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 $\alpha, \beta$ 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 $\pi$-mal vorkomme; offensichtlich muss eine der Zahlen $a, b, c$ usw. denselben Teiler $\pi$-mal enthalten. Daher enthält auch $k$, das von dieser Zahl geteilt wird, $\pi$-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 $\alpha, \beta, \gamma$ usw. durch $n$ teilbar.*

Die Zahl $k$ enthält nämlich keine anderen Primfaktoren als $a, b, c$ usw. Enthält sie den Faktor $a$ genau $\alpha'$-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 $l$ $\lambda$-mal, den Faktor $m$ $\mu$-mal usw. Nach dem *vorigen Artikel* sind daher $\lambda, \mu, \pi$ 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 $\alpha, \beta, \gamma$ 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.

$2^{\text{o}}$. Die Reihenfolge der Zahlen $\alpha, \beta, \gamma$ 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 $\delta$. Zunächst erfüllt offenbar jeder Wert von $x$, der die Kongruenz nach dem Modul $m$ erfüllt, sie auch nach dem Modul $\delta$ (Artikel 5). Es ist aber stets $ax \equiv 0 \pmod{\delta}$, da $\delta$ 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 $\delta$ 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 $\delta f$ 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 $\delta$ 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 $\delta$ 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 $\delta$, 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 $\alpha$, die nach $A$ der Eins, nach dem Produkt der übrigen Moduln aber der Null kongruent ist. Oder es sei $\alpha$ 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 $\alpha, \beta, \gamma$ 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 $\beta$ den Wert 4200 und für $\gamma$ 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 $\xi, \xi', \xi''$ 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., $\zeta, \zeta', \zeta''$ 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 $\xi, \xi', \xi''$ 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 $\alpha, \beta, \gamma$ 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 $\alpha$ verschiedene Werte von $x$ (das heißt, nach $m$ inkongruente, nämlich $p, p+\frac{m}{\alpha} \ldots p+\frac{(\alpha-1)m}{\alpha}$), $\beta$ 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 $\alpha$ 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 $\xi, \xi', \xi''$, $v, v', v''$, $\zeta, \zeta', \zeta''$ 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 $\phi$. Gesucht ist also $\phi A$.

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 $\phi$ so, dass $\phi A$ 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 $\mu, \nu$ 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 $\mu$ teilerfremd ist und $\mu N$ 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 $\delta$. 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 $\lambda, C$ den Wert $= \lambda'$. Dieser ist zugleich der größte gemeinsame Teiler von $A, B, C$[*]. Man bestimme Zahlen $k, \gamma$ 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 $\lambda', D$, 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 $\lambda'$ alle Zahlen $A, B, C$. Wäre es nicht der *größte* gemeinsame Teiler, so wäre dieser größer als $\lambda'$. Da dieser größte Teiler aber $A, B, C$ teilt, müsste er auch $k\alpha A + k\beta B + \gamma C$, also $\lambda'$ 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 $\Gamma$ 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 $\Gamma x^\gamma$ 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 $\tau$ Faktoren $p$ enthält, oder der eine nicht mehr als $\tau$ 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 $\delta$ 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 $\alpha, \beta, \gamma$ usw. positiv und kleiner als $p$ sind und $\alpha$ 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 $\mu, \nu$ 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 $\beta$ aus $1, 2, 3...p-1$, die in $(A)$ fehlt, multipliziere $\beta$ mit allen $\alpha, \alpha', \alpha''$ usw. und nenne die daraus entstehenden kleinsten Reste $\beta, \beta', \beta''$ 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 $\beta$ 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*, $\beta$ 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 $\beta, \beta', \beta''$ 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 $\gamma$ 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 $\gamma$ 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 $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $\psi d$ 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 $\delta$ 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 $\psi d$ 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 $\psi d$ entweder gleich oder kleiner als $\phi d$, 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 $\psi d$ *stets gleich* $\phi d$ *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 $a^\alpha$ gehört; ebenso Zahlen $B, C$ usw., die zu den Exponenten $b^\beta, c^\gamma$ 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 $a^\alpha$.

Denn die Potenz mit dem Exponenten $a^\alpha$ 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 $a^\alpha$ sein (Artikel 48). Da $a^\alpha$ nur durch sich selbst und niedrigere Potenzen von $a$ teilbar ist, muss $a^\alpha$ der Exponent sein, zu dem $h$ gehört. *Q. E. D.* Ebenso zeigt man, dass es Zahlen gibt, die zu den Exponenten $b^\beta, c^\gamma$ 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 $b^\beta, c^\gamma$ 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 $\delta$, so hat $\mathrm{Ind.}\, x$ genau $\delta$ nach $p-1$ inkongruente Werte und damit $\sqrt[n]{A}$ ebenso viele nach $p$ inkongruente Werte, sofern $\mathrm{Ind.}\, A$ durch $\delta$ 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 $\delta$, 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 $\delta$ nach dem Modul $p-1$ inkongruente Werte haben. Somit hat auch $x$ in diesem Fall $\delta$ verschiedene Werte (inkongruent nach dem Modul $p$). Daraus ergibt sich, dass auch der Ausdruck $\sqrt[\delta]{1}$ genau $\delta$ 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 $\delta$ 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 $\delta$ verschiedene Werte oder gar keinen hat, wenn $\delta$ 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 $\delta$ 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 $\delta$ 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 $\pm 12$) 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 $\mu, \nu$, seien ungleich, so ist einer größer, etwa $\mu > \nu$. Damit teilt $\mu$ die Zahl $n$ nicht. Bezeichnet man aber den Index von $a$ bei der Basis $b$ mit $\alpha$, so gilt nach dem vorigen Artikel $n \equiv \alpha m \,(\mathrm{mod.}\, p-1)$. Also teilt $\mu$ 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 $\varepsilon$ ein Wert von $\frac{dn}{dm} \pmod{p-1}$ und zugleich zu $p-1$ teilerfremd, so ist $a^\varepsilon$ 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 $\varepsilon$ 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, $a^{\varepsilon}$ 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 $\beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $a^\alpha$, 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 $a^\alpha$, $B$ zum Exponenten $b^\beta$ 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 $p^\nu$ Wurzeln hat, die $A$, ebenso viele, die $B$ usw. nach dem Modul $p$ kongruent sind. Damit ist die Anzahl aller Wurzeln $kp^\nu$ oder $e$, wie behauptet. Den Beweis führen wir so: *Zuerst* zeigen wir, dass mit einer Wurzel $\alpha$, 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 $p^\nu$ 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 $p^\nu$, 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 $\nu$ 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 $\nu$, für den er falsch ist, sei $= \varphi$. Dann sieht man leicht: Ist $t$ durch $p^{\varphi-1}$, aber nicht durch $p^{\varphi}$ 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 $\nu$.

**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 $p^\nu$ 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 $\alpha'$, die $A$ und damit auch $\alpha$ 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 $\alpha^t$ kongruent, nicht aber nach dem Modul $p^n$, der eine höhere Potenz ist. Also kann $\alpha'$ 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 $\alpha$ 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 $\nu$ 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 $p^\nu$ 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 $p^\nu$ 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 $\alpha$, $B^{b-1}(B-1)$ mit $\beta$ 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 $\mu$ das kleinste gemeinsame Vielfache der Zahlen $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ usw. kleiner als ihr Produkt. Denn die Zahlen $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $p^\mu$ kongruent ist, so erhält man daraus ein Quadrat, das $A$ nach dem Modul $p^\nu$ 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 $\alpha$ 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 $\alpha$ 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 $p^\mu$ 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 $p^\mu$ 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 $\pm 5$ 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* $\pm 7$.

**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 $\chi$.

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

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 $(\alpha)$ 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 $(\beta)$ $\pm apNa'$. 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 $(\gamma)$ $\pm aNp$. *Q. E. D. Im zweiten Fall* folgt aus $(\beta)$ $\pm apRa'$, daraus $\pm pNa'$, $\pm a'Np$ und schließlich zusammen mit $hRp$ nach $(\gamma)$ $\pm aNp$. *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 $(\alpha)$, das mit $(\alpha)$ in (2) übereinstimmt, folgt wie dort, dass entweder gleichzeitig $hRp$, $hRa'$ oder $hNp$, $hNa'$

gilt. Im ersten Fall würde aber nach ($\beta$) $aRa'$ gelten, entgegen der Voraussetzung. Also gilt $hNp$, nach ($\gamma$) 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 $\pm 2$ 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 $\pm 2$ nicht ein Rest aller Primzahlen der Form $8n+1$, so sei die kleinste Primzahl dieser Form, von der $\pm 2$ 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 $\pm 2$ 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 $Q, a^\alpha$; $Q, b^\beta$ usw. ab (Artikel 105).

II. Um die Beziehung von $Q, a^\alpha$ zu bestimmen (für die übrigen $Q, b^\beta$ 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 $QRa^\alpha$; ist dagegen $e < \alpha$ und der Exponent ungerade, so gilt $QNa^\alpha$; ist schließlich $e < \alpha$ und der Exponent gerade, so hat $Q$ zu $a^\alpha$ 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 $QRa^\alpha$, 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 $QRa^\alpha$.

($B$) Wenn $a$ eine andere Primzahl ist. Dann hat $Q$ zu $a^\alpha$ 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 $\alpha$ entweder $= -1$ oder $= \pm 2$ ist. Dann ist $A$ ein Rest aller Zahlen, von denen entweder beide $\alpha$ und $Q$ Reste sind oder keine von beiden, dagegen ein Nichtrest aller Zahlen, von denen genau eine der Zahlen $\alpha, Q$ 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 $\mu, \nu$ 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 $\mu, \nu$ 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 $\mu'$, die andere Gleichung $\mu' m + \nu' n = 1$ mit $\mu$ und subtrahieren, so ergibt sich $\mu' - \mu = n(\mu'\nu - \mu\nu')$. Multiplizieren

wir ebenso die erste mit $\nu'$ und die zweite mit $\nu$, 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 $\mu, \nu$ 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 $\mu, \nu$, die $v$ liefern, andere Zahlen $\mu', \nu'$ 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 $\mu', \nu'$ hervorgehende Wert der Formel übertrifft den aus $\mu, \nu$ 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 $\mu, \nu$ und $\mu', \nu'$ 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 $\mu, \nu$ und $\mu', \nu'$ 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 $\alpha$, 19 mit $2\beta$ 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 $\mu, \nu$ 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 $\mu, \nu$ 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 $\Delta$. Umgekehrt teilt $\Delta$ 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 $\mu, \nu$ 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 $\mu', \nu', m', n'$ 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 $\mu, \nu$ 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 $\gamma$ 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 $\alpha$ 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 $\pm 3$, $\pm 4$. 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 $\alpha$, $\beta$, $\gamma$, $\delta$ die Werte $\alpha'$, $\beta'$, $\gamma'$, $\delta'$ 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 $\mu$ 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 $\mu$, so erhält man alle Darstellungen von $M$, bei denen der größte gemeinsame Teiler der Zahlen $x, y$ gleich $\mu$ 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 $\nu$ 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 $\alpha, \beta, \gamma$ usw. ungerade ist, oder $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ usw. $+\frac{1}{2}$, wenn alle $\alpha, \beta, \gamma$ 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 $a$: $\mp 1$, 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 $F^\lambda, F^\mu, F^\nu$ mit den jeweiligen Indizes $\lambda, \mu, \nu$, sodass $\lambda, \mu, \nu$ verschiedene Zahlen zwischen 0 und $2n-1$ einschließlich der Grenzen sind. Dann sind die Formen $F^{\lambda-1}$ und $F^\lambda$, 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 $\alpha$ 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 $\alpha''$ 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 $\alpha^m$ das Vorzeichen $+, +, -, -$ hat, je nachdem $m \equiv 0, 1, 2, 3 \pmod 4$. Ist $a$ negativ, so erhält man durch einen ähnlichen Schluss $\alpha''$ negativ, $\alpha'''$ positiv und entweder $>$ oder $= \alpha''$; $\alpha''''$ positiv und $> \alpha'''$; $\alpha'''''$ negativ und $> \alpha''''$ usw., sodass die Folge $\alpha', \alpha'', \alpha'''$ usw. fortwährend wächst und das Glied $\alpha^m$ 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: $\beta, \beta', \beta''$ 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 $\alpha^m$ und $\gamma^m$ dasselbe Vorzeichen, wenn $a$ positiv ist. Entgegengesetzte, wenn $a$ negativ ist, und ebenso $\beta^m$ und $\delta^m$; 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 $\alpha^m$ 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 $m, \mu, m', n, \nu, n'$ 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 $\nu$ 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 $\nu$ 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* $\gamma$ *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* $\alpha$ *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 $\alpha$ noch $\beta = 0$ ist, der erste Teil des Satzes auch für den zweiten Fall bewiesen (denn die Bedingung, dass weder $\gamma$ 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 $\gamma$ 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 $\gamma$ oder $\delta = 0$ ist. Aber *alle diese Fälle sind unmöglich*. Für den *ersten* Teil des Satzes nehmen wir an, weder $\gamma$ 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 $\delta$ 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 $\alpha$ 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 $\beta$ 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 $\gamma$ oder $\delta$ 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 $\alpha$ und $\beta$ 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 $\alpha^m$ 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 $\beta^m$ zu $\delta^m$ 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 $\beta^m$ zu $\delta^m$ 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 $\Phi$, $\varphi$ mit derselben Determinante entscheiden, ob sie äquivalent sind oder nicht.*

*Lösung.* Wir suchen zwei reduzierte Formen $F$, $f$, die zu den gegebenen Formen $\Phi$, $\varphi$ 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 $\Phi$, $\varphi$ 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 $\Phi^n$, $\varphi^\nu$ reduziert sind. Da $\Phi$, $\varphi$ nach Voraussetzung eigentlich äquivalent sind, muss $\Phi^n$ in der Periode von $\varphi^\nu$ enthalten sein. Sei $\varphi^\nu = f$, und ihre Periode bis zur Form $\Phi^n$ sei

$$f,\ f',\ f'' \dots f^{m-1},\ \Phi^n$$

sodass $\Phi^n$ 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 $\varphi$ in die letzte $\Phi$ finden. Bei den übrigen Formen der Folge ist das leicht zu sehen; für $f^{m-1}$, $\Psi^{n-1}$ 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 $\Psi^{n-1}$, der Form $(g, h, i)$, *d.h.* der Form $f^{m-1}$, nach rechts benachbart.

Sind die Formen $\Phi$, $\varphi$ uneigentlich äquivalent, so ist $\varphi$ zu der Form eigentlich äquivalent, die $\Phi$ entgegengesetzt ist. Wir können also eine eigentliche Transformation von $\varphi$ in die zu $\Phi$ entgegengesetzte Form finden. Erfolgt diese durch die Substitution $\alpha, \beta, \gamma, \delta$, so sehen wir leicht, dass $\varphi$ uneigentlich in $\Phi$ selbst transformiert wird, und zwar durch die Substitution $\alpha, -\beta, \gamma, -\delta$.

Damit ist auch klar, dass wir für die Formen $\Phi$, $\varphi$, wenn sie sowohl eigentlich als auch uneigentlich äquivalent sind, *zwei* Transformationen finden können, eine eigentliche und eine uneigentliche.

*)Es entsteht also $\Psi$ aus $\Phi$, 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 $\Phi$, so können wir daraus *alle* gleichartigen Transformationen von $\varphi$ in $\Phi$ ableiten, sofern wir alle Lösungen der unbestimmten Gleichung $tt - Duu = mm$ angeben können. Dabei bezeichnet $D$ die Determinante der Formen $\Phi, \varphi$ 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 $\gamma^n$ 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 $\mu$ strikt zwischen 0 und $n$ liegen. Die entsprechende Form $f^\mu$ 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, $\alpha^n$ und $\frac{b}{a'}\beta^n$ dasselbe Vorzeichen haben, ebenso $\delta^n$ 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 $\infty$, 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 $\upsilon$ ganzzahlig und daher auch $\tau$, weil $\tau\tau = D\upsilon\upsilon + mm$.

2° Offenbar kann $\upsilon$ 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 $\upsilon$ 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 $\rho$ 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 $u^\lambda$ 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 $u^\lambda$ 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 $u^\lambda$ 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 $\Phi, \varphi$ 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 $\varphi$ in $\Phi$, etwa $\alpha, \beta, \gamma, \delta$. Offenbar kann es keine anderen als dazu gleichartige Transformationen geben. Sind aber $\varphi, \Phi$ 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 $\varphi$ 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 $\varphi$ in $\Phi$ 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 $\beta$ und $\delta$ teilerfremd sind. Wir bestimmen $\alpha$, $\gamma$ 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 $\beta$, die dritte mit $\alpha$ 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 $\Phi$ eigentlich äquivalent, die somit nach Voraussetzung auch zu $F'$ eigentlich äquivalent ist. Wir suchen nach Artikel 206 eine eigentliche Transformation von $F$ in $\Phi$, etwa $\alpha, \beta, \gamma, \delta$, und ebenso eine eigentliche Transformation von $F'$ in $\Phi$, etwa $\alpha', \beta', \gamma', \delta'$. Dann geht $\Phi$ 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 $\Phi$ 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 $\beta g$ 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 $\beta$, $\delta$ 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 $\Omega$.

Ist *z.B.* die Form $f$ gleich $(2, 5, 7)$ und gilt $e = 5$, so enthält $\Omega$ 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 $\Omega$ 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 $\gamma, \delta$ (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 $\Omega$ 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 $\Omega$ bezeichnen wir dieselbe Gesamtheit von Formen wie im vorhergehenden Artikel. Daraus wählen wir alle Formen aus, denen $F$ eigentlich äquivalent ist; sie seien $\Phi, \Phi', \Phi''$ 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 $\Phi, \Phi'$ usw. geliefert wird). Da die Methode für alle Formen $\Phi, \Phi'$ usw. dieselbe ist, sprechen wir nur von einer.

Es sei $\Phi$ gleich $(M; K)$ und $e = MN$, sodass $f$ in $\Phi$ übergeht, und zwar durch die eigentliche Substitution $M, K, 0, N$. Ferner bezeichnen wir alle eigentlichen Transformationen von $\Phi$ in $F$ mit $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$. Dann geht offenbar $f$ in $\Phi$ 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 $\Phi$ in $F$ eine eigentliche Transformation von $f$ in $F$. — Die übrigen Formen $\Phi', \Phi''$ 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 $\gamma, \delta$. Die Zahlen $m, g, h, k$ bestimmen wir wie dort. Dann ist $(m; k)$ unter den Formen $\Phi, \Phi'$ 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 $\Phi$ oder $\Phi'$ usw. in $F$ nicht dieselbe Transformation von $f$ in $F$ erzeugen können. Dass aber auch verschiedene Formen, *z.B.* $\Phi$ und $\Phi'$, 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 $\Phi$ in $F$ *als auch* aus der eigentlichen Transformation $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \mathfrak{d}'$ von $\Phi'$ 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 $\Phi, \Phi'$ 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 $\Omega$ 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 $\xi, \upsilon$ 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 $\rho$ 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 $\rho$ 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 $\mu, \mu', \mu''$ 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 $m,\alpha,\beta$ 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 $\zeta,\zeta',\zeta''$ 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 $\alpha$, $\beta$ 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 $\alpha$, $\beta$ 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 $\alpha$, $\beta$, $\gamma$ 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 $A^\alpha$, $B^\beta$, $C^\gamma$ usw. Ist also ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$ nach dem Modul $A^\alpha$ gleich $(\mathfrak{A}, \mathfrak{A}')$; nach dem Modul $B^\beta$ gleich $(\mathfrak{B}, \mathfrak{B}')$; nach dem Modul $C^\gamma$ 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 $A^\alpha$, $B^\beta$, $C^\gamma$ usw. gilt (Artikel 32), so sieht man leicht, dass $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ nach allen Moduln $A^\alpha$, $B^\beta$, $C^\gamma$ 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; $\lambda$, $\mu$ sind beliebige verschiedene ganze Zahlen zwischen 0 und $n$ einschließlich, deren größere $\mu$ 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 $(\lambda, \mu)$, sodass

$$\Sigma(\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1$$

gilt. (Mit dem Buchstaben $\Sigma$ bezeichnen wir die Summe aller Werte des Ausdrucks, der auf ihn folgt, die entstehen, wenn man $\lambda$, $\mu$ 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 $\nu$ 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 $\lambda$, $\mu$ 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 $\Delta$ 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 $\Delta$ 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 $\Delta$ 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 $4\Delta$ 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 $\Delta$. 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 $\Omega$ 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 $\mu$ 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 ($\Omega$) 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega'$ 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 $\Omega$ und $\Omega'$ 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 $\Omega'$ ein, so bestätigt man mithilfe der Gleichungen $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ und der letzten drei Gleichungen $\Omega$ 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 $\Phi$ 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 $\Psi$ 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 $\Psi$ 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 $\Phi$. Die übrigen Gleichungen überlassen wir den Lesern zur Bestätigung.

V. Aus den Gleichungen $\Phi$ 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 $\Phi$ 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 $\Phi$ entsprechende Gleichungen, die wir mit $\Phi'$ bezeichnen, und neun weitere, den Gleichungen $\Psi$ entsprechende, die wir mit $\Psi'$ 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 $\Phi'$

$$(1,2)' = aa'\mathfrak{n}'', \quad (1,3)' = aa''\mathfrak{n}', \quad \text{etc.}$$

und die Gleichungen $\Psi'$

$$(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}', \quad \text{etc.}$$

(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 $\Phi$ und $\Phi'$ 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 $\alpha$, $\beta$, $\gamma$, $\delta$ 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 $\Psi$ die Werte von $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$ und aus den ersten drei Gleichungen $\Psi'$ 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 $\alpha$, $\beta$, $\gamma$, $\delta$ übergeht. — Nimmt man aber anstelle der ersten drei Gleichungen in $\Psi$ und $\Psi'$ 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 $\Psi$, $\Psi'$, 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 $\alpha$, $\beta$, $\gamma$, $\delta$ 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 $\mu$ 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 $\mu$, 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 $\mu$, $c$, $c'$, $b - b'$ 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 $\lambda$ ist. Dann ist $h^{\lambda}$ 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 $h^\lambda$ 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 $h^\lambda$ 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 $\mu$. Also kann $aa'$ auch durch die Form $F$ so dargestellt werden, dass die Werte der Unbestimmten den größten gemeinsamen Teiler $\mu$ 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 $\alpha, \gamma$ teilerfremd sind. Wählt man dann $\beta, \delta$ 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 $\varphi$ die einfachste Form der Ordnung $O$; $\mathfrak{F}$, $\mathfrak{f}$ seien eigentlich primitive Formen der Determinante $D$, die mit $\varphi$ 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 $\alpha e$, $\gamma e$ 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 $\beta$, $\delta$ 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 $\gamma$ 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 $\gamma$ 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 $\gamma k$ und somit auch $\gamma$ 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 $\mu$

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 $\pm 2$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$, 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 $\Omega$ 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 $\alpha$, $\beta$ 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 $\alpha$ den Wert $-\alpha$, für $\beta$ 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, $\alpha$, $\beta$, $\gamma$ 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 $\alpha$, $\beta$, $\alpha'$, $\beta'$ 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 $\alpha$, $\beta$, $\alpha'$, $\beta'$ 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 $\beta'$, $-\gamma'$, $-\beta''$, $\gamma''$ 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 $\beta'$, $\gamma'$, $\beta''$, $\gamma''$ 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 $\beta$, $\gamma$, $\gamma'$ 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 $\beta$, $\gamma$, $\gamma'$ 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 $\beta$ und $\gamma'$ 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 $\beta$, $\gamma'$ auf diese Weise bestimmt, so lässt sich der Wert von $\gamma$ 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 $\alpha$ 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 $\beta$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi, \chi$ eigentlich äquivalente binäre Formen, so ist jede Darstellung von $D$ durch $F$, die einer Darstellung der Form $\varphi$ durch $f$ adjungiert ist, auch einer Darstellung der Form $\chi$ durch $f$ adjungiert.

Seien $p, q$ die Unbestimmten der Form $\chi$; die Form $\varphi$ gehe in $\chi$ durch die eigentliche Substitution $t = \alpha p + \beta q$, $u = \gamma p + \delta q$ über, und irgendeine Darstellung der Form $\varphi$ 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 $\chi$ 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 $\varphi$ 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 $\chi$ 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 $\varphi, \chi$ 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, $\varphi$ werde durch $f$ dargestellt, indem man

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u$$

setzt, $\chi$ 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 $\varphi$ 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 $\chi$, 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 $\varphi, \chi$ 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 $\lambda, \mu, \nu$ 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 $\Delta$ 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 $\Delta D$ 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 $\mu$, so sind offenbar alle Koeffizienten der Form $F$ durch $\mu\mu$ teilbar. Also muss auch $\Delta D$ 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 $\mu$ 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 $\Delta$ 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 $\varphi$ 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 $f, \varphi$ 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 $\Delta$ 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, $\varphi$ durch keine ternäre Form mit der Determinante $\Delta$ eigentlich dargestellt werden kann. Sind also $\Delta, D$ teilerfremd, so muss $\Delta$ eine charakteristische Zahl der Form $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $(\Omega)$, 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 $\zeta, \eta$ 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 $\Delta$ 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 $(\Omega)$ 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 $\Delta$ 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 $\varphi$ eine primitive Form und $\Delta$ 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 $\Delta$ zu $D$ teilerfremd ist, der Ausdruck $\Delta(p, -q, r)$ nur dann ein quadratischer Rest von $D$ sein kann, wenn $\varphi$ 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 $\Delta$ nicht zu $D$ teilerfremd sein. Also können $p, q, r$ keinen gemeinsamen Teiler haben; mit anderen Worten, $\varphi$ 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 $\Delta$, $D$ 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 $\Delta$ zu $D$ teilerfremd ist.

III. Ist dies geschehen, so muss offenbar jede eigentliche Darstellung der Form $\varphi$ 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 $\Delta$, $D$ teilerfremd sind, $b, b'\, a''$ notwendig ganze Zahlen sind (denn diese drei Zahlen ergeben sowohl mit $D$ als auch mit $\Delta$ 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 $\varphi$ 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 $k$, $\mathfrak{k}$, $\zeta$, $\eta$ 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 $\Delta$ positiv, $D$ negativ und $\varphi$ eine negative Form, so ist $g$ eine negative definite Form. Ist dagegen $\Delta$ positiv und entweder $D$ positiv oder $D$ negativ und $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ zum Quadratteiler $ee$ oder $e'e'$ oder $e''e''$ usw. *gehört*. Alle Darstellungen der Form $\varphi$, 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 $\varphi$ 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 $\varphi$; $\kappa$, $\mu$ positive ganze Zahlen (deren Produkt also $= e$ ist); $\lambda$ eine positive ganze Zahl kleiner als $\mu$ (oder auch null). Diese Formen findet man mit den zugehörigen Transformationen folgendermaßen:

Man setze $\kappa$ der Reihe nach jedem positiven Teiler von $e$ gleich (einschließlich 1 und $e$) und $\mu = \frac{e}{\kappa}$. Für jedes Paar bestimmter Werte von $\kappa$, $\mu$ gebe man $\lambda$ 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 $\varphi$ übergeht, findet man nun, indem man die Form bestimmt, in die $\varphi$ 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 $\Phi$ eine dieser Formen, die in $\varphi$ durch die Substitution $T = \kappa t + \lambda u$, $U = \mu u$ übergeht. Man suche alle *eigentlichen* Darstellungen der Form $\Phi$ 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 $\kappa$ nur solche Teiler von $e$ nehmen muss, deren Quadrat den ersten Koeffizienten der Form $\varphi$ 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 $\Phi$, sodass aus jeder ihrer eigentlichen Darstellungen weitere Darstellungen abgeleitet werden. Ich behaupte, dass man so sämtliche Darstellungen der Form $\varphi$ erhält, die zum Teiler $ee$ gehören, und zwar jede genau einmal.

*Beweis.* I. Dass die ternäre Form $f$ durch jede Substitution $(\rho)$ tatsächlich in $\varphi$ übergeht, ist so offensichtlich, dass keine weitere Erklärung nötig ist. Dass aber jede Darstellung $(\rho)$ 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 $(\rho)$ der Form $\varphi$ 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 $\kappa$, $\lambda$, $\mu$, 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 $\kappa$ den positiv genommenen größten gemeinsamen Teiler von $\alpha$, $\alpha'$, $\alpha''$ 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 $\lambda$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ enthalten, nicht durch $f$ eigentlich dargestellt werden. Denn alle diese Formen haben eine Determinante mit demselben Vorzeichen wie $\varphi$. Sind diese Determinanten negativ, so sind sie alle positive oder alle negative Formen, je nachdem $\varphi$ 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 $(\tau)$, $(\tau')$, $(\tau'')$ usw. in sich selbst und durch die Substitution $(t)$ in $f'$ über, so erhält man offenbar durch Verbindung der Transformation $(t)$ mit $(\tau)$, $(\tau')$, $(\tau'')$ 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 $(\Omega)$ 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 $\alpha$, $\alpha'$, $\alpha''$ im ersten Fall jeweils mit $\beta$, $\beta'$, $\beta''$, im zweiten mit $\gamma$, $\gamma'$, $\gamma''$ vertauscht.

III. Sind alle $a$, $a'$, $a''$ gleich, so verlangen die Gleichungen $1, 2, 3$, dass von den drei Zahlen $\alpha$, $\alpha'$, $\alpha''$ sowie von $\beta$, $\beta'$, $\beta''$ und auch von $\gamma$, $\gamma'$, $\gamma''$ 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 $\alpha$, $\beta$, $\gamma$ nur eine $= \pm 1$ sein kann; ebenso von $\alpha'$, $\beta'$, $\gamma'$ und von $\alpha''$, $\beta''$, $\gamma''$. 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 $\varphi$ 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 $\varphi$ 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 $\beta b$, $\alpha b$, also auch $\alpha$ und $\beta$ 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 $\varphi$ 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 $\varphi$ 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 $\Omega$ 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 $\Omega$ ein vollständiger Charakter. Nach Art. 233 V kann 1 nur für solche Formen eine charakteristische Zahl sein, deren Charakter $\Omega$ ist. Nun ist $\Omega$ 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 $\Omega$, 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 $\Omega$ noch kein vollständiger Charakter; die Beziehung zur Zahl 4 muss hinzukommen. Offenbar muss aber $\Omega$ 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 $\Omega$ 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 $\varphi$ 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 $\varphi$, also auch der entgegengesetzten Form $(p, -q, r)$, so gibt es eigentliche Darstellungen der Form $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$, $\varphi'$ beliebige äquivalente binäre Formen und $(\Theta)$ eine gegebene Transformation der ersten in die zweite, so ergibt die Verbindung einer beliebigen Darstellung der Form $\varphi$ durch eine ternäre Form $f$ mit der Substitution $(\Theta)$ eine Darstellung der Form $\varphi'$ durch $f$. Dabei entstehen aus eigentlichen Darstellungen von $\varphi$ eigentliche Darstellungen von $\varphi'$, aus verschiedenen verschiedene und schließlich aus allen sämtliche. All dies lässt sich sehr leicht durch Rechnung bestätigen. Die eine der Formen $\varphi$, $\varphi'$ lässt sich also auf genauso viele Arten durch $f$ darstellen wie die andere.

I. Sei zuerst $\varphi = tt + uu$ und $\varphi'$ eine beliebige andere positive binäre Form mit der Determinante $-1$, zu der $\varphi$ daher äquivalent ist. Es gehe $\varphi$ in $\varphi'$ durch die Substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ über. Die Form $\varphi$ 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 $\varphi'$ 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 $\varphi'$ eine beliebige andere positive binäre Form mit der Determinante $-2$, in die $\varphi$ durch die Substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ übergeht. Dann folgt wie im vorigen Fall, dass sich $\varphi$ und somit auch $\varphi'$ nur auf eine einzige Weise in drei Quadrate zerlegen lässt: $\varphi$ in $tt + uu + uu$ und $\varphi'$ 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 $\varphi$, $\varphi'$, $\varphi''$ usw. Man bestimme sämtliche eigentlichen Darstellungen aller dieser Formen durch $F$. Ihre Anzahl ist daher $3\,.\,2^{\mu+3}k = K$, wobei $\mu$ 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 $\Omega$ bezeichnen, enthält notwendig sämtliche Darstellungen von $M$.

III. Es bleibt also nur zu untersuchen, ob in $\Omega$ *identische* Darstellungen auftreten können. Nach Art. 280, III sind die Darstellungen in $\Omega$, die aus verschiedenen Formen, *zum Beispiel* aus $\varphi$ und $\varphi'$, hergeleitet wurden, notwendig verschieden. Es bleibt daher nur die Frage, ob verschiedene Darstellungen derselben Form, *zum Beispiel* von $\varphi$, durch $F$ identische Darstellungen der Zahl $M$ durch $xx + yy + zz$ ergeben können. Nun ist sofort klar: Kommt unter den Darstellungen von $\varphi$ 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 $\varphi$ 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 $\varphi$ in sich selbst durch

$$t = \alpha t + \beta u, \quad u = \gamma t + \delta u$$

gegeben, so werden alle Darstellungen der Form $\varphi$, 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 $\varphi$ in sich selbst gibt, nämlich $\alpha, \beta, \gamma, \delta = 1, 0, 0, 1$ und $= -1, 0, 0, -1$. (Da $\varphi$ 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 $\Omega$ 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 $\varphi$ 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 $\mu$ 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 $\varphi$,

$\varphi'$, $\varphi''$ zu bestimmen. Zunächst bestätigt man leicht, dass alle (48) Darstellungen der Form $\varphi$, 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 $\varphi$ in drei Quadrate aufzuschreiben; ebenso bei den übrigen $\varphi'$, $\varphi''$ usw. Gehört ferner $\varphi$ 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 $\varphi$ entgegengesetzten Klasse werde die zu $\varphi$ entgegengesetzte Form gewählt, und diese sei $= \varphi'$. Dann sieht man ohne Mühe: Werden die eigentlichen Zerlegungen der Form $\varphi$ allgemein durch

$$(gt+hu)^2 + (g't+h'u)^2 + (g''t+h''u)^2$$

gegeben, so werden alle Zerlegungen der Form $\varphi'$ 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 $\varphi$ 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* $(\Omega)$ *in ganzen Zahlen lösbar.*

*Beweis.* Ist $(\Omega)$ überhaupt in ganzen Zahlen lösbar, so auch durch Werte von $x, y, z$, die keinen gemeinsamen Teiler haben. Denn beliebige Werte, die der Gleichung $\Omega$ 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 $\mu$, 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 $(\Omega)$ 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 $(\Omega)$ 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 $\mu$, so ist dieser

offenbar zu $a, b, c$ und somit zu $abc$ teilerfremd. Durch Division jener Werte durch $\mu$ 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 $\mu$, 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 $\mu$ auch $A, B, C$ teilen, entgegen der Voraussetzung. Man kann also ganze Zahlen $\alpha, \beta, \gamma$ 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 $(\Omega)$, 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 $\varphi$ 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 $\Omega$. 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 $\varphi$ die Form $(161, -63, 24)$, als Wert des Ausdrucks $\sqrt{} - \varphi \pmod{105} = (7, -51)$ und als Darstellung der Form $\varphi$ 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 $\Omega$ 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 $\Omega$ lösbar, so nur durch gerade Werte von $x, y, z$, *was ein Widerspruch ist*, da beliebige Werte, die der Gleichung $\Omega$ 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 $(\omega)$ 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 $(\Omega)$ durch $X = P, Y = Q,\ Z = R$ erfüllt, so wird offenbar $(\omega)$ 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 $\alpha, \beta$ Konstanten, und zwar

$$\alpha = \frac{4}{\pi\pi} = 0{,}4052847346$$

wobei $\pi$ 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 $\mu$ 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 $\varphi m$ 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 $\mu$ 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 $\varphi n$ Klassen, deren Perioden dasselbe ganze Geschlecht umfassen, und $\varphi e$ 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 $\varphi n$ 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 $\varphi n$ 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 $2^\mu$, 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 $\varepsilon$ 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 $\alpha, \beta$ 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 $\alpha', \beta'$ 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 $\alpha$ im vorigen Artikel, etwa $\beta$ durch die Kongruenz $\beta acd$ usw. $\equiv m$ (mod. $b$), $\gamma$ durch $\gamma abd$ 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 $\nu$ 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 $\mu$ 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 $p^\mu$ 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 $p^\mu$ 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 $\lambda$ 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 $p^\mu$ 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 $p^\mu$ 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 $p^\mu$ kongruent sind. Es sei $10^e$ die kleinste Potenz von 10, die nach $p^\mu$ 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 $\alpha, \beta$ 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 $r^\beta$, also 1, wenn $\beta = 0$, indem man die ersten $\alpha$ 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 $p^\mu$ 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 $\alpha$ und $\beta$ Zahlen sind, von denen wenigstens eine nicht 0 ist, so beginnt die Mantisse nach den ersten $\alpha$ oder $\beta$ Ziffern aus Perioden zu bestehen, je nachdem $\alpha$ oder $\beta$ 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 $\alpha$ oder $\beta$ 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 $\Omega$ 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 $\alpha, \beta, \gamma$ usw., die alle positiv und kleiner als $E$ gewählt werden dürfen. Gibt man also $y$ einen Wert, der einer der Zahlen $\alpha, \beta, \gamma$ 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 $\Omega$ sofort alle Zahlen der Formen $Et + \alpha, Et + \beta, Et + \gamma$ usw. als unbrauchbar ausgeschlossen werden, und es genügt, die übrigen, deren Gesamtheit $\Omega'$ 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 $\alpha', \beta', \gamma'$ usw., wie sie verschiedene quadratische Nichtreste hat, denen $y$ nach dem Modul $E'$ nicht kongruent sein kann. Daher darf man wiederum aus $\Omega'$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ alle Zahlen der Form $3t + 1$ auszuschließen; die Anzahl der verbleibenden Zahlen $\Omega'$ 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 $\Omega$ 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 $p^\mu$, einer Potenz der Primzahl $p$, die Ausschlusszahl $p$ oder $p^\nu$ bei $\nu < \mu$ überflüssig wird. Da nämlich $p^\mu$ unter den Werten von $V$ nur seine Reste übrig gelassen hat, sind erst recht keine Nichtreste von $p$ oder einer beliebigen niedrigeren Potenz $p^\nu$ mehr vorhanden. Ist aber $p$ oder $p^\nu$ bereits vor $p^\mu$ verwendet worden, so kann die letztere offenbar nur solche Werte von $V$ entfernen, die zugleich Reste von $p$ (oder $p^\nu$) und Nichtreste von $p^\mu$ sind. Daher genügt es, nur solche Nichtreste von $p^\mu$ für $a, b, c$ usw. zu nehmen.

**322.**

Die Berechnung der Zahlen $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $\alpha, \beta, \gamma$ 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 $p^\mu$, 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 $\mu$ gerade ist; oder mit sämtlichen Nichtresten von $p$ kleiner als $p$, wenn $\mu$ 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 $2^\mu$, nachdem die niedrigeren bereits verwendet worden sind, so muss man $a = 2^{\mu-1}, b = 3.2^{\mu-2}$ setzen, wenn $\mu$ 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 $\mu$ 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 $\Omega$ entfernt werden können, nachdem die Zahlen $\alpha, \beta, \gamma$ 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 $\Omega$ 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 $\Omega$ 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 $p^\nu$ 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 $\alpha, \beta, \gamma$ 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. $Ep^\nu$) gilt, der entsprechende Wert von $V \equiv a$ (mod. $E$), also ein Nichtrest von $E$ wird; ebenso verhält es sich mit den übrigen Zahlen $\beta, \gamma$ 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. $Ep^\nu$) gilt. Somit liefern alle Werte von $x$, für die $xx$ keiner der Zahlen $\alpha, \beta, \gamma$ usw. nach dem Modul $Ep^\nu$ 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 $\alpha, \beta, \gamma$ usw. sämtliche quadratischen Reste von $Ep^\nu$ aus, die $g, g', g''$ usw. seien, berechne die Werte der Ausdrücke $\sqrt{g}, \sqrt{g'}.\sqrt{g''}$ usw. (mod. $Ep^\nu$) 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 $\Omega$ entfernen kann und dass keinem Wert von $x$, der nach diesem Ausschluss in $\Omega$ 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 $\alpha, \beta, \gamma$ usw. keine quadratischen Reste von $Ep^\nu$ 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 $\Omega$ 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 $\Omega$ weniger Glieder enthält, was man leicht im Voraus abschätzen kann. — Schließlich brauchen wir kaum zu bemerken, dass, wenn nach einigen Ausschlüssen *sämtliche* Zahlen aus $\Omega$ 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 $\Omega$ 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 $\Omega$ zu entfernen; die sechzehn übrigen seien mit $\Omega'$ 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 $\Omega'$ sämtliche Zahlen der Formen $25t \pm 3,\ 25t \pm 7$, so bleiben diese zehn ($\Omega''$): $173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577$. 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 $\Omega''$ die Zahlen der Formen $49t \pm 9,\ 49t \pm 19,\ 49t \pm 23$, so bleiben diese fünf ($\Omega'''$): 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 $\alpha, \beta$ usw. $= 8, 10, 5, 0, 1$, von denen drei Reste von 11 sind, nämlich $0, 1, 5$. Daraus folgt, dass aus $\Omega'''$ 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 $\Omega$ 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 $\alpha, \beta, \gamma$ 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 $\alpha, \beta$ 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 $\mu$ 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 $\alpha, \beta$, $\gamma$ usw. der Zahl $k$ nach dem Modul $p$ kongruent sind und daher $p^\mu$ nichts aus $\Omega$ 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 $\alpha$ 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 $\mu$ gerade ist; oder mit sämtlichen Nichtresten von $p$ unter dieser Grenze, wenn $\mu$ ungerade ist und $eRp$ oder, was hier dasselbe bedeutet, $-2mrn'Rp$ gilt; oder mit sämtlichen Resten, außer 0, wenn $\mu$ 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 $p^\mu$ 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 $\mu$ 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 $\mu, \nu$ 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 $\Omega$, so genügt es offenbar, sämtliche Primteiler von $M$, die in $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ übrig bleibt, so zeigt das vollständige, bis 997 fortgesetzte Schema, dass *überhaupt* keine andere in $\Omega$ 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 $127 \times 7853$ 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 $\mu$ 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 $2^\mu$, so ist $M$ aus $\mu$ 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 $\pi$ 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 $\pi$ 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 $p^\lambda$ 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* $\lambda$*-ten Potenzen der Wurzeln der Gleichung* $(W)$ *sind, wobei* $\lambda$ *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 $\Omega$ 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 $\Omega$, 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 $\lambda, \mu$ nach $n$ kongruente ganze Zahlen sind, $r^\lambda = r^\mu$ gilt. Sind dagegen $\lambda, \mu$ nach dem Modul $n$ inkongruent, so sind $r^\lambda$ und $r^\mu$ ungleich; denn in diesem Fall lässt sich eine ganze Zahl $\nu$ 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 $\Omega$ überein. Allgemeiner folgt daraus leicht, dass $\Omega$ 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 $\omega$ entweder dem Winkel $\frac{P}{n}$ oder einem seiner Vielfachen gleich ist.

**340.**

Bezeichnet man also eine Wurzel aus $\Omega$ 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 $r^\lambda$ darstellen, wobei $\lambda$ 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 $r^\sigma$ 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 $\lambda$

$$\varphi(a^\lambda, b^\lambda, c^\lambda \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \ldots + A^\nu r^{(n-1)\lambda}$$

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* $(\Omega)$ *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 $\Omega$ 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 $\Omega$, 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 $n^\lambda$ 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 $\Omega$ selbst gelangt. Wir werden nämlich zeigen: Zerlegt man die Zahl $n-1$ auf beliebige Weise in ganzzahlige Faktoren $\alpha, \beta, \gamma$ usw. (für die man jeweils Primzahlen nehmen kann), so lässt sich $X$ in $\alpha$ Faktoren vom Grad $\frac{n-1}{\alpha}$ zerlegen, deren Koeffizienten durch eine Gleichung vom Grad $\alpha$ bestimmt werden; jeder dieser Faktoren wiederum in $\beta$ andere vom Grad $\frac{n-1}{\alpha\beta}$ mithilfe einer Gleichung vom Grad $\beta$ usw. Bezeichnet also $\nu$ die Anzahl der Faktoren $\alpha, \beta, \gamma$ usw., so führt sich die Bestimmung der Wurzeln $\Omega$ auf die Lösung von $\nu$ Gleichungen der Grade $\alpha, \beta, \gamma$ 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 $r^\lambda$, wobei $\lambda$ 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 $\Omega$ gewählt wird. Allgemein sind somit $[\lambda], [\mu]$ gleich oder ungleich, je nachdem, ob $\lambda, \mu$ 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 $\lambda$ durch $n$ nicht teilbar oder teilbar ist.

*Sämtliche Wurzeln $\Omega$ 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 $\Omega$ übereinstimmen; ganz ebenso stimmen allgemeiner

$$[\lambda], [\lambda g], [\lambda gg] \ldots [\lambda g^{n-2}] \quad \text{mit} \quad \Omega$$

überein, wobei $\lambda$ 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 $\mu, \nu$ 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 $\mu$ eine beliebige positive Zahl $< f$ und $\nu$ 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* $(f, \lambda)$, 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* $\Omega$.

**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 $(f, \lambda)$ besteht, auch $(f, \lambda h), (f, \lambda hh)$ usw.; bezeichnet also allgemein $[\lambda']$ irgendeine Wurzel aus $(f, \lambda)$, so ist diese Periode mit $(f, \lambda')$ 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 $\Omega$ überein; in den übrigen Fällen besteht $\Omega$ 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 $(f, \lambda)$ mit einer von ihnen überein, sofern $[\lambda]$ zu $\Omega$ gehört, das heißt, wenn $\lambda$ durch $n$ nicht teilbar ist. Die Periode $(f, 0)$ oder $(f, kn)$ besteht dagegen offenbar aus $f$ Einheiten. Ebenso leicht sieht man, dass, wenn $\lambda$ 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 $\Omega$ übereinstimmt. — So besteht *zum Beispiel* für $n = 19$, $f = 6$ die Gesamtheit $\Omega$ 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 $(bc, \lambda)$ 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* $(f,\lambda)$ *bestehe aus den Wurzeln* $[\lambda],[\lambda'],[\lambda'']$ *usw. Dann ist das Produkt aus* $(f,\lambda)$ *und* $(f,\mu)$ *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 $\lambda$, $\lambda',\lambda''$ 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 $(f,\nu)$ 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 $\lambda$ eine durch $n$ nicht teilbare Zahl ist, und schreibt man der Kürze wegen $p$ für $(f,\lambda)$, so lässt sich jede andere gleichartige Periode $(f,\mu)$, wobei auch $\mu$ 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 $\alpha,\beta$ 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 $(f,\mu)$ 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 $\lambda$ völlig unabhängig; *das heißt*, dieselben Gleichungen gelten auch dann noch, welchen

anderen Wert man $\lambda$ auch gibt. Diese Bemerkung erstreckt sich offenbar auch auf Gleichung I, sofern man $\lambda$ als durch $n$ nicht teilbar annimmt. — Nehmen wir $(f,\mu) = p'$ an; denn man sieht sehr leicht, dass, wenn $(f,\mu)$ 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 $\lambda$ unabhängig sind, ist klar, dass auch $Z$ nicht von $\lambda$ abhängt, also gilt, welche durch $n$ nicht teilbare ganze Zahl man auch für $\lambda$ 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 $\zeta, \zeta', \zeta''$ usw., $\eta, \eta', \eta''$ 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 $(f, \lambda)$ 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 $(f, \lambda)$ 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 $\mu, \mu', \mu''$ 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 $\theta, \theta'$ 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 $\mu, \mu', \mu''$ 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 $\varphi$ 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 $\alpha, \beta, \gamma$ usw. symmetrische Funktionen der Wurzeln, nämlich $\alpha$ die Summe aller Wurzeln, $\beta$ die Summe ihrer paarweisen Produkte, $\gamma$ die Summe ihrer Produkte zu je dreien usw. Daher ist in der Gleichung, deren Wurzeln die in der Periode $(f, \lambda)$ 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 $\alpha, \beta, \gamma$ 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 $\beta, \gamma$ usw. nach dem Newtonschen Satz aus den Potenzsummen der Wurzeln abzuleiten. Es ist nämlich unmittelbar klar, dass die Summe der Quadrate der in $(f, \lambda)$ 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 $\alpha, \beta, \gamma$; die Periode $(\beta\gamma, \lambda)$, die $\beta\gamma$ Glieder hat, bestehe aus $\beta$ kleineren Perioden mit $\gamma$ Gliedern, nämlich $(\gamma, \lambda).(\gamma, \lambda'), (\gamma, \lambda'')$ usw. Wir nehmen an, dass in einer Funktion von $\beta$ 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 $(\gamma, g^{\mu})$ und $(\gamma, g^{\alpha\nu+\mu})$, wobei $\nu$ 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 $\beta$ Perioden mit $\gamma$ 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 $\beta$ 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 $\beta$ Perioden mit $\gamma$ 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 $\beta$ Perioden mit $\gamma$ Gliedern durch eine Gleichung vom Grad $\beta$ 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 $\gamma$ Gliedern sind, die in einer gegebenen Periode mit $\beta\gamma$ Gliedern enthalten sind, bekannte Größen, sobald die Zahlenwerte aller $\alpha$ Perioden mit $\beta\gamma$ Gliedern bekannt sind. — Übrigens lässt sich die Berechnung der Koeffizienten dieser Gleichungen oft bequemer ausführen, besonders wenn $\beta$ 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 $\Omega$ 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 $\Omega$ in $\alpha$ Perioden mit $a$ Gliedern ein; jede einzelne von diesen wiederum in $\beta$ Perioden mit $b$ Gliedern, jede einzelne von diesen erneut in $\gamma$ Perioden usw. Nach dem vorigen Artikel suche man die Gleichung vom Grad $\alpha$, $(A)$, deren Wurzeln jene $\alpha$ 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 $\Omega$, und es ist völlig beliebig, welche Wurzel aus $\Omega$ 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 $\alpha$ Summen mit $a$ Gliedern gefunden, so suche man nach dem vorigen Artikel die Gleichung $(B)$ vom Grad $\beta$, deren Wurzeln die $\beta$ 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 $\beta$ zu ermitteln, deren Wurzeln jeweils die einzelnen $\beta$ 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 $\gamma$ sämtliche

$\alpha\beta\gamma$ Summen mit $c$ Gliedern bestimmt werden. Man muss nämlich *entweder eine* Gleichung vom Grad $\gamma$, deren Wurzeln die $\gamma$ 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 $\gamma$ aufstellen, deren Wurzeln jeweils die $\gamma$ 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 $\zeta$ Gliedern. Stellt man daher nach Artikel 348 die Gleichung vom Grad $\zeta$ auf, deren Wurzeln die $\zeta$ Wurzeln aus $\Omega$ 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 $\Omega$ 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 $\zeta$, die jeweils alle $\zeta$ Wurzeln in den einzelnen übrigen Perioden mit $\zeta$ Gliedern darstellen, alle übrigen Wurzeln $\Omega$ gefunden werden.

Übrigens ist klar, dass, sobald die erste Gleichung $(A)$ gelöst ist oder die Werte aller $\alpha$ Summen mit $a$ Gliedern bekannt sind, nach Artikel 348 unmittelbar auch die Zerlegung der Funktion $X$ in $\alpha$ 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 $\beta$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\alpha, \beta, \gamma$ 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 $\Omega$ in zwei Perioden bestimmt.*

**356.**

Die Hilfsgleichungen, durch die für jeden Wert von $n$ die Summen bestimmt werden, welche die Menge $\Omega$ 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 $\Omega$ 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 $\alpha, \beta, \gamma$ 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 $\beta$ und $\gamma$ 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 $\Omega$ 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 $\beta, \gamma$ 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 $g^{\lambda}$, 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 $\varepsilon$ 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 $\lambda$, 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 $\lambda$ 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 $\alpha, \beta, \gamma$. Der Kürze wegen werden wir die Untersuchung gleich so anlegen, dass sie auch die Fälle einschließt, in denen $\alpha$ 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 $\alpha$ Summen von $\beta\gamma$ Gliedern $(\beta\gamma, 1), (\beta\gamma, g)$, $(\beta\gamma, gg) \ldots (\beta\gamma, g^{\alpha-1})$ die Summen von $\gamma$ Gliedern abzuleiten sind. Diese Aufgabe haben wir oben auf eine gemischte Gleichung vom Grad $\beta$ 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 $\beta$ 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 $\beta$ 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 $R^\beta$ 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 $\beta$ 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 $\beta$ 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 $\beta$ 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 $t^\beta$, 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 $\gamma$ 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 $\beta$ 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 $\omega$ 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 $\Omega$ 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 $\Omega$ 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 $\omega$, 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 $\varphi$ 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 $\omega$ 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 $\alpha, \beta$, 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 $\varphi$ 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 $\varphi$ den Kosinus oder Sekans bezeichnet, die unteren, wenn $\varphi$ 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 $\lambda, \mu$, 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 $\varphi$ 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 $\varphi$ 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 $2^\mu$ 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 $\zeta$ (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 $a^\alpha$ 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 $\gamma$ dieselbe Größe wie in Artikel 302 und $\pi$, 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<br>(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;<br>(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;<br>(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<br>7462686567 164 |
| 71 | (0) . . 0140845070 4225352112 6760563380 28169; (1) . . 8732394366 1971830985<br>9154929577 46478 |
| 73 | (0) . . 01369863; (1) . . 06849315; (2) . . 34246575; (3) . . 71232876; (4) . . 56164383<br>(5) . . 80821917; (6) . . 04109589; (7) . . 20547945; (8) . . 02739726 |
| 79 | (0) . . 0126582278 481; (1) . . 3670886075 949; (2) . . 6455696202 531<br>(3) . . 7215189873 417; (4) . . 9240506329 113; (5) . . 7974683544 303 |
| 81 | (0) . . 012345679; (1) . . 135802469; (2) . . 493827160; (3) . . 432098765;<br>(4) . . 753086419; (5) . . 283950617 |
| 83 | (0) . . 0120481927 7108433734 9397590361 4457831325 3<br>(1) . . 6024096385 5421686746 9879518072 2891566265 0 |
| 89 | (0) . . 0112359550 5617977528 0898876404 4943820224 7191<br>(1) . . 3370786516 8539325842 6966292134 8314606741 5730 |
| 97 | (0) . . 0103092783 5051546391 7525773195 8762886597 9381443298 9690721649<br>4845360824 7422680412<br>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 $\pm 7$, 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 ($\Omega$) 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 $\Omega$ 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 $\Omega$ in zwei Perioden bestimmt, 356.
Beweis des im vierten Abschnitt erwähnten Satzes, 357.
Die Gleichung zur Einteilung der Wurzeln $\Omega$ 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 $\lambda'$ der größte gemeinsame Teiler der Zahlen $\lambda, C$, und man bestimme Zahlen $k, \gamma$ so, dass $k\lambda + \gamma C = \lambda'$ ist; daraus folgt $k\alpha A + k\beta B + \gamma C = \lambda'$. Offenbar ist aber $\lambda'$ 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 $(\alpha)$, das mit $(\alpha)$ in (2) übereinstimmt, folgt ebenso wie dort, dass entweder zugleich $hRp$, $hRa'$ oder $hNp$, $hNa'$ gilt. Im ersten Fall würde aber aus $(\delta)$ folgen, dass $aRa'$ gilt, entgegen der Voraussetzung; daher ist $hNp$ und somit nach $(\gamma)$ 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.