755(*3*). 914. 929. 959. 974(*3*) . . .	7
20	734. 761. 881. 926 . . .	4
21	794. 899	2
22	866	1
23	941	1

Irreg. 5 alle *3* pr. 7394

G. IV. . .(417). . . . .(6620)

1	21. 24. 30. 33. 40. 42. 45. 48. 57. 60. 70. 72. 78. 85. 88. 93. 102. 112. 130. 133. 177. 190. 232. 253 . . .	24
2	56. 65. 66. 69. 77. 80. 84. 90. 96. 114. 117. 126. 132. 136. 138. 141. 144. 145. 150. 153. 154. 156. 160. 180. 184. 192. 198. 205. 208. 213. 217. 220. 225. 228. 238. 252. 258. 265. 282. 288. 301. 310. 322. 328. 333. 340. 352. 372. 400. 418. 438. 442. 445. 448. 498. 505. 522. 553. 568. 592. 598. 658. 697. 708. 742. 793. 928 :	67
3	104. 110. 129. 140. 152. 170. 174. 176. 182. 186. 189. 195. 200. 201. 204. 216. 222. 231. 234. 237. 245. 246. 249. 255. 261. 270. 286. 294. 297. 300. 304. 309. 315. 318. 325. 342. 348. 364. 366. 368. 370. 378. 393. 396. 405. 417. 424. 430. 432. 435. 450. 453. 460. 472. 473. 477. 483. 490. 492. 493. 496. 513. 517. 533. 537. 540. 550. 555. 565. 588. 595. 597. 606. 610. 618. 627. 637. 648. 669. 670. 682. 685. 688. 700. 702. 715. 730. 748. 753. 762. 784. 795. 808. 813. 814. 817. 826. 827. 837. 856. 913. 918. 925. 933. 940. 942. 949. 970. 973. 988 .	110
4	161. 185. 221. 224. 248·. 260. 272. 276. 305. 306. 308. 320. 350. 354. 369. 376. 377. 380. 384. 392. 399. 402. 406. 410. 414. 441. 444. 468. 469. 481. 485. 495. 501. 518. 532. 544. 558. 564. 573. 574. 576(*2*). 580(*2*). 582. 589. 612. 632 640. 642. 646. 657. 663. 712. 717. 721. 732. 735. 736. 738. 745. 768. 785. 786. 790. 820(*2*). 832. 834. 850. 852. 855. 865. 868. 873. 882. 889. 900(*2*). 903. 904. 933. 938. 946. 975. 994	82
5	209. 230. 266. 290. 296. 321. 344. 365. 381. 413. 425. 437. 455. 470. 474. 476. 488. 489. 534. 572. 590. 608. 615. 629. 633. 636. 638. 649. 664. 666. 678. 681. 726. 737. 750. 752. 754. 774. 781. 822. 830. 872. 874. 917. 921. 968. 1000	47
6	329. 416. 426. 434. 464. 497. 516. 549. 594. 602. 605. 620. 621. 650. 651. 684. 704. 713. 725. 756. 759. 782. 800. 801. 804. 810. 812. 819. 833. 848. 864. 876. 890. 894. 901. 905. 915. 948. 954. 976. 978. 980. 981. 985. 987. 996	46
7	341. 374. 494. 506. 530. 536. 581. 654. 806. 845. 849. 860. 893. 902. 906. 909. 935. 962	18
8	545. 584. 644. 656. 710. 740. 749. 789. 846. 869. 884(*2*). 896. 992 . . .	13
9	944. 950. 989	3
10	689. 776. 824. 836	4
11	854. 965. 986	3
pr. 6904		

G. VIII. . .(87). . . . .(1496)

1	105. 120. 165. 168. 210. 240. 273. 280. 312. 330. 345. 357. 385. 408. 462. 520. 760	17

2	264. 285. 336. 360. 390. 420. 429. 456. 465. 480. 504. 510. 525. 528. 552. 561. 570. 585. 600. 609. 616. 624. 630. 645. 660. 672. 690. 693. 720. 765. 777. 792. 798. 805. 858. 870. 880. 897. 910. 912. 952. 957. 960	43
3	440. 546. 560. 665. 680. 696. 705. 714. 728. 741. 744. 780. 816. 825. 861. 885. 888. 924. 930. 936. 945. 966. 969. 984. 990 .	25
4	770	1
5	920	1

G. XVI. . . . .(1). . . . . (16)

1	840	1

Gesamtzahl aller

$$\text{Geschlechter} = 3277$$
$$\text{Klassen } p.p.p = 15467$$
$$\sqrt{1} + \sqrt{2} + \ldots + \sqrt{1000} = 21097{,}661$$
$$\text{Quotient} = 0{,}733$$

Irreg. 11, 5(*2*), 6(*3*)

Tausendergruppe III.

G. I. . . . . (64). . . . . (2470)

13	2143	1
15	2203. 2347. 2647. 2683 . .	4
21	2011. 2083. 2179. 2251. 2467. 2503. 2707. 2767 . .	8
23	2671	1
25	2887	1
27	2003. 2187*. 2803	3
29	2287. 2311. 2383	3
31	2927	1
33	2027. 2267. 2423. 2539. 2731. 2851. 2971	7
35	2087. 2239. 2543	3
37	2447	1
39	2131. 2207. 2371. 2659. 2791. 2963	6
41	2551. 2719	2
43	2663	1
45	2039. 2063. 2243*. 2699*. 2843	5
49	2111	1
51	2531. 2687	2
53	2711	1
57	2099. 2339. 2459. 2591. 2879	5
59	2399. 2903	2
63	2351. 2579. 2819	3

69	2411	1
73	2999	1
87	2939	1
Irreg. 3		

G. II. . . .(311). . . . .(11646)

6	2017. 2062	2
7	2293. 2335	2
8	2095. 2113. 2137. 2302. 2308. 2377. 2578. 2878. 2962	9
9	2023. 2038. 2047. 2053. 2122. 2167. 2188. 2221. 2227. 2283. 2403(*3*). 2437(*3*). 2443. 2458. 2515. 2557. 2563(*3*). 2566. 2572. 2787. 2797. 2902. 2923. 2998, ...	24
10	2164. 2281. 2407. 2452. 2473. 2487. 2500. 2527. 2638. 2722. 2743. 2818. 2836. 2857. 2983	15
11	2182. 2215. 2263. 2326. 2374. 2623. 2662. 2677. 2815. 2863. 2917. 2935 ..	12
12	2059. 2098. 2107. 2116. 2209. 2307. 2323. 2395. 2419. 2468. 2479. 2587. 2593. 2611. 2689. 2692. 2713. 2827. 2947. 2953. 2995	21
13	2102. 2197. 2218. 2362. 2367. 2428. 2524. 2762. 2809. 2823. 2839. 2854. 2908	13
14	2007. 2018. 2127. 2258. 2359. 2401. 2446. 2455. 2612. 2734. 2753. 2932 ..	12
15	2043. 2071. 2092. 2151. 2191. 2237. 2269. 2284. 2299. 2303. 2319. 2341. 2363. 2476. 2523. 2575. 2578. 2599. 2602. 2643. 2727. 2732. 2764. 2875. 2883. 2899. 2956. 2986 ..	28
16	2048. 2153. 2194. 2206. 2386. 2434. 2462. 2521. 2617. 2633. 2657. 2833 ..	12
17	2026. 2029. 2103. 2119. 2234. 2333. 2389. 2391. 2463. 2918	10
18	2155. 2161. 2199. 2228. 2417. 2491. 2511. 2547. 2619(*3*). 2627. 2644. 2723. 2763(*3*). 2783. 2867. 2897. 2916. 2943. 2979	19
19	2031. 2069. 2381. 2477. 2554. 2738. 2746. 2799. 2858	9
20	2078. 2297. 2375. 2402. 2404. 2498. 2559. 2777. 2866. 2942. 2959	11
21	2012. 2123. 2138. 2147. 2171. 2183. 2186. 2213. 2259. 2342. 2348. 2357. 2427. 2507. 2571. 2693. 2749. 2779. 2911. 2931. 2972	21
22	2089. 2271. 2439. 2567. 2594. 2798	6
23	2614. 2615. 2837	3
24	2019. 2195. 2273. 2327. 2372. 2631. 2654. 2811. 2974. 2991	10
25	2042. 2396. 2582. 2588 ..	4
26	2642. 2807. 2969	3
27	2051. 2075(*3*). 2252. 2291. 2315(*3*). 2426. 2675(*3*). 2747. 2759. 2859. 2891(*3*). 2951. 2957	13
28	2066. 2129. 2279. 2495. 2564	5

29	2231. 2741	2
30	2036. 2081. 2126. 2159. 2393. 2483. 2603. 2606. 2708. 2801. 2855. 2978. 2987	13
31	2471. 2621. 2735. 2876 ..	4
32	2084. 2174. 2276. 2306. 2519. 2558	6
33	2309. 2435. 2636. 2861. 2906	5
34	2804. 2831. 2894	3
35	2549. 2909	2
36	2219(*3*). 2846	2
38	2441	1
39	2141. 2246. 2474. 2651. 2771	5
40	2729	1
41	2789	1
42	2609	1
43	2966	1

Irreg. 10

G. IV...(430).....(16232)

3	2608	1
4	2020. 2077. 2212. 2242. 2248. 2272. 2332. 2353. 2368. 2410. 2533. 2542(*2*) 2605. 2773. 2788. 2842. 2893	17
5	2032. 2073. 2074. 2101. 2118. 2125. 2152. 2158. 2173. 2178. 2202. 2230. 2247. 2290. 2398. 2422. 2433, 2494. 2577. 2641. 2776. 2830. 2853. 2965 ..	24
6	2022. 2025. 2028. 2035. 2050. 2052. 2067. 2068. 2082. 2086. 2096. 2104. 2115. 2132. 2139. 2148. 2157. 2163. 2172. 2223. 2257. 2260. 2268. 2275. 2278. 2305. 2317. 2322. 2338. 2358. 2388. 2412. 2413. 2425. 2451. 2475. 2482. 2488. 2493. 2512. 2517. 2538. 2545. 2548. 2592. 2598. 2620. 2629. 2650. 2653. 2658. 2667. 2668. 2676. 2682. 2695. 2698. 2704. 2710. 2715. 2718. 2725. 2740. 2748. 2752. 2755. 2758. 2794.	
	2802. 2872. 2892. 2907. 2914. 2938. 2977. 2997 ..	76
7	2008. 2033. 2044. 2055. 2058. 2094. 2110. 2140. 2146. 2149. 2165. 2217. 2238. 2270. 2314. 2382. 2416. 2431. 2438. 2497. 2502. 2509. 2535. 2536. 2556. 2583. 2607. 2703. 2761. 2766. 2782. 2812. 2881. 2913. 2930.. 2941. 2973	37
8	2004. 2005. 2034. 2041. 2056. 2134. 2176(*2*). 2192. 2236. 2245. 2254(*2*). 2286. 2292. 2298. 2304. 2312. 2313. 2329(*2*). 2343. 2350. 2356. 2454. 2506. 2513. 2528. 2560. 2569. 2589. 2601. 2628(*2*). 2655. 2674. 2686. 2733. 2742. 2775. 2785. 2817. 2845. 2847. 2848(*2*) 2868. 2884. 2944. 2946. 2949. 2980(*2*)	47

9	2014. 2049. 2060. 2076. 2079. 2091. 2106. 2108. 2117. 2124. 2133(*3*). 2175. 2181. 2198. 2214. 2221. 2235(*3*). 2241. 2253. 2266. 2295. 2300. 2318. 2344. 2349. 2355. 2361. 2387. 2430(*3*). 2461. 2522 2555. 2581. 2595. 2626. 2634. 2635. 2637. 2646(*3*). 2673. 2700(*3*). 2716. 2770. 2778. 2781. 2795. 2806. 2828. 2835(*3*). 2862. 2887. 2888. 2890. 2895. 2950. 2955. 2988. 2989 ..	58
10	2057. 2061. 2150. 2154. 2166. 2177. 2249. 2250. 2255. 2282. 2449. 2514. 2529. 2532. 2596. 2656. 2678. 2724. 2751. 2810. 2844. 2869. 2871. 2874. 2896. 2919. 2929. 2948. 2975	29
11	2135. 2204. 2216. 2334. 2364. 2421. 2489. 2492. 2570. 2573. 2645. 2648. 2649. 2672. 2757. 2841. 2922. 2933. 3934. 2967 ..	20
12	2006. 2009. 2045. 2105. 2156. 2168. 2169. 2196. 2211. 2225. 2229. 2316. 2331. 2366. 2379(*2*). 2390. 2420(*2*). 2432. 2450. 2466. 2484. 2499. 2597. 2661. 2691. 2696. 2701. 2702(*2*). 2739. 2754. 2780. 2816. 2822. 2824. 2825. 2852. 2873. 2900. 2993(*2*)	39
13	2015. 2222. 2453. 2469. 2481. 2510. 2679. 2721. 2792. 2826. 2901. 2984 ..	12
14	2114. 2144. 2162. 2274. 2324. 2354. 2384. 2429. 2486. 2501. 2525. 2587. 2744. 2768. 2774	15
15	2096. 2189. 2264. 2285. 2321. 2330. 2378. 2406. 2444. 2526. 2534. 2537. 2540. 2630. 2684. 2690. 2694. 2750. 2796. 2813. 2864. 2889	22
16	2180. 2201. 2336. 2546. 2561. 2624(*2*). 2639. 2669. 2882. 2921. 2994. 2996	12
17	2021. 2456. 2666. 2726 ..	4
18	2054. 2369. 2414. 2504. 2516. 2681. 2705. 2786. 2915. 2924	10
19	2294	1
20	2714. 2756(*2*). 2936. 2954. 2981	5
21	2834	1

Irreg. 13 (2). 6 (3). Sa. .19

G. VIII. . .(184). . . .(6344)

2	2002. 2013. 2080. 2088. 2128. 2170. 2233. 2277. 2392. 2632. 2737. 2832. 2068	13
3	2037. 2065. 2160. 2185. 2190. 2193. 2200. 2205. 2220. 2262. 2325. 2346. 2352. 2370. 2373. 2380. 2418. 2424. 2440. 2457. 2472. 2485. 2508. 2530. 2550. 2553. 2562. 2590. 2613. 2622. 2680. 2685. 2697. 2728. 2800. 2808. 2860. 2905. 2920. 2937. 2970. 2982. 2992	43
4	2010. 2016. 2046. 2072. 2100. 2112(*2*). 2130. 2142. 2208. 2232. 2244. 2256. 2265. 2289. 2296. 2320. 2328. 2337. 2340. 2365. 2385(*2*). 2397. 2400(*2*). 2436. 2442. 2445. 2448(*2*). 2464. 2465. 2470. 2478. 2490. 2496. 2568. 2580. 2584. 2652. 2665. 2688. 2706. 2709. 2717. 2745. 2772. 2790. 2793. 2821. 2829. 2850(*2*). 2865. 2880. 2898. 2928. 2940. 2952. 2958. 2985	57

5	2030. 2070. 2085. 2093. 2109. 2121. 2136. 2226. 2288. 2360. 2394. 2405. 2409. 2415. 2460. 2505. 2541. 2544. 2552. 2585. 2610. 2618. 2625. 2664. 2670. 2712. 2769. 2814. 2838. 2877. 2886. 2904. 2910. 2926. 2990: 3000 ..	36
6	2001. 2064. 2090. 2240. 2301. 2376. 2408. 2480. 2564. 2574. 2600. 2604. 2660. 2720. 2736. 2784. 2820. 2912. 2925. 2961. 2964. 2976	22
7	2024. 2120. 2210. 2345. 2616. 2765. 2870	7
8	2576. 2840. 2849. 2945. 2960	5
9	2261	1

Irreg. 5 (2)

G. XVI. . . .(11). . . . .(400)

2	2040. 2145. 2280. 2310. 2520. 2640. 2730. 2760 ..	8
3	2184. 2805. 2856	3

Gesamtsumme aller

Geschlechter *p.p.p*	= 4054	erwartet	4051,3
Klassen *p.p.p*	= 37092	..	37074,3
.. impr. *p.p*	= 6182		

Irreg. 18(*2*). 19(*3*). Sa= 37

Tausendergruppe X.
Geschlechter I.

27	9067
33	9283. 9403. 9643
35	9007
39	9547. 9739. 9787. 9967
41	9319
45	9043. 9463. 9907(*3*)
49	9871
51	9199. 9343. 9883
55	9391
57	9103. 9127. 9619'
63	9091. 9187. 9811(*3*). 9859
67	9151
69	9511. 9587. 9931
71	9679
75	9227. 9439. 9887. 9923
77	9631
87	9323
89	9767
91	9431. 9839

93	9203
95	9623
97	9311
99	9011
101	9479
105	9419. 9743
111	9059. 9803
119	9791
123	9467
129	9551
133	9719
135	9491. 9851
139	9239
147	9371
165	9539

.57. . .4401.

Geschlechter II.

12	9667	1
13	9157. 9277	2
14	9172	1
15	9013. 9307. 9388	3
16	9433. 9508. 9991	3
17	9223. 9535. 9703	3
18	9003(*3*). 9055. 9241. 9298. 9355. 9475. 9523. 9583. 9748(*3*). 9783. 9934(*3*)	11
19	9034. 9133. 9466. 9487. 9661. 9727	6
20	9124. 9183. 9442. 9598. 9697. 9892	6
21	9004. 9046. 9115. 9235. 9397. 9427. 9607. 9613. 9733. 9829. 9862. 9868 . .	12
22	9742. 9847	2
23	9181. 9382. 9927. 9973 . .	4
24	9406. 9409. 9423. 9502. 9507. 9601. 9763. 9817. 9874	9
25	9293. 9375. 9559. 9781. 9949	5
26	9079. 9337. 9543. 9655. 9769. 9778. 9838	7
27	9031. 9094. 9109. 9123. 9167. 9175. 9211. 9247. 9349. 9531(*3*). 9563. 9574(*3*). 9627(*3*). 9663. 9683(*3*). 9747(*3*). 9751. 9963(*3*)	18
28	9137. 9327. 9604. 9634. 9649. 9886. 9895. 9903. 9943	9
29	9098. 9148. 9244. 9532 . .	4
30	9001. 9076. 9147. 9271. 9346. 9358. 9363. 9364. 9459. 9571. 9687. 9691. 9755. 9857. 9938. 9979 . .	16
31	9263. 9901	2
32	9111. 9377. 9662. 9986 . .	4
33	9068. 9267. 9421. 9527. 9692. 9799	6
34	9122. 9166. 9326. 9332. 9458. 9556. 9586. 9826. 9998	9

35	9279. 9754	2
36	9049. 9083. 9143. 9259. 9347. 9379. 9395. 9451. 9497(*3*). 9668	10
37	9274. 9788	2
38	9524. 9567. 9908	3
39	9107. 9171. 9242. 9286. 9287. 9484. 9707. 9771. 9914. 9987	10
40	9023. 9188. 9278. 9473 ..	4
41	9302	1
42	9041. 9428. 9518. 9651. 9827. 9939. 9947	7
43	9578. 9647. 9722	3
44	9047. 9602	2
45	9019(*3*). 9251(*3*). 9411. 9437. 9626. 9899(*3*).	6
46	9038. 9351. 9407. 9721. 9759. 9983	6
47	9173. 9935. 9946	3
48	9092. 9566. 9731. 9863 ..	4
49	9221. 9335. 9599. 9677. 9818	5
50	9902	1
51	9383. 9413. 9575. 9819 ..	4
52	9359. 9689. 9833	3
54	9099(*3*). 9134. 9155. 9209	4
55	9629	1
56	9182. 9314	2
57	9029. 9179. 9356. 9461. 9659. 9836	6
59	9596	1
60	9131. 9257. 9572. 9875. 9995	5
61	9533	1
62	9119	1
63	9194. 9206. 9404. 9671. 9971	5
64	9521	1
65	9959	1
66	9236. 9611	2
67	9941	1
69	9014. 9071. 9341. 9644 ..	4
70	9806	1
71	9446	1
72	9161	1
75	9299	1
76	9764. 9929	2
77	9866	1
80	9026. 9281	2
81	9749	1
85	9974	1

Summe 265. .19580

Irreg. 14.

Geschlechter IV.

6	9823	1
7	9178. 9262. 9340. 9367. 9718. 9802. 9937	7
8	9087. 9088. 9118(*2*). 9193. 9202. 9208. 9232. 9412(*2*). 9457(*2*). 9472. 9538. 9562. 9577. 9865	14
9	9022. 9037. 9073. 9097. 9132. 9139. 9162. 9163(*3*). 9342(*3*). 9370. 9493. 9612(*3*). 9615. 9622. 9678. 9772. 9832. 9843. 9853. 9898. 9925. 9958. 9997	23
10	9025. 9058. 9190. 9238. 9289. 9517. 9553. 9573. 9628. 9732. 9793. 9808. 9837. 9850. 9913. 9942. 9948. 10000	18
11	9052. 9237. 9258. 9304. 9322. 9402. 9447. 9496. 9670. 9738. 9753. 9813. 9970	13
12	9018. 9027. 9028. 9121. 9142. 9153. 9186. 9207. 9219. 9220(*2*). 9228. 9243(*2*). 9268. 9292. 9295. 9297. 9378. 9387. 9445. 9469. 9483. 9498. 9505. 9522. 9526. 9550. 9580. 9595(*2*). 9652. 9673(*2*). 9676. 9682. 9700. 9706. 9745. 9762. 9835. 9872. 9916. 9922. 9952. 9955(*2*). 9972(*2*)	43
13	9082. 9117. 9249. 9255. 9313. 9318. 9415. 9418. 9448. 9454. 9468. 9478. 9514. 9549. 9557. 9637. 9712. 9713. 9846. 9993 . .	20
14	9017. 9032. 9066. 9217. 9226. 9253. 9353. 9354. 9436. 9501. 9529. 9542. 9642. 9658. 9664. 9757. 9775. 9784. 9820. 9878. 9988	21
15	9033. 9051. 9063. 9106. 9136. 9195. 9196. 9212. 9250. 9276. 9325. 9331. 9339. 9443. 9452. 9582. 9639. 9766. 9777. 9795. 9822. 9882. 9904. 9921. 9969. 9978	26
16	9214(*2*). 9216(*2*). 9248(*2*). 9252. 9301. 9316(*2*). 9544. 9610. 9736. 9797. 9807. 9814. 9848. 9961. 9985	15
17	9002. 9057. 9070. 9158. 9254. 9303. 9410. 9564. 9606. 9711. 9852. 9893. 9897. 9919. 9965	15
18	9012. 9015. 9069(*3*). 9075(*3*). 9154. 9234. 9315(*3*). 9357. 9362. 9376. 9385(*3*). 9396. 9398. 9444. 9477. 9482. 9495. 9558. 9603. 9675(*3*). 9693(*3*). 9715. 9723. 9782. 9801(*3*). 9844. 9873. 9891. 9910. 9915. 9964	31
19	9053. 9095. 9146. 9565. 9638. 9694. 9773. 9815. 9879. 9951. 9957. 9977 . .	12
20	9039. 9054. 9062. 9081. 9169. 9500. 9503(*2*). 9589. 9591. 9593. 9608. 9616. 9650. 9653. 9714. 9796. 9992	17
21	9036. 9126. 9197. 9201. 9229. 9261. 9334. 9368. 9392. 9414. 9481. 9489. 9499. 9515. 9561. 9699. 9708. 9710. 9770. 9774. 9855. 9909	22
22	9084. 9138. 9189. 9233. 9245. 9305. 9317. 9441. 9654. 9684. 9725. 9756. 9841. 9953. 9956. 9962. 9999	17
23	9365. 9695. 9917. 9994 . .	4
24	9113. 9159. 9275. 9291. 9308. 9399. 9422(*2*). 9426. 9474. 9488. 9519. 9579. 9641. 9666. 9728 . .	15

25	9101. 9125. 9231. 9294. 9530. 9584. 9609. 9830. 9981	9
26	9218. 9290. 9794. 9812. 9876. 9924	6
27	9038. 9050. 9074. 9164. 9260(*3*). 9369. 9374. 9509. 9704. 9726. 9831. 9989	12
28	9089. 9116. 9494. 9536. 9716. 9734. 9881(*2*). 9926. 9980	9
29	9215. 9449. 9617. 9674. 9698. 9761	6
30	9005. 9035. 9056. 9077. 9140. 9284. 9386. 9455. 9506. 9621. 9746. 9932. 9950	13
31	9191. 9884	2
32	9104(*2*). 9224. 9344(*2*). 9665. 9809(*2*)	5
33	9149. 9329. 9389. 9635. 9740	5
34	9110. 9824. 9911	3
35	9470	1
36	9266(*2*). 9476. 9779 . .	3
37	9854	1
38	9569. 9701	2
39	9896	1
40	9554	1
41	9869	1
42	9434. 9686	2

Summe 416. . .30144
Irreg. 20(*2*). 11(*3*)

Geschlechter VIII.

4	9108. 9310. 9328. 9373. 9430. 9568. 9640. 9982.	
5	9010. 9102. 9160. 9333. 9417. 9592. 9618. 9625. 9685. 9688. 9717. 9730. 9877. 9976	14
6	9040. 9042. 9045. 9072. 9085. 9100. 9112. 9130. 9145. 9150. 9206. 9213. 9265. 9270. 9288. 9300. 9352. 9408. 9432. 9438. 9465. 9492. 9552. 9585. 9597. 9648. 9696. 9760. 9790. 9804. 9810. 9828. 9867. 9888. 9900. 9928. 9940. 9990	38
7	9078. 9080. 9090. 9093. 9174. 9256. 9321. 9361. 9381. 9453. 9462. 9528. 9633. 9646. 9724. 9752. 9805. 9858. 9885. 9906 . .	20
8	9016(*2*). 9024. 9060. 9135. 9144. 9156. 9168. 9184. 9192. 9198. 9222. 9225. 9273. 9280(*2*). 9285. 9312(*2*). 9348. 9372. 9393. 9394. 9400. 9424. 9460. 9485. 9486. 9490. 9510(*2*). 9513(*2*). 9537. 9540(*2*). 9588. 9600(*2*). 9645. 9669. 9702(*2*). 9729. 9735. 9758. 9780. 9792(*2*). 9816. 9856. 9860. 9930. 9975. 9984	46
9	9061. 9064. 9105. 9114. 9180. 9185. 9200. 9272. 9390. 9420. 9450(*3*). 9471. 9541. 9548. 9555(*3*). 9630. 9657. 9705. 9709. 9720(*3*). 9825(*3*). 9849(*3*). 9889 . . .	23
10	9020. 9128. 9152. 9210. 9330. 9338. 9366. 9440. 9525. 9534. 9594. 9620. 9636. 9741. 9750. 9798. 9821. 9834. 9918	19
11	9006. 9129. 9170. 9230. 9306. 9309. 9336. 9429. 9456. 9681. 9737. 9786. 9894. 9968	14

12	9021. 9065. 9141. 9204. 9264. 9324. 9425. 9435. 9461. 9504. 9516(*2*).	
	9560. 9605. 9632. 9680(*2*). 9900. 9861. 9864. 9905. 9920. 9936. 9954. 9996 ..	23
13	9545. 9594. 9842. 9966 ..	4
14	9096. 9269. 9296. 9350. 9380. 9416. 9581. 9789. 9944	9
15	9246. 9320. 9512. 9590. 9624. 9776. 9785	7
16	9401. 9614. 9845	3
17	9086. 9890	2
18	9044. 9656	2
19	9176	1

Summe 233. .16680
Irreg. 11(*2*), 5(*3*)

Geschlechter XVI.

3	9030. 9048. 9177. 9281. 9384. 9480. 9520. 9570. 9672. 9870. 9933	11
4	9120. 9165. 9345. 9360. 9405. 9690. 9744. 9765. 9768. 9880. 9912. 9945. 9960	13
5	9009. 9576. 9660. 9840 ..	4

28. . .1680.

Geschlechter XXXII.

2	9240	1

1. . .64

Summe aller

Klassen *p.p.p.*	72549
erwartet	72572
$\Sigma\gamma\sqrt{D}$	72775
Geschlechter *p.p.p.*	4595
erwartet	4594,9

Irreg. 31(*2*). 32(*3*). . .63
Größter Quotient
1,729662 aus 9434. IV, 42
kleinster
0,2421048 aus 9823. IV, 6

Anzahl der Klassen

kleiner als die Hälfte der Wurzel	244
kleiner als die Wurzel größer als die Hälfte	566
größer als die Wurzel	199

Achthundert negative Determinanten.
der Form $-(15n + 7)$.

G. I. . . . . (93). . . . . (2793)

1	7	1
3	67	1
5	127	1
7	487	1
9	307(*3*). 367. 547. 907. 1087	5
11	967	1
13	607. 727	2
15	787. 1327. 1567. 1747. 1867. 2347. 2647	7
17	4447	1
19	3607. 4327. 5527	3
21	1627. 1987. 2467. 2707. 2767. 3067. 3187. 3907. 5107. 5647	10
23	1447. 3847	2
25	2887	1
27	3307. 3547(*3*). 4027(*3*). 4987. 6007. 6427. 7027. 9067. 10627	9
29	2287. 7207. 7687	3
31	3727. 8647	2
33	3967. 4567. 5167. 6547. 6967. 7867. 8167. 10987 .	8
35	9007	1
37	6367	1
39	4507. 5347. 7507. 9547. 9787. 9967. 10567. 11467. 11587. 11827	10
41	11047	1
43	5407. 6247. 8527. 8887 . .	4
45	5227(*3*). 5827. 6067(*3*). 6607. 8287. 8467. 8707. 9907(*3*). 10267	9
47	7927. 11887	2
51	6907. 10687	2
53	11287	1
57	9127	1
61	11527	1
63	9187	1
69	10867	1

Irreg. 6

G. II. . . . .(343). . . .(10010)

1	22. 37	2
2	52. 82. 97. 142	4
3	157. 172. 187. 202. 247. 262. 277. 397. 427. 652 . .	10
4	292. 337. 382. 457. 562. 577. 772. 862	8
5	412. 757. 847. 877. 982 . .	5
6	622. 667. 802. 1027. 1042. 1282. 1297. 1387. 1507. 1807. 2017. 2062	12
7	502. 892. 997. 1117. 1237. 1372. 1402. 1597. 1642. 1852	10
8	1252. 1657. 1822. 2137. 2302. 2377. 2962. 3217. 4687	9
9	922. 1132. 1147. 1207. 1267(*3*). 1687. 1882. 1927. 2047. 2122. 2167. 2227. 2437(*3*). 2557. 2572. 2797. 2902. 3037. 3292. 3427. 3532. 5692 . .	22
10	937. 1492. 1522. 2407. 2452. 2527. 2722. 2857. 3007. 3412. 3697. 4057. 4162. 4372. 4852	15
11	1942. 2182. 2662. 2677. 2917. 3637. 3802. 4957. 5077. 5212. 6127. 6637 . .	12
12	1732. 1762. 1777. 2107. 2587. 2692. 2827. 2947. 3127. 3202. 3742. 3787. 4132. 4222. 4267. 4387. 4657. 4747. 4867. 4882. 5182. 5587. 5707. 5947. 7417. 7492. 7522. 7987. 8002. 9667	30
13	2197. 2362. 3622. 3862. 4207. 4282. 5482. 6742. 6847. 6997. 8422. 8572. 8842. 9157. 9277. 10207. 11302	17
14	2932. 3022. 3457. 3487. 5422. 5602. 5812. 5887. 6337. 8017. 8782. 9172 . .	12
15	2092. 2602. 3142. 3517. 3667. 3877. 4087. 4357. 4492. 4627. 5047. 5062. 5437. 6022. 6442. 6667. 6727. 6892. 6922. 7087. 7162. 7387. 7477. 7627. 8227. 8677. 8812. 8947. 9307. 10147. 10732. 10957	32
16	2617. 3247. 4612. 4702. 6217. 7177. 8452. 8962. 10327. 10462. 11617 . . .	11
17	4762. 4927. 5197. 5287. 5557. 6037. 6502. 6652. 6982. 7132. 7327. 7402. 7642. 7702. 8047. 8317. 10042. 11482	18
18	4297. 5737. 5767. 5857(*3*). 6187. 6382. 6577. 6787. 7057. 7267(*3*). 7732. 7807. 8107(*3*). 8212. 8347. 8407. 8482. 8737. 8767. 10747(*3*). 10882. 11257. 11347. 11707 . . .	24
19	4252. 4597. 4822. 5722. 6172. 9487. 9727. 10597. 10837. 11062. 11197. 11677	12
20	3442. 4177. 7012. 8542. 9442. 9697. 9892. 10162. 10177	9
21	5242. 5932. 6487. 7147. 7447. 8182. 8332. 9397. 9427. 9607. 9862. 10012. 10102. 10342. 10927. 11002. 11227. 11317. 11767. 11962	20
22	6082. 6772. 7297. 7537. 7822. 9742. 9847. 11167 .	8
23	6277. 6397. 7237. 7717. 8902. 9382. 10522. 10762 .	8
24	7747. 7972. 8377. 9502. 9817. 10372. 10657. 10807. 10852. 10942. 11107. 11422. 11812	13
25	10477	1
26	7342. 7762. 9337. 11647 .	4

27	8587. 9247. 10357. 10447. 11212	5
28	11497	1
29	9532. 11722	2
30	10027. 11182. 11602. 11947	4
32	11332	1
34	10702	1
35	11437	1

Irreg. 6

G. IV....(310)....(9688)

1	112. 232	2
2	217. 322. 352. 442. 532. 592. 697. 742. 1012 ...	9
3	472. 517. 637. 682. 817. 1072. 1162. 1177. 1192. 1222. 1432. 1612	12
4	712. 832. 1057. 1312(*2*). 1357. 1417. 1462. 1477. 1537. 1552. 1582(*2*). 1717. 1792. 1897. 1912. 1957. 2077. 2212. 2242. 2272. 2332. 2542(*2*). 2842. 3172(*2*). 3322. 3502(*2). 3712	27
5	1102. 1342. 1702. 2032: 2152. 2422. 3082. 3367. 3382. 3397. 3817. 3922. 4102. 4342. 5272. 5377 ..	16
6	1837. 1972. 2257. 2317. 2482. 2512. 2752. 2872. 2977. 3052. 3232. 3337. 3577. 3592. 3652. 3892. 3937. 3997. 4012. 4117. 4192. 4237. 4417. 4432. 4477. 4537. 4552. 4642. 4717. 4792. 4942. 4972. 5317. 5362. 5467. 5497. 5842. 6157. 6262. 6307. 6352. 6472. 6682. 6862. 7282. 7837. 10432	47
7	2497. 2782. 2812. 3097. 3112. 3277. 3352. 3562. 3982. 4582. 4732. 5122. 5137. 5302. 5902. 5977. 6142. 6517. 7792. 9262. 9367. 9802. 9937	23
8	3262(*2*). 3682. 3757. 3772. 3832. 4402. 4672(*2*). 4777(*2*). 5002. 5017.. 5257. 5392. 5572. 5632. 5752. 5917. 5962. 6052(*2*). 6112. 6202. 6532. 6697. 6757. 6817. 7252. 7312. 7357. 7582(*2*). 7597. 8122. 8197. 8257. 8497. 8992(*2*). 9202. 9232. 9412(*2*). 9457(*2*). 9472. 9562. 9577. 10132(*2*). 10312. 10537. 10642. 11092. 11377. 11512. 11572. 11797	50
9	4042. 4072. 4147. 4837. 4897. 4912(*3*). 5452. 5542. 5677. 5782. 5872. 6322. 6412. 6457. 7102. 7117. 7372. 7852. 7942. 8062. 8092. 8152. 8242(*3*). 8752. 8827(*3*). 9022. 9037. 9097. 9622. 9772. 9832. 9997. 10222. 10252(*3*). 10717. 10822. 11407. 11692. 11782. 11992	40
10	4462. 4807. 5092. 5332. 6292. 6592. 6712. 6802. 6937. 7432. 7897. 8077. 8137. 8302. 8557. 8617. 8692. 8857. 8977. 9517. 10057. 10087. 10297. 10402. 10552. 10777. 10972. 11122. 11272. 11932	30
11	5662. 7222. 7567. 7612. 7882. 8362. 8662. 8917. 9052. 9322. 10417. 10492. 11452. 11902	14
12	5617. 6562. 6877. 7042. 7552. 7957. 8392. 8722. 9142. 9292. 9652. 9682. 9922. 9952. 10237. 10387. 10612. 10672. 11017. 11542. 11737. 11917	22

13	8872. 9082. 9637. 9712. 10117. 11632	6
14	8032. 9217. 9757. 11662. 11842	5
15	8797. 10072. 10507 ...	3
16	10282. 10897. 11392(*2*). 11857	4

Irreg. 19

G. VIII. ...(54). ...(1856)

2	952. 1672. 2002. 2392. 2632. 2737	6
3	2992. 3157. 3952. 4522. 5032. 5797. 6097. 6232. 6832. 7912	10
4	3472. 4312. 5152(*2*). 5992. 6622. 6952. 7072(*2*). 7672(*2*). 8437. 8512. 8932. 9982. 11152. 11872	14
5	5512. 7192. 7462. 7657. 7777. 8632. 9592. 9877. 11242. 11362. 11557 ...	11
6	8272. 9112. 9352. 10192. 10582. 10792. 10912. 11032. 11077. 11137. 11752. 11977	12
7	8602	1

Irreg. 3

Alle Geschlechter 2451 erwartet 2445,10
alle Klassen 24347 erwartet 24358,82

$$\left.\begin{array}{l}\left.\begin{array}{ll}8n\,.\,.\,.\,.\,. & 3068\\ 8n+4\,.\,. & 3010\end{array}\right\} 6078\\ \left.\begin{array}{ll}8n+2\,.\,. & 3062\\ 8n+6\,.\,. & 3034\end{array}\right\} 6096\end{array}\right\} 12174$$

$$\left.\begin{array}{l}\left.\begin{array}{ll}8n+1\,.\,. & 3076\\ 8n+5\,.\,. & 3026\end{array}\right\} 6102\\ \left.\begin{array}{ll}8n+3\,.\,. & 3033\\ 8n+7\,.\,. & 3038\end{array}\right\} 6071\end{array}\right\} 12173$$

$7n\,.\,.\,.\,.\,.$	$115\,.\,.$	3411
$7n+1\,.\,.$	$115\,.\,.$	3009
$7n+2\,.\,.$	$114\,.\,.$	2975
$7n+4\,.\,.$	$114\,.\,.$	2993
$R\,7\,.\,.\,.$	$343\,.\,.$	8977
$7n+3\,.\,.$	$114\,.\,.$	3979
$7n+5\,.\,.$	$114\,.\,.$	3998
$7n+6\,.\,.$	$114\,.\,.$	3982
$N\,7\,.\,.\,.$	$342\,.\,.$	11959

Impr. Klassen 4049

Eigentliche zusammen mit uneigentlichen
28396 erwartet 28418,62

Achthundert negative Determinanten.
der Form $-(15n + 13)$

G. I. . . .(91). . . . .(2561)

3	43. 163	2
5	103	1
7	223. 343. 463	3
9	283. 643. 823. 883. 1423 .	5
11	1303	1
13	2143	1
15	523. 1123. 1723. 2203. 2683	5
17	1663. 1783	2
19	1063. 1543. 3343. 3463 . .	4
21	1483. 2083. 2503. 4603. 5923	5
23	4783. 6703	2
25	5023. 5503	2
27	2803. 3163. 3643. 3943. 4243. 4363. 4483. 4723. 4903. 5443(*3*). 6043. 6763. 6883. 7723(*3*). 8563. 8803(*3*). 11383 .	17
29	2383. 3583. 3823. 5743. 8863	5
31	11863	1
33	4423. 4663. 5623. 5683. 6163. 6343. 6823. 7603. 8443. 9283. 9403. 9643 . .	12
35	11503	1
39	4003. 7243. 7963. 11743. 11923	5
41	10903	1
43	8263	1
45	5323. 5563(*3*). 9043. 9463. 10243. 10663. 10723(*3*). 11083 . . .	8
51	8623. 9343. 9883. 10303. 11443	5
57	8923. 9103	2

G. II. . . .(340). . . .(10110)

1.	13. 28. 58	3
2	73. 148. 193	3
3	118. 268. 298. 358. 403 .	5
4	178. 313. 388. 478. 583 .	5
5	373. 508. 538. 613. 853. 1093. 1213. 1318	8
6	433. 628. 673. 718. 763. 898. 1003. 1033. 1108. 1138. 1198. 1243. 1588. 1618. 1873	15
7	703. 733. 778. 838. 1183. 1453. 1948. 2293	8
8	943. 958. 1153. 1348. 1438. 1828. 2113. 2308. 2578. 2878	10
9	1018. 1228(*3*). 1363. 1468. 1603. 1843. 1933. 1963. 2023. 2038. 2053. 2188. 2443. 2458. 2563(*3*). 2923. 2998. 3238. 3523. 3628. 3733. 3763. 4348. 4678. 5413	25

10	1678. 1753. 1858. 2473. 2638. 2743. 2818. 2983. 3028. 3103. 3118. 3508. 4153	13
11	1693. 1903. 2263. 2623. 2863. 3418. 3703. 3868. 3958. 4918. 5098. 8023. 8143	13
12	1993. 2098. 2323. 2593. 2713. 2953. 3283. 3313. 3403. 3433. 3778. 3883. 4063. 4258. 4273. 4513. 4843. 5188. 5233. 5758. 5938. 6073. 6238. 8068 . .	24
13	2218. 2428. 2908. 3373. 3613. 3853. 3898. 4093. 4618. 4933. 5383. 5818. 5878. 6598. 7078. 8383. 8743. 10333. 10543	19
14	3673. 3988. 4078. 4183. 4468. 4948. 5218. 5263. 6103. 6388. 6658. 6673. 7438. 7753. 7858. 8233. 8353. 11113. 11278	19
15	2518. 3148. 3223. 4138. 4813. 5203. 5398. 5653. 5803. 6268. 6403. 6463. 6778. 6988. 7123. 7303. 7363. 7468. 7483. 8053. 8458. 8698. 9013. 9388. 10483. 10588	26
16	2833. 4993. 6178. 6628. 7183. 7393. 8548. 8578. 9433. 9508. 10558	11
17	3253. 4303. 5308. 5578. 7333. 7558. 8038. 9223. 9703	9
18	3043. 3793. 4963. 5458. 5998. 6283(*3*). 6418. 6553. 6583(*3*). 6793. 7543. 9298. 9523. 9583. 9748(*3*). 10003. 10018. 10228. 10603. 10753. 10798(*3*). 11698 . . .	22
19	5158. 5638. 6373. 6733. 7573. 7933. 8983. 9133. 10198. 11173	10
20	3748. 5143. 6223. 6718. 6898. 7063. 7423. 8098. 8158. 9598. 10063. 10513. 10993. 11428. 11953 . . .	15
21	4198. 6133. 6508. 6523. 7213. 7318. 7948. 7978. 8518. 9613. 9733. 9868. 10093. 10123. 10363. 10378. 10453. 10828. 11023. 11068. 11263. 11323. 11878	23
22	5113. 5953. 5983. 7663. 7783. 7873. 7903. 7993. 8713. 10273. 10708. 11668. 11758	13
23	5788. 8278. 8293. 8893. 9973. 10423. 10618	7
24	4798. 6943. 7003. 7108. 8083. 8503. 8683. 8818. 9763. 10843. 10963. 11143. 11203 11353. 11563	15
25	10783. 11548	2
26	8788. 9778. 9838	3
27	8203. 11683(*3*)	2
28	9943. 10078. 11038. 11593 .	4
29	9148	1
30	9358. 11623	2
31	11983	1
32	10183. 10468	2
33	11338	1
40	11833	1

G. IV. . . .(320). . . .(10088)

1	88. 133. 253	3
2	208. 238. 328. 418. 448. 553. 568. 598. 658. 793. 928	11

3	493. 688. 748. 808. 913. 973. 988. 1048. 1258. 1558. 1708. 1978. 2608 . .	13
4	868. 1078. 1168. 1393. 1408. 1498. 1513(*2*). 1528. 1633. 1738. 1813. 1918(*2*). 2248. 2353. 2368. 2533. 2773. 2788(*2*). 2893. 3088. 3193. 3298. 3448	23
5	1273. 1333. 1378. 1573. 1648. 1798. 2158. 2173. 2398. 3133. 3178. 3388. 3928. 3973. 4558. 4873 . .	16
6	1888. 2068. 2278. 2338. 2413. 2488. 2548. 2653. 2668. 2698. 2758. 2938. 3073. 3208. 3268. 3478.	
	3598. 3658. 3718. 4018. 4033. 4108. 4123. 4168. 4288. 4393. 4438. 4453. 4708. 4753. 4768. 4978. 5083. 5128. 5173. 5293. 5338. 5518. 5548. 5713. 5728. 6028. 6433. 6493. 6913. 7018. 7093. 7228. 7813. 8248. 9823	51
7	2008. 3538. 3568. 3838. 4213. 4333. 4498. 4543. 4573. 5038. 5488. 5608. 5833. 5863. 6013. 6193. 6253. 6538. 6568. 6973. 7198. 7408. 9178. 9718. 10858. 10873	26
8	2848(*2*). 3013. 3058. 3328. 3358(*2*). 3493. 4228. 4318(*2*). 4633(*2*). 4738. 5008. 5248(*2*). 5428. 5533. 5668. 5908. 6148(*2*). 6208(*2*). 6868(*2*). 6958(*2*). 7033. 7168. 7288. 7588. 7648. 7828. 8308. 8338. 8638(*2*). 8653. 8878(*2*). 9088. 9118(*2*). 9193. 9208. 9538. 10033. 10138. 11533. 11848	40
9	3688. 4378. 4528. 4588. 4693. 4828. 5068(*3*). 5773. 6313. 6359. 6643. 6748. 7258. 7513. 7528. 7678. 7693(*3*). 7708. 7738. 7918. 8188. 8218. 8323(*3*). 8488. 8668. 8908. 8998. 9073. 9163(*3*). 9493. 9853. 9898. 9958. 10213. 10288. 10393. 10693. 11158. 11188. 11608. 11803. 11818. 11893	43
10	4858. 5053. 5473. 5968. 6058. 6088. 6613. 7153. 7273. 7453. 7498. 7798. 8128. 8173. 8473. 8593. 8608. 8758. 8773. 8833. 8953. 9058. 9238. 9553. 9628. 9793. 9808. 9913. 10108. 10438. 10888. 10978. 11053. 11293. 11398. 11458. 11938	37
11	6298. 7618. 7768. 8413. 8728. 10648. 11638. 11653	8
12	5353. 5893. 6838. 6928. 7048. 7348. 7633. 7843. 8428. 9028. 9268. 9673(*2*). 10048. 10258. 10348. 10768. 11008. 11218. 11308. 11488. 11578. 11788. 11908. 11998	24
13	8938. 9313. 9418. 9448. 9478. 10498. 10678. 10918. 11098. 11518	10
14	6478. 7138. 9253. 9658. 9988. 10573. 10633. 10933. 11233. 11728	10
15	8368. 10408. 10813. 11413. 11773	5

G. VIII. . . .(48). . . .(1600)

2	1288. 1768. 2128. 2233. 2968. 4048	6
3	2728. 3553. 3913. 4648. 4888. 5278. 6448	7

4	3808. 5593. 5698. 5848. 6118. 6328(*2*). 6688(*2*). 6853. 7378. 8398. 8848. 8968. 9328. 9373. 9568. 10168(*2*). 10528(*2*). 10948. 11368. 11713(*2*)	20
5	4408. 5368. 6808. 9688. 10153. 10738	6
6	7888. 8533. 9928. 10318. 11473. 11968	6
7	8113. 11128. 11248	3

G. XVI....(1).....(32)

2	8008	1

Summe G. 2451 Cl. 24391

Irreg. 37 impr. 4075

			$15n+7$,13	
$7n$.....	115..	3435...	230..	6846
$7n+1$..	114..	2988...	229..	5997
$7n+2$..	114...	2987...	228..	5962
$7n+4$..	114..	2994...	228..	5987
$R\,7$...	342..	8969...	685..	17946
$7n+3$..	114..	4005...	228..	7984
$7n+5$..	114..	3975...	228..	7973
$7n+6$..	115..	4007...	229..	7989
$N\,7$...	343..	11987...	685..	23946
Alle .	800.	24391..	1600..	48738

Quot. min. 0,2349782 aus 163,2608
max. 0,7354322 aus 11833

Det. der Form

$-(15n+13)$..	68	305	271	128	27
$-(15n+7)$...	69	316	264	130	21
	0,3	0,4	0,5	0,6	

[Det. in Hundertergruppe 10000 der Form $15n$]

G. VIII....(3).....(1464)

48	999975
63	999945
72	999930

G. XVI....(3).....(2224)

39	999915
*44	999900
56	999990(*2*)

G. XXXII. .(1). . . . . .(576)
18 999960
104. 4264
Impr. 592

[Quotient $< \frac{1}{2} <$ $< 1 <$]

in Hundertergruppe	11	Det.	24.	1.	56. . 19
	12		28		51 21
	13		21		58 21
	14		27		57 16
	15		21		62 17
	16		22		56 22
	17		29		52 19
	18		25.		57 18
	19		22		64 14
	20		21		61 18
	21		18		62 20
	22		18		63 19
	23		19		61 20
	24		27		55 18
	25		31		51 18
	26		26		54 20
	27		30		51 19
	28		27		53 20
	29		23		57 20
	30		24		58 18
	117		24		56 20
	118		20		61 19
	119		24		61 15
	120		29		52 19

Negative Determinanten.

in Hundertergruppe		Quotient		
1	max.	1,271998	aus Det.	89
	min.	0,2626128		58
2		1,435917		194
		0,2349782		163

22	1,685723	2141
	0,2808228	2143
23	1,645848	2246
	0,2923654	2293
24	1,479278	2369
	0,2897240	2335
27	1,6445315	2609
	0,2895883	2683
28	1,5527075	2789
	0,3030216	2783
29	1,5778996	2834
	0,2974718	2893
30	1,604748	2939
	0,2936893	2968
91	1,684117	9026
	0,2835515	9067
92	1,586777	9176
	0,2717044	9157
93	1,660820	9281
	0,2699414	9277
94	1,518533	9371
	0,2893063	9367
95	1,729662	9434
	0,3287980	9472
96	1,689400	9539
	0,3269906	9577
97	1,707014	9686
	0,2440986	9667
99	1,650848	9869
	0,2420048	9823
100	1,702214	9974
	0,2808862	9937
117	1,6654535	11681
	0,2964744	11650
118	1,810938	11714
	0,294621	11797
119	1,579112	11864
	0,2846194	11863
120	1,5326965	11921
	0,3287433	11992

Positive Determinanten.

Hundertergruppe 1.
Quadratische Determinanten entfallen: 10.

G. I. . . .(12)
1 2. 5. 13. 17. 29. 41. 53. 61. 73. 89. 97
3 37
G. II. . . .(51)
1 3. 6. 7. 8. 10. 11. 12. 14. 18. 19. 20. 21. 22. 23. 26. 27. 28. 31. 32. 33. 38. 43. 44. 45. 46. 47. 50. 52. 54. 57. 58. 59. 62. 65. 67. 68. 69. 71. 74. 76. 77. 83. 85. 86. 92. 93. 94. 98
2 34. 82
3 79
G. IV. . .(27)
1 15. 24. 30. 35. 39. 40. 42. 48. 51. 55. 56. 60. 63. 66. 70. 72. 75. 78. 80. 84. 87. 88. 90. 91. 95. 96. 99

Hundertergruppe 2.
Es entfallen: 4.

G. I. . . .(11)
1 109. 113. 125. 137. 149. 157. 173. 181. 193
3 101. 197
G. II. . . .(41)
1 103. 106. 107. 108. 116. 117. 118. 122. 124. 127. 128. 129. 131. 133. 134. 139. 142. 151. 153. 158. 161. 162. 163. 164. 166. 167. 172. 174. 177. 179. 185. 188. 191. 199
2 145. 146. 178. 194
3 141. 148. 189
G. IV. . .(40)
1 102. 104. 105. 110. 111. 112. 114. 115. 119. 123. 126. 130. 132. 135. 136. 138. 140. 143. 147. 152. 154. 155. 156. 159. 160. 165. 170. 171. 175. 176. 180. 182. 183. 184. 186. 187. 190. 192. 198. 200
G. VIII. . .(4)
1 120. 150. 168. 195

Hundertergruppe 3.

G. I
1 233. 241. 277. 281. 293
3 229. 257. 269
G. II
1 201. 202. 206. 211. 212. 213. 214. 217. 218. 229. 236. 237. 239. 242. 243. 244. 245. 249. 250. 251. 253. 261. 262. 263. 265. 268. 271. 278. 283. 284. 292. 297. 298

2 205. 221. 274
3 223. 226. 254. 291
G. IV
1 203. 204. 207. 215. 216. 222. 228. 230. 232. 234. 238. 246. 247. 248. 252. 258. 259. 260. 266. 267. 270. 272. 273. 275. 276. 279. 282. 285. 286. 287. 290. 294. 295. 296. 299. 300
2 219. 220. 224. 288
3 235
G. VIII
1 210. 231. 240. 255. 264. 280

Hundertergruppe 9.

G. I. . . . .(7)
1 809. 821. 853. 857. 881
3 829. 877
G. II. . . .(32)
1 801. 811. 823. 827. 833. 838. 844. 845. 849. 859. 862. 863. 865. 869. 873. 878. 883. 886. 887. 889. 893
2 802. 818. 866
3 813. 837. 839. 842. 892
5 817
6 898
14 (841)
G. IV. . . .(52)
1 803. 804. 805. 806. 807. 808. 810. 814. 815. 822. 824. 825. 826. 830. 831. 832. 834. 835. 836. 843. 846. 847. 848. 850. 851. 852. 854. 856. 860. 861. 864. 867. 868. 871. 872. 875. 879. 882. 885
2 812. 820. 828. 876. 884. 890. 891. 896. 897
3 874. 894. 895. 899
G. VIII. . .(8)
1 816. 819. 855. 858. 888
2 870. 880. (900)
G. XVI. . .(1)
1 840

Hundertergruppe 10.

G. I. . . .(6). . . . .(8)
1 929. 937. 941. 953. 977
3 997
G. II. . .(38). . . .(130)
1 907. 908. 911. 913. 917. 919. 921. 922. 926. 932. 947. 949. 956. 958. 964. 965. 967. 971. 972. 974. 981. 983. 989. 991. 998
2 914
3 905. 909. 916. 925. 933. 934. 973. 985. 993
5 982

6 901
[15 961]
G. IV. . . .(40). . .(224)
1 902. 918. 923. 927. 928. 931. 938. 942. 944. 945. 946. 948. 950. 951. 954. 955. 957. 962. 968. 969. 970. 976. 978. 980. 986. 988. 995. 996. 999. 1000
2 939. 943. 959. 963. 979. 992
3 906. 940
4 904. 994
G. VIII. . .(16). . .(144)
1 903. 912. 915. 920. 924. 930. 935. 936. 952. 966. 975. 984. 987. 990
2 910. 960

Summe 370

G. I
1 313. 317
3 349. 373. 389. 397. 557. 677. 701. 709. 733. 757. 761
5 401
7 577
G. II
1 301. 302. 307. 309. 311. 314.
2 305
3 316. 321. 325. 326
5 727
G. IV
1 303. 304. 308. 310. 318. 319. 320. 327
2 306. 322. 323
G. VIII
1 312. 315

TAFEL
ZUR
KREISTEILUNG.

2	5
4	17
6	37
8	5 . 13
10	101
12	5 . 29
14	197
17	5 . 29
19	181
22	5 . 97
27	5 . 73
30	17 . 53
32	5 . 5 . 41
34	13 . 89
38	5 . 17 . 17
43	5 . 5 . 37
46	29 . 73
50	41 . 61
57	5 . 5 . 5 . 13
70	13 . 13 . 29
73	5 . 13 . 41
76	53 . 109
81	17 . 193
91	41 . 101
98	5 . 17 . 113
100	73 . 137
111	61 . 101
117	5 . 37 . 37
123	5 . 17 . 89
129	53 . 157
133	5 . 29 . 61
157	5 . 5 . 17 . 29
172	5 . 61 . 97
174	13 . 17 . 137
183	5 . 17 . 197
191	17 . 29 . 37
193	5 . 5 . 5 . 149
211	113 . 197
216	13 . 37 . 97
237	5 . 41 . 137
242	5 . 13 . 17 . 53
253	5 . 37 . 173

3	5
5	13
7	5 . 5
9	41
11	61
13	5 . 17
15	113
18	5 . 5 . 13
21	13 . 17
23	5 . 53
28	5 . 157
31	13 . 37
33	5 . 109
37	5 . 137
41	29 . 29
44	13 . 149
47	5 . 13 . 17
55	17 . 89
68	5 . 5 . 5 . 37
72	5 . 17 . 61
75	29 . 97
80	37 . 173
83	5 . 13 . 53
93	5 . 5 . 173
99	13 . 13 . 29
105	37 . 149
112	5 . 13 . 193
119	73 . 97
128	5 . 29 . 113
132	5 . 5 . 17 . 41
142	5 . 37 . 109
162	5 . 29 . 181
173	5 . 41 . 73
182	5 . 5 . 5 . 5 . 53
185	109 . 157
192	5 . 73 . 101
200	13 . 17 . 181
212	5 . 89 . 101
233	5 . 61 . 89
239	13 . 13 . 13 . 13
251	17 . 17 . 109
255	13 . 41 . 61

265	13 . 37 . 73	268	5 . 5 . 13 . 13 . 17
278	5 . 13 . 29 . 41	293	5 . 5 . 17 . 101
294	13 . 61 . 109	302	5 . 17 . 29 37
307	5 . 5 . 5 . 13 . 29	313	5 . 97 . 101
319	17 . 41 . 73	327	5 . 17 . 17 . 37
342	5 . 149 . 157	343	5 . 5 . 13 . 181
360	29 . 41 . 109	378	5 . 17 . 41 . 41
394	29 . 53 . 101	401	37 . 41 . 53
403	5 . 109 . 149	408	5 . 13 . 13 . 197
411	13 . 73 . 89	437	5 . 13 . 13 . 113
438	5 . 17 . 37 . 61	443	5 . 5 . 5 . 5 . 157
447	5 . 13 . 29 . 53	463	5 . 13 . 17 . 97
467	5 . 113 . 193	499	13 . 61 . 157
500	53 . 53 . 89	507	5 . 5 . 53 . 97
512	5 . 13 . 37 . 109	515	13 . 101 . 101
524	37 . 41 . 181	538	5 . 13 . 61 . 73
557	5 . 5 . 5 . 17 . 73	560	53 . 61 . 97
568	5 . 5 . 5 . 29 . 89	577	5 . 13 . 13 . 197
599	17 . 61 . 173	606	13 . 13 . 41 . 53
616	13 . 17 . 17 . 101	621	29 . 61 . 109
657	5 . 5 . 89 . 97	660	37 . 61 . 193
682	5 . 5 . 5 . 61 . 61	684	13 . 17 . 29 . 73
693	5 . 5 . 5 . 17 . 113	697	5 . 13 . 37 . 101
701	17 . 97 . 149	743	5 . 5 . 61 . 181
746	13 . 13 . 37 . 89	757	5 . 5 . 73 . 157
772	5 . 13 . 53 . 173	776	73 . 73 . 113
785	13 . 137 . 173	798	5 . 13 . 97 . 101
818	5 . 5 . 5 . 53 . 101	829	17 . 17 . 29 . 41
853	5 . 13 . 29 . 193	882	5 . 5 . 29 . 29 . 37
905	13 . 17 . 17 . 109	919	37 . 101 . 113
922	5 . 17 . 73 . 137	924	53 . 89 . 181
931	13 . 17 . 37 . 53	945	29 . 89 . 173
948	5 . 17 . 97 . 109	993	5 . 5 . 13 . 37 . 41
999	17 . 149 . 197	1032	5 . 5 . 13 . 29 . 113
1057	5 . 5 . 5 . 41 . 109	1067	5 . 17 . 37 . 181
1068	5 . 5 . 5 . 5 . 5 . 5 . 73	1087	5 . 13 . 61 . 149
1118	5 . 5 . 17 . 17 . 173	1123	5 . 13 . 89 . 109
1143	5 . 5 . 17 . 29 . 53	1148	5 . 29 . 61 . 149
1196	53 . 137 . 197	1228	5 . 17 . 113 . 157
1239	41 . 97 . 193	1270	61 . 137 . 193
1303	5 . 41 . 41 . 101	1341	73 . 109 . 113
1385	41 . 149 . 157	1393	5 . 5 . 197 . 197
1407	5 . 5 . 17 . 17 . 137	1432	5 . 5 . 5 . 5 . 17 . 193
1433	5 . 29 . 73 . 97	1467	5 . 29 . 41 . 181
1477	5 . 13 . 97 . 173	1560	17 . 37 . 53 . 73
1567	5 . 41 . 53 . 113	1568	5 . 5 . 5 . 13 . 17 . 89
1597	5 . 37 . 61 . 113	1607	5 . 5 . 13 . 29 . 137
1636	17 . 29 . 61 . 89	1744	137 . 149 . 149

1772	5 . 17 . 17 . 41 . 53	1818	5 . 5 . 5 . 137 . 193
1823	5 . 17 . 113 . 173	1832	5 . 5 . 17 . 53 . 149
1893	5 . 5 . 13 . 37 . 149	1918	5 . 5 . 37 . 41 . 97
1929	13 . 13 . 101 . 109	1955	13 . 29 . 37 . 137
1984	13 . 29 . 53 . 197	2010	13 . 17 . 101 . 181
2013	5 . 29 . 89 . 157	2018	5 . 5 . 29 . 41 . 137
2042	5 . 29 . 149 . 193	2059	13 . 41 . 41 . 97
2153	5 . 13 . 181 197	2163	5 . 13 . 17 . 29 . 73
2191	89 . 149 . 181	2309	13 . 53 . 53 . 73
2350	17 . 17 . 97 . 197	2428	5 . 41 . 149 . 193
2436	13 . 13 . 13 . 37 . 73	2515	101 . 173 . 181
2540	13 . 29 . 109 . 157	2547	5 . 37 . 89 . 197
2621	13 . 37 . 37 . 193	2673	5 . 13 . 17 . 53 . 61
2697	5 41 . 113 . 157	2738	5 . 13 . 29 . 41 . 97
2801	17 . 29 . 73 . 109	2818	5 . 5 . 5 . 17 . 37 . 101
2917	5 . 13 . 29 . 37 . 61	2943	5 . 5 . 5 . 5 . 13 . 13 . 41
3039	17 . 61 . 61 . 73	3112	5 . 13 . 13 . 73 . 157
3141	13 . 13 . 17 . 17 . 101	3149	17 . 29 . 89 . 113
3166	17 . 41 . 73 . 197	3207	5 . 5 . 29 . 41 . 173
3323	5 . 13 . 29 . 29 . 101	3362	5 . 13 . 17 . 53 . 193
3405	29 . 29 . 61 . 113	3458	5 . 73 . 181 . 181
3521	29 . 37 . 53 . 109	3532	5 . 5 . 17 . 149 . 197
3583	5 . 13 . 17 . 37 . 157	3740	41 . 41 . 53 . 157
3782	5 . 5 . 29 . 109 . 181	3793	5 . 5 . 53 . 61 . 89
3957	5 . 5 . 13 . 13 . 17 . 109	4193	5 . 5 . 5 . 5 . 5 . 29 . 97
4217	5 . 13 . 29 . 53 . 89	4232	5 . 5 . 41 . 101 . 173
4246	13 . 17 . 29 . 29 . 97	4327	5 . 89 . 109 . 193
4484	17 . 89 . 97 . 137	4535	17 . 53 . 101 . 113
4545	13 . 37 . 109 . 197	4581	13 . 53 . 97 . 157
4594	13 . 17 . 29 . 37 . 89	4662	5 . 13 . 13 . 17 . 17 . 89
4747	5 . 17 . 41 . 53 . 61	4906	13 . 53 . 181 . 193
4937	5 . 73 . 173 . 193	4952	5 . 37 . 41 . 53 . 61
5052	5 . 13 . 41 . 61 . 157	5087	5 . 17 . 29 . 29 . 181
5257	5 . 5 . 13 . 17 . 41 . 61	5283	5 . 13 . 17 . 73 . 173
5357	5 . 5 . 61 . 97 . 97	5443	5 . 5 . 5 . 5 . 137 . 173
5507	5 . 5 . 13 . 13 . 37 . 97	5648	5 . 17 . 53 . 73 . 97
5667	5 . 29 . 37 . 41 . 73	5701	29 . 53 . 97 . 109
5767	5 . 13 . 17 . 101 . 149	5928	5 . 29 . 29 . 61 . 137
5962	5 . 13 . 29 . 109 . 173	6065	17 . 53 . 137 . 149
6107	5 . 5 . 17 . 17 . 29 89	6118	5 . 5 . 13 . 41 . 53 . 53
6252	5 . 17 . 29 . 101 . 157	6481	17 . 37 . 173 . 193
6682	5 . 5 . 5 . 29 . 109 . 113	6898	5 . 13 . 17 . 17 . 17 . 149
6908	5 . 13 . 73 . 89 113	6943	5 . 5 . 5 . 29 . 61 . 109
6962	5 . 37 . 37 . 73 . 97	7093	5 . 5 . 13 . 17 . 29 . 157
7161	17 . 101 . 109 . 137	7443	5 . 5 . 5 . 37 . 53 . 113
7697	5 . 17 . 29 . 61 . 197	7782	5 . 5 . 13 . 17 . 97 . 113
8224	13 . 17 . 29 . 61 . 173	8307	5 . 5 . 5 . 5 . 5 . 61 . 181
8368	5 . 5 . 17 . 37 . 61 . 73		

8393	5 . 5 . 13 . 29 . 37 . 101
8578	5 . 37 . 41 . 89 . 109
9152	5 . 29 . 41 . 73 . 193
9298	5 . 41 . 53 . 73 . 109
9466	29 . 37 . 37 . 37 . 61
9703	5 . 13 . 13 . 17 . 29 . 113
9872	5 . 13 . 13 . 29 . 41 . 97
10298	5 . 17 . 61 . 113 . 181
10833	5 . 17 . 41 . 113 . 149
11471	13 . 17 . 41 . 53 . 137
12332	5 . 5 . 13 . 41 . 101 . 113
12882	5 . 5 . 17 . 37 . 61 . 173
13043	5 . 5 . 17 . 17 . 61 . 193
13241	29 . 101 . 173 . 173
13545	17 . 17 . 53 . 53 . 113
14140	17 . 29 . 37 . 97 . 113
14573	5 . 17 . 73 . 109 . 157
14773	5 . 13 . 13 . 29 . 61 . 73
14958	5 . 13 . 101 . 173 . 197
16513	5 . 29 . 53 . 113 . 157
17191	13 . 17 . 61 . 97 . 113
17766	13 . 37 . 73 . 89 . 101
18258	5 . 29 . 97 . 137 . 173
18543	5 . 5 . 13 . 17 . 29 . 29 . 37
19283	5 . 37 . 37 . 157 . 173
19534	13 . 13 . 13 . 29 . 53 . 113
19703	5 . 13 . 13 . 29 . 89 . 89
19911	13 . 17 . 29 . 157 . 197
20457	5 . 5 . 13 . 29 . 149 . 149
21705	13 . 17 . 61 . 101 . 173
22008	5 . 41 . 109 . 149 . 157
22231	29 . 37 . 41 . 41 . 137
24331	13 . 17 . 89 . 101 . 149
24816	17 . 17 . 61 . 181 . 193
25523	5 . 53 . 73 . 113 . 149
25793	5 . 5 . 17 . 29 . 137 . 197
26018	5 . 5 . 13 . 97 . 109 . 197
28205	13 . 29 . 73 . 97 . 149
28862	5 . 17 . 17 . 53 . 73 . 149
30027	5 . 29 . 89 . 181 . 193
30383	5 . 17 . 17 . 37 . 89 . 97
32258	5 . 13 . 37 . 41 . 61 . 173
32807	5 . 5 . 5 . 13 . 61 . 61 . 89
32973	5 . 13 . 37 . 37 . 41 . 149
34208	5 . 13 . 13 . 17 . 29 . 53 . 53
35857	5 . 5 . 17 . 61 . 137 . 181
37057	5 . 5 . 5 . 5 . 73 . 101 . 149
37770	13 . 17 . 29 . 41 . 61 . 89
8457	5 . 5 . 53 . 137 . 197
9133	5 . 17 . 37 . 89 . 149
9193	5 . 5 . 5 . 5 . 17 . 41 . 97
9431	17 . 97 . 149 . 181
9667	5 . 13 . 41 . 89 . 197
9762	5 . 17 . 37 . 157 . 193
9901	13 . 13 . 29 . 73 . 137
10312	5 . 29 . 53 . 101 . 137
11018	5 . 5 . 157 . 157 . 197
11981	13 . 17 . 41 . 89 . 89
12433	5 . 13 . 61 . 101 . 193
12943	5 . 5 . 5 . 5 . 13 . 13 . 13 . 61
13068	5 . 5 . 5 . 53 . 149 . 173
13252	5 . 13 . 13 . 37 . 41 . 137
13918	5 . 5 . 13 . 37 . 89 . 181
14318	5 . 5 . 5 . 13 . 17 . 41 . 181
14646	13 . 37 . 41 . 73 . 149
14942	5 . 13 . 13 . 37 . 37 . 193
15075	13 . 17 . 53 . 89 . 109
16928	5 . 17 . 109 . 157 . 197
17557	5 . 5 . 5 . 17 . 29 . 41 . 61
17923	5 . 61 . 61 . 89 . 97
18432	5 . 5 . 5 . 17 . 29 . 37 . 149
19123	5 . 29 . 37 . 173 . 197
19326	13 . 29 . 61 . 109 . 149
19653	5 . 37 . 61 . 109 . 157
19902	5 . 73 . 89 . 89 . 137
20080	13 . 29 . 61 . 89 . 197
21124	29 . 41 . 53 . 73 . 97
21907	5 . 5 . 29 . 29 . 101 . 113
22157	5 . 5 . 13 . 37 . 137 . 149
24263	5 . 13 . 17 . 41 . 73 . 89
24778	5 . 29 . 149 . 157 . 181
25462	5 . 13 . 17 . 37 . 101 . 157
25683	5 . 13 . 17 . 17 . 97 . 181
25943	5 . 5 . 5 . 13 . 29 . 37 . 193
27493	5 . 5 . 17 . 17 . 17 . 17 . 181
28322	5 . 13 . 13 . 13 . 13 . 41 . 137
29757	5 . 5 . 41 . 61 . 73 . 97
30103	5 . 13 . 17 . 41 . 73 . 137
31752	5 . 17 . 17 . 37 . 109 . 173
32406	17 . 17 . 17 . 37 . 53 . 109
32885	13 . 13 . 109 . 149 . 197
33307	5 . 5 . 5 . 5 . 17 . 53 . 197
34367	5 . 13 . 37 . 41 . 53 . 113
36673	5 . 17 . 29 . 37 . 73 . 101
37448	5 . 13 . 13 . 53 . 173 . 181
38326	29 . 37 . 41 . 173 . 193

38807	5 . 5 . 5 . 17 . 37 . 61 . 157	39082	5 . 5 . 41 . 73 . 137 . 149
39307	5 . 5 . 5 . 13 . 13 . 13 . 29 97	39818	5 . 5 . 5 . 5 . 17 . 37 . 37 . 109
40188	5 . 13 . 37 . 61 . 101 . 109	40515	17 . 53 . 61 . 109 . 137
40568	5 . 5 . 5 . 13 . 53 . 97 . 197	41187	5 . 17 . 37 . 37 . 37 . 197
41319	13 . 41 . 101 . 101 . 157	41688	5 . 17 . 41 . 53 . 97 . 97
42658	5 . 13 . 13 . 97 . 149 . 149	42932	5 . 5 . 5 . 29 . 29 . 89 . 197
43633	5 . 13 . 29 . 41 . 109 . 113	43932	5 . 5 . 5 . 5 . 13 . 17 . 89 . 157
44179	13 . 13 . 13 . 17 . 17 . 29 . 53	44507	5 . 5 . 13 . 113 . 149 . 181
44733	5 . 89 . 101 . 113 . 197	45050	13 . 41 . 109 . 181 . 193
45068	5 . 5 . 5 . 41 . 61 . 73 . 89	46444	13 . 41 . 149 . 157 . 173
46617	5 . 53 . 137 . 173 . 173	47403	5 . 13 . 29 . 37 . 89 . 181
47783	5 . 13 . 17 . 53 . 101 . 193	48187	5 . 97 . 101 . 137 . 173
48737	5 . 29 . 29 . 53 . 73 . 73	49083	5 . 13 . 17 . 73 . 109 . 137
50052	5 . 17 . 41 . 41 . 89 . 197	51115	17 . 17 . 17 . 29 . 53 . 173
51387	5 . 17 . 37 . 53 . 89 . 89	51412	5 . 17 . 61 . 61 . 61 . 137
51917	5 . 13 . 37 . 53 . 97 . 109	52571	37 . 41 . 61 . 109 . 137
54193	5 . 5 . 5 . 5 . 5 . 41 . 73 . 157	54358	5 . 13 . 29 . 73 . 109 . 197
54507	5 . 5 . 37 . 53 . 157 . 193	57532	5 . 5 . 17 . 41 . 41 . 41 . 113
66347	5 . 13 . 13 . 17 . 37 . 41 . 101	67333	5 . 17 . 53 . 61 73 . 113
67852	5 . 13 . 37 . 89 . 137 . 157	68463	5 . 13 . 17 . 113 . 137 . 137
71564	37 . 61 . 97 . 149 . 157	71700	13 . 29 . 37 . 41 . 89 . 101
72662	5 . 13 . 17 . 29 . 37 . 61 . 73	74043	5 . 5 . 13 . 37 . 37 . 61 . 101
75382	5 . 5 . 13 . 17 . 73 . 73 . 193	78629	13 . 17 . 41 . 41 . 53 . 157
80593	5 . 5 . 17 . 17 . 17 . 137 . 193	80802	5 . 37 . 41 . 53 . 109 . 149
81141	13 . 61 . 137 . 157 . 193	81749	13 . 17 . 17 . 53 . 97 . 173
83071	37 . 61 . 89 . 89 . 193	83247	5 . 13 . 13 . 13 . 29 . 73 . 149
84141	13 . 29 . 29 . 41 . 53 . 149	85353	5 . 13 . 17 . 37 . 41 . 41 . 53
86143	5 . 5 . 13 . 17 . 61 . 101 . 109	88668	5 . 5 . 13 . 17 . 73 . 101 . 193
88699	29 . 53 . 89 . 149 . 193	88733	5 . 13 . 41 . 97 . 97 . 157
88868	5 . 5 . 29 . 37 . 37 . 73 . 109	89361	29 . 37 . 137 . 157 . 173
89471	13 . 13 . 41 . 41 . 73 . 193	90212	5 . 13 . 37 . 89 . 193 . 197
90657	5 . 5 . 13 . 17 . 61 . 89 . 137	93020	13 . 13 . 17 . 17 . 29 . 41 . 149
93197	5 . 37 . 53 . 53 . 61 . 137	99557	5 . 5 . 5 . 5 . 41 . 41 . 53 . 89
99893	5 . 5 . 29 . 181 . 193 . 197	101343	5 . 5 . 13 . 29 . 41 . 97 . 137
102163	5 . 37 . 41 . 41 . 97 . 173	104818	5 . 5 . 5 . 5 . 17 . 29 181 . 197
106242	5 . 53 . 53 . 73 . 101 . 109	109637	5 . 13 . 17 . 29 . 37 . 37 . 137
112595	17 . 29 . 41 . 53 . 61 . 97	112782	5 . 5 . 17 . 37 . 41 . 109 . 181
114669	17 . 37 . 53 . 53 . 61 . 61	117251	41 . 97 . 101 . 109 . 157
117307	5 . 5 . 5 . 13 . 149 . 157 . 181	117372	5 . 13 . 17 . 17 . 53 . 101 . 137
128482	5 . 5 . 17 . 29 . 89 . 101 . 149	129553	5 . 13 . 13 . 17 . 61 . 61 . 157
133749	13 . 13 . 37 . 53 . 137 . 197	136293	5 . 5 . 17 . 41 . 53 . 89 . 113
136404	13 . 17 . 29 . 97 . 173 . 173	137717	5 . 13 . 53 . 89 . 157 . 197
137883	5 . 13 . 17 . 29 . 29 . 53 . 193	141743	5 . 5 . 89 . 149 . 157 . 193
143382	5 . 5 . 13 . 13 . 17 . 17 . 113 . 149	145046	13 . 29 . 37 . 101 . 109 . 137
145231	13 . 37 . 37 . 41 . 97 . 149	148158	5 . 53 . 61 . 61 . 113 . 197
148582	5 . 5 . 13 . 53 . 73 . 97 . 181	150522	5 . 13 . 17 . 29 . 37 . 97 . 197
155317	5 . 41 . 61 . 73 . 73 . 181	157308	5 . 13 . 29 . 29 . 41 . 61 . 181
157318	5 . 5 . 5 . 5 . 5 . 5 . 13 . 37 37 . 89	159772	5 . 37 . 53 . 101 . 149 . 173

160590	29 . 29 . 29 . 89 . 109 . 109
161832	5 . 5 . 13 . 13 . 29 . 37 . 53 . 109
162014	13 . 17 . 73 . 89 . 101 . 181
173932	5 . 5 . 5 . 5 . 5 . 13 . 73 . 101 . 101
174118	5 . 5 . 17 . 41 . 89 . 113 . 173
177144	17 . 29 . 73 . 89 97 . 101
180107	5 . 5 . 13 . 29 . 97 . 113 . 157
181343	5 . 5 . 17 . 37 . 53 . 109 . 181
181743	5 . 5 . 17 . 17 . 73 . 173 . 181

184133	5 . 29 . 73 . 101 . 101 . 157
189782	5 . 5 . 13 . 61 . 89 . 137 . 149
190393	5 . 5 . 13 . 13 . 137 . 173 . 181
191407	5 . 5 . 13 . 13 . 17 . 37 . 61 . 113
191807	5 . 5 . 5 . 13 . 17 . 41 . 109 . 149
194708	5 . 5 . 29 . 41 . 73 . 101 . 173
201106	17 . 17 . 61 . 89 . 149 . 173
208048	5 . 53 . 89 . 109 . 113 . 149
210195	61 . 113 . 137 . 149 . 157
210943	5 . 5 . 5 . 13 . 37 . 37 . 73 . 137
211765	13 . 17 . 53 . 89 . 137 . 157
216676	13 . 29 . 41 . 97 . 173 . 181
219602	5 . 17 . 17 . 53 . 53 . 109 . 109
221382	5 . 5 . 13 . 73 . 101 . 113 . 181
228068	5 . 5 . 5 . 17 . 29 . 61 . 101 . 137
232643	5 . 5 . 13 . 13 . 13 . 41 . 61 . 197
236151	17 . 17 . 41 . 89 . 137 . 193
247643	5 . 5 . 17 . 29 . 73 . 173 . 197
249501	13 . 53 . 53 . 61 . 89 . 157
251103	5 . 13 . 17 . 17 . 89 . 109 . 173
256638	5 . 13 . 29 . 37 . 61 . 113 . 137
260359	13 . 13 . 17 . 41 . 53 . 61 . 89
262433	5 . 17 . 29 . 29 . 53 . 61 . 149
263317	5 . 17 . 17 . 17 . 89 . 101 . 157
263557	5 . 5 . 5 . 13 . 37 . 41 . 73 . 193
265842	5 . 13 . 17 . 17 . 101 . 193 . 193
267657	5 . 5 . 41 . 41 . 61 . 89 . 157
281897	5 . 13 . 29 . 37 . 37 . 89 . 173
286018	5 . 5 . 13 . 13 . 53 . 53 . 61 . 113
287228	5 . 17 . 17 . 29 . 73 . 149 . 181
289038	5 . 17 . 17 . 37 . 89 . 97 . 181
292362	5 . 13 . 17 . 41 . 61 . 157 . 197
298307	5 . 5 . 5 . 5 . 41 . 53 . 181 . 181
307939	13 . 29 . 61 . 101 . 137 . 149
309070	13 . 29 . 101 . 113 . 149 . 149
320078	5 . 13 . 41 . 61 . 73 . 89 . 97
322392	5 . 13 . 17 . 41 . 89 . 149 . 173
330182	5 . 5 . 5 . 5 . 5 . 13 . 29 . 37 . 41 . 61
331068	5 . 5 . 5 . 5 . 53 . 101 . 181 . 181
383807	5 . 5 . 5 . 13 . 37 . 73 . 97 . 173
385692	5 . 13 . 17 . 61 . 89 . 137 . 181

389163	5 . 13 29 . 41 . 89 . 101 . 109
390112	5 . 13 . 17 . 17 . 17 . 17 . 17 . 17 . 97
403639	29 . 29 . 37 . 97 . 137 . 197
409557	5 . 5 . 5 . 5 . 13 . 13 . 73 . 73 . 149
411787	5 . 17 . 17 . 53 . 97 . 101 . 113
418048	5 . 97 . 97 . 109 . 173 . 197
444753	5 . 53 . 109 . 113 . 157 . 193
447342	5 . 17 . 29 . 41 . 97 . 137 . 149
464307	5 . 5 . 5 . 29 . 37 . 73 . 101 . 109
465525	13 . 13 . 29 . 89 . 97 . 113 . 197
465694	13 . 13 . 17 . 29 . 73 . 181 . 197
478707	5 . 5 . 13 . 13 . 13 . 17 . 41 . 41 . 73
485298	5 . 13 . 13 13 . 13 . 29 . 29 . 37 . 53
494607	5 . 5 . 29 . 89 . 101 . 137 . 137
500150	41 . 61 . 73 . 73 . 137 . 137
508929	13 . 13 . 37 . 53 . 53 . 73 . 101
518734	13 . 17 . 37 . 37 . 53 . 97 . 173
520463	5 . 13 . 41 . 61 . 73 . 101 . 113
534568	5 . 5 . 5 . 13 . 89 . 89 . 149 . 149
538275	17 . 61 . 73 . 97 . 109 . 181
548630	37 . 41 . 89 . 109 . 113 . 181
566793	5 . 5 . 17 . 29 . 29 . 41 . 97 . 113
567923	5 . 13 . 17 . 17 . 17 . 41 . 109 . 113
571459	13 . 13 . 13 . 13 . 17 . 37 . 61 . 149
586455	29 . 41 . 73 . 89 . 113 . 197
606325	13 . 37 . 97 . 137 . 149 . 193
607533	5 . 17 . 29 . 73 . 97 . 97 . 109
617427	5 . 13 . 13 . 17 . 29 . 53 . 89 . 97
623888	5 . 13 . 37 . 41 . 113 . 181 . 193
627391	41 . 41 . 53 . 113 . 113 . 173
662843	5 . 5 . 17 . 113 . 137 . 173 . 193
672717	5 . 89 . 97 . 157 . 173 . 193
683982	5 . 5 . 17 . 29 . 61 . 61 . 101 . 101
700107	5 . 5 . 13 . 17 . 41 . 53 . 137 . 149
703175	13 . 17 . 17 . 29 . 97 . 149 . 157
704683	5 . 13 . 29 . 61 . 97 . 113 . 197
721068	5 . 5 . 5 . 5 . 17 . 29 . 109 . 113 . 137
780262	5 . 17 . 17 . 29 . 37 . 41 . 61 . 157
783568	5 . 5 . 5 . 5 . 17 . 29 . 101 . 109 . 181
791532	5 . 5 . 53 . 89 . 149 . 181 . 197
793921	17 . 17 . 17 . 29 . 73 . 157 . 193
812447	5 . 29 . 29 . 41 . 89 . 137 . 157
832902	5 . 13 . 13 . 13 . 17 . 109 . 173 . 197
848871	29 . 53 . 73 . 113 . 157 . 181
899168	5 . 5 . 17 . 37 . 53 . 73 . 97 . 137
907567	5 . 29 . 37 . 41 . 89 . 109 . 193
911111	17 . 41 . 101 . 173 . 173 . 197
936513	5 . 37 . 37 . 41 89 . 97 . 181

1000193	5 . 5 . 5 . 29 . 53 . 101 . 149 . 173
1010027	5 . 13 . 61 . 89 . 89 . 109 . 149
1024240	37 . 61 . 109 . 157 . 157 . 173
1031675	13 . 13 . 17 . 53 . 73 . 113 . 157 . 197
1049433	5 . 13 . 61 . 89 . 89 . 89 . 197
1059193	5 . 5 . 5 . 5 . 13 . 13 . 13 . 37 . 61 . 181
1067157	5 . 5 . 41 . 113 . 157 . 173 . 181
1068182	5 . 5 . 5 . 17 . 17 . 41 . 61 . 73 . 173
1083493	5 . 5 . 13 . 61 . 61 . 61 . 73 . 109
1089593	5 . 5 . 61 . 89 . 149 . 149 . 197
1131527	5 . 41 . 53 . 53 . 73 . 97 . 157
1139557	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 37 . 73 . 181
1143007	5 . 5 . 13 . 41 . 61 . 73 . 101 . 109
1197943	5 . 5 . 5 . 5 . 5 . 17 . 17 . 37 . 109 . 197
1264557	5 . 5 . 5 . 5 . 5 . 13 . 13 . 29 . 53 . 197
1306143	5 . 5 . 29 . 37 . 37 . 61 . 73 . 193
1351742	5 . 17 . 53 . 109 . 137 . 157 . 173
1373307	5 . 5 . 5 . 5 . 17 . 29 . 101 . 157 . 193
1387203	5 . 29 . 41 . 41 . 113 . 181 . 193
1402232	5 . 5 . 17 . 37 . 41 . 113 . 137 . 197
1413443	5 . 5 . 13 . 29 . 37 . 41 . 89 . 157
1477034	37 . 37 . 41 . 53 . 53 . 101 . 137
1518057	5 . 5 . 5 . 13 . 13 . 41 . 61 . 113 . 193
1528649	13 . 37 . 53 . 61 . 61 . 109 . 113
1615463	5 . 13 . 17 . 37 . 53 . 73 . 73 . 113
1618855	17 . 29 . 37 . 53 . 89 . 97 . 157
1635786	29 . 29 . 41 . 89 . 89 . 97 . 101
1664957	5 . 5 . 13 . 37 . 73 . 89 . 113 . 157
1750507	5 . 5 . 13 . 53 . 53 . 89 . 109 . 173
1766693	5 . 5 . 5 . 5 . 5 . 5 . 29 . 97 . 157 . 173
1824257	5 . 5 . 17 . 29 . 97 . 109 . 113 . 113
1909461	13 . 13 . 17 . 17 . 41 . 53 . 89 . 193
1954207	5 . 5 . 13 . 61 . 61 . 89 . 113 . 157
1984933	5 . 17 . 37 . 37 . 37 . 53 . 89 . 97
2036069	17 . 41 . 41 . 61 . 61 . 101 . 193
2050706	13 . 17 . 17 . 17 . 41 . 53 . 157 . 193
2052057	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 29 . 73 . 97 . 193
2126007	5 . 5 . 17 . 29 . 29 . 181 . 181 . 193
2277387	5 . 13 . 29 . 29 . 53 . 89 . 89 . 113
2298668	5 . 5 . 13 . 13 . 17 . 17 . 29 . 37 . 37 . 109
2343692	5 . 17 . 41 . 41 . 61 . 73 . 89 . 97
2353918	5 . 5 . 13 . 17 . 29 . 29 . 61 . 113 . 173
2379723	5 . 13 . 29 . 37 . 53 . 53 . 97 . 149
2457057	5 . 5 . 5 . 5 . 13 . 17 . 41 . 53 . 89 . 113
2471717	5 . 37 . 41 . 109 . 137 . 149 . 181
2475918	5 . 5 . 17 . 53 . 61 . 157 . 157 . 181
2478328	5 . 13 . 29 . 37 . 89 . 97 . 101 . 101
2484968	5 . 5 . 13 . 61 . 97 . 113 . 157 . 181

2680168	5 . 5 . 29 . 61 . 73 . 109 . 137 . 149
2733307	5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 13 . 17 . 37 . 173
2809305	13 . 17 . 29 . 37 . 37 . 61 . 73 . 101
2923783	5 . 13 . 17 . 37 . 41 . 109 . 149 . 157
2959007	5 . 5 . 17 . 37 . 97 . 101 . 157 . 181
3014557	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 41 . 53 . 53 . 101
3025001	13 . 13 . 17 . 17 . 61 . 73 . 109 . 193
3136570	13 . 13 . 29 . 37 . 53 . 61 . 97 . 173
3139557	5 . 5 . 5 . 5 . 5 . 5 . 13 . 29 . 73 . 73 . 157
3272693	5 . 5 . 5 . 13 . 37 . 41 . 101 . 137 . 157
3370437	5 . 13 . 13 . 13 . 13 . 41 . 73 . 97 . 137
3449051	13 . 13 . 13 . 53 . 61 . 89 . 97 . 97
3637197	5 . 13 . 17 . 29 . 61 . 89 . 193 . 197
3800438	5 . 13 . 29 . 29 . 97 . 101 . 149 . 181
3801448	5 . 29 . 37 . 53 . 61 . 73 . 101 . 113
3815076	13 . 13 . 17 . 37 . 53 . 109 . 137 . 173
3894873	5 . 13 . 13 . 37 . 89 . 101 . 137 . 197
3911450	29 . 29 . 41 . 97 . 137 . 173 . 193
3931663	5 . 13 . 29 . 37 . 41 . 109 . 137 . 181
4000300	13 . 13 . 13 . 17 . 17 . 73 . 137 . 181 . 181
4079486	13 . 17 . 17 . 53 . 61 . 73 . 137 . 137
4218932	5 . 5 . 5 . 5 . 29 . 41 . 41 . 61 . 61 . 157
4466678	5 . 13 . 17 . 73 . 97 . 109 . 149 . 157
4650839	17 . 17 . 89 . 113 . 137 . 157 . 173
4697282	5 . 5 . 13 . 113 . 113 . 137 . 197 . 197
4751232	5 . 5 . 13 . 17 . 29 . 73 . 97 . 101 . 197
4773557	5 . 5 . 5 . 29 . 29 . 41 . 113 . 149 . 157
5033696	13 . 17 . 37 . 37 . 89 . 89 . 97 . 109

5982670	13 . 13 . 13 . 17 . 41 . 53 . 53 . 53 . 157
6151956	13 . 17 . 29 . 29 . 73 . 97 . 113 . 149
6208047	5 . 17 . 17 . 17 . 17 . 29 . 41 . 41 . 197 . 197
6225244	29 . 37 . 41 . 53 . 53 . 53 . 61 . 97
6315768	5 . 5 . 17 . 17 . 53 . 61 . 73 . 149 . 157
6356150.	13 . 29 . 37 . 37 . 61 . 61 . 109 . 193
6367252	5 . 13 . 17 . 29 . 29 . 61 . 73 . 97 . 101
6656382	5 . 5 . 13 . 29 . 41 . 41 . 137 . 137 . 149
6817837	5 . 17 . 17 . 53 . 61 . 149 . 173 . 193
6829610	13 . 17 . 17 . 53 . 61 . 101 . 193 . 197
6981694	13 . 41 . 97 . 137 . 181 . 193 . 197
7138478	5 . 29 . 37 . 41 . 73 . 89 . 181 . 197
7620661	5 . 17 . 37 . 73 . 101 . 101 . 137 . 181
7691443	5 . 5 . 5 . 37 . 53 . 97 . 101 . 109 . 113
8082212	5 . 13 . 17 . 17 . 37 . 53 . 97 . 101 . 181
8571779	13 . 13 . 29 . 41 . 73 . 101 . 137 . 181
8809432	5 . 5 . 5 . 13 . 89 . 101 . 149 . 181 . 197
9407318	5 . 5 . 5 . 5 . 5 . 5 . 37 . 41 . 53 . 73 . 193

9548768	5 . 5 . 13 . 13 . 17 . 41 . 53 . 61 . 61 . 157
9614382	5 . 5 . 29 . 37 . 53 . 61 . 61 . 101 . 173
9639557	5 . 5 . 5 . 5 . 5 . 5 . 13 . 17 . 17 . 53 . 109 . 137
9689961	13 . 29 . 29 . 37 . 61 . 113 . 113 . 149
10328193	5 . 5 . 5 . 13 . 17 . 29 . 53 . 53 . 137 . 173
10669731	17 . 89 . 97 . 101 . 101 . 193 . 197
11131086	13 . 13 . 17 . 17 . 37 . 61 . 73 . 89 . 173
12477035	17 . 17 . 17 . 29 . 29 . 29 . 37 . 97 . 181
12514913	5 . 13 . 41 . 53 . 137 . 149 . 157 . 173
12750353	5 . 13 . 17 . 17 . 41 . 61 . 73 . 137 . 173
14698000	13 . 13 . 17 . 17 . 29 . 61 . 97 . 149 . 173
15165443	5 . 5 . 5 . 5 . 37 . 53 . 61 . 97 . 101 . 157
15986082	5 . 5 . 13 . 17 . 109 . 109 . 137 . 157 . 181
16317267	5 . 13 . 17 . 17 . 61 . 61 . 101 . 109 . 173
18378313	5 . 13 . 13 . 17 . 37 . 61 . 137 . 193 . 197
18975991	13 . 17 . 17 . 17 . 53 . 61 . 89 . 97 . 101
20198495	13 . 17 . 41 . 89 . 101 . 101 . 137 . 181
22866693	5 . 5 . 5 . 5 . 41 . 61 . 73 . 101 . 113 . 197
23747457	5 . 5 . 17 . 17 . 17 . 17 . 17 . 17 . 37 . 73 . 173
24208144	29 . 29 . 29 . 37 . 37 . 53 . 61 . 61 . 89
24280807	5 . 5 . 5 . 5 . 13 . 13 . 17 . 53 . 109 . 157 . 181
24310918	5 . 5 . 13 . 13 . 37 . 41 . 53 . 89 . 113 . 173
31011557	5 . 5 . 5 . 13 . 17 . 61 . 97 . 109 . 137 . 197
32944452	5 . 13 . 13 . 29 . 29 . 41 . 53 . 53 . 89 . 149
34436768	5 . 5 . 17 . 61 . 97 . 101 . 137 . 173 . 197
34602875	13 . 17 . 17 . 29 . 37 . 53 . 113 . 137 . 181
45500682	5 . 5 . 5 . 37 . 53 . 53 . 61 . 89 . 149 . 197
53365057	5 . 5 . 5 . 13 . 37 . 89 . 97 . 101 . 157 . 173
58305593	5 . 5 . 13 . 17 . 37 . 37 . 101 . 109 . 137 . 149
75505943	5 . 5 . 5 . 37 . 37 . 53 . 89 . 137 . 149 . 173
95665578	5 . 13 . 37 . 41 . 73 . 181 . 181 . 197 . 197
111530944	13 . 13 . 13 . 13 . 13 . 17 . 37 . 37 . 53 . 157 . 173
121042733	5 . 17 . 41 . 73 . 97 . 97 . 101 . 157 . 193
160007778	5 . 13 . 13 . 17 . 17 . 29 . 29 . 73 . 73 . 149 . 157
167207057	5 . 5 . 5 . 5 . 17 . 17 . 17 . 29 . 73 . 109 . 109 . 181
168623905	13 . 13 13 . 13 . 17 . 29 . 29 . 37 . 89 . 97 . 109
185507821	13 . 13 . 17 . 29 . 29 . 53 . 61 . 101 . 113 . 193
193788912	5 . 13 . 17 . 17 . 37 . 37 . 37 . 53 . 73 . 101 . 101
201229582	5 . 5 . 13 . 13 . 17 . 17 . 17 . 17 . 17 . 53 . 97 . 101
211823957	5 . 5 . 17 . 17 . 53 . 101 . 137 . 149 . 157 . 181
284862638	5 . 13 . 17 . 17 . 17 . 17 . 29 . 29 . 41 . 41 . 97 . 109
299252491	13 . 29 . 37 . 97 . 109 . 109 . 113 . 157
317742693	5 . 5 . 5 . 13 . 29 . 41 . 73 . 89 . 137 . 149 . 197
327012132	5 . 5 . 13 . 17 . 17 . 29 . 89 . 109 . 149 . 157 . 173
599832943	5 . 5 . 5 . 5 . 13 . 17 . 29 . 37 . 37 . 41 . 73 97 . 113
830426722	5 . 13 . 13 . 61 . 97 . 149 . 157 . 173 . 173 . 197
1112115023	5 . 17 . 17 . 61 . 73 . 113 . 157 . 173 . 173 . 181
1282794079	13 . 17 . 29 . 29 . 73 . 89 . 97 . 113 . 181 . 197 . 197

2189376182	5 . 5 . 5 . 17 . 17 . 29 . 29 . 53 . 61 . 61 . 89 . 89 . 101
2971354082	5 . 5 . 13 . 17 . 29 . 41 . 53 . 53 . 113 . 149 . 157 . 181
3955080927	5 . 13 . 17 . 17 . 17 . 17 . 53 . 53 . 61 . 61 . 101 . 149 . 173 . 197
8193535810	13 . 13 . 29 . 29 . 61 . 109 . 109 . 137 . 157 . 157 . 193
14033378718	5 . 5 . 13 . 13 . 17 . 17 . 61 . 61 . 61 . 61 . 73 . 73 . 157 . 181

5	2. 3. 7
13	5. 8. 18. 57. 239
17	4. 13. 21. 38. 47. 268
29	12. 17. 41. 70. 99. 157. 307
37	6. 31. 43. 68. 117. 191. 302. 327. 882. 18543*
41	9. 32. 73. 132. 278. 378. 829. 993. 2943
53	23. 30. 83. 182. 242. 401. 447. 606. 931. 1143*. 1772. 6118. 34208. 44179. 85353. 485298
61	11. 50. 72. 133. 255. 438. 682. 2673. 2917. 4747*. 4952. 5257. 9466. 12943. 17557. 114669. 330182
73	27. 46. 173. 265. 319. 538. 557. 684. 1068. 1560*. 2163. 2309. 2436. 3039. 5667. 8368. 14773. 48737. 72662. 478707*
89	34. 55. 123. 233. 411. 500. 568. 746. 1568. 1636*. 3793. 4217. 4594. 4662. 6107. 11981. 19703. 24263. 32807. 37770*. 45068. 51387. 99557. 157318. 260359. 24208144
97	22. 75. 119. 172. 216. 463. 507. 560. 657. 1433*. 1918. 2059. 2738. 4193. 4246. 5357. 5507. 5648. 6962. 9193*. 9872. 17923. 21124. 29757. 30383. 39307. 41688. 112595. 320078. 390112*. 617427. 1984933. 2343692. 3449051. 6225244
101	10. 91. 111. 192. 212. 293. 313. 394. 515. 616*. 697. 798. 818. 1303. 2818. 3141. 3323. 8393. 17766. 36673*. 66347. 71700. 74043. 173932. 177144. 508929. 683982. 1635786. 2478328. 2809305*. 3014557. 6367252. 18975991. 193788912. 201229582. 2189376182
109	33. 76. 142. 251. 294. 360. 512. 621. 905. 948*. 1057. 1123. 1929. 2801. 3521. 3957. 5701. 6943. 8578. 9298*. 15075. 32406. 39818. 40188. 51917. 86143. 88868. 106242. 160590. 161832*. 219602. 389163. 464307. 607533. 1083493. 1143007. 2298668. 5033696. 168623905. 284862638*
113	15. 98. 128. 437. 693. 776. 919. 1032. 1341. 1567*. 1597. 3149. 3405. 4535. 6682. 6908. 7443. 7782. 9703. 12332*. 13545. 14140. 17191. 19534. 21907. 34367. 43633. 57532. 67333. 136293*. 191407. 286018. 411787. 520463. 566793. 567923. 1528649. 1615463. 1824257. 2277387*. 2457057. 3801448. 7691443. 599832943
137	37. 100. 174. 237. 922. 1407. 1607. 1955. 2018. 4484*. 5928. 7161. 9901. 10312. 11471. 13252. 19902. 22231. 28322. 30103*. 40517. 49083. 51412. 52571. 68463. 90657. 93197. 101343. 109637. 117372*. 145046. 210943. 228068. 256638. 494607. 500150. 721068. 899168. 1477034. 3370434*. 4079486. 9639557

149	44. 105. 193. 403. 701. 1087. 1148. 1744. 1832. 1893*. 5767. 6065. 6898. 9133. 10833. 14646. 18432. 19326. 20457. 22157*. 24331. 25523. 28205. 28862. 32973. 37057. 39082. 42658. 80802. 83247*. 84141. 93020. 128482. 143382. 145231. 189782. 191807. 208048. 262433. 307939*. 309070. 409557. 447342. 534568. 571459. 700107. 1010027. 2379723. 2680168. 6151956*. 6656382. 9689961. 32944452. 58305593
157	28. 129. 185. 342. 443. 499. 757. 1228. 1385. 2013*. 2540. 2697. 3112. 3583. 3740. 4581. 5052. 6252. 7093. 14573*. 16513. 19653. 22008. 25462. 38807. 41319. 43932. 54193. 67852. 71564*. 78629. 88733. 117251. 129553. 180107. 184133. 210195. 211765. 249503. 263317*. 267657. 703175. 780262. 812447. 1131527. 1413443. 1618855. 1664957. 1954207. 2923783*. 3139557. 3272693. 4218932. 4466678. 4773557. 5982670. 6315768. 9548768. 15165443. 160007778*. 299252491
173	80. 93. 253. 599. 772. 785. 945. 1118. 1477. 1823*. 3207. 4232. 5283. 5443. 5962. 8224. 12882. 13068. 13241. 18258*. 19283. 21705. 31752. 32258. 46444. 46617. 48187. 51115. 81749. 89361*. 102163. 136404. 159772. 174118. 194718. 201106. 251103. 281897. 322392. 383807*. 518734. 627391. 1000193. 1024240. 1068182. 1351742. 1750507. 1766693. 2353918. 2733307*. 3136570. 3815076. 4650839. 9614382. 10328193. 11131086. 12514913. 12750353. 14698000. 16317267*. 23747457. 24310918. 53365057. 75505943. 111530944. 327012132
181	19. 162. 200. 343. 524. 743. 924. 1067. 1467. 2010*. 2191. 2515. 3458. 3782. 5087. 8307. 9431. 10298. 13918. 14318*. 24778. 25683. 27493. 35857. 37448. 44507. 47403. 112782. 117307. 148582*. 155317. 157308. 162014. 181343. 181743. 190393. 216676. 221382. 287228. 289038*. 298307. 331068. 385692. 538275. 548630. 783568. 848871. 936513. 1059193. 1067157*. 1139557. 2471717. 2475918. 2484968. 2959007. 3800438. 3931663. 4000300. 7620662. 8082212*. 8571779. 12477035. 15986092. 20198495. 24280807. 34602875. 167207057. 211823957. 1112115023. 2971354082*. 14033378718
193	81. 112. 467. 660. 853. 1239. 1270. 1432. 1818. 2042*. 2428. 2621. 3362. 4327. 4906. 4937. 6481. 9152. 9762. 12433*. 13043. 14942. 24816. 25943. 30027. 28326. 45050. 47783. 54507. 75382*. 80593. 81141. 83071. 88668. 88699. 89471. 137883. 141743. 236151. 263557*. 265842. 444753. 606385. 623888. 662843. 672717. 793921. 907567. 1306143. 1373307*. 1387203. 1518057. 1909461. 2036069. 2050706. 2052057. 2126007. 3025001. 3911450. 6356150*. 6817837. 9407318. 121042733. 185507821. 8193535810
197	14. 183. 211. 408. 577. 999. 1196. 1393. 1984. 2153*. 2350. 2547. 3166. 3532. 4545. 7697. 8457. 9667. 11018. 14958*. 16928. 19123. 19911. 20080. 25793. 26018. 32885. 33307. 40568. 41187*. 42932. 44733. 50052. 54358. 90212. 99893. 104818. 133749. 137719. 148158*. 150522. 232643. 247643. 292362. 403639. 418048. 465525. 465694. 586455. 704683*. 791532. 832902. 911111. 1031675. 1049433. 1089593. 1197943. 1264557. 1402232. 3637197*. 3894873. 4697282. 4751232. 6208047. 6829610. 6981694. 7138478. 8809432. 10669731. 18378313*. 22866693. 31011557. 34436768. 45500682. 95665578. 317742693. 830426722. 1282794079. 3955080927

Zerlegbare $aa + 4$.

1	5	3	13
5	29	7	53
9	5 . 17	11	5 . 5 . 5
13	173	19	5 . 73
21	5 . 89	23	13 . 41
25	17 . 37	29	5 . 13 . 13
31	5 . 193	39	5 . 5 . 61
43	17 . 109	49	5 . 13 . 37
53	29 . 97	59	5 . 17 . 41
61	5 . 5 . 149	63	29 . 137
81	5 . 13 . 101	83	61 . 113
99	5 . 37 . 53	101	5 . 13 . 157
111	5 . 5 . 17 . 29	121	5 . 29 . 101
127	13 . 17 . 73	141	5 . 41 . 97
143	113 . 181	161	5 . 5 . 17 . 61
169	5 . 29 . 197	179	5 . 13 . 17 . 29
199	5 . 89 . 89	205	13 . 53 . 61
211	5 . 5 . 13 . 137	213	17 . 17 . 157
219	5 . 53 . 181	237	13 . 29 . 149
247	17 . 37 . 97	261	5 . 5 . 5 . 5 . 109
283	13 . 61 . 101	309	5 . 13 . 13 . 113
311	5 . 5 . 53 . 73	335	13 . 89 . 97
359	5 . 149 . 173	393	13 . 109 . 109
417	17 . 53 . 193	419	5 . 13 . 37 . 73
469	5 . 29 . 37 . 41	485	17 . 101 . 137
527	29 . 61 . 157	535	17 . 113 . 149
611	5 . 5 . 109 . 137	679	5 . 13 . 41 . 173
691	5 . 29 . 37 . 89	705	13 . 13 . 17 . 173
749	5 . 29 . 53 . 73	759	5 . 29 . 29 . 137
761	5 . 5 . 5 . 41 . 113	829	5 . 13 . 97 . 109
841	5 . 17 . 53 . 157	943	17 . 17 . 17 . 181
961	5 . 5 . 17 . 41 . 53	1011	5 . 5 . 5 . 13 . 17 . 37
1043	13 . 13 . 41 . 157	1047	89 . 109 . 113
1089	5 . 5 . 13 . 41 . 89	1131	5 . 17 . 101 . 149
1159	5 . 37 . 53 . 137	1305	97 . 97 . 181
1351	5 . 17 . 109 . 197	1371	5 . 41 . 53 . 173
1381	5 . 13 . 13 . 37 . 61	1499	5 . 41 . 97 . 113
1581	5 . 41 . 89 . 137	1745	13 . 29 . 41 . 197
1801	5 . 37 . 89 . 197	1899	5 . 37 . 101 . 193
2025	13 . 29 . 73 . 149	2343	13 . 37 . 101 . 113
2355	17 . 41 . 73 . 109	2441	5 . 13 . 29 . 29 . 109

2677	17 . 17 . 137 . 181
3039	5 . 5 . 13 . 157 . 181

3339	5 . 5 . 41 . 73 . 149
3351	5 . 13 . 13 . 97 . 137
3377	13 . 61 . 73 . 197
3717	29 . 53 . 89 . 101
3749	5 . 17 . 37 . 41 . 109
4021	5 . 17 . 37 . 53 . 97
4123	17 . 29 . 29 . 29 . 41
4215	13 . 73 . 97 . 113
4761	5 . 5 . 5 . 13 . 13 . 29 . 37
4989	5 . 5 . 5 . 13 . 17 . 17 . 53
5041	5 . 13 . 13 . 17 . 29 . 61
5567	13 . 17 . 17 . 73 . 113
5573	29 . 61 . 97 . 181
5717	13 . 13 . 41 . 53 . 89
5821	5 . 13 . 37 . 73 . 193
6061	5 . 5 . 13 . 17 . 61 . 109
6261	5 . 5 . 5 . 53 . 61 . 97
6989	5 . 5 . 5 . 53 . 73 . 101
7319	5 . 17 . 73 . 89 . 97
7745	13 . 13 . 37 . 53 . 181
8049	5 . 17 . 53 . 73 . 197
8579	5 . 29 . 53 . 61 . 157
8879	5 . 29 . 41 . 89 . 149
9801	5 . 17 . 73 . 113 . 137
9817	17 . 37 . 37 . 41 . 101
9947	73 . 89 . 97 . 157
10039	5 . 5 . 13 . 17 . 17 . 29 . 37
12383	37 . 109 . 193 . 197
12605	17 . 37 . 41 . 61 . 101
12815	13 . 13 . 41 . 137 . 173
13251	5 . 17 . 101 . 113 . 181
13489	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 137
13507	17 . 17 . 41 . 89 . 173
14261	5 . 5 . 5 . 89 . 101 . 181
14901	5 . 13 . 13 . 13 . 17 . 29 . 41
16041	5 . 73 . 89 . 89 . 89
20511	5 . 5 . 5 . 13 . 17 . 97 . 157
20769	5 . 29 . 37 . 37 . 41 . 53
20875	13 . 29 . 53 . 113 . 193
21139	5 . 5 . 17 . 37 . 157 . 181
21161	5 . 5 . 13 . 89 . 113 . 137
21189	5 . 5 . 37 . 61 . 73 . 109
22805	13 . 17 . 89 . 137 . 193
23311	5 . 5 . 29 . 41 . 101 . 181
23901	5 . 29 . 137 . 149 . 193
23915	13 . 29 . 73 . 113 . 173
25689	5 . 5 . 29 . 41 . 149 . 149
27355	13 . 37 . 53 . 149 . 197

27411	5 . 5 . 41 . 61 . 61 . 197
27429	5 . 17 . 29 . 37 . 73 . 113
27611	5 . 5 . 41 . 61 . 89 . 137
29169	5 . 13 . 29 . 41 . 101 . 109
29691	5 . 17 . 17 . 29 . 109 . 193
29929	5 . 13 . 17 . 61 . 97 . 137
31351	5 . 37 . 149 . 181 . 197
32003	13 . 17 . 17 . 41 . 61 . 109
32139	5 . 5 . 13 . 17 . 73 . 197
32239	5 . 5 . 5 . 5 . 5 . 37 . 89 . 101
37579	5 . 17 . 29 . 41 . 89 . 157
44301	5 . 13 . 37 . 53 . 89 . 173.
47389	5 . 5 . 53 . 97 . 101 . 173
47761	5 . 5 . 5 . 5 . 17 . 17 . 73 . 173
47829	5 . 17 . 37 . 41 . 113 . 157
49813	13 . 53 . 101 . 181 . 197
57989	5 . 5 . 5 . 53 . 53 . 61 . 157
63911	5 . 5 . 13 . 13 . 17 . 29 . 37 . 53
66361	5 . 5 . 41 . 113 . 193 . 197
79011	5 . 5 . 5 . 5 . 13 . 89 . 89 . 97
79871	5 . 29 . 37 . 61 . 101 . 193
81487	13 . 13 . 73 . 73 . 73 . 101
81669	5 . 13 . 29 . 113 . 173 . 181
86487	17 . 17 . 41 . 41 . 89 . 173
91587	17 . 29 . 29 . 37 . 101 . 157
95963	13 . 13 . 41 . 89 . 109 . 137
99011	5 . 5 . 5 . 5 . 5 . 13 . 29 . 53 . 157
99407	17 . 29 . 37 . 41 . 73 . 181
108111	5 . 5 . 13 . 17 . 97 . 113 . 193
110211	5 . 5 . 13 . 37 . 73 . 101 . 137
114611	5 . 5 . 13 . 13 . 89 . 181 . 193
115983	13 . 17 . 37 . 61 . 149 . 181
117281	5 . 29 . 61 . 89 . 101 . 173
128359	5 . 13 . 17 . 29 . 53 . 89 . 109
139701	5 . 13 . 53 . 149 . 193 . 197
140489	5 . 5 . 5 . 41 . 113 . 173 . 197
140871	5 . 13 . 17 . 37 . 61 . 73 . 109
142047	29 . 29 . 41 . 53 . 61 . 181
148939	5 . 5 . 29 . 29 . 73 . 97 . 149
183739	5 . 5 . 5 . 13 . 29 41 . 101 . 173
191279	5 . 13 . 13 . 29 . 73 . 113 . 181
203091	5 . 17 . 17 . 41 . 61 . 101 . 113
205111	5 . 5 . 13 . 73 . 97 . 101 . 181
206707	29 . 37 . 53 . 61 . 109 . 113
207171	5 . 13 . 17 . 29 . 89 . 101 . 149
211221	5 . 13 . 13 . 37 . 61 . 149 . 157
228179	5 . 13 . 13 . 61 . 73 . 101 . 137
234333	37 . 37 . 37 . 41 . 137 . 193

234881	5 . 13 . 13 . 17 . 17 . 17 . 97 . 137
241511	5 . 5 . 5 . 5 . 13 . 17 . 37 . 101 . 113
244299	5 . 13 . 17 . 37 . 97 . 101 . 149
245293	109 . 113 . 137 . 181 . 197
247699	5 . 13 . 17 . 41 . 61 . 149 . 149
257665	13 . 17 . 101 . 109 . 157 . 173
263489	5 . 5 . 5 . 5 . 5 . 5 . 29 . 37 . 41 . 101
269459	5 . 17 . 37 . 37 . 53 . 61 . 193
289589	5 . 5 . 29 . 61 . 97 . 113 . 173
302111	5 . 5 . 41 . 61 . 97 . 101 . 149
306757	17 . 29 . 53 . 101 . 181 . 197
313489	5 . 5 . 5 . 5 . 5 . 17 . 17 . 17 . 37 . 173
317039	5 . 5 . 53 . 61 . 89 . 89 . 157
326957	37 . 37 . 41 . 101 . 109 . 173
349835	17 . 41 . 73 . 97 . 137 . 181
355989	5 . 5 . 5 . 5 . 13 . 17 . 37 . 137 . 181
387921	5 . 61 . 101 . 137 . 181 . 197
396783	13 . 13 . 29 . 61 . 61 . 89 . 97
408489	5 . 5 . 5 . 5 . 13 . 29 . 73 . 89 . 109
466489	5 . 5 . 5 . 13 . 17 . 29 . 61 . 61 . 73
563235	13 . 17 . 41 . 61 . 61 . 97 . 97
567629	5 . 13 . 37 . 73 . 109 . 113 . 149
582997	37 . 41 . 73 . 113 . 157 . 173
588489	5 . 5 . 5 . 5 5 . 61 . 89 . 137 . 149
628261	5 . 5 . 5 . 13 . 17 . 29 . 41 . 61 . 197
634205	37 . 53 . 73 . 109 . 149 . 173
637855	13 . 37 . 41 . 41 . 61 . 73 . 113
834267	17 . 17 . 17 . 29 . 137 . 181 . 197
840421	5 . 13 . 17 . 137 . 149 . 173 . 181
851929	5 . 17 . 53 . 73 . 89 . 137 . 181
922769	5 . 13 . 13 . 17 . 41 . 61 . 137 . 173
966391	5 . 13 . 17 . 29 29 . 37 . 157 . 173
1029353	61 . 61 . 89 . 109 . 149 . 197
1165689	5 . 5 . 29 . 41 . 41 . 53 . 109 . 193
1230349	5 . 13 . 13 . 17 . 17 . 29 . 37 . 53 . 109
1299241	5 . 13 . 13 . 37 . 89 . 89 . 173 . 197
1341429	5 . 29 . 61 . 73 . 89 . 173 . 181
1362611	5 . 5 . 13 37 . 89 . 89 . 101 . 193
1493911	5 . 5 . 13 . 29 . 101 . 109 . 137 . 157
1499001	5 . 13 . 13 . 17 . 73 . 73 . 149 . 197
1780489	5 . 5 . 5 . 29 . 37 . 41 . 53 . 73 . 149
1996199	5 . 13 . 13 . 17 . 17 . 37 . 53 53 . 157
2028211	5 . 5 . 13 . 17 . 41 . 41 . 53 . 61 . 137
2050005	17 . 29 . 61 . 73 . 89 . 137 . 157
2159739	5 . 5 . 5 . 5 . 13 . 17 . 37 . 41 . 113 . 197
3376311	5 . 5 . 13 . 13 . 13 . 17 . 17 . 61 . 61 . 193
3666653	13 . 13 . 17 . 41 . 53 . 97 . 149 . 149
3872099	5 . 13 . 13 . 17 . 37 . 41 . 41 . 97 . 173

4370811	5 . 5 . 13 . 17 . 53 . 61 . 89 . 197
4490249	5 . 13 . 29 . 61 . 73 . 89 . 137 . 197
4705711	5 . 5 . 13 . 17 . 17 . 17 . 17 . 41 . 101 . 197
5125339	5 . 5 . 17 . 17 . 29 . 37 . 97 . 181 . 193
5472411	5 . 5 . 17 . 29 . 41 . 41 . 89 . 109 . 149
6101547	13 . 13 . 13 . 17 . 29 . 37 . 61 . 97 . 157
6489011	5 . 5 . 5 . 5 . 17 . 37 . 41 . 89 . 149 . 197
8175989	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 97 . 149 . 181
8649761	5 . 5 . 5 . 13 . 17 . 37 . 61 . 101 . 109 . 109
8812979	5 . 17 . 17 . 17 . 29 . 73 . 89 . 97 . 173
9530277	13 . 13 . 17 . 17 . 17 . 73 . 89 . 113 . 149
10126399	5 . 13 . 17 . 29 . 29 . 53 . 89 . 149 . 157
10251621	5 . 13 . 17 . 17 29 . 61 . 101 . 173 . 181
10763489	5 . 5 . 5 . 5 . 5 . 5 . 61 . 61 . 101 . 109 . 181
10831321	5 . 17 . 29 . 29 . 41 . 61 . 73 . 89 . 101
11398611	5 . 5 . 13 . 17 . 53 . 97 . 137 . 173 . 193
11483821	5 . 29 . 53 . 61 . 101 . 113 . 157 . 157
15035789	5 . 5 . 37 . 41 . 41 . 53 . 101 . 157 . 173
17363031	5 . 13 . 13 . 41 . 73 . 89 . 89 . 101 . 149

23866411	5 . 5 . 13 . 17 . 17 . 17 . 61 . 157 . 193 . 193
25252451	5 . 13 . 29 . 37 . 41 . 97 . 97 . 137 . 173
31456571	5 . 13 . 17 . 41 . 97 . 101 . 109 . 113 . 181
34411159	5 . 13 . 37 . 41 . 61 . 73 . 89 . 157 . 193
35272357	13 . 13 . 13 . 13 . 17 . 29 . 61 . 97 . 101 . 137
35944451	5 . 13 . 17 . 17 . 17 . 29 . 73 . 89 109 . 197
61017271	13 . 13 . 13 . 17 . 29 . 37 . 61 . 97 . 157
107402539	5 . 5 . 13 . 29 . 37 . 61 . 109 . 149 . 173 . 193
143828743	29 . 29 . 37 . 37 . 53 . 97 . 113 . 157 . 197
148757489	5 . 5 . 5 . 13 . 13 . 17 . 37 . 41 . 41 . 61 . 109 . 149
150446761	5 . 5 . 5 . 13 . 17 . 37 . 53 . 113 . 137 . 137 . 197
322564791	5 . 13 . 17 . 29 . 29 . 29 . 37 . 53 . 101 . 101 . 193
657182319	5 . 17 . 17 . 61 . 97 . 97 . 113 . 149 . 157 . 197
1359685525	13 . 17 . 53 . 61 . 61 . 97 . 113 . 157 . 157 . 157
4949475989	5 . 5 . 5 . 5 . 5 . 13 . 13 . 29 . 29 . 37 . 37 . 41 . 61 . 89 . 181
28608252345	13 . 29 . 29 . 29 . 37 . 53 . 61 . 73 . 97 . 113 . 149 . 181
112899039159	5 . 13 . 13 . 17 . 17 . 17 . 17 . 29 . 37 . 41 . 61 . 73 . 73 . 73 . 173

5	1. 11
13	3. 29
17	9
29	5. 111. 179
37	25. 49. 1011. 4761. 10039
41	23. 59. 469. 4123. 14901
53	7. 99. 961. 4989. 20769. 63911

61	39. 61. 205. 1381. 5041
73	19. 127. 311. 419. 749. 466489
89	21. 199. 691. 1089. 5717. 16041
97	53. 141. 247. 335. 4021. 6261. 7319. 79011. 396783. 563235*
101	81. 121. 283. 3717. 6989. 9817. 12605. 32239. 81487. 263489*. 10831321
109	43. 261. 393. 829. 2355. 2441. 3749. 6061. 21189. 29169*. 32003. 128359. 140871. 408489. 1230349. 8649761
113	83. 309. 761. 1047. 1499. 2343. 5567. 27429. 203091. 206707*. 244299. 637855
137	63. 211. 485. 611. 759. 1159. 1581. 3351. 9801. 13489*. 21161. 27611. 29929. 95963. 110211. 228179. 234881. 2028211. 35272357
149	61. 237. 535. 1131. 2025. 3339. 8879. 25689. 148939. 207171*. 244299. 247699. 302111. 567629. 588489. 1780489. 3666653. 5472411. 9530277. 17363031*. 148757489
157	101. 213. 527. 841. 1043. 8579. 9947. 20511. 37579. 47829*. 57989. 91587. 99011. 211221. 317039. 1493911. 1996199. 2050005. 6101547. 10126399*. 11483821. 61017271. 1359685525
173	13. 359. 679. 705. 1371. 12815. 13507. 23915. 44301. 47389*. 47761. 86487. 117281. 183739. 257665. 289589. 313489. 326957. 582997. 634205*. 922769. 966391. 3872099. 8812979. 15035789. 25252451. 112899039159
181	143. 219. 943. 1305. 2677. 3039. 5573. 7745. 13251. 14261*. 21139. 23311. 81669. 99407. 115983. 142047. 191279. 205111. 349835. 355989*. 840421. 851929. 1341429. 8175989. 10251621. 10763489. 31456571. 4949475989. 28608252345
193	31. 417. 1899. 4215. 5821. 20875. 22805. 23901. 29691. 79871*. 108111. 114611. 234333. 269459. 1165689. 1362611. 3376311. 5125339. 11398611. 23866411*. 34411159. 107402539. 322564791
197	169. 1351. 1745. 1801. 3377. 8049. 12383. 27355. 27411. 31351*. 32139. 49813. 66361. 139701. 140489. 245293. 306757. 387921. 628261. 834267*. 1029353. 1299241. 1499001. 2159739. 4370811. 4490249. 4705711. 6489011. 35944451. 143828743*. 150446761. 657182319

Zerlegbare $aa + 9$

1	5	2	13
4	5 . 5	5	17
7	29	8	73
10	109	11	5 . 13
13	89	14	5 . 41
16	5 . 53	17	149
19	5 . 37	22	17 . 29
26	5 . 137	28	13 . 61
29	5 . 5 . 17	31	5 . 97
37	13 . 53	41	5 . 13 . 13
46	5 . 5 . 5 . 17	50	13 . 193
55	37 . 41	56	5 . 17 . 37
65	29 . 73	67	13 . 173
68	41 . 113	71	5 . 5 . 101

73	17 . 157	76	5 . 13 . 89
79	5 . 5 . 5 . 5 . 5	80	13 . 17 . 29
89	5 . 13 . 61	94	5 . 29 . 61
106	5 . 13 . 173	109	5 . 29 . 41
119	5 . 13 . 109	124	5 . 17 . 181
128	13 . 13 . 97	131	5 . 17 . 101
143	53 . 193	154	5 . 5 . 13 . 73
155	61 . 197	158	13 . 17 . 113
163	97 . 137	166	5 . 37 . 149
167	13 . 29 . 37	175	17 . 17 . 53
181	5 . 29 . 113	191	5 . 41 . 89
196	5 . 5 . 29 . 53	211	5 . 61 . 73
232	13 . 41 . 101	239	5 . 29 . 197
241	5 . 37 . 157	254	5 . 5 . 29 . 89
271	5 . 5 . 13 . 113	281	5 . 53 . 149
284	5 . 13 . 17 . 73	301	5 . 13 . 17 . 41
314	5 . 13 . 37 . 41	352	17 . 37 . 197
379	5 . 5 . 13 . 13 . 17	413	17 . 29 . 173
419	5 . 97 . 181	430	17 . 73 . 149
436	5 . 193 . 197	437	17 . 41 . 137
446	5 . 5 . 73 . 109	454	5 . 5 . 5 . 17 . 97
464	5 . 17 . 17 . 149	521	5 . 5 . 61 . 89
529	5 . 5 . 29 . 193	535	13 . 101 . 109
544	5 . 13 . 29 . 157	547	41 . 41 . 89
574	5 . 13 . 37 . 137	610	37 . 89 . 113
629	5 . 5 . 41 . 193	704	5 . 5 . 5 . 5 . 13 . 61
722	37 . 73 . 193	746	5 . 5 . 113 . 197
796	5 . 5 . 5 . 37 . 137	811	5 . 17 . 53 . 73
821	5 . 5 . 13 . 17 . 61	848	29 . 137 . 181
869	5 . 13 . 37 . 157	943	37 . 61 . 197
971	5 . 5 . 109 . 173	991	5 . 17 . 53 . 109
1015	17 . 157 . 193	1042	13 . 17 . 17 . 17 . 17
1055	13 . 13, 37 . 89	1070	61 . 137 . 137
1081	5 . 13 . 89 . 101	1129	5 . 5 . 13 . 37 . 53

1144	5 . 17 . 89 . 173
1175	41 . 113 . 149
1259	5 . 13 . 89 . 137
1298	13 . 29 . 41 . 109
1309	5 . 53 . 53 . 61
1324	5 . 13 . 149 . 181
1421	5 . 5 . 5 . 41 . 197
1559	5 . 17 . 17 . 29 . 29
1618	97 . 137 . 197
1627	13 . 17 . 53 . 113
1646	5 . 5 . 29 . 37 . 101
1675	13 . 29 . 61 . 61

1687	73 . 101 . 193
1805	13 . 29 . 29 . 149
1831	5 . 13 . 17 . 37 . 41
1909	5 . 13 . 17 . 17 . 97
1979	5 . 5 . 29 . 37 . 73
2069	5 . 13 . 13 . 17 . 149
2182	13 . 29 . 73 . 173
2351	5 . 13 . 17 . 41 . 61
2528	17 . 41 . 53 . 173
2596	5 . 5 . 17 . 101 . 257
2719	5 . 13 . 29 . 37 . 53
2839	5 . 61 . 73 . 181
2953	13 . 17 . 109 . 181
3038	17 . 29 . 97 . 193
3089	5 . 17 . 37 . 37 . 41
3458	29 . 41 . 89 . 113
3496	5 . 5 . 37 . 73 . 181
3571	5 . 5 . 37 . 61 . 113
3677	13 . 13 . 13 . 17 . 181
4136	5 . 13 . 17 . 113 . 137
4171	5 . 5 . 5 . 13 . 53 . 101
4196	5 . 5 . 41 . 89 . 193
4237	37 . 41 . 61 . 97
4459	5 . 17 . 29 . 37 . 109
4489	5 . 53 . 193 . 197
4496	5 . 5 . 13 . 37 . 41 . 41
4565	13 41 . 113 . 173
4786	5 . 13 . 53 . 61 . 109
5029	5 . 5 . 13 . 13 . 41 . 73
5111	5 . 13 . 13 . 13 . 29 . 41
5125	37 . 37 . 53 . 181
5198	13 . 13 . 29 . 37 . 149
5401	5 . 17 . 29 . 61 . 97
5549	5 . 13 . 41 . 53 . 109
5579	5 . 5 . 5 . 13 . 61 . 157
5605	13 . 17 . 17 . 37 . 113
5921	5 . 5 . 5 . 17 . 73 . 113
6329	5 . 5 . 5 . 5 . 5 . 13 . 17 . 29
6346	5 . 5 . 13 . 17 . 37 . 197
6421	5 . 5 . 5 . 17 . 89 . 109
6494	5 . 37 . 37 . 61 . 101
6641	5 . 13 . 37 . 53 . 173
6821	5 . 5 . 53 . 97 . 181
7196	5 . 5 . 17 . 37 . 37 . 89
7271	5 . 5 . 17 . 37 . 41 . 41
7489	5 . 29 . 41 . 53 . 89
7616	5 . 13 . 53 . 113 . 149
7646	5 . 5 . 13 . 13 . 101 . 137

7729	5 . 5 . 97 . 109 . 113
7934	5 . 17 . 53 . 89 . 157
9650	29 . 113 . 157 . 181
10012	13 . 13 . 29 . 113 . 181
10154	5 . 5 . 17 . 41 . 61 . 97
10447	29 . 73 . 149 . 173
10736	5 . 13 . 97 . 101 . 181
11074	5 . 13 . 61 . 157 . 197
11671	5 . 5 . 5 . 41 . 97 . 137
12109	5 . 17 . 41 . 109 . 193
12191	5 . 37 . 41 . 97 . 101
13561	5 . 13 . 13 . 17 . 37 . 173
14029	5 . 5 . 13 . 29 . 53 . 197
15004	5 . 5 . 13 . 37 . 97 . 193
16096	5 . 5 . 13 . 13 . 13 . 53 . 89
16291	5 . 13 . 17 . 29 . 41 . 101
17029	5 . 5 . 17 . 41 . 53 . 157
17357	13 . 41 . 41 . 61 . 113
17668	17 . 29 . 37 . 109 . 157
18671	5 . 5 . 5 . 5 . 5 . 17 . 17 . 193
19504	5 . 5 . 17 . 89 . 89 . 113
20651	5 . 61 . 61 . 73 . 157
20813	17 . 37 . 53 . 73 . 89
22085	13 . 41 . 53 . 89 . 97
22367	17 . 17 . 37 . 149 . 157
22700	13 . 17 . 29 . 37 . 41 . 53
23425	29 . 29 . 41 . 73 . 109
23671	5 . 5 . 5 . 5 . 13 . 29 . 29 . 41
23879	5 . 5 . 13 . 61 . 73 . 197
24001	5 . 61 . 61 . 113 . 137
24311	5 . 53 . 61 . 101 . 181
25645	89 . 137 . 149 . 181
26141	5 . 13 . 17 . 37 . 61 . 137
27341	5 . 13 . 17 . 17 . 101 . 197
27731	5 . 13 . 29 . 37 . 37 . 149
27805	13 . 37 . 73 . 101 . 109
27844	5 . 13 . 13 . 13 . 13 . 61 . 89
28804	5 . 5 . 29 . 37 . 157 . 197
28973	17 . 41 . 73 . 73 . 113
30544	5 . 17 . 29 . 37 . 53 . 193
33629	5 . 5 . 13 . 89 . 113 . 173
34010	13 . 13 . 29 . 53 . 61 . 73
38608	13 . 41 . 137 . 137 . 149
39704	5 . 5 . 5 . 13 . 73 . 97 . 137
40030	17 . 41 . 97 . 137 . 173
40304	5 . 5 . 73 . 73 . 89 . 137
42173	29 . 29 . 89 . 109 . 109
42421	5 . 5 . 5 . 5 . 13 . 37 . 41 . 73

43864	5 . 13 . 37 . 89 . 89 . 101
47296	5 . 5 . 5 . 13 . 73 . 109 . 173
47335	13 . 29 . 89 . 173 . 193
48046	5 . 5 . 5 . 5 . 13 . 29 . 97 . 101
48829	5 . 5 . 5 . 5 . 17 . 29 . 53 . 73
49883	13 . 17 . 17 . 41 . 41 . 197
49924	5 . 17 . 41 . 73 . 97 . 101
54871	5 . 5 . 13 . 17 . 53 . 53 . 97
54926	5 . 37 . 41 . 41 . 89 . 109
55709	5 . 97 . 109 . 149 . 197
57701	5 . 37 . 41 . 41 . 53 . 101
57839	5 . 13 . 13 . 13 . 13 . 13 . 17 . 53
62402	13 . 13 . 17 . 89 . 97 . 157
66584	5 . 13 . 17 . 17 . 53 61 . 73
70171	5 . 5 . 5 . 17 . 37 . 173 . 181
71021	5 . 5 . 13 . 13 . 13 . 17 . 37 . 73
71276	5 . 17 . 61 . 89 . 101 . 109
71354	5 . 5 . 17 . 37 . 41 . 53 . 149
73972	13 . 17 . 29 . 53 . 89 . 181
78829	5 . 5 . 5 . 5 . 29 . 37 . 41 . 113
79051	5 . 13 . 13 . 37 . 37 . 37 . 73
84563	13 . 17 . 17 . 17 . 17 . 37 . 89
84818	17 . 29 . 29 . 61 . 73 . 113
86221	5 . 5 . 61 . 73 . 173 . 193
88411	5 . 13 . 37 . 73 . 113 . 197
95071	5 . 5 . 13 . 37 . 61 . 61 . 101
95188	13 . 13 . 13 . 17 . 41 . 61 . 97
105274	5 . 41 . 53 . 73 . 89 . 157
109279	5 . 5 . 29 . 37 . 41 . 61 . 89
109991	5 . 13 . 53 . 89 . 109 . 181
112171	5 . 5 . 5 . 17 . 109 . 157 . 173
114499	5 . 29 . 29 . 41 . 193 . 197
114896	5 . 5 . 13 . 41 . 61 . 109 . 149
115079	5 . 5 . 5 . 5 . 29 . 53 . 61 . 113
116881	5 . 13 . 53 . 73 . 157 . 173
127114	5 . 17 . 29 . 29 . 37 . 41 . 149
133523	17 . 29 . 41 . 53 . 53 . 157
134764	5 . 17 . 97 . 101 . 113 . 193
137659	5 . 13 . 37 . 137 . 149 . 193
141581	5 . 13 . 13 . 17 . 37 109 . 173
146794	5 . 13 . 41 41 . 53 . 61 . 61
147409	5 . 13 . 13 . 41 . 53 . 61 97
154679	5 . 5 . 29 . 37 . 41 . 73 . 149
154729	5 . 5 . 17 . 17 . 61 . 157 . 173
157454	5 . 5 . 5 . 13 . 37 . 41 . 89 . 113
167689	5 . 13 . 13 . 13 . 73 . 89 . 197
170107	13 . 17 . 17 . 29 . 37 . 37 . 97
174427	61 . 89 . 113 . 137 . 181

178336	5 . 13 . 13 . 41 . 61 . 101 . 149
178988	17 . 37 . 37 . 73 . 109 . 173
180416	5 . 13 . 17 . 29 . 89 . 101 . 113
190021	5 . 5 . 17 . 41 . 53 . 113 . 173
190541	5 . 17 . 41 . 137 . 193 . 197
193546	5 . 5 . 5 . 13 . 13 . 97 . 101 . 181
193829	5 . 5 . 5 . 5 . 5 . 29 . 89 . 137
219754	5 . 5 . 13 . 17 . 17 . 53 . 89 . 109
249871	5 . 5 . 13 . 17 . 17 . 29 . 73 . 157
250250	37 . 41 . 53 . 61 . 113 . 113
252328	13 . 41 . 89 . 97 . 101 . 137
263681	5 . 13 . 13 . 37 . 101 . 101 . 109
265256	5 . 17 . 29 . 41 . 61 . 101 . 113
280750	13 . 13 . 17 . 61 . 61 . 73 . 101
286904	5 . 5 . 17 . 29 . 29 . 41 . 41 . 137
293687	17 . 37 . 61 . 73 . 89 . 173
311921	5 . 5 . 5 . 17 . 53 . 61 . 73 . 97
313454	5 . 5 . 5 . 13 . 13 . 13 . 13 . 13 . 29 . 73
314257	17 . 17 . 73 . 109 . 109 . 197
316739	5 . 17 . 37 . 41 . 73 . 73 . 73
324952	29 . 37 . 41 . 89 . 149 . 181
341569	5 . 17 . 29 . 29 . 53 . 89 . 173
347543	17 . 29 . 41 . 113 . 137 . 193
356809	5 . 13 . 29 . 37 . 41 . 113 . 197
377804	5 . 5 . 13 . 109 . 113 . 181 . 197
386722	13 . 29 . 109 . 109 . 173 . 193
393079	5 . 5 . 5 . 13 . 17 . 137 . 137 . 149
415825	17 . 37 . 37 . 109 . 173 . 197
419246	5 . 5 . 29 . 53 . 137 . 173 193
423475	17 . 41 . 89 . 89 . 109 . 149
448280	41 . 41 . 41 . 89 . 181 . 181
496004	5 . 5 . 13 . 17 . 37 . 41 . 149 . 197
512579	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 53 . 97
520921	5 . 5 . 5 . 13 . 53 . 97 . 109 . 149
524704	5 . 5 . 5 . 13 . 13 . 29 . 41 . 97 . 113
528967	17 . 29 . 101 . 109 . 149 . 173
539996	5 . 5 . 13 . 13 . 37 . 109 . 109 . 157
541829	5 . 5 . 5 . 13 . 17 . 29 . 41 . 41 . 109
550985	37 . 41 . 61 . 101 . 109 . 149
554279	5 . 5 . 13 . 13 . 37 . 61 . 89 . 181
599510	13 . 17 . 29 . 29 . 109 . 113 . 157
693775	17 . 17 . 17 . 41 . 97 . 109 . 113
700061	5 . 13 . 41 . 53 . 89 . 101 . 193
713291	5 . 17 . 29 . 29 . 29 . 41 . 41 . 73
744421	5 . 5 . 5 . 13 37 . 149 . 157 . 197
745249	5 . 13 . 13 . 29 . 29 . 53 . 73 . 101
792113	29 . 61 . 89 . 101 . 109 . 181
847319	5 . 17 . 37 . 73 . 101 . 113 . 137

859379	5 . 5 . 17 . 29 . 29 . 53 . 101 . 193

895208	13 . 17 . 17 . 17 . 29 . 41 . 61 . 173
895861	5 . 17 . 29 . 89 . 97 . 109 . 173
937766	5 . 13 . 17 . 29 . 41 . 53 . 73 . 173
947329	5 . 5 . 5 . 37 . 73 . 89 . 109 . 137
970454	5 . 5 . 5 . 37 . 73 . 97 . 149 . 193
984934	5 . 13 . 17 . 29 . 29 . 61 . 109 . 157
987406	5 . 17 . 53 . 73 . 101 . 149 . 197
1196173	53 . 89 . 97 . 101 . 113 . 137
1202704	5 . 5 . 5 . 17 . 17 . 37 . 61 . 113 . 157
1256084	5 . 13 . 17 . 29 . 53 . 61 . 97 . 157
1297090	13 . 29 . 37 . 41 . 109 . 137 . 197
1460288	13 . 13 . 13 . 17 . 29 . 101 . 101 . 193
1717025	13 . 29 41 . 53 . 73 . 157 . 157
1799921	5 . 5 . 5 . 5 . 5 . 17 . 29 . 37 . 157 . 181
1800254	5 . 5 . 17 . 37 . 97 . 101 . 109 . 193
2153956	5 . 17 . 101 . 101 . 157 . 173 . 197
2253046	5 . 5 . 5 . 5 . 5 . 5 . 29 . 41 . 53 . 149 . 173
2347195	17 . 29 . 41 . 53 . 137 . 137 . 137
2362579	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 29 . 37 . 197
2382560	13 . 29 . 37 . 101 . 113 . 181 . 197
2454779	5 . 5 . 13 . 41 . 73 . 109 . 157 . 181
2473954	5 . 5 . 5 . 13 . 17 . 17 . 29 . 41 . 97 . 113
2579296	5 . 5 . 5 . 5 . 5 . 17 . 29 . 41 . 61 . 89 . 97
2710934	5 . 17 . 17 . 17 . 37 . 41 . 53 . 61 . 61
2867521	5 . 5 . 17 . 61 . 73 . 101 . 137 . 157
2960596	5 . 5 . 13 . 17 . 41 . 53 . 73 . 73 . 137
3045079	5 . 5 . 5 . 5 . 13 . 17 . 17 . 101 . 113 . 173
3287839	5 . 17 . 17 . 17 . 29 . 53 . 53 . 73 . 73
3386888	13 . 13 . 17 . 29 . 37 . 137 . 157 . 173
3569269	5 . 13 . 29 . 41 . 53 . 89 . 101 . 173
4046131	5 . 13 . 17 . 29 . 89 . 101 . 157 . 181
4546271	5 . 5 . 13 . 17 . 41 . 53 . 53 . 109 . 149
4699704	5 . 5 . 5 . 13 . 61 . 73 . 113 . 137 . 197
4889605	37 . 41 . 53 . 61 . 73 . 173 . 193
8026096	5 . 5 . 17 . 37 . 37 . 89 . 101 . 109 . 113
8182343	17 . 17 . 29 . 41 . 73 . 73 . 101 . 181
8931226	5 . 37 . 53 . 61 . 89 . 89 . 113 . 149
9237421	5 . 5 . 5 . 5 . 5 . 5 . 13 . 17 . 17 . 29 . 29 . 29 . 149
9250762	41 . 89 . 97 . 101 . 101 . 137 . 173
10419736	5 . 13 . 13 . 29 . 37 . 73 . 101 . 109 . 149
11077571	5 . 5 . 13 . 13 . 41 . 109 . 113 . 149 . 193
12519856	5 . 13 . 37 37 . 41 . 53 . 61 . 97 . 137
13237028	17 . 29 . 37 . 41 . 61 . 149 . 149 . 173
13382956	5 . 13 . 17 . 29 . 29 . 37 . 137 . 193 . 197
14937769	5 . 13 . 17 . 37 . 53 . 61 . 61 . 101 . 137

19912579	5 . 5 . 5 . 5 . 5 . 13 . 41 . 41 . 97 . 173 . 173
20620229	5 . 5 . 37 . 37 . 61 . 73 . 73 . 97 . 197
22181629	5 . 5 . 13 . 13 . 13 . 17 . 29 . 37 . 41 . 53 . 113
23504986	5 . 13 . 13 . 13 . 29 . 29 . 29 . 41 . 53 . 73
25674911	5 . 13 . 29 . 37 . 41 . 73 . 89 . 113 . 157
26999399	5 . 13 . 13 . 29 . 37 . 97 . 109 . 193 . 197
33399844	5 . 17 . 17 . 29 . 37 . 37 . 41 . 73 . 73 . 89
33753059	5 . 13 . 13 . 41 . 89 . 97 . 101 . 109 . 173
34618846	5 . 5 . 13 . 13 . 13 . 17 . 17 . 37 . 97 . 109 . 193
34792409	5 . 13 . 13 . 13 . 17 . 29 . 41 . 101 . 137 . 197
40103726	5 . 17 . 37 . 41 . 109 . 109 . 197
41494546	5 . 5 . 5 . 13 . 61 . 61 . 89 . 109 . 149 . 197
48279454	5 . 5 . 5 . 5 . 13 . 29 . 41 . 41 . 41 . 61 . 181
60740461	5 . 13 . 17 . 17 . 17 . 41 . 73 . 97 . 101 . 197
64370954	5 . 5 . 5 . 13 . 17 . 37 . 53 . 61 . 73 . 89 . 193
96499349	5 . 13 . 17 . 29 37 . 41 . 61 . 73 . 137 . 157
105742171	5 . 5 . 5 . 13 . 17 . 29 . 29 . 37 . 41 . 41 . 53 . 73
110518796	5 . 5 . 5 . 13 . 37 . 53 . 53 . 61 . 73 . 109 . 149
111009121	5 . 5 . 13 . 17 . 17 . 37 . 37 . 37 . 73 . 113 . 157
113737804	5 . 5 . 13 . 13 . 29 . 29 . 53 . 73 . 89 . 97 . 109
117290203	17 . 29 . 37 . 41 . 53 . 73 . 109 . 113 . 193
149574656	5 . 29 . 41 . 61 . 73 . 137 . 173 . 181 . 197
163030454	5 . 5 . 5 . 13 . 13 . 17 . 37 . 37 . 53 . 73 . 89 . 157
165242573	13 . 29 . 37 . 41 . 73 . 97 . 109 . 157 . 197
178643779	5 . 5 . 13 . 41 . 41 . 61 . 113 . 137 . 157 . 197
200760094	5 . 13 . 17 . 17 . 37 . 37 . 37 . 41 . 53 . 101 . 193
323643829	5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 37 . 61 . 73 . 73 . 97
401580454	5 . 5 . 5 . 13 . 53 . 61 . 73 . 73 . 97 . 137 . 137 . 193
478666540	17 . 17 . 29 . 37 . 41 . 61 . 73 . 149 . 157 . 173
1411168679	5 . 5 . 13 . 17 . 17 . 89 . 113 . 157 . 173 . 197 . 197

5	1. 4. 79
13	2. 11. 41
17	5. 29. 46. 379. 1042
29	7. 22. 80. 1559. 6329
37	19. 56. 167
41	14. 55. 109. 301. 314. 1831. 3089. 4496. 5111. 7271*. 23671
53	16. 37. 175. 196. 1129. 2719. 22700. 57839
61	28. 89. 94. 704. 821. 1309. 1675. 2351. 146794. 2710934*
73	8. 65. 154. 211. 284. 811. 1979. 5029. 34010. 42421*. 48829. 66584. 71021. 79051. 313454. 316739. 713291. 3287839. 23504986. 105742171*
89	13. 76. 191. 254. 521. 547. 1055. 7196. 7489. 16096*. 20813. 27844. 84563. 109279. 33399844
97	31. 128. 454. 1909. 4237. 5401. 10154. 22085. 54871. 95188*. 147409. 170107. 311921. 512579. 2579296. 323643829

101	71. 131. 232. 1081. 1646. 4171. 6494. 12191. 16291. 43864*. 48046. 49924. 57701. 95071. 280750. 745249
109	10. 119. 446. 535. 991. 1298. 4459. 4786. 5549. 6421*. 23425. 27805. 42173. 54926. 71276. 219754. 263681. 541829. 113737804

113	68. 158. 181. 271. 610. 1627. 3458. 3571. 5605. 5921*. 7729. 17357. 19504. 28973 78829. 84818. 115079. 157454. 180416. 250250*. 265256. 524704. 693775. 2473954. 8026096. 22181629
137	26. 163. 437. 574. 796. 1070. 1259. 4136. 7646. 11671*. 24001. 26141. 39704. 40304. 193829. 252328. 286904. 847319. 947329. 1196173*. 2347195. 2960596. 12519856. 14937769
149	17. 166. 281. 430. 464. 1175. 1805. 2069. 5198. 7616*. 27731. 38608. 71354. 114896. 127114. 154679. 178336. 393079. 423475. 520921*. 550985. 4546271. 8931226. 9237421. 10419736. 110518796
157	73. 241. 544. 869. 2596. 5579. 7934. 17029. 17668. 20651*. 22367. 62402. 105274. 133523. 249871. 539996. 599510. 984934. 1202704. 1256084*. 1717025. 2867521. 25674911. 96499349. 111009121. 163030454
173	67. 106. 413. 971. 1144. 2182. 2528. 4565. 6641. 10447*. 13561. 33629. 40030. 47296. 112171. 116881. 141581. 154729. 178988. 190021*. 293687. 341569. 528967. 895208. 895861. 937766. 2253046. 3045079. 3386888. 3569269*. 9250762. 13237028. 19912579. 33753059. 478666540
181	124. 419. 848. 1324. 2839. 2953. 3496. 3677. 5125. 6821*. 9650. 10012. 10736. 24311. 25645. 70171. 73972. 109991. 174427. 193546*. 324952. 448280. 554279. 792113. 1799921. 2454779. 4046131. 8182343. 48279454
193	50. 143. 529. 629. 722. 1015. 1687. 3038. 4196. 12109*. 15004. 18671. 30544. 47335. 86221. 134764. 137659. 347543. 386722. 419246*. 700061. 859379. 970454. 1460288. 1800254. 4889605. 11077571. 34618846. 64370954. 117290203*. 200760094. 401580454
197	155. 239. 352. 436. 746. 943. 1421. 1618. 4489. 6346*. 11074. 14029. 23879. 27341. 28804. 49883. 55709. 88411. 114499. 167689*. 190541. 314257. 356809. 377804. 415825. 496004. 744421. 987406. 1297090. 2153956*. 2362579. 2382560. 4699704. 13382956. 26620229. 26999399. 34792409. 40103726. 41494546. 60740461*. 149574656. 165242573. 178643779. 1411168679

Zerlegbare $aa + 16$.

1	17
3	5 . 5
5	41
7	5 . 13
9	97
11	137
13	5 . 37
17	5 . 61

19	13 . 29
23	5 . 109
27	5 . 149
33	5 . 13 . 17
35	17 . 73
39	29 . 53
45	13 . 157
47	5 . 5 . 89
53	5 . 5 . 113
61	37 . 101
67	5 . 17 . 53
77	5 . 29 . 41
87	5 . 37 . 41
97	5 . 5 . 13 . 29
103	5 . 5 . 5 . 5 . 17
105	61 . 181
131	89 . 193
135	17 . 29 . 37
137	5 . 13 . 17 . 17
141	101 . 197
147	5 . 5 . 5 . 173
173	5 . 53 . 113
227	5 . 13 . 13 . 61
241	13 . 41 . 109
253	5 . 5 . 13 . 197
257	5 . 73 . 181
263	5 . 101 . 137
271	17 . 29 . 149
279	13 . 53 . 113
309	29 . 37 . 89
357	5 . 13 . 37 . 53
383	5 . 13 . 37 . 61
397	5 . 5 . 5 . 13 . 97
403	5 5 . 73 . 89
487	5 . 13 . 41 . 89
505	37 . 61 . 113
545	17 . 101 . 173
569	41 . 53 . 149
579	13 . 17 . 37 . 41
619	29 . 73 . 181
647	5 . 5 . 5 . 17 . 197
677	5 . 29 . 29 . 109
747	5 . 5 . 13 . 17 . 101
851	13 . 17 . 29 . 113
897	5 . 5 . 5 . 41 . 157
903	5 . 5 . 13 . 13 . 193
987	5 . 17 . 73 . 157
1021	13 . 17 . 53 . 89

1203	5 . 5 . 13 . 61 . 73
1237	5 . 29 . 61 . 173
1293	5 . 13 . 17 . 17 . 89
1353	5 . 5 . 5 . 5 . 29 . 101
1359	13 . 17 . 61 . 137
1463	5 . 13 . 13 . 17 . 149
1553	5 . 5 . 13 . 41 . 181
1717	5 . 41 . 73 . 197
1837	5 . 17 . 29 . 37 . 37
1929	137 . 157 . 173
2203	5 . 5 . 13 . 109 . 137
2223	5 . 29 . 173 . 197
2243	5 . 13 . 17 . 29 . 157
2301	29 . 41 . 61 . 73
2447	5 . 5 . 17 . 37 . 193
2455	29 . 37 . 41 . 137
2477	5 . 13 . 13 . 53 . 137
2593	5 . 13 . 13 . 73 . 109
2687	5 . 17 . 29 . 29 . 101
2823	5 . 17 . 29 . 53 . 61
2957	5 . 13 . 17 . 41 . 193
3095	17 . 37 . 97 . 157
3113	5 . 13 . 29 . 53 . 97
3153	5 . 5 . 13 . 13 . 13 . 181
3247	5 . 5 . 53 . 73 . 109
3293	5 . 101 . 109 . 197
3603	5 . 5 . 5 . 17 . 41 . 149
3607	5 . 13 . 13 . 89 . 173
3777	5 . 13 41 . 53 . 101
3847	5 . 5 . 29 . 137 . 149
4453	5 . 5 . 17 . 37 . 97
4497	5 . 5 . 61 . 89 . 149
4505	13 . 13 . 29 . 41 . 101
4601	29 . 37 . 109 . 181
4647	5 . 5 . 5 . 13 . 97 . 137
4853	5 5 . 5 . 29 . 73 . 89
4897	5 . 5 . 5 . 5 . 17 . 37 . 61
5337	5 . 13 . 17 . 149 . 173
5473	5 . 17 . 53 . 61 . 109
5635	13 . 13 . 13 . 97 . 149
5897	5 . 5 . 5 . 29 . 53 . 181
5921	13 . 89 . 157 . 193
6051	13 . 17 . 29 . 29 . 197
6081	37 . 53 . 109 . 173
6427	5 . 17 . 53 . 53 . 173
6605	61 . 73 . 97 . 101
6727	5 . 13 . 61 . 101 . 113
7345	17 . 89 . 181 . 197

7413	5 . 17 . 37 . 101 . 173
7547	5 . 5 . 13 . 13 . 13 . 17 . 61
7683	5 . 17 . 37 . 137 . 137
7703	5 . 5 . 13 . 41 . 61 . 73
7963	5 . 13 . 89 . 97 . 113
8141	73 . 89 . 101 . 101
8523	5 . 37 . 41 . 61 . 157
8747	5 . 5 . 101 . 157 . 193
9133	5 . 13 . 61 . 109 . 193
9353	5 . 5 . 5 . 13 . 13 . 41 . 101
10003	5 . 5 . 13 . 37 . 53 . 157
11967	5 . 13 . 17 . 29 . 41 . 109
12045	13 . 29 . 53 . 53 . 137
12257	5 . 29 . 53 . 113 . 173
12603	5 . 5 . 5 . 5 . 13 . 113 . 173
12667	5 . 37 . 73 . 109 . 109
13397	5 . 5 . 5 . 13 . 17 . 73 . 89
16897	5 . 5 . 5 . 17 . 29 . 41 . 113
17477	5 . 17 . 17 . 29 . 37 . 197
17635	13 . 41 . 53 . 101 . 109
17853	5 . 5 . 5 . 109 . 149 . 157
19991	17 . 29 . 61 . 97 . 137
20167	5 . 41 . 97 . 113 . 181
23677	5 . 53 . 97 . 113 . 193
24447	5 . 5 . 13 . 13 . 17 . 53 . 157
24785	13 . 13 . 17 . 29 . 73 . 101
25617	5 . 13 . 29 . 37 . 97 . 97
28581	13 . 53 . 73 . 109 . 149
29217	5 . 13 . 37 . 37 . 53 . 181
29853	5 . 5 . 5 . 17 . 41 . 53 . 193
36107	5 . 13 . 17 . 53 . 113 . 197
36823	5 . 13 . 17 . 41 . 173 . 173
37579	5 . 17 . 29 . 41 . 89 . 157
38863	5 . 13 . 17 . 17 . 37 . 41 . 53
39653	5 . 5 . 29 . 101 . 109 . 197
40853	5 . 5 . 5 . 13 . 61 . 113 . 149
41373	5 . 13 . 29 . 29 . 173 . 181
44269	17 . 53 . 61 . 181 . 197
44947	5 . 5 . 13 . 17 . 17 . 137 . 157

45793	5 . 13 . 37 . 89 . 97 . 101
52157	5 . 17 . 17 . 17 . 37 . 41 . 73
52379	37 . 73 . 89 . 101 . 113
52393	5 . 17 . 29 . 41 . 157 . 173
57323	5 . 13 . 17 29 41 . 41 . 61
57803	5 . 5 . 89 . 97 . 113 . 137
66333	5 . 13 . 17 . 17 . 29 . 41 . 197

67327	5 . 37 . 41 . 61 . 97 . 101
68215	37 . 61 . 101 . 137 . 149
69347	5 . 5 . 101 . 101 . 109 . 173
73467	5 . 29 . 41 . 89 . 101 . 101
74133	5 . 13 . 13 . 41 . 41 . 53 . 73
81413	5 . 13 . 29 . 29 . 29 . 37 . 113
82817	5 . 13 . 73 . 89 . 109 . 149
82893	5 . 17 . 37 . 73 . 173 . 173
103317	5 . 13 . 13 . 29 . 37 . 61 . 193
104293	5 . 13 . 61 . 101 . 157 . 173
113699	29 . 29 . 29 . 53 . 73 . 137
126497	5 . 5 . 13 . 53 . 61 . 97 . 157
130553	5 . 5 . 13 . 53 . 97 . 101 . 101
132143	5 . 29 . 53 . 193 . 193
139477	5 . 37 . 41 . 97 . 137 . 193
150897	5 . 5 . 5 . 13 . 29 . 61 . 89 . 89
154821	29 . 37 . 41 . 41 . 97 . 137
158373	5 . 13 . 17 . 37 . 61 . 89 . 113
158509	17 . 17 . 53 . 101 . 109 . 149
161399	17 . 17 . 53 . 89 . 97 . 197
162383	5 . 17 . 89 . 149 . 149 . 157
171293	5 . 17 . 29 . 41 . 41 . 73 . 97
172569	13 . 29 . 29 . 101 . 149 . 181
174727	5 . 13 . 17 . 37 . 53 . 73 . 193
232147	5 . 5 . 5 . 13 . 41 . 41 . 109 . 181
239387	5 . 53 . 97 . 109 . 113 . 181
240347	5 . 5 . 17 . 41 . 89 . 193 . 193
242897	5 . 5 . 5 . 17 . 17 . 97 . 113 . 149
251817	5 . 13 . 29 . 41 . 53 . 113 . 137
260033	5 . 13 . 13 . 17 . 29 . 29 . 29 . 193
260575	17 . 29 . 61 . 73 . 157 . 197
300527	5 . 13 . 17 . 37 . 113 . 113 . 173
374203	5 . 5 . 17 . 89 . 113 . 181 . 181
378671	13 . 13 . 37 . 41 . 53 . 61 . 173
434441	13 . 13 . 37 . 37 . 41 . 101 . 197
577603	5 . 5 . 5 . 5 . 29 . 29 . 41 . 113 . 137
648447	5 . 5 . 13 . 17 . 61 . 61 . 113 . 181
650103	5 . 5 . 5 . 5 . 29 . 37 . 73 . 89 . 97
658783	5 . 17 . 17 . 29 . 41 . 41 . 61 . 101
696353	5 . 5 . 5 . 5 17 . 17 . 37 . 37 . 37 . 53
748853	5 . 5 . 5 . 5 . 5 . 61 . 109 . 137 . 197
870487	5 . 13 . 61 . 73 . 97 . 137 . 197
873503	5 . 5 . 13 . 13 61 . 109 . 157 . 173
970497	5 5 . 17 . 37 . 53 . 73 . 113 . 137
1193679	13 29 . 41 . 41 . 101 113 . 197
1229533	5 . 13 . 13 . 53 . 53 . 53 . 61 . 197
1259837	5 . 13 . 13 . 13 . 17 . 29 . 37 . 89 . 89
1335487	5 . 17 . 89 . 97 . 113 . 137 . 157

1404163	5 . 13 . 13 . 37 . 41 . 97 . 101 . 157
1626475	13 . 29 . 41 . 73 . 109 . 137 . 157
2008103	5 . 5 . 5 . 13 . 41 . 53 . 61 . 97 . 193
2083893	5 . 13 . 17 . 53 . 73 . 89 . 101 . 113
2116091	17 . 29 . 37 . 101 . 113 . 137 . 157
2373167	5 . 17 . 29 . 37 . 41 . 53 . 157 . 181
2960653	5 . 5 . 13 . 13 . 17 . 17 . 17 . 101 . 113
3258603	5 . 5 . 5 . 37 . 41 . 61 . 61 . 101 . 149
3611583	5 . 17 . 29 . 37 . 61 . 109 . 137 . 157
3898603	5 . 5 . 5 . 13 . 13 . 37 . 41 . 73 . 73 . 89
4945505	13 . 13 . 17 . 17 . 17 . 29 . 89 . 101 . 113
5431603	5 . 5 . 5 . 17 . 17 . 29 . 41 . 73 . 97 . 97
8180243	5 . 13 . 29 . 29 . 37 . 37 . 41 . 53 . 53 . 113 . 193
8268383	5 . 13 . 13 . 29 . 41 . 73 . 73 . 113 . 113
9993613	5 . 13 . 29 . 37 . 53 . 53 . 61 . 61 . 137
10311423	5 . 41 . 41 . 61 . 109 . 113 . 113 . 149
15305803	5 . 5 . 13 . 37 . 53 . 101 . 109 . 173 . 193
16626883	5 . 17 . 73 . 101 . 109 . 149 . 157 . 173
17545053	5 . 5 . 13 . 17 . 17 . 41 . 53 . 101 . 109 . 137
17916571	17 . 37 . 37 . 61 . 73 . 109 . 157 . 181
18500917	5 . 13 . 29 . 41 . 41 . 61 . 89 . 101 . 197
19344643	5 . 13 . 13 . 29 . 41 . 73 . 73 . 113 . 113
20278927	5 . 13 . 17 . 29 . 53 . 73 . 113 . 149 . 197
22858302	5 . 5 . 17 . 17 . 17 . 17 . 17 . 29 . 53 . 61 . 157
38648107	5 . 17 . 17 . 29 . 97 . 109 . 109 . 157 . 197
40473647	5 . 5 . 5 . 5 . 13 . 37 . 41 . 73 . 97 . 137 . 137
46113113	5 . 13 . 13 . 17 . 29 . 37 . 53 . 73 . 181 . 197
1082687431	13 . 17 . 29 53 . 61 . 97 . 109 157 . 173 . 197
1254102921	13 . 13 . 17 . 17 . 41 . 53 . 61 . 97 . 101 . 137 . 181

5	3
13	7
17	1. 33. 103. 137
29	19. 97
37	13. 135. 1837
41	5. 77. 87. 579
53	39. 67. 357. 38863. 696353
61	17. 227. 383. 2823. 4897. 7547. 57323
73	35. 1203. 2301. 7703. 52157. 74133
89	47. 309. 403. 487. 1021. 1293. 4853. 13397. 150897. 1259837*. 3898603
97	9. 397. 3113. 4453. 25617. 171293. 650103. 5431603
101	61. 747. 1353. 2687. 3777. 4505. 6605. 8141. 9353. 24785*. 45793. 67327. 73467. 130553. 658783
109	23. 241. 677. 2593. 3247. 5473. 11967. 12667. 17635
113	53. 173. 279. 505. 851. 6727. 7963. 16897. 52379. 81413*. 158373. 2083893. 2960653. 4945505. 8268383. 19344643

137	11. 263. 1359. 2203. 2455. 2477. 4647. 7683. 12045. 19991*. 57803. 113699. 154821. 251817. 577603. 970497. 9993613. 17545053. 40473647
149	11. 271. 569. 1463. 3603. 3849. 4497. 5635. 28581. 40853*. 68215. 82817. 158509. 242897. 3258603. 10311423
157	45. 897. 987. 2243. 3095. 8523. 10003. 17853. 24447. 37579*. 44947. 126497. 162384. 1335487. 1404163. 1626475. 2116091. 3611583. 22858302
173	147. 545. 1237. 1929. 3607. 5337. 6081. 6427. 7413. 12257*. 12603. 36823. 52393. 69347. 82893. 104293. 300527. 378671. 873503. 16626883*
181	105. 257. 619. 1553. 3153. 4601. 5897. 20167. 29217. 41373*. 172569. 232147. 239387. 374203. 648447. 2373167. 17916571. 1254102921
193	131. 903. 2447. 2957. 5921. 8747. 9133. 23677. 29853. 103317. 132143 139477. 174727. 240347. 260033. 2008103. 8180243 15305803
197	141. 253. 647. 1717. 2223. 3293. 6051. 7345. 17477. 36107*. 39653. 44269. 66333. 161399. 260575. 434441. 748853. 870487. 1193679. 1229533*. 18500917. 20278927. 38648107. 46113113. 1082687431

Zerlegbare $aa + 25$**.**

1	13
2	29
3	17
4	41
6	61
7	37
8	89
9	53
11	73
12	13 . 13
13	97
14	13 . 17
17	157
19	193
27	13 . 29
31	17 . 29
37	17 . 41
38	13 . 113
44	37 . 53
48	17 . 137
51	13 . 101
53	13 . 109
54	17 . 173
56	29 . 109
62	53 . 73
67	37 . 61
71	17 . 149

78	41 . 149
81	37 . 89
84	73 . 97
86	41 . 181
89	29 . 137
97	53 . 89.
99	17 . 17 . 17
116	13 . 17 . 61
118	13 . 29 . 37
119	41 . 173
127	41 . 197
151	101 . 113
157	13 . 13 . 73
168	13 . 41 . 53
174	157 . 193
181	13 . 13 . 97
201	17 . 29 . 41
207	13 . 17 . 97
209	13 . 41 . 41
227	149 . 173
252	17 . 37 . 101
259	13 . 29 . 89
267	181 . 197
274	13 . 53 . 109
303	17 . 37 . 73
309	17 . 53 53
311	13 . 61 . 61
324	13 . 41 . 197
326	13 . 13 . 17 . 37
354	17 . 73 . 101
363	13 . 37 . 137
376	13 . 73 . 149
377	17 . 37 . 113
414	37 . 41 . 113
433	29 . 53 . 61
437	29 . 37 . 89
454	13 . 101 . 157
488	37 . 41 . 157
521	13 . 53 . 197
573	13 . 73 . 173
611	29 . 41 . 157
636	13 . 29 . 29 . 37
638	13 . 173 . 181
677	13 . 17 . 17 . 61
733	37 . 53 . 137
753	13 . 113 . 193
768	13 . 17 . 17 . 157
816	41 . 109 . 149

819	17 . 109 . 181
857	13 . 13 . 41 . 53
858	37 . 101 . 197
898	13 . 17 . 41 . 89
959	29 . 101 . 157
984	29 . 173 . 193
1092	61 . 113 . 173
1104	13 . 29 . 53 . 61
1177	37 . 97 . 193
1252	73 . 109 . 197
1364	13 . 13 . 101 . 109
1431	13 . 17 . 41 . 113
1442	13 . 17 . 97 . 97
1544	17 . 17 . 73 . 113
1561	13 . 17 . 37 . 149
1733	97 . 113 . 137
1767	13 . 29 . 41 . 101
1887	29 . 29 . 29 . 73
2128	17 . 41 . 73 . 89
2144	13 . 29 . 89 . 137
2341	13 . 41 . 53 . 97
2434	17 . 29 . 61 . 197
2751	17 . 41 . 61 . 89
2887	13 . 17 . 109 . 173
2989	13 . 17 . 17 . 29 . 41
3199	13 . 13 . 13 . 17 . 137
3323	37 . 37 . 37 . 109
3471	17 . 37 . 61 . 157
3522	13 . 17 . 37 . 37 . 41
3654	13 . 61 . 113 . 149
3686	17 . 41 . 101 . 193
3788	17 . 61 . 101 . 137.
4219	17 . 41 . 113 . 113
4264	17 . 61 . 89 . 197
4458	13 . 89 . 89 . 193
4798	13 . 89 . 101 . 197
4814	17 . 17 . 17 . 53 . 89
5154	17 . 89 . 97 . 181
5251	13 . 13 . 29 . 29 . 97
5706	13 . 101 . 137 . 181
5927	13 . 13 . 37 53 . 53
6001	29 . 73 . 97 . 173
6157	17 . 53 . 109 . 193
6581	29 . 53 . 73 . 193
6616	13 . 17 . 37 53 . 101
7359	13 . 97 . 109 . 197
7676	53 . 73 . 97 . 157
7753	41 . 61 . 61 . 197

8147	29 . 37 . 157 . 197
8231	17 . 101 . 109 . 181
8776	13 . 13 . 37 . 109 113
9209	73 . 73 . 73 . 109
10049	41 . 89 . 101 . 137
10061	13 . 17 . 29 . 53 . 149
10501	37 . 73 . 137 . 149
12468	13 . 29 . 41 . 89 . 113
12526	17 . 17 . 29 . 97 . 193
13786	73 . 101 . 149 . 173
13787	89 97 . 101 . 109
14067	13 . 29 37 . 41 . 173
14756	13 . 37 . 41 . 61 . 181
15807	13 . 17 . 29 . 101 . 193
17057	13 . 13 . 53 . 109 . 149
18123	13 . 29 . 37 . 61 . 193
18771	13 . 13 . 13 17 . 53 . 89
18823	13 . 29 . 41 . 73 . 157
19553	13 . 17 . 17 . 17 . 41 . 73
19751	17 . 17 . 17 . 29 . 37 . 37
20502	13 . 53 . 61 . 73 . 137
21009	13 . 17 . 37 . 137 . 197
21319	13 . 37 . 37 . 113 . 113
21527	13 . 53 . 61 . 137 . 149
21644	13 . 13 . 17 . 41 . 41 . 97
23488	29 . 37 . 53 . 89 . 109
24101	13 . 29 . 61 . 73 . 173
24358	17 . 29 . 41 . 149 . 197
25401	13 . 17 . 97 . 101 . 149
26707	29 . 29 . 37 . 73 . 157
30467	17 . 41 . 41 . 109 . 149
31226	17 . 53 . 61 . 113 . 157
33381	29 . 37 . 53 . 97 . 101
38011	13 . 41 . 89 . 97 . 157
38134	17 . 41 . 97 . 137 . 157
40559	13 . 17 . 17 . 37 . 61 . 97
41037	29 . 41 . 73 . 89 . 109
41891	17 . 37 . 73 . 97 . 197
44407	13 . 17 . 17 37 . 41 . 173
48062	13 . 17 . 53 . 53 . 61 . 61
49943	17 . 37 . 73 . 157 . 173
50051	13 . 17 . 173 . 181 . 181
56913	13 . 17 . 37 . 37 . 53 . 101
60347	13 . 17 . 29 . 29 . 97 . 101
68626	13 . 13 17 . 53 . 157 . 197
85699	37 . 61 89 . 101 . 181
87989	17 . 53 . 113 . 193 . 197
93469	13 . 13 . 13 . 17 . 29 . 37 . 109

95473	13 . 13 . 13 . 73 . 157 . 181
101151	37 . 41 . 101 . 173 . 193
108871	17 . 53 173 . 193 . 197
121479	17 . 17 . 29 . 41 . 109 . 197
141777	13 . 17 . 37 . 73 . 113 . 149
144808	13 . 41 . 61 . 61 . 97 . 109
152762	13 . 41 . 41 . 97 . 101 . 109
152803	13 . 29 . 37 . 41 . 137 . 149
155187	73 . 97 . 101 . 113 149
160314	29 . 37 41 . 61 . 61 . 157
172561	13 . 13 . 13 . 13 . 37 . 73 . 193
183971	17 . 37 . 41 . 73 . 89 . 101
188618	13 . 17 . 17 29 53 . 61 . 101
214482	29 . 37 . 53 . 61 . 89 . 149
214631	13 . 29 . 41 . 73 . 137 . 149
234852	17 . 41 . 53 . 73 . 113 . 181
249014	13 . 73 . 73 . 89 . 89 . 113
257841	13 . 29 . 61 . 89 . 101 . 149
279007	13 . 13 . 17 . 29 . 29 . 89 . 181
329219	17 . 37 . 73 . 89 . 89 . 149
329848	13 . 17 . 17 . 29 . 37 . 137 . 197
382537	13 . 17 . 17 . 29 . 61 . 101 . 109
422419	17 . 17 . 17 . 41 . 53 . 61 . 137
458742	17 . 17 . 113 . 173 . 193 . 193
484041	13 . 29 . 37 . 37 . 61 . 61 . 61
546534	13 . 13 . 37 . 41 . 41 . 157 . 181
564812	13 . 37 . 37 . 41 . 53 . 73 . 113
735331	13 . 13 . 37 . 41 . 53 . 101 197
743781	13 . 13 . 13 . 13 . 17 . 37 . 89 . 173
867847	17 . 89 . 89 . 137 . 137 . 149
938003	13 . 29 . 53 . 61 . 61 . 61 . 97
1000154	13 . 13 . 29 . 29 . 37 . 37 53 . 97.
1964806	13 . 13 . 17 . 29 . 41 . 73 . 113 . 137
2144583	13 . 41 . 53 . 61 . 73 . 101 . 181
3589859	17 . 17 . 73 . 109 . 113 . 137 . 181
3879591	13 . 37 . 53 . 89 . 113 . 149 . 197
5693622	13 . 13 . 13 . 53 . 97 . 101 . 157 . 181
6991009	13 17 . 17 . 37 . 53 . 113 . 149 . 197
7062082	13 . 29 . 29 . 41 . 53 . 73 . 149 193
8489259	13 . 17 . 29 . 29 . 29 . 41 . 41 . 41 . 97
8717008	13 . 13 17 . 17 . 37 . 37 . 89 . 113 . 113
9707868	13 . 29 . 29 . 37 . 101 . 113 . 137 . 149
10305788	13 . 17 . 37 . 53 101 . 109 . 113 . 197
17462342	13 . 37 . 61 . 61 . 89 . 89 . 137 157
38722306	13 . 13 . 29 . 37 . 61 . 89 . 89 . 109 . 157
48162204	13 . 17 . 37 . 37 . 41 . 53 . 101 . 181 . 193
60920523	13 . 17 . 17 . 53 . 61 . 61 . 101 . 137 . 181

63769026	17 . 29 . 37 . 41 . 53 . 89 . 101 . 101 . 113
111771087	13 . 17 . 37 . 61 . 61 . 89 . 113 . 137 . 149
141757784	13 . 17 . 53 . 61 . 89 . 113 . 137 . 137 . 149
172642653	13 . 17 . 29 . 73 . 89 . 89 . 137 . 149 . 197
190067607	73 . 89 . 97 . 101 . 101 . 109 . 149 . 173
308956283	13 . 29 . 29 . 37 . 41 . 53 . 61 . 73 . 89 . 137
569329071	13 . 13 . 29 . 37 . 41 . 97 . 101 . 109 . 137 . 149

13	1. 12
17	3. 14. 99
29	2. 27. 31
37	7. 118. 326. 636. 19751
41	4. 37. 201. 209. 2989. 3522
53	9. 44. 168. 309. 857. 5927
61	6. 67. 116. 311. 433. 677. 1104. 48062. 484041
73	11. 62. 157. 303. 1887. 19553
89	8. 81. 97. 259. 437. 898. 2128. 2751. 4814. 18771*
97	13. 84. 181. 207. 1442. 2341. 5251. 21644. 40559. 938203*. 1000154. 8489259
101	51. 252. 354. 1767. 6616. 33381. 56913. 60347. 183971. 188618*
109	53. 56. 274. 1364. 3323. 9209. 13787. 23488. 41037. 93469*. 144808. 152762. 382537
113	38. 151. 377. 414. 1431. 1544. 4219. 8776. 12468. 21319*. 249014. 564812. 8717008. 63769026
137	48. 89. 363. 733. 1733. 2144. 3199. 3788. 10049. 20502*. 422419. 1964806. 308956283
149	71. 78. 376. 816. 1561. 3654. 10061. 10501. 17057. 21527*. 25401. 30467. 14777. 152803. 155187. 214482. 214631. 257841. 329219. 867847*. 9707868. 111771087. 141757784. 569329071
157	17. 454. 488. 611. 768. 959. 3471. 7676. 18823. 26707*. 31226. 38011. 38134. 160314. 17462342. 38722306
173	54. 119. 227. 573. 1092. 2887. 6001. 13786. 14067. 24101*. 44407. 49943. 743781. 190067607
181	86. 638. 819. 5154. 5706. 8231. 14756. 50051. 85699. 95473*. 234852. 279007. 546534. 2144583. 3589859. 5693622. 60920523
193	19. 174. 753. 984. 1177. 3686. 4458. 6157. 6581. 12526*. 15807. 18123. 101151. 172561. 458742. 7062082. 48162204
197	127. 267. 324. 521. 858. 1252. 2434. 4264. 4798. 7359*. 7753. 8147. 21009. 24358. 41891. 68626. 87989. 108871. 121479. 329848*. 735331. 3879591. 6991009. 10305788. 172642653

Zerlegbare $aa + 36$.

1	37
5	61
7	5 . 17
11	157
13	5 . 41
17	5 . 5 . 13
23	5 . 113
35	13 . 97
41	17 . 101
43	5 . 13 . 29
61	13 . 17 . 17
67	5 . 5 . 181
73	5 . 29 . 37
85	53 . 137
89	73 . 109
95	13 . 17 . 41
113	5 . 13 . 197
115	89 . 149
127	5 . 53 . 61
191	13 . 53 . 53
203	5 . 73 . 113
217	5 . 5 . 5 . 13 . 29
233	5 . 5 . 41 . 53
293	5 . 89 . 193
295	13 . 37 . 181
307	5 . 109 . 173
347	5 . 13 . 17 . 109
445	37 . 53 . 101
479	29 . 41 . 193
517	5 . 5 . 17 . 17 . 37
565	29 . 101 . 109
617	5 . 5 . 97 . 157
667	5 . 5 . 13 . 37 . 37
673	5 . 17 . 73 . 73
737	5 . 13 . 61 . 137
763	5 . 13 . 13 . 13 . 53
953	5 . 13 . 89 . 157
971	13 . 29 . 41 . 61
1183	5 . 5 . 17 . 37 . 89
1333	5 . 5 . 17 . 37 . 113
1463	5 . 41 . 53 . 197
1517	5 . 5 . 13 . 73 . 97
1673	5 . 13 . 17 . 17 . 149
1717	5 . 5 . 5 . 5 . 53 . 89
1873	5 . 41 . 109 . 157

2201	13 . 41 . 61 . 149
2251	17 . 17 . 89 . 197
2383	5 . 5 . 13 . 101 . 173
2557	5 . 13 . 17 . 61 . 97
2567	5 . 5 . 29 . 61 . 149
2963	5 . 89 . 109 . 181
3181	13 . 37 . 109 . 193
3553	5 . 13 . 29 . 37 . 181
3767	5 . 5 . 17 . 173 . 193
4031	41 . 61 . 73 . 89
4277	5 . 17 . 29 . 41 . 181
4883	5 . 5 . 37 . 149 . 173
5009	13 . 97 . 101 . 197
5321	13 . 13 . 29 . 53 . 109
5467	5 . 5 . 5 . 5 . 17 . 29 . 97
5495	13 . 13 . 29 . 61 . 101
5497	5 . 173 . 181 . 193
6217	5 . 5 . 5 . 37 . 61 . 137
6221	29 . 73 . 101 . 181
6655	29 . 41 . 193 . 193
6827	5 . 17 . 61 . 89 . 101
7547	5 . 37 . 37 . 53 . 157
7717	5 . 5 . 5 . 53 . 89 . 101
7813	5 . 17 . 61 . 61 . 193
7861	13 . 17 . 137 . 157
7919	37 . 97 . 101 . 173
8459	13 . 17 . 41 . 53 . 149
10261	13 . 17 . 53 . 89 . 101
10565	13 . 13 . 41 . 89 . 181
13763	5 . 13 . 17 . 37 . 41 . 113
13823	5 . 13 . 109 . 149 181
14543	5 . 13 . 29 . 29 . 53 . 73
15245	13 . 37 . 61 . 89 . 89
15733	5 . 5 . 29 . 29 . 61 . 193
17617	5 . 5 . 29 . 41 . 53 . 197
18659	13 . 17 . 97 . 109 . 149
22345	17 . 29 . 53 . 97 . 197
22481	13 . 17 . 17 . 17 . 41 . 193
22583	5 . 5 . 17 . 101 . 109 . 109
22733	5 . 5 . 13 . 13 . 13 . 97 . 97
22867	5 . 5 29 . 37 . 101 . 193
23753	5 . 37 . 113 . 137 . 197
29129	13 . 53 . 89 . 101 . 137
29995	13 . 13 . 13 . 13 . 17 . 17 . 109
30845	13 . 13 . 17 . 41 . 41 . 197
31885	13 . 17 29 . 41 . 53 . 73
32647	5 . 13 . 17 . 73 . 73 . 181
38893	5 . 73 . 109 . 193 . 197

38923	5 . 17 . 37 . 53 . 61 . 149
39347	5 . 13 . 41 . 53 . 97 . 113
42133	5 . 5 . 17 . 17 . 17 . 97 . 149
44327	5 . 29 . 29 . 37 . 73 . 173
48967	5 . 5 . 5 . 13 . 17 . 29 . 41 . 73

49517	5 . 5 . 29 . 113 . 173 . 173
54167	5 . 5 . 13 . 13 . 37 . 137 . 137
61117	5 . 5 . 13 . 29 . 61 . 73 . 89
62825	13 . 17 . 37 . 41 . 61 . 193
74603	5 . 13 . 17 . 29 . 29 . 53 . 113
87217	5 . 5 . 5 . 17 . 17 . 29 . 53 . 137
96227	5 . 17 . 53 . 109 . 109 . 173
125909	13 . 17 . 61 . 73 . 89 . 181
130613	5 . 41 . 53 . 73 . 137 . 157
141709	13 . 13 . 29 . 37 . 37 . 41 . 73
151163	5 . 29 . 61 . 109 . 137 . 173
161035	13 . 41 . 53 . 61 . 101 . 149
171655	89 . 97 . 109 . 173 . 181
174565	29 . 37 . 37 . 41 . 97 . 193
182743	5 . 17 . 29 . 29 . 29 . 89 . 181
189353	5 . 17 . 109 . 157 . 157 . 157
191203	5 . 53 . 53 . 73 . 181 . 197
206407	5 . 17 . 17 . 29 . 41 . 137 . 181
256693	5 . 17 . 17 . 29 . 61 . 149 . 173
387833	5 . 13 . 37 . 53 . 53 . 61 . 73
427795	13 . 17 . 37 . 37 . 53 . 101 . 113
429347	5 . 13 . 13 . 37 . 173 . 173 . 197
449921	13 . 29 . 37 . 41 . 41 . 89 . 97
533789	13 . 13 . 29 . 29 . 113 . 113 . 157
726029	17 . 17 . 29 . 29 . 101 . 109 . 197
837533	5 . 5 . 5 . 37 . 97 . 101 . 113 . 137
1097105	13 . 17 . 17 . 97 . 109 . 157 . 193
1396529	13 . 13 . 13 . 37 . 41 . 53 . 61 . 181
2390717	5 . 5 . 5 . 13 . 17 . 29 . 29 . 37 . 61 . 109
2525527	5 . 13 . 17 . 61 . 89 97 . 97 . 113
5318933	5 . 5 . 13 . 17 . 29 . 89 . 97 . 113 . 181
6920333	5 . 5 . 13 . 17 . 17 . 17 . 37 . 61 . 97 . 137
9439957	5 . 17 . 17 . 17 . 17 . 17 . 37 . 37 . 53 . 173
11776417	5 . 5 . 17 . 41 . 73 . 73 . 89 . 97 . 173
45435967	5 . 5 . 5 . 29 . 41 . 53 . 61 . 113 . 193 . 197
70145903	5 . 13 . 13 . 17 . 41 . 53 . 73 . 97 . 113 . 197
90115783	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 13 . 17 . 61 . 73
716295433	5 . 5 . 13 . 13 . 29 . 29 . 37 . 41 . 61 . 89 89 . 197
2009136133	5 . 5 . 13 . 17 . 41 . 61 . 73 . 89 . 97 . 113 . 181 . 197

5	.
13	17
17	7. 61
29	43. 217
37	1. 73. 517. 667
41	13. 95
53	191. 233. 763
61	5. 127. 971
73	673. 14543. 31885. 48967. 141709. 387833. 90115783
89	1183. 1717. 4031. 15245. 61117
97	35. 1517. 2557. 5467. 22733. 449921
101	41. 445. 5495. 6827. 7717. 10261
109	89. 347. 565. 5321. 22583. 29995. 2390717
113	23. 203. 1333. 13763. 39347. 74603. 427795. 2525527
137	85. 737. 6217. 29129. 54167. 87217. 837533. 6920333
149	115. 1673. 2201. 2567. 8459. 18659. 38923. 42133. 161035
157	11. 617. 953. 1873. 7547. 7861. 130613. 189353. 533789
173	307. 2383. 4883. 7919. 44327. 49517. 96227. 151163. 256693. 9439957*. 11776417
181	67. 295. 2963. 3553. 4277. 6221. 10565. 13823. 32647. 125909*. 171655. 182743. 206407. 1396529. 5318933
193	293. 479. 3181. 3767. 5497. 6655. 7813. 15733. 22481. 22867*. 62825. 174565. 1097105
197	113. 1463. 2251. 5009. 17617 22345. 23753. 30845. 38893. 191203*. 429347. 726029. 45435967. 70145903. 716295433. 2009136133

Zerlegbare $aa + 49$**.**

1	5 . 5
2	53
3	29
4	5 . 13
5	37
6	5 . 17
8	113
9	5 . 13
10	149
11	5 . 17
12	193
13	109
15	137
16	5 . 61
17	13 . 13
19	5 . 41
22	13 . 41

23	17 . 17
24	5 . 5 . 5 . 5
26	5 . 5 . 29
29	5 . 89
30	13 . 73
31	5 . 101
32	29 . 37
39	5 . 157
40	17 . 97
41	5 . 173
43	13 . 73
45	17 . 61
48	13 . 181
51	5 . 5 . 53
55	29 . 53
57	17 . 97
60	41 . 89
61	5 . 13 . 29
69	5 . 13 . 37
74	5 . 5 . 13 . 17
79	5 . 17 . 37
96	5 . 17 . 109
99	5 . 5 . 197
101	5 . 5 . 5 . 41
103	73 . 73
104	5 . 41 . 53
106	5 . 37 . 61
108	13 . 17 . 53
113	13 . 17 . 29
116	5 . 37 . 73
118	89 . 157
121	5 . 13 . 113
122	109 . 137
132	101 . 173
137	97 . 97
139	5 . 13 . 149
142	17 . 29 . 41
149	5 . 5 . 5 . 89
152	13 . 13 . 137
159	5 . 17 . 149
171	5 . 29 . 101
176	5 . 5 . 17 . 73
181	5 . 17 . 193
186	5 . 13 . 13 . 41
199	5 . 5 . 13 . 61
205	109 . 193
214	5 . 53 . 173
227	17 . 37 . 41

229	5 . 29 . 181
234	5 . 97 . 113
249	5 . 5 . 17 . 73
251	5 . 5 . 13 . 97
264	5 . 13 . 29 . 37
289	5 . 61 . 137
295	13 . 17 . 197
296	5 . 89 . 197
314	5 . 109 . 181
316	5 . 13 . 29 . 53
321	5 . 13 . 13 . 61
331	5 . 97 . 113
334	5 . 13 . 17 . 101
347	13 . 41 . 113
351	5 . 5 . 5 . 17 . 29
373	13 . 53 . 101
374	5 . 5 . 29 . 193
449	5 . 5 . 37 . 109
474	5 . 5 . 89 . 101
533	17 . 61 . 137
550	13 . 17 . 37 . 37
554	5 . 29 . 29 . 73
555	13 . 17 . 17 . 41
589	5 . 13 . 17 . 157
591	5 . 181 . 193
594	5 . 13 . 61 . 89
601	5 . 5 . 5 . 5 . 17 . 17
606	5 . 17 . 29 . 149
634	5 . 37 . 41 . 53
641	5 . 13 . 29 . 109
667	13 . 109 . 157
676	5 . 5 . 101 . 181
691	5 . 17 . 53 . 53
719	5 . 13 . 41 . 97
776	5 . 5 . 13 . 17 . 109
799	5 . 5 . 113 . 113
809	5 . 29 . 37 . 61
824	5 . 5 . 157 . 173
839	5 . 17 . 41 . 101
844	5 . 17 . 17 . 17 . 29
899	5 . 5 . 5 . 53 . 61
906	5 . 13 . 73 . 173
919	5 . 13 . 73 . 89
979	5 . 13 . 73 . 101
992	13 . 17 . 61 . 73
1009	5 . 17 . 53 . 113
1031	5 . 13 . 13 . 17 . 37
1041	5 . 29 . 37 . 101

1111	5 . 17 . 53 . 137
1128	17 . 29 . 29 . 89
1179	5 . 13 . 17 . 17 37
1186	5 . 29 . 89 . 109
1221	5 . 29 . 53 . 97
1252	13 . 17 . 41 . 173
1364	5 . 37 . 89 . 113

1374	5 . 5 . 13 . 37 . 157
1395	13 . 29 . 29 . 89
1556	5 . 13 . 193 . 193
1592	17 . 29 . 53 . 97
1609	5 . 17 . 97 . 157
1621	5 . 13 . 17 . 29 . 41
1629	5 . 13 137 . 149
1649	5 . 5 . 5 . 73 . 149
1689	5 . 17 . 97 . 173
1751	5 . 5 . 13 53 . 89
1766	5 . 29 . 137 . 157
1929	5 . 37 89 . 113
1949	5 5 . 17 . 41 . 109
2069	5 . 41 . 53 . 197
2076	5 . 5 . 13 . 89 . 149
2151	5 5 . 37 . 41 . 61
2374	5 . 5 . 17 . 89 . 149
2381	5 . 29 . 113 . 173
2521	5 37 . 89 . 193
2578	13 . 17 . 17 . 29 . 61
2595	17 . 37 . 53 101
2607	17 . 29 . 61 . 113
2659	5 . 37 . 97 . 197
2817	13 . 37 . 73 . 113
2851	5 5 . 5 . 13 41 . 61
2930	17 . 41 . 109 . 113
2944	5 61 . 157 . 181
2999	5 . 5 . 13 . 101 . 137
3100	17 . 29 101 . 193
3156	5 . 17 . 17 . 61 . 113
3251	5 5 . 29 . 37 . 197
3501	5 . 5 . 13 . 109 . 173
3547	17 . 37 . 73 . 137
3709	5 . 13 . 29 . 41 . 89
3753	13 . 41 . 73 . 181
4034	5 . 13 . 29 . 89 . 97
4065	13 . 37 . 89 . 193
4211	5 . 97 . 101 . 181
4286	5 . 13 . 41 . 61 . 113

4324	5 . 5 . 17 . 29 . 37 . 41
4399	5 . 5 . 5 . 5 . 113 . 137
4556	5 . 29 37 . 53 . 73
4629	5 . 73 . 149 . 197
4630	17 . 37 . 173 197
4657	37 . 37 . 89 . 89
4715	13 . 13 . 17 . 53 . 73
4749	5 . 5 . 13 . 13 . 17 . 157
4754	5 . 13 . 17 . 113 . 181
4778	37 . 41 . 101 . 149
4918	13 . 13 . 13 . 101 . 109
4927	29 . 53 . 53 . 149
5024	5 . 5 . 5 . 5 . 41 . 197
5101	5 . 5 . 5 . 29 . 37 . 97
5191	5 . 13 . 17 . 89 . 137
5221	5 . 101 . 137 . 197
5226	5 . 5 . 5 . 41 . 73 . 73
5841	5 . 13 . 37 . 41 . 173
6008	41 . 41 . 109 . 197
6029	5 . 17 . 29 . 73 . 101
6309	5 . 13 . 53 . 53 . 109
6381	5 . 17 . 17 . 73 . 193
6574	5 . 5 . 13 13 . 53 . 193
6899	5 5 . 5 . 5 . 13 . 29 . 101
6998	13 . 17 . 37 . 53 . 113
7276	5 . 5 . 13 . 29 . 41 . 137
7316	5 . 17 . 53 . 109 . 109
7440	13 . 17 . 41 . 41 . 149
7914	5 . 29 . 61 . 73 97
8149	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 17
8219	5 . 37 . 41 . 61 . 73
8251	5 . 5 . 13 . 17 . 61 . 101
8515	37 . 89 . 101 . 109
8753	13 . 137 137 . 157
8919	5 . 17 . 41 . 101 . 113
9161	5 . 13 . 29 . 113 . 197
9301	5 . 5 . 73 . 137 . 173
9546	5 . 13 . 97 . 97 . 149
9616	5 . 13 . 13 . 17 . 41 . 157
9837	13 . 17 . 37 . 61 . 97
9993	13 149 149 . 173
10291	5 . 17 . 37 . 113 . 149
10630	13 . 13 . 61 . 97 . 113
10651	5 . 5 . 13 . 37 . 53 . 89
10727	29 . 97 . 113 . 181
10761	5 . 41 . 53 . 73 . 73
10887	41 . 89 . 109 . 149
11185	53 . 89 . 89 . 149

11632	29 . 149 . 173 . 181
12151	5 . 5 . 13 . 13 . 101 . 173
12489	5 . 13 . 13 . 17 . 61 . 89
13101	5 . 5 . 5 . 5 . 17 . 41 . 197
13329	5 . 13 . 73 . 97 . 113
14351	5 . 5 . 5 . 5 . 37 61 . 73
14656	5 . 41 . 61 . 89 . 193
14811	5 . 13 . 109 . 113 . 137
15356	5 41 . 61 . 109 . 173
15425	17 . 29 . 29 . 53 . 157
15661	5 . 13 . 61 . 157 . 197
16393	61 . 101 . 113 193
16446	5 . 29 . 109 . 109 157
17247	13 . 37 37 . 61 137
18099	5 . 5 . 17 . 29 . 97 . 137
18976	5 . 5 . 5 . 13 . 37 . 53 . 113
19743	13 . 17 . 41 . 137 . 157
20297	13 . 13 . 13 . 29 . 53 . 61
20999	5 . 13 . 29 . 149 . 157
21768	97 . 137 . 181 . 197
21834	5 . 17 . 29 . 41 . 53 . 89
22156	5 . 13 . 13 . 53 . 97 . 113
22569	5 . 41 . 41 . 157 . 193
25726	5 . 5 . 5 . 29 . 41 . 61 . 73.
25931	5 . 13 . 17 . 41 . 41 . 181
26016	5 . 17 . 29 . 37 . 41 . 181
26337	113 . 113 . 157 . 173
27200	13 . 37 . 97 . 101 . 157
27564	5 . 13 . 13 . 73 . 109 . 113
27721	5 . 17 . 17 . 29 . 53 . 173
29254	5 . 13 . 13 . 53 . 97 . 197
29501	5 . 5 . 13 . 17 . 17 . 41 . 113
30179	5 . 61 . 73 . 113 . 181.
30424	5 . 5 . 13 . 17 . 29 . 53 . 109
31274	5 . 5 . 5 . 5 . 13 . 17 . 73 . 97
32491	5 . 13 . 37 . 41 . 53 . 101
33258	13 . 17 . 17 . 37 . 73 . 109
34134	5 . 13 . 41 . 53 . 73 . 113
35303	17 . 37 . 61 . 109 . 149
35361	5 . 41 . 113 . 137 . 197
35524	5 . 5 . 5 . 17 . 17 . 181 . 193
36149	5 . 5 . 5 . 13 . 13 . 157 . 197
37409	5 . 61 . 89 . 149 . 173
37836	5 . 17 . 17 . 61 . 109 . 149
38601	5 . 5 . 5 . 13 . 17 . 149 . 181
39901	5 . 5 . 13 . 13 . 29 . 73 . 89
41801	5 . 5 . 41 . 61 . 89 . 157
41859	5 . 73 . 89 . 149 . 181

43416	5 . 13 . 13 . 13 . 29 . 61 . 97
44677	13 . 53 . 97 . 109 . 137
44976	5 . 5 . 5 . 5 . 5 13 . 17 . 29 . 101
46229	5 . 17 . 29 . 41 . 97 . 109
48317	13 . 13 . 29 . 37 . 41 . 157
49099	5 . 5 . 41 . 73 . 89 . 181
50632	17 . 73 . 101 . 113 . 181
51176	5 . 5 . 17 . 17 . 37 . 97 . 101
54274	5 . 5 . 5 . 37 . 53 . 61 . 197
55774	5 . 5 . 5 . 13 . 89 . 137 . 157
58881	5 . 13 . 53 . 61 . 73 . 113
64051	5 . 5 . 73 . 73 . 89 . 173
64644	5 . 29 . 37 . 61 . 113 . 113
67785	17 . 53 . 109 . 149 . 157
69983	13 . 13 . 17 . 61 . 89 . 157
72851	5 . 5 . 5 . 17 . 17 . 17 . 29 . 149
73043	13 . 17 . 37 . 41 . 73 . 109
73672	17 . 17 . 37 . 53 . 61 . 157
73721	5 . 29 . 29 53 . 89 137
76534	5 . 29 . 53 . 53 . 197
80841	5 . 17 . 61 . 73 . 89 . 97
82307	13 . 53 . 157 . 173 . 181
83430	13 . 17 . 29 . 37 . 149 197
87369	5 . 13 . 17 . 89 . 197 . 197
88213	37 . 41 . 97 . 137 . 193
88406	5 . 17 . 53 . 89 . 101 . 193
88989	5 . 13 . 17 . 17 . 41 . 53 . 97
89149	5 . 5 . 5 . 29 . 89 . 109 . 113
92049	5 . 5 . 13 . 17 . 29 . 137 . 193
102735	13 . 13 . 13 . 89 . 137 . 197
124029	5 . 13 . 13 . 37 . 37 . 61 . 109
131863	13 . 17 . 37 . 97 . 97 . 113
133149	5 . 5 . 5 . 5 . 5 . 41 101 . 137
138199	5 . 5 . 13 . 17 . 101 . 109 . 157
139551	5 . 5 . 13 . 29 . 53 . 101 . 193
141633	17 . 17 . 17 . 17 . 29 . 41 . 101
148439	5 . 37 . 41 . 73 101 . 197
150410	17 . 37 . 41 . 61 . 73 . 197
150681	5 . 29 . 53 . 97 . 97 . 157
154876	5 . 5 . 17 . 41 . 73 . 109 . 173
157995	29 . 37 . 41 . 53 . 53 . 101
160168	17 . 37 . 41 . 53 . 137 . 137
163609	5 . 13 . 13 . 37 . 41 . 53 . 137
166851	5 . 5 . 5 . 5 . 5 . 13 . 41 . 61 . 137
167124	5 . 5 . 13 . 13 . 29 . 37 . 61 . 101
174074	5 . 5 . 13 . 17 . 157 . 181 . 193
178149	5 . 5 . 5 . 5 . 17 . 89 . 97 . 173
179565	13 . 17 . 29 . 113 . 113 . 197

187249	5 . 5 . 17 . 17 . 109 . 113 . 197
189538	73 . 109 . 149 . 157 . 193
207814	5 . 13 . 17 . 17 . 97 . 137 . 173
213263	29 . 37 . 41 . 73 . 73 . 97
217351	5 . 5 . 5 . 13 . 13 . 17 . 17 . 53 . 73
231755	13 . 17 . 17 . 17 . 61 . 61 . 113
273694	5 . 17 . 37 . 41 . 53 . 97 . 113
281226	5 . 5 . 5 . 5 . 61 . 73 . 157 . 181
288901	5 . 5 . 29 . 37 . 53 . 149 . 197
299399	5 . 5 . 5 . 5 . 13 . 29 . 37 . 53 . 97
307519	5 . 13 . 17 . 17 . 29 . 29 . 41 . 73
343066	5 . 13 . 17 . 17 . 17 . 41 . 89 . 101
345094	5 . 13 17 . 37 . 113 . 149 . 173
361409	5 . 13 . 17 . 53 . 61 . 101 . 181
375967	5 . 17 . 37 . 53 . 61 . 149
401444	5 . 13 . 17 . 17 . 29 . 29 . 101 . 101
408628	41 . 53 . 89 . 89 . 89 . 109
415848	13 . 17 . 17 . 37 . 101 . 109 . 113
417317	13 . 41 . 61 . 113 . 137 . 173
428021	5 . 13 . 37 . 41 . 61 . 97 . 157
448976	5 . 5 . 5 . 17 . 61 . 89 . 101 . 173
462953	29 . 41 . 53 . 101 . 113 . 149
521044	5 . 13 . 13 . 17 . 17 . 73 . 97 . 157
527329	5 . 17 . 37 . 61 . 61 . 109 . 109
658576	5 . 5 . 13 . 13 . 13 . 13 . 53 . 73 . 157
689601	5 . 5 . 5 . 37 . 41 . 73 . 89 . 193
788493	13 . 41 . 109 . 157 . 173 . 197
935601	5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 29 . 41 . 41
979976	5 . 5 . 5 . 5 . 17 . 17 . 137 . 197 197
1055864	5 . 13 . 17 . 29 . 37 . 53 . 113 . 157

1538221	5 . 13 . 13 . 29 . 53 . 61 . 109 . 137
1686759	5 . 13 . 29 . 29 . 41 . 41 . 113 . 137
2001229	5 . 13 . 17 . 29 . 41 . 53 . 149 . 193
2446492	13 . 41 . 73 . 89 . 101 . 109 . 157
3254151	5 . 5 . 13 . 17 . 29 . 41 . 61 . 73 . 181
3297075	37 . 41 . 53 . 53 . 73 . 101 . 173
3643774	5 . 5 . 5 . 13 . 17 . 41 . 109 . 137 . 157
4515359	5 . 13 . 13 . 13 . 17 . 17 . 113 . 157 . 181
5307581	5 . 17 . 37 . 53 . 73 . 73 . 101 . 157
5456999	5 . 5 . 41 . 73 . 73 . 101 . 137 . 197
7936717	13 . 29 . 37 . 41 . 41 . 41 . 181 . 181
8555207	13 . 17 . 41 . 53 61 . 73 . 109 . 157
12448726	5 . 5 5 . 5 . 13 . 13 . 13 . 41 . 89 . 157 . 197
21432319	5 . 17 . 37 . 73 . 149 . 173 . 197 . 197
40407039	5 . 17 . 37 . 41 . 53 . 89 . 97 . 101 . 137
41719774	5 . 5 . 5 . 17 . 17 . 29 . 29 . 41 . 41 . 173 . 197

118135085 | 17 17 . 37 . 41 . 61 . 101 . 109 . 137 . 173

5	1. 24
13	4. 9. 17
17	6. 11. 23. 74. 601. 8149
29	3. 26. 61. 113. 351. 844
37	5. 32. 69. 79. 264. 550. 1031. 1179
41	19. 22. 101. 142. 186. 227. 555. 1621. 4324. 935601*
53	2. 51. 55. 104. 108. 316. 634. 691
61	16. 45. 106. 199. 321. 809. 899. 2151. 2578. 2851*. 20297
73	30. 43. 103. 116. 176. 249. 554. 992. 4556. 4715*. 5226. 8219. 10761. 14351. 25726. 217351. 307519
89	29. 60. 149. 594. 919. 1128. 1395. 1751. 3709. 4657*. 10651. 12489. 21834. 39901
97	40. 57. 137. 251. 719. 1221. 1592. 4034. 5101. 7914*. 9837. 31274. 43416. 80841. 88989. 213263. 299399
101	31. 171. 334. 373. 474. 839. 979. 1041. 2595. 6029*. 6899. 8251. 32491. 44976. 51176. 141633. 157995. 167124. 343066. 401444*
109	13. 96. 449. 641. 776. 1186. 1949. 4918. 6309. 7316*. 8515. 30424. 33258. 46229. 73043. 124029. 408628. 527329
113	8. 121. 234. 331. 347. 799. 1009. 1364. 1929. 2607*. 2817. 2930. 3156. 4286. 6998. 8919. 10630. 13329. 18976. 22156. 27564*. 29501. 34134. 58881. 64644. 89149. 131863. 231755. 273694. 415848
137	15. 122. 152. 289. 533. 1111. 2999. 3547. 4399. 5191*. 7276. 14811. 17247. 18099. 44677. 73721. 133149. 160168. 163609. 166851*. 1538221. 1686759. 40407039
149	10. 139. 159. 606. 1629. 1649. 2076. 2374. 4778. 4927*. 7440. 9546. 10291. 10887. 11185. 35303. 37836. 72851. 375967. 462953*
157	39. 118. 589. 667. 1374. 1609. 1766. 4749. 8753. 9616*. 15425. 16446. 19743. 20999. 27200. 41801. 48317. 55774. 67785. 69983*. 73672. 138199. 150681. 428021. 521044. 658576. 1055864. 2446492. 3643774. 5307581*. 8555207
173	41. 132. 214. 824. 906. 1252. 1689. 2381. 3501. 5841*. 9301. 9993. 12151. 15356. 26337. 27721. 37409. 64051. 154876. 178149*. 207814. 345094. 417317. 448976. 3297075. 118135085
181	48. 229. 314. 676. 2944. 3753. 4211. 4754. 10727. 11632*. 25931. 26016. 30179. 38601. 41859. 49099. 50632. 82307. 281226. 361409*. 3254151. 4515359. 7936717
193	12. 181. 205. 374. 591. 1556. 2521. 3100. 4065. 6381*. 6574. 14656. 16393. 22569. 35524. 88213. 88406. 92049. 139551*. 174074. 189538. 689601. 2001229
197	99. 295. 296. 2069. 2659. 3251. 4629. 4630. 5024. 5221*. 6008. 9161. 13101. 15661. 21768. 29254. 35361. 36149. 54274. 76534*. 83430. 87369. 102735. 148439. 150410. 179565. 187249. 288901. 788493. 979976*. 5456999. 12448726. 21432319. 41719774

Zerlegbare $aa + 64$.

1	5 . 13
3	73
5	89
7	113
9	5 . 29
11	5 . 37
15	17 . 17
19	5 . 5 . 17
21	5 . 101
25	13 . 53
27	13 . 61
29	5 . 181
31	5 . 5 . 41
49	5 . 17 . 29
51	5 . 13 . 41
53	13 . 13 . 17
63	37 . 109
67	29 . 157
69	5, 5 . 193
79	5 . 13 . 97
81	5 . 5 . 5 . 53
85	37 . 197
95	61 . 149
115	97 . 137
121	5 . 17 . 173
131	5 . 5 . 13 . 53
149	5 . 61 . 73
155	13 . 17 . 109
159	5 . 37 . 137
181	5 . 5 . 13 . 101
183	13 . 29 . 89
219	5 . 5 . 17 . 113
223	17 . 29 . 101
233	5 . 37 . 113
281	5 . 5 . 29 . 109
309	5 . 97 . 197
339	5 . 13 . 29 . 61
359	5 . 17 . 37 . 41
381	5 . 5 . 37 . 157
389	5 . 13 . 17 . 137
391	5 . 13 . 13 . 181
393	17 . 61 . 149
433	37 . 37 . 137
441	5 . 13 . 41 . 73
455	29 . 37 . 193

461	5 . 17 . 41 . 61
467	13 . 97 . 173
529	5 . 17 . 37 . 89
571	5 . 13 . 29 . 173
581	5 . 5 . 5 . 37 . 73
661	5 . 17 . 53 . 97
703	13 . 193 . 197
707	41 . 89 . 137
717	53 . 89 . 109
729	5 . 13 . 13 . 17 . 37
831	5 . 5 . 5 . 5 . 5 . 13 . 17
873	53 . 73 . 197
879	5 . 29 . 73 . 73

911	5 . 13 . 113 . 113
937	13 . 17 . 29 . 137
989	5 . 13 . 101 . 149
1035	17 . 29 . 41 . 53
1097	41 . 149 . 197
1141	5 . 17 . 17 . 17 . 53
1169	5 . 5 . 5 . 13 . 29 . 29
1171	5 . 13 . 17 . 17 . 73
1191	5 . 53 . 53 . 101
1247	13 . 37 . 53 . 61
1343	29 . 37 . 41 . 41
1419	5 . 5 . 5 . 89 . 181
1491	5 . 37 . 61 . 197
1589	5 . 41 . 109 . 113
1609	5 . 41 . 73 . 173
1613	13 . 17 . 61 . 193
1637	13 13 . 101 . 157
1681	5 . 5 . 17 . 61 . 109
1691	5 . 13 . 29 . 37 . 41
1749	5 . 17 . 17 . 29 . 73
1839	5 . 37 . 101 . 181
1861	5 . 37 . 97 . 193
1999	5 . 41 . 101 . 193
2019	5 . 5 . 41 . 41 . 97
2041	5 . 73 . 101 . 113
2055	13 . 17 . 97 . 197
2081	5 . 5 . 5 . 5 . 13 . 13 41
2131	5 . 5 . 13 . 89 . 157
2201	5 . 53 . 101 . 181
2445	13 . 29 . 101 . 157
2479	5 . 73 . 113 . 149
2601	5 . 13 . 29 . 37 . 97
2625	5 . 13 . 53 . 73 . 137

2771	5 . 73 . 109 . 193
2989	5 . 13 . 13 . 97 . 109
3171	5 . 13 . 37 . 37 . 113
3199	5 . 13 . 29 . 61 . 89
3413	29 . 41 . 97 . 101
3721	5 . 17 . 29 . 41 . 137
4031	5 . 5 . 13 . 17 . 17 . 173
4061	5 . 17 . 17 . 101 . 113
4109	5 . 13 . 13 . 13 . 29 . 53
4315	13 41 . 181 . 193
4419	5 . 5 . 5 . 13 . 61 . 197
4541	5 . 17 . 41 . 61 . 97
4979	5 . 29 . 37 . 97 . 157
5097	13 . 61 . 181 . 181
5169	5 . 5 . 5 . 37 . 53 . 109
5381	5 . 5 . 13 . 41 . 41 . 53
5459	5 . 13 . 17 . 149 . 181
5761	5 . 17 . 37 . 61 . 173
5869	5 . 5 . 89 . 113 . 137
6081	5 . 5 . 5 . 29 . 101 . 101
7781	5 . 5 . 29 . 37 . 37 . 61
9039	5 . 29 . 37 . 97 . 157
9779	5 . 37 . 73 . 73 . 97
10519	5 . 37 . 37 . 53 . 61
10527	41 . 109 . 137 . 181
10831	5 . 5 . 5 . 5 . 17 . 61 . 181
11511	5 . 17 . 41 . 193 . 197
13331	5 . 5 . 5 . 5 . 5 . 29 . 37 . 53
13581	5 . 5 . 5 . 17 . 29 41 . 73
13889	5 . 41 . 89 . 97 . 109
13911	5 . 13 . 13 . 29 . 53 . 149
14451	5 . 29 . 73 . 109 . 181
16069	5 . 5 . 13 . 37 . 109 . 197
16985	17 . 29 . 53 . 61 . 181
17421	5 . 13 . 137 . 173 . 197
18511	5 . 13 . 17 . 17 . 17 . 29 . 37
18563	13 . 37 . 41 . 101 . 173
18685	17 . 29 . 73 . 89 . 109
24061	5 . 29 . 29 . 37 . 61 . 61
24261	5 . 17 . 17 . 37 . 101 . 109
27665	13 37 . 41 . 197 . 197
29019	5 . 5 . 37 . 53 . 89 . 193
29981	5 . 5 . 37 . 41 . 137 . 173
31669	5 . 5 . 5 . 5 . 13 . 17 . 53 . 137
58397	13 . 17 . 29 . 37 . 73 . 197
59279	5 . 13 . 53 . 73 . 89 . 157
88789	5 . 13 17 . 29 . 37 . 61 . 109
103481	5 . 5 . 13 . 13 . 17 . 29 . 53 . 97

132081	5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 89 . 193
170529	5 . 17 . 29 . 41 . 53 . 61 . 89
213331	5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 37 . 137
383229	5 . 17 . 17 . 61 . 89 . 97 . 193
728391	5 . 13 . 73 . 97 . 101 . 101 . 113
1934581	5 . 5 . 5 . 5 . 13 . 17 . 17 . 17 . 29 . 53 . 61
2446081	5 . 5 . 5 . 13 . 17 . 17 . 37 . 53 . 73 . 89
4056181	5 . 5 . 13 . 17 . 29 . 41 . 101 . 137 . 181
5106581	5 . 5 . 5 . 13 . 17 . 37 . 41 . 61 . 101 . 101
14836119	5 . 5 . 13 . 13 . 17 . 17 . 17 . 17 . 29 . 137 . 157

13	1
17	15. 19. 53. 831
29	9. 49. 1169
37	11. 729. 18511
41	31. 51. 359. 1343. 1691. 2081
53	25. 81. 131. 1035. 1141. 4109. 5381. 13331
61	27. 339. 461. 1247. 7781. 10519. 24061. 1934581
73	3. 149. 441. 581. 879. 1171. 1749. 13581
89	5. 183. 529. 3199. 170529. 2446081
97	79.661. 2019. 2601. 4541. 9779. 103481
101	21. 181. 223. 1191. 3413. 6081. 5106581
109	63. 155. 281. 717. 1681. 2989. 5169. 13889. 18685. 24261*. 88789
113	7. 219. 233. 911. 1589. 2041. 3171. 4061. 728391
137	115. 159. 389. 433. 707. 937. 2625. 3721. 5869. 31669*. 213331
149	95. 393. 989. 2479. 13911
157	67. 381. 1637. 2131. 2445. 4979. 9039. 59279. 1483619
173	121. 467. 571. 1609. 4031. 5761. 18563. 29981
181	29. 391. 1419. 1839. 2201. 5097. 5459. 10527. 10831. 14451*. 16985. 4056181
193	69. 455. 1613. 1861. 1999. 2771. 4315. 29019. 132081. 383229
197	85. 309. 703. 873. 1097. 1491. 2055. 4419. 11511. 16069*. 17421. 27665. 58397

Zerlegbare $aa + 81$**.**

1	41
2	5 . 17
4	97
5	53
7	5 . 13
8	5 . 29
10	181
11	101
13	5 . 5 . 5
17	5 . 37

19	13 . 17
20	13 . 37
22	5 . 113
23	5 . 61
28	5 . 173
32	5 . 13 . 17
37	5 . 5 . 29
38	5 . 5 61
40	41 . 41
43	5 . 193
49	17 . 73
50	29 . 89
53	5 . 17 . 17
58	5 . 13 . 53
59	13 . 137
62	5 . 5 . 157
71	13 . 197
79	29 . 109
83	5 . 17 . 41
91	37 . 113
95	29 . 157
97	5 · 13 . 73
98	5 . 13 . 149
101	53 . 97
112	5 . 5 . 5 . 101
122	5 . 41 . 73
124	13 . 29 . 41
128	5 . 37 . 89
137	5 . 5 . 13 . 29
139	89 . 109
163	5 . 5 . 13 . 41
188	5 . 5 . 13 . 109
191	101 . 181
202	5 . 13 . 17 . 37
215	13 . 13 . 137
217	5 . 53 . 89
247	5 . 41 . 149
248	5 . 109 . 113
253	5 . 13 . 17 . 29
268	5 . 73 . 197
287	5 . 5 . 17 . 97
292	5 . 13 . 13 . 101
313	5 . 5 . 37 . 53
317	5 . 89 . 113
323	5 . 53 . 197
352	5 . 137 . 181
376	17 . 53 . 157
389	17 . 61 . 73

406	17 . 89 . 109
409	13 . 41 . 157
427	5 . 17 . 29 . 37
461	13 . 13 . 17 . 37
472	5 . 29 . 29 . 53
487	5 . 5 . 5 . 13 . 73
491	17 . 41 . 173
533	5 . 157 . 181
547	5 . 173 . 173
553	5 . 13 . 13 . 181
566	13 . 157 . 157
575	37 . 41 . 109
578	5 . 13 . 53 . 97
587	5 . 5 . 61 . 113
617	5 . 13 . 29 . 101
631	13 . 17 . 17 . 53
662	5 . 5 . 89 . 197
683	5 . 13 . 37 . 97
694	53 . 61 . 149
733	5 . 17 . 29 . 109
737	5 . 5 . 5 . 41 . 53
763	5 . 5 . 5 . 17 . 137
797	5 . 17 . 37 . 101
862	5 . 5 . 5 . 5 . 29 . 41
877	5 . 13 . 61 . 97
920	17 . 17 . 29 . 101
1018	5 . 17 . 89 . 137
1037	5 . 5 . 137 . 157
1060	13 . 13 . 61 . 109
1108	5 . 41 . 53 . 113
1118	5 . 53 . 53 . 89
1168	5 . 29 . 97 . 97
1201	37 . 101 . 193
1229	13 . 13 . 41 . 109
1243	5 . 17 . 61 . 149
1265	73 . 97 . 113
1277	5 . 17 . 53 . 181
1313	5 . 5 . 29 . 29 . 41
1436	13 . 41 . 53 . 73
1447	5 . 17 . 109 . 113
1463	5 . 5 . 13 . 37 . 89
1475	13 . 13 . 41 . 157
1487	5 . 5 . 5 . 5 . 29 . 61
1585	53 . 137 . 173
1639	41 . 181 . 181
1645	13 . 29 . 37 . 97
1685	17 . 37 . 37 . 61
1702	5 . 17 . 173 . 197

1703	5 . 29 . 73 . 137
1787	5 . 5 . 13 . 17 . 17 . 17
1807	5 . 53 . 61 . 101
2008	5 . 13 . 17 . 41 . 89
2009	13 . 29 . 53 . 101
2041	97 . 109 . 197
2051	29 . 29 . 41 . 61
2125	13 . 29 . 53 . 113
2138	5 . 5 . 5 . 13 . 29 . 97
2293	5 . 17 . 157 . 197
2312	5 . 5 . 29 . 73 . 101
2450	13 . 17 . 157 . 173
2531	17 . 29 . 73 . 89
2623	5 . 41 . 97 . 173
2705	17 . 29 . 41 . 181
2888	5 . 5 . 5 . 5 . 5 . 17 . 157
2906	13 . 37 . 97 . 181
3088	5 . 5 . 13 . 13 . 37 . 61
3238	5 . 5 . 41 . 53 . 193
3322	5 . 13 . 41 . 41 . 101
3347	5 . 13 . 17 . 37 . 137
3503	5 . 13 . 13 . 53 . 137
3517	5 . 13 . 17 . 29 . 193
3791	29 . 37 . 37 . 181
3988	5 . 5 . 29 . 97 . 173
4010	13 . 13 . 17 . 29 . 193
4112	5 . 5 . 5 . 17 . 73 . 109
4354	17 . 61 . 101 . 181
4388	5 . 5 . 5 . 13 . 17 . 17 . 41
4429	29 . 41 . 73 . 113
4648	5 . 13 . 29 . 73 . 157
4657	5 . 101 . 109 . 197
4837	5 . 5 . 41 . 101 . 113
5083	5 . 29 . 41 . 41 . 53
5162	5 . 5 . 61 . 101 . 173
5557	5 . 13 . 17 . 89 . 157
5747	5 . 109 . 157 . 193
5792	5 . 13 . 13 . 29 . 37 . 37
5833	5 . 17 . 17 . 61 . 193
6013	5 . 5 . 5 . 5 . 5 . 5 . 13 . 89
6233	5 . 13 . 37 . 41 . 197
6458	5 . 17 . 37 . 89 . 149
6532	5 . 5 . 37 . 113 . 157
6689	13 . 97 . 113 . 157
6883	5 . 13 . 13 . 17 . 17 . 97
7097	5 . 29 . 29 . 53 113
7160	53 . 61 . 101 . 157
7793	5 . 13 . 29 . 89 . 181

8158	5 . 13 . 13 . 17 . 41 . 113
8273	5 . 29 . 53 . 61 . 73
8638	5 . 5 . 5 . 13 . 17 . 37 . 73
9028	5 . 13 . 73 . 89 . 193
9101	41 . 73 . 101 . 137
9295	61 . 73 89 . 109
9562	5 . 5 . 13 . 29 . 89 . 109
9587	5 . 5 . 13 . 13 . 73 . 149
9607	5 . 17 . 29 . 97 . 193
10118	5 . 37 . 53 . 53 . 197
10577	5 . 29 . 41 . 97 . 97
11563	5 . 5 13 29 . 41 . 173
12143	5 . 29 . 29 . 89 . 197
12565	13 . 17 . 29 . 109 . 113
15233	5 . 29 . 73 . 97 . 113
16237	5 . 5 . 5 . 17 . 17 . 41 . 89
16522	5 . 17 . 29 . 37 . 41 . 73
16777	5 . 13 . 13 . 17 . 97 . 101
17888	5 . 5 . 5 5 . 37 . 101 . 137
17972	5 . 13 . 29 . 53 . 53 . 61
18887	5 . 5 . 29 . 37 . 61 . 109
18974	13 . 13 . 17 . 29 . 29 . 149
19558	5 . 13 . 13 . 41 . 61 . 181
20362	5 . 5 . 5 . 113 . 149 . 197
23368	5 . 13 . 13 . 53 . 89 . 137
24083	5 . 13 . 157 . 157 . 181
24499	13 . 17 . 61 . 113 . 197
24958	5 . 17 . 37 . 37 . 53 . 101
29153	5 . 13 . 17 . 29 . 89 . 149
29242	5 . 17 . 17 . 61 . 89 . 109
29765	17 . 37 . 41 . 89 . 193
30218	5 . 13 . 41 . 41 . 61 . 137
31487	5 . 5 . 5 . 5 . 5 . 41 . 53 . 73
31843	5 . 13 . 17 . 17 . 137 . 197
34763	5 . 5 . 5 . 5 . 17 . 29 . 37 . 53
35137	5 . 5 . 17 . 73 . 101 . 197
35783	5 . 13 . 17 . 17 . 173 . 197
37147	5 . 13 . 17 . 41 . 97 . 157
38201	13 . 17 . 17 . 29 . 37 . 181
44987	5 . 5 . 5 . 13 . 29 . 109 . 197
46963	5 . 5 . 13 . 29 . 29 . 53 . 73
56387	5 . 5 . 13 . 17 . 53 . 61 . 89
57037	5 . 5 . 13 . 17 . 37 . 73 . 109
60743	5 . 13 . 17 . 17 . 17 . 53 . 109
61337	5 . 5 . 41 . 109 . 113 . 149
69107	5 . 17 . 53 . 53 . 73 . 137
69244	13 . 13 . 29 . 37 . 137 . 193
79813	5 . 5 . 13 . 17 . 53 . 73 . 149

86528	5 . 17 . 29 . 97 . 173 . 181
87263	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 149
97577	5 . 29 . 61 . 73 . 73 . 101
98063	5 . 5 . 73 . 97 . 157 . 173
121933	5 . 13 41 . 97 . 149 . 193
132683	5 . 17 . 29 . 109 . 181 . 181
157723	5 . 13 . 13 . 29 . 53 . 61 . 157
168703	5 . 37 . 37 . 61 . 173 . 197
181508	5 . 41 . 41 . 101 . 197 . 197
195787	5 . 5 . 13 . 17 . 29 . 37 . 53 . 61
237322	5 . 13 . 13 . 13 . 17 . 17 . 113 . 157
269861	13 . 37 . 41 . 101 . 101 . 181
278297	5 . 5 . 13 . 37 . 97 . 113 . 113
297212	5 . 5 . 13 . 97 . 113 . 137 . 193
314387	5 . 5 . 41 . 41 . 73 . 89 . 181
327737	5 . 5 . 5 . 5 . 13 . 13 . 29 . 89 . 197

349487	5 . 5 . 5 . 29 . 29 . 53 . 97 . 113
474013	5 . 5 . 5 . 13 . 17 . 17 . 29 . 73 . 113.
609161	13 . 73 . 73 . 113 . 137 . 173
647665	29 . 37 . 53 . 97 . 193 . 197
934862	5 . 5 . 5 . 13 . 13 . 17 . 17 . 37 . 53 . 73
1125533	5 . 13 . 41 . 89 . 101 . 137 . 193
1158413	5 . 5 . 29 . 37 . 41 . 61 . 73 . 137
1880912	5 . 5 . 13 . 17 . 37 . 53 . 53 . 61 . 101
2023513	5 . 5 . 5 . 5 . 37 . 41 . 97 . 113 . 197
2092285	17 . 17 . 37 . 37 . 37 . 41 . 41 . 89
2898587	5 . 5 . 17 . 29 . 73 . 137 . 173 . 197
3559861	13 . 37 . 61 . 89 . 109 . 113 . 197
4034153	5 . 13 . 13 . 17 . 29 . 41 . 53 . 89 . 101
4676188	5 . 5 . 17 . 37 . 37 . 37 . 89 . 101 . 113
4802183	5 . 73 . 97 . 109 . 113 . 137 . 193
4947916	17 . 17 . 37 . 53 . 61 . 73 . 89 . 109
6678737	5 . 5 . 5 . 17 . 17 . 29 . 41 . 53 . 97 . 101
9578563	5 . 5 . 13 . 17 . 17 . 17 . 29 . 61 . 109 . 149
34928797	5 . 13 . 13 . 17 . 29 . 37 . 53 . 53 . 73 . 193
59554033	5 . 13 . 13 . 13 . 37 . 61 . 73 . 89 . 101 . 109

5	13
13	7
17	2. 19. 32. 53. 1787
29	8. 37. 137. 253
37	17. 20. 202. 427. 461. 5792
41	1. 40. 83. 124. 163. 862. 1313. 4388
53	5. 58. 313. 472. 631. 737. 5083. 34763

61	23. 38. 1487. 1685. 2051. 3088. 17972. 195787
73	49. 97. 122. 389. 487. 1436. 8273. 8638. 16522. 31487. 46963. 934862
89	50. 128. 217. 1118. 1463. 2008. 2531. 6013. 16237. 56387. 2092285
97	4. 101. 287. 578. 683. 877. 1168. 1645. 2138. 6883. 10577
101	11. 112. 292. 617. 797. 920.1807. 2009. 2312. 3322. 16777. 24958. 97577. 1880912. 4034153. 6678737
109	79. 139. 188. 406. 575. 733. 1060. 1229. 4112. 9295. 9562. 18887. 29242. 57037. 60743. 4947916. 59554033
113	22. 91. 248. 317. 587. 1108. 1265. 1447. 2125. 4429. 4837. 7097. 8158. 12565. 15233. 278297. 349487. 474013. 4676188
137	59. 215. 763. 1018. 1703. 3347. 3503. 9101. 17888. 23368. 30218. 69107. 1158413
149	98. 247. 694. 1243. 6458. 9587. 18974. 29153. 61337. 79813. 87263. 9578563
157	62. 95. 376. 409. 566. 1037. 1475. 2888. 4648. 5557. 6532. 6689. 7160. 37147. 157723. 237322
173	28. 491. 547. 1585. 2450. 2623. 3988. 5162. 11563. 98063. 609161
181	10. 191. 352. 533. 553. 1277. 1639. 2705. 2906. 3791. 4354. 7793. 19558. 24083. 38201. 86528. 132683. 269861. 314387
193	43. 1201. 3238. 3517. 4010. 5747. 5833. 9028. 9607. 29765. 69244. 121933. 297212. 1125533. 4802183. 34928797
197	71. 268. 323. 662. 1702. 2041. 2293. 4657. 6233. 10118. 12143. 20362. 24499. 31843. 35137. 35783. 44987. 168703. 181508. 327737. 647665. 2023513. 2898587. 3559861

NEUE QUADRATUR DES KREISES.

I. Acotg .5 = (2) − (13).

26684971	0210071265	7279572372	8848455203	4183360499	1499728341	833
	364	7220869565	2173913043	4782608695	6521739130	434
		4977954329	5694145758	6618876941	4575866188	769
		(43)	204560302	8420465116	2790697674	418
		(47)	299441	4645858042	5531914893	617
		(51)	441	5293752324	0156862745	098
		(55)	6550690367	0843578181	818	
		(59)	9770521	2254817540	338	
		(63)	14640	2730743726	600	
		(67)	22	0259630730	860	
		(71)	332561019	920		
		(75)	503719	091		
		(79)	765	142		
		(83)	1	165		
		(87)	1			
26684971	0210071630	9478396268	6921374192	0505397169	7498644659	104
0,2000640569	5190437336	8654456654	4566544566	5445665445	6654456654	456
	7710131	0688316235	2941176470	5882352941	1764705882	352
		185127900	6896551724	1379310344	8275862068	965
		266673	0412205651	4831745270	7696610135	634
			7830238	1276333963	9002267573	696
		(53)	16	9947155749	8300377358	490
		(57)	252833663	2909752140	350	
		(61)	378007	0506907695	003	
		(65)	567	5921253449	092	
		(69)	8555011744	329		
		(73)	12937990	364		
		(77)	19625	419		
		(81)	29	850		
		(85)	45			
0,2000640569	5198147467	9528161463	4824308667	9015775954	9600162348	045
26684971	0210071630	9478396268	6921374192	0505397169	7498644659	104
0,1973955598	4988075837	0049765194	7902934475	8510378785	2101517688	941

II. $\operatorname{Acotg} .70 = 2(2) - 2(13) - (29)$

0,0142857142	8571428571	4285714285	7142857142	8571428571	4285714285	714
3) 29154	5189504373	1778425655	9766763848	3965014577	2594752186	588
5) 5	9499018266	1986077229	7257095257	9282441839	7096447908	609
7) 12142656	7890201240	2509644305	1546792335	0693284989	369	
9) 2478	0932222490	0490308090	6745213631	0887896588	773	
11) 5057333106	6306222511	8552396982	3736915897	263		
13) 1032108	7972715555	6146643346	3229334064	468		
15) 210	6344484227	6644111559	8665965170	217		
17) 429866221	2709519206	4407891013	300			
19) 87727	8002593779	4298858753	268			
21) 17	9036327059	9549856909	949			
23) 36538025	9306030583	042				
25) 7456	7399858373	588				
27) 1	5217836705	790				
29) 3105680	960					
31) 633	812					
33) 128						
9718	1729834791	0592808551	9922254616	1321671525	7531584062	196
1734665	2555743034	3215663472	1649541762	1527612141	338	
459757555	1482383864	7141126998	3976083263	387		
14	0422965615	1776274103	9911064344	681		
4617	2526452304	1805203092	277			
1588609	8230696981	871				
563623581	695					
20	447					
9718	1731569456	3608309155	5043272185	4416655304	3545867487	890
0,0142857142	8571428571	4285714285	7142857142	8571428571	4285714285	714
1	1899803653	2397215445	9451419051	5856488367	9419289581	721
275	3436913610	0054478676	7416134847	8987544065	419	
79392	9844055042	7395895642	0248410312	651		
25286248	3100559953	3200464177	252			
8525539383	8073802709	997				
298	2695994334	943				
107092	446					
3						
0,0142857144	0471232500	0119922734	6518096163	0866047064	6911326560	146
9718	1731569456	3608309155	5043272185	4416655304	3545867487	890
0,0142847425	8739663043	6511613579	1474823977	6449391760	3365459072	256

III. $\operatorname{Acotg} .99 = -(2) + 2(13) - (29).$

0,0101010101	0101010101	0101010101	0101010101	0101010101	0101010101	010
3) 10306	1015212836	4555667892	0621375472	9212335579	0228548210	397
5) 1	0515357128	1335022514	8344109925	0559046254	0127571528	232
7) 1072886	1471414653	8633643925	1020361090	3228255032	295	
9) 109	4670081768	6617552662	3737477845	2290911973	781	
11) 111689631	8506950061	4898861083	3430495960	817		
13) 11395	7383788077	7534424942	4633550708	689		
15) 1	1627118027	5561425816	2373699984	767		
17) 1186319	5620402145	2725474308	742			
19) 121	0406654464	0491044329	589			
21) 123498281	2431434654	048				
23) 12600	5796595391	761				
25) 1	2856422466	625				
27) 1311745	991					
29) 133	837					
31) 13						
3435	3671737612	1518555964	0207125157	6404111859	6776182736	799
153269	4495916379	1233377703	5860051584	3318322147	470	
10153602	8955177278	3172623734	8493681450	983		
775141201	8370761721	0824913332	317			
6	3705613392	8446897069	978			
547	8512895451	815				
48583	184					
3435	3671890881	6024625946	1170821347	7513162840	6372940772	546
0,0101010101	0101010101	0101010101	0101010101	0101010101	0101010101	010
2103071425	6267004502	9668821985	0111809250	8025514305	646	
12	1630099085	4068616962	4859719760	5810101330	420	
876	5952599082	9041109610	9587196208	360		
69783	5036494243	8395616135	808			
5880870	5353877840	668				
514256898	665					
4	615					
0,0101010101	2204081538	7998024565	9791117914	9156023837	7787572825	192
3435	3671890881	6024625946	1170821347	7513162840	6372940772	546
0,0101006665	8532190657	1973398619	8620296567	1642860997	1414632052	646

IV. $\operatorname{Acotg} .307 = -3(2) + 3(5) + (13) + (29).$

	0,0032573289	9022801302	9315960912	0521172638	4364820846	9055374592	833
	3)	345 6088648397	3443000295	0769987174	1094169326	1556823471	597
	5)	36669764	6489336152	1087234559	3817877050	8899421286	416
	7)	389 0732490417	2580304164	8671007839	6274855960	501	
	9)	41281419	3298311709	4522474201	4009658191	131	
	11)	438 0037913381	6985798496	2620441698	672		
	13)	46473043	8878046300	7405517516	808		
	15)	493 0879254719	3742187243	551			
	17)	52317576	3638805103	367			
	19)	555	9995380734	067			
	21)	58897127	616				
	23)	624	909				
0,0032	115	2029549465	7814333365	0256662391	3698056442	0518941157	199
	55	5818927202	4654329166	4095858262	8039265137	214	
	39	8185264852	8816890772	3874585608	970		
	32	8725283647	9582812482	903			
	29	2157651617	582				
	27	169					
	115	2029549521	3633260607	3096256443	5336089154	4173256031	037
	0,0032573289	9022801302	9315960912	0521172638	4364820846	9055374592	833
	7333952	9297867230	4217446911	8763575410	1779884257	283	
	4586824	3699812412	1613608244	6001073132	347		
	3574849	5298311253	9031193655	139			
	3077504	4919929711	962				
	2804625	124					
	0,0032573289	9030135255	8618414966	8442006812	0043393260	0790259974	688
	115	2029549521	3633260607	3096256443	5336089154	4173256031	037
	0,0032573174	7000585734	4985154359	5345750368	4707304105	6617003943	651

TAFEL DER BÖGEN ZU GEGEBENEN PRIMTANGENTEN
IN EINHEITEN DES RADIUS, AUF 110 ZIFFERN.

2	0,7853981633	9744830961	5660845819	8757210492	9234984377	6455243736	1480769541	
5	0,4636476090	0080611621	4256231461	2144020285	3705428612	0263810933	0887201978	6
13	0,5880026035	4756755124	5611080625	0854276017	0724605592	4353726047	2072	
17	0,2449786631	2686415417	2082481211					
29	0,3805063771	1236486630	3587916810	4331044974	0571365810	0837576305	623	
37	0,1651486774	1462683827	9128289643	9435540983	8			

ZUR BERECHNUNG DER GEWÖHNLICHEN LOGARITHMEN.

Man bestimme die Logarithmen von

$$\log \frac{1025}{*} = a$$
$$\log \frac{1024^2}{*} = b$$
$$\log \frac{81^2}{*} = c$$
$$\log \frac{125^2}{*} = d$$
$$\log \frac{99^2}{*} = e$$

($*$ zeigt einen um 1 kleineren Nenner als Zähler an) dann gilt, wie man sich leicht überzeugen kann:

$$\log 2 = \frac{14\frac{3}{4} + \frac{5}{4}a + 2b - \frac{3}{4}c - 2d + e}{49} = f$$

Außerdem lässt sich leicht herleiten

$$\log 41 = a + 12f - 2 = g$$
$$\log 3 = \frac{1 + c + 4f + g}{8}$$

$\log 11 \,.\, 31$ und $\log \frac{11}{7}$ und also auch $\log 7 \,.\, 31$

	$\frac{7}{23 \,.\, 73}$	$\frac{1680^2}{*}$	hieraus 73
$\frac{17}{23 \,.\, 73}$	$\frac{136000}{*}$	aus diesen $\frac{7}{23}$	$\left[\text{und } \frac{7}{23},\ \frac{7}{17}\right]$
$\frac{7 \,.\, 73}{17}$	$\frac{511^2}{*}$		
$7 \,.\, 7 \,.\, 43$	$\frac{512001}{*}$	$\frac{7 \,.\, 7}{17}$ hieraus und $\frac{7}{17}$	$\left[\text{und } \frac{7}{23}\right]$
$17 \,.\, 43$	$\frac{730^2}{*}$		

wird 7, 17, 23, 43

---

a,	$\frac{81}{8}$	$\frac{81}{80}$	
b,	$\frac{41}{4}$	$\frac{6561}{6560}$	
c,	2	$\frac{1025}{1024}$	
d,	7	$\frac{2401}{2400}$	
e,	29	$\frac{1681^2}{1680.1682}$	
f,	43	$\frac{512001}{512000}$	
g,	23 . 73	$\frac{1680^2}{1679.1681}$	
h,	17	$\frac{136000}{135999}$	
i,	73	$\frac{511^2}{510.512}$	$\frac{730^2}{729.731}$
k,	13	$\frac{729^2}{728.730}$	
l,	19	$\frac{512^2}{511.513}$	
m,	47	$\frac{2116^2}{2115.2117}$	
n,	61	$\frac{2500^2}{2499.2501}$	
o,	31	$\frac{17081^2}{17080.17082}$	
p,	11	$\frac{1024^2}{1023.1025}$	$\frac{2001^2}{2000.2002}$
q,	71	$\frac{10935^2}{10934.10936}$	
r,	53	$\frac{788800}{788799}$	
s,	67	$\frac{274700}{274699}$	$\frac{3751^2}{*}$
t,	37	$\frac{1000000}{999999}$	$\frac{1331^2}{1330.1332}$

u,	59	$\frac{3481^2}{3480.3481}$	
v,	89	$\frac{4095^2}{4094.4096}$	
w,	83	$\frac{6889^2}{6888.6890}$	
x,	79	$\frac{3879^2}{3880.3882}$	
y,	97	$\frac{13871^2}{13870.13872}$	$\frac{46656^2}{46655.46657}$

[Die Anwendung dieser Brüche zur Bestimmung der Logarithmen der nebenstehenden kleinen Primzahlen mit Hilfe der noch wachsenden Potenzen von $\frac{1}{x}$ fortschreitenden sehr rasch konvergierenden Reihen für $\log \frac{x}{x-1}$ ergibt sich unmittelbar aus dem zu Anfang ausgeführten Beispiel.

Es lassen sich übrigens zur Bestimmung der Logarithmen der kleinsten Primzahlen 2, 3, 7 noch vorteilhaftere Reihen aufstellen, wenn man diese Zahlen von Gauss auf geeignete Weise mit den von Huyghens (Hugenii, Opera varia, Lugduni 1724 S. 457) angegebenen verbindet:

2	1000
	$1024 = 2^{10}$
3	$32805 = 3^8 \,.\, 5$
	$32768 = 2^{15}$
7	$2400 = 100 \,.\, 2^3 \,.\, 3$
	$2401 = 7^4$
11	$9800 = 100 \,.\, 2 \,.\, 7^2$
	$9801 = 3^4 \,.\, 11^2$
13	$123200 = 100 \,.\, 2^4 \,.\, 7 \,.\, 11$
	$123201 = 3^6 \,.\, 13$
17	$2600 = 100 \,.\, 2 \,.\, 13$
	$2601 = 3^2 \,.\, 17^2$
19	$28899 = 3^2 \,.\, 13^2 \,.\, 19$
	$28900 = 100 \,.\, 17^2$
23	$25920 = 10 \,.\, 2^5 \,.\, 3^4$
	$25921 = 7^2 \,.\, 23^2$
29	$613088 = 2^5 \,.\, 7^2 \,.\, 17 \,.\, 23$
	$613089 = 3^6 \,.\, 29^2$

31 $116280 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 17 \,.\, 19.$
$116281 = 11^2 \,.\, 31$
37 $165648 = 2^4 \,.\, 3 \,.\, 7 \,.\, 17 \,.\, 29$
$165649 = 11^2 \,.\, 37$
41 $1413720 = 10 \,.\, 2^2 \,.\, 3^3 \,.\, 7 \,.\, 11 \,.\, 17$
$1413721 = 29^2 \,.\, 41^2$
43 $978120 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 11 \,.\, 13 \,.\, 19$
$978121 = 23^2 \,.\, 43^2$
47 $664848 = 2^5 \,.\, 3^6 \,.\, 7 \,.\, 13$
$664849 = 31^2 \,.\, 47^2$
53 $3059000 = 100 \,.\, 7 \,.\, 19 \,.\, 23$
$3059001 = 3^2 \,.\, 11^2 \,.\, 53^2$
59 $5851560 = 10 \,.\, 2^2 \,.\, 3 \,.\, 11^2 \,.\, 13 \,.\, 31$
$5851561 = 41^2 \,.\, 59^2$
61 $3575880 = 10 \,.\, 2^2 \,.\, 3^3 \,.\, 7 \,.\, 11 \,.\, 43$
$3575881 = 31^2 \,.\, 61^2$
67 $1620528 = 2^4 \,.\, 3 \,.\, 7^2 \,.\, 13$
$1620529 = 19^2 \,.\, 67^2$
71 $2016399 = 3 \,.\, 7^2 \,.\, 11 \,.\, 29 \,.\, 43$
$2016400 = 100 \,.\, 2^2 \,.\, 71^2$
73 $5116644 = 2^2 \,.\, 3^2 \,.\, 13^2 \,.\, 29^2$
$5116645 = 7 \,.\, 17 \,.\, 19 \,.\, 31 \,.\, 73$
79 $5997600 = 100 \,.\, 2^3 \,.\, 3^2 \,.\, 7^2 \,.\, 17$
$5997601 = 31^2 \,.\, 79^2$
83 $1164240 = 10 \,.\, 2^3 \,.\, 3^3 \,.\, 7^2 \,.\, 11$
$1164241 = 13^2 \,.\, 83^2$
89 $2859480 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 13^2 \,.\, 47$
$2859481 = 19^2 \,.\, 89^2.$
97 $1138488 = 2^3 \,.\, 3 \,.\, 13 \,.\, 41 \,.\, 89$
$1138489 = 11^2 \,.\, 97^2$

Zur Bestimmung der Logarithmen für alle die Primzahlen, welche kleiner als 200 sind, kann man mit Vorteil die in den Tafeln zur Kreisteilung gefundenen Zerlegungen von $aa + 1$, $a + 2$, $..aa + 81$ benutzen, wenn man sich auf diejenigen Zahlen a beschränkt, welche selbst nur Primzahlen unter 200 als Teiler enthalten. Die übrigen a lassen sich dann zur Bestimmung der Logarithmen der darin vorkommenden größeren Primteiler verwenden.]

NACHLASS. DIE ERSTEN ZEHNTAUSEND QUADRATE.

	10	20	30	40	50	60	70	80	90	
00	1000	4000	9000	16000	25000	36000	49000	64000	81000	000
1	02	04	06	08	10	12	14	16	18	001
2	04	08	12	16	20	24	28	32	36	004
3	06	12	18	24	30	36	42	48	54	009
4	08	16	24	32	40	48	56	64	72	016
5	10	20	30	40	50	60	70	80	81090	025
6	12	24	36	48	60	72	84	64096	81108	036
7	14	28	42	56	70	84	49098	64112	26	049
8	16	32	48	64	80	36096	49112	28	44	064
09	18	36	54	72	25090	36108	26	44	62	081
10	20	40	60	80	25100	20	40	60	80	100
1	22	44	66	88	10	32	54	76	81198	121
2	24	48	72	16096	20	44	68	64192	81216	144
3	26	52	78	16104	30	56	82	64208	34	169
4	28	56	84	12	40	68	49196	24	52	196
5	30	60	90	20	50	80	49210	40	70	225
6	32	64	9096	28	60	36192	24	56	81288	256
7	34	68	9102	36	70	36204	38	72	81306	289
8	36	72	08	44	80	16	52	64288	24	324
19	38	76	14	52	25190	28	66	64304	42	361
20	40	80	20	60	25200	40	80	20	60	400
1	42	84	26	68	10	52	49294	36	78	441
2	44	88	32	76	20	64	49308	52	81396	484
3	46	92	38	84	30	76	22	68	81414	529
4	1048	4096	44	16192	40	36288	36	64384	32	576
5	50	4100	50	16200	50	36300	50	64400	50	625
6	52	04	56	08	60	12	64	16	68	676
7	54	08	62	16	70	24	78	32	81486	729
8	56	12	68	24	80	36	49392	48	81504	784
29	58	16	74	32	25290	48	49406	64	22	841
30	60	20	80	40	25300	60	20	80	40	900
1	62	24	86	48	10	72	34	64496	58	961
2	65	29	93	57	21	85	49	64513	77	024
3	67	33	9199	65	31	36397	63	29	81595	089
4	69	37	9205	73	41	36409	77	45	81613	156
5	71	41	11	81	51	21	49491	61	31	225
6	73	45	17	89	61	33	49505	77	49	296
7	75	49	23	16297	71	45	19	64593	67	369
8	77	53	29	16305	81	57	33	64609	81685	444
39	79	57	35	13	25391	69	47	25	81703	521
40	81	61	41	21	25401	81	61	41	21	600
1	83	65	47	29	11	36493	75	57	39	681
2	85	69	53	37	21	36505	49589	73	57	764
3	87	73	59	45	31	17	49603	64689	75	849
4	89	77	65	53	41	29	17	64705	81793	936
5	92	82	72	62	52	42	32	22	81812	025
6	94	86	78	70	62	54	46	38	30	116
7	96	90	84	78	72	66	60	54	48	209
8	1098	94	90	86	82	78	74	70	66	304
94	1100	4198	9296	16394	25492	36590	49688	64786	81884	401

11	21	31	41	51	61	71	81	91	
1210	4410	9610	16810	26010	37210	50410	65610	82810	000
12	14	16	18	20	22	24	26	28	201
14	18	22	26	30	34	38	42	46	404
16	22	28	34	40	46	52	58	64	609
18	26	34	42	50	58	66	74	82882	816
21	31	41	51	61	71	81	65691	82901	025
23	35	47	59	71	83	50495	65707	19	236
25	39	53	67	81	37295	50509	23	37	449
27	43	59	75	26091	37307	23	39	55	664
29	47	65	83	26101	19	37	55	73	881
32	52	72	16892	12	32	52	72	82992	100
34	56	78	16900	22	44	66	65788	83010	321
36	60	84	08	32	56	80	65804	28	544
38	64	90	16	42	68	50594	20	46	769
40	68	9696	24	52	80	50608	36	64	996
43	73	9703	33	63	37393	23	53	83083	225
45	77	09	41	73	37405	37	69	83101	456
47	81	15	49	83	17	51	65885	19	689
49	85	21	57	26193	29	65	65901	37	924
52	90	28	66	26204	42	80	18	56	161
1254	94	34	74	14	54	50694	34	74	400
56	4498	40	82	24	66	50708	50	83192	641
58	4502	46	90	34	78	22	66	83210	884
61	07	53	16999	45	37491	37	83	29	129
63	11	59	17007	55	37503	51	65999	47	376
65	15	65	15	65	15	65	66015	65	625
67	19	71	23	75	27	79	31	83283	876
70	24	78	32	86	40	50794	48	83302	129
72	28	84	40	26296	52	50808	64	20	384
74	32	90	48	26306	64	22	80	38	641
76	36	9796	56	16	76	36	66096	56	900
79	41	9803	65	27	37589	51	66113	75	161
81	45	09	73	37	37601	65	29	83393	424
83	49	15	81	47	13	79	45	83411	689
85	53	21	89	57	25	50893	61	29	956
88	58	28	17098	68	38	50908	78	48	225
90	62	34	17106	78	50	22	66194	66	496
93	66	40	14	88	62	36	66210	83484	769
95	71	47	23	26399	75	51	27	83503	044
1297	75	53	31	26409	87	65	43	21	321
1299	79	59	39	19	37699	79	59	39	600
1301	83	65	47	29	37711	50993	75	57	881
04	88	72	56	40	24	51008	66292	76	164
06	92	78	64	50	36	22	66308	83594	449
08	4596	84	72	60	48	36	24	83612	736
11	4601	91	81	71	61	51	41	31	025
13	05	9897	89	81	73	65	57	49	316
15	09	9903	17197	26491	85	79	73	67	609
17	13	09	17205	26501	37797	51093	66389	83685	904
1320	4618	9916	17214	26512	37810	51108	66406	83704	201

	10	20	30	40	50	60	70	80	90	
50	1102	4202	9302	16402	25502	36602	49702	64802	81902	500
1	04	06	08	10	12	14	16	18	20	601
2	06	10	14	18	22	26	30	34	38	704
3	08	14	20	26	32	38	44	50	56	809
4	10	18	26	34	42	50	58	66	74	916
5	13	23	33	43	53	63	73	83	81993	025
6	15	27	39	51	63	75	49787	64899	82011	136
7	17	31	45	59	73	87	49801	64915	29	249
8	19	35	51	67	83	36699	15	31	47	364
59	21	39	57	75	25593	36711	29	47	65	481
60	23	43	63	83	25603	23	43	63	82083	600
1	25	47	69	91	13	35	57	79	82101	721
2	27	51	75	16499	23	47	71	64995	19	844
3	29	55	81	16507	33	59	49885	65011	37	969
4	32	60	88	16	44	72	49900	28	56	096
5	34	64	9394	24	54	84	14	44	74	225
6	36	68	9400	32	64	36796	28	60	82192	356
7	38	72	06	40	74	36808	42	76	82210	489
8	40	76	12	48	84	20	56	65092	28	624
69	42	80	18	56	25694	32	70	65108	46	761
70	1144	84	24	64	25704	44	84	24	64	900
1	47	89	31	73	15	57	49999	41	82283	041
2	49	93	37	81	25	69	50013	57	82301	184
3	51	4297	43	89	35	81	27	73	19	329
4	53	4301	49	16597	45	36893	41	65189	37	476
5	55	05	55	16605	55	36905	55	65205	55	625
6	57	09	61	13	65	17	69	21	73	776
7	59	13	67	21	75	29	83	37	82391	929
8	62	18	74	30	86	42	50098	53	82409	084
79	64	22	80	38	25796	54	50112	70	28	241
80	66	26	86	46	25806	66	26	65286	46	400
1	68	30	92	54	16	78	40	65302	64	561
2	70	34	9498	62	26	36990	54	18	82482	724
3	72	38	9504	70	36	37002	68	34	82500	889
4	75	43	11	79	47	15	83	51	19	056
5	77	47	17	87	57	27	50197	67	37	225
6	79	51	23	16695	67	39	50211	83	55	396
7	81	55	29	16703	77	51	25	65399	73	569
8	83	59	35	11	87	63	39	65415	82591	744
89	85	63	41	19	25897	75	53	31	82609	921
90	88	68	48	28	25908	37088	68	48	28	100
1	90	72	54	36	18	37100	82	64	46	281
2	92	76	60	44	28	12	50296	80	64	464
3	94	80	66	52	38	24	50310	65496	82682	649
4	96	84	72	60	48	36	24	65512	82700	836
5	1199	89	79	69	59	49	39	29	19	025
6	1201	93	85	77	69	61	53	45	37	216
7	03	4397	91	85	79	73	67	61	55	409
8	05	4401	9597	16793	89	85	81	77	73	604
9	1207	4405	9603	16801	25999	37197	50395	65693	82791	801

11	21	31	41	51	61	71	81	91	
1322	4622	9922	17222	26522	37822	51122	66422	83722	500
24	26	28	30	32	34	36	38	40	801
27	31	35	39	43	47	51	55	59	104
29	35	41	47	53	59	65	71	77	409
31	39	47	55	63	71	79	66487	83795	716
34	44	54	64	74	84	51194	66504	83814	025
36	48	60	72	84	37896	51208	20	32	336
38	52	66	80	26594	37908	22	36	50	649
40	56	72	88	26604	20	36	52	68	964
43	61	79	17297	15	33	51	69	83887	281
45	65	85	17305	25	45	65	66585	83905	600
47	69	91	13	35	57	79	66601	23	921
50	74	9998	22	46	70	51294	18	42	244
52	78	10004	30	56	82	51308	34	60	569
54	82	10	38	66	37994	22	50	78	896
57	87	17	47	77	38007	37	67	83997	225
1359	91	23	55	87	19	51	83	84015	556
1361	4695	29	63	26697	31	65	66699		889
64	4700	36	72	26708	44	80	66716		224
66	04	42	80	18	56	51394	32		561
68	08	48	88	28	68	51408			900
71	13	55	17397	39	81	23			241
73	17	61	17405	49	38093	37			584
75	21	67	13	59	38105	51			929
78	26	74	22	70	18	66			276
80	30	80	30	80	30	80			625
82	34	86	38	26790	42	51494			976
85	39	93	47	26801	55	51509			329
87	43	10099	55	11	67	23			684
90	48	10106	64	22	80	38			041
92	52	12	72	32	38192	52			400
94	56	18	80	42	38204	66			761
97	61	25	89	53	17	81			124
1399	65	31	17497	63	29	51595			489
1401	69	37	17505	73	41	51609			856
04	74	44	14	84	54	24			225
06	78	50	22	26894	66	38			596
08	82	56	30	26904	78	52			969
11	87	63	39	15	38291	67			344
13	91	69	47	25	38303	81			721
16	4796	76	56	36	16	51696			100
18	4800	82	64	46	28	51710			481
20	04	88	72	56	40	24			864
23	09	10195	81	67	53	39			249
25	13	10201	89	77	65	53			636
28	18	08	17598	88	78	68			025
30	22	14	17606	26998	38390	82			416
32	26	20	14	27008	38402	51796			809
35	31	27	23	19	15	51811			204
1437	4835	10233	17631	27029	38427	51825			601

NACHLASS INDIZES DER PRIMZAHLEN IM HÖHEREN ZAHLENBEREICH.

	$-1+2i$	$-1-2i$	-3	$3+2i$	$3-2i$	$1+4i$	$1-4i$	$-5+2i$	$-5-2i$	$-1+6i$	$-1-6i$	$5+4i$	$5-4i$	-7	$7+2i$	$7-2i$	$-5+6i$	$-5-6i$	$-3+8i$	$-3-8i$	$5+8i$	$5-8i$	$9+4i$	$9-4i$
	i	i	$1-i$	$-1-i$	$+1-i$	$+1-2i$	$+1-2i$	$+1+i$	$-1+i$	$+1+i$	$-1+i$	$+2-i$	$+1-2i$	$+1-2i$	$-1+i$	$1+i$	$1-i$	$-1-i$	$1+i$	$-1-i$	$1-i$	$1-i$	$1+i$	$1+4i$
i	1	1	2	3	3	4	4	7	7	9	9	10	10	12	13	13	15	15	18	18	22	22	24	24
$1+i$	2	3	3	7	4	7	5	1	22	1	28	32	2	46	40	1	16	31	1	37	23	23	1	7
$1-i$	1	2	1	4	1	3	1	22	15	28	19	22	32	34	27	40	1	16	55	19	1	1	73	79
$-1+2i$	$*$	3	7	4	5	9	2	18	12	13	6	27	21	25	19	10	35	9	68	65	10	40	20	63
$-1-2i$	1	$*$	5	11	4	14	15	12	18	6	31	31	17	31	10	45	39	5	11	68	40	54	81	44
-3	3	1	$*$	2	2	3	5	17	3	16	16	25	35	16	21	47	12	12	6	42	51	29	14	50
$3+2i$	2	1	6	$*$	1	13	9	13	23	14	35	26	33	3	4	44	28	52	9	44	79	38	36	23
$3-2i$	3	2	2	7	$*$	15	11	9	27	17	14	3	6	21	44	4	52	28	44	27	82	57	89	60
$1+4i$	1	2	3	9	7	$*$	6	15	20	21	2	8	9	29	22	24	38	11	23	52	27	81	78	1
$1-4i$	2	3	1	1	3	10	$*$	20	1	2	3	19	8	11	24	22	41	38	52	5	15	5	79	18
$-5+2i$	0	2	1	3	11	11	12	$*$	25	5	28	29	24	30	51	41	19	36	71	66	8	75	91	58
$-5-2i$	2	0	3	5	9	4	13	11	$*$	28	23	24	39	18	15	25	36	49	30	53	53	8	70	85
$-1+6i$	3	0	4	8	3	5	10	19	22	$*$	29	33	5	22	27	33	34	59	39	67	65	12	39	32
$-1-6i$	0	1	4	9	8	6	3	22	5	11	$*$	15	3	10	7	1	29	34	49	21	12	87	32	9
$5+4i$	3	3	5	6	11	4	3	5	16	25	15	$*$	32	9	16	9	46	32	69	13	26	55	4	43
$5-4i$	1	1	7	5	6	5	12	16	19	33	7	32	$*$	15	35	16	32	46	31	15	33	70	37	28
-7	1	3	4	7	1	1	7	10	10	10	10	1	11	$*$	28	28	23	53	51	33	83	61	11	5
$7+2i$	1	0	1	10	12	2	8	21	9	1	25	36	7	44	$*$	43	55	26	37	10	87	85	27	89
$7-2i$	0	3	3	2	10	8	14	23	7	7	19	37	36	20	17	$*$	26	25	46	55	19	65	23	21
$-5+6i$	1	1	0	6	10	10	1	25	6	4	27	2	4	43	37	8	$*$	31	21	43	85	2	45	29
$-5-6i$	3	3	0	10	6	7	6	6	11	9	4	4	22	13	8	11	1	$*$	25	39	46	19	83	3
$-3+8i$	0	3	6	5	4	15	18	7	26	3	33	9	31	23	1	6	33	13	$*$	26	28	24	73	13
$-3-8i$	1	0	2	4	11	8	19	26	21	15	21	21	19	17	6	27	43	3	62	$*$	24	28	67	7
$5+8i$	2	0	7	7	10	11	15	4	5	9	8	38	13	19	39	7	25	2	24	56	$*$	30	77	79
$5-8i$	0	2	5	10	1	9	13	19	4	8	27	23	18	37	33	13	2	55	56	24	74	$*$	1	35
$9+4i$	0	1	2	8	5	14	7	11	14	35	4	28	25	39	3	39	21	7	1	11	49	1	$*$	90
$9\quad 4i$	3	0	6	11	8	1	2	14	25	4	17	35	28	33	13	29	37	51	65	19	23	71	6	$*$
$-1+10i$	2	2	5	2	0	7	7	16	17	31	17	21	10	5	46	35	50	45	39	34	57	42	10	54
$-1-10i$	2	2	7	0	2	1	1	3	16	35	13	30	31	35	9	46	15	50	70	21	86	79	42	22
$3+10i$	1	3	2	0	9	6	5	14	24	23	24	17	18	38	49	50	54	56	14	2	69	51	65	31
$3-10i$	1	3	6	3	0	3	10	24	14	24	5	38	27	26	50	23	56	54	38	50	29	3	49	47
$-7+8i$	3	2	7	1	9	14	9	22	9	7	22	7	15	12	5	23	48	6	4	47	11	68	58	82
$-7-8i$	2	1	5	3	7	15	2	23	22	22	25	5	37	36	49	31	6	48	29	4	68	77	46	70
-11	2	2	0	11	5	5	3	1	15	24	24	37	7	40	12	12	15	45	61	7	16	16	94	34
$-11+4i$	0	1	3	4	3	7	15	14	27	29	13	36	29	26	32	21	57	29	54	30	41	18	9	38
$-11-4i$	3	0	1	9	4	9	1	13	14	31	11	39	36	38	47	32	59	27	66	18	62	63	26	39
$7+10i$	3	1	3	3	4	12	0	3	1	26	10	23	20	4	6	12	44	22	29	31	47	14	12	75
$7-10i$	3	1	1	4	9	0	4	15	17	10	26	20	13	28	12	6	22	44	13	47	58	25	69	84
$11+6i$	2	3	4	11	7	0	12	17	4	20	12	7	14	17	18	49	8	29	43	18	13	11	75	20
$11-6i$	1	2	4	1	5	4	0	4	3	12	20	34	37	23	23	18	59	8	54	25	77	35	44	69
$-23+2i$	1	0	7	2	8	15	4	27	1	20	18	18	32	7	33	36	24	7	26	28	72	66	38	77
$-23-2i$	0	3	5	8	2	12	9	15	13	18	20	32	38	1	36	7	37	24	28	62	22	72	35	26
$-9+20i$	0	0	2	11	1	3	6	8	16	19	3	20	37	15	42	37	5	42	53	59	39	56	61	16
$-9-10i$	0	0	6	7	5	10	5	16	8	21	1	7	20	9	11	42	42	35	41	71	56	17	16	19
$-7+12i$	2	1	4	0	11	9	4	12	13	1	14	11	22	20	30	5	42	19	59	50	81	64	87	87

HILFSTAFEL

ZUR LÖSUNG DER UNBESTIMMTEN GLEICHUNG

$$A = fxx + gyy$$

MIT DEM AUSSCHLUSSVERFAHREN.

Es wird vorausgesetzt, dass als Ausschlusszahl eine Primzahl p gewählt wurde, durch die keine der Zahlen A, f, g teilbar ist. Die Tafel beschränkt sich außerdem auf die beiden Fälle, in denen der Wert des Ausdrucks $\frac{A}{f}(\text{mod.}p)$ entweder ein bestimmter quadratischer Rest (stets 1) oder ein bestimmter quadratischer Nichtrest modulo p ist. Schließlich hat man sich damit begnügt, die Tafel nur für den Fall einzurichten, dass fg ein quadratischer Rest von p ist, und den entgegengesetzten Fall ganz übergangen. Der sechste Abschnitt der *Disquisitiones Arithmeticae* gibt ausreichend Anleitung, wie sich das, was die Tafel nicht unmittelbar enthält, leicht aus ihr ableiten lässt.

Beispiele. Die zu lösende Gleichung sei $21680143 = xx + 78yy$

1) Ausschlusszahl $= 5$ $\qquad fg = \text{N}, \quad \frac{A}{f} \equiv 3 \equiv 2 \,.\, 2^2$
Aus der Tafel $1, 4$ für $fg = R$ und daher $0, 2, 3$ für $fg = \text{N}$, und für den obigen Fall $0, 1, 4$ oder ausgeschlossen $5n \pm 2$

2) Ausschlusszahl $= 7$ $\qquad fg = R, \quad \frac{A}{f} \equiv 2 \equiv 1, 3^2$
Aus der Tafel $0, 1, 2, 5, 6$ Für den vorliegenden Fall $0, 3, 6, 1, 4$ und ausgeschlossen $7n \pm 2$

3) Ausschlusszahl $= 11$ $\qquad fg = R, \quad \frac{A}{f} \equiv 1$
Man erhält also $0, 1, 3, 5, 6, 8, 10$; ausgeschlossen $11n \pm 2, 4$

4) Ausschlusszahl $= 17$ $\qquad fg = \text{N}, \quad \frac{A}{f} \equiv 9 \equiv 1 \,.\, 3^1$

$$0 \,.\, 1 \,.\, 3 \,.\, 4 \,.\, 6$$
$$0 \,.\, 3 \,.\, 8 \,.\, 5 \,.\, 1$$
$$0, 2, 3, 4, 6, 7$$
$$\text{Ausschlusszahl} \quad \pm 1, 5, 8$$

p	Wert von $\frac{A}{f}(\text{mod}.p)$	Zahlen, denen x modulo p kongruent sein muss, wenn sie positiv oder negativ genommen werden.
3	1	$0, 1$
	2	1
5	1	$0, 1$
	2	1
7	1	$0, 1, 2$
	6	$2, 3$
11	1	$0, 1, 3, 5$
	10	$1, 3, 4$
13	1	$0, 1, 2, 6$
	2	$1, 4, 5$
17	1	$0, 1, 3, 4, 6$
	3	$1, 2, 4, 6$
19	1	$0, 1, 2, 3, 4, 7$
	18	$1, 3, 6, 7, 8$
23	1	$0, 1, 4, 8, 9, 10, 11$
	22	$1, 2, 3, 4, 6, 8$
29	1	$0, 1, 5, 6, 8, 9, 11, 13$
	2	$1, 3, 5, 6, 8, 13, 14$
31	1	$0, 1, 2, 4, 5, 7, 10, 11, 13$
	30	$4, 5, 6, 8, 11, 12, 13, 14$
37	1	$0, 1, 2, 7, 8, 10, 11, 14, 16, 18$
	2	$1, 3, 6, 7, 8, 14, 15, 17, 18$
41	1	$0, 1 \,.\, 3, 9, 12, 13, 14, 16, 17, 18, 19$
	3	$1, 2, 6, 7, 8, 9, 11, 12, 13, 17$
43	1	$0, 1, 2, 3, 7, 8, 9, 11, 13, 17, 18, 20$
	42	$1, 2, 5, 6, 7, 8, 9, 16, 17, 19, 21$
47	1	$0, 1, 4, 6, 9, 10, 11, 16, 18, 19, 20, 22, 23$
	46	$2, 3, 5, 9, 13, 15, 16, 18, 19, 21, 22, 23$
53	1	$0, 1, 4, 5, 8, 10, 12, 13, 14, 16, 19, 20, 21, 22$
	2	$1, 3, 7, 8, 11, 12, 15, 16, 18, 21, 24, 25, 26$
59	1	$0, 1, 3, 5, 10, 11, 13, 14, 15, 17, 19, 22, 23, 24, 25, 29$
	58	$1, 3, 6$

Ausschluss-zahl p	$\frac{A}{f}$	$\frac{f}{A}$	$fgRp$		
			Zugelassen		Ausgeschlossen
3	1	1	0	1 . 2	
	2	2	1 . 2		0
5	1	1	0	1 . 4	2 . 3
	2	3	1 . 4		0 . 2 . 3
	3	2	2 . 3		0 . 1 . 4
	4	4	0	2 . 3	1 . 4
7	1	1	0 . 2 . 5	1 . 6	3 . 4
	2	4	0 . 1 . 6	3 . 4	2 . 5
	3	5	1 . 3 . 4 . 6		0 . 2 . 5
	4	2	0 . 3 . 4	2 . 5	1 . 6
	5	3	1 . 2 . 5 . 6		0 . 3 . 4
	6	6	2 . 3 . 4 . 5		0 . 1 . 6
11	1	1	0 . 3 . 5 . 6 . 8	1 . 10	2 . 4 . 7 . 9
	2	6	1 . 2 . 3 . 8 . 9 . 10		0 . 4 . 5 . 6 . 7
	3	4	0 . 3 . 4 . 7 . 8	5 . 6	1 . 2 . 9 . 10
	4	3	0 . 1 . 5 . 6 . 10	2 . 9	3 . 4 . 7 . 8
	5	9	0 . 1 . 2 . 9 . 10	4 . 7	3 . 5 . 6 . 8
	6	2	1 . 4 . 5 . 6 . 7 . 10		0 . 2 . 3 . 8 . 9
	7	8	2 . 3 . 5 . 6 . 8 . 9		0 . 1 . 4 . 7 . 10
	8	7	2 . 4 . 5 . 6 . 7 . 9		0 . 1 . 3 . 8 . 10
	9	5	0 . 2 . 4 . 7 . 9	3 . 8	1 . 5 . 6 . 10
	10	10	1 . 3 . 4 . 7 . 8 . 10		0 . 2 . 5 . 6 . 9
13	1	1	0 . 2 . 6 . 7 . 11	1 . 12	3 . 4 . 5 . 8 . 9 . 10
	2	7	1 . 4 . 5 . 8 . 9 . 12		0 . 2 . 3 . 6 . 7 . 10 . 11
	3	9	0 . 2 . 5 . 8 . 11	4 . 9	1 . 3 . 6 . 7 . 10 . 12
	4	10	0 . 1 . 4 . 9 . 12	2 . 11	3 . 5 . 6 . 7 . 8 . 10
	5	8	1 . 2 . 3 . 10 . 11 . 12		0 . 4 . 5 . 6 . 7 . 8 . 9
	6	11	3 . 4 . 6 . 7 . 9 . 10		0 . 1 . 2 . 5 . 8 . 11 . 12
	7	2	2 . 4 . 6 . 7 . 9 . 11		0 . 1 . 3 . 5 . 8 . 10 . 12
	8	5	2 . 3 . 5 . 8 . 10 . 11		0 . 1 . 4 . 6 . 7 . 9 . 12
	9	3	0 . 5 . 6 . 7 . 8	3 . 10	1 . 2 . 4 . 9 . 11 . 12
	10	4	0 . 1 . 3 . 10 . 12	6 . 7	2 . 4 . 5 . 8 . 9 . 11
	11	6	1 . 5 . 6 . 7 . 8 . 12		0 . 2 . 3 . 4 . 9 . 10 . 11
	12	12	0 . 3 . 4 . 9 . 10	5 . 8	1 . 2 . 6 . 7 . 11 . 12
17	1	1	0 . 3 . 4 . 6 . 11 . 13 . 14	1 . 16	2 . 5 . 7 . 8 . 9 . 10 . 12 . 15
	2	9	0 . 1 . 2 . 7 . 10 . 15 . 16	6 . 11	3 . 4 . 5 . 8 . 9 . 12 . 13 . 14
	3	6	1 . 2 . 4 . 6 . 11 . 13 . 15 . 16		0 . 3 . 5 . 7 . 8 . 9 . 10 . 12 . 14
	4	13	0 . 5 . 6 . 8 . 9 . 11 . 12	2 . 15	1 . 3 . 4 . 7 . 10 . 13 . 14 . 16
	5	7	1 . 2 . 3 . 8 . 9 . 14 15 . 16		0 . 4 . 5 . 6 . 7 . 10 . 11 . 12 . 13
	6.	3	2 . 5 . 6 . 7 . 10 . 11 . 12 . 15		0 . 1 . 3 . 4 . 8 . 9 . 13 . 14 . 16
	7	5	3 . 4 . 5 . 7 . 10 . 12 . 13 . 14		0 . 1 . 2 . 6 . 8 . 9 . 11 . 15 . 16
	8	15	0 . 2 . 3 . 4 . 13 . 14 . 15	5 . 12	1 . 6 . 7 . 8 . 9 . 10 . 11 . 16
	9	2	0 . 1 . 5 . 8 9 . 12 . 16	3 . 14	2 . 4 . 6 . 7 . 10 . 11 . 13 . 15
	10	12	1 . 3 . 5 . 6 . 11 . 12 . 14 . 16		0 . 2 . 4 . 7 . 8 . 9 . 10 . 13 . 15
	11	14	3 . 6 . 7 . 8 . 9 . 10 . 11 . 14		0 . 1 . 2 . 4 . 5 . 12 . 13 . 15 . 16
	12	10	2 . 4 . 5 . 8 . 9 . 12 . 13 . 15		0 . 1 . 3 . 6 . 7 . 10 . 11 . 14 . 16
	13	4	0 . 2 . 3 . 7 . 10 . 14 . 15	8 . 9	1 . 4 . 5 . 6 . 11 . 12 . 13 . 16
	14	11	1 . 4 . 7 . 8 . 9 . 10 . 13 . 16		0 . 2 . 3 . 5 . 6 . 11 . 12 . 14 . 15
	15	8	0 . 4 . 6 . 8 . 9 . 11 . 13	.7 . 10	1 . 2 . 3 . 5 . 12 . 14 . 15 . 16
	16	16	0 . 1 . 5 . 7 . 10 . 12 . 16	4 . 13	2 . 3 . 6 . 8 . 9 . 11 . 14 . 15
p	$\frac{A}{f}$	$\frac{f}{A}$	Ausgeschlossen		Zugelassen
			$fgNp$		

NACHLASS. HILFSTAFEL ZUR LÖSUNG DER GLEICHUNG

$$A = fxx + gyy.$$

Ausschluss-zahl p	$\frac{A}{f}$	$\frac{f}{A}$	$fgRp$ Zugelassen	$fgRp$	$fgRp$ Ausgeschlossen
19	1	1	0 2 . 3 . 4 . 7 . 12 . 15 . 16 . 17	1 . 18	5 . 6 . 8 9 . 10 . 11 . 13 . 14
	2	10	1 . 2 . 4 . 6 . 9 . 10 . 13 . 15 . 17 . 18		0 . 3 . 5 . 7 . 8 . 11 . 12 . 14 . 16
	3	13	4 . 5 . 6 . 7 . 9 . 10 . 12 . 13 . 14 . 15		0 . 1 . 2 . 3 . 8 . 11 . 16 . 17 . 18
	4	5	0 . 4 . 5 . 6 . 8 . 11 . 13 . 14 . 15	2 . 17	1 . 3 . 7 . 9 . 10 . 12 . 16 . 18
	5	4	0 . 1 . 2 . 6 . 8 . 11 . 13 . 17 . 18	9 . 10	3 4 . 5 . 7 . 12 . 14 . 15 . 16
	6	16	0 . 1 . 3 . 4 . 9 . 10 . 15 . 16 . 18	5 . 14	2 6 . 7 . 8 . 11 . 12 . 13 . 17
	7	11	0 . 1 . 3 . 5 . 6 . 13 . 14 . 16 . 18	8 . 11	2 . 4 . 7 . 9 . 10 . 12 . 13 . 15
	8	12	1 . 2 . 4 . 7 . 8 . 11 . 12 . 15 . 17 . 18		0 . 3 . 5 . 6 9 . 10 . 13 14 . 16
	9	17	0 . 2 . 6 . 7 . 9 . 10 . 12 . 13 . 17	3 . 16	1 . 4 . 5 . 8 . 11 . 14 . 15 . 18
	10	2	1 . 2 . 3 . 5 . 9 . 10 . 14 . 16 . 17 . 18		0 . 4 . 6 . 7 . 8 . 11 . 12 . 13 . 15
	11	7	0 . 2 5 . 8 . 9 . 10 . 11 . 14 . 17	7 . 12	1 . 3 . 4 6 . 13 . 15 . 16 . 18
	12	8	1 · 5 . 7 . 8 . 9 . 10 . 11 . 12 . 14 . 18		0 . 2 . 3 . 4 . 6 . 13 . 15 . 16 . 17
	13	3	2 . 3 . 4 . 5 . 8 . 11 . 14 . 15 . 16 . 17		0 . 1 . 6 . 7 . 9 . 10 . 12 . 13 . 18
	14	15	3 . 4 . 6 . 8 . 9 . 10 . 11 . 13 . 15 . 16		0 . 1 . 2 5 . 7 . 12 . 14 . 17 . 18
	15	14	2 . 3 . 5 . 6 . 7 . 12 . 13 . 14 . 16 . 17		0 . 1 . 4 . 8 . 9 . 10 . 11 . 15 . 18
	16	6	0 . 3 . 7 . 8 . 9 . 10 . 11 . 12 . 16	4 . 15	1 . 2 . 5 . 6 . 13 . 14 . 17 . 18
	17	9	0 . 1 . 4 . 5 . 6 . 13 . 14 . 15 . 18	6 . 13	2 . 3 . 8 . 9 . 10 . 11 . 16 . 17
	18	18	1 . 3 . 6 . 7 . 8 . 11 . 12 . 13 . 16 . 18		0 . 2 . 4 . 5 . 9 . 10 . 14 . 15 . 17
23	1	1	0.4.8.9.10.11.12.13.14.15.19	1 . 22	2 . 3 . 5 . 6 . 7 . 16 . 17 . 18 . 20 . 21
	2	12	0 . 1 . 3 . 4 . 6 9 . 14 . 17 . 19 . 20 . 22	5 . 18	2 . 7 . 8 . 10 . 11 . 12 . 13 . 15 . 16 . 21
	3	8	0 . 1 . 5 . 6 . 8 . 10 . 13 . 15 . 17 . 18 . 22	7 . 16	2 . 3 . 4 . 9 . 11 . 12 . 14 . 19 . 20 . 21
	4	6	0 . 1 . 3 . 5 . 7 . 8 . 15 . 16 . 18 . 20 . 22	2 . 21	4 . 6 . 9 . 10 . 11 . 12 . 13 . 14 . 17 . 19
	5	14	1 . 2 . 4 . 5 . 7 . 9 . 14 . 16 . 18 . 19 . 21 . 22		0 . 3 . 6 . 8 . 10 . 11 . 12 . 13 . 15 . 17 . 20
	6	4	0 . 2 . 4 . 5 . 6 . 7 . 16 . 17 . 18 . 19 . 21	11 . 12	1 . 3 . 8 . 9 . 10 . 13 . 14 . 15 . 20 . 22
	7	10	1 . 2 . 7 . 8 . 9 . 11 12 . 14 . 15 . 16 . 21 . 22		0 . 3 4 . 5 . 6 . 10 . 13 . 17 . 18 . 19 . 20
	8	3	0 . 2 . 5 . 6 . 8 . 11 . 12 . 15 17 . 18 . 21	10 . 13	1 . 3 . 4 . 7 . 9 . 14 . 16 . 19 . 20 . 22
	9	18	0 . 1 . 4 7 . 10 . 11 . 12 . 13 . 16 . 19 . 22	3 . 20	2 . 5 . 6 . 8 . 9 . 14 . 15 . 17 . 18 . 21
	10	7	1 . 2 . 3 . 5 . 10 . 11 . 12 . 13 . 18 . 20 . 21 . 22		0 . 4 . 6 . 7 . 8 . 9 . 14 . 15 . 16 . 17 . 19
	11	21	3 . 4 . 5 . 7 . 8 . 10 13 . 15 . 16 . 18 . 19 . 20		0 . 1 . 2 . 6 . 9 . 11 . 12 . 14 . 17 . 21 . 22
	12	2	0 . 2 . 3 . 7 . 10 . 11 . 12 . 13 . 16 . 20 . 21	9 . 14	1 . 4 . 5 . 6 . 8 . 15 . 17 . 18 . 19 . 22
	13	16	0 . 1 . 2 . 3 . 8 . 9 . 14 . 15 . 20 . 21 . 22	6 . 17	4 . 5 . 7 . 10 . 11 . 12 . 13 . 16 . 18 . 19
	14	5	1 . 5 . 6 . 9 . 10 11 . 12 . 13 14 . 17 . 18 . 22		0 . 2 . 3 . 4 . 7 . 8 . 15 . 16 . 19 . 20 . 21
	15	20	3 . 5 . 6 . 7 . 9 . 11 . 12 . 14 . 16 . 17 . 18 . 20		0 . 1 . 2 . 4 . 8 . 10 . 13 15 . 19 . 21 . 22
	16	13	0 . 2 . 6 . 7 . 9 . 10 . 13 . 14 . 16 . 17 21	4 . 19	1 . 3 . 5 . 8 . 11 . 12 . 15 . 18 . 20 . 22
	17	19	1 . 2 . 3 . 4 . 6 . 10 . 13 . 17 . 19 . 20 . 21 . 22		0 . 5 . 7 . 8 . 9 . 11 . 12 . 14 . 15 . 16 . 18
	18	9	0 . 3 . 4 . 5 . 9 . 11 . 12 . 14 . 18 . 19 . 20	8 . 15	1 . 2 . 6 . 7 . 10 . 13 . 16 . 17 . 21 . 22
	19	17	1 . 4 . 6 . 7 . 8 . 11 . 12 . 15 . 16 . 17 . 19 . 22		0 . 2 . 3 . 5 . 9 . 10 . 13 . 14 . 18 . 20 . 21
	20	15	2 . 4 . 5 . 8 . 9 . 10 . 13 . 14 . 15 . 18 19 . 21		0 . 1 . 3 . 6 . 7 . 11 . 12 . 16 . 17 . 20 . 22
	21	11	3 . 6 . 7 . 8 . 9 . 10 . 13 . 14 . 15 . 16 . 17 . 20		0 . 1 . 2 . 4 . 5 . 11 . 12 . 18 . 19 . 21 . 22
	22	22	2 . 3 . 4 . 6 8 . 11 . 12 . 15 . 17 . 19 . 20 . 21		0 . 1 . 5 . 7 . 9 . 10 . 13 . 14 . 16 . 18 . 22

p	$\frac{A}{f}$	$\frac{f}{A}$	Ausgeschlossen	$fgNp$	Zugelassen

ACHTER ABSCHNITT.

AUSFÜHRLICHERE BETRACHTUNG EINIGER UNTERSUCHUNGEN ZUR KREISTEILUNG.

367.

Was wir im späteren Teil des siebten Abschnitts von Artikel 355 an dargelegt haben, gibt gewiss gewichtige Beispiele für die große Fruchtbarkeit der Theorie der Kreisteilung und für den erstaunlichen Zusammenhang, der dieses Gebiet mit verschiedenen *arithmetischen* Untersuchungen verbindet. Wegen der allzu engen Grenzen von Raum und Zeit konnten wir dieses Feld dort jedoch nur leicht berühren; je weiter wir darin vordringen, desto reicher ist die Ernte, mit der es unsere Bemühungen belohnt. Deshalb wollen wir hier die eine oder andere der dort begonnenen Fragen erneut aufnehmen und ausführlicher behandeln: Die Leser werden gewiss mit großem Staunen sehen, dass die Lösung mehrerer arithmetischer Probleme, die jeder für himmelweit von diesem Gebiet entfernt gehalten hätte, auf dieser Grundlage beruht.

368.

Ein besonders fruchtbares Thema bietet die in Artikel 356 begonnene Untersuchung. Dort teilten wir die Gesamtheit der Wurzeln der Gleichung $x^n - 1 = 0$ (ohne eins) in zwei Klassen und zeigten, wie die Summe in jeder Klasse zu bestimmen ist. Dabei ergaben sich $= -\frac{1}{2} + \frac{1}{2}\sqrt{n}$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{n}$ für den Fall, dass n die Form $4n+1$ hat, oder $= -\frac{1}{2} + \frac{1}{2}\sqrt{-n}$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{-n}$ für den Fall, dass n die Form $4n+3$ hat. Wir hatten uns dort aber nicht nur auf den Fall beschränkt, dass n eine *Primzahl* ist, sondern auch, was noch viel schwerer wog, das *Vorzeichen* des Wurzelausdrucks unbestimmt gelassen oder vielmehr versäumt, diese mit wenigen Worten angedeutete Bestimmung durch einen festen Beweis zu stützen. Diese Mängel müssen wir daher vor allem anderen beheben.

.369.

Nun sei n eine beliebige positive ganze Zahl und R eine Wurzel der Gleichung $x^n - 1. = 0$, deren Potenzen vor der Potenz mit Exponenten n sämtlich von eins verschieden sind (siehe Artikel 359, II.). Wie in Abschnitt VII bezeichnen wir mit $[\lambda]$ die Potenz R^λ, sodass $[0] = 1$, $[1]$, $[2]$, $[3] \ldots . [n-1]$ alle Wurzeln der Gleichung $x^n - 1 = 0$ darstellen. Ferner bezeichnen wir die Summe

$$[0] + [1] + [4] + [9] + \ldots . + [(n-1)^2] \quad \text{mit } \Sigma[\mathfrak{Q}]$$

und allgemeiner

$$[0] + [\lambda] + [4\lambda] + [9\lambda] \ldots . + [\lambda(n-1)^2] \quad \text{mit } \Sigma[\mathfrak{Q}\lambda]$$

Dabei bezeichnet $\mathfrak{Q}$ ohne nähere Festlegung die Quadrate der Zahlen $0, 1, 2, 3 \ldots . n-1$. Wie allgemein $[\lambda] = [\mu]$ gilt, wenn λ, μ beliebige (positive oder negative) ganze Zahlen sind, die modulo n kongruent sind, so gilt offenbar auch $\Sigma[\mathfrak{Q}\lambda] = \Sigma[\mathfrak{Q}\mu]$, wenn $\lambda \equiv \mu$. Nach diesen Vorbereitungen erhalten wir Folgendes.

370.

Aufgabe. *Das Produkt der beiden Summen* $\Sigma[\mathfrak{Q}]$ *und* $\Sigma[-\mathfrak{Q}]$ *bestimmen.*
Lösung. Wegen $nn \equiv 0$, $(n+1)^2 \equiv 1$, $(n+2)^2 \equiv 4$ usw. (mod.n) ergibt sich leicht, dass $\Sigma[\mathfrak{Q}]$ wird

$$\begin{aligned} &= [1] + [4] + [9] + [16] \ldots . + [nn] \\ &= [4] + [9] + [16] + [25] \ldots . + [(n+1)]^2 \\ &= [9] + [16] + [25] + [36] \ldots . + [(n+2)^2] \end{aligned}$$

usw. oder allgemein

$$= [kk] + [(k+1)^2] + [(k+2)^2] + [(k+3)^2] \ldots . + [(n+k-1)^2]$$

Daraus folgt für $[-kk] \times \Sigma[\mathfrak{Q}]$

$$= [0] + [2k+1] + [4k+4] + [6k+9] \ldots . + [(n-1)^2 + 2(n-1)k]$$

Damit entwickelt sich $\Sigma[-\mathfrak{Q}] \times \Sigma[\mathfrak{Q}]$ zu

$$\begin{aligned} &- [0] + [1] + [4] + [9] \ldots . + [(n-1)^2] \\ &+ [0] + [3] + [8] + [15] \ldots . + [nn-1] \\ &+ [0] + [5] + [12] + [21] \ldots . + [nn+2n-3] \\ &+ [0] + [7] + [16] + [27] \ldots . + [nn+4n-5] \\ &+ \text{usw.} \\ &+ [0] + [2n-1] + [4n] + [6n+3] \ldots . + [3nn-6n+3] \end{aligned}$$

Addiert man diese Teile *spaltenweise*, so erhält man

$$\begin{aligned} n[0] + [1] \times \frac{1-[2n]}{1-[2]} + [4]\frac{1-[4n]}{1-[4]} + [9]\frac{1-[6n]}{1-[6]} \\ + \text{usw.} + [(n-1)^2] \times \frac{1-[2nn-2n]}{1-[2n-2]} \end{aligned}$$

In diesem Ausdruck verschwinden alle Teile außer dem ersten, wenn n ungerade ist; denn dann werden $1-[2n]$, $1-[4n]$, $1-[6n]$ usw. sämtlich $= 0$, dagegen keiner der Nenner $1-[2]$, $1-[4]$, $1-[6]$, $1-[8]$ usw. bis $1-[2n-2]$. Ist n hingegen gerade, so ist auch einer der Nenner $= 0$, nämlich $1-[n]$, dem der

Term $[\frac{1}{4}nn] \times \frac{1-[nn]}{1-[n]}$ entspricht; die Summe der Teile, aus denen dieser entstanden ist, wird jedoch $= n[\frac{1}{4}nn]$. Hier sind erneut zwei Fälle zu unterscheiden. Ist n durch vier teilbar, so gilt $\frac{1}{4}nn \equiv 0 \,(\mathrm{mod}.n)$ und daher $[\frac{1}{4}nn] = 1$; ist n dagegen das Doppelte einer ungeraden Zahl, so gilt $\frac{1}{4}nn \equiv \frac{1}{2}n \,(\mathrm{mod}.n)$ und daher notwendig $[\frac{1}{4}nn] = -1$. Schließlich folgt daraus

1) für einen ungeraden Wert von n ist das gesuchte Produkt $= n$

2) für einen durch vier teilbaren Wert ist das Produkt $= 2n$

3) für einen Wert, der das Doppelte einer ungeraden Zahl ist, ist es $= 0$.

Q. E. I.

371.

Es lohnt sich nun, die Beschaffenheit der Summe $\Sigma[\mathfrak{Q}]$ näher zu betrachten.

I. Da man die Quadrate 0, 1, 4, 9, 16 usw. durch ihre kleinsten Reste modulo n ersetzen darf, gilt offenbar: Bezeichnet M ohne nähere Festlegung die quadratischen Reste der Zahl n von 0 bis $n-1$ und m die Anzahl der Wurzeln der Kongruenz $xx \equiv M(\mathrm{mod}.m)$, so ist $\Sigma[\mathfrak{Q}] = \Sigma m[M]$. Wie die Zahl m zu bestimmen ist, haben wir in den Artikeln 104, 105 gezeigt.

II. Ist n eine (ungerade) Primzahl, so gilt für $M = 0$ die Gleichung $m = 1$, für jeden anderen Wert von M hingegen $m = 2$. Ist n eine Potenz einer ungeraden Primzahl $= p^\nu$, so gilt $m = 2$ für jeden Wert von M, der nicht durch p teilbar ist —

— — — — — — — — — — — — — — — — —

372.

Ist n eine (ungerade) Primzahl, so bestehen die Reste m aus null, wofür $M = 1$ gilt, und $\frac{1}{2}(n-1)$ anderen Zahlen, für die $M = 2$ gilt. Bezeichnen wir diese Reste (ohne den Rest 0) ohne nähere Festlegung mit μ, so ist unsere Folge $= 1 + 2\Sigma r^\mu$. Bezeichnet ferner ν ohne nähere Festlegung alle übrigen Zahlen unter n, deren Anzahl ebenfalls $\frac{1}{2}(n-1)$ ist und die alle quadratischen Nichtreste von n unter n umfassen, so gilt offenbar

$$1 + \Sigma r^\mu + \Sigma r^\nu = 1 + r + rr + r^3 \ldots . + r^{n-1} = \frac{1 - r^n}{1 - r} = 0$$

Setzen wir also die Summe unserer Folge, das heißt $1 + 2\Sigma r^\mu = A$, so gilt $1 + 2\Sigma r^\nu = -A$ und außerdem $\Sigma r^\mu - \Sigma r^\nu = A$.

Nach Artikel 356 gilt daher $A = \pm\sqrt{n}$ oder $\pm\sqrt{-n}$, je nachdem, ob n die Kongruenz $\equiv 1$ oder $\equiv 3 \,(\mathrm{mod}.4)$ erfüllt. Das Vorzeichen der Wurzel ist dadurch aber noch nicht bestimmt.

Ersetzt man in unserer Folge, die wir mit Π bezeichnen wollen, r durch eine andere gleichartige Wurzel der Gleichung $x^n - 1 = 0$, etwa $r' = r^\lambda$, so sei Π' das Ergebnis.

373.

Ist n das Quadrat oder eine höhere Potenz einer Primzahl, etwa $= p^\pi$, so bestehen einige Reste m aus nicht durch p teilbaren Zahlen; andere sind durch pp, aber nicht durch eine höhere Potenz von p teilbar; wieder andere lassen sich durch p^4, aber nicht. durch p^5 teilen, und so weiter bis zu denen, die durch $p^{\pi-2}$, aber nicht durch $p^{\pi-1}$ oder durch $p^{\pi-1}$, aber nicht durch p^π teilbar sind, je nachdem, ob π gerade oder ungerade ist. Schließlich kommt der Rest 0 hinzu, der einzige durch p^π teilbare Rest (vgl. Artikel 102). Bezeichnen wir nun ohne nähere Festlegung mit μ die quadratischen Reste der Zahl p unter p ohne null (deren Anzahl $= \frac{1}{2}(p-1)$ ist), so lassen sich diese verschiedenen Restklassen wie folgt darstellen. Die ersten, die nicht durch p teilbar sind, werden durch $\mu + kp$ dargestellt; dabei sind für k alle ganzen Zahlen von 0 bis $p^{\pi-1} - 1$ einzusetzen, sodass die Anzahl aller in dieser Form enthaltenen Reste $= \frac{1}{2}(p-1)p^{\pi-1}$ ist; für jeden von ihnen gilt $M = 2$. Die Summe aller diesen Resten entsprechenden Terme in Π ist

$$= 2\Sigma r^{\mu+kp} = 2\Sigma r^\mu \,.\, \Sigma r^{kp}$$
$$= 2\Sigma r^\mu \,.\, \frac{r^{p^\pi} - 1}{r^p - 1} = 0$$

Die zweite Klasse der Reste wird durch $\mu pp + kp^3$ dargestellt; dabei sind für k alle ganzen Zahlen von 0 bis $p^{\pi-3} - 1$ einzusetzen, sodass die Anzahl aller in dieser Form enthaltenen Reste $= \frac{1}{2}(p-1)p^{\pi-3}$ ist; für jeden von ihnen gilt jedoch $M = 2p$. Die Summe der daraus entstehenden Terme in Π wird

$$= 2p\Sigma r^{\mu pp+kp^3} = 2p\Sigma r^{\mu pp} \,.\, \Sigma r^{kp^3}$$
$$= 2p\Sigma r^{\mu pp} \,.\, \frac{r^{p^\pi} - 1}{r^{p^3} - 1} = 0$$

vorausgesetzt, dass $\pi > 3$. Ebenso wird die dritte, vierte usw. Klasse durch $\mu p^4 + kp^5$, $\mu p^6 + kp^7$ usw. dargestellt, wobei für k alle ganzen Zahlen von 0 bis $p^{\pi-5} - 1$, $p^{\pi-7} - 1$ usw. zu nehmen sind; für diese gilt $M = 2pp$, $M = 2p^3$ usw. Die Summe der aus der dritten, vierten usw. Klasse entstehenden Terme in Π verschwindet, sofern jeweils $\pi > 5$, $\pi > 7$ usw.. gilt.

Daraus folgt für den Fall, dass π gerade ist: In Π bleiben nur die dem Rest 0 entsprechenden Terme übrig, die $= 1$ sind; für diese gilt aber $M = p^{\frac{1}{2}\pi}$, sodass die Summe aller Terme in $\Pi = p^{\frac{1}{2}\pi}$ wird.

GAUSS AN DIRICHLET.

An Herrn
Herrn Lejeune Dirichlet in Paris.

Schon früher hätte ich Ihnen meinen Dank für die mir so freundlich übersandte Abhandlung und die große Freude, die Sie mir damit bereitet haben, ausgesprochen, wenn ich nicht zunächst etwas über den Erfolg dessen hätte erfahren wollen, was ich in Berlin im Hinblick auf Ihre Wünsche und, wie ich hinzufügen kann, meine eigenen zu tun versucht habe. Ich freue mich außerordentlich, jetzt aus einem Brief des Sekretärs der Akademie in Berlin zu erfahren, dass wir hoffen können, man werde Ihnen bald im Vaterland eine angemessene feste Stelle verschaffen wollen.

Je seltener diese Neigung ist, desto mehr freut es mich, dass Sie sich dem Teil der Mathematik so stark verbunden fühlen, der seit jeher mein Lieblingsstudium ist. Ich wünsche Ihnen von Herzen äußere Verhältnisse, unter denen Sie möglichst weitgehend Herr Ihrer Zeit und der Wahl Ihrer Arbeiten bleiben. Mich selbst hinderten gleich nach dem Erscheinen meiner Disquisitiones andersartige Beschäftigungen und später meine äußeren Verhältnisse sehr daran, meiner Neigung in dem gewünschten Maß zu folgen. Statt eines zweiten Teils dieses Werks, den ich früher beabsichtigte, werde ich mich aller Wahrscheinlichkeit nach darauf beschränken müssen, von Zeit zu Zeit eine Abhandlung über einen einzelnen Gegenstand vorzulegen. Die drei bisher erschienenen Abhandlungen dieser Art im 16. Band der hiesigen Commentationen und im ersten und vierten Band der Commentationes recentiores enthalten jedoch (abgesehen von einem Teil der zweiten) keine der Fragen, die ich schon 1801 für die Fortsetzung im Blick hatte, sondern neue. Auch meine späteren Arbeiten dieser Art betreffen daher einen neuen Gegenstand, nämlich die Theorie der biquadratischen Reste, die ich in etwa drei Abhandlungen darzustellen denke. Die erste davon wird bald für den sechsten Band der Comment. rec. gedruckt werden; die Hauptmaterialien für das Übrige sowie für die ähnliche Theorie der kubischen Reste sind im Wesentlichen als erledigt anzusehen, obwohl davon noch wenig ordentlich zu Papier gebracht ist.

Empfehlen Sie mich bitte Herrn von Humboldt, falls er noch in Paris ist, und entschuldigen Sie, dass ich ihm jetzt nicht selbst schreibe, mit meiner Sorge, mein Brief könnte ihn nicht erreichen, da er, wie ich höre, Paris verlassen wollte.

Mit aufrichtiger Hochschätzung

Ihr ergebenster

Göttingen, den 13. September 1826. C. F. Gauss.

Für Ihren freundlichen Brief und die freundliche Übersendung Ihrer beiden Abhandlungen danke ich Ihnen, mein sehr geschätzter Freund, aufs Verbindlichste. Mit Freude sehe ich das wachsende Interesse, das man jetzt den Untersuchungen der höheren Arithmetik entgegenzubringen beginnt. Die gelungene Art, wie Sie das Zweite über die biquadratische Residualität der Zahl 2 aus dem Ersten ableiten, hat mir sehr gefallen.

Vermutlich hat der 6. Band unserer Commentationen jetzt Breslau erreicht, sodass Ihnen meine Commentatio prima über die biquadratischen Reste inzwischen wohl bekannt ist. Bei einer passenden Gelegenheit würde ich Ihnen auch gern einen Sonderabdruck übersenden. Für das darin vorkommende Theorem hätte ich zwischen mehreren Beweisarten wählen können; Ihnen wird aber nicht entgehen, warum ich hier den dort ausgeführten Beweis vorgezogen habe: vor allem deshalb, weil die Einordnung von 2 bei den Moduln, für die es quadratischer Nichtrest ist (unter B oder D), als wesentlicher Bestandteil des Theorems gelten muss, auf den die meisten anderen Beweisarten nicht anwendbar scheinen.

Die ganze Untersuchung, deren Stoff ich schon seit 23 Jahren vollständig besitze, die Beweise der Haupttheoreme (zu denen das Theorem in der ersten Abhandlung noch *nicht* zu rechnen ist) aber seit etwa 14 Jahren — (wobei ich wünsche und hoffe, an Letzteren, den Beweisen, noch einiges vereinfachen zu können) —, habe ich auf ungefähr 3 Abhandlungen angelegt. Mit der Abfassung der zweiten habe ich bereits begonnen und hoffe, sie bald zu vollenden, sofern die mir neuerdings wieder übertragenen Vermessungsarbeiten dabei nicht noch eine Verzögerung verursachen.

Das Schlusstheorem $b \equiv \frac{1}{2}rr \pmod{p}$ hatte ich schon vor drei Jahren ebenfalls in den hiesigen gel. Anzeigen bekannt gemacht und auf den merkwürdigen Knoten hingewiesen, der dabei noch zu lösen war; bisher habe ich aber nicht gehört, dass jemand einen Versuch dazu unternommen hätte. Vor einigen Tagen ist mir nun die Lösung für die *eine Hälfte* tatsächlich gelungen. Dieser Fund hat mir umso mehr Freude gemacht, als er sich überhaupt nicht auf Induktion stützt — denn ich gestehe, dass ich gerade *diesen* Zusammenhang nicht erwartet hätte —, sondern a priori auf die Verbindung anderer *sehr verschlungener* und interessanter, schon 28 Jahre alter, aber noch völlig unveröffentlichter Untersuchungen, die in der Schlussanmerkung der Disquis. Arithm. S. 668 [Gauss Werke Bd. I. S. 466] leicht angedeutet sind.

Es handelt sich dabei um ein ausreichendes Kriterium für den Fall, dass p die Form $8n + 5$ hat.

Die Anzahl der Klassen, welche die binären Formen in jeder der beiden Gattungen für die Determinante $-p$ bilden, sei $= k$. Der Anfang einer von mir bis zur Determinante -3000 aufgestellten Tafel steht in Disquis. Arithm. S. 520. [Art. 303.] Außerdem ist zu beachten, dass für ein p der angenommenen Form stets $k = 2m + 1$ gilt, wenn m die Anzahl der Zerlegungen von p in drei positive Quadrate bezeichnet (ich sage positive, um 0 auszuschließen). Dies

hat LEGENDRE durch Induktion gefunden; in den Disquis. Arithm. wurde es erstmals aus der Theorie der *ternären* Formen bewiesen. Es gilt zum Beispiel

für $p=$	5,	13,	29,	37,	53,	61,	101,	109,	149,	157	usw.
$k=$	1,	1,	3,	1,	3,	3,	7,	3,	7,	3	
$m=$	0,	0,	1,	0,	1,	1,	3,	1,	3,	1	
			4		1	9	1 4 16	9	1 4 36	4	
			9		16	16	36 16 36	36	4 64 64	9	
			16		36	36	64 81 49	64	144 81 49	144	

Unter dieser Voraussetzung ist der Wert von b, der $\equiv \frac{1}{2}rr \,(\mathrm{mod}.p)$ ist, stets

$$\equiv 2k + a - 1 \equiv 4m + a + 1 \;(\mathrm{mod}.8)$$

Dadurch ist das Vorzeichen von b vollständig bestimmt. Hier sehen Sie 22 Beispiele; damit verdopple ich den Umfang der am Ende der Abhandlung gegebenen Tafel.

p	k	a	b	p	k	a	b
5	1	+1	+2	181	5	+9	+10
13	1	−3	−2	197	5	+1	−14
29	3	+5	+2	229	5	−15	+2
37	1	+1	−6	269	11	+13	+10
53	3	−7	−2	277	3	+9	+14
61	3	+5	−6	293	9	+17	+2
101	7	+1	−10	317	5	−11	+14
109	3	−3	+10	349	7	+5	+18
149	7	−7	−10	373	5	−7	+18
157	3	−11	−6	389	11	+17	−10
173	7	+13	+2	397	3	−19	−6

Die Vorschrift lässt sich also auch so ausdrücken; (stets unter der Voraussetzung $p \equiv 5 \;(\mathrm{mod}.8)$)

$$\begin{aligned} &\text{Es ist } b \equiv a + 1 \;(\mathrm{mod}.8), && \text{wenn } m \text{ gerade} \\ &\qquad b \equiv a + 5 && \text{wenn } m \text{ ungerade.} \end{aligned}$$

Ich wage noch keine Vermutung darüber, ob ein noch einfacheres Kriterium möglich ist, mit dem sich der Fall des geraden m von dem ungeraden Fall *im Voraus* unterscheiden ließe, also ohne den Wert von m selbst zu kennen, da diese Verbindung, wie ich schon oben bemerkt habe, noch ganz neu ist.

Für den Fall $p \equiv 1 \pmod{8}$ bleibt zwar die obige Kongruenz $b \equiv 2k + a - 1 \pmod{8}$ richtig, sie entscheidet aber nicht mehr über das Vorzeichen von b, da sowohl der positive als auch der negative Wert von b ihr genügt. Hier ist nämlich k immer gerade, $= 2m$ (wenn m dieselbe Bedeutung wie oben hat) oder $= 2m + 2$, wenn m die Anzahl der Zerlegungen von p in 3 positive *ungleiche* Quadrate bezeichnet, und $b \equiv 0 \pmod{4}$ oder $b \equiv -b \pmod{8}$. Ich vermute, dass der Fall $p \equiv 1 \pmod{8}$ oder $b \equiv 0 \pmod{4}$ einer tieferen Untersuchung bedarf und vielleicht wiederum

$$b \equiv 4 \pmod{8} \quad \text{leichter als } b \equiv 0 \pmod{8}$$
$$b \equiv 8 \pmod{16} \quad \text{leichter als } b \equiv 0 \pmod{16}$$

usw.

Mit ausgezeichneter Hochachtung beharre ich

Ihr freundschaftlich ergebenster

Göttingen, den 30. Mai 1828. C. F. Gauss.

BEMERKUNGEN.

In diesen zweiten Band von Gauss' Werken habe ich alle Abhandlungen, Aufsätze und Tafeln aus dem Gebiet der höheren Arithmetik aufgenommen, soweit sie nicht schon in den sieben Abschnitten der *Disqu. Arithm.* enthalten sind: die fünf in den '*Commentationes societatis regiae scientiarum Gottingensis*' (in Quart) veröffentlichten Abhandlungen, die in den '*Göttingischen Gelehrten Anzeigen*' (in Oktav) erschienenen Besprechungen sowohl dieser eigenen als auch einiger fremder Schriften (von Gauss nicht unterzeichnet, aber durch die Akten der Göttinger Universitätsbibliothek als seine Arbeiten bestätigt), sowie eine Auswahl aus dem handschriftlichen Nachlass.

Beim zweiten Abdruck habe ich noch die Tafeln 'Circuli quadratura nova', 'Zur Berechnung der Logarithmen', 'Quadratorum myrias prima', 'Indizes der Primzahlen im höheren Zahlenbereich', 'Hilfstafel zur Lösung der unbestimmten Gleichung $A = fxx + gyy$ mit dem Ausschlussverfahren', ferner 'Sectio octava', soweit sie niedergeschrieben ist, und schließlich zwei Briefe von Gauss an Dirichlet als wesentliche Stücke der Geschichte der höheren Arithmetik hinzugefügt.

Damit die Gegenstände in einem so umfangreichen Band leichter zu überblicken sind, werden die Lehrsätze einheitlich durch den Druck hervorgehoben. Um den Gebrauch sowohl der älteren Ausgaben als auch der vorliegenden zu erleichtern, sind bei Verweisen auf die Disq. Arithm. die Seitenzahlen durch die Artikelnummern ersetzt, bei Angaben von Abhandlungen die Veröffentlichungsorte durch die eigenen Titel. Die Anmerkung, die ursprünglich Artikel 2 der Abhandlung '*Theorematis arithmetici demonstratio nova*' beigegeben war und eine Berichtigung von Artikel 139 der Disqu. Arithm. enthielt, ist dort an der betreffenden Stelle eingefügt. Die Anmerkung auf Seite 91 ist einer handschriftlichen Notiz entnommen. Im Übrigen unterscheidet sich die vorliegende Ausgabe von den früheren nur durch die Berichtigung einiger Druckfehler. Die von mir hinzugefügten Einschaltungen sind durch eckige Klammern [ ] gekennzeichnet.

Die *Tafel des quadratischen Charakters der Primzahlen* ist nach dem Muster der Tabula II der Disqu. Arithm. gedruckt, die in Artikel 99 beschrieben und (in Artikel 331) vorzugsweise zur Zerlegung von Zahlen verwendet wird. Die Schriftzüge der Handschrift mit dem Titel '*Quadratorum numeris primis divisorum residua lateralia*' ähneln am meisten denen des zweiten Teils der Tafel zur Umwandlung gemeiner Brüche in Dezimalbrüche. Anstelle der waagerechten Striche, die einen quadratischen Rest anzeigen, enthält sie kleine Kreise; diejenigen in benachbarten waagerechten oder senkrechten Reihen sind jeweils durch Linien verbunden. Bei der Korrektur fielen mir mehrere Fehler auf. Bei einer einmaligen Vergleichung mit Jacobi's *Canon Arithme-*

ticus fand ich dann 190 Abweichungen in den angegebenen Charakteren und durch direkte Bestimmung Übereinstimmung mit jenen gedruckten Tafeln. Entsprechend ist die Ausgabe hier berichtigt.

Der erste Teil der *Tafel zur Umwandlung gemeiner Brüche in Dezimalbrüche* ist hier ähnlich wie Tabula III der Disqu. Arithm. eingerichtet. Er enthält für die Primzahlen und ihre Potenzen p^π zwischen 3 und 463 die Mantissen (1), (2)..(0) der Dezimalbrüche von $\frac{10.r}{p^\pi}$, $\frac{10.rr}{p^\pi}$..$\frac{10}{p^\pi}$. Dabei bedeutet r die Einheit, sodass (1) = (2) = ..(0) gilt, wenn 10 eine Primitivwurzel von p^π ist; andernfalls bezeichnet r die kleinste derjenigen Primitivwurzeln von p^π, für die als Basis der Index von 10 seinen kleinsten Wert annimmt. Die von 1 verschiedenen Werte von r habe ich zur Erleichterung des Gebrauchs auf Seite 420 der Tafel beigefügt. Die Handschrift, die auch noch nicht die Unterscheidungsziffern der verschiedenen Perioden enthält, ähnelt äußerlich am meisten der Analysis residuorum und scheint zeitlich vor dem hier als zweiten Teil der ganzen Tafel angeordneten Stück zu liegen. Dieser zweite Teil enthält für die Primzahlen und ihre Potenz p^π zwischen 467 und 997 die Mantissen der Dezimalbrüche von $\frac{100}{p^\pi}$. Die Handschrift gibt die Teiler in absteigender Reihenfolge an und schließt mit den Worten: *Explicitus October* 11. 1795. Im Druck habe ich beim Teiler 191 in Periode (1) die 71. Ziffer hinzugefügt und beim Teiler 829 eine Zahl zwischen der 151. und 152. Ziffer weggelassen.

Der erste Teil der *Tafel der Häufigkeit der Primzahlen*, die Gauss selbst in einem Brief (Seite 444) erläutert, gibt die Anzahl der Primzahlen in jeder der ersten 1000 Tausendergruppen an und liegt in einer Handschrift von Gauss vor. Im Nachlass fehlen jedoch die im Brief angedeuteten Abzählungen der Hundertergruppen der ersten Million, die eine bestimmte Anzahl von Primzahlen enthalten. Der andere Teil der Tafel, für die zweite und dritte Million, stammt aus einer Handschrift von Goldschmidt allein. Herr Meissel hat durch Abzählung und durch seine Formel die folgenden Berichtigungen zu Seite 436 und 437 gefunden:

Tausender-gruppe	Gauss	Wahrer Wert	Tausender-gruppe	Gauss	Wahrer Wert
20	102	104	546	68	69
159	87	77	601	75	76
199	96	86	625	68	78
206	85	83	668	73	74
245	78	88	675	69	73
289	85	77	784	74	75
290	84	85	800	81	71
334	80	81	879	68	78
352	80	81	985	74	70
501	78	79			

Die im Brief von Gauss an Encke erwähnte Formel Encke's scheint die folgende

$$\frac{n}{\log n} \sqrt[2\log n]{10}$$

zu sein, die Encke in einem Brief an Gauss vom 4. Dezember 1849 mitteilt.

Die *Tafel der Anzahl der Klassen binärer quadratischer Formen* gibt die Anzahl der Geschlechter und Klassen sowie den Index der Irregularität für die negativen Determinanten in den Hundertergruppen 1 bis 30, 43, 51, 61, 62, 63, 91 bis 100, 117 bis 120 an; ferner in einer gesonderten Zusammenstellung für die der 1., 3. und 10. Tausendergruppe, für die ersten 800 der Formen $-(15n+7)$ und $-(15n+13)$ sowie für einige sehr große Determinanten; außerdem für die positiven Determinanten der 1., 2., 3., 9. und 10. Hundertergruppe und für einige weitere. Die Handschrift besteht aus einzelnen Zetteln mit unterschiedlich eingerichteten Tafeln. So steht bei den älteren das Wort Ordo anstelle von Genus, bei den einzelnen Hundertergruppen mit Ausnahme der 9. und 10. positiver Determinanten, aber auch bei einzelnen vorläufigen Zusammenstellungen in Tausendergruppen. Zur besseren Übersicht ist hier durchweg die Bezeichnung der Disqu. Arithm. gewählt. Aus Platzmangel stehen die größten und kleinsten Quotienten der Klassenanzahl geteilt durch die Determinante sowie die Anzahl der Determinanten, deren Quotient innerhalb bestimmter Grenzen liegt, nicht unter den einzelnen Hundertergruppen, sondern zusammen am Ende der Tafel für die negativen Determinanten. Einige erhaltene Aufzeichnungen scheinen darauf hinzudeuten, dass Gauss zunächst die Klassen für diejenigen Determinanten berechnet hat, die derselben Hundertergruppe und demselben Rest beim Teiler 15 angehören. Die Determinanten dieser Abteilungen wurden dann nach der Anzahl der Geschlechter und Klassen geordnet, zuletzt alle derselben Hundertergruppe angehörigen auf die hier wiedergegebene Weise. In die Tafeln der einzelnen Hundertergruppen sind manche spätere Berichtigungen eingefügt, nicht aber in die Zusammenstellungen in Tausendergruppen. Datierungen enthalten nur die beiden Tafeln mit den Determinanten der Formen $-(15n+7)$ und $-(15n+13)$, und zwar entsprechend '*Expl. In. Febr. 1801*' und '*Expl. 27 Febr. 1807.*'

In diesen Tafeln habe ich unter anderem die folgenden Fehler bemerkt. Zur leichteren Kontrolle füge ich die Periodenzahlen der Fundamentalklassen hinzu, etwa 4 . 4 . 2 bei der Determinante -11713 sowie die Zahlen, die durch Formen der jeweiligen Fundamentalklassen dargestellt werden, etwa 31 . 37 . 2. Wie in meiner Abhandlung in Band 14 der Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen sind dabei als Fundamentalklassen solche Klassen genommen, die zusammen mit den Klassen ihrer Perioden durch Komposition jede eigentlich primitive Klasse der Determinante einmal und nur einmal erzeugen.

Die folgenden Angaben sind bereits weggelassen:

Hundertergruppe 9	G. IV ...	3.,	$-827[21 :: 3]$
26	IV	14	$-2587[24 :: 11]$
26	VIII	6	$-2564[56 :: 3]$
91	I	111	$-9059[117 :: 5]$
120	IV	32	$-11956^{*}2^{*}[36 . 2 :: 11 . 49]$
1	I	2	$+37[3 :: 3]$
2	I	2	$+101[3 :: 4]$

und hinzugefügt:

Hundertergruppe 9	G. IV ...	3..	$-828[6 . 2 :: 31 . 23]$
26	IV	14	$-2586[28 . 2 :: 7 . 2]$
26	VIII	6	$-2565[12 . 2 . 2 :: 7 . 2 . 5]$
91	I	117	$-9059[117 :: 5]$
120	IV	32	$-11966^{*}2^{*}[32 . 4 :: 5 . 83]$
1	I	3	$+37[3 :: 3]$
2	I	3	$+101[3 :: 4]$

Bei der Tafel für Hundertergruppe 3 und der letzten auf Seite 476, die in der Handschrift zusammen mit einer äußerlich anders als hier gedruckt eingerichteten Aufzeichnung der Hundertergruppen 1 und 2 vorkommen, sind die zwölf Abteilungen statt mit I. Ordo unicus. 1; I. O. 2; I. O. 3; I. O. 4; II. Ordines duo. 1. 1; II. O. 1. 2; II. O. 2. 2; II. O. 3. 3; III. Ordines quatuor. 1. 1. 1. 1; III. O. 1. 1. 2. 2; III. O. 2. 2. 2. 2; IV. Ordines octo 1. 1. 1. 1. 1. 1. 1. 1; hier auf die sonst verwendete Weise mit G. I. 1; G. I. 3; G. I. 5; G. I. 7; G. II. 1; G. II. 2; G. II. 3; G. II. 5; G. IV. 1; G. IV. 2; G. IV. 3; G. VIII. 1; bezeichnet. Die Rechnung ergibt nämlich etwa 269. I. 3 [3 :: 4]; 235. IV. 3 [6 . 2 :: 3 . 5]; 401. I. 5 [5 :: 9]; 577. I. 7 [7 :: 3]; 727. II. 5 [10 :: 3]. (Genera I statt Genus I auf Seite 469 ist ein Druckfehler).

Wegen Druckfehlern ist wegzulassen:

Hundertergruppe 27.	G. IV	16...	$-2624^{*}3^{*}$
93	IV	16	-9216
118	VIII	4	$-11713^{*}3^{*}$

und hinzuzufügen:

Hundertergruppe 27.	G. IV	16...	$-2624^{*}2^{*}[16 . 4 :: 3 . 16]$
93	IV	16	$-9216^{*}2^{*}[16 . 4 :: 5 . 9]$
118	VIII	4	$-11713^{*}2^{*}[4 . 4 . 2 :: 31 . 37 . 2]$

Nach meiner Berechnung ist außerdem wegzulassen:

Hundertergruppe 10.	G. II	9 ...	$-972[6 . 3 :: 7 . 13]$
17	IV	4	$-1660[10 . 2 :: 11 . 5]$
20	IV	12	$-1982[24 :: 3]$
21	IV	6	$-2096[30 . 2 :: 3 . 4]$
23	IV	9	$-2221[18 :: 10]$
24	IV	12	$-2376[12 . 2 . 2 :: 5 . 8 . 8]$
29	IV	9	$-2887[25 :: 8]$
61	IV	7	$-6028[12 . 2 :: 13 . 4]$
96	VIII	13	$-9594[20 . 2 . 2 :: 31 . 2 . 13]$
118	IV	25	$-11780[16 . 4 . 2 :: 3 . 8 . 19]$
118	VIII	16	$-11780[16 . 4 . 2 :: 3 . 8 . 19]$
119	VIII	16	$-11840[24 . 2 . 2 :: 5 . 9 . 7]$
Tausendergruppe I	G. II ...	3 ...	$-541[10 :: 11]$
I	II	4	$-415[10 :: 13]$
I	II	8	$-527[18 :: 3]$
I	II	8	$-722[18 :: 3]$
I	II	9	$-194[20 :: 5]$
I	II	9	$-459[6 . 3 :: 5 . 9]$
I	II	9	$-972[6 . 3 :: 7 . 13]$
I	II	11	$-842[26 :: 13]$
I	IV	3	$-784[8 . 2 :: 5 . 4]$
I	IV	4	$-532[4 . 2 :: 13 . 7]$
I	IV	5	$-425[12 . 2 :: 3 . 17]$
I	IV	5	$-608[12 . 2 :: 13 . 27]$
I	IV	5	$-629[18 . 2 :: 5 . 2]$
III	II	15	$-2578[16 :: 13]$
X	I	111	$-9059[117 :: 5]$
Formen $-(15n + 13)$	IV	4	$-2788^*2^*[8 . 2 :: 19 . 17]$

und hinzuzufügen:

Hundertergruppe 10.	G. II	9	$-972^*3^*[6 . 3 :: 7 . 13]$
17	IV	12	$-1700[24 . 2 :: 3 . 17]$
20	IV	12	$-1937[24 . 2 :: 7 . 2]$
21	IV	6	$-2097[12 . 2 :: 47 . 2]$
23	IV	9	$-2224[18 . 2 :: 5 . 16]$
24	IV	12	$-2366[24 . 2 :: 3 . 2]$
29	IV	9	$-2885[18 . 2 :: 3 . 5]$
61	IV	6	$-6028[12 . 2 :: 13 . 4]$
96	VIII	13	$-9546[26 . 2 . 2 :: 5 . 3 . 37]$
118	IV	25	$-11750[50 . 2 :: 3 . 47]$

118	VIII	16	$-11780^*2^*[16\,.\,4\,.\,2 :: 3\,.\,8\,.\,19]$
119	VIII	16	$-11840^*2^*[16\,.\,4\,.\,2 :: 3\,.\,16\,.\,5]$
Tausendergruppe I.	G. II	5 ...	$-415[10 :: 13]$
I	II	5	$-541[10 :: 11]$
I	II	9	$-459^*3^*[6\,.\,3 :: 5\,.\,9]$
I	II	9	$-527[18 :: 3]$
I	II	9	$-722[18 :: 3]$
I	II	9	$-972^*3^*[6\,.\,3 :: 7\,.\,13]$
I	II	10	$-194[20 :: 5]$
I	II	13	$-842[26 :: 13]$
I	IV	2	$-532[4\,.\,2 :: 13\,.\,7]$
I	IV	4	$-784[8\,.\,2 :: 5\,.\,4]$
I	IV	6	$-425[12\,.\,2 :: 3\,.\,17]$
I	IV	6	$-608[12\,.\,2 :: 13\,.\,27]$
I	IV	9	$-629[18\,.\,2 :: 5\,.\,2]$
III	II	15	$-2518[30 :: 19]$
X	I	117	$-9059[117 :: 5]$
Formen $-(15n+13)$	IV	4	$-2788[8\,.\,2 :: 19\,.\,17]$

Die Tafeln *zur Kreisteilung* geben für 2452 Zahlen der Formen $aa+1$, $aa+4$, $aa+9$, ... $aa+81$ sämtliche ungeraden Primteiler p neben dem zugehörigen a an, und zwar in den Fällen, in denen alle Primteiler unter 200 liegen; nur dann werden $aa+1$ usw. zerlegbar genannt.

Zur leichteren Übersicht beim Gebrauch hat Gauss für jede Tafel, aus der sich die vollständigen Zerlegungen von Zahlen einer der besonderen Formen bestimmen lassen, eine Hilfstafel aufgestellt. Sie enthält neben jeder Primzahl p diejenigen Zahlen a, deren um 1 oder 4 ... vermehrtes Quadrat p als größten Primteiler hat.

Der Hauptzweck der Tafeln ist die Erleichterung der genauen Berechnung von Bögen, deren Kotangenten gegebene rationale Zahlen sind. Zunächst lassen sich mit ihrer Hilfe die Bögen für kleine Kotangenten aus Bögen für große Kotangenten zusammensetzen. Dadurch werden die noch nötigen Berechnungen der Reihen, die die Bögen durch ihre Kotangenten ausdrücken, auf ein sehr geringes Maß beschränkt. Die darauf gerichteten Entwicklungen im handschriftlichen Nachlass sind wenig umfangreich; die folgende ist am weitesten fortgeführt. Darin bezeichnen

$$\begin{array}{l}[2]\ [5]\ [13]\ [17]\ [29]\ [37]\ [41]\ [53]\ [61]\ldots[197]\\ (18)\ (57)\ (239)\ \left(\frac{79}{3}\right)\ldots\end{array}$$

die Bögen zu den Kotangenten

$$1\quad 2\quad \frac{3}{2}\quad 4\quad \frac{5}{2}\quad 6\quad \frac{5}{4}\quad \frac{7}{2}\quad \frac{6}{5}\ldots 14\quad 18\quad 57\quad 239\quad \frac{79}{3}\ldots$$

Mit Hilfe der Tafeln wurde durch Zerlegung von $18+i$, $57+i$, $239+i$ in ihre komplexen Primfaktoren

$$\begin{aligned}(18) &= 2[2] - 2[5] - [13]\\ (57) &= -[2] + 3[5] - [13]\\ (239) &= 3[2] \qquad - 4[13]\end{aligned}$$

gefunden und daraus

$$\begin{aligned}[2] &= 12(18) + 8(57) - 5(239)\\ [5] &= 7(18) + 5(57) - 3(239)\\ [13] &= 9(18) + 6(57) - 4(239)\end{aligned}$$

ferner mit Hilfe der Tafeln

$$\begin{aligned}(268) &= -2[5] + 2[13] - [17] \quad \cdot\\ (38) &= -[5] \qquad\quad + 2[17]\end{aligned}$$

und daraus durch Elimination von [17] und Einsetzen der zuvor erhaltenen Werte von [5], [13]

$$(38) + 2(268) = (18) - (57) - (239)$$

Die Elimination von (18) ergab dann die neue Bestimmung

$$\begin{aligned}[2] &= 12(38) + 20(57) + 7(239) + 24(268)\\ [5] &= 7(38) + 12(57) + 4(239) + 14(268)\\ [13] &= 9(38) + 15(57) + 5(239) + 18(268)\\ [17] &= 4(38) + 6(57) + 2(239) + 7(268)\end{aligned}$$

Nach der aufeinanderfolgenden Anwendung der Kotangenten 117, 327, 882, 18543, 307, 278, 378, 829, 993, 2943, 447, 606, 931, 1143, 1772, 6118, 34208, 44179, 85353, 485298, 17772, 9466, 330182, 5257, 114669, 12943 sind schließlich $[2][5]\dots[61]$ durch $(5257), (9466)\dots(485298)$ ausgedrückt und ihre Koeffizienten in den folgenden Spalten zusammengestellt:

	5257	9466	12943	34208	44179	85353	114669	330182	485298
2	+2805	−398	+1950	+1850	+2021	+2097	+1484	+1389	+808
5	+1656	−235	+1151	+1092	+1193	+1238	+876	+820	+477
13	+2100	−298	+1460	+1385	+1513	+1570	+1111	+1040	+605
17	+875	−124	+608	+577	+630	+654	+463	+433	+252
29	+1359	−193	+945	+896	+979	+1016	+719	+673	+391
37	+590	−84	+410	+389	+425	+441	+312	+292	+170
41	+2410	−342	+1675	+1589	+1736	+1802	+1275	+1193	+694
53	+994	−141	+691	+655	+716	+743	+526	+492	+286
61	+2481	−352	+1725	+1637	+1788	+1855	+1313	+1229	+715

Von der Richtigkeit dieser Gleichungen, die zur Bestimmung von [2][5] . . . . [61] dienen können, überzeugt man sich unmittelbar anhand der Zerlegungen, die sich aus den obigen Tafeln ergeben:

(5257) =	[2]	+2[5]	−[13]	+[17]	.	.	−[41]	.	−[61]
(9466) =	2[2]	.	.	.	−[29]	−3[37]	.	.	−[61]
(12943) =	[2]	−4[5]	+3[13]	.	.	.	.	.	−[61]
(34208) =	2[2]	−[5]	−2[13]	+[17]	+[29]	.	.	−2[53]	.
(44179) =	3[2]	.	−3[13]	−2[17]	−[29]	.	.	+[53]	.
(85353) =	−[2]	−[5]	+[13]	−[17]	.	−[37]	+2[41]	−[53]	.
(114669) =	−3[2]	.	.	+[17]	.	+[37]	.	+2[53]	+2[61]
(330182) =	−4[2]	+5[5]	+[13]	.	+[29]	−[37]	−[41]	.	+[61]
(485298) =	−2[2]	−[5]	+4[13]	.	−2[29]	+[37]	.	+[53]	.

Die bisher von den Rechnern verwendeten Verfahren zur Bestimmung von $\frac{\pi}{4} = (1)$ stellt Gauss in der folgenden Übersicht zusammen

Machin	$(1) = 4(5) - (239)$
	auch Clausen
Euler	$= (2) + (3)$
	(Euler an Goldbach 1746 Mai 28)
Vega	$= 5(7) + 2(\frac{79}{3})$
	(Vega Thesaurus logar. p. 633)
Vega	$= 2(3) + (7)$
	auch Clausen (Astr. Nachr. Bd. 25. S. 209)
Rutherford	$= 4(5) - (70) + (99)$
	(Philos. Trans. 1841. p. 283)
Dase	$= (2) + (5) + (8)$
	(Crelle Journal. Bd. 27. S. 198)
Gauss. 1.	$= 12(18) + 8(57) - 5(239)$
Gauss. 2.	$= 12(38) + 20(57) + 7(239) + 24(268)$

Die ersten Rechnungen für die Tafeln stammen aus der Zeit der Ausarbeitung der *Disquiss. Arr.*; sie wurden dann besonders in den Jahren 1846 und 47 vorangebracht. Am 21. Juli 1847 waren 2283 Zerlegungen in der hier wiedergegebenen Ordnung in Tafeln gebracht. Die übrigen 169 wurden später berechnet, und ich habe sie in diesen Abdruck eingeordnet, der sich in der Einrichtung vom Original nur durch die zur Erleichterung des Satzes verwendete Wiederholung der Faktoren anstelle von Potenzen unterscheidet.

Die Handschriften mit diesen letzten Rechnungen scheinen die Ergebnisse in der Form zu enthalten, in der sie unmittelbar gefunden wurden. Die Reihenfolge der Zahlen a lässt vermuten, dass nur für die kleineren die Teiler von $aa + 1$ usw. aufgesucht wurden und die größeren Zahlen daraus durch

besondere Kunstgriffe hervorgingen. Aufgezeichnet ist aber nur die folgende Regel: *Aus drei Zahlen* a, $2a - n$, $2a + n$ *findet sich eine vierte*

$$\frac{4a^3 - (nn-3)a}{nn+1}$$

Diese ist für $n = 0$ *und* $n = 1$ *stets eine ganze Zahl, sonst nur*

$$\textit{für}\quad a \equiv 0 \quad \textit{und} \quad \equiv \pm\sqrt{-1} \quad mod(nn+1) \quad \textit{wenn } n \textit{ gerade}$$
$$\textit{und für}\quad a \equiv 0 \quad \textit{und} \quad \equiv \pm\sqrt{-1} \quad mod\frac{nn+1}{2} \quad \textit{wenn } n \textit{ ungerade}$$

Beispiele	$a = 253,$	$n = 6,$	1750507
	$a = 294,$	$n = 11,$	832902
	$a = 119,$	$n = 1,$	3370437
	$a = 57,$	$n = 3,$	74043
	$a = 123,$	$n = 9,$	90657

Zur vierten Zahl gehören nämlich keine anderen Primteiler als zu den ersten drei; davon sind nur diejenigen ungeraden Primteiler ausgeschlossen, die zur Zahl n gehören.

Die Tafel '*Quadratorum myrias prima*' enthält in der Überschriftenzeile die Tausender und Hunderter, in der ersten senkrechten Spalte die Zehner und Einer der Grundzahl, ferner in der letzten senkrechten Spalte jeder einzelnen Tafel die drei niedrigsten Ziffern des Quadrats und im Inneren die vier oder fünf höheren Ziffern des Quadrats.

Die Tafel '*Indizes der Primzahlen im höheren Zahlenbereich*' enthält in der obersten waagerechten Reihe den jeweiligen Modul, in der zweiten Reihe die verwendete Basis, in der ersten senkrechten Spalte die Restzahlen und im Inneren die Indizes. Die Sterne $*$ bezeichnen die Nullreste.

Die Handschrift des Fragments '*Achter Abschnitt. Ausführlichere Betrachtung einiger Untersuchungen zur Kreisteilung*' scheint aus der Zeit der Umarbeitung der 'Analysis residuorum' in die 'Disquisitiones arithmeticae' zu stammen. Die Briefe von Gauss an Dirichlet bestätigen die Ansicht, dass Gauss auch in der höheren Arithmetik erheblich mehr entdeckt hat, als sich im Nachlass findet.

Schering.

INHALT.

GAUSS' WERKE, BAND II. HÖHERE ARITHMETIK.

Abhandlungen.

Ein neuer Beweis eines arithmetischen Satzes	1808 Jan. . .	Seite 1
Summation einiger besonderer Reihen	1808 Aug. . .	— 9
Neue Beweise und Erweiterungen des Fundamentaltheorems in der Theorie der quadratischen Reste	1817 Febr. .	— 47
Theorie der biquadratischen Reste. Erste Abhandlung	1825 Apr. .	— 65
Theorie der biquadratischen Reste. Zweite Abhandlung	1831 Apr. .	— 93

Besprechungen eigener Schriften.

Ein neuer Beweis eines arithmetischen Satzes	1808 Mai . .	— 151
Summation einiger besonderer Reihen	1808 Sept. .	— 155
Fundamentaltheorem in der Theorie der Reste usw.	1817 März .	— 159
Theorie der biquadratischen Reste. Abh. I.	1825 April .	— 165
Theorie der biquadratischen Reste. Abh. II.	1831 April .	— 169

Besprechungen fremder Schriften.

[Dalberg] Untersuchungen über die arithmetische und geometrische Irreduzibilität der Zahlen und ihrer Potenzen	1809 März .	— 181
Chernac. Arithmetisches Sieb	1812 März .	— 181
Burckhardt. Teilertafeln	1814 Nov. 1816 Nov. 1817 Aug. .	— 183
Erchinger. Konstruktion des Siebzehnecks	1825 Dez. .	— 186
Seeber. Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen	1831 Juli . .	— 188

Nachlass.

Untersuchung der Reste:
Sechstes Kapitel. Erster Teil. Lösung der Kongruenz $x^m - 1 \equiv 0$ Seite 199
. . . . . .
Achtes Kapitel. Allgemeine Untersuchungen über Kongruenzen — 212
. . . . . .
Weiterentwicklung der Untersuchungen über reine Gleichungen — 243
. . . . . .
Beweis einiger Sätze über die Perioden der Klassen binärer quadratischer Formen . . . . . — 266
Über den Zusammenhang zwischen der Anzahl der Klassen, in die binäre quadratische Formen zerfallen, und ihrer Determinante. I. II . . X — 269
. . . . . .
Geometrischer Aspekt der ternären Formen . . . . . — 305
Zur Theorie der biquadratischen Reste. I. . . VI . . . . . — 313
Zur Theorie der komplexen Zahlen. I. . . VI . . . . . — 387
Tafel des quadratischen Charakters der Primzahlen . . . . . — 399
Tafel zur Umwandlung gemeiner Brüche in Dezimalbrüche . . . . . — 411
Tafel der Häufigkeit der Primzahlen . . . . . — 435
Tafel der Anzahl der Klassen binärer quadratischer Formen . . . . . — 449
Tafel zur Kreisteilung . . . . . — 477
Neue Quadratur des Kreises . . . . . -. . . . . — . 497
Zur Berechnung der Logarithmen . . . . . — 501
Die ersten zehntausend Quadrate . . . . . — 504
Indizes der Primzahlen im höheren Zahlenbereich . . . . . ,. . . . . — 506
Hilfstafel zur Lösung der Gleichung $A = fxx + gyy$ . . . . . — 509
Achter Abschnitt. Ausführlichere Betrachtung einiger Untersuchungen zur Kreisteilung. — 510
Briefe von Gauss an Dirichlet . . . . . — 514

Bemerkungen . . . . . — 519

GÖTTINGEN,
DRUCK DER DIETRICHSCHEN UNIVERSITÄTSBUCHDRUCKEREI.
W. FR. KAESTNER.

Carl Friedrich Gauss

Werke

Band III

Ein neuer Beweis des Satzes, dass jedes Polynom in einer Variablen in reelle Faktoren ersten oder zweiten Grades zerlegt werden kann

Vollständige Dissertation von 1799 und vollständiger zweiter Beweis von 1815

Moderne deutsche Übersetzung

Es folgen die historischen Titelblätter und die vollständige Dissertation von 1799, Artikel 1–24, mit den zehn historischen Fußnoten von Gauss und allen vier Figuren. Es folgt der vollständige zweite Beweis, Artikel 1–20 mit beiden historischen Fußnoten und seinem Titelblatt. Er wurde 1815 vorgelegt und 1816 veröffentlicht. Spätere Texte des dritten Bandes sind in diesem Leseband nicht enthalten. Historische Verweise behalten die Nummerierung der Vorlage bei.

Historische Vorlage: Carl Friedrich Gauss, *Werke*, dritter Band, Göttingen, 1866; Dissertation erstmals 1799 bei C. G. Fleckeisen in Helmstedt erschienen. Die ursprünglich deutschen Titelblätter sind in modernem Deutsch wiedergegeben; das historische Original wird gesondert bewahrt.

Mit OpenAI GPT-6.1 Sol KI-übersetzt ins Deutsche; KI-erzeugter Satz.

Quellen und Terminologie

Historischer Text: Carl Friedrich Gauss, *Werke*, dritter Band, Göttingen, 1866. Diese englischen und deutschen Texte sind aus der originalsprachlichen Ausgabe KI-übersetzt. Die folgenden menschlichen Übersetzungen und Schriften werden für die angegebene Terminologie und den Sprachgebrauch herangezogen; ihr fortlaufender Wortlaut wird nicht übernommen. Die ursprünglichen mathematischen Formulierungen von Gauss bleiben maßgeblich.

Paul Taylor; Bernard Leak. Taylors englische Übersetzung des zweiten Beweises von Gauss für den Fundamentalsatz der Algebra, mit Korrekturen von Leak, 1983. Die entsprechenden Passagen des zweiten Beweises von 1815 wurden für die englische Terminologie zu Polynomen, Teilern, Graden, symmetrischen Funktionen und Beweisen herangezogen. Verwandte Terminologie wurde auch für die Dissertation von 1799 herangezogen, zu der diese Arbeit keine Parallelübersetzung ist. Fortlaufender Text aus dieser menschlichen Übersetzung wird nicht übernommen. Ihr späterer Gebrauch komplexer Größen ersetzt hier nicht die Definition imaginärer Größen von Gauss. Die herangezogene Online-Ausgabe nennt Dezember 1983 als Übersetzungsdatum, August 2003 für die LaTeX-Fassung und den 8. Juni 2007 als letztes Änderungsdatum der zugrunde liegenden Quelle. Ihre Danksagung nennt Mark Wainwright für die Rückgabe von Taylors Notizen und Nikita Danilov für die Korrektur von Tippfehlern.
`https://www.paultaylor.eu/misc/gauss.html`

H. Maser. Deutscher Übersetzer und Herausgeber, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Verwandte deutsche Terminologie für algebraische Funktionen, Wurzeln, Teilbarkeit, Quotienten und Grade; keine Parallelübersetzung dieser Dissertation.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead und Adam Miller Hiltebeitel. Übersetzer von Gauss' *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX-Ausgabe. Verwandte englische Terminologie für Geometrie, Koordinaten und unendlich kleine Größen; keine Parallelübersetzung der Dissertation von 1799.
`https://www.gutenberg.org/ebooks/36856`

Ulrich Görtz. *Algebra*, Wintersemester 2021/22, Abschnitt 3.1.1, Beispiele 3.1–3.2. Verwandter zeitgenössischer deutscher Sprachgebrauch zu Polynomen, Unbestimmten, Summen, Zählern und Nennern sowie zur mathematischen Argumentation. Diese Quelle dient der Terminologie; sie ist keine Parallelübersetzung der beiden Beweise. Fortlaufender Text und moderne ringtheoretische Argumente werden nicht übernommen.
`https://math.ug/a-ws2122/sect0006.html`

KI-Urheberschaft und Quellen. Mit OpenAI GPT-6.1 Sol KI-übersetzt; KI-erzeugter Satz. Gauss ist der Autor des historischen mathematischen Textes. Die genannten menschlichen Übersetzungen werden für ihre angegebenen Beiträge zu Terminologie und Sprachgebrauch gewürdigt.

Bibliografische Metadaten: `CITATIONS.bib`.

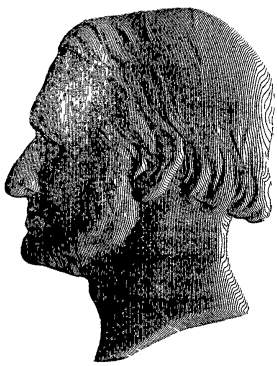
CARL FRIEDRICH GAUSS: WERKE

BAND III.

CARL FRIEDRICH GAUSS

WERKE

DRITTER BAND



HERAUSGEGEBEN
VON DER
KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
ZU GÖTTINGEN

1866.

EIN NEUER BEWEIS
DES SATZES,
DASS JEDES POLYNOM

IN EINER VARIABLEN
IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES
ZERLEGT WERDEN KANN

ZUR ERLANGUNG
DER HÖCHSTEN WÜRDEN IN DER PHILOSOPHIE
DER HOCHBERÜHMTEN PHILOSOPHISCHEN FAKULTÄT
DER ACADEMIA JULIA CAROLINA

VORGELEGT VON
CARL FRIEDRICH GAUSS

HELMSTEDT
BEI C. G. FLECKEISEN. MDCCLXXXXIX.

EIN NEUER BEWEIS DES SATZES, **DASS JEDES POLYNOM** IN EINER VARIABLEN IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES ZERLEGT WERDEN KANN.

1.

Jede bestimmte algebraische Gleichung lässt sich auf die Form

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

bringen, wobei m eine positive ganze Zahl ist. Bezeichnen wir die linke Seite dieser Gleichung mit X und nehmen wir an, dass die Gleichung $X = 0$ durch mehrere ungleiche Werte von x erfüllt wird, etwa indem wir $x = \alpha$, $x = \beta$, $x = \gamma$ usw. setzen, so ist die Funktion X durch das Produkt aus den Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. teilbar. Umgekehrt: Wenn das Produkt aus mehreren linearen Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. die Funktion X teilt, so wird die Gleichung $X = 0$ erfüllt, wenn man x irgendeiner der Größen α, β, γ usw. gleichsetzt. Ist schließlich X gleich einem Produkt aus m solchen linearen Faktoren (ob sie nun alle verschieden oder einige von ihnen identisch sind), so können keine anderen linearen Faktoren die Funktion X teilen. Eine Gleichung vom Grad m kann daher nicht mehr als m Wurzeln haben. Zugleich ist aber klar, dass eine Gleichung vom Grad m *weniger* Wurzeln haben kann, auch wenn sich X in m lineare Faktoren zerlegen lässt: Sind nämlich einige dieser Faktoren identisch, so ist die Anzahl der verschiedenen Möglichkeiten, die Gleichung zu erfüllen, notwendig kleiner als m. Der Einheitlichkeit halber haben es die Mathematiker dennoch vorgezogen, auch in diesem Fall zu sagen, die Gleichung habe m Wurzeln und nur einige davon seien einander gleich; was sie sich durchaus erlauben können.

2.

Was bisher dargelegt wurde, wird in den Büchern über Algebra ausreichend bewiesen und verstößt nirgends gegen die geometrische Strenge. Doch scheinen die Analysten allzu voreilig und ohne vorherigen stichhaltigen Beweis den Satz angenommen zu haben, auf dem fast die gesamte Lehre von den Gleichungen beruht: *Jede Funktion wie X lässt sich stets in m lineare Faktoren zerlegen*, oder, was damit völlig übereinstimmt, *jede Gleichung vom Grad m hat tatsächlich m Wurzeln.* Da schon bei quadratischen Gleichungen sehr häufig Fälle auftreten, die diesem Satz widersprechen, waren die Algebraiker gezwungen, um auch diese Fälle unter ihn zu bringen, eine imaginäre Größe zu erfinden, deren Quadrat -1 ist. Darauf erkannten sie: Lässt man

Größen der Form $a + b\sqrt{-1}$ ebenso zu wie reelle, so gilt der Satz nicht nur für quadratische, sondern auch für kubische und biquadratische Gleichungen. Daraus durfte man jedoch keineswegs schließen, dass sich nach Zulassung der Größen der Form $a + b\sqrt{-1}$ jede Gleichung fünften oder höheren Grades erfüllen lässt oder, wie man gewöhnlich sagt (obwohl ich diese schlüpfrige Formulierung nicht gutheißen möchte), dass die Wurzeln jeder Gleichung auf die Form $a + b\sqrt{-1}$ gebracht werden können. Der Sache nach unterscheidet sich dieser Satz in nichts von dem im Titel dieser Schrift ausgesprochenen; einen neuen strengen Beweis dafür zu geben, ist das Ziel der vorliegenden Dissertation.

Seit die Analysten erkannt haben, dass es unendlich viele Gleichungen gibt, die überhaupt keine Wurzel hätten, wenn nicht Größen der Form $a + b\sqrt{-1}$ zugelassen würden, hat man solche erdachten Größen als eine besondere Art von Größen betrachtet, sie zur Unterscheidung von den *reellen* als *imaginäre* bezeichnet und in die gesamte Analysis eingeführt. Mit welchem Recht? Das erörtere ich hier nicht. — Ich werde meinen Beweis ohne jede Hilfe imaginärer Größen durchführen, obwohl es auch mir erlaubt wäre, dieselbe Freiheit in Anspruch zu nehmen, deren sich alle neueren Analysten bedient haben.

3.

Was in den meisten elementaren Büchern als Beweis unseres Satzes angeführt wird, ist zwar so gehaltlos und von geometrischer Strenge so weit entfernt, dass es kaum der Erwähnung wert ist; damit aber nichts fehlt, will ich es dennoch kurz berühren. ‘Um zu zeigen, dass jede Gleichung

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

oder $X = 0$ tatsächlich m Wurzeln hat, unternimmt man den Beweis, dass sich X in m lineare Faktoren zerlegen lässt. Dazu nimmt man m lineare Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. an, wobei α, β, γ usw. noch unbekannt sind, und setzt ihr Produkt der Funktion X gleich. Durch Vergleich der Koeffizienten erhält man dann m Gleichungen, aus denen sich, wie man sagt, die Unbekannten α, β, γ usw. bestimmen lassen, da auch ihre Anzahl m ist. Man könne nämlich $m - 1$ Unbekannte eliminieren, sodass eine Gleichung übrig bleibe, die nur noch diejenige Unbekannte enthalte, die man beliebig auswählt.’ Von den übrigen Einwänden gegen eine solche Schlussweise will ich schweigen und nur fragen: Woher können wir sicher wissen, dass diese letzte Gleichung tatsächlich irgendeine Wurzel hat? Warum könnte es nicht sein, dass weder diese letzte noch die vorgelegte Gleichung durch irgendeine Größe im gesamten Bereich der reellen und imaginären Größen erfüllt wird? — Im Übrigen werden Sachkundige leicht erkennen, dass diese letzte Gleichung notwendig mit der vorgelegten *völlig identisch* ist, sofern die

Rechnung richtig durchgeführt wurde: Nach Elimination der Unbekannten β, γ usw. muss nämlich die Gleichung

$$\alpha^m + A\alpha^{m-1} + B\alpha^{m-2} + \text{usw.} + M = 0$$

entstehen. Mehr braucht über diese Schlussweise nicht gesagt zu werden.

Einige Autoren, die die Schwäche dieser Methode bemerkt zu haben scheinen, nehmen als *Axiom* an, jede Gleichung habe tatsächlich Wurzeln, wenn nicht mögliche, dann unmögliche. Was sie unter möglichen und unmöglichen Größen verstehen wollen, scheinen sie nicht hinreichend deutlich erläutert zu haben. Sollen die möglichen Größen dasselbe wie die reellen, die unmöglichen dasselbe wie die imaginären bezeichnen, so darf jenes Axiom keineswegs zugestanden werden, sondern bedarf notwendig eines Beweises. Doch scheinen die Ausdrücke nicht in diesem Sinn gemeint zu sein; vielmehr scheint der Sinn des Axioms dieser zu sein: 'Obwohl wir noch nicht sicher sind, dass es notwendig m reelle oder imaginäre Größen gibt, die eine gegebene Gleichung vom Grad m erfüllen, wollen wir dies dennoch eine Zeit lang voraussetzen; sollte es nämlich geschehen, dass sich so viele reelle und imaginäre Größen nicht finden lassen, so bleibt uns gewiss der Ausweg zu sagen, die übrigen seien unmöglich.' Zieht jemand diese Ausdrucksweise der einfachen Aussage vor, die Gleichung werde in diesem Fall nicht so viele Wurzeln haben, so habe ich nichts dagegen. Benutzt er dann aber diese unmöglichen Wurzeln, als wären sie etwas Wirkliches, und sagt zum Beispiel, die Summe aller Wurzeln der Gleichung $x^m + Ax^{m-1} + \text{usw.} = 0$ sei $= -A$, auch wenn sich unmögliche darunter befinden (was eigentlich bedeutet: *auch wenn einige fehlen*), so kann ich dies keineswegs gutheißen. Denn unmögliche Wurzeln, in diesem Sinn genommen, sind dennoch Wurzeln; dann darf jenes Axiom auf keinen Fall ohne Beweis zugestanden werden, und wäre es abwegig zu fragen, ob es nicht Gleichungen geben könnte, die nicht einmal unmögliche Wurzeln haben?[*)]

[*)] Unter einer imaginären Größe verstehe ich hier stets eine Größe der Form $a + b\sqrt{-1}$, solange b nicht $= 0$ ist. In diesem Sinn haben alle Mathematiker ersten Ranges jenen Ausdruck stets gebraucht. Ich meine, man sollte diejenigen nicht anhören, die eine Größe $a + b\sqrt{-1}$ nur dann imaginär nennen wollen, wenn $a = 0$ ist, dagegen unmöglich, wenn nicht $a = 0$ ist; denn diese Unterscheidung ist weder nötig noch von irgendeinem Nutzen. — Sollen imaginäre Größen überhaupt in der Analysis beibehalten werden (was aus mehreren Gründen ratsamer erscheint, als sie abzuschaffen, sofern sie nur hinreichend sicher begründet werden), so muss man sie notwendig als ebenso möglich wie die reellen betrachten. Daher möchte ich die reellen und die imaginären Größen lieber unter der gemeinsamen Bezeichnung *mögliche Größen* zusammenfassen. Dagegen würde ich eine Größe *unmöglich* nennen, die Bedingungen erfüllen soll, die sich selbst bei Zulassung imaginärer Größen nicht erfüllen lassen, jedoch so, dass diese *Ausdrucksweise* dasselbe bedeutet, wie wenn man sagt, eine solche Größe gebe es im gesamten Bereich der Größen nicht. Daraus eine besondere Art von Größen zu bilden, würde ich keineswegs gestatten. Sagt jemand, ein geradliniges gleichseitiges rechtwinkliges Dreieck sei unmöglich, so wird niemand widersprechen. Wollte er aber ein solches unmögliches Dreieck als eine neue Art von Dreiecken betrachten und andere Eigenschaften der Dreiecke darauf

4.

Bevor ich die Beweise anderer Mathematiker für unseren Satz durchgehe und darlege, was mir an jedem von ihnen zu beanstanden scheint, bemerke ich: Es genügt, nur zu zeigen, dass sich jede Gleichung eines beliebigen Grades

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

oder $X = 0$ (wobei die Koeffizienten A, B usw. als reell vorausgesetzt werden) auf wenigstens eine Weise durch einen Wert von x der Form $a + b\sqrt{-1}$ erfüllen lässt. Bekanntlich ist X dann durch den reellen quadratischen Faktor $xx - 2ax + aa + bb$ teilbar, wenn b nicht $= 0$ ist, und durch den reellen linearen Faktor $x - a$, wenn $b = 0$ ist. In beiden Fällen ist der Quotient reell und von niedrigerem Grad als X; und da dieser auf dieselbe Weise einen reellen Faktor ersten oder zweiten Grades haben muss, ist klar, dass die Fortsetzung dieses Verfahrens die Funktion X schließlich in reelle lineare oder quadratische Faktoren zerlegt oder, wenn man für jeden reellen quadratischen Faktor lieber zwei imaginäre lineare verwendet, in m lineare Faktoren.

5.

Der erste Beweis des Satzes stammt von dem ausgezeichneten Mathematiker D'Alembert, *Recherches sur le calcul intégral, Histoire de l'Acad. de Berlin, Année* 1746, S. 182 ff. Er findet sich auch bei Bougainville, *Traité du calcul intégral, à Paris* 1754, S. 47 ff. Die Hauptschritte dieser Methode sind folgende.

Zunächst zeigt er: Wird irgendeine Funktion X der veränderlichen Größe x entweder für $x = 0$ oder für $x = \infty$ gleich $= 0$ und kann sie einen unendlich kleinen positiven reellen Wert annehmen, wenn man x einen reellen Wert gibt, so kann diese Funktion auch einen unendlich kleinen negativen reellen Wert durch einen Wert von x annehmen, der entweder reell ist oder die imaginäre Form $p + q\sqrt{-1}$ hat. Bezeichnet nämlich Ω einen unendlich kleinen Wert von X und ω den entsprechenden Wert von x, so behauptet er, ω lasse sich durch

anwenden, wer könnte das Lachen zurückhalten? Das hieße mit Worten spielen oder vielmehr sie missbrauchen. — Zwar haben auch die größten Mathematiker häufig Wahrheiten, die die Möglichkeit der Größen, auf die sie sich beziehen, offenkundig voraussetzen, auf solche angewendet, deren Möglichkeit noch zweifelhaft war. Auch will ich nicht bestreiten, dass derartige Freiheiten meist nur die Form und gleichsam die Hülle der Schlussfolgerungen betreffen, die der Scharfblick eines wahren Mathematikers bald durchdringen kann. Dennoch scheint es ratsamer und der Erhabenheit einer Wissenschaft, die mit Recht als vollkommenstes Muster von Klarheit und Gewissheit gerühmt wird, angemessener, solche Freiheiten entweder ganz zu verbannen oder sie wenigstens sparsamer und nur dort zu gebrauchen, wo auch weniger Geübte erkennen können, dass die Sache ohne ihre Hilfe vielleicht weniger kurz, aber ebenso streng hätte erledigt werden können. — Im Übrigen will ich nicht bestreiten, dass man das, was ich hier gegen den Missbrauch der unmöglichen Größen gesagt habe, in gewisser Hinsicht auch gegen die imaginären einwenden könnte; doch behalte ich mir deren Verteidigung sowie eine ausführlichere Darstellung dieser ganzen Sache für eine andere Gelegenheit vor.

eine rasch konvergierende Reihe $a\Omega^\alpha + b\Omega^\beta + c\Omega^\gamma$ usw. ausdrücken, deren Exponenten α, β, γ usw. fortwährend zunehmende rationale Größen sind, die daher wenigstens von einer bestimmten Entfernung vom Anfang an positiv werden und die Glieder, in denen sie vorkommen, unendlich klein machen. Kommt nun unter diesen Exponenten kein Bruch mit geradem Nenner vor, so werden alle Glieder der Reihe sowohl für einen positiven als auch für einen negativen Wert von Ω reell. Finden sich dagegen unter jenen Exponenten Brüche mit geradem Nenner, so haben für einen negativen Wert von Ω die entsprechenden Glieder bekanntlich die Form $p+q\sqrt{-1}$. Wegen der unendlichen Konvergenz der Reihe genügt es aber im ersten Fall, nur das erste (das heißt größte) Glied beizubehalten; im zweiten braucht man nicht über dasjenige Glied hinauszugehen, das zuerst einen imaginären Teil hervorbringt.

Durch ähnliche Überlegungen lasse sich zeigen: Kann X durch einen reellen Wert von x einen unendlich kleinen negativen Wert annehmen, so kann diese Funktion durch einen reellen Wert von x oder einen imaginären der Form $p + q\sqrt{-1}$ einen unendlich kleinen positiven reellen Wert erhalten.

Daraus schließt er zweitens, dass es auch einen endlichen reellen Wert von X gibt, im ersten Fall einen negativen, im zweiten einen positiven, der durch einen imaginären Wert von x der Form $p + q\sqrt{-1}$ hervorgebracht werden kann.

Hieraus folgt: Ist X eine solche Funktion von x, die durch einen reellen Wert v von x einen reellen Wert V erhält und durch einen reellen Wert von x auch einen um eine unendlich kleine Größe größeren oder kleineren reellen Wert annimmt, so kann sie auch einen reellen Wert erhalten, der entsprechend um eine unendlich kleine und folglich um eine endliche Größe kleiner oder größer als V ist, indem man x einen Wert der Form $p + q\sqrt{-1}$ gibt. Das ergibt sich ohne Schwierigkeit aus dem Vorhergehenden, wenn man sich für X den Ausdruck $V + Y$ und für x den Ausdruck $v + y$ eingesetzt denkt.

Schließlich behauptet der ausgezeichnete D'Alembert: Nimmt man an, dass X ein ganzes Intervall zwischen zwei reellen Werten R, S durchlaufen kann (das heißt sowohl R als auch S und allen dazwischenliegenden reellen Werten gleich werden kann), indem man x stets Werte der Form $p + q\sqrt{-1}$ gibt, so kann die Funktion X noch um jede endliche reelle Größe vermehrt oder vermindert werden (je nachdem, ob $S > R$ oder $S < R$ ist), wobei x stets die Form $p + q\sqrt{-1}$ behält. Gäbe es nämlich eine reelle Größe U (zwischen der und R der Wert S liegen soll), der X durch einen solchen Wert von x nicht gleich werden könnte, so müsste es einen *größten* Wert von X geben (wenn $S > R$ ist; einen kleinsten dagegen, wenn $S < R$ ist), etwa T, den sie durch einen Wert $p + q\sqrt{-1}$ von x erreichte, sodass man x keinen Wert derselben Form geben könnte, der die Funktion X auch nur um den kleinsten Betrag näher an U brächte. Setzt man nun in dieser Gleichung zwischen X und x überall $p + q\sqrt{-1}$ für x ein und setzt dann sowohl den reellen Teil als

auch den Teil, der den Faktor $\sqrt{-1}$ enthält, nach Weglassung dieses Faktors gleich null, so kann man aus den beiden entstehenden Gleichungen (in denen p, q und X zusammen mit Konstanten vorkommen) durch Elimination zwei andere gewinnen. In der einen stehen p, X und Konstanten; die andere ist von p frei und enthält nur q, X und Konstanten. Da also X durch reelle Werte von p, q alle Werte von R bis T durchlaufen hat, kann X nach dem Vorhergehenden noch näher an den Wert U herankommen, wenn man p, q entsprechend Werte der Formen $\alpha + \gamma\sqrt{-1}$ und $\beta + \delta\sqrt{-1}$ gibt. Dann wird aber $x = \alpha - \delta + (\gamma + \beta)\sqrt{-1}$, hat also weiterhin die Form $p + q\sqrt{-1}$, entgegen der Voraussetzung.

Nimmt man jetzt an, dass X eine Funktion wie $x^m + Ax^{m-1} + Bx^{m-2} +$ usw. $+ M$ bezeichnet, so sieht man ohne Schwierigkeit, dass man x solche reellen Werte geben kann, dass X ein ganzes Intervall zwischen zwei reellen Werten durchläuft. Daher kann x einen Wert der Form $p + q\sqrt{-1}$ erhalten, durch den X gleich $= 0$ wird. Q. E. D.[*)]

6.

Die Einwände, die sich gegen den Beweis von D'Alembert erheben lassen, laufen im Wesentlichen auf Folgendes hinaus.

1. Der ausgezeichnete d'A. zweifelt nicht an der *Existenz* der Werte von x, denen gegebene Werte von X entsprechen, sondern setzt sie voraus und untersucht nur die *Form* jener Werte.

Obwohl dieser Einwand für sich genommen sehr schwer wiegt, betrifft er hier doch nur die Ausdrucksweise, die sich leicht so ändern lässt, dass er vollständig entfällt.

2. Die Behauptung, ω lasse sich stets durch eine Reihe der von ihm angegebenen Art ausdrücken, ist gewiss falsch, wenn X auch eine beliebige transzendente Funktion bezeichnen soll (wie d'A. an mehreren Stellen andeutet). Das ist zum Beispiel klar, wenn man $X = e^{\frac{1}{x}}$ oder $x = \frac{1}{\log X}$ setzt. Beschränken wir jedoch den Beweis auf den Fall, dass X eine algebraische Funktion von x ist (was für die vorliegende Aufgabe genügt), so ist der Satz allerdings richtig. — Im Übrigen hat d'A. zur Bestätigung seiner Voraussetzung nichts angeführt. Der berühmte Bougainville setzt voraus, dass X eine algebraische

[*)] Es ist zu beachten, dass der ausgezeichnete d'Alembert in seiner eigenen Darstellung dieses Beweises geometrische Betrachtungen benutzt und X als Abszisse, x als Ordinate einer Kurve betrachtet hat (nach der Gewohnheit aller Mathematiker des ersten Teils dieses Jahrhunderts, bei denen der Begriff der Funktion weniger gebräuchlich war). Da jedoch alle seine Schlussfolgerungen, wenn man nur auf ihren wesentlichen Inhalt sieht, auf keinen geometrischen, sondern auf rein analytischen Grundlagen beruhen und die Ausdrücke imaginäre Kurven und imaginäre Ordinaten etwas hart erscheinen und den heutigen Leser leichter befremden können, habe ich hier eine rein analytische Darstellungsform vorgezogen. Diese Anmerkung habe ich hinzugefügt, damit niemand, der den eigentlichen Beweis von d'Alembert mit dieser kurzen Darstellung vergleicht, vermutet, es sei etwas Wesentliches verändert worden.

Funktion von x ist, und empfiehlt zur Auffindung der Reihe das NEWTONsche Parallelogramm.

3. Er bedient sich unendlich kleiner Größen freier, als es mit geometrischer Strenge vereinbar ist oder wenigstens in unserer Zeit (in der sie mit Recht in schlechtem Ruf stehen) von einem gewissenhaften Analysten zugestanden würde. Auch erläutert er den Sprung von einem unendlich kleinen Wert von Ω zu einem endlichen nicht deutlich genug. Seinen Satz, dass Ω auch einen endlichen Wert annehmen kann, scheint er weniger aus der Möglichkeit eines unendlich kleinen Wertes von Ω zu folgern als vielmehr daraus: Bezeichnet Ω eine sehr kleine Größe, so komme man wegen der raschen Konvergenz der Reihe dem wahren Wert von ω umso näher, je mehr Glieder der Reihe man nimmt; oder je mehr Glieder man in die für ω genommene Summe einbezieht, desto genauer werde die Gleichung erfüllt, die die Beziehung zwischen ω und Ω beziehungsweise x und X ausdrückt. Abgesehen davon, dass diese ganze Argumentation zu unbestimmt erscheint, um daraus irgendeinen strengen Schluss zu ziehen, bemerke ich, dass es durchaus Reihen gibt, die, wie klein man auch den Wert der Größe ansetzt, nach deren Potenzen sie fortschreiten, dennoch immer divergieren, sodass man, wenn man sie nur weit genug fortsetzt, zu Gliedern gelangen kann, die größer als jede gegebene Größe sind[*)]. Das tritt ein, wenn die Koeffizienten der Reihe eine hypergeometrische Progression bilden. Daher hätte notwendig bewiesen werden müssen, dass im vorliegenden Fall eine solche hypergeometrische Reihe nicht entstehen kann.

Im Übrigen scheint mir, dass der ausgezeichnete d'A. hier zu Unrecht zu unendlichen Reihen gegriffen hat und dass diese zur Begründung dieses Fundamentalsatzes der Gleichungslehre nicht geeignet sind.

4. Aus der Annahme, dass X den Wert S, nicht aber den Wert U annehmen kann, folgt noch nicht, dass zwischen S und U notwendig ein Wert T liegt, den X erreichen, aber nicht überschreiten kann. Es bleibt noch ein anderer Fall: Zwischen S und U könnte eine Grenze liegen, der X beliebig nahe kommen kann, ohne sie jemals zu erreichen. Aus den vom ausgezeichneten d'A. angeführten Gründen folgt nur, dass X jeden einmal erreichten Wert noch um eine endliche Größe überschreiten kann. Ist sie etwa gleich $= S$ geworden, so kann sie noch um eine endliche Größe Ω vermehrt werden; danach kommt ein neuer Zuwachs Ω' hinzu, dann wieder ein Zuwachs Ω'' usw., sodass, wie viele

[*)] Bei dieser Gelegenheit bemerke ich nebenbei, dass sehr viele dieser Reihen auf den ersten Blick äußerst stark zu konvergieren scheinen, zum Beispiel größtenteils diejenigen, mit denen der ausgezeichnete EULER im hinteren Teil der *Inst. Calc. Diff.*, Kapitel VI, S. 441–474 die Summe anderer Reihen möglichst genau bestimmt (die übrigen Reihen auf S. 475–478 können nämlich tatsächlich konvergieren). Soweit ich weiß, hat dies bisher niemand bemerkt. Daher wäre sehr zu wünschen, dass deutlich und streng gezeigt würde, warum derartige Reihen, die anfangs sehr schnell, dann allmählich immer langsamer konvergieren und schließlich immer stärker divergieren, dennoch eine nahezu wahre Summe liefern, sofern man nur nicht zu viele Glieder nimmt, und wie weit man eine solche Summe sicher als genau ansehen darf?

Zuwächse auch schon hinzugefügt sind, keiner als der letzte angesehen werden darf, sondern stets noch ein neuer hinzukommen kann. Doch obwohl die *Anzahl* der möglichen Zuwächse durch keine Grenzen beschränkt ist, könnte es durchaus geschehen, dass bei fortwährender Abnahme der Zuwächse $\Omega, \Omega', \Omega''$ usw. die Summe $S + \Omega + \Omega' + \Omega''$ usw. dennoch eine Grenze niemals erreicht, wie viele Glieder man auch betrachtet.

Dieser Fall kann zwar nicht vorkommen, wenn X ein Polynom in x bezeichnet; ohne Beweis, dass dies nicht geschehen kann, muss die Methode dennoch notwendig als unvollständig gelten. Ist dagegen X eine transzendente oder auch eine gebrochene algebraische Funktion, so kann jener Fall durchaus eintreten, zum Beispiel immer dann, wenn einem bestimmten Wert von X ein unendlich großer Wert von x entspricht. Dann scheint sich die Methode von D'Alembert nicht ohne viele Umwege und in manchen Fällen vielleicht überhaupt nicht auf unbezweifelbare Grundlagen zurückführen zu lassen.

Aus diesen Gründen kann ich den Beweis von D'Alembert nicht für befriedigend halten. Dennoch scheint mir seine eigentliche Beweiskraft durch alle diese Einwände keineswegs gebrochen. Ich glaube, dass sich auf derselben Grundlage (wenn auch auf ganz andere Weise und wenigstens mit größerer Umsicht) nicht nur ein strenger Beweis unseres Satzes aufbauen lässt, sondern daraus auch alles gewonnen werden kann, was man sich für die Theorie *transzendenter* Gleichungen wünschen könnte. Über diese sehr wichtige Sache werde ich bei anderer Gelegenheit ausführlicher sprechen; man vergleiche inzwischen unten Artikel 24.

7.

Nach D'Alembert veröffentlichte der ausgezeichnete Euler seine Untersuchungen über denselben Gegenstand in *Recherches sur les racines imaginaires des équations, Hist. de l'Acad. de Berlin A.* 1749, S. 223 ff. Er gab dort zwei Methoden an; der wesentliche Inhalt der ersten ist folgender.

Zunächst unternimmt der ausgezeichnete Euler den Beweis, dass, wenn m irgendeine Potenz der Zahl 2 bezeichnet, die Funktion $x^{2m} + Bx^{2m-2} + Cx^{2m-3} + \text{usw.} + M = X$ (in der der Koeffizient des zweiten Gliedes $= 0$ ist) stets in zwei reelle Faktoren zerlegt werden kann, in denen x bis zum Grad m aufsteigt. Dazu nimmt er zwei Faktoren an,

$$x^m - ux^{m-1} + \alpha x^{m-2} + \beta x^{m-3} + \text{usw.}, \text{ und } x^m + ux^{m-1} + \lambda x^{m-2} + \mu x^{m-3} \text{ usw.}$$

wobei die Koeffizienten u, α, β usw., λ, μ usw. noch unbekannt sind, und setzt ihr Produkt der Funktion X gleich. Der Vergleich der Koeffizienten liefert dann $2m-1$ Gleichungen. Offenbar muss nur bewiesen werden, dass man den Unbekannten u, α, β usw., λ, μ usw. (deren Anzahl ebenfalls $2m-1$ ist) solche reellen Werte geben kann, die jene Gleichungen erfüllen. Euler behauptet nun: Betrachtet man zunächst u als bekannt, sodass die Anzahl der Unbekannten

um eins kleiner ist als die der Gleichungen, so lassen sich durch geeignete Verbindung dieser Gleichungen nach bekannten algebraischen Methoden alle α, β usw., λ, μ usw. rational und ohne irgendein Wurzelziehen durch u und die Koeffizienten B, C usw. bestimmen; sie erhalten also reelle Werte, sobald u reell wird. Außerdem kann man alle α, β usw., λ, μ usw. eliminieren, sodass eine Gleichung $U = 0$ entsteht, in der U ein Polynom allein in u und den bekannten Koeffizienten ist. Diese Gleichung selbst nach der gewöhnlichen Eliminationsmethode zu entwickeln, wäre eine ungeheure Arbeit, wenn die vorgelegte Gleichung $X = 0$ von etwas höherem Grad ist, und für einen unbestimmten Grad ganz unmöglich (nach Eulers eigenem Urteil, S. 239). Hier genügt es jedoch, eine Eigenschaft dieser Gleichung zu kennen: Das konstante Glied in U (das die Unbekannte u nicht enthält) ist notwendig negativ. Daraus folgt bekanntlich, dass die Gleichung wenigstens eine reelle Wurzel hat oder dass sich u und somit auch α, β usw., λ, μ usw. auf wenigstens eine Weise reell bestimmen lassen. Jene Eigenschaft lässt sich durch die folgenden Überlegungen bestätigen. Da $x^m - ux^{m-1} + \alpha x^{m-2} +$ usw. ein Faktor der Funktion X sein soll, muss u die Summe von m Wurzeln der Gleichung $X = 0$ sein und daher ebenso viele Werte haben, wie man auf verschiedene Weise aus $2m$ Wurzeln m auswählen kann, also nach den Grundsätzen der Kombinatorik $\frac{2m.\overline{2m-1}.\overline{2m-2}.\ldots.\overline{m+1}}{1.2.3\ldots m}$ Werte. Diese Zahl ist stets das Doppelte einer ungeraden Zahl (den nicht schwierigen Beweis lasse ich weg). Setzt man sie also $= 2k$, so ist ihre Hälfte k ungerade; die Gleichung $U = 0$ hat aber den Grad $2k$. Da nun in der Gleichung $X = 0$ das zweite Glied fehlt, ist die Summe aller $2m$ Wurzeln 0. Ist also die Summe irgendwelcher m Wurzeln $+p$, so ist die Summe der übrigen $-p$; das heißt: Gehört $+p$ zu den Werten von u, so gehört auch $-p$ dazu. Hieraus schließt Euler, dass U das Produkt aus k quadratischen Faktoren wie $uu - pp$, $uu - qq$, $uu - rr$ usw. ist, wobei $+p$, $-p$, $+q$, $-q$ usw. alle $2k$ Wurzeln der Gleichung $U = 0$ bezeichnen. Wegen der ungeraden Anzahl dieser Faktoren ist daher das konstante Glied in U das Quadrat des Produkts pqr usw. mit negativem Vorzeichen. Das Produkt pqr usw. lässt sich aber stets aus den Koeffizienten B, C usw. rational bestimmen und ist deshalb notwendig eine reelle Größe. Sein Quadrat mit negativem Vorzeichen ist somit gewiss eine negative Größe. Q. E. D.

Da diese beiden reellen Faktoren von X den Grad m haben und m eine Potenz der Zahl 2 ist, lässt sich jeder auf dieselbe Weise erneut in zwei reelle Faktoren vom Grad $\frac{1}{2}m$ zerlegen. Durch wiederholte Halbierung der Zahl m muss man schließlich zu zwei gelangen; daher erhält man durch Fortsetzung des Verfahrens die Funktion X offenbar in reelle quadratische Faktoren zerlegt.

Wird dagegen eine Funktion vorgelegt, in der das zweite Glied nicht fehlt, etwa $x^{2m} + Ax^{2m-1} + Bx^{2m-2} +$ usw. $+ M$, wobei $2m$ weiterhin eine Zweierpotenz bezeichnet, so geht sie durch die Substitution $x = y - \frac{A}{2m}$ in eine

ähnliche Funktion ohne zweites Glied über. Daraus folgt leicht, dass auch diese Funktion in reelle quadratische Faktoren zerlegt werden kann.

Ist schließlich eine Funktion vom Grad n vorgelegt, wobei n eine Zahl bezeichnet, die keine Zweierpotenz ist, so setze man die nächstgrößere Zweierpotenz über n gleich $= 2m$ und multipliziere die vorgelegte Funktion mit beliebigen $2m - n$ reellen linearen Faktoren. Aus der Zerlegbarkeit des Produkts in reelle quadratische Faktoren ergibt sich ohne Schwierigkeit, dass auch die vorgelegte Funktion in reelle Faktoren zweiten oder ersten Grades zerlegbar sein muss.

8.

Gegen diesen Beweis lässt sich Folgendes einwenden.

1. Die Regel, nach der Euler schließt, dass sich aus $2m-1$ Gleichungen alle $2m-2$ Unbekannten α, β usw., λ, μ usw. rational bestimmen lassen, ist keineswegs allgemein, sondern lässt sehr häufig Ausnahmen zu. Betrachtet man zum Beispiel in Artikel 3 eine der Unbekannten als bekannt und versucht, die übrigen durch sie und die gegebenen Koeffizienten rational auszudrücken, so findet man leicht, dass dies unmöglich ist und keine unbekannte Größe anders als durch eine Gleichung vom Grad $m-1$ bestimmt werden kann. Obwohl sich hier unmittelbar a priori erkennen lässt, dass dies notwendig so geschehen musste, könnte man doch mit Recht bezweifeln, ob sich die Sache nicht auch im vorliegenden Fall für manche Werte von m ebenso verhält, sodass sich die Unbekannten α, β usw., λ, μ usw. aus u, B, C usw. nur durch eine Gleichung von vielleicht höherem Grad als $2m$ bestimmen lassen. Für den Fall, dass die Gleichung $X = 0$ vierten Grades ist, leitet Euler rationale Werte der Koeffizienten durch u und die gegebenen Koeffizienten her; dass dies aber auch bei allen höheren Gleichungen möglich ist, bedurfte gewiss einer ausführlicheren Erklärung. — Im Übrigen scheint es der Mühe wert, jene Formeln, die α, β usw. rational durch u, B, C usw. ausdrücken, tiefer und in größter Allgemeinheit zu untersuchen. Dies und andere zur Eliminationstheorie gehörende Dinge (ein keineswegs erschöpftes Thema) werde ich bei einer anderen Gelegenheit ausführlicher behandeln.

2. Selbst wenn bewiesen worden ist, dass sich unabhängig vom Grad der Gleichung $X = 0$ stets Formeln finden lassen, die α, β usw., λ, μ usw. rational durch u, B, C usw. ausdrücken, ist doch sicher, dass diese Formeln für manche bestimmten Werte der Koeffizienten B, C usw. *unbestimmt* werden können. Dann ist es nicht nur unmöglich, jene Unbekannten aus u, B, C usw. rational zu bestimmen, sondern in manchen Fällen entsprechen einem reellen Wert von u tatsächlich keine reellen Werte von α, β usw., λ, μ usw. Zur Bestätigung verweise ich den Leser der Kürze halber auf Eulers Abhandlung selbst, in der die Gleichung vierten Grades auf S. 236 ausführlicher behandelt wird. Jeder wird sofort sehen, dass die Formeln für die Koeffizienten α, β unbestimmt werden, wenn $C = 0$ ist und für u der Wert 0 angenommen wird, und dass

sich ihre Werte nicht nur nicht ohne Wurzelziehen angeben lassen, sondern nicht einmal reell sind, wenn $BB-4D$ eine negative Größe ist. Zwar lässt sich in diesem Fall leicht erkennen, dass u noch andere reelle Werte hat, denen reelle Werte von α, β entsprechen; dennoch könnte man befürchten, dass die Auflösung dieser Schwierigkeit (die Euler überhaupt nicht berührt hat) bei höheren Gleichungen weit größere Mühe macht. Gewiss darf diese Sache in einem genauen Beweis keineswegs stillschweigend übergangen werden.

3. Der ausgezeichnete Euler setzt stillschweigend voraus, dass die Gleichung $X = 0$ insgesamt $2m$ Wurzeln hat, und setzt ihre Summe $= 0$, weil das zweite Glied in X fehlt. Wie ich über diese Freiheit denke (deren sich alle Autoren zu diesem Gegenstand bedienen), habe ich schon oben in Artikel 3 erklärt. Der Satz, dass die Summe aller Wurzeln einer Gleichung ihrem ersten Koeffizienten mit umgekehrtem Vorzeichen gleich ist, scheint nur auf Gleichungen anwendbar, die Wurzeln haben. Da nun gerade durch diesen Beweis gezeigt werden soll, dass die Gleichung $X = 0$ tatsächlich Wurzeln hat, scheint es nicht zulässig, ihre Existenz vorauszusetzen. Ohne Zweifel werden diejenigen, die den Fehlschluss in dieser Argumentation noch nicht durchschaut haben, antworten, *hier werde nicht bewiesen, dass die Gleichung $X = 0$ erfüllt werden kann* (denn das bedeutet der Ausdruck, sie habe Wurzeln), *sondern nur, dass sie durch Werte von x erfüllt werden kann, die in der Form $a + b\sqrt{-1}$ enthalten sind; das Erstere werde dagegen als Axiom vorausgesetzt.* Da sich aber außer der reellen und der imaginären Form $a + b\sqrt{-1}$ keine anderen Formen von Größen denken lassen, scheint nicht hinreichend klar, wie sich das, was bewiesen werden soll, von dem unterscheidet, was als Axiom vorausgesetzt wird. Selbst wenn es möglich wäre, noch andere Formen von Größen zu ersinnen, etwa die Form F, F', F'' usw., dürfte man dennoch nicht ohne Beweis zugestehen, dass eine Gleichung durch irgendeinen Wert von x erfüllt werden kann, der entweder reell oder in der Form $a+b\sqrt{-1}$ oder in der Form F oder in F' usw. enthalten ist. Jenes Axiom kann daher keinen anderen Sinn haben als diesen: Jede Gleichung lässt sich *entweder* durch einen reellen Wert der Unbekannten erfüllen *oder* durch einen imaginären Wert in der Form $a + b\sqrt{-1}$ *oder* vielleicht durch einen Wert in einer anderen, bisher unbekannten Form *oder* durch einen Wert, der überhaupt in keiner Form enthalten ist. Wie sich aber solche Größen, von denen man sich nicht einmal eine Vorstellung machen kann — ein wahrer Schatten eines Schattens —, addieren oder multiplizieren lassen, versteht man gewiss nicht mit der Klarheit, die in der Mathematik stets gefordert wird[*)].

[*)] Diese ganze Sache wird durch eine andere, bereits im Druck befindliche Untersuchung sehr erhellt werden. Dort hätte ich bei einem zwar ganz anderen, aber dennoch analogen Gegenstand eine ähnliche Freiheit mit genau demselben Recht gebrauchen können, wie es hier bei den Gleichungen von allen Analysten geschehen ist. Obwohl ich mithilfe solcher Fiktionen die Beweise mehrerer Wahrheiten mit wenigen Worten hätte abschließen können, die ohne

Im Übrigen will ich die Schlussfolgerungen, die Euler aus seiner Voraussetzung gezogen hat, durch diese Einwände keineswegs verdächtig machen. Vielmehr bin ich sicher, dass sie sich durch eine weder schwierige noch von der EULERSCHEN sehr verschiedene Methode so bestätigen lassen, dass niemandem auch nur der geringste Zweifel bleiben dürfte. Ich beanstande allein die *Form*, die zwar beim *Finden* neuer Wahrheiten von großem Nutzen sein kann, beim *Beweisen* vor der Öffentlichkeit aber keineswegs billigenswert erscheint.

4. Zum Beweis der Behauptung, das Produkt pqr usw. lasse sich aus den Koeffizienten in X *rational* bestimmen, hat der ausgezeichnete Euler überhaupt nichts angeführt. Alles, was er hierzu bei Gleichungen *vierten Grades* erläutert, ist Folgendes (wobei a, b, c, d die Wurzeln der vorgelegten Gleichung $x^4 + Bxx + Cx + D = 0$ sind):

'Man wird mir ohne Zweifel einwenden, ich hätte hier vorausgesetzt, die Größe pqr sei eine reelle Größe und ihr Quadrat $ppqqrr$ sei positiv; das sei noch zweifelhaft gewesen, da die Wurzeln a, b, c, d imaginär seien und es daher sehr wohl geschehen könne, dass das Quadrat der aus ihnen zusammengesetzten Größe pqr negativ sei. Darauf antworte ich, dass dieser Fall niemals eintreten kann; denn wie imaginär auch die Wurzeln a, b, c, d sein mögen, weiß man doch, dass $a + b + c + d = 0$ gelten muss: $ab + ac + ad + bc + bd + cd = B$; $abc + abd + acd + bcd = -C$[*)]; $abcd = D$, wobei diese Größen B, C, D reell sind. Da aber $p = a + b$, $q = a + c$, $r = a + d$ ist, lässt sich ihr Produkt $pqr = (a + b)(a + c)(a + d)$, *wie man weiß*, durch die Größen B, C, D bestimmen und wird folglich reell sein, ebenso wie wir gesehen haben, dass tatsächlich $pqr = -C$ und $ppqqrr = CC$ ist. Ebenso wird man leicht erkennen, dass derselbe Umstand bei höheren Gleichungen eintreten muss und man mir von dieser Seite keine Einwände machen kann.' Die Bedingung, dass sich das Produkt pqr usw. *rational* durch B, C usw. bestimmen lässt, hat Euler nirgends hinzugefügt; doch scheint er sie stets mitverstanden zu haben, da der Beweis ohne sie keine Beweiskraft haben kann. Nun ist zwar bei Gleichungen vierten Grades richtig, dass die Entwicklung des Produkts $(a + b)(a + c)(a + d)$ den Ausdruck $aa(a + b + c + d) + abc + abd + acd + bcd = -C$ ergibt; doch scheint nicht hinreichend klar, wie sich das Produkt bei allen höheren Gleichungen rational durch die Koeffizienten bestimmen lässt. Der berühmte DE FONCENEX, der dies zuerst bemerkt hat (*Miscell. phil. math. soc. Taurin.*, Bd. I, S. 117), behauptet mit Recht, dass die Methode ohne einen strengen Beweis dieses Satzes ihre ganze Beweiskraft verliert. Er gesteht aber, dass ihm dieser Beweis ziemlich schwierig erscheint, und berichtet, welchen Weg

sie sehr schwierig wurden und die feinsten Kunstgriffe erfordern, habe ich doch vorgezogen, ganz darauf zu verzichten, und hoffe, dass ich nur wenige zufriedengestellt hätte, wenn ich die Methode der Analysten nachgeahmt hätte.

[*)] Euler hat irrtümlich C und setzt daher auch später fälschlich $pqr = C$.

er vergeblich versucht hat*). Dennoch lässt sich die Sache ohne große Schwierigkeit durch die folgende Methode erledigen (deren wesentlichen Inhalt ich hier nur andeuten kann). Obwohl bei Gleichungen vierten Grades nicht hinreichend klar ist, dass sich das Produkt $(a+b)(a+c)(a+d)$ durch die Koeffizienten B, C, D bestimmen lässt, sieht man doch leicht, dass dasselbe Produkt auch $= (b+a)(b+c)(b+d)$ sowie $= (c+a)(c+b)(c+d)$ und schließlich auch $= (d+a)(d+b)(d+c)$ ist. Das Produkt pqr ist daher ein Viertel der Summe $(a+b)(a+c)(a+d)+(b+a)(b+c)(b+d)+(c+a)(c+b)(c+d)+(d+a)(d+b)(d+c)$. Dass diese nach der Entwicklung ein Polynom in den Wurzeln a, b, c, d sein wird, in das alle auf dieselbe Weise eingehen, lässt sich ohne Mühe a priori erkennen. Solche Funktionen lassen sich aber stets rational durch die Koeffizienten der Gleichung ausdrücken, deren Wurzeln a, b, c, d sind. — Dasselbe ist auch klar, wenn man das Produkt pqr auf die Form

$$\tfrac{1}{2}(a+b-c-d) \times \tfrac{1}{2}(a+c-b-d) \times \tfrac{1}{2}(a+d-b-c)$$

bringt; denn man kann leicht voraussehen, dass dieses Produkt nach der Entwicklung alle a, b, c, d auf dieselbe Weise enthalten wird. Zugleich werden Sachkundige hieraus leicht entnehmen, wie dies auf höhere Gleichungen anzuwenden ist. — Eine vollständige Darstellung des Beweises, die ich der Kürze wegen hier nicht beifügen kann, behalte ich mir zusammen mit einer ausführlicheren Untersuchung von Funktionen, die mehrere Veränderliche auf dieselbe Weise enthalten, für eine andere Gelegenheit vor.

Im Übrigen bemerke ich, dass sich außer diesen vier Einwänden noch manches andere an Eulers Beweis beanstanden ließe. Das übergehe ich jedoch stillschweigend, um nicht etwa als allzu strenger Kritiker zu erscheinen, zumal das Vorhergehende hinreichend zu zeigen scheint, dass der Beweis jedenfalls in der von Euler vorgelegten Form keineswegs als vollständig gelten kann.

Nach diesem Beweis hat Euler noch einen anderen Weg gezeigt, den Satz für Gleichungen, deren Grad keine Zweierpotenz ist, auf die Auflösung solcher Gleichungen zurückzuführen. Da diese Methode aber für Gleichungen, deren Grad eine Zweierpotenz ist, nichts lehrt und außerdem allen vorigen Einwänden (außer dem vierten) ebenso ausgesetzt ist wie der erste allgemeine Beweis, ist es nicht nötig, sie hier ausführlicher zu erläutern.

*) In diese Darstellung scheint sich ein Fehler eingeschlichen zu haben: Auf S. 118, Zeile 5, muss man nämlich anstelle des Zeichens p ("man wählte nur diejenigen, in denen p vorkam", usw.) notwendig *ein und dieselbe beliebige Wurzel der vorgelegten Gleichung* oder etwas Ähnliches lesen, da das Erstere keinen Sinn hat.

9.

In derselben Abhandlung hat der ausgezeichnete Euler auf S. 263 versucht, unseren Satz noch auf einem anderen Weg zu bestätigen, dessen wesentlicher Inhalt Folgendes ist. Für eine vorgelegte Gleichung $x^n + Ax^{n-1} + Bx^{n-2}$ usw. $= 0$ konnte bisher zwar kein analytischer Ausdruck gefunden werden, der ihre Wurzeln darstellt, wenn der Exponent $n > 4$ ist; dennoch scheint sicher zu sein (wie Euler behauptet), dass er nichts anderes enthalten kann als Rechenoperationen und Wurzelziehungen, die umso verwickelter miteinander verbunden sind, je größer n ist. Gibt man dies zu, so zeigt Euler sehr gut, dass sich der Wert der Formel, wie verwickelt die Wurzelzeichen auch miteinander verbunden sein mögen, stets durch die Form $M + N\sqrt{-1}$ darstellen lässt, wobei M, N reelle Größen sind.

Gegen diese Schlussweise lässt sich einwenden, dass nach den Bemühungen so vieler großer Mathematiker nur sehr geringe Hoffnung bleibt, jemals zur allgemeinen Auflösung algebraischer Gleichungen zu gelangen, sodass es immer wahrscheinlicher wird, dass eine solche Auflösung überhaupt unmöglich und widersprüchlich ist. Dies darf umso weniger paradox erscheinen, *als das, was man gewöhnlich die Auflösung einer Gleichung nennt, eigentlich nichts anderes ist als ihre Zurückführung auf reine Gleichungen.* Denn die Auflösung reiner Gleichungen wird dadurch nicht gelehrt, sondern vorausgesetzt; und wenn man eine Wurzel der Gleichung $x^m = H$ durch $\sqrt[m]{H}$ ausdrückt, hat man sie keineswegs gelöst und nicht mehr getan, als wenn man zur Bezeichnung einer Wurzel der Gleichung $x^n + Ax^{n-1} +$ usw. $= 0$ irgendein Zeichen ersänne und die Wurzel diesem gleichsetzte. Es ist wahr, dass reine Gleichungen wegen der Leichtigkeit, ihre Wurzeln näherungsweise zu finden, und wegen des eleganten Zusammenhangs, den alle ihre Wurzeln untereinander haben, alle übrigen weit übertreffen. Daher ist keineswegs zu tadeln, dass die Analysten ihre Wurzeln durch ein besonderes Zeichen bezeichnet haben. Daraus aber, dass sie dieses Zeichen ebenso wie die Rechenzeichen für Addition, Subtraktion, Multiplikation, Division und Potenzierung unter dem Namen *analytische Ausdrücke* zusammengefasst haben, folgt keineswegs, dass sich eine Wurzel jeder Gleichung durch sie darstellen lässt. Oder, um die Worte beiseitezulassen: Ohne hinreichenden Grund wird vorausgesetzt, dass sich die Auflösung jeder Gleichung auf die Auflösung reiner Gleichungen zurückführen lässt. Vielleicht wäre es nicht so schwierig, diese Unmöglichkeit schon für den fünften Grad mit aller Strenge zu beweisen; meine Untersuchungen darüber werde ich an anderer Stelle ausführlicher vorlegen. Hier genügt es, dass die allgemeine Lösbarkeit der Gleichungen, in jenem Sinn verstanden, noch sehr zweifelhaft ist und daher ein Beweis, dessen ganze Beweiskraft von jener Voraussetzung abhängt, beim gegenwärtigen Stand der Sache kein Gewicht hat.

10.

Später versuchte auch der berühmte DE FONCENEX, nachdem er in EULERS erstem Beweis einen Mangel bemerkt hatte (oben Artikel 8, Einwand 4), den er nicht beheben konnte, noch einen anderen Weg und legte ihn in der genannten Abhandlung auf S. 120 vor[*)]. Er besteht in Folgendem.

Es sei die Gleichung $Z = 0$ vorgelegt, wobei Z eine Funktion vom Grad m der Unbekannten z bezeichnet. Ist m eine ungerade Zahl, so steht bereits fest, dass diese Gleichung eine reelle Wurzel hat. Ist aber m gerade, so versucht der berühmte Foncenex auf folgende Weise zu beweisen, dass die Gleichung wenigstens eine Wurzel der Form $p + q\sqrt{-1}$ hat. Es sei $m = 2^n i$, wobei i eine ungerade Zahl bezeichnet, und es werde vorausgesetzt, dass $zz + uz + M$ ein Teiler der Funktion Z ist. Dann sind die einzelnen Werte von u die Summen von je zwei Wurzeln der Gleichung $Z = 0$ mit umgekehrtem Vorzeichen; daher hat u insgesamt $\frac{m.m-1}{1.2} = m'$ Werte. Wird vorausgesetzt, dass u durch eine Gleichung $U = 0$ bestimmt wird (wobei U ein Polynom in u und den bekannten Koeffizienten in Z bezeichnet), so hat diese den Grad m'. Man sieht aber leicht, dass m' eine Zahl der Form $2^{n-1}i'$ sein wird, wobei i' eine ungerade Zahl bezeichnet. Ist nun m' nicht ungerade, so werde wiederum $uu + u'u + M'$ als Teiler von U vorausgesetzt. Durch ähnliche Überlegungen wird klar, dass u' durch eine Gleichung $U' = 0$ bestimmt wird, wobei U' eine Funktion vom Grad $\frac{m'.m'-1}{1.2}$ in u' ist. Setzt man $\frac{m'.m'-1}{1.2} = m''$, so ist m'' eine Zahl der Form $2^{n-2}i''$, wobei i'' eine ungerade Zahl bezeichnet. Ist nun m'' nicht ungerade, so werde $u'u' + u''u' + M''$ als Teiler der Funktion U' angenommen. Dann wird u'' durch eine Gleichung $U'' = 0$ bestimmt, die, wenn man ihren Grad gleich m''' setzt, für m''' eine Zahl der Form $2^{n-3}i'''$ ergibt. Offenbar ist in der Folge der Gleichungen $U = 0$, $U' = 0$, $U'' = 0$ usw. die Gleichung an der Stelle n von ungeradem Grad und hat daher eine reelle Wurzel. Wir setzen der Kürze halber $n = 3$, sodass die Gleichung $U'' = 0$ eine reelle Wurzel u'' hat; denn man sieht ohne Mühe, dass dieselbe Schlussweise für jeden anderen Wert von n gilt. Dann behauptet der berühmte de Foncenex, dass sich der Koeffizient M'' durch u'' und die Koeffizienten in U' (die, wie man leicht erkennt, Polynome in den Koeffizienten in Z sind), also durch u'' und die Koeffizienten in Z rational bestimmen lässt und daher reell ist. Hieraus folgt, dass die Wurzeln der Gleichung $u'u' + u''u' + M'' = 0$ in der Form $p + q\sqrt{-1}$ enthalten sein werden; sie werden aber offenbar zugleich die Gleichung $U' = 0$ erfüllen. Es gibt daher einen Wert von u', der in der Form $p + q\sqrt{-1}$ enthalten ist. Nun lässt sich der Koeffizient M' auf dieselbe Weise wie zuvor rational durch u' und die Koeffizienten in Z bestimmen und wird daher ebenfalls in der Form $p + q\sqrt{-1}$ enthalten sein. Somit werden die

[*)] Im zweiten Band derselben *Miscellanea*, S. 337, sind Erläuterungen zu dieser Abhandlung enthalten. Diese betreffen jedoch nicht die vorliegende Untersuchung, sondern die Logarithmen negativer Größen, von denen in derselben Abhandlung die Rede war.

Wurzeln der Gleichung $uu + u'u + M'$ in derselben Form enthalten sein und zugleich die Gleichung $U = 0$ erfüllen; das heißt, diese Gleichung wird eine Wurzel in der Form $p + q\sqrt{-1}$ haben. Schließlich folgt hieraus auf ähnliche Weise, dass auch M in derselben Form enthalten ist, ebenso eine Wurzel der Gleichung $zz + uz + M = 0$, die offenbar auch die vorgelegte Gleichung $Z = 0$ erfüllen wird. Daher wird jede Gleichung wenigstens eine Wurzel der Form $p + q\sqrt{-1}$ haben.

11.

Die Einwände 1, 2 und 3, die ich gegen EULERS ersten Beweis erhoben habe (Artikel 8), haben gegen diese Methode dieselbe Beweiskraft, jedoch mit dem Unterschied, dass der zweite Einwand, dem EULERS Beweis nur in einigen besonderen Fällen ausgesetzt war, den vorliegenden in allen Fällen treffen muss. Man kann nämlich a priori beweisen: Selbst wenn eine Formel gegeben ist, die den Koeffizienten M' rational durch u' und die Koeffizienten in Z ausdrückt, muss diese für mehrere Werte von u' notwendig unbestimmt werden. Ebenso wird die Formel, die den Koeffizienten M'' durch u'' darstellt, für gewisse Werte von u'' unbestimmt usw. Dies erkennt man am deutlichsten, wenn man eine Gleichung vierten Grades als Beispiel nimmt. Wir setzen also $m = 4$, und die Wurzeln der Gleichung $Z = 0$ seien α, β, γ, δ. Dann ist klar, dass die Gleichung $U = 0$ sechsten Grades sein wird und ihre Wurzeln $-(\alpha+\beta)$, $-(\alpha+\gamma)$, $-(\alpha+\delta)$, $-(\beta+\gamma)$, $-(\beta+\delta)$, $-(\gamma+\delta)$ sind. Die Gleichung $U' = 0$ ist dagegen fünfzehnten Grades, und die Werte von u' sind

$$\begin{gathered}
2\alpha+\beta+\gamma, \quad 2\alpha+\beta+\delta, \quad 2\alpha+\gamma+\delta, \\
2\beta+\alpha+\gamma, \quad 2\beta+\alpha+\delta, \quad 2\beta+\gamma+\delta, \\
2\gamma+\alpha+\beta, \quad 2\gamma+\alpha+\delta, \quad 2\gamma+\beta+\delta, \\
2\delta+\alpha+\beta, \quad 2\delta+\alpha+\gamma, \quad 2\delta+\beta+\gamma, \\
\alpha+\beta+\gamma+\delta, \quad \alpha+\beta+\gamma+\delta, \quad \alpha+\beta+\gamma+\delta
\end{gathered}$$

Bei dieser Gleichung muss man nun stehen bleiben, da ihr Grad ungerade ist. Sie wird tatsächlich die reelle Wurzel $\alpha + \beta + \gamma + \delta$ haben (die dem ersten Koeffizienten in Z mit umgekehrtem Vorzeichen gleich und daher nicht nur reell, sondern auch rational sein wird, wenn die Koeffizienten in Z rational sind). Man kann aber ohne Mühe erkennen: Ist eine Formel gegeben, die den Wert von M' rational durch den zugehörigen Wert von u' ausdrückt, so wird sie notwendig für $u' = \alpha + \beta + \gamma + \delta$ unbestimmt. Denn dieser Wert ist *dreimal* eine Wurzel der Gleichung $U' = 0$, und ihm entsprechen drei Werte von M', nämlich $(\alpha + \beta)(\gamma + \delta)$, $(\alpha + \gamma)(\beta + \delta)$ und $(\alpha + \delta)(\beta + \gamma)$, die alle irrational sein können. Offenbar könnte aber eine rationale Formel in diesem Fall weder einen irrationalen Wert von M' noch drei verschiedene Werte liefern. Aus diesem Beispiel lässt sich hinreichend entnehmen, dass die Methode des berühmten DE FONCENEX keineswegs befriedigt. Soll sie aber in

jeder Hinsicht vollständig werden, so muss die Eliminationstheorie weit tiefer untersucht werden.

12.

Schließlich hat der ausgezeichnete La Grange unseren Satz in der Abhandlung *Sur la forme des racines imaginaires des équations, Nouv. Mém. de l'Acad. de Berlin* 1772, S. 222 ff., behandelt. Dieser große Mathematiker hat sich besonders bemüht, die Mängel in Eulers erstem Beweis zu ergänzen, und tatsächlich vor allem das, was oben (Artikel 8) den zweiten und vierten Einwand ausmacht, so tief untersucht, dass nichts weiter zu wünschen bleibt, außer dass vielleicht in der früheren Untersuchung über die Eliminationstheorie, auf der diese ganze Untersuchung beruht, einige Zweifel übrig zu sein scheinen. — Den dritten Einwand hat er jedoch überhaupt nicht berührt; vielmehr baut die ganze Untersuchung auf der Voraussetzung auf, jede Gleichung vom Grad m habe tatsächlich m Wurzeln.

Nach sorgfältiger Erwägung dessen, was bisher dargelegt wurde, hoffe ich daher, dass den Sachkundigen ein neuer, aus ganz anderen Grundsätzen abgeleiteter Beweis dieses höchst wichtigen Satzes nicht unwillkommen sein wird. Diesen darzustellen, gehe ich nun sogleich an.

13.

Lemma. *Bezeichnet m eine beliebige positive ganze Zahl, so ist die Funktion $\sin\varphi \,.\, x^m - \sin m\varphi \,.\, r^{m-1}x + \sin(m-1)\varphi \,.\, r^m$ durch $xx - 2\cos\varphi \,.\, rx + rr$ teilbar.*

Beweis. Für $m = 1$ wird jene Funktion $= 0$ und ist daher durch jeden Faktor teilbar; für $m = 2$ wird der Quotient gleich $\sin\varphi$, und für jeden größeren Wert ist der Quotient $\sin\varphi \,.\, x^{m-2} + \sin 2\varphi \,.\, rx^{m-3} + \sin 3\varphi \,.\, rrx^{m-4} + \text{usw.} + \sin(m-1)\varphi \,.\, r^{m-2}$. Denn man bestätigt leicht, dass nach Multiplikation dieser Funktion mit $xx - 2\cos\varphi \,.\, rx + rr$ das Produkt der vorgelegten Funktion gleich wird.

14.

Lemma. *Sind die Größe r und der Winkel φ so bestimmt, dass die Gleichungen*

$$\begin{aligned} &r^m \cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + Br^{m-2}\cos(m-2)\varphi + \text{usw.} \\ &\qquad + Krr\cos 2\varphi + Lr\cos\varphi + M = 0 \quad . \quad . \quad [1] \\ &r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + Br^{m-2}\sin(m-2)\varphi + \text{usw.} \\ &\qquad + Krr\sin 2\varphi + Lr\sin\varphi = 0 \quad . \quad . \quad [2] \end{aligned}$$

gelten, so ist das Polynom $x^m + Ax^{m-1} + Bx^{m-2} + usw. + Kxx + Lx + M = X$ durch den quadratischen Faktor $xx - 2\cos\varphi . rx + rr$ teilbar, sofern nicht $r\sin\varphi = 0$ gilt; ist dagegen $r\sin\varphi = 0$, so ist dasselbe Polynom durch den linearen Faktor $x - r\cos\varphi$ teilbar.

Beweis. I. Nach dem vorigen Artikel sind alle folgenden Größen durch $xx - 2\cos\varphi \,.\, rx + rr$ teilbar:

$$\begin{array}{rll}
\sin\varphi \,.\, rx^m & -\sin m\varphi \,.\, r^m x & +\sin(m-1)\varphi \,.\, r^{m+1} \\
A\sin\varphi \,.\, rx^{m-1} & -A\sin(m-1)\varphi \,.\, r^{m-1}x & +A\sin(m-2)\varphi \,.\, r^m \\
B\sin\varphi \,.\, rx^{m-2} & -B\sin(m-2)\varphi \,.\, r^{m-2}x & +B\sin(m-3)\varphi \,.\, r^{m-1} \\
 & \text{usw.} & \text{usw.} \\
K\sin\varphi \,.\, rxx & -K\sin 2\varphi \,.\, rrx & +K\sin\varphi \,.\, r^3 \\
L\sin\varphi \,.\, rx & -L\sin\varphi \,.\, rx & * \\
M\sin\varphi \,.\, r & * & +M\sin(-\varphi) \,.\, r
\end{array}$$

Daher ist auch ihre Summe durch $xx - 2\cos\varphi \,.\, rx + rr$ teilbar. Die ersten Teile dieser Größen bilden aber die Summe $\sin\varphi \,.\, rX$; die zweiten ergeben zusammen nach [2] den Wert 0. Dass auch die Summe der dritten Teile verschwindet, erkennt man leicht, wenn man [1] mit $\sin\varphi$ und [2] mit $\cos\varphi$ multipliziert und das erste Produkt vom zweiten abzieht. Daraus folgt, dass das Polynom $\sin\varphi \,.\, rX$ durch $xx - 2\cos\varphi \,.\, rx + rr$ teilbar ist, und damit auch das Polynom X, sofern nicht $r\sin\varphi = 0$ gilt. Q. E. P.

II. Ist dagegen $r\sin\varphi = 0$, so ist entweder $r = 0$ oder $\sin\varphi = 0$. Im ersten Fall ist nach [1] auch $M = 0$, und daher ist X durch x oder durch $x - r\cos\varphi$ teilbar; im zweiten Fall ist $\cos\varphi = \pm 1$, $\cos 2\varphi = +1$, $\cos 3\varphi = \pm 1$ und allgemein $\cos n\varphi = \cos\varphi^n$. Wegen [1] ergibt sich also $X = 0$, wenn man $x = r\cos\varphi$ setzt, und folglich ist das Polynom X durch $x - r\cos\varphi$ teilbar. Q. E. S.

15.

Der vorige Satz wird gewöhnlich mit Hilfe imaginärer Größen bewiesen; siehe Euler, *Introd. in Anal. Inf.*, Bd. I, S. 110. Ich hielt es für der Mühe wert zu zeigen, wie er sich ebenso leicht ohne ihre Hilfe herleiten lässt. Es ist nun klar, dass zum Beweis unseres Satzes nur noch Folgendes zu zeigen ist: *Für jedes vorgegebene Polynom X der Form $x^m + Ax^{m-1} + Bx^{m-2} + usw. + Lx + M$ lassen sich r und φ so bestimmen, dass die Gleichungen* [1] *und* [2] *gelten.* Daraus folgt nämlich, dass X einen reellen Faktor ersten oder zweiten Grades besitzt. Die Division ergibt notwendig einen reellen Quotienten niedrigeren Grades, der aus demselben Grund ebenfalls einen Faktor ersten oder zweiten Grades besitzt. Setzt man dieses Verfahren fort, so wird X schließlich in reelle lineare oder quadratische Faktoren zerlegt. Diesen Satz zu beweisen ist also das Ziel der folgenden Untersuchungen.

16.

Man denke sich eine feste unendliche Ebene (die Ebene der Tafel, Fig. 1) und darin eine feste unendliche Gerade GC, die durch einen festen Punkt C geht. Man wähle eine Länge als Einheit, sodass sich alle Geradenlängen durch Zahlen ausdrücken lassen. In jedem Punkt P der Ebene, dessen Abstand vom Mittelpunkt C gleich r ist und dessen Winkel $GCP = \varphi$ beträgt, errichte man eine Senkrechte gleich dem Wert des Ausdrucks

$$r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + \text{usw.} + Lr \sin \varphi$$

den ich im Folgenden der Kürze halber stets mit T bezeichnen werde. Den Abstand r betrachte ich stets als positiv. Für Punkte auf der anderen Seite der Achse muss der Winkel φ entweder als größer als zwei rechte Winkel oder als negativ angesehen werden (was hier auf dasselbe hinausläuft). Die Endpunkte dieser Senkrechten (die für einen positiven Wert von T oberhalb der Ebene, für einen negativen unterhalb und bei verschwindendem Wert in der Ebene selbst zu nehmen sind) liegen auf einer stetigen gekrümmten Fläche, die sich nach allen Richtungen ins Unendliche erstreckt. Ich werde sie im Folgenden der Kürze halber die *erste Fläche* nennen. Ganz ebenso beziehe man auf dieselbe Ebene, denselben Mittelpunkt und dieselbe Achse eine andere Fläche, deren Höhe über jedem Punkt der Ebene gleich

$$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + \text{usw.} + Lr \cos \varphi + M$$

ist; diesen Ausdruck werde ich der Kürze halber stets mit U bezeichnen. Diese Fläche, die ebenfalls stetig ist und sich nach allen Richtungen ins Unendliche erstreckt, werde ich von der vorigen durch die Bezeichnung *zweite Fläche* unterscheiden. Damit ist klar, dass die ganze Aufgabe darin besteht zu zeigen, dass es mindestens einen Punkt gibt, der zugleich in der Ebene, auf der ersten Fläche und auf der zweiten Fläche liegt.

17.

Man erkennt leicht, dass die erste Fläche teils oberhalb, teils unterhalb der Ebene liegt. Denn offenbar lässt sich der Abstand r vom Mittelpunkt so groß wählen, dass die übrigen Glieder in T gegenüber dem ersten Glied $r^m \sin m\varphi$ verschwinden; dieses kann aber durch geeignete Wahl des Winkels φ sowohl positiv als auch negativ werden. Die feste Ebene wird daher notwendig von der ersten Fläche geschnitten. Diese Schnittlinie der Ebene mit der ersten Fläche werde ich die *erste Linie* nennen; sie wird also durch die Gleichung $T = 0$ bestimmt. Aus demselben Grund wird die Ebene von der zweiten Fläche geschnitten; der Schnitt bildet eine durch die Gleichung $U = 0$ bestimmte Kurve, die ich die *zweite Linie* nennen werde. Eigentlich besteht jede der beiden Kurven aus mehreren Zweigen, die vollständig voneinander getrennt sein können, während jeder für sich eine stetige Linie ist. Die erste Linie ist

sogar stets eine sogenannte zusammengesetzte Kurve, und die Achse GC ist als Teil dieser Kurve anzusehen: Welchen Wert man r auch gibt, es gilt stets $T = 0$, wenn $\varphi = 0$ oder $= 180°$ ist. Doch ist es besser, die Gesamtheit aller Zweige, die durch sämtliche Punkte mit $T = 0$ gehen, als eine einzige Kurve zu betrachten (entsprechend dem in der höheren Geometrie allgemein üblichen Gebrauch), und ebenso sämtliche Zweige durch alle Punkte mit $U = 0$. Es ist nun klar, dass die Aufgabe darauf zurückgeführt ist zu zeigen, dass es mindestens einen Punkt in der Ebene gibt, in dem irgendein Zweig der ersten Linie von einem Zweig der zweiten Linie geschnitten wird. Dazu müssen wir die Beschaffenheit dieser Linien näher betrachten.

18.

Zunächst bemerke ich, dass beide Kurven algebraisch sind, und zwar bei Darstellung durch rechtwinklige Koordinaten vom Grad m. Wählt man nämlich den Anfangspunkt der Abszissen in C, die Abszissen x in Richtung G und die Ordinaten y in Richtung P, so gilt $x = r\cos\varphi$, $y = r\sin\varphi$ und daher allgemein, welchen Wert n auch haben mag,

$$\begin{aligned} r^n \sin n\varphi &= nx^{n-1}y - \frac{n\,.\,n-1\,.\,n-2}{1\,.\,2\,.\,3}x^{n-3}y^3 \\ &\quad + \frac{n\,\ldots\,n-4}{1\,\ldots\,.5}x^{n-5}y^5 - \text{usw.}, \\ r^n \cos n\varphi &= x^n - \frac{n\,.\,n-1}{1\,.\,2}x^{n-2}yy \\ &\quad + \frac{n\,.\,n-1\,.\,n-2\,.\,n-3}{1\,.\,2\,.\,3\,.\,4}x^{n-4}y^4 - \text{usw.} \end{aligned}$$

Also bestehen sowohl T als auch U aus mehreren Gliedern der Form $ax^\alpha y^\beta$, wobei α und β positive ganze Zahlen bezeichnen, deren Summe im größten Fall $= m$ ist. Ferner lässt sich leicht voraussehen, dass alle Glieder von T den Faktor y enthalten und die erste Linie somit eigentlich aus einer Geraden (mit der Gleichung $y = 0$) und einer Kurve vom Grad $m - 1$ zusammengesetzt ist; doch brauchen wir auf diese Unterscheidung hier nicht einzugehen.

Wichtiger wird die Untersuchung sein, ob die erste und die zweite Linie ins Unendliche verlaufende Arme besitzen und wie viele und welcher Art diese sind. In unendlicher Entfernung vom Punkt C fällt die erste Linie, deren Gleichung $\sin m\varphi + \frac{A}{r}\sin(m-1)\varphi + \frac{B}{rr}\sin(m-2)\varphi$ usw. $= 0$ lautet, mit der Linie zusammen, deren Gleichung $\sin m\varphi = 0$ ist. Diese stellt m Geraden dar, die sich im Punkt C schneiden. Die erste ist die Achse GCG'; die übrigen sind gegen sie unter den Winkeln $\frac{1}{m}180$, $\frac{2}{m}180$, $\frac{3}{m}180$ usw. Grad geneigt. Die erste Linie besitzt daher $2m$ unendliche Zweige, welche den Umfang eines mit unendlichem Radius beschriebenen Kreises in $2m$ gleiche Teile zerlegen: Der erste Zweig schneidet den Umfang im Schnittpunkt von Kreis und Achse, der zweite im Abstand $\frac{1}{m}180°$, der dritte im Abstand $\frac{2}{m}180°$ usw. Ebenso besitzt

die zweite Linie in unendlicher Entfernung vom Mittelpunkt eine durch die Gleichung $\cos m\varphi = 0$ ausgedrückte Asymptote. Diese ist eine Gesamtheit von m Geraden, die sich ebenfalls im Punkt C unter gleichen Winkeln schneiden, jedoch so, dass die erste mit der Achse CG den Winkel $\frac{1}{m}90°$ bildet, die zweite den Winkel $\frac{3}{m}90°$, die dritte den Winkel $\frac{5}{m}90°$ usw. Daher besitzt auch die zweite Linie $2m$ unendliche Zweige, von denen jeder die Mitte zwischen zwei benachbarten Zweigen der ersten Linie einnimmt. Sie schneiden also den Umfang eines mit unendlich großem Radius beschriebenen Kreises in Punkten, deren Winkelabstände von der Achse $\frac{1}{m}90°$, $\frac{3}{m}90°$, $\frac{5}{m}90°$ usw. betragen. Ferner ist klar, dass die Achse selbst stets zwei unendliche Zweige der ersten Linie bildet, nämlich den ersten und den an der Stelle $m+1$. Sehr deutlich zeigt sich diese Lage der Zweige in Fig. 2, die für den Fall $m = 4$ gezeichnet ist. Die Zweige der zweiten Linie sind dort zur Unterscheidung von denen der ersten punktiert dargestellt; dasselbe gilt auch für die vierte Figur[*]. — Da diese Folgerungen aber von größter Bedeutung sind und unendlich große Größen bei manchen Lesern Anstoß erregen könnten, werde ich im nächsten Artikel zeigen, wie man sie auch ohne die Hilfe von Unendlichkeiten herleiten kann.

19.

Satz. *Bleibt alles wie oben, so lässt sich um den Mittelpunkt C ein Kreis beschreiben, auf dessen Umfang $2m$ Punkte mit $T = 0$ und ebenso viele mit $U = 0$ liegen, und zwar so, dass jeder der letzteren zwischen zweien der ersteren liegt.*

Die Summe aller positiv genommenen Koeffizienten A, B usw. K, L, M sei $= S$, und man wähle R zugleich $> S\sqrt{2}$ und > 1[*]. Dann behaupte ich, dass für den mit dem Radius R beschriebenen Kreis notwendig gilt, was der Satz ausspricht. Der Kürze halber bezeichne man den Punkt dieses Umfangs, der $\frac{1}{m}45$ Grad von dessen Schnitt mit dem linken Teil der Achse entfernt ist, oder für den $\varphi = \frac{1}{m}45°$ gilt, mit (1); ebenso den Punkt im Abstand $\frac{3}{m}45°$ von diesem Schnitt, oder für den $\varphi = \frac{3}{m}45°$ gilt, mit (3); ferner den Punkt mit $\varphi = \frac{5}{m}45°$ mit (5) usw. bis zu $(8m-1)$. Dieser liegt $\frac{8m-1}{m}45$ Grad von jenem Schnitt entfernt, wenn man stets in derselben Richtung fortschreitet (oder $\frac{1}{m}45°$ in der entgegengesetzten Richtung). So erhält man insgesamt $4m$ Punkte auf dem Umfang in gleichen Abständen. Zwischen $(8m-1)$ und (1) liegt ein Punkt mit $T = 0$; ebenso liegt je ein solcher Punkt zwischen (3) und (5), zwischen (7) und (9), zwischen (11) und (13) usw., sodass ihre Anzahl

[*] Die vierte Figur wurde unter der Annahme $X = x^4 - 2xx + 3x + 10$ gezeichnet, sodass Leser, die mit allgemeinen und abstrakten Untersuchungen weniger vertraut sind, die gegenseitige Lage beider Kurven an einem konkreten Fall betrachten können. Die Länge der Linie CG wurde als $= 10$ angenommen ($CN = 1{,}26255$.)

[*] Ist $S > \sqrt{\frac{1}{2}}$, so folgt die zweite Bedingung aus der ersten; ist dagegen $S < \sqrt{\frac{1}{2}}$, so folgt die erste aus der zweiten.

$2m$ beträgt. Auf dieselbe Weise liegen je einzelne Punkte mit $U = 0$ zwischen (1) und (3), zwischen (5) und (7), zwischen (9) und (11); ihre Anzahl ist also ebenfalls $= 2m$. Außer diesen $4m$ Punkten gibt es schließlich auf dem ganzen Umfang keine weiteren, in denen entweder T oder U den Wert $= 0$ hat.

Beweis. I. Im Punkt (1) ist $m\varphi = 45^\circ$ und daher

$$T = R^{m-1}(R\sqrt{\tfrac{1}{2}} + A\sin(m-1)\varphi + \tfrac{B}{R}\sin(m-2)\varphi + \text{usw.} + \tfrac{L}{R^{m-2}}\sin\varphi)$$

Die Summe $A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi$ usw. kann aber gewiss nicht größer als S sein und ist daher notwendig kleiner als $R\sqrt{\frac{1}{2}}$. Daraus folgt, dass der Wert von T in diesem Punkt gewiss positiv ist. Umso mehr hat also T einen positiven Wert, wenn $m\varphi$ zwischen 45° und 135° liegt, d. h. der Wert von T ist vom Punkt (1) bis (3) stets positiv. Aus demselben Grund hat T vom Punkt (9) bis (11) überall einen positiven Wert und allgemein von jedem Punkt $(8k+1)$ bis $(8k+3)$, wobei k eine beliebige ganze Zahl bezeichnet. Ebenso hat T überall zwischen (5) und (7), zwischen (13) und (15) usw. und allgemein zwischen $(8k+5)$ und $(8k+7)$ einen negativen Wert; in allen diesen Intervallen kann es also nirgends $= 0$ sein. Da dieser Wert aber in (3) positiv und in (5) negativ ist, muss er irgendwo zwischen (3) und (5) $= 0$ sein; ebenso irgendwo zwischen (7) und (9), zwischen (11) und (13) usw. bis einschließlich des Intervalls zwischen $(8m-1)$ und (1), sodass insgesamt in $2m$ Punkten $T = 0$ gilt. Q. E. P.

II. Dass es außer diesen $2m$ Punkten keine weiteren mit dieser Eigenschaft gibt, erkennt man folgendermaßen. Da zwischen (1) und (3), zwischen (5) und (7) usw. keine solchen Punkte liegen, könnte es mehr davon nur geben, wenn in irgendeinem Intervall zwischen (3) und (5) oder zwischen (7) und (9) usw. mindestens zwei lägen. Dann müsste aber T irgendwo in demselben Intervall ein *Maximum* oder *Minimum* sein, und daher wäre $\frac{\mathrm{d}T}{\mathrm{d}\varphi} = 0$. Es ist jedoch $\frac{\mathrm{d}T}{\mathrm{d}\varphi} = mR^{m-2}(R\cos m\varphi + \frac{m-1}{m}A\cos(m-1)\varphi + \text{usw.})$, und $\cos m\varphi$ ist zwischen (3) und (5) stets negativ und $> \sqrt{\frac{1}{2}}$. Daraus erkennt man leicht, dass $\frac{\mathrm{d}T}{\mathrm{d}\varphi}$ in diesem ganzen Intervall eine negative Größe ist; ebenso ist es zwischen (7) und (9) überall positiv, zwischen (11) und (13) negativ usw. Es kann also in keinem dieser Intervalle 0 sein, und die Annahme kann nicht bestehen. Folglich usw. Q. E. S.

III. Ganz ebenso beweist man, dass U überall zwischen (3) und (5), zwischen (11) und (13) usw. und allgemein zwischen $(8k+3)$ und $(8k+5)$ einen negativen Wert hat, dagegen zwischen (7) und (9), zwischen (15) und (17) usw. und allgemein zwischen $(8k+7)$ und $(8k+9)$ einen positiven. Daraus folgt sofort, dass irgendwo zwischen (1) und (3), zwischen (5) und (7) usw., also in $2m$ Punkten, $U = 0$ gelten muss. In keinem dieser Intervalle kann aber $\frac{\mathrm{d}U}{\mathrm{d}\varphi} = 0$ sein (was man leicht ebenso wie oben beweist). Daher gibt es auf dem Kreisumfang nicht mehr als jene $2m$ Punkte, in denen $U = 0$ gilt. Q. E. T. und Q.

Der Teil des Satzes, wonach es nicht mehr als $2m$ Punkte mit $T = 0$ und nicht mehr als $2m$ Punkte mit $U = 0$ gibt, lässt sich übrigens auch daraus beweisen, dass die Gleichungen $T = 0$, $U = 0$ Kurven vom Grad m darstellen. Aus der höheren Geometrie ist bekannt, dass solche Kurven von einem Kreis als Kurve zweiten Grades nicht in mehr als $2m$ Punkten geschnitten werden können.

20.

Beschreibt man um denselben Mittelpunkt einen anderen Kreis mit einem größeren Radius als R und teilt ihn auf dieselbe Weise, so liegt auch auf ihm zwischen den Punkten (3) und (5) ein Punkt mit $T = 0$, ebenso zwischen (7) und (9) usw. Man erkennt leicht, dass solche zwischen (3) und (5) auf den beiden Umfängen liegenden Punkte einander umso näher sein müssen, je weniger sich der Radius dieses Kreises vom Radius R unterscheidet. Dasselbe gilt, wenn man einen Kreis mit einem etwas kleineren Radius als R beschreibt, der jedoch größer als $S\sqrt{2}$ und 1 bleibt. Daraus versteht man ohne Mühe, dass der Umfang des mit dem Radius R beschriebenen Kreises in dem Punkt zwischen (3) und (5), in dem $T = 0$ gilt, tatsächlich von irgendeinem Zweig der ersten Linie *geschnitten* wird; dasselbe gilt für die übrigen Punkte mit $T = 0$. Ebenso ist klar, dass der Umfang dieses Kreises in allen $2m$ Punkten mit $U = 0$ von irgendeinem Zweig der zweiten Linie geschnitten wird. Diese Folgerungen lassen sich auch so ausdrücken: Beschreibt man um den Mittelpunkt C einen Kreis von der erforderlichen Größe, so treten $2m$ Zweige der ersten Linie und ebenso viele der zweiten in ihn ein, und zwar so, dass je zwei benachbarte Zweige der ersten Linie durch irgendeinen Zweig der zweiten voneinander getrennt werden. Siehe Fig. 2, in der der Kreis nun eine endliche statt einer unendlichen Größe hat. Die den einzelnen Zweigen beigeschriebenen Zahlen dürfen nicht mit den Zahlen verwechselt werden, mit denen ich im vorigen und in diesem Artikel der Kürze halber bestimmte Grenzen auf dem Umfang bezeichnet habe.

21.

Aus dieser gegenseitigen Lage der in den Kreis eintretenden Zweige lässt sich die Notwendigkeit eines Schnittes irgendeines Zweiges der ersten Linie mit einem Zweig der zweiten innerhalb des Kreises auf so viele verschiedene Arten herleiten, dass ich beinahe nicht weiß, welche Methode vor den übrigen zu wählen ist. Am deutlichsten scheint mir die folgende. Bezeichnen wir (Fig. 2) den Punkt des Kreisumfangs, in dem er vom linken Teil der Achse geschnitten wird (der selbst einer der $2m$ Zweige der ersten Linie ist), mit 0; den nächsten Punkt, in dem ein Zweig der zweiten Linie eintritt, mit 1; den darauf folgenden, in dem der zweite Zweig der ersten Linie eintritt, mit 2; und so fort bis $4m - 1$. Damit tritt in jedem mit einer geraden Zahl bezeichneten Punkt ein Zweig der zweiten Linie in den Kreis ein, dagegen ein Zweig der zweiten

Linie in allen mit ungeraden Zahlen bezeichneten Punkten. Aus der höheren Geometrie ist nun bekannt, dass jede algebraische Kurve (oder jeder einzelne Teil einer algebraischen Kurve, falls sie aus mehreren zusammengesetzt ist) entweder in sich zurückkehrt oder nach beiden Seiten ins Unendliche verläuft. Tritt also irgendein Zweig einer algebraischen Kurve in ein begrenztes Gebiet ein, so muss er es notwendig irgendwo wieder verlassen[*]. Daraus schließt man leicht, dass jeder mit einer geraden Zahl bezeichnete Punkt (oder der Kürze halber *jeder gerade Punkt*) innerhalb des Kreises durch einen Zweig der ersten Linie mit einem anderen geraden Punkt verbunden sein muss; ebenso jeder mit einer ungeraden Zahl bezeichnete Punkt durch einen Zweig der zweiten Linie mit einem anderen solchen Punkt. Obwohl diese Verbindung von je zwei Punkten je nach der Beschaffenheit des Polynoms X sehr verschieden sein und daher nicht allgemein bestimmt werden kann, lässt sich doch leicht beweisen, dass *sie, wie sie auch beschaffen sein mag, stets einen Schnitt der ersten mit der zweiten Linie hervorbringt.*

22.

Der Beweis dieser Notwendigkeit lässt sich wohl am bequemsten durch Widerspruch führen. Nehmen wir also an, die Verbindung je zweier gerader und je zweier ungerader Punkte könne so eingerichtet werden, dass daraus kein Schnitt eines Zweiges der ersten Linie mit einem Zweig der zweiten entsteht. Da die Achse ein Teil der ersten Linie ist, ist offenbar der Punkt 0 mit dem Punkt $2m$ verbunden. Der Punkt 1 kann daher mit keinem jenseits der Achse liegenden Punkt verbunden sein, d. h. mit keinem Punkt, der durch eine größere Zahl als $2m$ bezeichnet wird; sonst würde die Verbindungslinie notwendig die Achse schneiden. Nimmt man also

[*]Es scheint gewiss hinreichend gut bewiesen zu sein, dass eine algebraische Kurve weder irgendwo plötzlich abbrechen kann (wie es etwa bei der transzendenten Kurve mit der Gleichung $y = \frac{1}{\log x}$ geschieht), noch sich nach unendlich vielen Windungen gleichsam in irgendeinem Punkt verlieren kann (wie die logarithmische Spirale); und meines Wissens hat niemand dagegen einen Zweifel erhoben. Sollte dennoch jemand einen Beweis verlangen, der keinerlei Zweifeln ausgesetzt ist, so werde ich es übernehmen, ihn bei einer anderen Gelegenheit zu geben. Im vorliegenden Fall ist aber klar: Verließe irgendein Zweig, etwa 2, den Kreis nirgends wieder (Fig. 3), so könnte man zwischen 0 und 2 in den Kreis eintreten, dann um diesen ganzen Zweig herumgehen (der sich im Kreisgebiet verlieren müsste) und schließlich zwischen 2 und 4 wieder aus dem Kreis austreten, ohne auf dem ganzen Weg irgendwo die erste Linie zu treffen. Dass dies widersinnig ist, erkennt man daran, dass man beim Eintritt in den Kreis die erste Fläche über sich hatte, beim Austritt aber unter sich. Man müsste daher notwendig irgendwo auf die erste Fläche selbst, also auf einen Punkt der ersten Linie getroffen sein. — Aus dieser Überlegung, die sich auf Grundsätze der Geometrie der Lage stützt, die nicht weniger gültig sind als die der Geometrie der Größe, folgt übrigens nur, dass man, wenn man auf irgendeinem Zweig der ersten Linie in den Kreis eintritt, an einer anderen Stelle wieder austreten kann, wobei man stets auf der ersten Linie bleibt; nicht aber, dass der Weg eine stetige Linie in dem Sinne ist, wie man es in der höheren Geometrie versteht. Hier genügt jedoch, dass der Weg im gewöhnlichen Sinne eine stetige Linie ist, d. h. nirgends unterbrochen, sondern überall zusammenhängend.

an, 1 sei mit dem Punkt n verbunden, so ist $n < 2m$. Aus einem ähnlichen Grund gilt $n' < n$, wenn man annimmt, 2 sei mit n' verbunden; sonst würde nämlich der Zweig $2 \ldots n'$ notwendig den Zweig $1 \ldots n$ schneiden. Aus demselben Grund ist der Punkt 3 mit einem der zwischen 4 und n' liegenden Punkte verbunden. Nimmt man an, 3, 4, 5 usw. seien mit n'', n''', n'''' usw. verbunden, so liegt offenbar n''' zwischen 5 und n'', n'''' zwischen 6 und n''' usw. Es ist also klar, dass man schließlich zu irgendeinem Punkt h gelangt, der mit dem Punkt $h + 2$ verbunden ist. Dann schneidet der Zweig, der im Punkt $h + 1$ in den Kreis eintritt, notwendig den Zweig, der die Punkte h und $h + 2$ verbindet. Da aber der eine dieser beiden Zweige zur ersten Linie und der andere zur zweiten gehört, ist nun klar, dass die Annahme widersprüchlich ist und daher notwendig irgendwo ein Schnitt der ersten mit der zweiten Linie stattfindet. Verbindet man dies mit dem Vorhergehenden, so ergibt sich aus allen dargelegten Untersuchungen, dass der Satz, *jedes Polynom in einer Variablen lasse sich in reelle Faktoren ersten oder zweiten Grades zerlegen*, mit voller Strenge bewiesen ist.

23.

Aus denselben Grundsätzen lässt sich übrigens ohne große Schwierigkeit herleiten, dass es nicht nur einen, sondern mindestens m Schnitte der ersten mit der zweiten Linie gibt. Allerdings kann die erste Linie auch von mehreren Zweigen der zweiten im selben Punkt geschnitten werden; in diesem Fall besitzt das Polynom X mehrere gleiche Faktoren. Da es hier jedoch genügt, die Notwendigkeit eines einzigen Schnittes bewiesen zu haben, halte ich mich der Kürze halber nicht länger dabei auf. Aus demselben Grund gehe ich hier auch auf andere Eigenschaften dieser Linien nicht näher ein, etwa darauf, dass die Schnitte stets unter rechten Winkeln erfolgen; oder dass, wenn mehrere Arme beider Kurven in demselben Punkt zusammenkommen, ebenso viele Arme der ersten wie der zweiten Linie vorhanden sind, die abwechselnd liegen und sich unter gleichen Winkeln schneiden usw.

Schließlich bemerke ich, dass es keineswegs unmöglich ist, den vorigen Beweis, den ich hier auf geometrische Grundsätze gestützt habe, auch in rein analytischer Form darzustellen. Doch glaubte ich, die hier entwickelte Darstellung werde weniger abstrakt ausfallen und die eigentliche Kraft des Beweises werde hier viel deutlicher vor Augen geführt, als von einem analytischen Beweis zu erwarten wäre.

Zum Abschluss werde ich noch eine andere Methode zum Beweis unseres Satzes andeuten. Auf den ersten Blick wird sie nicht nur von dem vorigen Beweis, sondern auch von allen übrigen oben angeführten Beweisen sehr verschieden erscheinen; ihrem Wesen nach ist sie dennoch eigentlich dieselbe wie die von D'Alembert. Den Vergleich mit dieser und die Untersuchung der Parallele zwischen beiden überlasse ich den Sachkundigen, allein für die sie hinzugefügt ist.

24.

Über der Ebene von Fig. 4 denke ich mir die erste und die zweite Fläche in Bezug auf die Achse CG und den festen Punkt C auf dieselbe Weise wie oben beschrieben. Man nehme irgendeinen Punkt auf irgendeinem Zweig der ersten Linie, also einen Punkt mit $T = 0$ (etwa einen beliebigen Punkt M auf der Achse). Gilt in ihm nicht auch $U = 0$, so gehe man von diesem Punkt auf der ersten Linie in der Richtung weiter, in der der absolute Betrag von U abnimmt. Nimmt im Punkt M der absolute Betrag von U nach beiden Seiten ab, so ist es gleichgültig, in welcher Richtung man weitergeht; was zu tun ist, wenn U nach beiden Seiten wächst, werde ich sogleich zeigen. Es ist also klar, dass man, wenn man stets auf der ersten Linie weitergeht, notwendig schließlich zu einem Punkt gelangt, in dem $U = 0$ gilt, oder zu einem solchen, in dem der Wert von U ein Minimum wird, etwa zum Punkt N. Im ersten Fall ist das Gesuchte gefunden. Im zweiten lässt sich beweisen, dass sich in diesem Punkt mehrere Zweige der ersten Linie schneiden (und zwar eine gerade Anzahl von Zweigen), von denen die Hälfte so beschaffen ist, dass beim Abbiegen in einen von ihnen (nach dieser oder jener Seite) der Wert von U weiterhin abnimmt. (Den Beweis dieses Satzes, der eher lang als schwierig ist, muss ich der Kürze halber weglassen.) Auf diesem Zweig kann man also wieder weitergehen, bis U entweder $= 0$ wird (wie es in Fig. 4 in P geschieht) oder wiederum ein Minimum. Dann biegt man erneut ab und gelangt notwendig schließlich zu einem Punkt, in dem $U = 0$ gilt.

Gegen diesen Beweis könnte man den Zweifel vorbringen, ob es nicht möglich sei, dass, wie weit man auch fortschreitet und obwohl der Wert von U stets abnimmt, diese Abnahmen doch immer langsamer werden und jener Wert irgendeine Grenze nirgends erreicht. Dieser Einwand entspräche dem vierten in Artikel 6. Es wäre aber nicht schwer, eine Grenze anzugeben, jenseits deren sich der Wert von U notwendig nicht nur immer schneller ändern muss, sondern auch nicht mehr *abnehmen* kann. Der Wert 0 muss also notwendig schon vor dem Erreichen dieser Grenze vorgekommen sein. Dies und das Übrige, was ich in diesem Beweis nur andeuten konnte, behalte ich mir für eine andere Gelegenheit zu einer ausführlicheren Behandlung vor.

Die Grundsätze, auf denen dieser Beweis beruht, haben wir Anfang Oktober 1797 *entdeckt.*

Fig 1.

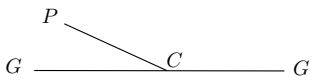


Fig.2.

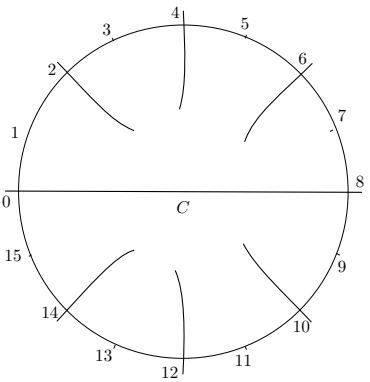


Fig 4

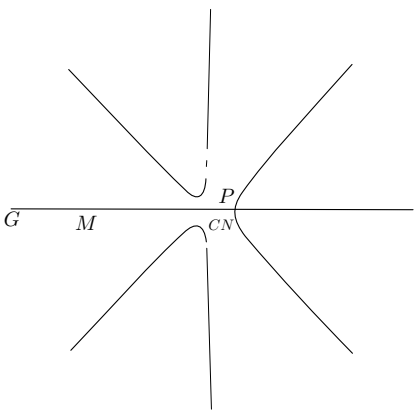
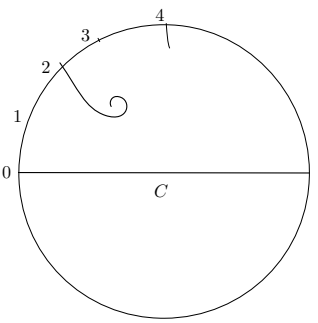


Fig 3



Gauss, Werke, Band III, Seite 30

EIN WEITERER NEUER BEWEIS

DES SATZES

DASS JEDES POLYNOM

IN EINER VARIABLEN

IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES

ZERLEGT WERDEN KANN

V O N

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
VORGELEGT, 1815, DEZEMBER 7.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. III.

Göttingen MDCCCXVI.

EIN WEITERER NEUER BEWEIS DES SATZES, DASS JEDES POLYNOM IN EINER VARIABLEN IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES ZERLEGT WERDEN KANN.

1.

Obwohl der Beweis des Satzes über die Zerlegung von Polynomen in Faktoren, den ich in einer vor sechzehn Jahren veröffentlichten Abhandlung gegeben habe, sowohl an Strenge als auch an Einfachheit nichts zu wünschen übrig zu lassen scheint, hoffe ich doch, dass es den Mathematikern nicht unwillkommen sein wird, wenn ich auf dieselbe höchst wichtige Frage zurückkomme und versuche, einen anderen, nicht weniger strengen Beweis aus ganz anderen Grundsätzen zu begründen. Jener frühere Beweis hängt nämlich wenigstens zum Teil von geometrischen Betrachtungen ab; der Beweis, den ich hier darzustellen beginne, wird dagegen auf rein analytischen Grundsätzen beruhen. In der angeführten Abhandlung habe ich die bedeutenderen analytischen Methoden besprochen, mit denen andere Mathematiker bis dahin unseren Satz zu beweisen versucht hatten, und ihre Mängel ausführlich dargelegt. Der schwerwiegendste und tatsächlich grundlegende dieser Mängel ist allen jenen Versuchen ebenso wie den neueren, die mir bekannt geworden sind, gemeinsam. Doch habe ich schon damals erklärt, dass er bei einem analytischen Beweis keineswegs unvermeidlich zu sein scheint. Die Sachkundigen mögen nun beurteilen, ob die damals gegebene Zusage durch diese neuen Bemühungen vollständig eingelöst ist.

2.

Der Hauptuntersuchung werden einige Voruntersuchungen vorausgeschickt, sowohl damit nicht der Eindruck entsteht, etwas fehle, als auch weil ihre Behandlung vielleicht selbst auf Dinge, die andere bereits berührt haben, noch etwas neues Licht werfen kann. Zunächst werden wir den größten gemeinsamen Teiler zweier Polynome in einer Unbestimmten behandeln. Dabei sei vorweg bemerkt, dass hier stets nur von Polynomen die Rede ist: Bildet man aus zweien von ihnen ein Produkt, so heißt jedes ein *Teiler* dieses Produkts. Der *Grad* eines Teilers bestimmt sich nach dem Exponenten der höchsten darin vorkommenden Potenz der Unbestimmten, ohne jede Rücksicht auf die Zahlenkoeffizienten. Im Übrigen können wir die Eigenschaften gemeinsamer

Teiler von Polynomen umso kürzer behandeln, als sie denen der gemeinsamen Teiler von Zahlen vollkommen entsprechen.

Sind zwei Polynome Y, Y' in der Unbestimmten x gegeben, von denen das erste einen höheren oder wenigstens keinen niedrigeren Grad als das zweite hat, so bilden wir die folgenden Gleichungen:

$$\begin{gathered} Y = qY' + Y'' \\ Y' = q'Y'' + Y''' \\ Y'' = q''Y''' + Y'''' \\ \text{usw. bis} \\ Y^{(\mu-1)} = q^{(\mu-1)}Y^{(\mu)} \end{gathered}$$

Dabei gilt folgende Regel: Zuerst wird Y auf die übliche Weise durch Y' dividiert; dann Y' durch den Rest Y'' der ersten Division, der einen niedrigeren Grad als Y' hat; dann wieder der erste Rest durch den zweiten, Y''', und so fort, bis man zu einer Division ohne Rest gelangt. Dass dies schließlich notwendig eintreten muss, folgt daraus, dass der Grad der Polynome Y', Y'', Y''' usw. fortwährend abnimmt. Dass diese Funktionen ebenso wie die Quotienten q, q', q'' usw. *Polynome* in x sind, braucht kaum erwähnt zu werden. Danach ist klar:

I. Geht man von der letzten dieser Gleichungen zur ersten zurück, so erkennt man, dass das Polynom $Y^{(\mu)}$ jedes der vorhergehenden teilt und daher gewiss ein gemeinsamer Teiler der vorgegebenen Polynome Y, Y' ist.

II. Geht man von der ersten Gleichung zur letzten weiter, so zeigt sich, dass jeder gemeinsame Teiler der Polynome Y, Y' auch jedes der folgenden und damit auch das letzte, $Y^{(\mu)}$, teilt. Die Polynome Y, Y' können daher keinen gemeinsamen Teiler höheren Grades als $Y^{(\mu)}$ haben. Jeder gemeinsame Teiler desselben Grades wie $Y^{(\mu)}$ steht zu diesem im Verhältnis einer Zahl zu einer Zahl; daher ist dieser selbst als größter gemeinsamer Teiler anzusehen.

III. Hat $Y^{(\mu)}$ den Grad 0, ist es also eine Zahl, so kann keine Funktion der Unbestimmten x im eigentlichen Sinne die Polynome Y, Y' teilen. In diesem Fall sagt man daher, diese Polynome hätten keinen gemeinsamen Teiler.

IV. Man nehme die vorletzte unserer Gleichungen und eliminiere daraus $Y^{(\mu-1)}$ mit Hilfe der drittletzten Gleichung; dann eliminiere man wiederum $Y^{(\mu-2)}$ mit Hilfe der vorhergehenden Gleichung und so fort. Auf diese Weise erhält man

$$\begin{aligned} Y^{(\mu)} &= +kY^{(\mu-2)} - k'Y^{(\mu-1)} \\ &= -k'Y^{(\mu-3)} + k''Y^{(\mu-2)} \\ &= +k''Y^{(\mu-4)} - k'''Y^{(\mu-3)} \\ &= -k'''Y^{(\mu-5)} + k''''Y^{(\mu-4)} \\ &\quad \text{usw.} \end{aligned}$$

wenn man annimmt, die Polynome k, k', k'' usw. seien nach der folgenden Regel gebildet:

$$\begin{aligned} k &= 1 \\ k' &= q^{(\mu-2)} \\ k'' &= q^{(\mu-3)}k' + k \\ k''' &= q^{(\mu-4)}k'' + k' \\ k'''' &= q^{(\mu-5)}k''' + k'' \\ &\quad \text{usw.} \end{aligned}$$

Damit gilt

$$\pm k^{(\mu-2)}Y \mp k^{(\mu-1)}Y' = Y^{(\mu)}$$

wobei die oberen Zeichen für gerades μ und die unteren für ungerades gelten. Haben also Y und Y' keinen gemeinsamen Teiler, so kann man auf diese Weise zwei Polynome Z, Z' in der Unbestimmten x finden, sodass

$$ZY + Z'Y' = 1$$

V. Diese Aussage gilt offenbar auch umgekehrt: Kann die Gleichung

$$ZY + Z'Y' = 1$$

so erfüllt werden, dass Z, Z' Polynome in der Unbestimmten x sind, dann können Y und Y' gewiss keinen gemeinsamen Teiler haben.

3.

Die zweite Voruntersuchung betrifft die Umformung symmetrischer Funktionen. Es seien a, b, c usw. unbestimmte Größen, und ihre Anzahl sei m. Mit λ' bezeichnen wir ihre Summe, mit λ'' die Summe ihrer Produkte aus je zweien, mit λ''' die Summe ihrer Produkte aus je dreien usw., sodass die Entwicklung des Produkts

$$(x-a)(x-b)(x-c)\dots.$$

den Ausdruck

$$x^m - \lambda' x^{m-1} + \lambda'' x^{m-2} - \lambda''' x^{m-3} + \text{usw.}$$

ergibt. Somit sind $\lambda', \lambda'', \lambda'''$ usw. symmetrische Funktionen der Unbestimmten a, b, c usw., d. h. solche, in denen diese Unbestimmten auf dieselbe Weise vorkommen, oder deutlicher: solche, die bei jeder Vertauschung dieser Unbestimmten untereinander unverändert bleiben. Allgemeiner ist offenbar jedes Polynom in $\lambda', \lambda'', \lambda'''$ usw. (ob es nur diese Unbestimmten oder noch andere, von a, b, c usw. unabhängige enthält) ein symmetrisches Polynom in den Unbestimmten a, b, c usw.

4.

Der umgekehrte Satz liegt etwas weniger nahe. Es sei ρ eine symmetrische Funktion der Unbestimmten a, b, c usw.; sie besteht also aus einer bestimmten Anzahl von Gliedern der Form

$$Ma^\alpha b^\beta c^\gamma \dots.$$

wobei α, β, γ usw. nichtnegative ganze Zahlen bezeichnen und M ein bestimmter oder wenigstens von a, b, c usw. unabhängiger Koeffizient ist (falls außer a, b, c usw. noch andere Unbestimmte in die Funktion ρ eingehen). Zunächst legen wir für diese einzelnen Glieder eine bestimmte Ordnung fest. Dazu ordnen wir zuerst die Unbestimmten a, b, c usw. in einer bestimmten, an sich völlig beliebigen Reihenfolge an, etwa so, dass a die erste Stelle einnimmt, b die zweite, c die dritte usw. Von den beiden Gliedern

$$Ma^\alpha b^\beta c^\gamma \dots. \quad \text{und} \quad Ma^{\alpha'} b^{\beta'} c^{\gamma'} \dots.$$

weisen wir dann dem ersten eine höhere Stelle in der Ordnung zu als dem zweiten, wenn

$$\begin{gathered} \text{oder} \quad \alpha > \alpha', \quad \text{oder} \quad \alpha = \alpha' \text{ und } \beta > \beta', \\ \text{oder} \quad \alpha = \alpha', \ \beta = \beta' \text{ und } \gamma > \gamma', \quad \text{oder usw.} \end{gathered}$$

also wenn die erste nicht verschwindende unter den Differenzen $\alpha - \alpha', \beta - \beta', \gamma - \gamma'$ usw. positiv ist. Da Glieder derselben Stelle in der Ordnung sich nur im Koeffizienten M unterscheiden und daher zu einem Glied zusammengefasst werden können, nehmen wir an, dass die einzelnen Glieder der Funktion ρ verschiedene Stellen in der Ordnung einnehmen.

Nun bemerken wir: Ist $Ma^\alpha b^\beta c^\gamma \ldots\ldots$ unter allen Gliedern der Funktion ρ das höchste in dieser Ordnung, so muss α größer oder wenigstens nicht kleiner als β sein. Wäre nämlich $\beta > \alpha$, so hätte das Glied $Ma^\beta b^\alpha c^\gamma \ldots\ldots$, das die Funktion ρ wegen ihrer Symmetrie ebenfalls enthalten muss, eine höhere Stelle als $Ma^\alpha b^\beta c^\gamma \ldots\ldots$, gegen die Voraussetzung. Ebenso ist β größer oder wenigstens nicht kleiner als γ; ferner ist γ nicht kleiner als der nächste Exponent δ usw. Daher sind die einzelnen Differenzen $\alpha - \beta$, $\beta - \gamma, \gamma - \delta$ usw. nichtnegative ganze Zahlen.

Zweitens betrachten wir ein Produkt aus beliebig vielen Polynomen in den Unbestimmten a, b, c usw. Sein höchstes Glied muss das Produkt der höchsten Glieder dieser Faktoren sein. Ebenso ist klar, dass die höchsten Glieder der Funktionen $\lambda', \lambda'', \lambda'''$ usw. jeweils a, ab, abc usw. sind. Daraus folgt, dass das höchste aus dem Produkt

$$p = M\lambda'^{\alpha-\beta}\lambda''^{\beta-\gamma}\lambda'''^{\gamma-\delta}\ldots\ldots$$

hervorgehende Glied $Ma^\alpha b^\beta c^\gamma \ldots\ldots$ ist. Setzt man also $\rho - p = \rho'$, so liegt das höchste Glied der Funktion ρ' in der Ordnung gewiss niedriger als das höchste Glied der Funktion ρ. Offenbar sind aber p und daher auch ρ' symmetrische Polynome in a, b, c usw. Behandelt man daher ρ' ebenso wie vorher ρ, so zerfällt es in $p' + \rho''$, wobei p' ein Produkt aus Potenzen von $\lambda', \lambda'', \lambda'''$ usw., multipliziert mit einem bestimmten oder wenigstens von a, b, c usw. unabhängigen Koeffizienten, ist, während ρ'' ein symmetrisches Polynom in a, b, c usw. ist, dessen höchstes Glied in der Ordnung niedriger liegt als das höchste Glied von ρ'. Fährt man auf dieselbe Weise fort, so wird ρ offenbar schließlich auf die Form $p + p' + p'' + p'''$ usw. gebracht, also in ein Polynom in $\lambda', \lambda'', \lambda'''$ usw. umgeformt.

5.

Den im vorigen Artikel bewiesenen Satz können wir auch so aussprechen: Ist irgendein symmetrisches Polynom ρ in den Unbestimmten a, b, c usw. gegeben, so lässt sich ein Polynom in ebenso vielen anderen Unbestimmten l', l'', l''' usw. angeben, das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in ρ übergeht. Außerdem zeigt man leicht, dass *dies nur auf eine einzige Weise möglich ist.* Nehmen wir nämlich an, zwei verschiedene Funktionen der Unbestimmten l', l'', l''' usw., etwa r und r', ergäben nach den Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. dieselbe Funktion von a, b, c usw. Dann wäre $r - r'$ eine Funktion von l', l'', l''' usw., die für sich nicht verschwindet,

nach jenen Substitutionen aber identisch verschwindet. Dass dies widersinnig ist, erkennen wir leicht, wenn wir bedenken, dass $r - r'$ notwendig aus einer bestimmten Anzahl von Teilen der Form

$$Ml'^{\alpha}l''^{\beta}l'''^{\gamma}\ldots\ldots$$

besteht, deren Koeffizienten M nicht verschwinden und die sich jeweils in ihren Exponenten unterscheiden.

Die aus diesen einzelnen Teilen hervorgehenden höchsten Glieder werden daher durch

$$Ma^{\alpha+\beta+\gamma+\text{usw.}}b^{\beta+\gamma+\text{usw.}}c^{\gamma+\text{usw.}}\ldots\ldots$$

dargestellt und gehören somit verschiedenen Stellen in der Ordnung an, sodass das höchste Glied überhaupt auf keine Weise wegfallen kann.

Die eigentliche Rechnung bei solchen Umformungen ließe sich durch mehrere Abkürzungen erheblich verkürzen. Dabei halten wir uns hier jedoch nicht auf, da für unseren Zweck schon die bloße Möglichkeit der Umformung genügt.

6.

Wir betrachten das Produkt aus $m(m-1)$ Faktoren

$$\begin{aligned}&(a-b)(a-c)(a-d)\ldots\ldots\\ \times&(b-a)(b-c)(b-d)\ldots\ldots\\ \times&(c-a)(c-b)(c-d)\ldots\ldots\\ \times&(d-a)(d-b)(d-c)\ldots\ldots\\ &\text{usw.}\end{aligned}$$

das wir mit π bezeichnen. Da es die Unbestimmten a, b, c usw. symmetrisch enthält, nehmen wir an, es sei auf die Form eines Polynoms in $\lambda', \lambda'', \lambda'''$ usw. gebracht. Dieses Polynom gehe in p über, wenn anstelle von $\lambda', \lambda'', \lambda'''$ usw. jeweils l', l'', l''' usw. eingesetzt werden. Danach nennen wir p die *Determinante* des Polynoms

$$y = x^m - l'x^{m-1} + l''x^{m-2} - l'''x^{m-3} + \text{usw.}$$

So haben wir zum Beispiel für $m = 2$

$$p = -l'^2 + 4l''$$

Ebenso findet man für $m = 3$

$$p = -l'^2l''^2 + 4l'^3l''' + 4l''^3 - 18l'l''l''' + 27l'''^2$$

Die Determinante des Polynoms y ist also ein Polynom in den Koeffizienten l', l'', l''' usw., das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in

das Produkt aus allen Differenzen zwischen je zweien der Größen a, b, c usw. übergeht. Im Fall $m = 1$, wenn also nur eine einzige Unbestimmte a und daher überhaupt keine Differenz vorhanden ist, empfiehlt es sich, die Zahl 1 selbst als Determinante des Polynoms y anzunehmen.

Bei der Festlegung des Begriffs der Determinante mussten die Koeffizienten des Polynoms y als unbestimmte Größen betrachtet werden. Die Determinante eines Polynoms mit bestimmten Koeffizienten,

$$Y = x^m - L'x^{m-1} + L''x^{m-2} - L'''x^{m-3} + \text{usw.}$$

ist eine bestimmte Zahl P, nämlich der Wert des Polynoms p für $l' = L', l'' = L''$, $l''' = L'''$ usw. Nehmen wir also an, Y lasse sich in lineare Faktoren zerlegen,

$$Y = (x - A)(x - B)(x - C)\ldots.$$

oder Y entstehe aus

$$\upsilon = (x - a)(x - b)(x - c)\ldots.$$

indem man $a = A, b = B, c = C$ usw. setzt, sodass dieselben Substitutionen $\lambda', \lambda'', \lambda'''$ usw. jeweils in L', L'', L''' usw. überführen, so ist P offenbar gleich dem Produkt aus den Faktoren

$$\begin{aligned}
&(A - B)(A - C)(A - D)\ldots.\\
\times&(B - A)(B - C)(B - D)\ldots.\\
\times&(C - A)(C - B)(C - D)\ldots.\\
\times&(D - A)(D - B)(D - C)\ldots.\\
&\text{usw.}
\end{aligned}$$

Ist also $P = 0$, so müssen sich unter den Größen A, B, C usw. wenigstens zwei gleiche befinden; ist dagegen nicht $P = 0$, so sind sämtliche Größen A, B, C usw. notwendig ungleich. Nun bemerken wir: Setzt man $\frac{\mathrm{d}Y}{\mathrm{d}x} = Y'$, oder

$$\begin{aligned}
Y' = mx^{m-1} - (m-1)L'x^{m-2} + (m-2)L''x^{m-3}\\
-(m-3)L'''x^{m-4} + \text{usw.}
\end{aligned}$$

so gilt

$$\begin{aligned}
Y' = &(x - B)(x - C)(x - D)\ldots.\\
&+ (x - A)(x - C)(x - D)\ldots.\\
&+ (x - A)(x - B)(x - D)\ldots.\\
&+ (x - A)(x - B)(x - C)\ldots.\\
&+ \text{usw.}
\end{aligned}$$

Sind also zwei der Größen A, B, C usw. gleich, etwa $A = B$, so ist Y' durch $x - A$ teilbar; mit anderen Worten, Y und Y' enthalten den gemeinsamen Teiler $x - A$. Nimmt man umgekehrt an, Y' habe mit Y irgendeinen gemeinsamen Teiler, so muss Y' einen der linearen Faktoren $x - A, x - B, x - C$ usw. enthalten, etwa den ersten, $x - A$. Dies kann offenbar nur geschehen, wenn A einer der übrigen Größen B, C, D usw. gleich ist. Aus alledem erhalten wir also zwei SÄTZE:

I. *Ist die Determinante des Polynoms* $Y = 0$*, so hat* Y *gewiss mit* Y' *einen gemeinsamen Teiler; haben also* Y *und* Y' *keinen gemeinsamen Teiler, so kann die Determinante des Polynoms* Y *nicht* $= 0$ *sein.*

II. *Ist die Determinante des Polynoms* Y *nicht* $= 0$*, so können* Y *und* Y' *gewiss keinen gemeinsamen Teiler haben; oder, wenn* Y *und* Y' *einen gemeinsamen Teiler haben, muss die Determinante des Polynoms* Y *notwendig* $= 0$ *sein.*

7.

Doch ist sorgfältig zu beachten, dass die ganze Kraft dieses sehr einfachen Beweises auf der Annahme beruht, das Polynom Y lasse sich in lineare Faktoren zerlegen. Gerade hier, wo die allgemeine Möglichkeit dieser Zerlegung bewiesen werden soll, wäre diese Annahme nichts anderes als eine Vorwegnahme des zu Beweisenden. Dennoch haben sich nicht alle, die analytische Beweise des Hauptsatzes versucht haben, vor genau solchen Fehlschlüssen gehütet. Den Ursprung dieses täuschenden Anscheins haben wir schon in der Formulierung der Untersuchung selbst bemerkt: Alle haben nur nach der *Form* der Wurzeln von Gleichungen gefragt, während sie deren voreilig angenommene *Existenz* hätten beweisen müssen. Doch ist über dieses Vorgehen, das sich allzu weit von Strenge und Klarheit entfernt, schon in der oben angeführten Abhandlung genug gesagt worden. Wir werden daher nun die Sätze des vorigen Artikels, von denen wir für unseren Zweck wenigstens einen nicht entbehren können, auf eine festere Grundlage stellen. Wir beginnen mit dem zweiten als dem leichteren.

8.

Wir bezeichnen mit ρ die Funktion

$$\begin{aligned}&\frac{\pi(x-b)(x-c)(x-d)\ldots..}{(a-b)^2(a-c)^2(a-d)^2\ldots..}\\&+\frac{\pi(x-a)(x-c)(x-d)\ldots..}{(b-a)^2(b-c)^2(b-d)^2\ldots..}\\&+\frac{\pi(x-a)(x-b)(x-d)\ldots..}{(c-a)^2(c-b)^2(c-d)^2\ldots..}\\&+\frac{\pi(x-a)(x-b)(x-c)\ldots..}{(d-a)^2(d-b)^2(d-c)^2\ldots..}\\&+\text{usw.}\end{aligned}$$

die, weil π durch jeden einzelnen Nenner teilbar ist, ein Polynom in den Unbestimmten x, a, b, c usw. ist. Ferner setzen wir $\frac{\mathrm{d}\upsilon}{\mathrm{d}x} = \upsilon'$, sodass gilt

$$\begin{aligned}\upsilon' = {}&(x-b)(x-c)(x-d)\ldots..\\&+(x-a)(x-c)(x-d)\ldots..\\&+(x-a)(x-b)(x-d)\ldots..\\&+(x-a)(x-b)(x-c)\ldots..\\&+\text{usw.}\end{aligned}$$

Für $x = a$ gilt offenbar $\rho\upsilon' = \pi$. Daraus schließen wir, dass das Polynom $\pi - \rho\upsilon'$ identisch durch $x - a$ und ebenso durch $x - b, x - c$ usw. sowie durch ihr Produkt υ teilbar ist. Setzen wir also

$$\frac{\pi - \rho\upsilon'}{\upsilon} = \sigma$$

so ist σ ein Polynom in den Unbestimmten x, a, b, c usw., das wie ρ hinsichtlich der Unbestimmten a, b, c usw. symmetrisch ist. Es lassen sich daher zwei Polynome r, s in den Unbestimmten x, l', l'', l''' usw. finden, die durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. jeweils in ρ, σ übergehen. Bezeichnen wir nun entsprechend das Polynom

$$\begin{aligned}&mx^{m-1} - (m-1)l'x^{m-2} + (m-2)l''x^{m-3}\\&-(m-3)l'''x^{m-4} + \text{usw.}\end{aligned}$$

also die Ableitung $\frac{\mathrm{d}y}{\mathrm{d}x}$, mit y', sodass y' durch dieselben Substitutionen in υ' übergeht, so geht offenbar $p - sy - ry'$ durch dieselben Substitutionen in $\pi - \sigma\upsilon - \rho\upsilon'$, also in 0 über und muss daher schon für sich identisch verschwinden (Artikel 5). Wir haben somit die identische Gleichung

$$p = sy + ry'$$

Nehmen wir nun an, durch die Substitution $l' = L', l'' = L'', l''' = L'''$ usw. ergebe sich $r = R, s = S$, so gilt ebenfalls identisch

$$P = SY + RY'$$

Da hier S, R Polynome in x sind, P dagegen eine bestimmte Größe oder Zahl ist, folgt von selbst, dass Y und Y' keinen gemeinsamen Teiler haben können, wenn nicht $P = 0$ ist. Dies ist genau der zweite Satz von Artikel 6.

9.

Den Beweis des ersten Satzes werden wir so abschließen, dass wir zeigen: Haben Y und Y' keinen gemeinsamen Teiler, so kann gewiss nicht $P = 0$ gelten. Dazu nehmen wir zunächst an, nach den Vorschriften von Artikel 2 seien zwei Polynome in der Unbestimmten x, nämlich fx und φx, gefunden worden, sodass die identische Gleichung

$$fx \,.\, Y + \varphi x \,.\, Y' = 1$$

gilt. Wir schreiben sie hier in der Form

$$fx \,.\, \upsilon + \varphi x \,.\, \upsilon' = 1 + fx \,.\, (\upsilon - Y) + \varphi x \,.\, \frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x}$$

oder, da

$$\begin{aligned} \upsilon' = {} & (x-b)(x-c)(x-d)\ldots. \\ & + (x-a) \,.\, \frac{\mathrm{d}[(x-b)(x-c)(x-d)\ldots.]}{\mathrm{d}x} \end{aligned}$$

gilt, in der folgenden Form:

$$\begin{aligned} & \varphi x \,.\, (x-b)(x-c)(x-d)\ldots. \\ & + \varphi x \,.\, (x-a) \,.\, \frac{\mathrm{d}[(x-b)(x-c)(x-d)\ldots.]}{\mathrm{d}x} \\ & + fx \,.\, (x-a)(x-b)(x-c)(x-d)\ldots. \\ & = 1 + fx \,.\, (\upsilon - Y) + \varphi x \,.\, \frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x} \end{aligned}$$

Der Kürze halber bezeichnen wir das Polynom

$$fx\,.\,(y-Y)+\varphi x\,.\,\frac{\mathrm{d}(y-Y)}{\mathrm{d}x}$$

in den Unbestimmten x, l', l'', l''' usw.

$$\text{mit}\quad F(x, l', l'', l''' \text{ usw.})$$

Damit gilt identisch

$$\begin{aligned}1+fx\,.\,(\upsilon-Y)+\varphi x\,.\,\frac{\mathrm{d}(\upsilon-Y)}{\mathrm{d}x}\\ =1+F(x,\lambda',\lambda'',\lambda''' \text{ usw.})\end{aligned}$$

Wir erhalten also die identischen Gleichungen [1]

$$\begin{aligned}&\varphi a\,.\,(a-b)(a-c)(a-d)\ldots.\\ &=1+F(a,\lambda',\lambda'',\lambda''' \text{ usw.})\\ &\varphi b\,.\,(b-a)(b-c)(b-d)\ldots.\\ &=1+F(b,\lambda',\lambda'',\lambda''' \text{ usw.})\\ &\varphi c\,.\,(c-a)(c-b)(c-d)\ldots.\\ &=1+F(c,\lambda',\lambda'',\lambda''' \text{ usw.})\\ &\text{usw.}\end{aligned}$$

Nehmen wir nun an, das Produkt aus allen Ausdrücken

$$\begin{gathered}1+F(a,l',l'',l''' \text{ usw.})\\ 1+F(b,l',l'',l''' \text{ usw.})\\ 1+F(c,l',l'',l''' \text{ usw.})\\ \text{usw.}\end{gathered}$$

das ein Polynom in den Unbestimmten a, b, c usw., l', l'', l''' usw. und hinsichtlich a, b, c usw. symmetrisch ist, werde durch

$$\psi(\lambda',\lambda'',\lambda''' \text{ usw.},\ l', l'', l''' \text{ usw.})$$

dargestellt. Dann ergibt die Multiplikation sämtlicher Gleichungen [1] die neue identische Gleichung [2]

$$\pi\varphi a\,.\,\varphi b\,.\,\varphi c\ldots. = \psi(\lambda',\lambda'',\lambda''' \text{ usw.},\ \lambda',\lambda'',\lambda''' \text{ usw.})$$

Da ferner das Produkt $\varphi a\,.\,\varphi b\,.\,\varphi c\ldots.$ die Unbestimmten a, b, c usw. symmetrisch enthält, lässt sich offenbar ein Polynom in den Unbestimmten

l', l'', l''' usw. finden, das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in $\varphi a \,.\, \varphi b \,.\, \varphi c \ldots$. übergeht. Dieses Polynom sei t. Dann gilt ebenfalls identisch [3]

$$pt = \psi(l', l'', l''' \text{ usw.}, \; l', l'', l''')$$

denn die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. führen diese Gleichung in die identische Gleichung [2] über.

Aus der Definition der Funktion F selbst folgt nun identisch

$$F(x, L', L'', L''' \text{ usw.}) = 0$$

Daher gilt auch identisch

$$\begin{gathered} 1 + F(a, L', L'', L''' \text{ usw.}) = 1 \\ 1 + F(b, L', L'', L''' \text{ usw.}) = 1 \\ 1 + F(c, L', L'', L''' \text{ usw.}) = 1 \\ \text{usw.} \end{gathered}$$

und somit ebenfalls identisch

$$\psi(\lambda', \lambda'', \lambda''' \text{ usw.}, \; L', L'', L''' \text{ usw.}) = 1$$

also auch identisch [4]

$$\psi(l', l'', l''' \text{ usw.}, \; L' . L'', L''' \text{ usw.}) = 1$$

Verbinden wir die Gleichungen [3] und [4] und setzen $l' = L', l'' = L'', l''' = L'''$ usw., so erhalten wir daher [5]

$$PT = 1$$

wobei T den Wert des Polynoms t bei diesen Substitutionen bezeichnet. Da dieser Wert notwendig eine endliche Größe ist, kann P gewiss nicht $= 0$ sein. Q. E. D.

10.

Aus dem Vorhergehenden ist nun klar, dass sich jedes Polynom Y in einer Unbestimmten x, dessen Determinante $= 0$ ist, in Faktoren zerlegen lässt, von denen keiner die Determinante 0 hat. Bestimmt man nämlich den größten gemeinsamen Teiler der Polynome Y und $\frac{\mathrm{d}Y}{\mathrm{d}x}$, so ist das erste damit in zwei Faktoren zerlegt. Hat einer dieser Faktoren[*)] wiederum die Determinante 0, so wird er auf dieselbe Weise in zwei Faktoren zerlegt. So fahren wir fort, bis Y schließlich in Faktoren zerlegt ist, von denen keiner die Determinante 0 hat.

Ferner sieht man leicht, dass sich unter diesen Faktoren, in die Y zerlegt wird, wenigstens einer befinden muss, der folgende Eigenschaft hat: Unter den Faktoren der Zahl, die seinen Grad angibt, kommt die Zahl zwei nicht öfter vor als unter den Faktoren der Zahl m, die den Grad des Polynoms Y angibt. Setzt man also $m = k \,.\, 2^{\mu}$, wobei k eine ungerade Zahl bezeichnet, so findet sich unter den Faktoren des Polynoms Y wenigstens einer vom Grad $k' \,.\, 2^{\nu}$, wobei auch k' ungerade ist und entweder $\nu = \mu$ oder $\nu < \mu$ gilt. Die Richtigkeit dieser Behauptung folgt von selbst daraus, dass m die Summe der Zahlen ist, welche die Grade der einzelnen Faktoren von Y angeben.

11.

Bevor wir weitergehen, erläutern wir einen Ausdruck, dessen Einführung bei allen Untersuchungen über symmetrische Funktionen sehr nützlich ist und der auch uns sehr gelegen kommt. Es sei M eine Funktion einiger der Unbestimmten a, b, c usw.; μ sei dabei die Anzahl derjenigen, die in den Ausdruck M eingehen, ohne Rücksicht auf andere Unbestimmte, die M etwa noch enthält. Vertauscht man diese μ Unbestimmten auf alle möglichen Arten sowohl untereinander als auch mit den übrigen $m - \mu$ aus a, b, c usw., so entstehen aus M andere, M ähnliche Ausdrücke. Insgesamt erhält man

$$m(m-1)(m-2)(m-3)\ldots\ldots(m-\mu+1)$$

Ausdrücke einschließlich M selbst. Ihre Gesamtheit nennen wir kurz die *Gesamtheit aller M*. Damit ist von selbst klar, was die Summe aller M, das Produkt aus allen M usw. bedeutet. So heißt zum Beispiel π das Produkt aus allen $a - b$, υ das Produkt aus allen $x - a$ und υ' die Summe aller $\frac{\upsilon}{x-a}$ usw.

Ist M hinsichtlich einiger der μ darin enthaltenen Unbestimmten symmetrisch, so ändern deren Vertauschungen untereinander die Funktion M nicht. In der Gesamtheit aller M kommt daher jedes Glied mehrfach vor, und zwar $1 \,.\, 2 \,.\, 3 \ldots\ldots \nu$ Mal, wenn ν die Anzahl der Unbestimmten ist, hinsichtlich deren M symmetrisch ist. Ist aber M nicht nur hinsichtlich ν Unbestimmter

[*)] Tatsächlich kann nur derjenige Faktor, der jener gemeinsame Teiler ist, die Determinante 0 haben. Doch würde der Beweis dieses Satzes hier zu einigen Umwegen führen; er ist hier auch nicht nötig, da man den anderen Faktor, selbst wenn auch dessen Determinante verschwinden könnte, auf dieselbe Weise behandeln und in Faktoren zerlegen dürfte.

symmetrisch, sondern außerdem hinsichtlich ν' anderer und ferner hinsichtlich ν'' anderer usw., so bleibt M unverändert, ob nun zwei der ersten ν Unbestimmten untereinander vertauscht werden oder zwei der zweiten ν' oder zwei der dritten ν'' usw. Es entsprechen somit stets

$$1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu\,.\quad 1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu'\,.\quad 1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu''\text{ usw.}$$

Vertauschungen identischen Gliedern. Behalten wir von diesen identischen Gliedern jeweils nur eines, so erhalten wir insgesamt

$$\frac{m(m-1)(m-2)(m-3)\,.\,.\,.\,.\,(m-\mu+1)}{1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu\,.\,1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu'\,.\,1\,.\,2\,.\,3\,.\,.\,.\,.\,.\,\nu''\text{ usw.}}$$

Glieder. Ihre Gesamtheit nennen wir die *Gesamtheit aller M mit ausgeschlossenen Wiederholungen*, um sie von der *Gesamtheit aller M mit zugelassenen Wiederholungen* zu unterscheiden. Wird nichts ausdrücklich bemerkt, so verstehen wir stets, dass die Wiederholungen zugelassen sind.

Ferner sieht man leicht, dass die Summe aller M oder das Produkt aus allen M oder allgemein irgendeine symmetrische Funktion aller M stets eine symmetrische Funktion der Unbestimmten a, b, c usw. ist, ob Wiederholungen zugelassen oder ausgeschlossen werden.

12.

Nun betrachten wir, mit u, x als Unbestimmten, das Produkt aus allen $u-(a+b)x+ab$ mit ausgeschlossenen Wiederholungen und bezeichnen es mit ζ. Somit ist ζ das Produkt aus den folgenden $\frac{1}{2}m(m-1)$ Faktoren:

$$\begin{gathered}u-(a+b)x+ab\\ u-(a+c)x+ac\\ u-(a+d)x+ad\\ \text{usw.}\\ u-(b+c)x+bc\\ u-(b+d)x+bd\\ \text{usw.}\\ u-(c+d)x+cd\\ \text{usw. usw.}\end{gathered}$$

Da diese Funktion die Unbestimmten a, b, c usw. symmetrisch enthält, lässt sich ein Polynom in den Unbestimmten u, x, l', l'', l''' usw. angeben, das wir mit z bezeichnen und das in ζ übergeht, wenn anstelle der Unbestimmten l', l'', l''' usw. $\lambda', \lambda'', \lambda'''$ usw. eingesetzt werden. Schließlich bezeichnen wir mit Z die Funktion allein der Unbestimmten u, x, in die z übergeht, wenn den

Unbestimmten l', l'', l''' usw. die bestimmten Werte L', L'', L''' usw. gegeben werden.

Diese drei Funktionen ζ, z, Z lassen sich als Polynome vom Grad $\frac{1}{2}m(m-1)$ in der Unbestimmten u mit unbestimmten Koeffizienten auffassen. Diese Koeffizienten sind

für ζ, Funktionen der Unbestimmten x, a, b, c usw.
für z, Funktionen der Unbestimmten x, l', l'', l''' usw.
für Z, Funktionen allein der Unbestimmten x.

Die einzelnen Koeffizienten von z gehen durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in die Koeffizienten von ζ und durch die Substitutionen $l' = L', l'' = L'', l''' = L'''$ usw. in die Koeffizienten von Z über. Was wir eben über die Koeffizienten gesagt haben, gilt ebenso für die Determinanten der Funktionen ζ, z, Z. Diese wollen wir nun näher untersuchen, und zwar mit dem Ziel, den folgenden Satz zu beweisen.

Satz. *Gilt nicht $P = 0$, so kann die Determinante der Funktion Z gewiss nicht identisch $= 0$ sein.*

13.

Der Beweis dieses Satzes wäre allerdings sehr leicht, wenn man annehmen dürfte, Y lasse sich in lineare Faktoren zerlegen:

$$(x-A)(x-B)(x-C)(x-D)\ldots..$$

Dann wäre nämlich auch gewiss, dass Z das Produkt aus allen $u-(A+B)x+AB$ und die Determinante der Funktion Z das Produkt aus den Differenzen zwischen je zweien der Größen

$$\begin{gathered}(A+B)x-AB\\(A+C)x-AC\\(A+D)x-AD\\\text{usw.}\\(B+C)x-BC\\(B+D)x-BD\\\text{usw.}\\(C+D)x-CD\\\text{usw. usw.}\end{gathered}$$

ist. Dieses Produkt kann aber nicht identisch verschwinden, wenn nicht einer seiner Faktoren selbst identisch $= 0$ wird. Daraus würde folgen, dass zwei der Größen A, B, C usw. gleich sind und somit die Determinante P des Polynoms $Y = 0$ wird, gegen die Voraussetzung.

Doch lassen wir diese Argumentation beiseite, die offenbar wie in Artikel 6 von einer Vorwegnahme des zu Beweisenden ausgeht, und gehen sogleich zu einem sicheren Beweis des Satzes von Artikel 12 über.

14.

Die Determinante der Funktion ζ ist das Produkt aus allen Differenzen zwischen je zweien der Ausdrücke $(a+b)x-ab$. Die Anzahl dieser Differenzen ist

$$\frac{1}{2}m(m-1)(\tfrac{1}{2}m(m-1)-1) = \frac{1}{4}(m+1)m(m-1)(m-2)$$

Diese Zahl gibt also den Grad der Determinante der Funktion ζ hinsichtlich der Unbestimmten x an. Die Determinante der Funktion z hat denselben Grad. Dagegen kann die Determinante der Funktion Z durchaus einen niedrigeren Grad haben, wenn einige Koeffizienten, von der höchsten Potenz von x an, verschwinden. Wir haben nun zu beweisen, dass in der Determinante der Funktion Z gewiss nicht *alle* Koeffizienten verschwinden können.

Betrachten wir die Differenzen, deren Produkt die Determinante der Funktion ζ ist, näher, so finden wir: Ein Teil von ihnen, nämlich die Differenzen zwischen je zweien der Ausdrücke $(a+b)x-ab$ mit einem gemeinsamen Element, liefert

$$\text{das Produkt aus allen} \quad (a-b)(x-c)$$

Aus den übrigen, nämlich den Differenzen zwischen je zweien der Ausdrücke $(a+b)x-ab$ mit verschiedenen Elementen, entsteht dagegen

$$\text{das Produkt aus allen} \quad (a+b-c-d)x-ab+cd,$$
$$\text{mit ausgeschlossenen Wiederholungen.}$$

Das erste Produkt enthält offenbar jeden Faktor $a-b$ genau $m-2$ Mal und jeden Faktor $x-c$ genau $(m-1)(m-2)$ Mal. Daraus schließen wir leicht, dass dieses Produkt

$$= \pi^{m-2}\upsilon^{(m-1)(m-2)}$$

ist. Bezeichnen wir also das zweite Produkt mit ρ, so ist die Determinante der Funktion ζ

$$= \pi^{m-2}\upsilon^{(m-1)(m-2)}\rho$$

Bezeichnen wir ferner mit r diejenige Funktion der Unbestimmten x, l', l'', l''' usw., die durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in ρ übergeht, und mit R die Funktion allein von x, in die r durch die Substitutionen $l' = L', l'' = L''$, $l''' = L'''$ usw. übergeht, so ist offenbar die Determinante der Funktion z

$$= p^{m-2}y^{(m-1)(m-2)}r$$

die Determinante der Funktion Z dagegen

$$= P^{m-2}Y^{(m-1)(m-2)}R$$

Da nach Voraussetzung P nicht $= 0$ ist, kommt es nun darauf an, zu beweisen, dass R gewiss nicht identisch verschwinden kann.

15.

Dazu führen wir noch eine weitere Unbestimmte w ein und betrachten das Produkt aus allen

$$(a+b-c-d)w+(a-c)(a-d)$$

mit ausgeschlossenen Wiederholungen. Da es a, b, c usw. symmetrisch enthält, lässt es sich als Polynom in den Unbestimmten $w, \lambda', \lambda'', \lambda'''$ usw. darstellen. Wir bezeichnen diese Funktion mit $f(w, \lambda', \lambda'', \lambda'''$ usw.). Die Anzahl jener Faktoren $(a+b-c-d)w+(a-c)(a-d)$ ist

$$= \frac{1}{2}m(m-1)(m-2)(m-3)$$

woraus wir leicht schließen, dass

$$f(0, \lambda', \lambda'', \lambda''' \text{ usw.}) = \pi^{(m-2)(m-3)}$$

und daher auch

$$f(0, l', l'', l''' \text{ usw.}) = p^{(m-2)(m-3)}$$

sowie

$$f(0, L', L'', L''' \text{ usw.}) = P^{(m-2)(m-3)}$$

gilt. Das Polynom $f(w, L', L'', L'''$ usw.) hat im Allgemeinen den Grad

$$\frac{1}{2}m(m-1)(m-2)(m-3)$$

in besonderen Fällen kann es aber durchaus einen niedrigeren Grad haben, wenn etwa einige Koeffizienten, von der höchsten Potenz von w an, verschwinden. Unmöglich ist dagegen, dass die ganze Funktion identisch $= 0$ ist, denn die eben gefundene Gleichung zeigt, dass wenigstens ihr letztes Glied nicht verschwindet. Wir nehmen an, das höchste Glied des Polynoms $f(w, L', L''$, L''' usw.) mit nicht verschwindendem Koeffizienten sei Nw^ν. Setzen wir nun $w = x - a$, so ist $f(x-a, L', L'', L'''$ usw.) offenbar ein Polynom in den Unbestimmten x, a oder, was dasselbe ist, ein Polynom in x mit Koeffizienten, die von der Unbestimmten a abhängen. Sein höchstes Glied ist dabei jedoch Nx^ν und hat somit einen bestimmten, von a unabhängigen Koeffizienten, der nicht $= 0$ ist. Ebenso sind $f(x-b, L', L'', L'''$ usw.), $f(x-c, L', L'', L'''$ usw.)

Polynome in der Unbestimmten x, deren höchstes Glied jeweils Nx^ν ist, während die Koeffizienten der folgenden Glieder jeweils von b, c usw. abhängen. Das Produkt aus den m Faktoren

$$\begin{gathered} f(x-a, L', L'', L''' \text{ usw.}) \\ f(x-b, L', L'', L''' \text{ usw.}) \\ f(x-c, L', L'', L''' \text{ usw.}) \\ \text{usw.} \end{gathered}$$

ist daher ein Polynom in x, dessen höchstes Glied $N^m x^{m\nu}$ ist, während die Koeffizienten der folgenden Glieder von den Unbestimmten a, b, c usw. abhängen.

Wir betrachten nun weiter das Produkt aus den folgenden m Faktoren:

$$\begin{gathered} f(x-a, l', l'', l''' \text{ usw.}) \\ f(x-b, l', l'', l''' \text{ usw.}) \\ f(x-c, l', l'', l''' \text{ usw.}) \\ \text{usw.} \end{gathered}$$

Da es eine Funktion der Unbestimmten x, a, b, c usw., l', l'', l''' usw. ist, und zwar hinsichtlich a, b, c usw. symmetrisch, lässt es sich als Funktion der Unbestimmten $x, \lambda', \lambda'', \lambda'''$ usw., l', l'', l''' usw. darstellen, die wir mit

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.},\ l', l'', l''' \text{ usw.})$$

bezeichnen. Somit ist

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.},\ \lambda', \lambda'', \lambda''' \text{ usw.})$$

das Produkt aus den Faktoren

$$\begin{gathered} f(x-a, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ f(x-b, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ f(x-c, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ \text{usw.} \end{gathered}$$

und daher identisch durch ρ teilbar, da man leicht sieht, dass jeder Faktor von ρ in einem jener Faktoren enthalten ist. Wir setzen also

$$\begin{aligned} &\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.},\ \lambda', \lambda'', \lambda''' \text{ usw.}) \\ &= \rho\psi(x, \lambda', \lambda'', \lambda''' \text{ usw.}) \end{aligned}$$

wobei das Zeichen ψ ein Polynom bezeichnet. Daraus folgt aber leicht, dass auch identisch

$$\begin{aligned} &\varphi(x, L', L'', L''' \text{ usw.},\ L', L'', L''' \text{ usw.}) \\ &= R\psi(x, L', L'', L''' \text{ usw.}) \end{aligned}$$

gilt. Oben haben wir jedoch bewiesen, dass das Produkt aus den Faktoren

$$f(x-a, L', L'', L''' \text{ usw.})$$
$$f(x-b, L', L'', L''' \text{ usw.})$$
$$f(x-c, L', L'', L''' \text{ usw.})$$
$$\text{usw.}$$

das $= \varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.},\ L', L'', L''' \text{ usw.})$ ist, das höchste Glied $N^m x^{m\nu}$ hat. Dasselbe höchste Glied hat daher auch die Funktion $\varphi(x, L', L'', L''' \text{ usw.}, L', L'', L''' \text{ usw.})$, und sie ist somit gewiss nicht identisch $= 0$. Folglich kann auch R nicht identisch $= 0$ sein und daher ebenso wenig die Determinante der Funktion Z. Q. E. D.

16.

Satz. *Es bezeichne $\varphi(u,x)$*[*)] *ein Produkt aus beliebig vielen Faktoren, in welche die Unbestimmten u, x nur linear eingehen, die also die Form*

$$\alpha + \beta u + \gamma x$$
$$\alpha' + \beta' u + \gamma' x$$
$$\alpha'' + \beta'' u + \gamma'' x$$
$$\text{usw.}$$

haben; ferner sei w eine weitere Unbestimmte. Dann ist die Funktion

$$\varphi(u + w\,.\,\tfrac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x},\ x - w\,.\,\tfrac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}) = \Omega$$

identisch durch $\varphi(u,x)$ teilbar.

Beweis. Setzen wir

$$\begin{aligned}\varphi(u,x) &= (\alpha + \beta u + \gamma x)Q \\ &= (\alpha' + \beta' u + \gamma' x)Q' \\ &= (\alpha'' + \beta'' u + \gamma'' x)Q'' \\ &\quad \text{usw.}\end{aligned}$$

so sind Q, Q', Q'' usw. Polynome in den Unbestimmten $u, x, \alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ usw., und es gilt

$$\begin{aligned}\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x} &= \gamma Q + (\alpha + \beta u + \gamma x)\,.\,\frac{\mathrm{d}Q}{\mathrm{d}x} \\ &= \gamma' Q' + (\alpha' + \beta' u + \gamma' x)\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}x} \\ &= \gamma'' Q'' + (\alpha'' + \beta'' u + \gamma'' x)\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}x} \\ &\quad \text{usw.}\end{aligned}$$

[*)] Jeder wird auch ohne unseren Hinweis sehen, dass die im vorigen Artikel eingeführten Zeichen auf diesen Artikel allein beschränkt sind und daher die jetzige Bedeutung der Zeichen φ, w nicht mit der früheren verwechselt werden darf.

$$\begin{aligned}\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u} &= \beta Q + (\alpha+\beta u+\gamma x)\,.\,\frac{\mathrm{d}Q}{\mathrm{d}u}\\ &= \beta' Q' + (\alpha'+\beta' u+\gamma' x)\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}u}\\ &= \beta'' Q'' + (\alpha''+\beta'' u+\gamma'' x)\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}u}\end{aligned}$$

usw.

Setzt man diese Werte in die Faktoren ein, deren Produkt Ω ist, nämlich in

$$\begin{gathered}\alpha+\beta u+\gamma x+\beta w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x}-\gamma w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}\\ \alpha'+\beta' u+\gamma' x+\beta' w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x}-\gamma' w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}\\ \alpha''+\beta'' u+\gamma'' x+\beta'' w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x}-\gamma'' w\,.\,\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}\\ \text{usw., jeweils}\end{gathered}$$

so erhalten diese die folgenden Werte:

$$\begin{gathered}(\alpha+\beta u+\gamma x)(1+\beta w\,.\,\tfrac{\mathrm{d}Q}{\mathrm{d}x}-\gamma w\,.\,\tfrac{\mathrm{d}Q}{\mathrm{d}u})\\ (\alpha'+\beta' u+\gamma' x)(1+\beta' w\,.\,\tfrac{\mathrm{d}Q'}{\mathrm{d}x}-\gamma' w\,.\,\tfrac{\mathrm{d}Q'}{\mathrm{d}u})\\ (\alpha''+\beta'' u+\gamma'' x)(1+\beta'' w\,.\,\tfrac{\mathrm{d}Q''}{\mathrm{d}x}-\gamma'' w\,.\,\tfrac{\mathrm{d}Q''}{\mathrm{d}u})\\ \text{usw.}\end{gathered}$$

Daher ist Ω das Produkt aus $\varphi(u,x)$ und den Faktoren

$$\begin{gathered}1+\beta w\,.\,\frac{\mathrm{d}Q}{\mathrm{d}x}-\gamma w\,.\,\frac{\mathrm{d}Q}{\mathrm{d}u}\\ 1+\beta' w\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}x}-\gamma' w\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}u}\\ 1+\beta'' w\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}x}-\gamma'' w\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}u}\end{gathered}$$

usw., also aus $\varphi(u,x)$ und einem Polynom in den Unbestimmten $u, x, w, \alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ usw. Q. E. D.

17.

Der Satz des vorigen Artikels ist offenbar auf die Funktion ζ anwendbar, die wir von nun an durch

$$f(u, x, \lambda', \lambda'', \lambda''' \text{ usw.})$$

darstellen. Dann ist

$$f(u + w \,.\, \tfrac{\mathrm{d}\zeta}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}\zeta}{\mathrm{d}u},\ \lambda', \lambda'', \lambda''' \text{ usw.})$$

identisch durch ζ teilbar. Den Quotienten, ein Polynom in den Unbestimmten u, x, w, a, b, c usw., das hinsichtlich a, b, c usw. symmetrisch ist, stellen wir durch

$$\psi(u, x, w, \lambda', \lambda'', \lambda''' \text{ usw.})$$

dar. Daraus schließen wir, dass auch identisch

$$\begin{aligned} &f(u + w \,.\, \tfrac{\mathrm{d}z}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}z}{\mathrm{d}u},\ l', l'', l''' \text{ usw.}) \\ &= z\psi(u, x, w, l', l'', l''' \text{ usw.}) \end{aligned}$$

sowie

$$\begin{aligned} &f(u + w \,.\, \tfrac{\mathrm{d}Z}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}Z}{\mathrm{d}u},\ L', L'', L''' \text{ usw.}) \\ &= Z\psi(u, x, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

gilt. Stellen wir also die Funktion Z einfach durch $F(u, x)$ dar, sodass

$$f(u, x, L', L'', L''' \text{ usw.}) = F(u, x)$$

gilt, so haben wir identisch

$$\begin{aligned} &F(u + w \,.\, \tfrac{\mathrm{d}Z}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}Z}{\mathrm{d}u}) \\ &= Z\psi(u, x, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

18.

Nehmen wir nun an, aus bestimmten Werten von u, x, nämlich aus $u = U, x = X$, ergebe sich

$$\frac{\mathrm{d}Z}{\mathrm{d}x} = X', \quad \frac{\mathrm{d}Z}{\mathrm{d}u} = U'$$

Dann gilt identisch

$$\begin{aligned} &F(U + wX',\ X - wU') \\ &= F(U, X) \,.\, \psi(U, X, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

Sooft U' nicht verschwindet, dürfen wir

$$w = \frac{X - x}{U'}$$

setzen. Daraus ergibt sich

$$F(U + \tfrac{XX'}{U'} - \tfrac{X'x}{U'},\ x)$$
$$= F(U, X)\,.\,\psi(U, X, \tfrac{X-x}{U'}, L', L'', L''' \text{ usw.})$$

Dies lässt sich auch so aussprechen:

Setzt man in der Funktion Z den Wert $u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$, so geht sie in

$$F(U, X)\,.\,\psi(U, X, \tfrac{X-x}{U'}, L', L'', L''' \text{ usw.})$$

über.

19.

Da im Fall, dass nicht $P = 0$ gilt, die Determinante der Funktion Z eine für sich nicht verschwindende Funktion der Unbestimmten x ist, ist die Anzahl der bestimmten Werte von x, bei denen diese Determinante den Wert 0 annehmen kann, offenbar endlich. Es lassen sich daher unendlich viele bestimmte Werte von x angeben, die jener Determinante einen von 0 verschiedenen Wert geben. Es sei X ein solcher Wert von x, den man außerdem als *reell* annehmen darf. Die Determinante der Funktion $F(u, X)$ ist dann nicht $= 0$. Nach Satz II von Artikel 6 können also die Funktionen

$$F(u, X) \quad \text{und} \quad \frac{\mathrm{d}F(u, X)}{\mathrm{d}u}$$

keinen gemeinsamen Teiler haben. Wir nehmen ferner an, es gebe einen bestimmten Wert von u, etwa U, der entweder reell oder imaginär, also von der Form $g + h\sqrt{-1}$ ist und $F(u, X) = 0$ bewirkt, sodass $F(U, X) = 0$ gilt. Dann ist $u - U$ ein Faktor des Polynoms $F(u, X)$, und die Funktion $\frac{\mathrm{d}F(u,X)}{\mathrm{d}u}$ ist daher gewiss nicht durch $u - U$ teilbar. Nehmen wir also an, diese Funktion, $\frac{\mathrm{d}F(u,X)}{\mathrm{d}u}$, erhalte den Wert U', wenn $u = U$ gesetzt wird. Dann kann gewiss nicht $U' = 0$ sein. Offenbar ist aber U' der Wert der partiellen Ableitung $\frac{\mathrm{d}Z}{\mathrm{d}u}$ für $u = U, x = X$. Bezeichnen wir ferner den Wert der partiellen Ableitung $\frac{\mathrm{d}Z}{\mathrm{d}x}$ bei denselben Werten von u, x mit X', so ist nach dem im vorigen Artikel Bewiesenen klar, dass die Funktion Z durch die Substitution

$$u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$$

identisch verschwindet und daher identisch durch den Faktor

$$u + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

teilbar ist. Setzen wir nun $u = xx$, so ist offenbar $F(xx, x)$ durch

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

teilbar und nimmt daher den Wert 0 an, wenn für x eine Wurzel der Gleichung

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'}) = 0$$

genommen wird, also wenn man

$$x = \frac{-X' \pm \sqrt{(4UU'U' + 4XX'U' + X'X')}}{2U'}$$

setzt. Diese Werte sind bekanntlich entweder reell oder von der Form $g + h\sqrt{-1}$.

Nun lässt sich leicht beweisen, dass bei denselben Werten von x auch die Funktion Y verschwinden muss. Denn $f(xx, x, \lambda', \lambda'', \lambda'''$ usw.) ist offenbar das Produkt aus allen $(x-a)(x-b)$ mit ausgeschlossenen Wiederholungen und somit $= v^{m-1}$. Daraus folgt von selbst

$$f(xx, x, l', l'', l'''\text{ usw.}) = y^{m-1}$$
$$f(xx, x, L', L'', L'''\text{ usw.}) = Y^{m-1}$$

oder $F(xx, x) = Y^{m-1}$, dessen bestimmter Wert also nur verschwinden kann, wenn zugleich der Wert von Y verschwindet.

20.

Mithilfe der vorangehenden Untersuchungen ist die *Lösung* der Gleichung $Y = 0$, also das Auffinden eines bestimmten Wertes von x, der entweder reell oder von der Form $g + h\sqrt{-1}$ ist und ihr genügt, auf die Lösung der Gleichung $F(u, X) = 0$ zurückgeführt, sofern die Determinante der Funktion Y nicht $= 0$ ist. Zu bemerken ist: Sind alle Koeffizienten in Y, also die Zahlen L', L'', L''' usw., reelle Größen, so sind auch alle Koeffizienten in $F(u, X)$ reell, sofern für X eine reelle Größe genommen wird, was zulässig ist. Der Grad der zweiten Gleichung $F(u, X) = 0$ wird durch die Zahl $\frac{1}{2}m(m-1)$ ausgedrückt. Ist also m eine gerade Zahl von der Form $2^\mu k$, wobei k eine unbestimmte ungerade Zahl bezeichnet, so hat die zweite Gleichung einen Grad von der Form $2^{\mu-1}k$.

Ist die Determinante der Funktion $Y = 0$, so lässt sich nach Artikel 10 ein anderes, sie teilendes Polynom $\mathfrak{Y}$ angeben, dessen Determinante nicht $= 0$ ist und dessen Grad durch eine Zahl von der Form $2^\nu k$ ausgedrückt wird, wobei entweder $\nu < \mu$ oder $\nu = \mu$ gilt. Jede Lösung der Gleichung $\mathfrak{Y} = 0$ genügt auch der Gleichung $Y = 0$. Die Lösung der Gleichung $\mathfrak{Y} = 0$ wird wiederum auf die Lösung einer anderen Gleichung zurückgeführt, deren Grad durch eine Zahl von der Form $2^{\nu-1}k$ ausgedrückt wird.

Daraus schließen wir also, dass sich allgemein die Lösung jeder Gleichung, deren Grad eine gerade Zahl von der Form $2^\mu k$ ist, auf die Lösung einer anderen Gleichung zurückführen lässt, deren Grad die Form $2^{\mu'}k$ hat, wobei

$\mu' < \mu$ gilt. Ist diese Zahl noch immer gerade, also μ' nicht $= 0$, so wird dieselbe Methode erneut angewandt. So fahren wir fort, bis wir zu einer Gleichung gelangen, deren Grad ungerade ist. Alle ihre Koeffizienten sind reell, sofern sämtliche Koeffizienten der ursprünglichen Gleichung reell waren. Eine solche Gleichung ungeraden Grades ist bekanntlich gewiss lösbar, und zwar durch eine reelle Wurzel. Daher sind auch alle vorhergehenden Gleichungen lösbar, entweder durch reelle Wurzeln oder durch Wurzeln von der Form $g + h\sqrt{-1}$.

Damit ist erwiesen, dass jedes Polynom Y von der Form $x^m - L'x^{m-1} + L''x^{m-2} -$ usw., wobei L', L'' usw. bestimmte reelle Größen sind, einen Faktor $x - A$ enthält, wobei A eine entweder reelle Größe oder eine Größe von der Form $g + h\sqrt{-1}$ ist. Im letzteren Fall sieht man leicht, dass Y auch durch die Substitution $x = g - h\sqrt{-1}$ den Wert 0 erhält, also durch $x - (g - h\sqrt{-1})$ und daher auch durch das Produkt $xx - 2gx + gg + hh$ teilbar ist. Jedes Polynom Y enthält also gewiss einen reellen Faktor ersten oder zweiten Grades. Da dasselbe wiederum für den Quotienten gilt, ist klar, dass sich Y in reelle Faktoren ersten oder zweiten Grades zerlegen lässt. Dies zu beweisen war das Ziel dieser Abhandlung.
