Carl Friedrich Gauss

Arithmetical Investigations

English translation

Volume I

This volume contains the historical title matter, dedication, preface, all seven sections, additions, tables, historical contents, Gauss's manuscript notes and the historical editor's closing note. The page references in the historical contents are those of the source.

Historical source: Carl Friedrich Gauss, Werke, Volume I, Göttingen, 1863. Disquisitiones Arithmeticae was first published in Leipzig in 1801.
AI-translated into English using OpenAI GPT-6.1 Sol.

Translation sources and terminology

Historical text: Carl Friedrich Gauss, *Werke*, Volume I, Göttingen, 1863. Historical editorial contributions retain their own authorship and signatures. Originally German passages are rendered in modern German in the German reader; their historical originals are supplied separately.
These English and German editions are AI-translated using OpenAI GPT-6.1 Sol, with AI-produced typesetting. The following named human translations and writings are scholarly references for the terminology and usage specified below. Gauss's original-language text remains the mathematical source.

H. Maser.

German translator and editor, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Corresponding arithmetical passages and German mathematical terminology.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead and Adam Miller Hiltebeitel.

Translators of Gauss's *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX edition. Related English geometrical terminology and usage.
`https://www.gutenberg.org/ebooks/36856`

Paul Taylor; Bernard Leak.

Taylor's English translation of Gauss's second proof of the fundamental theorem of algebra, with corrections by Leak, 1983. Related English algebraic terminology. The consulted online edition identifies the translation as December 1983, its LaTeX version as August 2003, and the underlying source as last modified on 8 June 2007. Its acknowledgements credit Mark Wainwright for returning Taylor's notes and Nikita Danilov for typo corrections.
`https://www.paultaylor.eu/misc/gauss.html`

Ulrich Görtz.

Algebra, WS 2021/22, 3.1.1–3.1.3 and opening of 3.1.4; *Lineare Algebra II*, SS 2021, 18.4. Contemporary German arithmetic and algebraic usage.
`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. Related contemporary German terminology for quadratic forms.
`https://arxiv.org/abs/1510.06214v3`

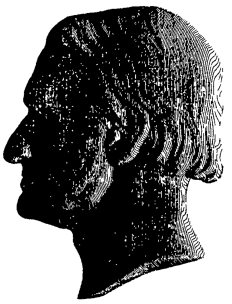
CARL FRIEDRICH GAUSS COLLECTED WORKS

VOLUME I.

CARL FRIEDRICH GAUSS

COLLECTED WORKS

VOLUME ONE



EDITED

BY THE

ROYAL SOCIETY OF SCIENCES

AT

GÖTTINGEN

1863.

ARITHMETICAL INVESTIGATIONS

BY

D. CARL FRIEDRICH GAUSS.

LEIPZIG

ON COMMISSION WITH GERH. FLEISCHER JR.

1801.

TO HIS MOST SERENE HIGHNESS
THE PRINCE AND LORD
CHARLES WILLIAM FERDINAND
DUKE OF BRUNSWICK AND LÜNEBURG.

MOST SERENE PRINCE

I consider it a great happiness that YOU allow me to dedicate this work to YOUR most exalted name; a sacred duty of gratitude binds me to offer it to YOU. For if YOUR favour, Most Serene Prince, had not first opened the way to learning for me, and if YOUR constant support had not sustained my studies, I could not have devoted myself entirely to mathematics, to which I have always been drawn by a passionate love. Indeed, it was YOUR kindness alone that enabled me to begin the very investigations of which this volume presents a part, continue them for several years, and put them in writing, by freeing me from other concerns so that I could give them my chief attention. When at last I wished to publish them, YOUR generosity removed every obstacle delaying their appearance. I can reflect on these great services YOU have rendered me and my efforts with a grateful heart and silent admiration more readily than I can celebrate them with fitting and worthy praise. I not only feel unequal to that task, but also believe that everyone knows how customary it is for YOU to show such exceptional generosity to all who seem to contribute to the cultivation of the finest studies. Even those sciences commonly thought harder to understand and less useful in everyday life are not excluded from YOUR protection: YOU YOURSELF, with a mind of such wisdom and such knowledge of everything that promotes the prosperity of human society, have fully recognised the close and necessary bond joining all the sciences. If YOU, Most Serene Prince, judge this book, a witness both to my deep gratitude towards YOU and to work devoted to a most noble science, not unworthy of the exceptional favour with which You have embraced me for so long, I will congratulate myself on having spent my efforts usefully and attained the honour I desired above all others

MOST SERENE PRINCE

Brunswick, July 1801.

Your Highness's most devoted servant
C. F. GAUSS.

PREFACE:

The investigations in this work belong to the part of mathematics that deals with integers; fractions are mostly excluded, and irrational quantities always are. What is called indeterminate or Diophantine analysis, which teaches us to select, from the infinitely many solutions of an indeterminate problem, those expressed by integers or at least by rational numbers (usually with the further condition that they be positive), is not this discipline itself but a very special part of it. Its relation to the discipline is much like that of the art of reducing and solving equations (Algebra) to the whole of Analysis. Just as all investigations into the general properties of quantities belong to the domain of *Analysis*, so integers (and fractions insofar as they are determined through integers) are the proper subject of ARITHMETIC. But what is usually taught under the name of Arithmetic hardly goes beyond the art of writing numbers and calculating (that is, representing numbers by suitable signs, for example in the decimal system, and carrying out arithmetical operations). Some further matters are added that either do not belong to Arithmetic at all (such as the theory of logarithms), or at least are not specific to integers but apply to all quantities. So it seems useful to distinguish two parts of Arithmetic: to assign these matters to elementary Arithmetic, and to reserve all general investigations into the properties specific to integers for *Higher Arithmetic*, which alone concerns us here.

Higher Arithmetic includes the matters that Euclid presented in Book VII and the following books of the Elements, with the elegance and rigour usual among the ancients; they are, however, confined to the very beginnings of this science. The celebrated work of Diophantus, devoted entirely to indeterminate problems, contains many questions whose difficulty and subtle methods inspire considerable respect for the author's ingenuity and insight, especially when we consider how few resources were available to him. But these problems call for dexterity and skilful handling rather than deeper principles; they are also too special and rarely lead to more general conclusions. So this book seems to mark an epoch in the history of mathematics more because it contains the first traces of symbolic notation and Algebra than because it enriched Higher Arithmetic with new discoveries. By far the greater part is owed to more recent scholars. Among them a few men, but men of immortal glory—P. DE FERMAT, L. EULER, L. LA GRANGE, A. M. LE GENDRE (to pass over a few others)—opened the way into the inner sanctuary of this divine science and revealed the riches it holds. I will not recount here which discoveries came from each of these mathematicians. These can be learned from the prefaces to the Additions with which the distinguished La Grange enriched Euler's Algebra, and to the work recently published by the distinguished Le Gendre that I will mention shortly. Most are also cited in their proper places in these Arithmetical Investigations.

The purpose of this work, which I publicly promised to publish five years ago, was to make known my investigations in Higher Arithmetic, some undertaken before that time and some afterwards. To explain why the science is taken up here almost from its beginnings, and why many investigations to which others have already devoted

their efforts are taken up again, I thought I should point out that, when I first turned to this kind of investigation at the beginning of 1795, I knew nothing of what more recent scholars had accomplished in this field and had no means of learning about it. While occupied with another task, I happened upon a remarkable arithmetical truth (unless I am mistaken, it was the theorem of article 108). I found it very beautiful in itself and suspected that it was connected with greater things, so I worked as hard as I could to understand its principles and find a rigorous proof. When I finally succeeded as I had hoped, these questions had so caught my interest that I could not leave them. As one thing kept opening the way to another, most of what is presented in the first four Sections of this work was completed before I had seen anything of the similar work of other mathematicians. Later, when I had the opportunity to read the writings of these great minds, I recognised that most of my thinking had been spent on matters long since settled. But following in their footsteps, I worked all the more eagerly to develop Arithmetic further; this led to various investigations, some of which are presented in Sections V, VI and VII. When, after some time, I decided to publish the fruits of my nightly work, I let myself be persuaded—all the more readily because several people wished it—to keep even the earlier investigations. At that time there was no book from which one could learn the work of other mathematicians on these subjects, scattered through the Transactions of Academies; many of my investigations were entirely new and most used new methods; and, finally, all were so *closely* connected with one another and with the later investigations that even the new material could not be explained conveniently enough without taking up the rest from the beginning.

Meanwhile an excellent work appeared by a man who had already done much for Higher Arithmetic: *Le Gendre, Essai d'une théorie des nombres, Paris, year VI.* He not only carefully collected and arranged everything accomplished so far in this science, but also added a great many new discoveries of his own. This book reached me late, after most of my work had already been printed, so I could not mention it wherever the similarity of the subjects might have provided an opportunity. It seemed necessary to add in the Additions some observations on just a few passages; I hope that this most courteous and fair-minded man will take them kindly.

During the printing of this work, repeatedly interrupted and prolonged by various obstacles into a fourth year, I continued investigations I had already begun but had decided to publish later to keep the book from becoming too large, and also began several new ones. Several others that, for the same reason, I had only touched on briefly, since a fuller treatment seemed less necessary (for example, those in articles 37, 82 and following, and elsewhere), were later taken up again and led to more general investigations that seem well worth publishing (compare also what is said in the Additions about article 306). Finally, the book grew far larger than I had expected, especially because of the length of Section V, so several things originally intended for it had to be cut, including the whole *eighth* Section (already mentioned at various places in this volume, and containing a general treatment of algebraic congruences of any degree). All this will easily fill a volume as large as the present one, and will be published as soon as an opportunity arises.

In several difficult questions I have used synthetic proofs and left out the analysis

by which they were found. The main reason was the need for brevity, which I had to consider as far as possible.

The theory of the division of the circle, or of regular polygons, treated in Section VII, does not *itself*, *in its own right*, belong to Arithmetic; its *principles*, however, must be drawn solely from Higher Arithmetic. This may be as unexpected to mathematicians as I hope the new truths drawn from this source will be welcome to them.

These are the matters I wished to explain to the reader in advance. It is not for me to judge the work itself. My greatest wish is that what fills gaps that have remained until now, or opens the way to new discoveries, may please those who have the advancement of the sciences at heart.

———————

ARITHMETICAL INVESTIGATIONS.

FIRST SECTION
ON
THE CONGRUENCE OF NUMBERS IN GENERAL.

Congruent numbers, moduli, residues and nonresidues.

1.

If the number a divides the difference between the numbers b, c, b and c are said to be *congruent with respect to* a; otherwise, *incongruent*: we call a itself the *modulus*. Each of the numbers b, c is called a *residue* of the other in the former case, but a *nonresidue* in the latter.

These notions apply to all integers, both positive and negative[*)], but are not to be extended to fractions. *For example,* -9 and $+16$ are congruent with respect to the modulus 5; -7 is a residue of $+15$ with respect to the modulus 11, but a nonresidue with respect to the modulus 3. Also, since every number divides zero, every number is regarded as congruent to itself modulo any modulus.

2.

All the residues of a given number a with respect to the modulus m are contained in the formula $a + km$, where k denotes an indeterminate integer. The simpler propositions that we will give later can be proved from this without difficulty; but anyone can see their truth just as easily by inspection.

From now on we will denote the congruence of numbers by the sign $\equiv$, adding the modulus in parentheses where necessary, $-16 \equiv 9 \pmod 5$. $-7 \equiv 15 \pmod{11}$[*)].

3.

THEOREM. *Given m successive integers*

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

and another integer A, exactly one of the former is congruent to the latter modulo m.

If $\frac{a-A}{m}$ is an integer, then $a \equiv A$; if it is a fraction, let the next greater integer (or, when it is negative, the next *smaller*, disregarding the sign) be $= k$. Then $A + km$ will fall between a and $a + m$, and so is the required number. It is clear that all the quotients $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$ etc. lie between $k-1$ and $k+1$; so no more than one of them can be an integer.

[*)] The modulus must always be taken *absolutely*, that is, without any sign.

[*)] We have adopted this sign because of the close analogy between equality and congruence. For the same reason, the distinguished Le Gendre, in the paper we will often cite below, kept the equality sign itself for congruence; we have hesitated to follow him, to avoid ambiguity.

Least residues.

4.

Every number will therefore have a residue both in the series $0, 1, 2, \ldots m-1$ and in the series $0, -1, -2, \ldots . -(m-1)$, which we will call *least residues*. It is clear that, unless 0 is a residue, there are always two, one *positive*, the other *negative*. If they are unequal in magnitude, one will be $< \frac{m}{2}$; otherwise both will be $= \frac{m}{2}$, without regard to sign. So every number has a residue not exceeding half the modulus, which will be called the *absolutely least residue*.

E.g. -13, modulo 5, has the least positive residue 2, which is also the absolutely least residue, while -3 is the least negative residue; $+5$, modulo 7, is its own least positive residue, while -2 is the least negative and also the absolutely least residue.

Elementary propositions concerning congruences.

5.

With these notions established, let us collect the properties of congruent numbers that are immediately apparent.

Numbers congruent modulo a composite number are also congruent modulo any divisor of it.

If several numbers are congruent to the same number modulo the same modulus, they will be congruent to one another (modulo that same modulus).

The modulus is also understood to be the same in the statements that follow.

Congruent numbers have the same least residues; incongruent numbers have different ones.

6.

If there are any number of integers A, B, C etc. and as many others a, b, c etc., congruent to them modulo any modulus,

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

If $A \equiv a, B \equiv b$, then $A - B \equiv a - b$.

7.

If $A \equiv a$, then also $kA \equiv ka$.

If k is a positive number, this is just a particular case of the proposition in the preceding article, with $A = B = C$ etc., $a = b = c$ etc. If k is negative, $-k$ will be positive, so $-kA \equiv -ka$, and then $kA \equiv ka$.

If $A \equiv a, B \equiv b$, then $AB \equiv ab$. For $AB \equiv Ab \equiv ba$.

8.

If there are any number of integers A, B, C etc. and as many others a, b, c etc. congruent to them, $A \equiv a, B \equiv b$ etc., the products of each set will be congruent, ABC etc. $\equiv abc$ etc.

By the preceding article, $AB \equiv ab$, and for the same reason $ABC \equiv abc$; in the same way, any number of further factors may be added.

If all the numbers A, B, C etc. are taken to be equal, and likewise the corresponding numbers a, b, c etc., we have this theorem: *If $A \equiv a$ and k is a positive integer, then $A^k \equiv a^k$.*

9.

Let X *be an algebraic function of the indeterminate x, of the form*

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

where A, B, C etc. denote any integers, and a, b, c etc. denote non-negative integers. Then, if values congruent modulo any modulus are assigned to the indeterminate x, the resulting values of the function X *will be congruent.*

Let f, g be congruent values of x. Then, by the preceding article, $f^a \equiv g^a$ and $Af^a \equiv Ag^a$, and in the same way $Bf^b \equiv Bg^b$ etc. Hence

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

It is also easy to see how to extend this theorem to functions of several indeterminates.

10.

So, if all consecutive integers are substituted for x, and the values of the function X are reduced to least residues, these will form a series in which the same terms recur after an interval of m terms (where m denotes the modulus); in other words, the series will be formed from a *period* of m terms repeated infinitely often. Let, for example, $\text{X} = x^3 - 8x + 6$ and $m = 5$; then, for $x = 0, 1, 2, 3$ etc., the values of X yield the least positive residues $1, 4, 3, 4, 3, 1, 4$ etc., where the first five, $1, 4, 3, 4, 3$, repeat indefinitely. And if the series is continued backwards, that is, negative values are assigned to x, the same period appears with the order of its terms reversed. This makes it clear that no terms other than those in this period can occur anywhere in the series.

11.

In this example, then, X can be neither $\equiv 0$ nor $\equiv 2$ (mod. 5), much less $= 0$ or $= 2$. It follows that the equations $x^3 - 8x + 6 = 0$ and $x^3 - 8x + 4 = 0$ cannot be solved by integers and consequently, as is well known, cannot be solved by rational numbers. In general it is evident that the equation $\text{X} = 0$, where X is a function of the unknown x, of the form

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

with A, B, C etc. integers and n a positive integer (a form to which, as is known, all algebraic equations can be reduced), has no rational root if the congruence $\text{X} \equiv 0$ cannot be satisfied modulo some modulus. But this criterion, which has arisen naturally here, will be treated more fully in Sect. VIII. This example can certainly give at least some idea of the usefulness of these investigations.

Some applications.

12.

Many things usually taught in arithmetic books rest on the theorems given in this chapter, for example the rules for testing whether a proposed number is divisible by 9, 11, or other numbers. *Modulo* 9 all powers of the number 10 are congruent to one. Thus, if the proposed number has the form $a + 10b + 100c +$ etc., it will give the same least residue modulo 9 as $a + b + c +$ etc. So, if the individual digits of a number written in decimal notation are added without regard to the positions they occupy, this sum and the proposed number give the same least residues. So the given number is divisible by 9 if the sum is divisible by 9, and conversely. The same also holds for the divisor 3. Since, *modulo* 11, $100 \equiv 1$, we have in general $10^{2k} \equiv 1$. $10^{2k+1} \equiv 10 \equiv -1$, and a number of the form $a + 10b + 100c +$ etc. gives the same least residue modulo 11 as $a - b + c$ etc.; the familiar rule follows at once. All similar rules are readily deduced from the same principle.

The preceding results also explain the rules usually recommended for checking arithmetic operations. When other numbers are to be obtained from given numbers by addition, subtraction, multiplication, or raising to powers, the given numbers are replaced by their least residues modulo an arbitrary modulus (usually 9 or 11, since in our decimal system residues for these moduli can be found so easily, as we have just shown). The numbers arising from this must be congruent to those derived from the proposed numbers; if they are not, we conclude that an error has crept into the calculation.

But these and similar matters are well known, so there is no need to spend more time on them.

SECTION TWO

ON

CONGRUENCES OF THE FIRST DEGREE.

Preliminary theorems on prime numbers, factors, etc.

13.

THEOREM. *The product of two positive numbers smaller than a given prime number is not divisible by that prime.*

Let p be prime, and a positive and $< p$: then there will be no positive number b smaller than p such that $ab \equiv 0 \pmod{p}$.

Proof. If anyone denies this, let us suppose that there are numbers b, c, d etc., all $< p$, such that $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$ etc. (mod. p). Let b be the smallest of all, so that all numbers smaller than b lack this property. Clearly $b > 1$: for if $b = 1$, we would have $ab = a < p$ (*hyp.*), so it would not be divisible by p. So p, being prime, cannot be divided by b, but will fall between the two nearest multiples of b, mb and $(m+1)b$. Let $p - mb = b'$; then b' will be a positive number and $< b$. Now, since we have supposed that $ab \equiv 0 \pmod{p}$, we also have $mab \equiv 0$ (art. 7), and so, subtracting this from $ap \equiv 0$, we obtain $a(p - mb) = ab' \equiv 0$; that is, b' must be included among the numbers b, c, d etc., although it is smaller than the least of them, b. *Q. E. A.*

14.

If neither a nor b can be divided by the prime number p: their product ab likewise cannot be divided by p.

Let the least positive residues of the numbers a, b, with respect to the modulus p, be α, β, neither of which will be 0 (*hyp.*) Now if $ab \equiv 0 \pmod{p}$, then, because $ab \equiv \alpha\beta$, we would also have $\alpha\beta \equiv 0$, which is incompatible with the preceding theorem.

A proof of this theorem was already given by Euclid, *El.* VII. 32. Nevertheless, we did not wish to omit it, both because several more recent writers have either passed off vague reasoning as a proof or omitted the theorem altogether, and because this simpler case makes it easier to understand the method used here, which we will use later to resolve much deeper matters.

15.

If none of the numbers a, b, c, d etc. can be divided by the prime number p, their product abcd etc. likewise cannot be divided by p.

By the preceding article, ab cannot be divided by p; therefore neither can abc; hence neither can $abcd$ etc.

16.

THEOREM. *Any composite number can be decomposed into prime factors in only one way.*

Proof. That every composite number can be decomposed into prime factors is known from the elements, but it is generally, and improperly, assumed without saying so that this cannot be done in several different ways. Let us suppose that a composite number A, which is $= a^\alpha b^\beta c^\gamma$ etc., where a, b, c etc. denote distinct prime numbers, can be decomposed into prime factors in yet another way. First, it is evident that no primes other than a, b, c etc. can enter this second system of factors, since any other prime cannot divide the number A composed of these. Likewise, none of the primes a, b, c etc. can be absent from this second system of factors, since otherwise it would not divide A (preceding art.). Thus these two decompositions into factors can differ only in that some prime occurs more often in one than in the other. Let p be such a prime, occurring m times in one decomposition, but n times in the other, and let $m > n$: now remove the factor p from each system n times, so that in one it still remains $m - n$ times, while from the other it has entirely disappeared. That is, there are two decompositions of the number $\frac{A}{p^n}$ into factors, one of which is wholly free of the factor p, while the other contains it $m - n$ times, contrary to what we have just proved.

17.

If, therefore, a composite number A is the product of B, C, D etc., it is clear that among the prime factors of the numbers B, C, D etc. there can be none except those that are also among the factors of the number A, and that each of these factors must occur in B, C, D etc., taken together, as often as in A. From this we obtain a criterion for whether the number B divides another number A or not. It will do so if B contains neither other prime factors nor any one of them more often than A; if either of these conditions fails, B will not divide A.

It can easily be derived from this, with the aid of counting combinations, that if $A = a^\alpha b^\beta c^\gamma$ etc., where, as above, a, b, c etc. denote distinct prime numbers: A has

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

distinct divisors, including 1 and A.

18.

If, then, $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\kappa l^\lambda m^\mu$ etc., and the primes a, b, c etc., k, l, m etc. are all distinct, it is clear that A and K have no common divisor except 1, or are coprime.

Given several numbers A, B, C etc., their *greatest common divisor* is determined as follows. Decompose them all into their prime factors, and select from these those that are common to all the numbers A, B, C etc. (if there are no such factors, no divisor will be common to all). Then record how often each of these prime factors is contained in each of A, B, C etc., or *what exponent* each has in the individual numbers A, B, C etc. Finally, assign to each prime factor the least of all the exponents it has in A, B, C etc., and form their product, which will be the common measure sought.

But when the *least common multiple* of the numbers A, B, C etc. is desired, proceed as follows. Collect all the primes that divide any one of the numbers A, B, C etc., assign to each the greatest of all the exponents it has in the numbers A, B, C etc., and thus form the product of them all, which will be the multiple sought.

Example. Let $A = 504 = 2^3 3^2 7$; $B = 2880 = 2^6 3^2 5$; $C = 864 = 2^5 3^3$. To find the greatest common divisor we have the prime factors $2, 3$, to which the exponents $3, 2$ are to be assigned; hence the result is $= 2^3 3^2 = 72$; but the least common multiple will be $2^6 3^3 5.7 = 60480$.

We omit the proofs because they are easy. Moreover, how these problems are to be solved when the resolution of the numbers A, B, C etc. into factors is not given is known from the elements.

19.

If the numbers a, b, c etc. are coprime to another number k, their product abc etc. is also coprime to k.

For since none of the numbers a, b, c etc. has a prime factor in common with k, and the product *abc* etc. cannot have prime factors other than those that are factors of one of the numbers a, b, c etc., the product *abc* etc. will likewise have no prime factor in common with k. So, by the preceding article, k is coprime to *abc* etc.

If the numbers a, b, c etc. are pairwise coprime, and each divides another number k: their product will also divide the number k.

This follows just as easily from arts. 17, 18. For let any prime divisor of the product *abc* etc. be p, occurring in it π times, and it is clear that one of the numbers a, b, c etc. must contain this same divisor π times. Therefore k also, which this number divides, contains π copies of the divisor p. The same holds for the remaining divisors of the product *abc* etc.

So *if two numbers m, n are congruent with respect to several moduli a, b, c etc. that are pairwise coprime, they will also be congruent with respect to their product.* For since $m - n$ is divisible by each of a, b, c etc., it can also be divided by their product.

Finally, *if a is coprime to b and ak is divisible by b, then ak will also be divisible by b.* For since ak is divisible both by a and by b, it can also be divided by ab; that is, $\frac{ak}{ab} = \frac{k}{b}$ will be an integer.

20.

When $A = a^\alpha b^\beta c^\gamma$ etc., where a, b, c etc. denote distinct prime numbers, is some power, say $= k^n$: all the exponents α, β, γ etc. will be divisible by n.

For the number k contains no prime factors other than a, b, c etc. Let it contain the factor a exactly α' times; then k^n, or A, will contain this factor $n\alpha'$ times; so $n\alpha' = \alpha$, and $\frac{\alpha}{n}$ is an integer. Similarly, $\frac{\beta}{n}$ etc. are shown to be integers.

21.

If a, b, c etc. are pairwise coprime, and their product abc etc. is a power, say $= k^n$, then each of the numbers a, b, c etc. is a power of the same kind.

Let $a = l^\lambda m^\mu p^\pi$ etc., where l, m, p etc. are distinct prime numbers. By *hypothesis*, none of these is a factor of b, c etc. So the product abc etc. contains the factor l λ times, the factor m μ times, etc. It follows from the *preceding article* that λ, μ, π etc. are divisible by n, and so

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

is an integer. The same holds for the remaining numbers b, c etc.

These facts about prime numbers were needed first; we now turn to matters more directly connected with our aim.

22.

If the numbers a, b, both divisible by a number k, are congruent modulo a number m coprime to k, then $\frac{a}{k}$ and $\frac{b}{k}$ are congruent modulo the same number.

For $a - b$ is clearly divisible by k, and also by m (*by hypothesis*). So, by *Article 19*, $\frac{a-b}{k}$ is divisible by m, that is, $\frac{a}{k} \equiv \frac{b}{k}$ (mod. m).

If, with the other conditions unchanged, m and k have greatest common divisor e, then $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$). For $\frac{k}{e}$ and $\frac{m}{e}$ are coprime. Now $a - b$ is divisible by both k and m, so $\frac{a-b}{e}$ is divisible by both $\frac{k}{e}$ and $\frac{m}{e}$, and therefore by $\frac{km}{ee}$. In other words, $\frac{a-b}{k}$ is divisible by $\frac{m}{e}$, or $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$).

23.

If a is coprime to m, and e, f are incongruent modulo m, then ae, af are also incongruent modulo m.

This is simply the converse of the theorem in the preceding article.

It follows that, if a is multiplied by every integer from 0 to $m-1$ and the products are reduced to their least residues modulo m, all these residues are distinct. None of these residues is $> m$, and there are m of them, just as many as the numbers from 0 to $m - 1$. So none of these numbers can be missing from the residues.

24.

The expression $ax + b$, where a, b are given numbers and x is an indeterminate or variable number, *can be made congruent to any given number modulo a number m coprime to a.*

Let c be the number to which the expression is to be congruent, and let the least positive residue of $c - b$ modulo m be e. By the preceding article, there must be a value of $x < m$ for which the least residue of the product ax modulo m is e. Call this value v. Then $av \equiv e \equiv c - b$, so $av + b \equiv c$ (mod. m). *Q. E. F.*

25.

By analogy with equations, we call an expression that states that two quantities are congruent a *congruence*. If it contains an unknown, we say that it is *solved* when a value of the unknown satisfying the congruence has been found (a *root*). This also explains what is meant by a *solvable congruence and an unsolvable congruence*. Finally, we can readily see that distinctions similar to those for equations apply here.

Examples of *transcendental* congruences will occur below. *Algebraic* congruences are divided into those of the first, second and higher *degrees*, according to the highest exponent of the unknown. We can also consider several congruences containing several unknowns, and investigate their *elimination*.

Solving congruences of the first degree.

26.

So, by Article 24, the congruence of the first degree $ax + b \equiv c$ is always solvable when the modulus is coprime to a. If v is a suitable value of x, or a root of the congruence, then clearly every number congruent to v modulo the modulus of the given congruence is also a root (Article 9). It is just as easy to see that every root must be congruent to v: if t is another root, then $av + b \equiv at + b$, so $av \equiv at$, and therefore $v \equiv t$ (Article 22). Thus the congruence $x \equiv v \pmod{m}$ gives the complete solution of the congruence $ax + b \equiv c$.

Solutions of a congruence obtained from congruent values of x are immediately apparent, and in this respect congruent numbers are to be regarded as equivalent. We will therefore count such solutions as one and the same. Since our congruence $ax + b \equiv c$ has no other solutions, we will say that it is solvable in only one way, or that it has only one root. For *example*, the congruence $6x + 5 \equiv 13 \pmod{11}$ has no roots other than those that are $\equiv 5 \pmod{11}$. Things are different for congruences of higher degrees, and even for congruences of the first degree when the unknown is multiplied by a number that is not coprime to the modulus.

27.

We still need to say something about how to find the solution of such a congruence. First, a congruence of the form $ax+t \equiv u$, whose modulus we assume to be coprime to a, depends on the congruence $ax \equiv \pm 1$: if $x \equiv r$ satisfies the latter, then $x \equiv \pm(u-t)r$ satisfies the former. The congruence $ax \equiv \pm 1$, with its modulus denoted by b, is equivalent to the indeterminate equation $ax = by \pm 1$. How to solve this is already well known, so it will be enough to give the computational algorithm here.

If the quantities A, B, C, D, E etc. depend on $\alpha, \beta, \gamma, \delta$ etc. through the relations

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

we use the following notation for brevity:

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

Now consider the indeterminate equation $ax = by \pm 1$, where a, b are positive. We may assume that a is not $< b$. Following the familiar algorithm for finding the

*)This relation can be studied much more generally, which we may take up on another occasion. Here we add only two propositions useful in the present investigation:

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

where the upper sign is taken when the number of terms $\alpha, \beta, \gamma \ldots \lambda, \mu$ is even, and the lower sign when it is odd.

2°. The order of the numbers α, β, γ etc. can be reversed: $[\alpha, \beta, \gamma \ldots \lambda, \mu] = [\mu, \lambda \ldots . \gamma, \beta, \alpha]$.

We omit the proofs here; they are not difficult.

greatest common divisor of two numbers, form the equations by ordinary division:

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

Here α, β, γ etc. and c, d, e etc. are positive integers, and b, c, d, e decrease successively until we reach $m = \mu n + 1$, as we know must eventually happen. Then

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

and, on setting

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

we have $ax = by + 1$ when the number of terms $\alpha, \beta, \gamma \ldots . \mu, n$ is even, or $ax = by - 1$ when it is odd. *Q. E. F.*

28.

The distinguished Euler was the first to give the general solution of indeterminate equations of this kind, in *Comment. Petrop. T.* VII, *p.* 46. His method substitutes other unknowns for x, y and is now well known. The distinguished La Grange approached the matter somewhat differently. The theory of continued fractions shows that, if the fraction $\frac{b}{a}$ is converted into the continued fraction

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

and, after its last part $\frac{x}{n}$ has been removed, the result is converted back to an ordinary fraction $\frac{x}{y}$, then $ax = by \pm 1$, provided that a is coprime to b. Both methods lead to the same algorithm. La Grange's investigations appear in *Hist. de l'Ac. de Berlin Année* 1767, *p.* 175, and, together with others, in the *Supplements added to the French translation of Euler's Algebra.*

29.

The congruence $ax + t \equiv u$, whose modulus is not coprime to a, is easily reduced to the preceding case. Let the modulus be m, and let the greatest common divisor of a, m be δ. First, every value of x satisfying the congruence modulo m clearly also satisfies it modulo δ (Article 5). But we always have $ax \equiv 0$ (mod. δ), since δ divides a. So the given congruence is not solvable unless $t \equiv u$ (mod. δ), that is, unless $t - u$ is divisible by δ.

Now put $a = \delta e$, $m = \delta f$, $t - u = \delta k$; then e is coprime to f. The given congruence $\delta ex + \delta k \equiv 0$ (mod. δf) is then equivalent to $ex + k \equiv 0$ (mod. f). In other words, every value of x satisfying the latter also satisfies the former, and conversely. For $ex + k$ is clearly divisible by f whenever $\delta ex + \delta k$ is divisible by δf, and conversely. We have already shown how to solve the congruence $ex + k \equiv 0$ (mod. f). This also shows that, if v is one value of x, then $x \equiv v$ (mod. f) gives the complete solution of the given congruence.

30.

When the modulus is composite, the following method is sometimes preferable.

Let the modulus be $= mn$ and the given congruence $ax \equiv b$. First solve this congruence modulo m, and suppose that it is satisfied when $x \equiv v \pmod{\frac{m}{\delta}}$, where δ denotes the greatest common divisor of m, a. Every value of x satisfying the congruence $ax \equiv b$ modulo mn clearly also satisfies it modulo m, and so has the form $v + \frac{m}{\delta}x'$, where x' is an indeterminate number. Conversely, however, not every number of the form $v + \frac{m}{\delta}x'$ satisfies the congruence modulo mn. To determine x' so that $v + \frac{m}{\delta}x'$ is a root of the congruence $ax \equiv b \pmod{mn}$, we can solve the congruence $\frac{am}{\delta}x' + av \equiv b \pmod{mn}$, which is equivalent to $\frac{a}{\delta}x' \equiv \frac{b-av}{m} \pmod{n}$. Thus the solution of any congruence of the first degree modulo mn can be reduced to the solution of two congruences modulo m and n. If n is itself a product of two factors, the solution of the congruence modulo n similarly depends on solving two congruences whose moduli are those factors. In general, solving a congruence with any composite modulus depends on solving other congruences whose moduli are factors of that number. These factors can always be chosen to be primes, if that seems convenient.

Example. Consider the congruence $19x \equiv 1 \pmod{140}$. First solve it modulo 2, giving $x \equiv 1 \pmod{2}$. Put $x = 1 + 2x'$; then $38x' \equiv -18 \pmod{140}$, which is equivalent to $19x' \equiv -9 \pmod{70}$. If this is again solved modulo 2, we get $x' \equiv 1 \pmod{2}$. Setting $x' = 1+2x''$ gives $38x'' \equiv -28 \pmod{70}$, or $19x'' \equiv -14 \pmod{35}$. Solving this modulo 5 gives $x'' \equiv 4 \pmod{5}$, and substituting $x'' = 4 + 5x'''$ gives $95x''' \equiv -90 \pmod{35}$, or $19x''' \equiv -18 \pmod{7}$. Finally, this gives $x''' \equiv 2 \pmod{7}$, and on setting $x''' = 2 + 7x''''$ we obtain $x = 59 + 140x''''$. So $x \equiv 59 \pmod{140}$ is the complete solution of the given congruence.

31.

Just as the root of the equation $ax = b$ is expressed by $\frac{b}{a}$, we will denote any root of the congruence $ax \equiv b$ by $\frac{b}{a}$, adding the modulus to distinguish the congruence. For example, $\frac{19}{17} \pmod{12}$ denotes any number that is $\equiv 11 \pmod{12}$[*)]. In general, what precedes shows that $\frac{a}{b} \pmod{c}$ represents nothing real (or, if one prefers, something imaginary) if a, c have a common divisor that does not divide b. Except in this case, the expression $\frac{b}{a} \pmod{c}$ always has real values, and indeed infinitely many. These are all congruent modulo c when a is coprime to c, or modulo $\frac{c}{\delta}$ when δ is the greatest common divisor of c, a.

The calculation rules for these expressions are much like those for ordinary fractions. Here are a few properties that follow easily from what precedes.

1. If, modulo c, $a \equiv \alpha$, $b \equiv \beta$, then the expressions $\frac{a}{b} \pmod{c}$ and $\frac{\alpha}{\beta} \pmod{c}$ are equivalent.
2. $\frac{a\delta}{b\delta} \pmod{c\delta}$ and $\frac{a}{b} \pmod{c}$ are equivalent.
3. $\frac{ak}{bk} \pmod{c}$ and $\frac{a}{b} \pmod{c}$ are equivalent when k is coprime to c.

Many other similar propositions could be given. But they present no difficulty and are not especially needed for what follows, so we move on.

[*)] which, by analogy, can be denoted by $\frac{11}{1} \pmod{12}$.

Finding a number congruent to given residues modulo given numbers.

32.

The problem of *finding all numbers that give specified residues modulo any number of given moduli* will be very useful later, and is easily solved using what precedes. First let there be two moduli A, B, for which the number we seek, z, is to be congruent to a, b, respectively. All values of z therefore have the form $Ax + a$, where x is indeterminate but must satisfy $Ax + a \equiv b \pmod{B}$. If the greatest common divisor of A, B is δ, the complete solution of this congruence has the form $x \equiv v \pmod{\frac{B}{\delta}}$, or equivalently $x = v + \frac{kB}{\delta}$, where k is an arbitrary integer. The formula $Av + a + \frac{kAB}{\delta}$ therefore includes all values of z, that is, $z \equiv Av + a \pmod{\frac{AB}{\delta}}$ is the complete solution of the problem. If the moduli A, B are joined by a third, C, for which the desired number z is to be $\equiv c$, we clearly proceed in the same way, since the first two conditions have already been combined into one. Specifically, if the greatest common divisor of $\frac{AB}{\delta}$. and C is $= \varepsilon$, and the congruence $\frac{AB}{\delta}x + Av + a \equiv c \pmod{C}$ has solution $x \equiv w \pmod{\frac{C}{\varepsilon}}$, then the congruence $z \equiv \frac{ABw}{\delta} + Av + a \pmod{\frac{ABC}{\delta\varepsilon}}$ solves the problem completely. We proceed similarly however many moduli are given. Notice that $\frac{AB}{\delta}$, $\frac{ABC}{\delta\varepsilon}$ are the least common multiples of A, B and A, B, C, respectively. So, for any number of moduli A, B, C etc., if their least common multiple is M, the complete solution has the form $z \equiv r \pmod{M}$. If any of the auxiliary congruences is unsolvable, we must conclude that the problem is impossible. Clearly this cannot happen when all the numbers A, B, C etc. are pairwise coprime.

Example. Let A, B, C and a, b, c be $504, 35, 16$ and $17, -4, 33$. The two conditions that z be $\equiv 17 \pmod{504}$ and $\equiv -4 \pmod{35}$ are equivalent to the single condition that it be $\equiv 521 \pmod{2520}$. Combining this with $z \equiv 33 \pmod{16}$ gives $z \equiv 3041 \pmod{5040}$.

33.

When the numbers A, B, C etc. are pairwise coprime, their product is known to be their least common multiple. In that case, all the congruences $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$ etc. are clearly equivalent to the single congruence $z \equiv r \pmod{R}$, where R is the product of A, B, C etc. Conversely, the single condition $z \equiv r \pmod{R}$ can therefore be split into several. If R is factored in any way into pairwise coprime factors A, B, C etc., the conditions $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$, $z \equiv r \pmod{C}$ etc. meet the requirement in full. This observation gives us a way not only to detect immediately any impossibility in the given conditions, but also to make the calculation more convenient and orderly.

34.

As above, let the given conditions be $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$. Factor each modulus into pairwise coprime factors: A into $A'A''A'''$ etc., B into $B'B''B'''$ etc., and so on. Choose these so that the numbers A', A'' etc., B', B'' etc. are primes or powers of primes. If one of the numbers A, B, C etc. is already a prime or a power of a prime, it needs no factorization. What precedes shows that we can replace the given conditions by $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$,

$z \equiv a$ (mod. A''') etc., $z \equiv b$ (mod. B'), $z \equiv b$ (mod. B'') etc. Now, unless all the numbers A, B, C etc. are pairwise coprime, for example if A is not coprime to B, the prime divisors of A, B clearly cannot all be different. Among the factors A', A'', A''' etc., at least one must have an equal, a multiple or a divisor among B', B'', B''' etc. *First*, if $A' = B'$, the conditions $z \equiv a$ (mod. A'), $z \equiv b$ (mod. B') must be identical, that is, $a \equiv b$ (mod. A' or B'), so either can be discarded. If $a \equiv b$ (mod. A') does not hold, the problem is impossible. *Second*, if B' is a multiple of A', the condition $z \equiv a$ (mod. A') must be included in $z \equiv b$ (mod. B'). In other words, the condition $z \equiv b$ (mod. A'), which follows from the latter, must be identical to the former. So the condition $z \equiv a$ (mod. A') can be discarded unless it conflicts with the other condition, in which case the problem is impossible. After all redundant conditions have been discarded in this way, all the remaining moduli among A', A'', A''' etc., B', B'', B''' etc. are clearly pairwise coprime. We can then be sure that the problem is possible and proceed by the rules already given.

35.

Example. If, as above, we require $z \equiv 17$ (mod. 504), $\equiv -4$ (mod. 35) and $\equiv 33$ (mod. 16), these conditions can be split into $z \equiv 17$ (mod. 8), $\equiv 17$ (mod. 9), $\equiv 17$ (mod. 7), $\equiv -4$ (mod. 5), $\equiv -4$ (mod. 7), $\equiv 33$ (mod. 16). We can discard $z \equiv 17$ (mod. 8), $z \equiv 17$ (mod. 7), since the former is included in $z \equiv 33$ (mod. 16), and the latter is identical to $z \equiv -4$ (mod. 7). This leaves

$$z \equiv \begin{cases} 17 & \text{(mod. 9)} \\ -4 & \text{(mod. 5)} \\ -4 & \text{(mod. 7)} \\ 33 & \text{(mod. 16)} \end{cases} \qquad \text{so} \quad z \equiv 3041 \text{ (mod. 5040)}.$$

It is usually more convenient to recombine separately those remaining conditions that came from the same original condition, since this is easily done. For *example*, if some of the conditions $z \equiv a$ (mod. A'), $z \equiv a$ (mod. A'') etc. have been discarded, the condition reconstructed from the rest is $z \equiv a$ modulo the product of all the remaining moduli among A', A'', A''' etc. Thus, in our example, the conditions $z \equiv -4$ (mod. 5), $z \equiv -4$ (mod. 7) immediately give back the condition $z \equiv -4$ (mod. 35) from which they came. This also shows that, as far as shortening the calculation is concerned, it does matter which redundant conditions we discard. But explaining this and other practical devices, which are learned much more easily through use than through rules, is not our purpose here.

36.

When all the moduli A, B, C, D etc. are pairwise coprime, the following method is often preferable. Find a number α that is congruent to unity modulo A and to zero modulo the product of the other moduli. Equivalently, let α be any value (usually the *least*) of the expression $\frac{1}{BCD \text{ etc.}}$ (mod. A), multiplied by BCD etc. (see Article 32). Similarly, let $\beta \equiv 1$ (mod. B) and $\equiv 0$ (mod. ACD etc.), $\gamma \equiv 1$ (mod. C) and $\equiv 0$ (mod. ABD etc.), etc. Then, if we seek a number z congruent modulo A, B, C, D etc. to a, b, c, d etc., respectively, we can put

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

For clearly $\alpha a \equiv a$ (mod. A.), whereas the remaining terms $\beta b, \gamma c$ etc. are all $\equiv 0$ (mod. A), so $z \equiv a$ (mod. A). The proof is similar for the other moduli. This solution is preferable to the earlier one when several such problems must be solved with the same moduli A, B, C etc., since the numbers α, β, γ etc. then have constant values. This occurs in the chronological problem of finding which year in the Julian Period has a given indiction, golden number and solar cycle. Here $A = 15$, $B = 19$, $C = 28$. Since the value of the expression $\frac{1}{19.28}$ (mod. 15), or $\frac{1}{532}$ (mod. 15), is 13, we have $\alpha = 6916$. Similarly, for β we find 4200, and for γ, 4845. The desired number is therefore the least residue of $6916a + 4200b + 4845c$, where a denotes the indiction, b the golden number and c the solar cycle.

Linear congruences with several unknowns.

37.

This is enough about congruences of the first degree with one unknown. We still have to consider congruences involving several unknowns. A fully rigorous treatment of every detail would require a lengthy account, and our purpose here is to give only what seems most worth attention, rather than to exhaust the subject. So we restrict the investigation to a few observations, leaving a fuller treatment for another occasion.

1) As with equations, we see that here too there must be as many congruences as unknowns to be determined.

2) So let the given congruences be

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

as many in number as the unknowns x, y, z etc.

Now determine numbers ξ, ξ', ξ'' etc. such that

$$\begin{array}{l} b\xi + b'\xi' + b''\xi'' + \text{etc.} = 0 \\ c\xi + c'\xi' + c''\xi'' + \text{etc.} = 0 \\ \qquad \text{etc.} \end{array}$$

and so that they are all integers with no common factor. The theory of linear equations shows that this is possible. Similarly, determine v, v', v'' etc., ζ, ζ', ζ'' etc., and so on, such that

$$\begin{array}{l} av + a'v' + a''v'' + \text{etc.} = 0 \\ cv + c'v' + c''v'' + \text{etc.} = 0 \\ \qquad \text{etc.} \end{array}$$

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

3) Clearly, if the congruences A, A', A'' etc. are multiplied by ξ, ξ', ξ'' etc., then by v, v', v'', etc., and so on, and the results are added, we obtain the congruences

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

which we write for brevity as

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

4) We must now distinguish several cases.

First, when all the coefficients of the unknowns, $\Sigma(a\xi), \Sigma(av)$ etc., are coprime to the modulus m, these congruences can be solved by the rules already given, and the complete solution of the problem is expressed by congruences of the form $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$ etc.[*)] For *example*, consider the congruences

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

We find $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, giving $-15x \equiv -26$, so $x \equiv 6 \pmod{8}$. Similarly, we find $15y \equiv -4$, $15z \equiv 1$, and therefore $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5) *Second*, suppose not all the coefficients $\Sigma(a\xi), \Sigma(bv)$ etc. are coprime to the modulus. Let α, β, γ etc. be the greatest common divisors of m with $\Sigma(a\xi), \Sigma(bv), \Sigma(c\zeta)$ etc., respectively. The problem is clearly impossible unless these divide $\Sigma(f\xi), \Sigma(fv), \Sigma(f\zeta)$ etc., respectively. If these conditions hold, the congruences in (3) are completely solved by $x \equiv p \pmod{\frac{m}{\alpha}}$, $y \equiv q \pmod{\frac{m}{\beta}}$, $z \equiv r \pmod{\frac{m}{\gamma}}$ etc. Or, if one prefers, there are α distinct values of x (that is, incongruent modulo m, namely $p, p + \frac{m}{\alpha} \ldots p + \frac{(\alpha-1)m}{\alpha}$), β distinct values of y etc. satisfying those congruences. Clearly every solution of the given congruences, if there are any at all, will be found among these. But we cannot reverse this conclusion. In general, not every combination of all α values of x with all values of y and all values of z etc. satisfies the problem. Only some combinations do, and their connection can be expressed by one or more congruences serving as conditions. A complete solution of this problem is not needed for what follows, so we will not pursue it further here, but will be content to give some idea of it through an example.

Let the given congruences be

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

[*)] This conclusion needs a proof, which we omit here. Strictly speaking, our analysis shows only that the given congruences cannot be solved by other values of the unknowns x, y etc.; it does not show that these values satisfy them. There might be no solution at all. A similar error in reasoning is often made in accounts of linear equations.

Here ξ, ξ', ξ'', v, v', v'', ζ, ζ', ζ'' are respectively $= 1, -2, 1,\ 1, 1, -1,\ -13, 22, -1$, giving $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. These give four values of x, namely $\equiv 2, 5, 8.\ 11$, one value of y, namely $\equiv 11$, and four values of z, namely $\equiv 0, 3, 6, 9 \pmod{12}$. To find which combinations of values of x and z are allowed, we substitute for x, y, z in the given congruences, respectively, $2 + 3t$, 11, $3u$. They become

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

which are easily seen to be equivalent to

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

The first clearly requires $u \equiv t + 1 \pmod{4}$. Substituting this value in the other congruences shows that they too are satisfied. So the values of x, namely $2, 5, 8, 11$ (obtained by setting $t \equiv 0.\ 1, 2, 3$), must be combined with the values of z, namely $z \equiv 3, 6, 9, 0$, respectively. Thus there are four solutions in all:

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

* * *

These investigations have achieved the aim of this section. We add a few more propositions based on similar principles, which we will often need later.

Various theorems.

38.

PROBLEM. *Find how many positive numbers are smaller than a given positive number A and coprime to it.*

For brevity, let the symbol ϕ, placed before a given number, denote the number of positive numbers coprime to it and smaller than it. We therefore seek ϕA.

I. When A is prime, clearly all numbers from 1 to $A-1$ are coprime to A. So in this case

$$\phi A = A - 1$$

II. When A is a power of a prime, say $= p^m$, none of the numbers divisible by p are coprime to A, whereas all the others are. So, from the $p^m - 1$ numbers, we must discard $p, 2p, 3p....(p^{m-1}-1)p$. This leaves $p^m - 1 - (p^{m-1}-1)$, or $p^{m-1}(p-1)$. Thus

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

III. The remaining cases are easily reduced to these by the following proposition: *If A is resolved into pairwise coprime factors M, N, P etc., then*

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

The proof is as follows. Let the numbers coprime to M and smaller than M be $m, m'.m''$ etc., so their number is $= \phi M$. Similarly, let the numbers coprime to N, P etc., respectively, and smaller than them be n, n', n'' etc., p, p', p'' etc., whose numbers are $\phi N, \phi P$ etc. Every number coprime to the product A is also coprime to each of its factors M, N, P etc., and conversely (Article 19). Also, every number congruent to one of m, m', m'' etc. modulo M is coprime to M, and conversely; the same holds for N, P etc. So the question becomes: how many numbers below A are congruent, modulo M, to one of m, m', m'' etc., modulo N, to one of n, n', n'' etc., and so on? By Article 32, all numbers giving specified residues modulo each of M, N, P etc. are congruent modulo their product A. So below A there is just one number congruent to given residues modulo each of M, N, P etc. The number we seek is therefore the number of combinations of each of m, m', m'' with each of n, n', n'' and each of p, p', p'' etc. The theory of combinations shows that this number is $= \phi M . \phi N . \phi P$ etc. *Q. E. D.*

IV. It is now easy to see how to apply this to the case in question. Resolve A into its prime factors, or write it in the form $a^\alpha b^\beta c^\gamma$ etc., where a, b, c etc. are distinct primes. Then

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

or, more neatly,

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

Example. Let $A = 60 = 2^2.3.5$, so that $\phi A = \frac{1}{2}.\frac{2}{3}.\frac{4}{5}.60 = 16$. The numbers coprime to 60 are $1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53. 59$.

The first solution of this problem appears in the distinguished Euler's paper *theoremata arithmetica nova methodo demonstrata*, Comm. nov. Ac. Petrop. VIII, p. 74. The proof was later repeated in another paper, *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII, p. 17.

39.

If we define the symbol ϕ so that ϕA gives the number of numbers coprime to A and *not greater than* A, then clearly $\phi 1$ is no longer $= 0$, but $= 1$. All other cases remain unchanged. Adopting this definition, we have the following theorem.

If a, a', a'' etc. are all the divisors of A, including unity and A itself, then

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

Example. Let $A = 30$; then $\phi 1 + \phi 2 + \phi 3 + \phi 5 + \phi 6 + \phi 10 + \phi 15 + \phi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Proof. Multiply all the numbers coprime to a and not greater than a by $\frac{A}{a}$, and likewise all those coprime to a' by $\frac{A}{a'}$, and so on. This gives $\phi a + \phi a' + \phi a''+$ etc. numbers, none greater than A. Now

1) these numbers are all distinct. Those generated from the *same* divisor of A are clearly distinct. If equal numbers were generated from different divisors M, N and numbers μ, ν coprime to them, respectively, that is, if $\frac{A}{M}\mu = \frac{A}{N}\nu$, then $\mu N = \nu M$. We may assume $M > N$. Since M is coprime to μ and divides μN, it also divides N: the greater divides the smaller. *Q. E. A.*

2) These numbers include every one of $1, 2, 3....A$. Let any number not exceeding A be t, and let the greatest common divisor of A, t be δ. Then $\frac{A}{\delta}$ is a divisor of A coprime to $\frac{t}{\delta}$. Clearly the number t is among those generated from the divisor $\frac{A}{\delta}$.

3) So the number of these numbers is A, and therefore

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

40.

If the greatest common divisor of A, B, C, D etc. is $= \mu$, numbers a, b, c, d etc. can be found such that

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

Proof. First consider just two numbers A, B, with greatest common divisor $= \lambda$. The congruence $Ax \equiv \lambda \pmod{B}$ is then solvable (Article 30). Let a root be $\equiv \alpha$, and put $\frac{\lambda - A\alpha}{B} = \beta$. Then $\alpha A + \beta B = \lambda$, as required.

On adding a third number C, let the greatest common divisor of the numbers λ, C be $= \lambda'$. This is also the greatest common divisor of A, B, C[*)]. Find numbers k, γ such that $k\lambda + \gamma C = \lambda'$; then $k\alpha A + k\beta B + \gamma C = \lambda'$.

[*)] For λ' clearly divides all of A, B, C. If it were not the *greatest* common divisor, that divisor would be greater than λ'. But, since this greatest common divisor divides A, B, C, it also divides $k\alpha A + k\beta B + \gamma C$, that is, λ': the greater divides the smaller. *Q. E. A.* — This follows even more easily from Article 18.

On adding a fourth number D, let the greatest common divisor of λ', D, which is easily seen to be also the greatest common divisor of A, B, C, D, be $= \lambda''$, and put $k'\lambda' + \delta D = \lambda''$. Then $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

We can proceed in the same way however many other numbers are added.

So, if the numbers A, B, C, D etc. have no common divisor, we can clearly obtain

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

41.

If p is prime and there are p objects, any number of which may be equal, provided they are not all equal, then the number of permutations of these objects is divisible by p.

Example. The five objects A, A, A, B, B can be arranged in ten different ways.

This theorem is easily proved from the familiar theory of permutations. Suppose there are a equal objects $= A$, then b equal objects $= B$, then c equal objects $= C$, and so on, where any of the numbers a, b, c etc. may also be unity, so that

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

The number of permutations is

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

The numerator of this fraction is clearly divisible by the denominator, since the number of permutations must be an integer. The numerator is divisible by p, whereas the denominator, being composed of factors smaller than p, is not divisible by p (Article 15). So the number of permutations is divisible by p (Article 19).

We hope, though, that some readers will also enjoy the following proof.

Call two permutations *similar* when the order of their objects differs only in this way: the object occupying the first position in one occupies another position in the other, while the remaining objects follow in the same order, and the object that was first follows the one that was last[*)]. Thus, in our example, the permutations $ABAAB$ and $ABABA$ are similar, since the objects in the first, second, etc. positions of the former occur in the third, fourth, etc. positions of the latter, in the same order.

Each permutation contains p objects, so we can obtain $p-1$ similar permutations by moving the object that was first to the second, third, etc. positions. If no two of these can be identical, then the total number of permutations is clearly divisible by p, since it is p times the number of mutually dissimilar permutations. So suppose that two permutations

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

obtained from each other by shifting the terms are identical, that is, $P = V$ etc. Let the term P, which is first in the former, occupy position $n+1$ in the latter. Then, in

[*)] If we imagine similar permutations written around a circle, with the last object next to the first, they do not differ at all, since no position can be called first or last.

the latter sequence, the term in position $n+1$ equals the first, that in position $n+2$ equals the second, and so on. Thus the term in position $2n+1$ again equals the first, and the same holds for $3n+1$ etc. In general, the term in position $kn+m$ equals that in position m. Here, if $kn+m$ exceeds p, either the sequence $V \ldots YZPQ \ldots T$ is to be repeated from the beginning, or we subtract from $kn+m$ the nearest smaller multiple of p. If we now choose k so that $kn \equiv 1 \pmod{p}$, which is possible because p is prime, it follows in general that the term in position m equals that in position $m+1$. Thus every term equals the next, *that is*, all terms are equal, contrary to the hypothesis.

42.

If the coefficients $A, B, C \ldots . N$, $a, b, c \ldots . n$ of two functions of the form

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

are all rational, but not all integers, and the product of (P) and (Q) is

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

then its coefficients $\mathfrak{A}, \mathfrak{B} \ldots . \mathfrak{Z}$ cannot all be integers.

Proof. Express all fractions among the coefficients A, B etc., a, b etc. in lowest terms, and choose any prime p dividing one or more of their denominators. We may assume that p divides the denominator of a fractional coefficient in (P). If (Q) is divided by p, then $\frac{(Q)}{p}$ clearly also has at least one fractional coefficient whose denominator contains the factor p, namely the first coefficient $\frac{1}{p}$.

There is clearly a fractional term in (P) whose denominator contains a *higher* power of p than the denominators of all preceding fractional terms, and a power *no lower* than the denominators of all following terms. Let this term be $= Gx^g$, and let the number of factors of p in the denominator of G be $= t$. There is a similar term in $\frac{(Q)}{p}$; let it be $= \Gamma x^\gamma$, and let the number of factors of p in the denominator of Γ be $= \tau$. Clearly $t + \tau$ is at least $= 2$. With these preparations, the term $x^{g+\gamma}$ in the product of (P) and (Q) has a fractional coefficient whose denominator contains $t + \tau - 1$ factors of p. The proof is as follows.

In (P), let the terms preceding Gx^g be $'Gx^{g+1}$, $''Gx^{g+2}$ etc., and those following it $G'x^{g-1}$, $G''x^{g-2}$ etc. Similarly, in $\frac{(Q)}{p}$, let Γx^γ be preceded by $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$ etc. and followed by $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$ etc. Then, in the product of (P), $\frac{(Q)}{p}$, the coefficient of $x^{g+\gamma}$ is

$$= G\Gamma + {}'G\Gamma' + {}''G\Gamma'' + \text{etc.}$$
$$+ {}'\Gamma G' + {}''\Gamma G'' + \text{etc.}$$

The term $G\Gamma$ is a fraction whose denominator, in lowest terms, contains $t + \tau$ factors of p. If fractional, the other terms have fewer factors of p in their denominators, since each is a product of two factors, one involving no more than t and the other fewer than τ factors of p, or one no more than τ and the other fewer than t. Thus $G\Gamma$ has the form $\frac{e}{fp^{t+\tau}}$, and the sum of the remaining terms has the form $\frac{e'}{f'p^{t+\tau-\delta}}$,

where δ is positive and e, f, f' are free of the factor p. Their total sum is therefore $= \frac{ef'+e'fp^{\delta}}{ff'p^{t+\tau}}$. Its numerator is not divisible by p, so no reduction can leave fewer than $t+\tau$ such factors in the denominator. The coefficient of $x^{g+\gamma}$ in the product of $(P), (Q)$ is consequently

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

that is, a fraction whose denominator contains $t+\tau-1$ factors of p.
Q. E. D.

43.

A congruence of degree m

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

whose modulus is a prime p not dividing A cannot be solved in more than m different ways, or have more than m roots incongruent modulo p (see Articles 25, 26).

If anyone denies this, suppose that there are congruences of various degrees m, n etc. having more than m, n etc. roots, and let the smallest such degree be m, so that all such congruences of lower degrees satisfy our theorem. Since it has already been proved for the first degree (Article 26), m must be $= 2$ or greater. The congruence

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

therefore has at least $m+1$ roots, say $x \equiv \alpha, x \equiv \beta, x \equiv \gamma$ etc. We may suppose all the numbers α, β, γ etc. positive and smaller than p, with α the least. Substitute for x the expression $y + \alpha$, so that the given congruence becomes

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

Clearly this is satisfied by setting $y \equiv 0$, or $\equiv \beta - \alpha$, or $\equiv \gamma - \alpha$, etc. All these roots are distinct, and their number is $= m+1$. Since $y \equiv 0$ is a root, N' must be divisible by p. So the expression

$$y(A'y^{m-1} + B'y^{m-2} + \text{etc.} + M') \text{ is } \equiv 0 \pmod{p},$$

when y is assigned one of the m values $\beta - \alpha, \gamma - \alpha$ etc., all of which are > 0 and $< p$. In each of these cases, therefore, we also have

$$A'y^{m-1} + B'y^{m-2} + \text{etc.} + M' \text{ is } \equiv 0 \text{ (Article 22)}$$

that is, the congruence $A'y^{m-1} + B'y^{m-2} + \text{etc.} + M' \equiv 0$
of degree $m-1$ has m roots and so contradicts our theorem. For A' is clearly $= A$ and therefore not divisible by p, as required. Yet we assumed that every congruence of degree lower than m satisfies the theorem. *Q. E. A.*

44.

Although we assumed here that the modulus p does not divide the coefficient of the highest term, the theorem is not restricted to this case. If the first coefficient, or

even some of the following ones, were divisible by p, these terms could be discarded, eventually lowering the degree of the congruence until its first coefficient was no longer divisible by p. This holds unless all the coefficients are divisible by p, in which case the congruence is an identity and the unknown is entirely unrestricted.

The distinguished La Grange was the first to state and prove this theorem (*Mém. de l'Ac. de Berlin, Année* 1768, *p.* 192). It also appears in the distinguished Le Gendre's paper *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris* 1785, *p.* 466. The distinguished Euler proved in *Nov. Comm. Ac. Petr.* XVIII, *p.* 93 that the congruence $x^n - 1 \equiv 0$ cannot have more than n distinct roots. Although this is a special case, the method used by this great man is easily adapted to all congruences. He had previously dealt with an even more restricted case in *Comm. nov. Ac. Petr.* V, *p.* 6, but that method cannot be applied generally. In Section VIII below we will prove the theorem in yet another way. However different all these methods may appear at first, those familiar with the subject who compare them will easily see that they all rest on the same principle. Since we consider this theorem here only as a lemma, and a full treatment does not belong here, we will not discuss composite moduli separately.

SECTION THREE

ON

RESIDUES OF POWERS.

The residues of the terms of a geometric progression beginning with unity form a periodic sequence.

45.

THEOREM. *In every geometric progression* $1, a, aa, a^3$ *etc., besides the first term* 1*, there is another term* a^t *congruent to unity modulo a number* p *coprime to* a*, with exponent* $t < p$*.*

Proof. Since the modulus p is coprime to a, and therefore to every power of a, no term of the progression is $\equiv 0 \pmod{p}$. Each is congruent to one of the numbers $1, 2, 3....p-1$. There are $p-1$ such numbers, so if more than $p-1$ terms of the progression are considered, they cannot all have distinct least residues. Thus at least two of the terms $1, a, aa, a^3....a^{p-1}$ are congruent. Let $a^m \equiv a^n$, with $m > n$. Dividing by a^n gives $a^{m-n} \equiv 1$ (Article 22), where $m - n < p$ and > 0.
Q. E. D.

Example. In the progression $2, 4, 8$ etc., the first term congruent to unity modulo 13 is $2^{12} = 4096$. But modulo 23, the same progression gives $2^{11} = 2048 \equiv 1$. Similarly, the sixth power of 5, namely 15625, is congruent to unity modulo 7, and the fifth power, 3125, modulo 11. So in some cases a power with exponent less than $p-1$ is congruent to unity; in others we must go as far as the power with exponent $p-1$.

46.

If the progression is continued beyond a term congruent to unity, the residues from the beginning occur again. If $a^t \equiv 1$, then $a^{t+1} \equiv a, a^{t+2} \equiv aa$ etc., until the term a^{2t} is reached. Its least residue is again $\equiv 1$, and it starts the *period* of residues once more. Thus there is a period containing t residues, which always repeats from the beginning as soon as it ends. No residues other than those in this period occur anywhere in the progression. In general, $a^{mt} \equiv 1$ and $a^{mt+n} \equiv a^n$, which in our notation is expressed as follows:

$$\textit{If } r \equiv \rho \ (mod.\, t), \quad \textit{then} \quad a^r \equiv a^\rho \ (mod.\, p).$$

47.

This theorem gives a shortcut for finding residues of powers, however large their exponents, once a power congruent to unity is known. For *example*, to find the residue obtained by dividing 3^{1000} by 13, we have, since $3^3 \equiv 1 \pmod{13}$, $t \equiv 3$. Since $1000 \equiv 1 \pmod{3}$, it follows that $3^{1000} \equiv 3 \pmod{13}$.

48.

If a^t is the *lowest* power congruent to unity, apart from $a^0 = 1$, which we leave out of consideration here, the t terms making up the period of residues are all distinct, as the proof of Article 45 readily shows. We can then reverse the proposition of Article 46: if $a^m \equiv a^n \pmod{p}$, then $m \equiv n \pmod{t}$. For if m, n were incongruent modulo t, their least residues μ, ν would differ. But $a^\mu \equiv a^m, a^\nu \equiv a^n$, so $a^\mu \equiv a^\nu$: *that is*, the powers below a^t would not all be incongruent, contrary to the hypothesis.

So, if $a^k \equiv 1 \pmod{p}$, then $k \equiv 0 \pmod{t}$, *that is*, k is divisible by t.

So far we have considered any moduli, provided they are coprime to a. We will now consider prime moduli separately, and later build a more general investigation on this foundation.

First we consider moduli that are prime numbers.

49.

THEOREM. *If p is prime and does not divide a, and a^t is the lowest power of a congruent to unity modulo p, then the exponent t is either $= p-1$ or a divisor of that number.*

Compare the examples in Article 45.

Proof. We have already shown that t is either $= p-1$ or $< p-1$. It remains to prove that in the latter case t always divides $p-1$.

I. Take the least positive residues of all the terms $1, a, aa....a^{t-1}$ and denote them by $\alpha, \alpha', \alpha''$ etc., so that $\alpha = 1, \alpha' \equiv a, \alpha'' \equiv aa$ etc. They are clearly all distinct: if two terms a^m, a^n gave the same residue, then, assuming $m > n$, we would have $a^{m-n} \equiv 1$ with $m - n < t$, *Q. E. A.*, since no power below a^t is congruent to unity (*by hypothesis*). All the numbers $\alpha, \alpha', \alpha''$ etc. are in the sequence $1, 2, 3...p-1$, but do not exhaust it, since $t < p-1$. Denote the collection of all $\alpha, \alpha', \alpha''$ etc. by (A). Thus (A) contains t terms.

II. Choose any number β from $1, 2, 3...p-1$ that is absent from (A). Multiply β by all of $\alpha, \alpha', \alpha''$ etc., and let the resulting least residues be β, β', β'' etc. Their number is again t. These residues are distinct both from each other and from all of $\alpha, \alpha', \alpha''$ etc. If the *first* assertion were false, we would have $\beta a^m \equiv \beta a^n$, and division by β would give $a^m \equiv a^n$, contrary to what we just proved. If the *second* were false, we would have $\beta a^m \equiv a^n$. When $m < n$, this gives $\beta \equiv a^{n-m}$, *that is*, β would be congruent to one of $\alpha, \alpha', \alpha''$ etc., contrary to the hypothesis. When $m > n$, multiplication by a^{t-m} gives $\beta a^t \equiv a^{t+n-m}$, or, since $a^t \equiv 1$, $\beta \equiv a^{t+n-m}$, the same contradiction. Denote the collection of all β, β', β'' etc., whose number is $= t$, by (B). We now have $2t$ numbers from $1, 2, 3...p-1$. If (A) and (B) include all these numbers, then $\frac{p-1}{2} = t$, and the theorem is proved.

III. If some numbers are still missing, let γ be one of them. Multiply all of $\alpha, \alpha', \alpha''$ etc. by it, and let the least residues of the products be $\gamma, \gamma', \gamma''$ etc. Denote their collection by $(C$. Then (C) contains t numbers from $1, 2, 3...p-1$, all distinct from each other and from the numbers in (A) and (B). The first two assertions are proved as in II; the third as follows. If $\gamma a^m \equiv \beta a^n$, then $\gamma \equiv \beta a^{n-m}$ or $\equiv \beta a^{t+n-m}$, according as $m < n$ or $> n$. In either case γ would be congruent to a member of (B), contrary

to the hypothesis. We thus have $3t$ numbers from $1, 2, 3...p-1$. If none are missing, $t = \frac{p-1}{3}$, and the theorem is proved.

IV. If some numbers are still missing, proceed in the same way to a fourth collection (D), and so on. Since there are only finitely many numbers $1, 2, 3....p-1$, they must eventually be exhausted. Their number is therefore a multiple of t, so t divides $p-1$. *Q. E. D.*

Fermat's theorem.

50.

Since $\frac{p-1}{t}$ is an integer, raising both sides of the congruence $a^t \equiv 1$ to the power with exponent $\frac{p-1}{t}$ gives $a^{p-1} \equiv 1$. *In other words,* $a^{p-1} - 1$ *is always divisible by* p *when* p *is prime and does not divide* a.

This theorem deserves close attention for both its elegance and its exceptional usefulness. It is usually called *Fermat's theorem*, after its discoverer; see *Fermatii Opera Mathem. Tolosae* 1679, *fol. p.* 163. He gave no proof, though he said he had one. The distinguished Euler was the first to publish a proof, in his paper *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T.* VIII[*]. It rests on expanding $(a+1)^p$. The form of the coefficients readily shows that $(a+1)^p - a^p - 1$ is always divisible by p. So $(a+1)^p - (a+1)$ is divisible by p whenever $a^p - a$ is divisible by p. Since $1^p - 1$ is always divisible by p, so is $2^p - 2$, and therefore $3^p - 3$ etc., and in general $a^p - a$. If p does not divide a, then $a^{p-1} - 1$ is also divisible by p. This is enough to show the character of the method. The distinguished Lambert gave a similar proof in *Actis Erudit.* 1769, *p.* 109. But expanding a binomial power seemed rather foreign to number theory, so the distinguished Euler sought another proof. It appears in *Comment. nov. Petr. T.* VII, *p.* 70, and entirely agrees with the proof we gave in the preceding article. We will meet some further proofs later. Here we may add one based on principles similar to those of Euler's first proof. The following proposition, of which our theorem is only a special case, will also be used in other investigations below.

51.

The polynomial $a + b + c +$ *etc., raised to the power with exponent* p*, is, modulo* p*,*

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

provided that p *is prime.*

Proof. The power with exponent p of the polynomial $a + b + c +$ etc. consists of terms of the form $\varkappa a^\alpha b^\beta c^\gamma$ etc., where $\alpha + \beta + \gamma$ etc. $= p$, and $\varkappa$ denotes the number of permutations of p objects, of which α, β, γ etc. are respectively $= a, b, c$ etc. In

[*] In an earlier paper this great man had not yet reached his goal: *Comm. Petr. T.* VI, *p.* 106. — In the famous controversy between Maupertuis and Konig, which began over the principle of least action but soon turned to unrelated matters, König said he possessed a manuscript in Leibniz's own hand containing a proof of this theorem entirely agreeing with Euler's: *Appel au public. p.* 106. Although we do not wish to deny the credibility of this testimony, Leibniz certainly never published his discovery. Compare *Hist. de l'Ac. de Prusse, A.* 1750, *p.* 530.

Article 41 we showed that this number is always divisible by p, unless all the objects are equal, *that is*, unless one of the numbers α, β, γ etc. is $= p$ and the others $= 0$. So all terms of $(a + b + c + \text{etc.})^p$, except a^p, b^p, c^p etc., are divisible by p. When considering congruence modulo p, we can therefore discard them, giving

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

If all the quantities a, b, c etc. are now set $= 1$, and their number $= k$, this gives $k^p \equiv k$, as in the preceding article.

How many numbers give periods whose number of terms is a given divisor of $p - 1$.

52.

Only divisors of $p-1$ can be the exponents of the lowest powers to which numbers are raised to become congruent to unity. So we ask whether all divisors of $p - 1$ can occur, and how many numbers belong to each exponent when all numbers not divisible by p are classified according to the exponent of their lowest power congruent to unity. We should first note that it is enough to consider the positive numbers from 1 to $p - 1$. Congruent numbers clearly have to be raised to the same lowest power to become congruent to unity, so any number belongs to the same exponent as its least positive residue. We must therefore find how, in this respect, the numbers $1, 2, 3 \ldots . p - 1$ are distributed among the individual factors of $p - 1$. For brevity, if d is a divisor of $p - 1$, including 1 and $p - 1$, let ψd denote the number of positive numbers smaller than p whose lowest power congruent to unity has exponent d.

53.

To make the investigation easier to follow, we give an example. For $p = 19$, the numbers $1, 2, 3 \ldots . 18$ are distributed among the divisors of 18 as follows:

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

Thus, in this case, $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. A little attention shows that as many numbers belong to each exponent as there are numbers no greater than it and coprime to it. So, at least in this case, using the notation of Article 39, $\psi d = \phi d$. We prove that this observation holds generally as follows.

I. Suppose we have a number a *belonging* to exponent d, *that is*, whose power with exponent d is congruent to unity, while all lower powers are incongruent to it. All its powers $aa, a^3, a^4 \ldots . a^d$, or their least residues, also have the first property: their powers with exponent d are congruent to unity. We can also say that the least residues of $a, aa, a^3 \ldots . a^d$, all distinct, are roots of the congruence $x^d \equiv 1$. Since this congruence cannot have more than d distinct roots, no numbers other than the least residues of $a, aa, a^3 \ldots . a^d$ exist between 1 and $p - 1$, inclusive, whose powers

with exponent d congruent to unity. Thus all numbers belonging to exponent d are among the least residues of $a, aa, a^3 \ldots . a^d$. We determine which ones they are, and how many, as follows. If k is coprime to d, no power of a^k with exponent $< d$ is congruent to unity. For let $\frac{1}{k} \,(\mathrm{mod.}\, d) \equiv m$ (see Article 31); then $a^{km} \equiv a$. If the power with exponent e of a^k were congruent to unity with $e < d$, we would also have $a^{kme} \equiv 1$, and therefore $a^e \equiv 1$, contrary to the hypothesis. So the least residue of a^k clearly belongs to exponent d. If, however, k has a common divisor δ with d, the least residue of a^k does not belong to exponent d, since its power with exponent $\frac{d}{\delta}$ is already congruent to unity. For $\frac{kd}{\delta}$ is divisible by d, or $\equiv 0 \,(\mathrm{mod.}\, d)$, and so $a^{\frac{kd}{\delta}} \equiv 1$. Thus as many numbers belong to exponent d as there are numbers among $1, 2, 3 \ldots . d$ coprime to d. But remember that this conclusion assumes we already have one number a belonging to exponent d. It remains uncertain whether there could be an exponent to which no number belongs at all. The conclusion is therefore limited to saying that ψd is either $= 0$ or $= \phi d$.

54.

II. Let all the divisors of $p-1$ be d, d', d'' etc. Since all numbers $1, 2, 3 \ldots . p-1$ are distributed among these, we have

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

But in Article 40 we proved that

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

The preceding article shows that ψd is equal to or smaller than ϕd, and cannot be larger. The same holds for $\psi d'$ and $\phi d'$, etc. If any of $\psi d, \psi d', \psi d''$ etc. were smaller than the corresponding term among $\phi d, \phi d', \phi d''$, or if several were, the two sums could not be equal. We finally conclude that *ψd is always equal to ϕd*, and therefore does not depend on the size of $p-1$.

55.

One special case of the preceding proposition deserves particular attention: *there are always numbers for which no power with exponent below $p-1$ is congruent to unity.* There are as many of them between 1 and $p-1$ as there are numbers below $p-1$ coprime to $p-1$. The proof of this theorem is far from as obvious as it may seem at first. Because of its importance, we may add another proof somewhat different from the preceding one: different methods often do much to clarify more difficult matters. Resolve $p-1$ into its prime factors, writing $p-1 = a^\alpha b^\beta c^\gamma$ etc., where a, b, c etc. are distinct primes. We will complete the proof by establishing the following:

I. We can always find a number A, or several, belonging to exponent a^α, and similarly numbers B, C etc. belonging to exponents b^β, c^γ etc., respectively.

II. The product of all the numbers A, B, C etc., or its least residue, belongs to exponent $p-1$. We prove these as follows.

I. Let g be one of the numbers $1, 2, 3 \ldots p-1$ *not* satisfying the congruence $x^{\frac{p-1}{a}} \equiv 1 \,(\mathrm{mod.}\, p)$, since these numbers cannot all satisfy a congruence of degree $< p-1$. I

claim that, if the power with exponent $\frac{p-1}{a^\alpha}$ of g is set $\equiv h$, this number, or its least residue, belongs to exponent a^α.

For the power with exponent a^α of h is clearly congruent to the power with exponent $p-1$ of g, *that is*, to unity. But the power with exponent $a^{\alpha-1}$ of h is congruent to the power with exponent $\frac{p-1}{a}$ of g, *that is*, it is incongruent to unity. Still less can the powers with exponents $a^{\alpha-2}$, $a^{\alpha-3}$ etc. of h be congruent to unity. Yet the exponent of the lowest power of h congruent to unity, or the exponent to which h belongs, must divide a^α (Article 48). Since a^α is divisible only by itself and lower powers of a, a^α must be the exponent to which h belongs. *Q. E. D.* The same method proves the existence of numbers belonging to exponents b^β, c^γ etc.

II. Suppose the product of all A, B, C etc. belongs not to exponent $p-1$ but to a smaller exponent t. Then t divides $p-1$ (Article 48), so $\frac{p-1}{t}$ is an integer greater than unity. This quotient is clearly either one of the primes a, b, c etc. or at least divisible by one of them (Article 17), for *example* by a; the reasoning is similar for the others.

So t divides $\frac{p-1}{a}$, and the product ABC etc. is also congruent to unity when raised to the power with exponent $\frac{p-1}{a}$ (Article 46). Each of B, C etc., excluding A, is clearly congruent to unity when raised to the power with exponent $\frac{p-1}{a}$, since the exponents b^β, c^γ etc. to which they belong divide $\frac{p-1}{a}$. Thus

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

So the exponent to which A belongs must divide $\frac{p-1}{a}$ (Article 48), *that is*, $\frac{p-1}{a^{\alpha+1}}$ must be an integer. But $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \text{ etc.}}{a}$ cannot be an integer (Article 15). We must therefore conclude that our assumption is impossible, *that is*, the product ABC etc. really does belong to exponent $p-1$. *Q. E. D.*

The second proof seems somewhat longer than the first; the first, on the other hand, is less direct than the second.

56.

This theorem is a striking example of the care often needed in number theory to avoid taking things for certain when they are not. The celebrated Lambert mentions this proposition in the paper cited above, *Acta Erudit.* 1769, *p.* 127, but does not even touch on the need for a proof. No one attempted a proof except the great Euler: *Comment. nov. Ac. Petrop. T.* XVIII, for 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, p. 85 onwards. See especially Article 37, where he discusses the need for a proof at greater length. But the proof given by this most perceptive man has two gaps. First, in Article 31 and the following articles, he tacitly assumes that the congruence $x^n \equiv 1$, expressing his reasoning in our notation, really has n distinct roots, though previously he had shown only that it cannot have *more*. Second, he derived the formula in Article 34 by induction alone.

Primitive roots, bases, indices.

57.

Following the distinguished Euler, we call numbers belonging to exponent $p-1$ *primitive roots*. If a is a primitive root, the least residues of the powers $a, aa, a^3 \ldots a^{p-1}$ are all distinct. So they must include all the numbers $1, 2, 3, \ldots p-1$, since there are just as many of these as of the least residues. In other words, every number not divisible by p is congruent to a power of a. This remarkable property is very useful, and greatly eases the arithmetic of congruences, much as logarithms ease ordinary arithmetic. We choose any primitive root a as a *base*, to which we refer all numbers not divisible by p. If $a^e \equiv b \,(\mathrm{mod.}\, p)$, we call e the *index* of b. For *example*, for modulus 19, taking the primitive root 2 as base gives the following correspondence:

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

For a fixed base, each number clearly has several indices, but they are all congruent modulo $p-1$. Whenever we discuss indices, those congruent modulo $p-1$ will therefore be regarded as equivalent, just as numbers themselves are regarded as equivalent when congruent modulo p.

Calculation with indices.

58.

The theorems on indices are entirely analogous to those on logarithms.

The index of a product of any number of factors is congruent to the sum of the indices of the individual factors modulo $p-1$.

The index of a power of a number is congruent to the product of the index of the given number and the exponent of the power, modulo $p-1$.

We omit the proofs because they are easy.

So, in constructing a table from which the indices of all numbers can be found for different moduli, we can omit both numbers greater than the modulus and composite numbers. A specimen is appended at the end of this work, *Table* I. Its first vertical column lists the primes and prime powers from 3 to 97, to be taken as moduli, with the chosen base beside each. The indices of successive primes follow, separated into groups of five by a small gap, with the primes arranged above in the same order. Thus the index of a given prime for a given modulus can be found easily and reliably.

For *example*, if $p = 67$, the index of 60, with 12 as base, is

$$\equiv 2\,\mathrm{Ind.}\,2 + \mathrm{Ind.}\,3 + \mathrm{Ind.}\,5 \;(\mathrm{mod.}\,66) \equiv 58 + 9 + 39 \equiv 40$$

59.

The index of any value of the expression $\frac{a}{b}(mod.p.)$, *(Article 31) is congruent modulo* $p-1$ *to the difference between the indices of the numerator* a *and denominator* b, *provided that the numbers* a, b *are not divisible by* p.

For let any such value be c. Then $bc \equiv a \,(\mathrm{mod.}\, p)$, so

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

and therefore

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

If we have a table giving the index of each number for any prime modulus, and another giving the number belonging to a given index, every congruence of the first degree can be solved very easily, since all can be reduced to congruences with prime moduli (Article 30).

For *example*, given the congruence

$$29x + 7 \equiv 0 \,(\mathrm{mod.}\, 47) \quad \text{then} \quad x \equiv \frac{-7}{29} (\mathrm{mod.}\, 47)$$

we obtain

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

The number with index 18 is 3, so $x \equiv 3 \,(\mathrm{mod.}\, 47)$. — We have not supplied the second table, but another can take its place, as we will show in Section VI.

Roots of the congruence $x^n \equiv A$.

60.

As in Article 31, where we introduced notation for roots of congruences of the first degree, we will now also use a symbol for roots of pure congruences of higher degrees. Just as $\sqrt[n]{A}$ means a root of the equation $x^n = A$, adding a modulus gives $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ to denote any root of the congruence $x^n \equiv A \,(\mathrm{mod.}\, p)$. We say that the expression $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ has as many values as it has values incongruent modulo p, since all values congruent modulo p are to be regarded as equivalent (Article 26). If A, B are congruent modulo p, the expressions $\sqrt[n]{A}, \sqrt[n]{B} \,(\mathrm{mod.}\, p)$ are clearly equivalent.

If we put $\sqrt[n]{A} \equiv x \,(\mathrm{mod.}\, p)$, then $n \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, A \,(\mathrm{mod.}\, p-1)$. The rules of the preceding section give the values of $\mathrm{Ind.}\, x$ from this congruence, and from them the corresponding values of x. Clearly x has as many values as the congruence $n \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, A \,(\mathrm{mod.}\, p-1)$ has roots. Thus $\sqrt[n]{A}$ has just one value when n is coprime to $p-1$. If, however, the numbers $n, p-1$ have greatest common divisor δ, then $\mathrm{Ind.}\, x$ has δ values incongruent modulo $p-1$, and $\sqrt[n]{A}$ has just as many values incongruent modulo p, provided that $\mathrm{Ind.}\, A$ is divisible by δ. If this condition fails, $\sqrt[n]{A}$ has no real value.

Example. Find the values of $\sqrt[15]{11} \,(\mathrm{mod.}\, 19)$. We must solve the congruence $15 \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, 11 \equiv 6 \,(\mathrm{mod.}\, 18)$, giving the three values $\mathrm{Ind.}\, x \equiv 4, 10, 16 \,(\mathrm{mod.}\, 18)$. The corresponding values of x are $6, 9, 4$.

61.

However convenient this method is when the necessary tables are available, we must not forget that it is indirect. So it is worth investigating how much direct methods can achieve. Here we will give what can be drawn from the preceding results, leaving other matters that require deeper considerations for Section VIII. We begin with the simplest case, where $A = 1$, that is, where we seek the roots of the congruence $x^n \equiv 1 \pmod{p}$. Taking any primitive root as the base, we must then have $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$. When n is coprime to $p-1$, this congruence has just one root, namely $\operatorname{Ind}. x \equiv 0 \pmod{p-1}$. Thus *in this case* $\sqrt[n]{1} \pmod{p}$ has a single value, namely $\equiv 1$. If, however, the numbers $n, p-1$ have greatest common divisor δ, the complete solution of the congruence $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$ is $\operatorname{Ind}. x \equiv 0 \pmod{\frac{p-1}{\delta}}$ (see Article 29). *In other words,* $\operatorname{Ind}. x$ must be congruent modulo $p-1$ to one of the numbers

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

or have δ values incongruent modulo $p-1$. So x also has δ different values in this case (incongruent modulo p). It follows that the expression $\sqrt[\delta]{1}$ also has δ different values, whose indices agree exactly with those just given. Thus the expression $\sqrt[\delta]{1} \pmod{p}$ is entirely equivalent to $\sqrt[n]{1} \pmod{p}$: the congruence $x^\delta \equiv 1 \pmod{p}$ has the same roots as $x^n \equiv 1 \pmod{p}$. The former has lower degree if δ and n are unequal.

Example. $\sqrt[15]{1} \pmod{19}$ has three values, since 3 is the greatest common divisor of $15, 18$, and these are also the values of $\sqrt[3]{1} \pmod{19}$. They are $1, 7, 11$.

62.

This reduction therefore saves us from having to solve any congruences of the form $x^n \equiv 1$ except those in which n divides $p-1$. Below we will show that congruences of this form can always be reduced further, although the preceding results are not enough for this. One case can already be settled here, namely $n = 2$. The values of $\sqrt[2]{1}$ are clearly $+1$ and -1, since there cannot be more than two, and $+1$ and -1 are always incongruent unless the modulus is $= 2$. In that case it is clear in itself that $\sqrt[2]{1}$ can have only one value. It follows that $+1$ and -1 are also the values of $\sqrt[2m]{1}$ when m is coprime to $\frac{p-1}{2}$. This always happens when the modulus is such that $\frac{p-1}{2}$ is a prime number (unless $p-1 = 2m$, in which case all the numbers $1, 2, 3 \ldots . p-1$ are roots), *for example* when $p = 3, 5, 7, 11, 23, 47, 59, 83, 107$, etc. As a corollary, note that the index of -1 is always $\equiv \frac{p-1}{2} \pmod{p-1}$, whichever primitive root is taken as the base. For $2 \operatorname{Ind}.(-1) \equiv 0 \pmod{p-1}$. Thus $\operatorname{Ind}.(-1)$ is either $\equiv 0$ or $\equiv \frac{p-1}{2} \pmod{p-1}$. But 0 is always the index of $+1$, and $+1$ and -1 must always have different indices (apart from the case $p = 2$, which need not concern us here).

63.

In Article 60 we showed that the expression $\sqrt[n]{A} \pmod{p}$ has δ different values or none at all, if δ is the greatest common divisor of $n, p-1$. Just as we have shown that $\sqrt[n]{A}$ and $\sqrt[\delta]{A}$ are equivalent when $A \equiv 1$, we will now prove more generally that the expression $\sqrt[n]{A}$ can always be reduced to another, $\sqrt[\delta]{B}$, to which it is equivalent. Denote any value of the former by x; then $x^n \equiv A$. Now let t be any value of

$\frac{\delta}{n} \pmod{p-1}$, which clearly has real values by Article 31. Then $x^{tn} \equiv A^t$, while $x^{tn} \equiv x^\delta$ because $tn \equiv \delta \pmod{p-1}$. So $x^\delta \equiv A^t$, and every value of $\sqrt[n]{A}$ is also a value of $\sqrt[\delta]{A^t}$. Whenever $\sqrt[n]{A}$ has real values, it is therefore entirely equivalent to $\sqrt[\delta]{A^t}$, since it has neither other values nor fewer. Yet when $\sqrt[n]{A}$ has no real value, $\sqrt[\delta]{A^t}$ may still have real values.

Example. If we seek the values of $\sqrt[21]{2} \pmod{31}$, the greatest common divisor of 21 and 30 is 3, and one value of $\frac{3}{21} \pmod{30}$ is 3. So if $\sqrt[21]{2}$ has real values, it is equivalent to $\sqrt[3]{2^3}$, or $\sqrt[3]{8}$. Indeed, the values of the latter expression, namely $2, 10.19$, are found to satisfy the former as well.

64.

To avoid the risk of carrying out this operation for nothing, we need a rule that lets us decide at once whether $\sqrt[n]{A}$ has real values. If a table of indices is available, this is straightforward: Article 60 shows that real values exist if the index of A, with any primitive root taken as the base, is divisible by δ, and otherwise do not exist. But this can also be determined without such a table. For if we set the index of A equal to k, then, if it is divisible by δ, $\frac{k(p-1)}{\delta}$ is divisible by $p-1$, and conversely. Now the index of $A^{\frac{p-1}{\delta}}$ is $\frac{k(p-1)}{\delta}$. So if $\sqrt[n]{A} \pmod{p}$ has real values, $A^{\frac{p-1}{\delta}}$ is congruent to unity; otherwise it is not. Thus in the example of the preceding article we have $2^{10} = 1024 \equiv 1 \pmod{31}$, from which we conclude that $\sqrt[21]{2} \pmod{31}$ has real values. Similarly, this tells us that $\sqrt[2]{-1} \pmod{p}$ always has two real values when p is of the form $4m+1$, but none when p is of the form $4m+3$, because $(-1)^{2m} = 1$ and $(-1)^{2m+1} = -1$. This elegant theorem, usually stated as follows: *If p is a prime of the form $4m+1$, a square aa can be found such that $aa+1$ is divisible by p; but if p is of the form $4m-1$, no such square exists*, was proved in this way by Euler in *Comm. nov. Acad. Petrop. T.* XVIII, *p.* 112, for the year 1773. He had given another proof much earlier, in *Comm. nov. T.* V, *p.* 5, which appeared in 1760. In an earlier paper, *Comm. nov. T.* IV, *p.* 25, he had not yet completed the matter. Later La Grange also gave a proof of the theorem, *Nouveaux Mém. de l'Ac. de Berlin A.* 1775, *p.* 342. We will give yet another proof in the next section, where this subject will be treated in its own right.

65.

Having shown how to reduce all expressions $\sqrt[n]{A} \pmod{p}$ to ones in which n divides $p-1$, and having obtained a test for whether real values exist, we will examine more closely expressions $\sqrt[n]{A} \pmod{p}$ in which n divides $p-1$. First we will show how the individual values of an expression are related; then we will give some methods that often allow one value to be found.

First, when $A \equiv 1$ and r is one of the n values of $\sqrt[n]{1} \pmod{p}$, so that $r^n \equiv 1 \pmod{p}$, all powers of r are also values of that expression. The number of different values among them equals the exponent to which r belongs (Article 48). So if r is a value belonging to the exponent n, the powers of r, namely $r, r^2, r^3 \ldots . r^n$ (the last of which may be replaced by *unity*), include all the values of $\sqrt[n]{1} \pmod{p}$. In Section VIII we will discuss more fully the methods available for finding such values belonging to the exponent n.

Second. When A is incongruent to unity and one value of $\sqrt[n]{A} \pmod{p}$, say z, is

known, the others are obtained as follows. Let the values of $\sqrt[n]{1}$ be

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

as just shown. Then all the values of $\sqrt[n]{A}$ are

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

For all these satisfy $x^n \equiv A$: if any one of them is put $\equiv zr^k$, its power with exponent n, namely $z^n r^{nk}$, because of $r^n \equiv 1$ and $z^n \equiv A$, is congruent to A. Article 23 readily shows that they are all different; and there cannot be more values than these, whose number is n, for the expression $\sqrt[n]{A}$. Thus, *for example,* if one value of $\sqrt[2]{A}$ is z, the other is $-z$. Finally, we must conclude that all values of $\sqrt[n]{A}$ cannot be found unless all values of $\sqrt[n]{1}$ are also known.

66.

Our second aim was to show when one value of $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ can be found directly, assuming that n divides $p-1$. This happens when some value is congruent to a power of A. Since this case occurs quite often, it is worth spending some time on it. Let such a value, *if one exists,* be z, so that $z \equiv A^k$ and $A \equiv z^n \,(\mathrm{mod.}\, p)$. It follows that $A \equiv A^{kn}$. So if we have a number k such that $A \equiv A^{kn}$, then A^k is the value sought. But this condition is equivalent to $1 \equiv kn \,(\mathrm{mod.}\, t)$, where t denotes the exponent to which A belongs (Articles 46, 48). For this congruence to be possible, n must be coprime to t. In that case $k \equiv \frac{1}{n} \,(\mathrm{mod.}\, t)$. But if t and n have a common divisor other than unity, no value z can be congruent to a power of A.

67.

Since this solution requires us to know t, let us see how to proceed when that number is unknown. First, it is easy to see that t must divide $\frac{p-1}{n}$ if $\sqrt[n]{A} \,(\mathrm{mod.}\, p)$ has real values, as we always assume here. For let y be any value. Then both $y^{p-1} \equiv 1$ and $y^n \equiv A \,(\mathrm{mod.}\, p)$ hold. Raising both sides of the latter congruence to the power with exponent $\frac{p-1}{n}$ gives $A^{\frac{p-1}{n}} \equiv 1$, so $\frac{p-1}{n}$ is divisible by t (Article 48). Now if $\frac{p-1}{n}$ is coprime to n, the congruence $kn \equiv 1$ of the preceding article can also be solved modulo $\frac{p-1}{n}$. Any value of k satisfying the congruence for this modulus clearly satisfies it also modulo t, which divides $\frac{p-1}{n}$ (Article 5). We have then found what was sought. But if $\frac{p-1}{n}$ is not coprime to n, remove from $\frac{p-1}{n}$ all its prime factors that also divide n, taking them out of $\frac{p-1}{n}$. This gives a number $\frac{p-1}{nq}$ coprime to n, where q denotes the product of all the prime factors removed. If the condition reached in the preceding article holds, namely that t is coprime to n, then t is also coprime to q, and therefore divides $\frac{p-1}{nq}$ as well. So if we solve $kn \equiv 1 \,(\mathrm{mod.}\, \frac{p-1}{nq})$ (which is possible because n is coprime to $\frac{p-1}{nq}$), the value of k will also satisfy the congruence modulo t, as required. The whole method consists in finding a number that can take the place of the unknown t. But we must remember that when $\frac{p-1}{n}$ is not coprime to n, we have assumed the condition of the preceding article to hold. If it fails, all the conclusions will be wrong. If, by following the rules given without regard to this, we find a value for z whose power with exponent n is not congruent to A, that tells us that the condition fails and this method cannot be used at all.

68.

Even in this case, however, the work may often prove useful. It is worth investigating how this false value is related to the true ones. Suppose, then, that k, z have been duly determined, but z^n is not $\equiv A \,(\mathrm{mod.}\, p)$. If we can determine the values of $\sqrt[n]{\frac{A}{z^n}} \,(\mathrm{mod.}\, p)$, multiplying each of them by z gives the values of $\sqrt[n]{A}$. For if v is a value of $\sqrt[n]{\frac{A}{z^n}}$, then $(vz)^n \equiv A$. But $\sqrt[n]{\frac{A}{z^n}}$ is simpler than $\sqrt[n]{A}$ in that $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ usually belongs to a smaller exponent than A. More precisely, if the greatest common divisor of t, q is d, then $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ belongs to the exponent d. This is proved as follows. Substituting the value of z gives $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \,(\mathrm{mod.}\, p)$. Now $kn - 1$ is divisible by $\frac{p-1}{nq}$ (preceding article), while $\frac{p-1}{n}$ is divisible by t (ibid.), or $\frac{p-1}{nd}$ by $\frac{t}{d}$. But $\frac{t}{d}$ is coprime to $\frac{q}{d}$ by hypothesis, so $\frac{p-1}{nd}$ is also divisible by $\frac{tq}{dd}$, or $\frac{p-1}{nq}$ by $\frac{t}{d}$. Thus $kn - 1'$ is also divisible by $\frac{t}{d}$, and $(kn-1)d$ by t. Hence $A^{(kn-1)d} \equiv 1 \,(\mathrm{mod.}\, p)$. It readily follows that $\frac{A}{z^n}$, raised to the power with exponent d, is congruent to unity. It is also easy to prove that $\frac{A}{z^n}$ cannot belong to an exponent smaller than d, but since this is not needed for our purpose, we will not dwell on it. We can therefore be certain that $\frac{A}{z^n} \,(\mathrm{mod.}\, p)$ always belongs to a smaller exponent than A, with just one exception: when t divides q, so that $d = t$.

But what do we gain from $\frac{A}{z^n}$ belonging to a smaller exponent than A? More numbers can occur as A than as $\frac{A}{z^n}$. When several such expressions $\sqrt[n]{A}$ have to be evaluated for the same modulus, this lets us obtain several from the same source. Thus, *for example,* we can always determine at least one value of $\sqrt[2]{A} \,(\mathrm{mod.}\, 29)$, provided that the values of $\sqrt[2]{-1} \,(\mathrm{mod.}\, 29)$ (which are ± 12) are known. The preceding article readily shows that one value of such expressions can always be determined directly when t is odd, and that d is $= 2$ when t is even. But no number except -1 belongs to the exponent 2.

Examples. Find $\sqrt[3]{31} \,(\mathrm{mod.}\, 37)$. Here $p - 1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$, and so $q = 3$. We must therefore have $3k \equiv 1 \,(\mathrm{mod.}\, 4)$, which is obtained by putting $k = 3$. Hence $z \equiv 31^3 \,(\mathrm{mod.}\, 37) \equiv 6$, and indeed we find $6^3 \equiv 31 \,(\mathrm{mod.}\, 37)$. If the values of $\sqrt[3]{1} \,(\mathrm{mod.}\, 37)$ are known, the remaining values of $\sqrt[3]{6}$ can also be determined. The former are $1, 10, 26$; multiplying 6 by them gives the remaining values $\equiv 23$ and 8.

If, instead, we seek a value of $\sqrt[2]{3} \,(\mathrm{mod.}\, 37)$, then $n = 2$, $\frac{p-1}{n} = 18$, and therefore $q = 2$. We must have $2k \equiv 1 \,(\mathrm{mod.}\, 9)$, giving $k \equiv 5 \,(\mathrm{mod.}\, 9)$. Thus $z \equiv 3^5 \equiv 21 \,(\mathrm{mod.}\, 37)$. But 21^2 is not $\equiv 3$, but $\equiv 34$. Now $\frac{3}{34} \,(\mathrm{mod.}\, 37) \equiv -1$ and $\sqrt[2]{-1} \,(\mathrm{mod.}\, 37) \equiv \pm 6$, giving the true values $\pm 6 \,.\, 21 \equiv \pm 15$.

This is about as much as we can give here on evaluating such expressions. Direct methods will clearly often turn out to be rather lengthy. But this drawback affects almost all direct methods in number theory, and we did not think it a reason to omit showing what they can achieve here. We should also note that explaining individually the special devices that often suggest themselves to someone experienced is outside our purpose.

Relations between indices in different systems.

69.

We now return to the roots we called primitive. We showed that, with any primitive root taken as the base, all numbers whose indices are coprime to $p-1$ are also primitive roots, and no others. This at once gives the number of primitive roots; see Article 53. In general, we may choose whichever primitive root we wish as the base. So here too, as in calculations with logarithms, there can be several systems, so to speak[*)]. Let us see how they are connected. Let a, b be two primitive roots and m another number. When a is taken as the base, let the index of b be $\equiv \beta$, and that of m be $\equiv \mu \,(\mathrm{mod.}\, p-1)$. When b is taken as the base, let the index of a be $\equiv \alpha$, and that of m be $\equiv \nu \,(\mathrm{mod.}\, p-1)$. Then $\alpha\beta \equiv 1 \,(\mathrm{mod.}\, p-1)$. For $a^\beta \equiv b$, so $a^{\alpha\beta} \equiv b^\alpha \equiv a \,(\mathrm{mod.}\, p)$ by hypothesis, and hence $\alpha\beta \equiv 1 \,(\mathrm{mod.}\, p-1)$. Similar reasoning gives $\nu \equiv \alpha\mu$ and $\mu \equiv \beta\nu \,(\mathrm{mod.}\, p-1)$. So a table of indices constructed for the base a can easily be converted into one with base b. For if, for the base a, the index of b is $\equiv \beta$, then for the base b the index of a is $\equiv \frac{1}{\beta} \,(\mathrm{mod.}\, p-1)$. Multiplying all the indices in the table by this number gives all the indices for the base b.

70.

Although a given number may have several indices when different primitive roots are taken as the base, they all agree in having the same greatest common divisor with $p-1$. For suppose the index of the given number for the base a is m, and for the base b is n. Suppose their greatest common divisors with $p-1$, namely μ, ν, are unequal. One is then larger, say $\mu > \nu$, so μ does not divide n. But if the index of a when b is taken as the base is denoted by α, then, by the preceding article, $n \equiv \alpha m \,(\mathrm{mod.}\, p-1)$. Thus μ also divides n, *contrary to the assumption.*

That this greatest common divisor of the indices of a given number and $p-1$ is independent of the base also follows from its being equal to $\frac{p-1}{t}$, where t is the exponent to which the number whose indices we are considering belongs. For if the index for any base is k, then t is the smallest number which, multiplied by k, gives a multiple of $p-1$, excluding zero (see Articles 48, 58). In other words, it is the smallest value of $\frac{0}{k} \,(\mathrm{mod.}\, p-1)$ other than zero. That this equals the greatest common divisor of k and $p-1$ follows readily from Article 29.

71.

It is also easy to prove that the base can always be chosen so that a number belonging to the exponent t has any given index whose greatest common divisor with $p-1$ is $= \frac{p-1}{t}$. Denote this divisor briefly by d, and let the desired index be $\equiv dm$. When any primitive root a is taken as the base, let the index of the given number be $\equiv dn$. Then m, n are coprime to $\frac{p-1}{d}$, or t. Now if ε is a value of $\frac{dn}{dm} \,(\mathrm{mod.}\, p-1)$ and is also coprime to $p-1$, then a^ε is a primitive root. Taking it as the base gives the number in question the index dm, as required (for $a^{\varepsilon dm} \equiv a^{dn} \equiv$ the given number). That $\frac{dn}{dm} \,(\mathrm{mod.}\, p-1)$ has values coprime to $p-1$ is proved as follows. This expression is equivalent to $\frac{n}{m} \,(\mathrm{mod.}\, \frac{p-1}{d})$, or $\frac{n}{m} \,(\mathrm{mod.}\, t)$; see Article 31, 2. All its

[*)] They differ, however, in that the number of systems for logarithms is infinite, while here it equals the number of primitive roots. Congruent bases clearly generate the same system.

values are coprime to t. For if a value e had a common divisor with t, this divisor would also have to divide me, and therefore n, to which me is congruent modulo t. This contradicts the hypothesis that n is coprime to t. So when every prime divisor of $p-1$ also divides t, *all* values of $\frac{n}{m}\,(\mathrm{mod.}\,t)$ are coprime to $p-1$, and their number is $= d$. But if $p-1$ has other prime divisors f, g, h, etc., that do not divide t, choose any value, writing $\frac{n}{m}\,(\mathrm{mod.}\,t) \equiv e$. Since t, f, g, h, etc., are all pairwise coprime, a number ε can be found that is congruent modulo t to e and, modulo f, g, h, etc., to any numbers respectively coprime to them (Article 32). Such a number is divisible by no prime factor of $p-1$, and is therefore coprime to $p-1$, as required. Finally, the theory of combinations readily gives $= \frac{p-1\,.\,f-1\,.\,g-1\,.\,h-1.\ \mathrm{etc.}}{t\,.\,f\,.\,g\,.\,h\,.\,\mathrm{etc.}}$ for the number of such values. But to keep this digression from growing too long, we omit the proof, since it is not particularly needed for our purpose.

Bases suited to particular uses.

72.

Although the choice of a primitive root as the base is generally entirely arbitrary, some bases can sometimes offer particular advantages over others. In Table I we always took 10 as the base when it was a primitive root. Otherwise we always chose the base so that the index of 10 was as small as possible, *that is,* $= \frac{p-1}{t}$, where t denotes the exponent to which 10 belongs. In Section VI we will show what this gains us, when the same table is put to other uses as well. But since some choice may still remain here, as the preceding article shows, we adopted a fixed rule: among all primitive roots meeting the requirement, we always chose the *smallest* as the base. Thus for $p = 73$, where $t = 8$ and $d = 9$, a^{ε} has $\frac{72\,.\,2}{8\,.\,3}$, *that is,* 6 values, namely $5, 14, 20, 28, 39, 40$. So we took the smallest, 5, as the base.

A method for finding primitive roots.

73.

Methods for finding primitive roots rely largely on trial. Comparing what we gave in Article 55 with what we will give below on solving the congruence $x^n \equiv 1$ provides almost everything that direct methods can achieve. Euler admits, in *Opusc. Analyt. T.* I, *p.* 152, that finding these numbers seems extremely difficult, and that their nature must be counted among the deepest mysteries of numbers. But they can be determined quite readily by trial, as follows. With experience, one learns to shorten the lengthy work by various special devices; these are learned much faster through practice than through rules.

1^0. Take any number coprime to p (we always use this letter for the modulus), say a. It usually shortens the calculation to choose as small a number as possible, *for example* 2. Determine its period (Article 46), *that is,* the least residues of its powers, until a power a^t is reached whose least residue is 1[*)]. If $t = p - 1$, then a is a primitive root.

2^0. But if $t < p - 1$, take another number b not contained in the period of a, and find its period in the same way. Denote the exponent to which b belongs by u. It is easy to see that u can neither equal t nor be a proper divisor of it: in either case we would have $b^t \equiv 1$, which is impossible, since the period of a includes all numbers whose power with exponent t is congruent to unity (Article 53). If u is $= p - 1$, then b is a primitive root. If u is not $= p - 1$ but is a multiple of t, we have gained a number belonging to a larger exponent, and have moved closer to our aim of finding a number belonging to the *largest* exponent. If u is neither $= p - 1$ nor a multiple of t, we can still find a number belonging to an exponent larger than t, u, namely the least common multiple of t, u. Let this be $= y$, and factor y into two coprime factors m, n, one dividing t and the other u[†)]. Now take the power with exponent $\frac{t}{m}$ of a, putting it $\equiv A$, and the power with exponent $\frac{u}{n}$ of b, putting it $\equiv B \pmod{p}$. The product AB will be a number belonging to the exponent n. For A clearly belongs to the exponent m, and B to n. So the product AB belongs to mn, since m, n are coprime. This can be proved in exactly the same way as in Article 55, II.

3^0. If now $y = p - 1$, then AB is a primitive root. Otherwise, as before, another number not in the period of AB must be used. This is either a primitive root, or belongs to an exponent larger than y, or at least allows us, as before, to find a number belonging to an exponent larger than y. Since the numbers obtained by repeating this operation belong to continually increasing exponents, we must eventually find one belonging to the *largest* exponent, *that is,* a primitive root, *as required.*

[*)] One readily sees that the powers themselves need not be known, since the least residue of each can easily be obtained from the least residue of the preceding power.

[†)] Article 18 readily shows how this can be done. Factor y into distinct primes or powers of distinct primes. Each factor divides one of the numbers t, u, or both. Assign each to t or u, according to which it divides; if it divides both, either assignment may be made. Let the product of those assigned to t be $= m$, and the product of the rest $= n$. It is then easy to see that m divides t, n divides u, and $mn = y$.

74.

An example will make these rules clearer. Let $p = 73$, and seek a primitive root for it. First try 2, whose period is

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

Since the power with exponent 9 is already congruent to unity, 2 is not a primitive root. Try another number not in the period of 2, *for example* 3, whose period is

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

So 3 is not a primitive root either. But the least common multiple of the exponents to which $2, 3$ belong, *that is,* of $9, 12$, is 36. By the rules of the preceding article, this factors into 9 and 4. We must therefore raise 2 to the power with exponent $\frac{9}{9}$, *that is,* keep 2 itself, and raise 3 to the power with exponent 3. Their product is 54, which therefore belongs to the exponent 36. Finally, calculating the period of 54 and again trying a number not in it, *for example* 5, will show that this number is a primitive root.

Various theorems on periods and primitive roots.

75.

Before leaving this subject, we will give a few propositions whose simplicity seems to make them worth attention.

The product of all the terms in the period of any number is $\equiv 1$ *when their number, or the exponent to which the number belongs, is odd, and* $\equiv -1$ *when that exponent is even.*

Example. For the modulus 13, the period of 5 consists of $1, 5, 12, 8$, whose product is $480 \equiv -1 \,(\mathrm{mod.}\, 13)$.

For the same modulus, the period of 3 consists of $1, 3, 9$, whose product is $27 \equiv 1 \,(\mathrm{mod.}\, 13)$.

Proof. Let the exponent to which the number belongs be t, and its index $\frac{p-1}{t}$. This is always possible with a suitable choice of base (Article 71). Then the index of the product of all terms of the period is

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

that is, $\equiv 0 \,(\mathrm{mod.}\, p-1)$ when t is odd, and $\equiv \frac{p-1}{2}$ when t is even. Thus in the first case the product $\equiv 1 \,(\mathrm{mod.}\, p)$, and in the second $\equiv -1 \,(\mathrm{mod.}\, p)$ (Article 62). *Q. E. D.*

76.

If the number in the preceding theorem is a primitive root, its period includes all the numbers $1, 2, 3 \ldots\ldots p-1$, whose product is therefore always $\equiv -1$ (for $p-1$ is always even, apart from the single case $p = 2$, where -1 and $+1$ are equivalent). This

elegant theorem, usually stated as follows: *the product of all numbers smaller than a given prime, increased by unity, is divisible by that prime*, was first stated by Waring and attributed to Wilson, Esq., *Meditt. algebr. Ed.* 3, *p.* 380. But neither could prove it. Waring admits that the proof seems all the harder because no *notation* can be devised to express a prime number. — In our view, however, truths of this kind should be drawn from concepts rather than notations. Later La Grange gave a proof, *Nouv. Mém. de l'Ac. de Berlin,* 1771. It rests on considering the coefficients obtained by expanding the product

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

Namely, if this product is put

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

the coefficients A, B, etc., M will be divisible by p, while N will be $= 1.2.3. \ldots .\, p-1$. Now for $x = 1$ the product is divisible by p, but is then $\equiv 1 + N \,(\text{mod.}\, p)$. So $1 + N$ must be divisible by p.

Finally, Euler gave a proof in *Opusc. analyt. T.* I, *p.* 329, agreeing with the one we have given here. If such men thought this theorem worth their consideration, we hope readers will not mind if we add another proof.

77.

When modulo p the product of two numbers a, b is congruent to unity, let us follow Euler in calling the numbers a, b *partners.* By the preceding section, every positive number smaller than p has exactly one positive partner smaller than p. It is easy to prove that among $1, 2, 3. \ldots .\, p-1$, only 1 and $p-1$ are their own partners. For numbers that are their own partners are roots of $xx \equiv 1$, which, being of the second degree, cannot have more than two roots, *that is,* any besides 1 and $p-1$. Removing these, the remaining numbers $2.3. \ldots .\, p-2$ are paired off. Their product is therefore $\equiv 1$, so the product of all the numbers $1, 2, 3 \ldots p-1$ is $\equiv p-1$, or $\equiv -1$. *Q. E. D.*

For example, for $p = 13$ the numbers $2, 3, 4. \ldots 11$ are paired as follows: 2 with 7; 3 with 9; 4 with 10; 5 with 8; 6 with 11. Namely, $2.7 \equiv 1$; $3.9 \equiv 1$, etc. So $2.3.4. \ldots 11 \equiv 1$, and therefore $1.2.3. \ldots 12 \equiv -1$.

78.

Wilson's theorem can be stated more generally as follows. *The product of all numbers smaller than any given number A and coprime to it is congruent modulo A to unity, taken either negatively or positively.* Unity is to be taken negatively when A has the form p^m or $2p^m$, where p denotes a prime other than 2, and also when $A = 4$; positively in every other case. The theorem as stated by Wilson is included in the first case. — *For example,* for $A = 15$ the product of $1, 2, 4, 7, 8, 11, 13, 14$ is $\equiv 1 \,(\text{mod.}\, 15)$. For brevity we give no proof. We only note that it can be carried out as in the preceding article, except that $xx \equiv 1$ may have more than two roots, requiring some special considerations. A proof could also be obtained by considering indices, as in Article 75, together with what we will soon give on nonprime moduli.

79.

We return to listing other propositions (Article 75).

The sum of all terms in the period of any number is $\equiv 0$, as in the example of Article 75, $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$.

Proof. Let the number whose period is in question be $= a$, and the exponent to which it belongs $= t$. The sum of all terms of the period is then

$$\equiv 1 + a + aa + a^3 + \text{etc.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}$$

But $a^t - 1 \equiv 0$, so this sum is always $\equiv 0$ (Article 22), unless $a - 1$ is divisible by p, or $a \equiv 1$. We must therefore exclude this case if we wish to call even a single term a *period*.

80.

The product of all primitive roots is $\equiv 1$, with the single exception $p = 3$, when there is just one primitive root, 2.

Proof. With any primitive root taken as the base, the indices of all primitive roots are the numbers coprime to $p - 1$ and smaller than it. The sum of these numbers, *that is,* the index of the product of all primitive roots, is $\equiv 0 \pmod{p - 1}$, so the product $\equiv 1 \pmod{p}$. For if k is coprime to $p - 1$, clearly $p - 1 - k$ is also coprime to $p - 1$. Thus the numbers coprime to $p - 1$ pair off into sums divisible by $p - 1$. (But k can never equal $p - 1 - k$, apart from the case $p - 1 = 2$, or $p = 3$, which we have excluded: in every other case $\frac{p-1}{2}$ is clearly not coprime to $p - 1$.)

81.

The sum of all primitive roots is either $\equiv 0$ (when $p - 1$ is divisible by a *square*) *or* $\equiv \pm 1$ (*mod.p*) (when $p - 1$ is a product of distinct primes; take the positive sign if their number is even and the negative sign if it is odd).

Examples. 1^0 For $p = 13$, the primitive roots are $2, 6, 7, 11$, whose sum is $26 \equiv 0 \pmod{13}$.

2^0 For $p = 11$, the primitive roots are $2, 6, 7, 8$, whose sum is $23 \equiv +1 \pmod{11}$.

3^0 For $p = 31$, the primitive roots are $3, 11, 12, 13, 17. 21, 22, 24$, whose sum is $123 \equiv -1 \pmod{31}$.

Proof. We showed above (Article 55, II) that if $p - 1$ is $= a^\alpha b^\beta c^\gamma$, etc. (where a, b, c, etc., denote distinct primes), and A, B, C, etc., are any numbers belonging respectively to the exponents $a^\alpha, b^\beta, c^\gamma$, etc., all products ABC, etc., are primitive roots. It is also easy to prove that every primitive root can be represented by such a product, and in only one way*).

So these products can take the place of the primitive roots themselves. Since in these products every value of A must be combined with every value of B, etc., the

*)Determine the numbers $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, etc., so that $\mathfrak{a} \equiv 1 \pmod{a^\alpha}$ and $\equiv 0 \pmod{b^\beta c^\gamma \text{etc.}}$; $\mathfrak{b} \equiv 1 \pmod{b^\beta}$ and $\equiv 0 \pmod{a^\alpha c^\gamma \text{etc.}}$, etc. (see Article 32). Then $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \text{etc.} \equiv 1 \pmod{p - 1}$ (Article 19). Now if any primitive root r is to be represented by a product ABC, etc., take $A \equiv r^{\mathfrak{a}}, B \equiv r^{\mathfrak{b}}, C \equiv r^{\mathfrak{c}}$, etc. Then A belongs to the exponent a^α, B to the exponent b^β, etc. The product of all A, B, C, etc., is $\equiv r \pmod{p}$. Finally, it is easy to see that A, B, C, etc., cannot be determined in any other way.

sum of all the products equals the product of the sum of all values of A, the sum of all values of B, the sum of all values of C, etc., as is known from the theory of combinations. Denote all values of A; B, etc., by A, A', A'', etc.; B, B', B'', etc., etc. Then the sum of all primitive roots

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

Now I say that if the exponent α is $= 1$, the sum $A + A' + A''$ + etc. will be $\equiv -1 \,(\text{mod.}\, p)$; but if α is > 1, this sum will be $\equiv 0$. The same applies to the other exponents β, γ, etc. Once this is proved, the truth of our theorem will be evident. For when $p - 1$ is divisible by a square, one of the exponents α, β, γ, etc., exceeds unity. So one of the factors whose product is congruent to the sum of all primitive roots is $\equiv 0$, and therefore so is the product itself. But when $p - 1$ is divisible by no square, all the exponents α, β, γ, etc., are $= 1$. The sum of all primitive roots is then congruent to a product with as many factors, each $\equiv -1$, as there are numbers a, b, c, etc. It is therefore $\equiv \pm 1$, according to whether their number is even or odd. The claims are proved as follows.

1^0. When $\alpha = 1$ and A is a number belonging to the exponent a, the other numbers belonging to this exponent are $A^2, A^3 \ldots . A^{a-1}$. But

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

is the sum of a complete period, and therefore $\equiv 0$ (Article 79). So

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

2^0. But when $\alpha > 1$ and A is a number belonging to the exponent a^α, the other numbers belonging to this exponent are obtained by removing from $A^2, A^3, A^4 \ldots . A^{a^\alpha - 1}$ the terms A^a, A^{2a}, A^{3a}, etc.; see Article 53. Their sum is therefore

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

that is, congruent to the difference of two periods, and thus $\equiv 0$. *Q. E. D.*

Moduli that are powers of primes.

82.

Everything given so far rests on the assumption that the modulus is prime. We still have to consider the case where a composite number is taken as the modulus. But the properties here are neither as elegant as in the previous case, nor do they require subtle devices to find them. Rather, almost everything can be drawn simply from applying the preceding principles. Going through every detail would therefore be unnecessary and tedious. So we will briefly give what this case shares with the previous one and what is particular to it.

83.

The propositions of Articles 45–48 have already been proved in general. But the proposition of Article 49 must be modified as follows:

If f denotes how many numbers are coprime to m and smaller than m, that is, if $f = \phi m$ (Article 38), the exponent t of the lowest power of a given number a coprime to m that is congruent to unity modulo m is either $= f$ or a proper divisor of that number.

The proof in Article 49 also applies here if we replace p everywhere by m, $p-1$ by f, and the numbers $1, 2, 3, \ldots p-1$ by the numbers coprime to m and smaller than m. We therefore refer the reader there. The other proofs mentioned there (Articles 50, 51) cannot be applied to this case without considerable complications. — But for the following propositions, Article 52 onward, a major difference appears between moduli that are powers of primes and those divisible by several primes. So we will consider moduli of the first kind separately.

84.

If the modulus $m = p^n$, where p is prime, then $f = p^{n-1}(p-1)$ (Article 38). Applying the investigations of Articles 53, 54 to this case, with the changes prescribed in the preceding article, shows that everything proved there also holds here, provided we have first proved that a congruence of the form $x^t - 1 \equiv 0 \,(\mathrm{mod.}\, p^n)$ cannot have more than t different roots. For a prime modulus we derived this from the more general proposition of Article 43. But that proposition, in its full extent, holds only for prime moduli, and so cannot be applied here. Nevertheless, we will prove the proposition for this particular case by a special method. Below, in Section VIII, we will show how to reach the same result more easily.

85.

We set out to prove the following theorem:

If the greatest common divisor of t and $p^{n-1}(p-1)$ is e, the congruence $x^t \equiv 1 \,(mod. p^n)$ has e different roots.

Let $e = kp^\nu$, where k does not contain the factor p, and therefore divides $p-1$. Then the congruence $x^t \equiv 1$ has, modulo p, exactly k different roots. Denote these by A, B, C, etc. Any root of the same congruence modulo p^n must be congruent modulo p to one of A, B, C, etc. We will now show that $x^t \equiv 1. \,(\mathrm{mod.}\, p^n)$ has p^ν roots congruent to A, as many congruent to B, etc., modulo p. The total number of roots will then be kp^ν, or e, as asserted. We will arrange the proof as follows. *First,* we show that if α is a root congruent to A modulo p, then

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

are also roots. *Second,* among numbers congruent to A modulo p, no numbers besides those of the form $\alpha + hp^{n-\nu}$ (where h is any integer) can be roots. This clearly gives p^ν different roots and no more. The same holds for roots congruent to each of B, C, etc. *Third,* we show how a root congruent to A modulo p can always be found.

86.

THEOREM. *If, as in the preceding article, t is divisible by p^ν but not by $p^{\nu+1}$, then*

$$(\alpha + hp^\mu)^t - \alpha^t \equiv 0\,(mod.p^{\mu+\nu}),$$
$$but\ \equiv \alpha^{t-1}hp^\mu t\,(mod.p^{\mu+\nu+1})$$

The latter part of the theorem does not hold when both $p = 2$ and $\mu = 1$.

We could prove this theorem by expanding the power of the binomial and showing that every term after the second is divisible by $p^{\mu+\nu+1}$. But examining the denominators of the coefficients leads to some complications, so we prefer the following method.

First suppose $\mu > 1$ and $\nu = 1$. Because

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

we have

$$(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha + \text{etc.} + \alpha^{t-1})$$

But $\alpha + hp^\mu \equiv \alpha\,(\text{mod.}\,p^2)$, so each term $(\alpha + hp^\mu)^{t-1}$, $(\alpha + hp^\mu)^{t-2}\alpha$, etc., is $\equiv \alpha^{t-1}(\text{mod.}\,p^2)$. Thus their sum is $\equiv t\alpha^{t-1}(\text{mod.}\,p^2)$, or of the form $t\alpha^{t-1} + Vp^2$, where V is some number. Hence $(\alpha + hp^\mu)^t - \alpha^t$ has the form

$$\alpha^{t-1}hp^\mu t + Vhp^{\mu+2},$$
$$that\ is,\ \equiv \alpha^{t-1}hp^\mu t(\text{mod.}\,p^{\mu+2}) \quad \text{and} \quad \equiv 0\,(\text{mod.}\,p^{\mu+1}).$$

So the theorem is proved in this case.

Now if the theorem failed for other values of ν, still with $\mu > 1$, there would necessarily be a boundary up to which it was always true and beyond which it was false. Let the smallest value of ν for which it is false be $= \varphi$. We readily see that if t is divisible by $p^{\varphi-1}$ but not by p^φ, the theorem is still true, but becomes false when t is replaced by tp. So we have

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

where u is an integer. But since the theorem is already proved for $\nu = 1$, we have

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

and therefore also

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

that is, the theorem is true even when t is replaced by tp, *that is,* for $\nu = \varphi$, contrary to the hypothesis. Thus the theorem is true for all values of ν.

87.

The case $\mu = 1$ remains. By a method entirely like the one used in the preceding article, without the binomial theorem, we can show that

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp\\ \alpha\alpha(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp\\ &\text{etc.}\end{aligned}$$

so their sum, since the number of terms $= t$, is

$$\equiv t\alpha^{t-1} + \tfrac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$$

Since t is divisible by p, $\dfrac{(t-1)t}{2}$ is also divisible by p in every case except $p = 2$, as already noted in the preceding article. In the other cases $\frac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0 \pmod{p^2}$, so that sum is also $\equiv t\alpha^{t-1} \pmod{p^2}$, as in the preceding article. The rest of the proof proceeds exactly as there.

We therefore conclude in general, with the single exception $p = 2$, that

$$(\alpha + hp^\mu)^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$$

and $(\alpha + hp^\mu)^t$ *not* $\equiv \alpha^t$ for any modulus that is a higher power of p than $p^{\mu+\nu}$, provided h is not divisible by p and p^ν is the highest power of p dividing t.

The first and second propositions we set out to prove in Article 85 follow at once:

first, if $\alpha^t \equiv 1$, then also $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

second, suppose a number α', congruent to A and therefore also to α modulo p, but not congruent to the latter modulo $p^{n-\nu}$, satisfied $x^t \equiv 1 \pmod{p^n}$. Put α' equal to $= \alpha + lp^\lambda$, with l not divisible by p. Then $\lambda < n - \nu$, and $(\alpha + lp^\lambda)^t$ is congruent modulo $p^{\lambda+\nu}$ to α^t, but not modulo p^n, which is a higher power. So α' cannot be a root of $x^t \equiv 1$.

88.

The *third* task was to find a root of $x^t \equiv 1 \pmod{p^n}$ congruent to A. Here we show only how this can be done if a root of the same congruence modulo p^{n-1} is already known. This clearly suffices: starting with the modulus p, for which A is a root, we can pass to the modulus p^2 and then to every successive power.

So let α be a root of $x^t \equiv 1 \pmod{p^{n-1}}$, and seek a root of the same congruence modulo p^n. Put this root $= \alpha + hp^{n-\nu-1}$; the preceding article shows that it must have this form. (The case $\nu = n - 1$ will be considered separately later; $n - 1$ cannot be exceeded by ν.) We must therefore have

$$(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^{n-1}}$$

But $$(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$$

So if h is chosen so that $1 \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$, or, since by hypothesis $1 \equiv \alpha^t \pmod{p^{n-1}}$ and t is divisible by p^ν, so that $\dfrac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1}h\dfrac{t}{p^\nu}$ is divisible by

p, the requirement is met. The preceding section shows that this is always possible, since we assume here that t cannot be divided by a power of p higher than p^ν, and so $\alpha^{t-1}\dfrac{t}{p^\nu}$ is coprime to p.

But if $\nu = n-1$, *that is,* t is divisible by p^{n-1} or even by a higher power of p, every value A satisfying $x^t \equiv 1$ modulo p also satisfies it modulo p^n. For let $t = p^{n-1}\tau$; then $t \equiv \tau (\mathrm{mod.}\, p-1)$. Since $A^t \equiv 1\,(\mathrm{mod.}\, p)$, we therefore also have $A^\tau \equiv 1\,(\mathrm{mod.}\, p)$. Put $A^\tau = 1 + hp$; then $A^t = (1+hp)^{p^{n-1}} \equiv 1 (\mathrm{mod.}\, p^n)$ by Article 87.

89.

Everything derived in Article 57 onward with the help of the theorem that $x^t \equiv 1$ cannot have more than t different roots also holds for a modulus that is a power of a prime. If we call the numbers belonging to the exponent $p^{n-1}(p-1)$ *primitive roots*, or equivalently the numbers whose periods contain all numbers not divisible by p, primitive roots exist here too. Everything given above on indices and their use, and on solving $x^t \equiv 1$, can also be applied here. Since there are no difficulties in doing so, repeating everything from the beginning would be unnecessary. We have also shown how to derive the roots of $x^t \equiv 1$ modulo p^n from those of the same congruence modulo p. But we must add a few things about moduli that are powers of 2, since they were excluded above.

Moduli that are powers of two.

90.

If a power of 2 higher than the second, say 2^n, is taken as the modulus, the power with exponent 2^{n-2} of any odd number is congruent to unity. For example, $3^8 = 6561 \equiv 1\,(\mathrm{mod.}\, 32)$.

Every odd number has one of the forms $1+4h$ or $-1+4h$, so the proposition follows at once from the theorem of Article 86.

Since the exponent to which any odd number belongs modulo 2^n must divide 2^{n-2}, it belongs to one of $1, 2, 4, 8 \ldots . 2^{2n-2}$. Which one can be decided easily as follows. Let the given number be $= 4h \pm 1$, and the exponent of the highest power of 2 dividing h be $= m$ (which may also be $= 0$, namely when h is odd). Then the exponent to which the given number belongs is $= 2^{n-m-2}$, provided $n > m+2$. But if $n =$ or $< m+2$, the given number is $\equiv \pm 1$, and so belongs either to the exponent 1 or to the exponent 2. For a number of the form $\pm 1 + 2^{m+2}k$ (equivalent to $4h \pm 1$), raised to the power with exponent 2^{n-m-2}, is congruent to unity modulo 2^n, but is not when raised to a power whose exponent is a lower power of 2. This follows readily from Article 86. So any number of the form $8k+3$ or $8k+5$ belongs to the exponent 2^{n-2}.

91.

Thus there are no *primitive roots* here in the sense used above: no numbers whose periods include all numbers smaller than the modulus and coprime to it. Yet an analogue is easy to see. A power of a number of the form $8k+3$ with odd exponent is always of the form $8k+3$, while one with even exponent is always of the form $8k+1$. So no power can have the form $8k+5$ or $8k+7$. Now the period of a number of the

form $8k+3$ contains 2^{n-2} different terms, each of the form $8k+3$ or $8k+1$, and there are no more than 2^{n-2} such numbers smaller than the modulus. Thus every number of the form $8k+1$ or $8k+3$ is congruent modulo 2^n to some power of any number of the form $8k+3$. Similarly, the period of a number of the form $8k+5$ can be shown to contain all numbers of the forms $8k+1$ and $8k+5$. So if a number of the form $8k+5$ is taken as the base, all numbers of the forms $8k+1$ and $8k+5$, taken positively, and all numbers of the forms $8k+3$ and $8k+7$, taken negatively, acquire real indices. Indices congruent modulo 2^{n-2} must here be treated as equivalent. This is how to understand our Table I, where for the moduli 16, 32 and 64 (no table is needed for the modulus 8) we always took 5 as the base. *For example,* the number 19, which is of the form $8n+3$ and must therefore be taken *negatively*, has, for the modulus 64, the index 7. This means $5^7 \equiv -19 \,(\mathrm{mod.}\, 64)$.

But numbers of the forms $8n+1$, $8n+5$, taken negatively, and those of the forms $8n+3$, $8n+7$, taken positively, would have to be assigned imaginary indices, so to speak. Introducing these reduces the calculation of indices to a very simple algorithm. But a fully rigorous treatment would take us too far afield, so we leave it for another occasion, when we may undertake a fuller account of the theory of imaginary quantities. In our view, no one has yet reduced that theory to clear concepts. Those with experience will readily find this algorithm for themselves. Those with less practice can still use the table just as people use logarithms without knowing recent authors' discussions of imaginary *logarithms*, provided they have a good grasp of the principles established above.

Moduli composed of several primes.

92.

For a modulus composed of several primes, almost everything about residues of powers can be derived from the general theory of congruences. But below we will show more fully how to reduce any congruence for such a modulus to congruences whose moduli are prime or powers of primes, so we need not spend much time on this here. We only note that the very fine property holding for the other moduli, namely that there always exist numbers whose periods include all numbers coprime to the modulus, fails here. There is just one exception: when the modulus is twice a prime or twice a power of a prime. For if the modulus m is put in the form $A^a B^b C^c$, etc., where A, B, C, etc., are distinct primes, and $A^{a-1}(A-1)$ is denoted by α, $B^{b-1}(B-1)$ by β, etc., and finally z is coprime to m, then $z^\alpha \equiv 1 \,(\mathrm{mod.}\, A^a)$. $z^\beta \equiv 1 \,(\mathrm{mod.}\, B^b)$, etc. So if μ is the least common multiple of α, β, γ, etc., then $z^\mu \equiv 1$ for all the moduli A^a, B^b, etc., and therefore also modulo m, their product. But except when m is twice a prime or twice a power of a prime, the least common multiple of α, β, γ, etc., is smaller than their product, since α, β, γ, etc., cannot be pairwise coprime, but certainly have the common divisor 2. So no number's period can contain as many terms as there are numbers coprime to the modulus and smaller than it, since their number equals the product of α, β, γ, etc. Thus, *for example,* for $m = 1001$ any number coprime to m, raised to the power with exponent 60, is congruent to unity, since 60 is a common multiple of $6, 10, 12$. — But the case where the modulus is

twice a prime or twice a power of a prime is entirely similar to the case of a prime or a power of a prime.

93.

We have already mentioned here and there the writings in which other mathematicians treated the subject of this section. But readers wanting some matters explained more fully than our wish for brevity allowed are referred particularly to the following papers by Euler. They are especially recommended for the clarity in which this great man always excelled above all others.

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

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.

Ibid. T. XVIII, *p.* 85 onward.

To these may be added *Opusculorum analyt. T.* I, papers 5 and 8.

FOURTH SECTION

ON

CONGRUENCES OF THE SECOND DEGREE.

Quadratic residues and nonresidues.

94.

THEOREM. *For any number m taken as modulus, among the numbers $0, 1, 2, 3....m-1$, at most $\frac{1}{2}m+1$ can be congruent to a square when m is even, and at most $\frac{1}{2}m+\frac{1}{2}$ when m is odd.*

Proof. Since the squares of congruent numbers are congruent, any number that can be congruent to a square will also be congruent to a square whose root is $< m$. So it is enough to consider the least residues of the squares $0, 1, 4, 9....(m-1)^2$. But we readily see that $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, etc. Thus, when m is even, the squares $(\frac{1}{2}m-1)^2$ and $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ and $(\frac{1}{2}m+2)^2$, etc. have the same least residues; when m is odd, the squares $(\frac{1}{2}m-\frac{1}{2})^2$ and $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ and $(\frac{1}{2}m+\frac{3}{2})^2$, etc. are congruent. So no numbers other than those congruent to one of the squares $0, 1, 4, 9....(\frac{1}{2}m)^2$ can be congruent to a square when m is even; when it is odd, every number congruent to a square must be congruent to one of $0, 1, 4, 9....(\frac{1}{2}m-\frac{1}{2})^2$. There are therefore at most $\frac{1}{2}m+1$ distinct least residues in the first case, and $\frac{1}{2}m+\frac{1}{2}$ in the second. *Q. E. D.*

Example. Modulo 13, the squares of the numbers $0, 1, 2, 3...6$ have the least residues $0, 1, 4, 9, 3, 12, 10$; after these, the same residues recur in reverse order, $10, 12, 3$, etc. So any number congruent to none of these residues, or equivalently congruent to one of $2, 5, 6, 7.\ 8, 11$, cannot be congruent to a square.

Modulo 15 we find the residues $0, 1, 4, 9, 1, 10, 6, 4$, after which the same residues recur in reverse order. Here the number of residues that can be congruent to a square is even smaller than $\frac{1}{2}m+\frac{1}{2}$, since they are $0, 1, 4, 6, 9, 10$. The numbers $2, 3, 5, 7, 8, 11, 12, 13, 14$, and those congruent to any one of them, cannot be congruent to a square modulo 15.

95.

It follows that, for any modulus, all numbers can be divided into two classes: one contains the numbers that can be congruent to a square, and the other those that cannot. We will call the former *quadratic residues of the number taken as modulus*[*)], and the latter its *quadratic nonresidues*, or simply *residues* and *nonresidues* whenever there is no risk of ambiguity. It is enough to classify all the numbers $0, 1, 2 \ldots m-1$, since congruent numbers must belong to the same class.

[*)] Strictly speaking, we are using the genitive here in a different sense from before. We should say that r is a residue of the square aa modulo m when $r \equiv aa \pmod{m}$; but for brevity, throughout this section we call r a quadratic residue *of m itself*, without any risk of ambiguity. From now on we will not use the word *residue* to mean a congruent number, except when speaking of *least* residues, where no doubt can arise.

In this investigation too, we will begin with prime moduli; this is to be understood even when we do not say so explicitly. The prime number 2 must, however, be excluded: we will consider only *odd* primes.

When the modulus is prime, there are as many residues smaller than it as nonresidues.

96.

Taking the prime number p as modulus, half the numbers $1, 2, 3 \ldots p-1$ are quadratic residues, and the rest are nonresidues; that is, there are $\frac{1}{2}(p-1)$ residues and just as many nonresidues.

For it is easy to prove that all the squares $1, 4, 9 \ldots \frac{1}{4}(p-1)^2$ are incongruent. If $rr \equiv r'r' (\mathrm{mod.}\, p)$ were possible with the numbers r, r' unequal and no greater than $\frac{1}{2}(p-1)$, then, taking $r > r'$, as we may, $(r-r')(r+r')$ would be positive and divisible by p. But both factors $r-r'$ and $r+r'$ are smaller than p, so this assumption is impossible (Article 13). Thus there are $\frac{1}{2}(p-1)$ quadratic residues among the numbers $1, 2, 3 \ldots p-1$. There cannot be more, since adding the residue 0 gives $\frac{1}{2}(p+1)$, and the total number of residues cannot exceed this. So the remaining numbers are nonresidues, and their number is $= \frac{1}{2}(p-1)$.

Since zero is always a residue, we exclude it and numbers divisible by the modulus from these investigations. This case needs no explanation and would only spoil the neatness of the theorems. For the same reason we have excluded the modulus 2.

97.

Several results that we will present in this section can also be derived from the principles of the previous section. Since it is useful to examine the same truth by different methods, we will show this connection. We readily see that all numbers congruent to a square have *even* indices, while those that cannot be congruent to any square have odd indices. Since $p-1$ is even, there are as many even indices as odd ones, namely $\frac{1}{2}(p-1)$, and therefore as many residues as nonresidues.

Examples. The residues for the following moduli are

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.
		etc.

The other numbers smaller than these moduli are nonresidues.

Whether a composite number is a residue or a nonresidue of a given prime depends on its factors.

98.

THEOREM. *The product of two quadratic residues of the prime number p is a residue; the product of a residue and a nonresidue is a nonresidue; and the product of two nonresidues is a residue.*

Proof. I. Let A, B be residues arising from the squares aa, bb, so that $A \equiv aa$, $B \equiv bb$. Their product AB is congruent to the square of ab, and is therefore a residue.

II. When A is a residue, say $\equiv aa$, and B is a nonresidue, AB is a nonresidue. For suppose, if possible, that $AB \equiv kk$, and let $\frac{k}{a} (\mathrm{mod.}\, p) \equiv b$. Then $aaB \equiv aabb$, so $B \equiv bb$: that is, B is a residue, contrary to the hypothesis.

Another proof. Multiply all the residues among $1, 2, 3 \ldots p-1$ (whose number is $= \frac{1}{2}(p-1)$) by A. All the products are quadratic residues, and they are all incongruent. If we now multiply the nonresidue B by A, the product will be congruent to none of those already obtained. If it were a residue, there would therefore be $\frac{1}{2}(p+1)$ incongruent residues, not yet including the residue 0, contrary to Article 96.

III. Let A, B be nonresidues. Multiply all the residues among $1, 2, 3 \ldots p-1$ by A; we obtain $\frac{1}{2}(p-1)$ mutually incongruent nonresidues (II). The product AB cannot be congruent to any of them; so if it were a nonresidue, there would be $\frac{1}{2}(p+1)$ mutually incongruent nonresidues, contrary to Article 96. So the product, etc. *Q. E. D.*

These theorems follow still more easily from the principles of the previous section. The indices of residues are always even, and those of nonresidues odd; so the index of the product of two residues or of two nonresidues is even, and the product itself is a residue. In contrast, the index of the product of a residue and a nonresidue is odd, so the product itself is a nonresidue.

Both methods of proof can also be used for the following theorems: *The value of the expression $\frac{a}{b}$ $(mod.\, p)$ is a residue when the numbers a, b are both residues or both nonresidues; it is a nonresidue when one of the numbers a, b is a residue and the other a nonresidue.* These also follow by reversing the preceding theorems.

99.

In general, a product of any number of factors is a residue both when all the factors are residues and when an even number of them are nonresidues. When an odd number of the factors are nonresidues, the product is a nonresidue. So we can readily decide whether a composite number is a residue if we know the character of each of its factors. For this reason, we have included only prime numbers in Table II. The table is arranged as follows. The moduli are placed in the margin[*)], and the successive prime numbers in the body of the table. When one of these primes is a residue of a modulus, a short line is placed in the corresponding space; when the prime is a nonresidue of the modulus, that space is left empty.

[*)] We will soon show how we can also dispense with composite moduli.

Composite moduli.

100.

Before moving on to more difficult matters, we must add a few observations about nonprime moduli.

If, for a prime number p, a power p^n is taken as modulus (where we assume that p is not 2), half the numbers not divisible by p and smaller than the modulus are residues, and half are nonresidues; that is, the number of each is $= \frac{1}{2}(p-1)p^{n-1}$.

For if r is a residue, it is congruent to a square whose root does not exceed half the modulus; see Article 94. We readily see that there are $\frac{1}{2}(p-1)p^{n-1}$ numbers not divisible by p and smaller than half the modulus. It remains to prove that their squares are all incongruent, or give distinct quadratic residues. If the squares of two numbers a, b, not divisible by p and smaller than half the modulus, were congruent, then $aa - bb$, or $(a-b)(a+b)$, would be divisible by p^n (taking $a > b$, as we may). This is possible only if *either* one of the numbers $a-b$. $a+b$ is divisible by p^n, which is impossible since each is $< p^n$, *or* one is divisible by p^m and the other by p^{n-m}, so both are divisible by p. But this too is impossible. Their sum and difference, $2a$ and $2b$, would then also be divisible by p, and therefore so would a and b, contrary to the hypothesis. — We conclude that, among the numbers not divisible by p and smaller than the modulus, there are $\frac{1}{2}(p-1)p^{n-1}$ residues; the remaining numbers, of which there are just as many, are nonresidues. *Q. E. D.* — This theorem can also be derived by considering indices, much as in Article 97.

101.

Every number not divisible by p that is a residue of p is also a residue of p^n; every nonresidue of p is also a nonresidue of p^n.

The latter part of this proposition needs no proof. If the first part were false, then among the numbers smaller than p^n and not divisible by p, more would be residues of p than of p^n, that is, more than $\frac{1}{2}p^{n-1}(p-1)$. But we readily see that the number of residues of p among these numbers is exactly $= \frac{1}{2}p^{n-1}(p-1)$.

It is just as easy to find an actual square congruent to a given residue modulo p^n, if a square congruent to it modulo p is known.

If we have a square aa congruent to the given residue A modulo p^μ, we can derive a square congruent to A modulo p^ν (where we assume $\nu > \mu$ and $=$ or $< 2\mu$) as follows. Put the root of the required square $= \pm a + xp^\mu$, a form that it must clearly have. We must then have $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A \,(\mathrm{mod.}\, p^\nu)$, or, since $2\mu \geq \nu$, $A - aa \equiv \pm 2axp^\mu \,(\mathrm{mod.}\, p^\nu)$. Let $A - aa = p^\mu d$; then x is the value of the expression $\pm\frac{d}{2a} \,(\mathrm{mod.}\, p^{\nu-\mu})$, which is equivalent to $\pm\frac{A-aa}{2ap^\mu} \,(\mathrm{mod.}\, p^\nu)$.

So a square congruent to A modulo p gives a square congruent to A modulo p^2; from here we can move up to the modulus p^4, then to p^8, etc.

Example. Given the residue 6, congruent modulo 5 to the square 1, we find the square 9^2 to which it is congruent modulo 25, then 16^2 to which it is congruent modulo 125, etc.

102.

As for numbers divisible by p, their squares are clearly divisible by pp. So all numbers divisible by p but not by pp are nonresidues of p^n. In general, given a number $p^k A$ where A is not divisible by p, we must distinguish the following cases:

1) When $k =$ or $> n$, we have $p^k A \equiv 0 \,(\mathrm{mod.}\, p^n)$, a residue.

2) When $k < n$ and the exponent is odd, $p^k A$ is a nonresidue.

For if $p^k A = p^{2\kappa+1} A \equiv ss \,(\mathrm{mod.}\, p^n)$, then ss would be divisible by $p^{2\kappa+1}$, which is possible only if s is divisible by $p^{\kappa+1}$. But then ss would also be divisible by $p^{2\kappa+2}$, and therefore (since $2\kappa + 2$ is certainly no greater than n) so would $p^k A$, *that is,* $p^{2\kappa+1} A$. Thus A would be divisible by p, contrary to the hypothesis.

3) When $k < n$ and the exponent is even. Then $p^k A$ is a residue or a nonresidue of p^n according as A is a residue or a nonresidue of p. For when A is a residue of p, it is also a residue of p^{n-k}. If $A \equiv aa (\mathrm{mod.}\, p^{n-k})$, then $Ap^k \equiv aap^k \,(\mathrm{mod.}\, p^n)$, and aap^k is a square. But when A is a nonresidue of p, $p^k A$ cannot be a residue of p^n. For suppose $p^k A \equiv aa \,(\mathrm{mod.}\, p^n)$; then aa must be divisible by p^k. The quotient is a square congruent to A modulo p^{n-k}, and therefore also modulo p; *that is, A* would be a residue of p, contrary to the hypothesis.

103.

Since we excluded the case $p = 2$, we must now say something about it. When the modulus is 2, every number is a residue, and there are no nonresidues. When the modulus is 4, all odd numbers of the form $4k + 1$ are residues, and all those of the form $4k + 3$ are nonresidues. Finally, when the modulus is 8 or a higher power of 2, all odd numbers of the form $8k + 1$ are residues, and the others, those of the forms $8k + 3,\ 8k + 5,\ 8k + 7$, are nonresidues. The latter part of this proposition is clear, since the square of any odd number, whether of the form $4k + 1$ or $4k - 1$, has the form $8k + 1$. We prove the first part as follows.

1) If either the sum or the difference of two numbers is divisible by 2^{n-1}, their squares are congruent modulo 2^n. For if one is put $= a$, the other has the form $2^{n-1}h \pm a$, whose square is $\equiv aa \,(\mathrm{mod.}\, 2^n)$.

2) Every odd number that is a quadratic residue of 2^n is congruent to a square whose root is odd and $< 2^{n-2}$. Let aa be any square congruent to that number, and let $a \equiv \pm\alpha (\mathrm{mod.}\, 2^{n-1})$, with α no greater than half the modulus (Article 4). Then $aa \equiv \alpha\alpha$, so the given number is also $\equiv \alpha\alpha$. Both a and α are clearly odd, and $\alpha < 2^{n-2}$.

3) The squares of all odd numbers smaller than 2^{n-2} are incongruent modulo 2^n. For let r and s be two such numbers. If their squares were congruent modulo 2^n, then $(r - s)(r + s)$ would be divisible by 2^n (taking $r > s$). But the numbers $r - s,\ r + s$ clearly cannot both be divisible by 4; so if one is divisible only by 2, to make their product divisible by 2^n, the other would have to be divisible by 2^{n-1}. *Q. E. A.* since both are $< 2^{n-2}$.

4) Finally, reduce these squares to their *least positive residues.* We obtain 2^{n-3} distinct quadratic residues smaller than the modulus*), each of the form $8k+1$. But there are exactly 2^{n-3} numbers of the form $8k+1$ smaller than the modulus, so they must all occur among those residues. *Q. E. D.*

To find a square congruent to a given number of the form $8k+1$ modulo 2^n, we can use a method like that of Article 101; see also Article 88. — Finally, what we said in general in Article 102 also applies to even numbers.

104.

The following facts about the number of distinct values (*that is,* values incongruent modulo the given modulus) admitted by an expression such as $V = \sqrt{A}\,(\mathrm{mod.}\, p^n)$, when A is a residue of p^n, follow easily from what precedes. (As before, we assume that p is prime, and for brevity include the case $n = 1$ from the outset.) I. If A is not divisible by p, V has *one* value for $p = 2,\ n = 1$, namely $V \equiv 1$; *two* when p is odd, and also for $p = 2,\ n = 2$: if one is put $\equiv v$, the other is $\equiv -v$; *four* for $p = 2,\ n > 2$: if one is put $\equiv v$, the others are $\equiv -v,\ 2^{n-1} + v,\ 2^{n-1} - v$. II. If A is divisible by p but not by p^n, let the highest power of p dividing A be $p^{2\mu}$ (its exponent must clearly be even), and let $A = ap^{2\mu}$. All values of V are then clearly divisible by p^μ, and the quotients are values of the expression $V' = \sqrt{a}\,(\mathrm{mod.}\, p^{n-2\mu})$. So all distinct values of V are obtained by multiplying all values of the expression V' lying between 0 and $p^{n-\mu}$ by p^μ. They are therefore given by

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

where v stands in turn for all *distinct* values of the expression V'. Their number is thus $p^\mu,\ 2p^\mu$ or $4p^\mu$, according as the number of the latter values (by case I) is 1, 2 or 4. III. If A is divisible by p^n, put $n = 2m$ or $= 2m - 1$ according as it is even or odd. We readily see that all numbers divisible by p^m, and no others, are values of V. So all its distinct values are $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, and their number is p^{n-m}.

105.

There remains the case where the modulus m is composed of several primes. Let $m = abc\ldots$, where a, b, c, etc. denote distinct primes or powers of distinct primes. If n is a residue of m, then n is clearly also a residue of each of a, b, c, etc.; so n is certainly a nonresidue of m if it is a nonresidue of any of a, b, c, etc. Conversely, if n is a residue of each of a, b, c, etc., it is also a residue of their product m. For suppose $n \equiv A^2,\ B^2, C^2$, etc. modulo a, b, c, etc., respectively. Find a number N congruent to A, B, C, etc. modulo a, b, c, etc., respectively (Article 32). Then $n \equiv NN$ modulo all these moduli, and therefore modulo their product m. — We readily see that combining *any* value of A, or of the expression $\sqrt{n}\,(\mathrm{mod.}\, a)$, with *any* value of B, with *any* value of C, etc., gives a value of N, or of the expression $\sqrt{n}\,(\mathrm{mod.}\, m)$; that distinct combinations give distinct values of N; and that all the combinations give all the values. So the number of all distinct values of N equals the product of the numbers of values of A, B, C, etc., which we showed how to determine in the preceding article. — Furthermore, if one value of the expression $\sqrt{n}\,(\mathrm{mod.}\, m)$, or of

*) Since the number of odd numbers below 2^{n-2} is 2^{n-3}.

N, is known, it is also a value of all of A, B, C, etc. Since all the other values of these quantities can then be derived by the preceding article, all the other values of N can readily be obtained from one.

Example. Let the modulus be 315, and ask whether 46 is a residue or a nonresidue of it. The prime divisors of 315 are $3, 5, 7$, and 46 is a residue of each of them, so it is also a residue of 315. Furthermore, since $46 \equiv 1$ and $\equiv 64 (\text{mod. } 9)$; $\equiv 1$ and $\equiv 16 \,(\text{mod. } 5)$; $\equiv 4$ and $\equiv 25 \,(\text{mod. } 7)$, we find the roots of the squares to which 46 is congruent modulo 315: $19, 26, 44, 89, 226, 271, 289, 296$.

A general criterion for deciding whether a given number is a residue or a nonresidue of a given prime.

106.

It follows from what precedes that, if we can always decide whether a given *prime number* is a residue or a nonresidue of a *given prime*, all other cases can be reduced to this one. We must therefore make every effort to find reliable criteria for this case. Before starting that investigation, we give a criterion drawn from the previous section which, though of almost no practical use, deserves mention for its simplicity and generality.

Any number A not divisible by the prime $2m + 1$ is a residue or a nonresidue of that prime according as $A^m \equiv +1$ or $\equiv -1 \,(\text{mod. } 2m + 1)$.

For the modulus $2m + 1$, let the index of A in any system be a. Then a is even when A is a residue of $2m + 1$, and odd when A is a nonresidue. The index of A^m is ma, *that is,* $\equiv 0$ or $\equiv m \,(\text{mod. } 2m)$, according as a is even or odd. Thus A^m is $\equiv +1$ in the first case, and $\equiv -1 \,(\text{mod. } 2m + 1)$ in the second. See Articles 57 and 62.

Example. 3 is a residue of 13 because $3^6 \equiv 1 \,(\text{mod. } 13)$, while 2 is a nonresidue of 13 because $2^6 \equiv -1 \,(\text{mod. } 13)$.

But whenever the numbers to be tested are even moderately large, this criterion is quite useless because of the enormous amount of calculation.

Investigations of the primes for which given numbers are residues or nonresidues.

107.

Given a modulus, it is very easy to specify all the numbers that are its residues or nonresidues. Put that number $= m$. We must determine the squares whose roots do not exceed half of m, or numbers congruent to these squares modulo m (still quicker methods are available in practice). Then all numbers congruent to one of them modulo m are residues of m, and all numbers congruent to none of them are nonresidues. — But the inverse question, *given a number, to specify all numbers of which it is a residue or a nonresidue*, calls for a much deeper investigation. We will therefore examine this problem, on whose solution the one proposed in the preceding article depends, starting with the simplest cases.

The residue -1.

108.

THEOREM. *For every prime of the form* $4n+1$, -1 *is a quadratic residue; for every prime of the form* $4n+3$, *it is a nonresidue.*

Example. -1 is a residue of the numbers $5, 13, 17, 29, 37, 41, 53, 61.73, 89, 97$, etc., arising respectively from the squares of $2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22$, etc.; it is a nonresidue of the numbers $3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83$, etc.

We already mentioned this theorem in Article 64. Its proof follows easily from Article 106: for a prime of the form $4n+1$ we have $(-1)^{2n} \equiv 1$, and for one of the form $4n+3$ we have $(-1)^{2n+1} \equiv -1$. This proof agrees with the one given there. But the theorem is so elegant and useful that another proof will not be out of place.

109.

Denote the collection of all residues of the prime p that are smaller than p, excluding the residue 0, by the letter C. Their number is always $= \frac{p-1}{2}$, so it is even when p has the form $4n+1$, and odd when p has the form $4n+3$. As in Article 77, where we considered numbers in general, call residues *partners* when their product is $\equiv 1 \pmod{p}$; for if r is a residue, $\frac{1}{r} \pmod{p}$ is clearly a residue too. Since a residue cannot have more than one partner among the residues C, all the residues C can be divided into classes, each containing two partner residues. If no residue were its own partner, *that is,* if each class contained two *unequal* residues, the total number of residues would be twice the number of classes. But if some residues are their own partners, *that is,* if some classes contain only one residue, or, if preferred, the same residue twice, let the number of these classes be $= a$, and that of the remaining classes $= b$; then the number of all residues C is $= a + 2b$. So when p has the form $4n+1$, a is even; when p has the form $4n+3$, a is odd. But no numbers smaller than p other than 1 and $p-1$ can be their own partners (see Article 77), and the first, 1, certainly occurs among the residues. So in the first case $p-1$ (or, equivalently here, -1) must be a residue, and in the second a nonresidue; otherwise in the former case we would have $a = 1$, and in the latter $= 2$, which is impossible.

110.

This proof too is due to the distinguished Euler, who also first found the earlier one. See *Opusc. Anal. Vol. I, p. 135.* — It is easy to see that it rests on principles like those of our second proof of Wilson's theorem in Article 77. But if we assume that theorem, we can give an even easier proof. Among the numbers $1, 2, 3 \ldots p-1$ there are $\frac{p-1}{2}$ quadratic residues of p and just as many nonresidues; so the number of nonresidues is even when p has the form $4n+1$, and odd when p has the form $4n+3$. Thus the product of all the numbers $1, 2, 3 \ldots p-1$ is a residue in the first case and a nonresidue in the second (Article 99). But this product is always $\equiv -1 \pmod{p}$; so -1 too is a residue in the first case and a nonresidue in the second.

111.

So if r is a residue of a prime of the form $4n+1$, $-r$ is also a residue of that prime, while all the nonresidues of such a prime remain nonresidues when their signs are reversed[*)]. The opposite happens for primes of the form $4n+3$: reversing the sign turns residues into nonresidues and vice versa. See Article 98.

We also readily derive the general rule: -1 *is a residue of every number divisible neither by* 4 *nor by any prime of the form* $4n+3$*, and a nonresidue of every other number.* See Articles 103 and 105.

[*)]So when we speak of any number as a residue or a nonresidue of a number of the form $4n+1$, we can disregard its sign altogether, or even give it the double sign $\pm$.

The residues +2 and −2.

112.

We move on to the residues +2 and −2.

Collecting from Table II all the primes for which +2 is a residue gives $7, 17, 23, 31, 41, 47, 71, 73, 79.89, 97$. We readily notice that none of them have either the form $8n + 3$ or the form $8n + 5$.

Let us see whether we can turn this observed pattern into a certainty.

First, every composite number of the form $8n + 3$ or $8n + 5$ must have a prime factor of one of the forms $8n + 3$ or $8n + 5$. For primes of the forms $8n + 1$, $8n + 7$ alone can produce only numbers of the form $8n + 1$ or $8n + 7$. So if our observation holds in general, there is no number at all of the form $8n + 3$, $8n + 5$ for which +2 is a residue. Certainly no such number below 100 has +2 as a residue. If there are such numbers beyond this bound, let the smallest be $= t$. Then t has either the form $8n + 3$ or $8n + 5$; +2 is a residue of it, but a nonresidue of all smaller numbers of these forms. Put $2 \equiv aa \pmod{t}$. We can always choose a odd and $< t$ (for a has at least two positive values smaller than t whose sum is $= t$, so one is even and the other odd; see Articles 104 and 105). Then let $aa = 2 + tu$, or $tu = aa - 2$. Now aa has the form $8n + 1$, so tu has the form $8n - 1$, and u has the form $8n + 3$ or $8n + 5$, according as t has the latter or the former form. But the equation $aa = 2 + tu$ also gives $2 \equiv aa \pmod{u}$, *that is,* 2 is also a residue of u. We readily see that $u < t$, so t is not the smallest counterexample to our observation, contrary to the hypothesis. Thus the pattern we found by inspection holds in general.

Combining this with the proposition of Article 111 gives the following theorems.

I. *For every prime of the form* $8n + 3$, +2 *is a nonresidue and* −2 *a residue.*

II. *For every prime of the form* $8n + 5$, *both* +2 *and* −2 *are nonresidues.*

113.

Similarly, inspection of Table II gives the following primes for which −2 is a residue: $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$[*)]. None have the forms $8n + 5$, $8n + 7$; let us see whether this observation too can be established as a general theorem. As in the preceding article, every composite number of the form $8n + 5$ or $8n + 7$ has a prime factor of the form $8n + 5$ or $8n + 7$. So if our observation holds in general, −2 cannot be a residue of any number of the form $8n + 5$ or $8n + 7$. If such numbers exist, let the smallest be $= t$, and put $-2 = aa - tu$. Choose a odd and smaller than t, as above; then u has the form $8n + 5$ or $8n + 7$, according as t has the form $8n + 7$ or $8n + 5$. From $aa + 2 = tu$ and $a < t$ we readily find that u is also smaller than t. Finally, −2 is a residue of u too; *that is,* t is not the smallest counterexample to our observation, contrary to the hypothesis. So −2 must be a nonresidue of every number of the forms $8n + 5$, $8n + 7$.

Combining this with the proposition of Article 111 gives these theorems:

I. *For every prime of the form* $8n + 5$, *both* −2 *and* +2 *are nonresidues,* as we already found in the preceding article.

II. *For every prime of the form* $8n + 7$, −2 *is a nonresidue and* +2 *a residue.*

[*)] By considering −2 as the product of +2 and −1; see Article 111.

In both proofs we could also have chosen an even value of a. We would then have had to distinguish the case where a has the form $4n+2$ from the case where a has the form $4n$. The argument proceeds just as above, without any difficulty.

114.

One case remains: the prime has the form $8n+1$. The preceding method does not handle this case, which requires quite different devices.

For the prime modulus $8n+1$, let a be any primitive root. Then (Article 62) $a^{4n} \equiv -1 \pmod{8n+1}$. This congruence can also be written $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n+1}$, or $(a^{2n}-1)^2 \equiv -2a^{2n}$. So both $2a^{2n}$ and $-2a^{2n}$ are residues of $8n+1$. Since a^{2n} is a square not divisible by the modulus, both $+2$ and -2 are residues as well (Article 98).

115.

It will be useful to add another proof of this theorem, related to the preceding one as the second proof of the theorem of Article 108 (Article 109) is related to the first (Article 108). Readers familiar with these matters will then see more easily that neither pair of proofs is as different as it may seem at first sight.

I. For any prime modulus of the form $4m+1$, among the smaller numbers $1, 2, 3 \ldots 4m$, there are m that can be congruent to a fourth power, while the remaining $3m$ cannot.

This follows easily from the principles of the previous section, but a proof without them is not difficult either. We proved that, for such a modulus, -1 is always a quadratic residue. So let $ff \equiv -1$. If z is any number not divisible by the modulus, the fourth powers of the four numbers $+z, -z, +fz, -fz$ (which are clearly incongruent) are congruent to one another. The fourth power of a number congruent to none of these four cannot be congruent to their fourth powers: otherwise the congruence $x^4 \equiv z^4$, of the fourth degree, would have more than 4 roots, contrary to Article 43. Thus all the numbers $1, 2, 3, \ldots 4m$ give only m incongruent fourth powers; among those same numbers, m are congruent to them, and the rest cannot be congruent to any fourth power.

II. For a prime modulus of the form $8n+1$, -1 can be congruent to a fourth power (-1 is a *biquadratic residue* of that prime).

For the number of all biquadratic residues smaller than $8n+1$ (excluding zero) is $= 2n$, *that is,* even. Also, if r is a biquadratic residue of $8n+1$, it is easy to prove that the value of the expression $\frac{1}{r} \pmod{8n+1}$ is one too. So all the biquadratic residues can be divided into classes as we divided the quadratic residues in Article 109; the rest of the proof proceeds in exactly the same way as there.

III. Now let $g^4 \equiv -1$, and let h be the value of the expression $\frac{1}{g} \pmod{8n+1}$. Then

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

(because $gh \equiv 1$). But $g^4 \equiv -1$, so $-h^2 \equiv g^4 h^2 \equiv g^2$, and finally $g^2 + h^2 \equiv 0$ and $(g \pm h)^2 \equiv \pm 2$; *that is,* both $+2$ and -2 are quadratic residues of $8n+1$. *Q. E. D.*

116.

The preceding results also readily give this general rule: $+2$ *is a residue of every number divisible neither by* 4 *nor by any prime of the form* $8n+3$ *or* $8n+5$*; it is a nonresidue of all the others* (*for example,* all numbers of the forms $8n+3$, $8n+5$, whether prime or composite).

-2 *is a residue of every number divisible neither by* 4 *nor by any prime of the form* $8n+5$ *or* $8n+7$*, and a nonresidue of all the others.*

These elegant theorems were already known to the perceptive Fermat, *Op. Mathem., p.* 168. But he never communicated the proof he claimed to have. Later the distinguished Euler repeatedly sought it in vain; the distinguished Lagrange was the first to find a rigorous proof, *Nouv. Mém. de l'Ac. de Berlin*, 1775, *pp.* 349, 351. Euler seems still to have been unaware of this when he wrote the paper preserved in *Opusc. Analyt.*, Vol. I, p. 259.

The residues $+3$ *and* -3*.*

117.

We move on to the residues $+3$ and -3, starting with the latter.

From Table II we find the following primes for which -3 is a residue: 3, 7. 13, 19, 31, 37, 43, 61, 67, 73, 79, 97. None have the form $6n+5$. We prove as follows that there are no primes of this form for which -3 is a residue beyond the table's range either. First, every composite number of the form $6n+5$ must have a prime factor of the same form. As long as no primes of the form $6n+5$ have -3 as a residue, no such composite numbers occur either. If there are such numbers beyond the table's range, let the smallest be $= t$, and put $-3 = aa - tu$. Choosing a even and smaller than t, we have $u < t$, and -3 is a residue of u. If a has the form $6n \pm 2$, then tu has the form $6n+1$, so u has the form $6n+5$. *Q. E. A.* For we assumed that t was the smallest counterexample to our observation. If a has the form $6n$, then tu has the form $36n+3$, so $\frac{1}{3}tu$ has the form $12n+1$, and $\frac{1}{3}u$ has the form $6n+5$. But -3 is clearly also a residue of $\frac{1}{3}u$, and $\frac{1}{3}u < t$, *Q. E. A.* Thus -3 cannot be a residue of any number of the form $6n+5$.

Every number of the form $6n+5$ has either the form $12n+5$ or $12n+11$, the former being included in $4n+1$ and the latter in $4n+3$. So we obtain the following theorems:

I. *For every prime of the form* $12n+5$*, both* -3 *and* $+3$ *are nonresidues.*

II. *For every prime of the form* $12n+11$*,* -3 *is a nonresidue and* $+3$ *a residue.*

118.

From Table II we find the following numbers for which $+3$ is a residue: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97. None have the form $12n+5$ or $12n+7$. That no numbers at all of the forms $12n+5$, $12n+7$ have $+3$ as a residue can be proved in exactly the same way as in Articles 112, 113 and 117, so we omit this work. Comparing with Article 111 gives the theorems:

I. *For every prime of the form* $12n+5$*, both* $+3$ *and* -3 *are nonresidues* (as we already found in the preceding article).

II. *For every prime of the form* $12n+7$*,* $+3$ *is a nonresidue and* -3 *a residue.*

119.

This method gives no result for numbers of the form $12n + 1$, which therefore require special devices. Inspection readily suggests that $+3$ and -3 are residues of every prime of this form. We need only prove that -3 is a residue of such numbers, since then $+3$ must be one too (Article 111). We will prove more generally that -3 is a residue of every prime of the form $3n + 1$.

Let p be such a prime, and let a, for the modulus p, belong to the exponent 3 (such numbers exist by Article 54, since 3 divides $p - 1$). Then $a^3 \equiv 1 \,(\mathrm{mod.}\, p)$, *that is,* $a^3 - 1$, or $(a^2 + a + 1)(a - 1)$, is divisible by p. But a cannot be $\equiv 1 \,(\mathrm{mod.}\, p)$, since 1 belongs to the exponent 1. So $a - 1$ is not divisible by p, but $a^2 + a + 1$ is, and therefore so is $4aa + 4a + 4$; *that is,* $(2a + 1)^2 \equiv -3 \,(\mathrm{mod.}\, p)$, or -3 is a residue of p. *Q. E. D.*

This proof, which is independent of the preceding ones, also covers the primes of the form $12n + 7$ already dealt with in the preceding article.

We also note that this argument could be presented along the lines of the method used in Articles 109 and 115, but for brevity we do not pursue this.

120.

The preceding results readily give the following theorems (see Articles 102, 103 and 105).

I. -3 *is a residue of all numbers divisible neither by* 8, *nor by* 9, *nor by any prime of the form* $6n + 5$, *and a nonresidue of all the others.*

II. $+3$ *is a residue of all numbers divisible neither by* 4, *nor by* 9, *nor by any prime of the form* $12n + 5$ *or* $12n + 7$, *and a nonresidue of all the others.*

Keep this particular case especially in mind:

-3 is a *residue* of all primes of the form $3n + 1$, or equivalently *all those that are residues of* 3; it is a *nonresidue* of all primes of the form $6n + 5$, or, excluding 2, all those of the form $3n + 2$, *that is, all those that are nonresidues of* 3. All the other cases clearly follow from this.

The propositions concerning the residues $+3$ and -3 were already known to Fermat, *Opera Wallisii*, Vol. II, *p.* 857. But the distinguished Euler first gave proofs, *Comm. nov. Petr.*, Vol. VIII, *p.* 105 ff. It is all the more surprising that proofs of the propositions concerning the residues $+2$ and -2, based on entirely similar devices, always escaped his insight. See also the paper by the distinguished Lagrange, *Nouv. Mém. de l'Ac. de Berlin*, 1775, *p.* 352.

The residues +5 and −5.

121.

Inspection suggests that +5 is a nonresidue of every odd number of the form $5n+2$ or $5n+3$, *that is,* of every odd number that is a nonresidue of 5. We prove that this rule has no exceptions as follows. Let the smallest exception, if there is one, be $= t$. It is therefore a nonresidue of 5, while 5 is a residue of t. Let $aa = 5 + tu$, with a even and smaller than t. Then u is odd and smaller than t, and +5 is a residue of u. If a is not divisible by 5, neither is u. But tu is clearly a residue of 5, so, since t is a nonresidue of 5, u is a nonresidue too. *That is,* there is an odd nonresidue of 5, of which +5 is a residue, smaller than t, contrary to the hypothesis. If a is divisible by 5, put $a = 5b$ and $u = 5v$; then $tv \equiv -1 \equiv 4 \pmod 5$, *that is, tv* is a residue of 5. The rest of the proof proceeds as in the first case.

122.

Thus, for all primes that are nonresidues of 5 and have the form $4n + 1$, *that is,* all primes of the form $20n + 13$ or $20n + 17$, both +5 and −5 are nonresidues. For all primes of the form $20n + 3$ or $20n + 7$, +5 is a nonresidue and −5 a residue.

In just the same way we can prove that −5 is a nonresidue of all primes of the forms $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$. It follows that +5 is a residue of all primes of the form $20n + 11$ or $20n + 19$, and a nonresidue of all those of the form $20n + 13$ or $20n + 17$. Every prime except 2 and 5 (of which ±5 is a residue) has one of the forms $20n + 1, 3, 7, 9, 11, 13, 17, 19$, so we can now decide every case except those of the form $20n + 1$ or $20n + 9$.

123.

Inspection readily suggests that +5 and −5 are residues of all primes of the form $20n + 1$ or $20n + 9$. If this holds in general, we have the elegant law that +5 *is a residue of every prime that is a residue of 5* (these have one of the forms $5n + 1$ or $5n + 4$, or one of $20n + 1, 9, 11, 19$; the third and fourth of the latter have already been dealt with), *but a nonresidue of every odd number that is a nonresidue of 5*, as we proved above. This theorem is enough to decide whether +5 (and therefore −5, considered as the product of +5 and −1) is a residue or a nonresidue of any given number. Finally, note the analogy between this theorem and the one concerning the residue −3 in Article 120.

But proving this observed pattern is not so easy. For a prime of the form $20n + 1$, or more generally of the form $5n + 1$, we can proceed much as in Articles 114 and 119. For the modulus $5n+1$, let a be any number belonging to the exponent 5; such numbers exist by the previous section. Then $a^5 \equiv 1$, or $(a-1)(a^4+a^3+a^2+a+1) \equiv 0 \pmod{5n+1}$. Since we cannot have $a \equiv 1$, and therefore cannot have $a-1 \equiv 0$, we must have $a^4+a^3+a^2+a+1 \equiv 0$. Thus $4(a^4+a^3+a^2+a+1) = (2aa+a+2)^2-5a^2$ is also $\equiv 0$, *that is,* $5a^2$ is a residue of $5n + 1$, and so is 5, since a^2 is a residue not divisible by $5n + 1$ (for a is not divisible by $5n + 1$ because $a^5 \equiv 1$). *Q. E. D.*

The case of a prime of the form $5n + 4$, however, requires subtler methods. The propositions used to resolve it will be treated more generally later, so we touch on them only briefly here.

I. If p is a prime and b a given quadratic nonresidue of p, the value of the expression

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

(from whose expansion the irrationality clearly disappears) is always divisible by p, whatever number is substituted for x. Inspection of the coefficients in the expansion of A shows that all terms from the second to the next-to-last, inclusive, are divisible by p, so $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}$. Since b is a nonresidue of p, we have $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (Article 106), while x^p is always $\equiv x$ (previous section). So $A \equiv 0$. *Q. E. D.*

II. In the congruence $A \equiv 0 \pmod{p}$, the indeterminate x has degree p, and all the numbers $0, 1, 2....p-1$ are roots. Let e be a divisor of $p+1$. Then the expression

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

(which we denote by B) is free of irrationality when expanded, and the indeterminate x has degree $e-1$ in it. Elementary analysis tells us that A is divisible by B identically. I now say that there are $e-1$ values of x which, substituted into B, make B divisible by p. For put $A \equiv BC$. Then x in C has degree $p-e+1$, so the congruence $C \equiv 0 \pmod{p}$ has at most $p-e+1$ roots. Thus all the remaining numbers among $0, 1, 2, 3....p-1$, whose number is $= e-1$, are roots of the congruence $B \equiv 0$.

III. Now let p have the form $5n+4$, let $e = 5$, let b be a nonresidue of p, and determine a so that

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

is divisible by p. This expression becomes

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

So $(b+5aa)^2 - 20a^4$ too is divisible by p, *that is,* $20a^4$ is a residue of p. Since $4a^4$ is a residue not divisible by p (we readily see that a cannot be divisible by p), 5 is also a residue of p. *Q. E. D.*

Thus the theorem stated at the beginning of this article holds in general. —

We also note that the proofs for both cases are due to the distinguished Lagrange, *Mém. de l'Ac. de Berlin*, 1775, *p.* 352 ff.

On ± 7.

124.

By a similar method we prove that

-7 *is a nonresidue of every number that is a nonresidue of* 7.

Inspection suggests, on the other hand, that

-7 *is a residue of every prime that is a residue of* 7.

But no one has yet proved this rigorously. For those residues of 7 that have the form $4n-1$, the proof is easy: a method already familiar from what precedes shows that $+7$ is always a nonresidue of such primes, and so -7 a residue. But this gains us little, since the remaining cases cannot be treated by this method. We can handle one more case much as in Articles 119, 123. If p is a prime of the form $7n+1$, and a, for the modulus p, belongs to the exponent 7, then

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

is clearly divisible by p, so $-7(a^2+a)^2$ is a residue of p. But $(a^2+a)^2$, being a square, is a residue of p, and is not divisible by p. For since a is assumed to belong to the exponent 7, it can be neither $\equiv 0$ nor $\equiv -1 \pmod{p}$; *that is,* neither a nor $a+1$ is divisible by p, and neither is the square $(a+1)^2a^2$. Thus 7 too is clearly a residue of p. *Q. E. D.* — But primes of the form $7n+2$ or $7n+4$ resist all the methods given so far. This proof too was first found by the distinguished Lagrange at the cited place. — In Section VII below we will show in general that the expression $\frac{4(x^p-1)}{x-1}$ can always be reduced to the form $X^2 \mp pY^2$ (taking the upper sign when p is a prime of the form $4n+1$, and the lower when it has the form $4n+3$), where X, Y denote rational functions of x, free of fractions. Lagrange did not carry out this decomposition beyond the case $p=7$; see the cited place, p. 352.

Preparation for the general investigation.

125.

The preceding methods do not suffice to establish general proofs, so it is time to present another that is free of this defect. We begin with a theorem whose proof eluded our efforts for quite some time, although at first sight it seems so obvious that some have not even seen the need for a proof. It is this: *Every number, except squares taken positively, is a nonresidue of some primes.* We will use this theorem only as an aid in proving others, so we treat here only the cases needed for that purpose. The remaining cases will follow of their own accord later. We will therefore show that *every prime of the form* $4n+1$*, taken either positively or negatively*[*)], *is a nonresidue of some primes*, and, if > 5, of primes smaller than itself.

First, suppose the prime p, of the form $4n+1$ (> 17; but $-13\,N3$, $-17\,N5$), is to be taken *negatively.* Let $2a$ be the even number immediately greater than $\sqrt{p}$. We readily see that $4aa$ is always $< 2p$, or $4aa - p < p$. Now $4aa-p$ has the form $4n+3$,

[*)] The need to exclude $+1$ is clear.

and $+p$ is a quadratic residue of $4aa - p$ (since $p \equiv 4aa \pmod{4aa - p}$). If $4aa - p$ is prime, $-p$ is therefore a nonresidue of it. If not, $4aa - p$ must have a factor of the form $4n + 3$; since $+p$ must be a residue of this factor too, $-p$ is a nonresidue of it. *Q. E. D.*

For primes taken *positively*, we distinguish two cases. *First*, let p be a prime of the form $8n + 5$. Let a be any positive number $< \sqrt{\frac{1}{2}p}$. Then $8n + 5 - 2aa$ is a positive number of the form $8n + 5$ or $8n + 3$, according as a is even or odd. It must therefore be divisible by a prime of the form $8n + 3$ or $8n + 5$, since a product of any number of factors of the forms $8n + 1$ and $8n + 7$ cannot have either the form $8n + 3$ or $8n + 5$. Let this prime be q; then $8n + 5 \equiv 2a^2 \pmod{q}$. But 2 is a nonresidue of q (Article 112), and therefore so are $2a^{2*)}$ and $8n + 5$. *Q. E. D.*

126.

But that every prime of the form $8n + 1$, taken positively, is a nonresidue of some smaller prime cannot be proved by such obvious devices. This truth is of the greatest importance, so we cannot pass over a rigorous proof, even though it is somewhat long. We first give the following

LEMMA. *Suppose two sequences of numbers*

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

(whether they have the same number of terms does not matter) *are such that, for any prime or prime power p dividing a term of the second sequence, or several terms, at least as many terms of the first sequence are divisible by p as of the second. Then I say that the product of all the numbers* (I) *is divisible by the product of all the numbers* (II).

Example. Let (I) consist of $12, 18, 45$ and (II) of $3, 4, 5, 6, 9$. Then the numbers of terms divisible by $2, 4, 3, 9, 5$ are respectively $2, 1, 3, 2, 1$ in (I) and $2, 1, 3, 1, 1$ in (II). The product of all terms of (I), $= 9720$, is divisible by the product of all terms of (II), 3240.

Proof. Let the product of all terms of (I) be $= Q$, and that of all terms of sequence (II) $= Q'$. Any prime divisor of Q' clearly also divides Q. We now show that every prime factor of Q' occurs in Q with an exponent at least as large as in Q'. Let p be such a divisor, and suppose that sequence (I) has a terms divisible by p, b terms divisible by p^2, c terms divisible by p^3, etc. Let a', b', c', etc. have analogous meanings for sequence (II). We readily see that p occurs in Q with exponent $a + b + c+$, etc., and in Q' with exponent $a' + b' + c'+$, etc. But a' is no greater than a, b' no greater than b, etc., by hypothesis; so $a' + b' + c'$, etc. is certainly not $> a + b + c$, etc. — Thus no prime can have a larger exponent in Q' than in Q, so Q is divisible by Q' (Article 17). *Q. E. D.*

*)Article 98. For a^2 is clearly a residue of q not divisible by q; otherwise the prime p too would be divisible by q. *Q. E. A.*

127.

LEMMA. *The progression* $1, 2, 3, 4, ...n$ *cannot have more terms divisible by any number* h *than the progression* $a, a+1, a+2.....a+n-1$*, which has the same number of terms.*

If n is a multiple of h, both progressions clearly have $\frac{n}{h}$ terms divisible by h. Otherwise, put $n = eh + f$, with $f < h$. The first sequence then has e terms divisible by h, and the second either just as many or $e + 1$.

As a corollary we obtain the proposition known from the theory of figurate numbers, but, unless we are mistaken, never yet proved directly, that

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

is always an integer.

Finally, the lemma could have been stated more generally as follows:

In the progression $a, a+1, a+2, ...a+n-1$, there are at least as many terms congruent modulo h to any given number r as there are in $1, 2, 3....n$ divisible by h.

128.

THEOREM. *Let* a *be any number of the form* $8n+1$*, let* p *be any number coprime to* a *of which* $+a$ *is a residue, and finally let* m *be arbitrary. Then I say that the progression*

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

according as m *is even or odd, has at least as many terms divisible by* p *as the progression*

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

We denote the first progression by (I) and the second by (II).

Proof. I. When $p = 2$, all terms of (I) except the first, *that is,* m terms, are divisible; there are just as many in (II).

II. Let p be odd, or twice or four times an odd number, and let $a \equiv rr \pmod{p}$. Then the progression $-m, -(m-1), -(m-2), ... + m$ (which has as many terms as (II) and will be denoted by (III)) has at least as many terms congruent modulo p to r as sequence (II) has terms divisible by p (preceding article). No two of them can differ only in sign and not in magnitude[*)]. Finally, each has a corresponding term of (I) divisible by p. For if $\pm b$ is a term of (III) congruent to r modulo p, then $a - bb$ is divisible by p. If b is even, the term $2(a - bb)$ of (I) is divisible by p. If b is odd, the term $\frac{1}{2}(a - bb)$ is divisible by p: for $\frac{a-bb}{p}$ is clearly an *even* integer, since $a - bb$ is divisible by 8, while the highest power of two dividing p is at most 4 (by hypothesis a has the form $8n + 1$, and bb, as the square of an odd number, has the same form,

[*)] For if $r \equiv -f \equiv +f \pmod{p}$, $2f$ would be divisible by p, and therefore so would $2a$ (because $ff \equiv a \pmod{p}$). This is possible only if $p = 2$, since a is coprime to p by hypothesis. But we have already treated this case separately.

so their difference has the form $8n$). Thus sequence (I) has as many terms divisible by p as (III) has terms congruent to r modulo p, *that is,* at least as many as (II) has terms divisible by p. *Q. E. D.*

III. Let p have the form $8n$, and let $a \equiv rr \pmod{2p}$. We readily see that a, being a residue of p by hypothesis, is also a residue of $2p$. Then sequence (III) has at least as many terms congruent to r modulo p as (II) has terms divisible by p, and all of them differ in magnitude. But each has a corresponding term of (I) divisible by p. For if $+b$ or $-b \equiv r \pmod{p}$, then $bb \equiv rr \pmod{2p}$[†], so the term $\frac{1}{2}(a - bb)$ is divisible by p. Thus (I) has at least as many terms divisible by p as (II). *Q. E. D.*

129.

THEOREM. *If a is a prime of the form $8n + 1$, then below $2\sqrt{a} + 1$ there must be a prime of which a is a nonresidue.*

Proof. Suppose, if possible, that a is a residue of all primes smaller than $2\sqrt{a} + 1$. Then a is also a residue of all composite numbers smaller than $2\sqrt{a} + 1$ (compare the rules for deciding whether a number is a residue of a composite number, Article 105). Let the integer immediately below $\sqrt{a}$ be $= m$. Then the sequence

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

has at least as many terms divisible by any number smaller than $2\sqrt{a} + 1$ as the sequence

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

So the product of all terms of (I) is divisible by the product of all terms of (II) (Article 126). But the former is either $= a(a-1)(a-4)....(a-mm)$ or half this product, according as m is even or odd. Thus the product $a(a-1)(a-4)....(a-mm)$ is certainly divisible by the product of all terms of (II); and since all these terms are coprime to a, this remains true when the factor a is omitted. But the product of all terms of (II) can also be written

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

So

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

is an integer, even though it is a product of fractions smaller than one. For $\sqrt{a}$ must be irrational, so $m+1 > \sqrt{a}$, and therefore $(m+1)^2 > a$. Thus our assumption is impossible. *Q. E. D.*

Since a is certainly > 9, we have $2\sqrt{a} + 1 < a$, so there is a prime $< a$ of which a is a nonresidue.

[†]For $bb - rr = (b-r)(b+r)$ is a product of two factors, one divisible by p by hypothesis, the other by 2 (since both b and r are odd); so $bb - rr$ is divisible by $2p$.

A general (fundamental) theorem is established by examining cases, and conclusions are drawn from it.

130.

Having rigorously proved that every prime of the form $4n+1$, taken both positively and negatively, is a nonresidue of some smaller prime, we now turn to a more exact and general comparison of primes, according to whether one is a residue or nonresidue of another.

We have rigorously proved above that -3 and $+5$ are residues or nonresidues of all primes that are respectively residues or nonresidues of $3, 5$.

Examining the following numbers shows that -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59, etc., are residues or nonresidues of all primes that, taken positively, are respectively residues or nonresidues of those primes. This examination is very easy with the help of Table II.

Anyone paying a little attention will notice that, among these primes, those of the form $4n + 1$ carry a positive sign, while those of the form $4n + 3$ carry a negative sign.

131.

We will soon prove that what we have found here by examining cases holds generally. Before taking up that task, however, we must work out everything that follows from the theorem if it is assumed true. We state the theorem itself as follows.

If p is a prime of the form $4n + 1$, then $+p$ (or, if p has the form $4n + 3$, then $-p$) is a residue or nonresidue of every prime that, taken positively, is a residue or nonresidue of p.

Since almost everything that can be said about quadratic residues rests on this theorem, the name *fundamental theorem*, which we will use from now on, is quite appropriate.

To present our reasoning as briefly as possible, we will use a, a', a'', etc., for primes of the form $4n + 1$, and b, b', b'', etc., for primes of the form $4n + 3$; A, A', A'', etc., for any numbers of the form $4n + 1$, and B, B', B'', etc., for any numbers of the form $4n + 3$. Finally, the letter R between two quantities will indicate that the first is a residue of the second, while the letter N will have the opposite meaning. *For example,* $+5R11$, $\pm 2N5$ will mean that $+5$ is a residue of 11, and $+2$ or -2 is a nonresidue of 5. Combining the fundamental theorem with the theorems of Article 111 now gives the following propositions easily.

	If		then
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.

These contain every case arising from the comparison of two primes. The following propositions concern any numbers, but their proofs are less immediate.

	If		then
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.	$-bRB$	. . . .	$\left\{\begin{array}{l}+BRb\\-BNb\end{array}\right.$

Since the proofs of all these propositions must be drawn from the same principles, we need not develop them all. The proof of Proposition 9, which we give, can serve as an example. First, observe that every number of the form $4n+1$ has either no factor of the form $4n+3$, or two, or four, etc.; *that is,* the number of such factors (which may include equal ones) is always even. Every number of the form $4n+3$, however, contains an odd number of factors of the form $4n+3$ (*that is,* either one, or three, or five, etc.). The number of factors of the form $4n+1$ remains undetermined.

Proposition 9 is proved as follows. Let A be the product of the prime factors a', a'', a''', etc., b, b', b'', etc. The number of factors b, b', b'', etc., will be even (there may also be none, which amounts to the same thing). Now, if a is a residue of A, it is also a residue of all the factors a', a'', a''', etc., b, b', b'', etc. So, by Propositions $1, 3$ of the preceding article, each of these factors is a residue of a, and so is their product

A. The same must hold for $-A$. — If, however, $-a$ is a residue of A, and therefore of all the factors a', a'', etc., b, b', etc., each of a', a'', etc., will be a residue of a, but each of b, b', etc., a nonresidue. Since the number of the latter is even, the product of all the factors, *that is,* A, will be a residue of a, and so will $-A$.

133.

Let us make the investigation still more general. Consider any two coprime odd numbers, with any signs, P and Q. Think of P as resolved into its prime factors without regard to its sign, and let p denote how many of these have Q as a nonresidue. If a prime of which Q is a nonresidue occurs several times among the factors of P, it must also be counted several times. Similarly, let q be the number of prime factors of Q of which P is a nonresidue. The numbers p, q will then have a certain relation to each other, depending on the nature of the numbers P, Q. Specifically, if one of p, q is even or odd, the forms of the numbers P, Q will tell us whether the other is even or odd. The following table presents this relation.

p, q will be both even or both odd when the numbers P, Q have the forms:

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

In contrast, one of the numbers p, q will be even and the other odd when the numbers P, Q have the forms:

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

Example. Let the given numbers be -55 and $+1197$, which belong to the fourth case. Now 1197 is a nonresidue of one prime factor of 55. That factor is the number 5, while -55 is a nonresidue of three prime factors of 1197, namely the numbers $3, 3, 19$.

If P and Q denote primes, these propositions reduce to those given in Article 131. In this case p and q cannot be greater than 1, so if p is assumed even, it must be $= 0$, *that is,* Q is a residue of P; if p is odd, Q is a nonresidue of P. And conversely. Thus, writing a, b in place of A, B, we obtain from 8 that if $-a$ is a residue or nonresidue of b, then $-b$ is a nonresidue or residue of a, which agrees with 3 and 4 of Article 131.

In general, however, Q can be a residue of P only if $p = 0$. So if p is odd, Q is certainly a nonresidue of P.

*) Let $l = 1$ if both $P, Q \equiv 3 \pmod 4$, otherwise $l = 0$
$m = 1$ if both P, Q are negative, otherwise $m = 0$
Then the relation depends on $l + m$.

The propositions of the preceding article can also be derived from this without difficulty.

We will soon see, moreover, that this general presentation is more than sterile speculation, since a complete proof of the fundamental theorem could hardly be carried out without it.

134.

We now turn to the deduction of these propositions.

I. As before, think of P as resolved into its prime factors, ignoring signs, and also resolve Q into factors in any way, but taking account of the sign of Q. Pair each of the former factors with each of the latter. If s denotes the number of all pairs in which the factor of Q is a nonresidue of the factor of P, then p and s will be both even or both odd. For let the prime factors of P be f, f', f'', etc., and among the factors into which Q has been resolved, let there be m that are nonresidues of f, m' nonresidues of f', m'' nonresidues of f'', etc. It is then easy to see that

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

while p expresses how many of the numbers m, m', m'', etc., are odd. It follows at once that s is even when p is even, and odd when p is odd.

II. This holds generally, however Q is resolved into factors. Let us turn to particular cases. First, consider the cases where one of the numbers, P, is positive, while the other, Q, has either the form $+A$ or the form $-B$. Resolve P, Q into their prime factors. Give every factor of P a positive sign, and every factor of Q a positive or negative sign according to whether it has the form a or b. Then Q will clearly have either the form $+A$ or $-B$, as required. Pair each factor of P with each factor of Q, and let s, as before, denote the number of pairs in which the factor of Q is a nonresidue of the factor of P. Similarly, let t denote the number of pairs in which the factor of P is a nonresidue of the factor of Q. The fundamental theorem shows that these two sets of pairs are identical, so $s = t$. Finally, what we have just proved gives $p \equiv s \pmod 2$, $q \equiv t \pmod 2$, and therefore $p \equiv q \pmod 2$.

We thus have Propositions $1, 3, 4$ and 6 of Article 133.

The remaining propositions can be obtained directly by a similar method, but require one new consideration. It is easier to derive them from the preceding results as follows.

III. Again, let P, Q denote any two coprime odd numbers, and p, q the numbers of prime factors of P, Q of which Q, P, respectively, are nonresidues. Finally, let p' be the number of prime factors of P of which $-Q$ is a nonresidue (when Q itself is negative, $-Q$ clearly denotes a positive number). Divide all the prime factors of P into four classes:

1) Factors of the form a of which Q is a residue.

2) Factors of the form b of which Q is a residue. Let their number be χ.

3) Factors of the form a of which Q is a nonresidue. Let their number be ψ.

4) Factors of the form b of which Q is a nonresidue. Their number $= \omega$.

We then easily see that $p = \psi + \omega$, $p' = \chi + \psi$.

Now, when P has the form $\pm A$, $\chi + \omega$, and therefore also $\chi - \omega$, is even. So $p' = p + \chi - \omega \equiv p \,(\text{mod. } 2)$. When P has the form $\pm B$, a similar argument shows that the numbers p, p' are incongruent modulo 2.

IV. Let us apply this to the individual cases. First, let both P and Q have the form $+A$. By Proposition 1, we have $p \equiv q \,(\text{mod. } 2)$; but $p' \equiv p \,(\text{mod. } 2)$, so also $p' \equiv q \,(\text{mod. } 2)$. This agrees with Proposition 2. — Similarly, let P have the form $-A$. With Q of the form $+A$, we have $p \equiv q \,(\text{mod. } 2)$ by Proposition 2, which we have just proved. From this, since $p' \equiv p$, we get $p' \equiv q$. Proposition 5 is therefore proved as well.

In the same way, Proposition 7 follows from 3; Proposition 8 from either 4 or 7; Proposition 9 from 6; and Proposition 10 from the same proposition.

Rigorous proof of the fundamental theorem.

135.

The preceding article did not prove the propositions of Article 133, but showed that their truth depends on the truth of the fundamental theorem, which we assumed for the time being. The method of deduction itself, however, shows that they hold for the numbers P, Q as long as the fundamental theorem holds when all the prime factors of these numbers are compared with one another, even if it does not hold generally. We now turn to the proof of the fundamental theorem itself, beginning with the following explanation.

We will say that the fundamental theorem is true up to a number M if it holds for any two primes neither of which exceeds M.

The same meaning applies when we say that the theorems of Articles 131, 132, 133 are true up to some bound. It is easy to see that if the fundamental theorem is known to be true up to a bound, these propositions will also hold up to that same bound.

136.

Checking the small numbers easily confirms the fundamental theorem and gives a bound up to which it certainly holds. We assume that this check has been made, but it does not matter how far we have taken it. It would even suffice to have confirmed it only up to the number 5, and this requires just the single observation that $+5N3$, $\pm 3N5$.

Now, if the fundamental theorem is not true generally, there will be some bound T up to which it holds, but it will no longer hold up to the next number, $T+1$. This is the same as saying that there are two primes, the larger of which is $T+1$, whose comparison contradicts the fundamental theorem, while any other two primes, provided both are smaller than $T+1$, agree with it. So the propositions of Articles 131, 132, 133 also hold up to T. We will now show that this supposition is impossible. We must distinguish the following cases according to the forms of $T+1$ and of the smaller prime, less than $T+1$, which we have supposed contradicts the theorem when compared with $T+1$. We denote that prime by p.

When both $T+1$ and p have the form $4n+1$, the fundamental theorem could fail in two ways, namely if we had simultaneously *either*

$$\begin{array}{rccc} & \pm pR(T+1) & \text{and} & \pm(T+1)Np \\ \textit{or, simultaneously} & \pm pN(T+1) & \text{and} & \pm(T+1)Rp \end{array}$$

When both $T+1$ and p have the form $4n+3$, the fundamental theorem would fail if we had simultaneously *either*

$$\begin{array}{rccc} & +pR(T+1) & \text{and} & -(T+1)Np \\ \text{(or, equivalently} & -pN(T+1) & \text{and} & +(T+1)Rp) \\ \textit{or} & +pN(T+1) & \text{and} & -(T+1)Rp \\ \text{(or} & -pR(T+1) & \text{and} & +(T+1)Np) \end{array}$$

When $T+1$ has the form $4n+1$, but p has the form $4n+3$, the fundamental theorem would fail if we had *either*

$$\begin{array}{rl} & \pm pR(T+1) \text{ and } +(T+1)Np \text{ (or } -(T+1)Rp) \\ \textit{or} & \pm pN(T+1) \text{ and } -(T+1)Np \text{ (or } +(T+1)Rp) \end{array}$$

When $T+1$ has the form $4n+3$, but p has the form $4n+1$, the fundamental theorem would fail if we had *either*

$$\begin{array}{rl} & +pR(T+1) \text{ (or } -pN(T+1)) \text{ and } \pm(T+1)Np \\ \textit{or} & +pN(T+1) \text{ (or } -pR(T+1)) \text{ and } \pm(T+1)Rp \end{array}$$

If we can prove that none of these eight cases can occur, we will also be certain that the truth of the fundamental theorem is not restricted by any bound. We now take up this task. But since some of these cases depend on others, we cannot keep the order in which we have listed them here.

137.

First case. When $T+1$ has the form $4n+1$ $(=a)$, and p has the same form, and moreover $\pm pRa$, we cannot have $\pm aNp$. This was the first case above.

Let $+p \equiv e^2 (\text{mod. } a)$, with e even and $< a$ (which can always be arranged). We must now distinguish two cases.

I. When e is not divisible by p, put $e^2 = p + af$. Then f is positive, of the form $4n+3$ (or of the form B), $< a$, and not divisible by p. Also $e^2 \equiv p (\text{mod. } f)$, *that is,* pRf, and therefore, by Proposition 11 of Article 132, $\pm fRp$ (since $p, f < a$, these propositions hold for them). But we also have $afRp$, so $\pm aRp$ as well.

II. When e is divisible by p, put $e = gp$, and $e^2 = p + aph$, or $pg^2 = 1 + ah$. Then h has the form $4n+3$ (B), and is coprime to p and g^2. Also pg^2Rh, and therefore pRh, which by Proposition 11 of Article 132 gives $\pm hRp$. But we also have $-ahRp$, because $-ah \equiv 1 (\text{mod. } p)$, so $\mp aRp$ as well.

138.

Second case. When $T+1$ has the form $4n+1$ $(=a)$, p the form $4n+3$, and $\pm pR(T+1)$, we cannot have $+(T+1)Np$, or $-(T+1)Rp$. This was the fifth case above.

As above, let $e^2 = p + fa$, with e even and $< a$.

I. When e is not divisible by p, f is not divisible by p either. Moreover, f is positive, of the form $4n+1$ (or A), and $< a$. We have $+pRf$, and therefore $+fRp$ (Proposition 10 of Article 132). But we also have $+faRp$, so $+aRp$, or $-aNp$.

II. When e is divisible by p, let $e = pg$, and $f = ph$. Then $g^2p = 1 + ha$. Now h is positive, of the form $4n+3$ (B), and coprime to p and g^2. Also $+g^2pRh$, and therefore $+pRh$, which gives $-hRp$ (Proposition 13 of Article 132). But $-haRp$, so $+aRp$ and $-aNp$.

139.

Third case. When $T+1$ has the form $4n+1$ $(=a)$, p the same form, and $\pm pNa$, we cannot have $\pm aRp$. (The second case above.)

Take a prime smaller than a of which $+a$ is a nonresidue; we proved above that such primes exist (Articles 125, 129). We must consider two cases separately, according to whether this prime has the form $4n+1$ or $4n+3$, since it has not been proved that such primes exist in *both* forms.

I. Let this prime have the form $4n+1$ and be $= a'$. Then $\pm a'Na$ (Article 131), and therefore $\pm a'pRa$. So let $e^2 \equiv a'p \pmod{a}$, with e even and $< a$. We must now distinguish four cases again.

1) When e is divisible by neither p nor a', put $e^2 = a'p \pm af$, taking the signs so that f is positive. Then $f < a$, and it is coprime to a' and p; for the upper sign it has the form $4n+3$, and for the lower sign the form $4n+1$. For brevity, let $[x,y]$ denote the number of prime factors of the number y of which x is a nonresidue. Then $a'pRf$, and therefore $[a'p,f]=0$. So $[f,a'p]$ is even (Propositions 1, 3 of Article 133), *that is,* either $=0$ or $=2$. Thus f is a residue of either both the numbers a',p or neither. The former is impossible, since $\pm af$ is a residue of a', and $\pm aNa'$ by hypothesis; this gives $\pm fNa'$. So f must be a nonresidue of both the numbers a',p. But since $\pm afRp$, we have $\pm aNp$. *Q. E. D.*

2) When e is divisible by p but not by a', let $e=gp$, and $g^2p = a' \pm ah$, choosing the sign so that h is positive. Then $h<a$, and it is coprime to a',g and p; for the upper sign it has the form $4n+3$, and for the lower sign the form $4n+1$. From the equation $g^2p = a' \pm ah$, on multiplying by p and a', we easily deduce $pa'Rh\ldots..(\alpha)$; $\pm ahpRa'\ldots.(\beta)$; $aa'hRp\ldots..(\gamma)$. From (α) follows $[pa',h]=0$, and therefore (Propositions 1, 3 of Article 133) $[h,pa']$ is even, *that is,* h is a nonresidue of either both p,a' or neither. *In the former case,* (β) gives $\pm apNa'$, and since $\pm aNa'$ by hypothesis, we have $\pm pRa'$. The fundamental theorem, which holds for the numbers p,a' smaller than $T+1$, then gives $\pm a'Rp$. From this and hNp, by (γ) we obtain $\pm aNp$. *Q. E. D. In the latter case,* (β) gives $\pm apRa'$, then $\pm pNa'$, $\pm a'Np$, and finally, together with hRp, by (γ) we obtain $\pm aNp$. *Q. E. D.*

3) When e is divisible by a' but not by p, the proof proceeds almost exactly as in the preceding case. It will present no difficulty to anyone who has understood that case thoroughly.

4) When e is divisible by both a' and p, and therefore also by their product $a'p$ (we assume the numbers a',p to be *unequal*, since otherwise what we are trying to prove, namely aNp, would already be contained in the hypothesis aNa'), let $e=ga'p$, and $g^2a'p = 1 \pm ah$. Then $h<a$, and it is coprime to a' and p; for the upper sign it has the form $4n+3$, and for the lower sign the form $4n+1$. It is easy to see that the following can be deduced from this equation: $a'pRh\ldots.(\alpha)$; $\pm ahRa'\ldots.(\beta)$; $\pm ahRp\ldots.(\gamma)$. From (α), which agrees with (α) in (2), we find as there that either hRp, hRa' hold simultaneously, or hNp, hNa'. But in the former case, (β) would give aRa', contrary to the hypothesis. So hNp, and therefore by (γ) also aNp.

II. When this prime has the form $4n+3$, the proof is so similar to the preceding one that we thought it unnecessary to give it. For those eager to work it out for themselves (which we strongly recommend), we only note that, after reaching an equation such

as $e^2 = bp \pm af$ (where b denotes that prime), it will make the argument clearer to consider the two signs separately.

140.

Fourth case. When $T+1$ has the form $4n+1$ $(= a)$, p the form $4n+3$, and $\pm pNa$, we cannot have $+aRp$, or $-aNp$. (The sixth case above.)

Since its proof is exactly like the proof of the third case, we omit its proof too for brevity.

141.

Fifth case. When $T+1$ has the form $4n+3$ $(= b)$, p the same form, and $+pRb$, or $-pNb$, we cannot have $+bRp$, or $-bNp$. (The third case above.)

Let $p \equiv e^2 \pmod{b}$, with e even and $< b$.

I. When e is not divisible by p, put $e^2 = p + bf$. Then f is positive, of the form $4n+3$, $< b$, and coprime to p. Also pRf, and therefore, by Proposition 13 of Article 132, $-fRp$. From this and $+bfRp$ we get $-bRp$, and therefore $+bNp$. *Q. E. D.*

II. When e is divisible by p, let $e = pg$, and $ggp = 1 + bh$. Then h has the form $4n+1$ and is coprime to p; $p \equiv g^2p^2 \pmod{h}$, and therefore pRh. This gives $+hRp$ (Proposition 10 of Article 132), which together with $-bhRp$ yields $-bRp$, or $+bNp$. *Q. E. D.*

142.

Sixth case. When $T+1$ has the form $4n+3$ $(= b)$, p the form $4n+1$, and pRb, we cannot have $\pm bNp$. (The seventh case above.)

We omit the proof, which is exactly like the preceding one.

143.

Seventh case. When $T+1$ has the form $4n+3$ $(= b)$, p the same form, and $+pNb$, or $-pRb$, we cannot have $+bNp$, or $-bRp$. (The fourth case above.)

Let $-p \equiv e^2 \pmod{b}$, with e even and $< b$.

I. When e is not divisible by p, let $-p = e^2 - bf$. Then f is positive, of the form $4n+1$, coprime to p, and smaller than b (for e is certainly no greater than $b-1$, and $p < b-1$, so $bf = e^2 + p < b^2 - b$, *that is,* $f < b-1$). Also $-pRf$, which gives $+fRp$ (Proposition 10 of Article 132); from this and $+bfRp$ we get $+bRp$, or $-bNp$.

II. When e is divisible by p, let $e = pg$, and $g^2p = -1 + bh$. Then h is positive, of the form $4n+3$, coprime to p, and $< b$. Also $-pRh$, which gives $+hRp$ (Proposition 14 of Article 132). From this and $bhRp$ follows $+bRp$, or $-bNp$. *Q. E. D.*

144.

Eighth case. When $T+1$ has the form $4n+3$ $(= b)$, p the form $4n+1$, and $+pNb$, or $-pRb$, we cannot have $\pm bRp$. (The last case above.)

The proof proceeds just as in the preceding case.

An analogous method for proving the theorem of Article 114.

145.

In the preceding proofs we always took an even value for e (Articles 137 .. 144). An odd value could also have been used, but we would then have had to introduce further distinctions. Those who enjoy these investigations will find it useful to try working out these cases for themselves. We would also then have had to assume the theorems concerning the residues $+2$ and -2. But since our proof was completed without these theorems, it gives us a new method of proving them. This is worth something, since the methods we used above to prove that ± 2 is a residue of every prime of the form $8n+1$ may seem less direct. We will assume that the remaining cases (concerning primes of the forms $8n+3$, $8n+5$, $8n+7$) have been proved by the methods given above, and that this theorem has only been found by examining examples. The following reasoning will turn this evidence into certainty.

If ± 2 were not a residue of all primes of the form $8n+1$, let the smallest prime of this form of which ± 2 is a nonresidue be $= a$, so that the theorem holds for all primes smaller than a. Then take a prime $< \frac{1}{2}a$ of which a is a nonresidue (its existence follows easily from Article 129). Let it be $= p$. The fundamental theorem then gives pNa, and this gives $\pm 2pRa$. — So let $e^2 \equiv 2p \pmod{a}$, with e odd and $< a$. We must now distinguish two cases.

I. When e is not divisible by p, let $e^2 = 2p + aq$. Then q is positive, of the form $8n+7$ or $8n+3$ (according to whether p has the form $4n+1$ or $4n+3$), $< a$, and not divisible by p. Divide all the prime factors of q into four classes: let there be e of the form $8n+1$, f of the form $8n+3$, g of the form $8n+5$, and h of the form $8n+7$. Let the product of the factors in the first class be E, and the products of the factors in the second, third and fourth classes respectively $F, G.H$[*)].

With this done, consider *first* the case where p has the form $4n+1$, or q the form $8n+7$. It is easy to see that $2RE$, $2RH$, which gives pRE, pRH, and finally ERp, HRp. Also 2 is a nonresidue of every factor of the form $8n+3$ or $8n+5$, and so is p; therefore each such factor is a nonresidue of p. It follows easily that FG is a residue of p if $f+g$ is even, and a nonresidue if $f+g$ is odd. But $f+g$ cannot be odd: listing all the cases shows that $EFGH$, or q, would have either the form $8n+3$ or $8n+5$ if $f+g$ were odd, whatever the individual e, f, g, h might be, contrary to the hypothesis. Thus $FGRp$, $EFGHRp$, or qRp, and finally, because $aqRp$, aRp, contrary to the hypothesis. *Second,* when p has the form $4n+3$, we can similarly show that pRE, and therefore ERp; $-pRF$, and therefore FRp; and finally that $g+h$ is even, so $GHRp$. This finally gives qRp, aRp, contrary to the hypothesis.

II. When e is divisible by p, the proof can be carried out in a similar way and worked out without difficulty by experienced readers (the only readers for whom this article is written). We omit it for brevity.

[*)] If a class contains no factors, we must write 1 in place of their product.

Solution of the general problem.

146.

The fundamental theorem and the propositions concerning the residues -1 and ± 2 always let us determine whether any given number is a residue or nonresidue of a given prime. It will be useful, however, to bring together here the other results given above, so that we have everything needed to solve the following

PROBLEM: *Given any two numbers P, Q, determine whether the second, Q, is a residue or nonresidue of the first, P.*

Solution. I. Let $P = a^\alpha b^\beta c^\gamma$, etc., where a, b, c, etc., denote distinct positive primes (since P must clearly be taken in absolute value). For brevity, in this article we will call the *relation* of two numbers x, y simply the relation in which the first, x, is a residue or nonresidue of the second, y. Thus the relation of Q, P depends on the relations of Q, a^α; Q, b^β, etc. (Article 105).

II. To find the relation of Q, a^α (the same applies to the others, Q, b^β, etc.), we must distinguish two cases.

1. When Q is divisible by a, put $Q = Q'a^e$, so that Q' is not divisible by a. If $e = \alpha$ or $e > \alpha$, then QRa^α; if $e < \alpha$ and the exponent is odd, then QNa^α; finally, if $e < \alpha$ and the exponent is even, Q has the same relation to a^α as Q' has to $a^{\alpha-e}$. This reduces the present case to

2. When Q is not divisible by a. Here we again distinguish two cases.

(A) When $a = 2$. Then QRa^α always holds when $\alpha = 1$. When $\alpha = 2$, Q must have the form $4n + 1$; finally, when $\alpha = 3$ or > 3, Q must have the form $8n + 1$. If this condition holds, then QRa^α.

(B) When a is another prime. Then Q has the same relation to a^α as to a (see Article 101).

III. The relation of any number Q to an odd prime a is found as follows. When $Q > a$, replace Q by its least positive residue modulo a[*]. This has the same relation to a as Q does.

Next, resolve Q, or the number taken in its place, into its prime factors p, p', p'', etc., adding the factor -1 when Q is negative. The relation of Q to a is known to depend on the relations of the individual p, p', p'', etc., to a. Specifically, if $2m$ of these factors are nonresidues of a, then QRa; if there are $2m + 1$, then QNa. It is easy to see that if among the factors p, p', p'', etc., two, four, six, or generally $2k$ equal ones occur, they can safely be left out.

IV. If the factors $p.p', p''$ include -1 and 2, their relation to a can be found from Articles 108, 112, 113, 114. The relation of the remaining factors to a depends on the relation of a to them (the fundamental theorem and the propositions of Article 131). Let p be one of them. Treating the numbers a, p as we previously treated Q and a, which are respectively larger, we find that the relation of a to p can either be determined from Articles 108—114 (if the least residue of a (mod. p) has no odd prime factors), or depends in turn on the relation of p to certain primes smaller than p. The same applies to the remaining factors p', p'', etc. It is now easy to see that

[*] *Residue* in the sense of Article 4. — It is usually better to take the *absolutely* least residue.

continuing this operation eventually brings us to numbers whose relations can be determined from the propositions of Articles 108—114. An example will make this clearer.

Example. We seek the relation of $+453$ to 1236. We have $1236 = 4.3.103$; $+453R4$ by II. 2 (A); $+453R3$ by II. 1. So it remains to find the relation of $+453$ to 103. This is the same as that of $+41$ $(\equiv 453, \text{ mod. } 103)$ to 103, and the same as that of $+103$ to 41 (by the fundamental theorem), or of -20 to 41. But $-20R41$, since $-20 = -1.2.2.5$; $-1R41$ (Article 108); and $+5R41$, because $41 \equiv 1$ and it is therefore a residue of 5 (by the fundamental theorem). Thus $+453R103$, and finally $+453R1236$. In fact, $453 \equiv 297^2 \pmod{1236}$.

Linear forms containing all primes of which any given number is a residue or nonresidue.

147.

Given any number A, we can exhibit certain *formulas* containing all numbers coprime to A of which A is a residue, or all numbers that can be *divisors* of numbers of the form $xx - A$ (where xx denotes an indeterminate square)[*)]. For brevity, however, we consider only those divisors that are odd and coprime to A, since the remaining cases easily reduce to these.

First, let A be either a positive prime of the form $4n + 1$ or a negative prime of the form $4n - 1$. By the fundamental theorem, all primes that, taken positively, are residues of A will be divisors of $xx - A$; all primes (except the number 2, which is always a divisor) that are nonresidues of A will be non-divisors of $xx - A$. Let all residues of A smaller than A (excluding zero) be r, r', r'', etc., and all nonresidues n, n', n'', etc. Every prime contained in one of the forms $Ak + r$, $Ak + r'$, $Ak + r''$, etc., will be a divisor of $xx - A$, while every prime in one of the forms $Ak + n$, $Ak + n'$, etc., will be a non-divisor, where k denotes an indeterminate integer. We call the former *divisor forms of* $xx - A$, and the latter *non-divisor forms.* There are $\frac{1}{2}(A-1)$ of each. Further, if B is an odd composite number and ARB, all prime factors of B lie in one of the former forms, and so does B. Thus *every* odd number contained in a non-divisor form is a non-divisor of $xx - A$. But this theorem cannot be reversed: if B is an odd composite non-divisor of $xx - A$, some prime factors of B will be non-divisors; if their number is *even*, B will nevertheless lie in a divisor form. See Article 99.

Example. In this way, for $A = -11$ we find the following divisor forms of $xx + 11$: $11k+1, 3, 4, 5, 9$; the non-divisor forms are $11k+2, 6, 7, 8, 10$. Thus -11 is a nonresidue of all odd numbers contained in one of the latter forms, but a residue of all primes belonging to one of the former.

[*)] We will simply call such numbers *divisors of* $xx - A$; the meaning of *non-divisors* is then clear.

Similar forms exist for the divisors and non-divisors of $xx - A$, whatever number A denotes. It is easy to see, however, that we need consider only values of A not divisible by any square. For if $A = a^2A'$, all divisors[*)] of $xx - A$ are also divisors of $xx - A'$, and the same holds for non-divisors. — We distinguish three cases: 1) when A has the form $+(4n+1)$ or $-(4n-1)$; 2) when A has the form $-(4n+1)$ or $+(4n-1)$; 3) when A is even, or has the form $\pm(4n+2)$.

148.

First case: when A has the form $+(4n+1)$ or $-(4n-1)$. Resolve A into its prime factors, giving a positive sign to those of the form $4n+1$, and a negative sign to those of the form $4n-1$ (so their product is $= A$). Let these factors be a, b, c, d, etc. Divide all numbers smaller than A and coprime to A into two classes. Put in the first class all numbers that are nonresidues of none of a, b, c, d, etc., or of two, or four, or generally an even number of them; in the second, those that are nonresidues of one of a, b, c, etc., or of three, etc., or generally an odd number. Denote the former by r, r', r'', etc., and the latter by n, n', n'', etc. Then $Ak + r$, $Ak + r'$, $Ak + r''$, etc., are divisor forms of $xx - A$, while $Ak + n$, $Ak + n'$, etc., are non-divisor forms of $xx - A$ (*that is, every prime except* 2 *is a divisor or non-divisor of* $xx - A$ *according to whether it lies in one of the former or latter forms*). For if p is a positive prime and a residue or nonresidue of one of a, b, c, etc., that number itself is a residue or nonresidue of p (by the fundamental theorem). So if a, b, c, etc., include m numbers of which p is a nonresidue, just as many are nonresidues of p. Thus if p lies in one of the former forms, m is even and ARp; if it lies in one of the latter, m is odd and ANp.

Example. Let $A = +105 = -3 \times +5 \times -7$. Then r, r', r'', etc., are the following: $1, 4, 16, 46, 64, 79$ (nonresidues of none of $3, 5, 7$); $2, 8, 23, 32, 53, 92$ (nonresidues of $3, 5$); $26, 41, 59, 89, 101, 104$ (nonresidues of $3, 7$); $13, 52, 73, 82, 97, 103$ (nonresidues of $5, 7$). — The numbers n, n', n'', etc., are the following: $11, 29, 44, 71, 74, 86$; $22, 37, 43, 58, 67, 88$; $19, 31, 34, 61, 76, 94$; $17, 38.47, 62, 68, 83$. The first six are nonresidues of 3, the next six nonresidues of 5, followed by the nonresidues of 7, and finally those that are nonresidues of all three at once.

The theory of combinations and Articles 32, 96 easily show that the number of r, r', r'', etc., is

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

and the number of n, n', n'', etc.,

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

where l denotes the number of a, b, c, etc.;

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

[*)] Those coprime to A, of course.

and each series is continued until it terminates. (There are t numbers that are residues of all of a, b, c, etc., $\frac{t \,.\, l \,.\, l-1}{1 \,.\, 2}$ that are nonresidues of two, etc.; but brevity does not permit us to explain this proof more fully.) The sum of each series*) is $= 2^{l-1}$. The first comes from

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

by joining the second and third terms, the fourth and fifth, etc.; the second comes from the same series by joining the first and second terms, the third and fourth, etc. Thus there are as many divisor forms of $xx - A$ as non-divisor forms, namely $\frac{1}{2}(a-1)(b-1)(c-1)$, etc.

149.

We can consider the *second and third cases* together here. We can always put $A = (-1)Q$, or $= (+2)Q$, or $= (-2)Q$, where Q denotes a number of the form $+(4n+1)$ or $-(4n-1)$, such as we considered in the preceding article. In general, let $A = \alpha Q$, with α either $= -1$ or $= \pm 2$. Then A is a residue of all numbers of which either both α and Q are residues or neither is; it is a nonresidue of all numbers of which exactly one of α, Q is a nonresidue. The divisor and non-divisor forms of $xx - A$ follow easily. If $\alpha = -1$, divide all numbers smaller than $4A$ and coprime to it into two classes. Put in the first those lying in a divisor form of $xx - Q$ and also in the form $4n+1$, and those lying in a non-divisor form of $xx - Q$ and also in the form $4n+3$; put the rest in the second. Let the former be r, r', r'', etc., and the latter n, n', n'', etc. Then A is a residue of all primes in one of the forms $4Ak + r$, $4Ak + r'$, $4Ak + r''$, etc., and a nonresidue of all primes in one of the forms $4Ak + n$, $4Ak + n'$, etc. — If $\alpha = \pm 2$, divide all numbers smaller than $8Q$ and coprime to it into two classes. Put in the first those lying in a divisor form of $xx - Q$ and also in one of the forms $8n+1$, $8n+7$ for the upper sign, or $8n+1$, $8n+3$ for the lower sign; also those lying in a non-divisor form of $xx - Q$ and in one of $8n+3$, $8n+5$ for the upper sign, or $8n+5$, $8n+7$ for the lower sign. Put the rest in the second class. Denoting the numbers of the first class by r, r', r'', etc., and those of the second by n, n', n'', etc., $\pm 2Q$ is a residue of all primes in one of the forms $8Qk + r$, $8Qk + r'$, $8Qk + r''$, etc., and a nonresidue of all primes in one of the forms $8Qk + n$, $8Qk + n'$, $8Qk + n''$, etc. It can easily be proved that here too there are as many divisor forms of $xx - A$ as non-divisor forms.

Example. This gives $+10$ as a residue of all primes in one of the forms $40k + 1, 3, 9, 13, 27, 31, 37, 39$, but a nonresidue of all primes contained in one of $40k + 7, 11, 17, 19, 21, 23, 29, 33$.

*) Leaving out the factor t.

150.

These forms have several quite notable properties, but we give just one. If B is a composite number coprime to A, and $2m$ of its prime factors lie in a non-divisor form of $xx - A$, then B lies in a divisor form of $xx - A$. If, however, the number of prime factors of B lying in a non-divisor form of $xx - A$ is odd, B too lies in a non-divisor form. We omit the proof, which is not difficult. It follows that every prime, and also every odd composite number coprime to A that lies in a non-divisor form, is a non-divisor: some prime factor of such a number must necessarily be a non-divisor.

The work of others on these investigations.

151.

The fundamental theorem, certainly one of the most elegant results of this kind, has not so far been stated by anyone in the simple form given above. This is all the more surprising since the distinguished Euler already knew certain other propositions resting on it, from which he could easily have returned to it. He knew that there are certain forms containing all prime divisors of numbers of the form $xx - A$, and other forms containing all prime non-divisors of numbers of that same form, so that the latter exclude the former; and he had found a method for determining these forms. But all his attempts to reach a proof were unsuccessful and only made this truth, found from examples, more probable. In his paper *Novae demonstrationes circa divisores numerorum formae* $xx + nyy$, read to the St Petersburg Academy on 20 November 1775 and preserved after the death of that great man in *Vol.* I of the Academy's *Nov. Act.*, p. 47 ff., he does seem to have thought he had succeeded. But an error entered here: on p. 65 he *tacitly* assumed that such divisor and non-divisor forms exist[*]. From this it was not difficult to derive *what* they must be, but the method he used to support this supposition does not seem suitable. In another paper, *De criteriis aequationis* $fxx + gyy = hzz$ *utrumque resolutionem admittat necne*, Opusc. Anal., Vol. I (where f, g, h are given, and x, y, z indeterminate), he found by examining examples that if the equation is solvable for some value $h = s$, it is also solvable for every other value congruent to s modulo $4fg$, provided it is a prime. The supposition we mentioned can easily be proved from this proposition. But the proof of this theorem too eluded all his efforts[*)]. This is not surprising, since in our view one had to start from the fundamental theorem. The truth of this proposition will, moreover, follow directly from what we teach in the next section.

After Euler, the distinguished Le Gendre worked on the same subject in his excellent paper *Recherches d'analyse indéterminée*, Hist. de l'Ac. des Sc., 1785, p. 465

[*]Namely, that there are numbers r, r', r'', etc.; n, n', n'', etc., all different and $< 4A$, such that all prime divisors of $xx - A$ lie in one of the forms $4Ak + r$, $4Ak + r'$, etc., and all prime non-divisors in one of $4Ak + n$, $4Ak + n'$, etc. (where k denotes an indeterminate number).

[*)]As he admits himself, in the cited work, p. 216: "A proof of this most elegant theorem is still wanted, after many have long sought it in vain. … Whoever succeeds in finding a proof of this theorem must therefore be thought to have achieved a great deal." — Many other passages of Opusc. Anall. show how eagerly that immortal man wanted a proof of this theorem and others that are only special cases of the fundamental theorem. Compare *Additamentum ad diss.* VIII, Vol. I, and *diss.* XIII, Vol. II, and several papers in Comment. Petrop., already cited in various places.

ff. He reached a theorem equivalent in substance to the fundamental theorem: if p, q denote two positive primes, the absolutely least residues of the powers $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$ modulo q, p, respectively, are either both $+1$ or both -1 when either p or q has the form $4n+1$. When both p and q have the form $4n+3$, one least residue is $+1$ and the other -1 (p. 516). By Article 106, it follows that the *relation* (in the sense of Article 146) of p to q and of q to p is *the same* when either p or q has the form $4n+1$, and *opposite* when both p and q have the form $4n+3$. This proposition is among those of Article 131; it also follows from 1, 3, 9 of Article 133. Conversely, the fundamental theorem can be derived from it. Le Gendre also attempted a proof; since it is highly ingenious, we will discuss it more fully in the next section. But he assumed several things without proof (as he himself admits on p. 520, *We have only assumed*, etc.), some of which have so far been proved by no one, and some, in our view at least, cannot be proved without the fundamental theorem itself. So his approach seems unable to reach the goal, and our proof must be regarded as the first. — We will, moreover, give *two other proofs* of this most important theorem below, entirely different from the preceding proof and from each other.

Quadratic congruences with a linear term.

152.

So far we have treated the pure congruence $xx \equiv A \pmod{m}$ and shown how to decide whether it is solvable. Finding *the roots themselves* was reduced in Article 105 to the case where m is a prime or a power of a prime, and the latter case in Article 101 to the case where m is a prime. For this case, what we gave in Article 61 ff., together with what we will teach in Sections V and VIII, contains almost everything that can be obtained by direct methods. But where these methods apply, they are usually infinitely longer than the indirect methods we will teach in Section VI, and are therefore notable more for their beauty than for their practical usefulness. — *Quadratic congruences with a linear term* can easily be reduced to pure ones. Given the congruence

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

to be solved modulo m, the following congruence is equivalent to it:

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

that is, every number satisfying either one also satisfies the other. This can be written as

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

from which all values of $2ax + b$ smaller than $4am$, if there are any, can be found. Denoting these by r, r', r'', etc., all solutions of the proposed congruence follow from the solutions of the congruences

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

which we taught how to find in Section II. We also observe that various tricks can usually shorten the solution. *For example,* in place of the proposed congruence one can find an equivalent congruence

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

in which a' divides m. Brevity does not allow us to explain this here; the last section may be consulted on these matters.

SECTION FIVE
QUADRATIC FORMS AND INDETERMINATE EQUATIONS OF THE SECOND DEGREE

Aim of the investigation; definition and notation of forms.

153.

In this section we will mainly study functions of two indeterminates x, y of the form

$$axx + 2bxy + cyy$$

where a, b, c are given integers. We will call these *forms of the second degree*, or simply *forms*. This investigation will provide the basis for solving the famous problem of finding all solutions of any indeterminate equation of the second degree in two unknowns, whether the unknowns are required to have integer values or only rational values. The distinguished Lagrange has already solved this problem in full generality. Many further results about the nature of *forms* have been discovered for the first time, either by this great geometer himself or by the distinguished Euler; others, discovered earlier by Fermat, have been supplied with proofs by them. But as we pursued our investigation of forms closely, so many new results presented themselves that we thought it worth taking up the whole subject again from the beginning. We had all the more reason to do so because we found that the discoveries of these men, scattered over many places, were known to few people; because the method we will use is largely our own; and finally because our results could not even be understood without a fresh account of theirs. We have no doubt that many excellent results in this field still lie hidden, on which others can try their strength. We will always give the history of notable results in its proper place.

We will denote the form $axx + 2bxy + cyy$, when the indeterminates x, y are not at issue, by (a, b, c). This notation will thus stand, without specifying the indeterminates, for the sum of three parts: the product of the given number a and the square of any indeterminate; the product of twice the number b, this indeterminate and another indeterminate; and the product of the number c and the square of the second indeterminate. *For example*, $(1, 0, 2)$ will denote the sum of a square and twice a square. Although the forms (a, b, c) and (c, b, a) denote the same thing if we consider only the *parts themselves*, they differ if we also consider the *order* of the parts. We will therefore distinguish them carefully from now on; the advantages of doing this will become clear enough in what follows.

Representation of numbers; determinant.

154.

We will say that a given number is *represented* by a given form if integer values are assigned to the indeterminates of the form so that its value equals the given number. We have the following

THEOREM. *If the number M can be represented by the form (a, b, c) so that the values of the indeterminates that give this representation are relatively prime, then $bb - ac$ is a quadratic residue of the number M.*

Proof. Let the values of the indeterminates be m, n, so that

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

and choose numbers μ, ν so that $\mu m + \nu n = 1$ (Article 40). Expansion easily shows that

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

or

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

So

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

that is, $bb - ac$ is a quadratic residue of M.

We will call the number $bb - ac$ the *determinant* of the form (a, b, c); we will show later that the properties of a form depend above all on the nature of this number.

Values of the expression $\sqrt{(bb - ac)}(mod.\, M)$ to which a representation of the number M by the form (a, b, c) belongs.

155.

Thus

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

is a value of the expression

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

Now the numbers μ, ν can be chosen in infinitely many ways so that $\mu m + \nu n = 1$, giving one value after another of that expression. Let us see how these values are related. Suppose not only that $\mu m + \nu n = 1$, but also that $\mu' m + \nu' n = 1$, and put

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

Multiplying the equation $\mu m + \nu n = 1$ by μ', the other equation $\mu' m + \nu' n = 1$ by μ, and subtracting gives $\mu' - \mu = n(\mu'\nu - \mu\nu')$. Similarly, multiplying the first by

ν' and the second by ν, and then subtracting, gives $\nu' - \nu = m(\mu\nu' - \mu'\nu)$. This immediately gives

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

or $v' \equiv v \pmod{M}$. So however μ, ν are chosen, the formula $\mu(mb + nc) - \nu(ma + nb)$ cannot give *different* (that is, incongruent) values of the expression $\sqrt{(bb - ac)} \pmod{M}$. If v is any value of that formula, we will say that the representation of the number M by the form $axx + 2bxy + cyy$ in which $x = m$, $y = n$ *belongs to the value* v *of the expression* $\sqrt{(bb - ac)}$*(mod.* M*)*. It is also easy to show that if one value of this formula is v and $v' \equiv v \pmod{M}$, the numbers μ, ν that give v can be replaced by other numbers μ', ν' that give v'. In fact, putting

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

gives

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

and the value of the formula obtained from μ', ν' exceeds the value obtained from μ, ν by the quantity $(\mu'\nu - \mu\nu')M$. This quantity becomes $= (\mu m + \nu n)(v' - v) = v' - v$, giving the value $= v'$.

156.

If we have two representations of the same number M by the same form (a, b, c), in each of which the values of the indeterminates are relatively prime, they may belong either to the same value of the expression $\sqrt{(bb - ac)} \pmod{M}$ or to different values. Let

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

and

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

Clearly, if

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

the congruence remains true however we replace μ, ν and μ', ν' by other suitable values. In this case we will say that the two representations belong to the *same* value of the expression $\sqrt{(bb - ac)} \pmod{M}$. But if the congruence fails for any choice of μ, ν and μ', ν', it will hold for none, and the representations will belong to *different* values. If, on the other hand,

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

we will say that the representations belong to *opposite* values of the expression $\sqrt{(bb - ac)}$. We will also use all these terms when considering several representations of the same number by *different* forms with the same determinant.

Example. Take the form $(3, 7, -8)$, with determinant $= 73$. It gives the following representations of the number 57:

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

For the first we can put $\mu = 2$, $\nu = -1$, giving the value of the expression $\sqrt{73} \pmod{57}$ to which the representation belongs:

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

Similarly, putting $\mu = 2$, $\nu = -1$, we find that the second representation belongs to the value $+4$. So the two representations belong to opposite values.

Before going further, we note that forms with determinant $= 0$ are excluded entirely from the investigations that follow. They would only disrupt the orderly form of the theorems and so need a treatment of their own.

A form containing another, or contained in another; proper and improper transformation.

157.

If a form F, with indeterminates x, y, can be changed into another form F', with indeterminates x', y', by substitutions

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

in which $\alpha, \beta, \gamma, \delta$ are integers, we will say that the first *contains* the second, or that the second *is contained in the first.* Let the form F be

$$axx + 2bxy + cyy$$

and the form F' be

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

We then have the following three equations:

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

Multiplying the second equation by itself and the first by the third, then subtracting and removing the terms that cancel, gives

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

It follows that the determinant of the form F' is divisible by the determinant of the form F, and that the quotient is a square. These determinants therefore have *the same sign.* If, in addition, the form F' can be changed into the form F by a similar substitution, that is, if both F' is contained in F and F in F', the determinants of the

forms are equal*) and $(\alpha\delta - \beta\gamma)^2 = 1$. In this case we will call the forms *equivalent*. Equality of determinants is therefore a necessary condition for equivalence of forms, although equivalence certainly does not follow from it alone. — We will call the substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ a *proper transformation* if $\alpha\delta - \beta\gamma$ is positive, and an *improper transformation* if $\alpha\delta - \beta\gamma$ is negative. We will say that the form F' is *properly* or *improperly* contained in the form F if F can be changed into F' by a proper or improper transformation. Thus, if the forms F, F' are equivalent, $(\alpha\delta - \beta\gamma)^2 = 1$, so that for a proper transformation $\alpha\delta - \beta\gamma = +1$, and for an improper one $= -1$. — We will call several transformations *similar* if they are all proper or all improper; a proper and an improper transformation will be called *dissimilar*.

Proper and improper equivalence.

158.

If the forms F, F' have equal determinants and F' is contained in F, then F is also contained in F', properly or improperly according as F' is properly or improperly contained in F. Suppose F changes into F' on putting

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

Then F' changes into F on putting

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

For this substitution clearly produces from F' the same result as putting in F

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \quad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

or

$$x = (\alpha\delta - \beta\gamma)x, \quad y = (\alpha\delta - \beta\gamma)y$$

This clearly changes F into $(\alpha\delta - \beta\gamma)^2 F$, that is, back into F (the preceding article). The second transformation is clearly proper or improper according as the first is proper or improper.

If both F' is *properly* contained in F and F in F', we will call the forms *properly equivalent*; if each is improperly contained in the other, we will call them *improperly equivalent*. — The use of these distinctions will soon become clear.

Example. The form $2xx - 8xy + 3yy$ changes, under the substitutions $x = 2x' + y'$, $y = 3x' + 2y'$, into the form $-13x'x' - 12x'y' - 2y'y'$, and the latter changes into the former on putting $x' = 2x - y$, $y' = -3x + 2y$. So the forms $(2, -4, 3)$, $(-13, -6, -2)$ are *properly equivalent*.

*)The preceding analysis clearly shows that this proposition also extends to forms with determinant $= 0$. But the equation $(\alpha\delta - \beta\gamma)^2 = 1$ must not be extended to that case.

The problems we will now take up are these. I. Given any two forms with the same determinant, determine whether they are equivalent, and whether properly, improperly, or in both ways, since this too is possible. If their determinants are unequal, determine whether at least one contains the other, properly, improperly, or in both ways. Finally, find all transformations of one into the other, both proper and improper. II. Given any form, determine whether a given number can be represented by it, and find all its representations. But forms with negative determinant need a different method here from forms with positive determinant. We will therefore first give what is common to both, then consider forms of each kind separately.

Opposite forms.

159.

If the form F contains the form F', and this in turn contains the form F'', then the form F also contains the form F''.

Let the indeterminates of the forms F, F', F'' be $x, y,\ x', y',\ x'', y''$ respectively, and suppose F changes into F' on putting

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

and F' into F'' on putting

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

Clearly, F will change into F'' on putting

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

or

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

So F contains F''.

Since

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

the result is positive if $\alpha\delta - \beta\gamma$ and $\alpha'\delta' - \beta'\gamma'$ are both positive or both negative, and negative if one is positive and the other negative. So the form F contains the form F'' *properly* if F contains F' in the same way as F' contains F'', and *improperly* if in different ways.

It follows that if we have any number of forms F, F', F'', F''', etc., each containing the next, the first contains the last, *properly* if the number of forms that contain their successor improperly is even, and *improperly* if this number is odd.

If the form F is equivalent to the form F', and the form F' to the form F'', then the form F is equivalent to the form F'': properly if the form F is equivalent to the form F' in the same way as the form F' is to the form F'', and improperly if in different ways.

For since the forms F, F' are respectively equivalent to F', F'', not only does each of the former contain the corresponding latter form, so that F contains F'', but the latter also contain the former. So F, F'' are equivalent. The preceding result shows that F contains F'' properly or improperly according as F is equivalent to F' in the same way as F' is to F'', or in different ways; the same is true of F'' containing F. Thus, in the first case F, F'' are properly equivalent, and in the second, improperly equivalent.

The forms $(a, -b, c)$, (c, b, a), $(c, -b, a)$ are equivalent to the form (a, b, c): the first two improperly, and the last properly.

For $axx + 2bxy + cyy$ changes into $ax'x' - 2bx'y' + cy'y'$ on putting $x = x' + 0.y'$, $y = 0.x' - y'$, and this transformation is improper because $1 \times -1 - 0.0 = -1$; into the form $cx'x' + 2bx'y' + ay'y'$ by the improper transformation $x = 0.x' + y'$, $y = x' + 0.y'$; and into the form $cx'x' - 2bx'y' + ay'y'$ by the proper transformation $x = 0.x' - y'$, $y = x' + 0.y'$.

It is therefore clear that any form equivalent to the form (a, b, c) is *properly* equivalent either to that form itself or to the form $(a, -b, c)$. Similarly, if any form contains the form (a, b, c) or is contained in it, it *properly* contains either the form (a, b, c) or the form $(a, -b, c)$, or is *properly* contained in one of them. We will call the forms (a, b, c), $(a, -b, c)$ *opposite*.

Neighboring forms.

160.

If the forms (a, b, c), (a', b', c') have the same determinant, and in addition $c = a'$ and $b \equiv -b' \pmod{c}$, or $b + b' \equiv 0 \pmod{c}$, we will call them *neighboring* forms. When a more precise description is needed, we will call the first a neighbor of the second *on the left*, and the second a neighbor of the first *on the right*.

For *example*, the form $(7, 3, 2)$ is a neighbor of the form $(3, 4, 7)$ on the right, and the form (3.1.3) is a neighbor of its opposite $(3, -1, 3)$ on both sides.

Neighboring forms are always properly equivalent. For the form $axx + 2bxy + cyy$ changes into the neighboring form $cx'x' + 2b'x'y' + c'y'y'$ under the substitution $x = -y'$, $y = x' + \frac{b+b'}{c}y'$ (which is proper because $0 \times \frac{b+b'}{c} - 1 \times -1 = 1$), as is easily proved by expansion using the equation $bb - ac = b'b' - cc'$; and $\frac{b+b'}{c}$ is an integer by hypothesis. — These definitions and conclusions do not apply if $c = a' = 0$. This case can occur only for forms whose determinant is a square.

The forms (a, b, c), (a', b', c') are properly equivalent if $a = a'$. $b \equiv b' \pmod{a}$. For the form (a, b, c) is properly equivalent to the form $(c, -b, a)$ (the preceding article), and the latter is a neighbor of the form (a', b', c') on the left.

Common divisors of the coefficients of forms.

161.

If the form (a, b, c) contains the form (a', b', c'), every common divisor of the numbers a, b, c also divides the numbers a', b', c', and every common divisor of the numbers $a, 2b, c$ divides $a', 2b', c'$.

For if the form $axx + 2bxy + cyy$ changes under the substitutions $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ into the form $a'x'x' + 2b'x'y' + c'y'y'$, we have the equations

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

from which the proposition follows immediately (for its second part, use $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$ in place of the second equation).

It follows that the greatest common divisor of the numbers $a, b(2b), c$ also divides the greatest common divisor of the numbers $a', b'(2b'), c'$. If, in addition, the form (a', b', c') contains the form (a, b, c), that is, if the forms are equivalent, the greatest common divisor of the numbers $a, b(2b), c$ equals the greatest common divisor of the numbers $a', b'(2b'), c'$, since each must then divide the other. Thus, if in this case $a, b(2b), c$ have no common divisor, that is, if their greatest common divisor $= 1$, then $a', b'(2b'), c'$ also have no common divisor.

Connection between all similar transformations of a given form into a given form.

162.

PROBLEM. *If the form*

$$AXX + 2BXY + CYY \quad \ldots \quad F$$

contains the form

$$axx + 2bxy + cyy \quad \ldots\ldots \quad f$$

and one transformation of the former into the latter is given, derive from it all the other transformations similar to it.

Solution. Let the given transformation be $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$. First suppose that another similar transformation $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$ is given, and investigate what follows from this. For the forms and their determinants, write $F, f, = D, d$, and put $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$. We have (Article 157) $d = Dee = De'e'$. Since by hypothesis e, e' have the same sign, $e = e'$. We have the following six equations:

$$\begin{aligned}
A\alpha\alpha + 2B\alpha\gamma + C\gamma\gamma &= a \quad \ldots\ldots\ [1]\\
A\alpha'\alpha' + 2B\alpha'\gamma' + C\gamma'\gamma' &= a \quad \ldots\ldots\ [2]\\
A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta &= b \quad \ldots\ldots\ [3]\\
A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' &= b \quad \ldots\ldots\ [4]\\
A\beta\beta + 2B\beta\delta + C\delta\delta &= c \quad \ldots\ldots\ [5]\\
A\beta'\beta' + 2B\beta'\delta' + C\delta'\delta' &= c \quad \ldots\ldots\ [6]
\end{aligned}$$

If, for brevity, we denote the numbers

$$\begin{gathered}
A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'\\
A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')\\
A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta'
\end{gathered}$$

by $a', 2b', c'$, we derive the following new equations from the preceding ones*):

$$a'a' - D(\alpha\gamma' - \gamma\alpha')^2 = aa \qquad \ldots\ldots\ldots \quad [7]$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab \qquad \ldots \quad [8]$$
$$4b'b' - D\big((\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee'\big) = 2bb + 2ac$$

Adding $2Dee' = 2d = 2bb - 2ac$ gives

$$4b'b' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4bb \qquad \ldots\ldots \quad [9]$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = bb$$

and subtracting $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = bb - ac$ gives

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac \qquad \ldots\ldots \quad [10]$$
$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc \qquad \ldots \quad [11]$$
$$c'c' - D(\beta\delta' - \delta\beta')^2 = cc \qquad \ldots\ldots\ldots \quad [12]$$

Now let the greatest common divisor of the numbers $a, 2b, c$ be m, and choose the numbers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ so that

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

(Article 40). Multiply the equations $7, 8, 9, 10, 11, 12$ by $\mathfrak{AA}, 2\mathfrak{AB}, \mathfrak{BB}, 2\mathfrak{AC}, 2\mathfrak{BC}, \mathfrak{CC}$ respectively and add the products. If, for brevity, we put

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T \qquad \ldots\ldots\ldots \quad [13]$$
$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')$$
$$+ \mathfrak{C}(\beta\delta' - \delta\beta') = U \qquad \ldots \quad [14]$$

where T, U are clearly integers, we obtain

$$TT - DUU = mm$$

So we have reached this elegant conclusion: *any two similar transformations of the form F into f give an integer solution of the indeterminate equation $tt - Duu = mm$*, namely $t = T,\ u = U$. Since in our reasoning we did not assume the transformations to be *different*, even *one* transformation considered twice must give a solution. In that case, however, because $\alpha' = \alpha,\ \beta' = \beta$, etc., we have $a' = a,\ b' = b,\ c' = c$, and so $T = m,\ U = 0$, a solution that is obvious in itself.

Now consider the first transformation and the solution of the indeterminate equation as known, and investigate how the second transformation can be derived from them, or how $\alpha', \beta', \gamma', \delta'$ depend on $\alpha, \beta, \gamma, \delta,\ T, U$. For this purpose, first multiply

*) These equations arise as follows: 7 comes from 1.2 (that is, by multiplying equation (1) by equation (2), or rather by multiplying the left side of the former by the left side of the latter, and its right side by the right side of the latter, and equating the products); 8 from $1.4 + 2.3$; the next, unnumbered equation from $1.6 + 2.5 + 3.4 + 3.4$; the next unnumbered one from 3.4; 11 from $3.6 + 4.5$; 12 from 5.6. We will always use similar notation in what follows. We must leave the expansion to the reader.

equation [1] by $\delta\alpha' - \beta\gamma'$, [2] by $\alpha\delta' - \gamma\beta'$, [3] by $\alpha\gamma' - \gamma\alpha'$, [4] by $\gamma\alpha' - \alpha\gamma'$, and add the products. This gives

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a \quad \ldots\ldots \quad [15]$$

Similarly, from

$$(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] - [6])$$

we get

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b \quad \ldots\ldots \quad [16]$$

Finally, from $(\delta\beta' - \beta\delta')([3] - [4]) + (\alpha\delta' - \gamma\beta')[5] + (\delta\alpha' - \beta\gamma')[6]$ we get

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c \quad \ldots\ldots \quad [17]$$

Substituting these values $(15, 16, 17)$ into 13 gives

$$(e + e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)$$

or

$$2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m \quad \ldots\ldots\ldots \quad [18]$$

from which T can be derived much more easily than from [13]. — Combining this equation with $15, 16, 17$ gives $ma' = Ta,\ 2mb' = 2Tb,\ mc' = Tc$. Substituting these values of $a', 2b', c'$ into equations 7—12 and writing TT as $mm + DUU$, we obtain, after the required changes,

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')^2 mm &= aaUU \\
(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')mm &= 2abUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 mm &= 4bbUU \\
(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')mm &= acUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')mm &= 2bcUU \\
(\beta\delta' - \delta\beta')^2 mm &= ccUU
\end{aligned}$$

Using equation [14] and the equation $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, we easily derive the following (multiply the first, second and fourth; the second, third and fifth; the fourth, fifth and sixth equations by $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ respectively, and add the products):

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')Umm &= maUU \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')Umm &= 2mbUU \\
(\beta\delta' - \delta\beta')Umm &= mcUU
\end{aligned}$$

and then, dividing by mU[*)],

$$\begin{aligned}
aU &= (\alpha\gamma' - \gamma\alpha')m \quad \ldots\ldots\ldots \quad [19] \\
2bU &= (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m \quad \ldots\ldots \quad [20] \\
cU &= (\beta\delta' - \delta\beta')m \quad \ldots\ldots\ldots \quad [21]
\end{aligned}$$

[*)] This would not be allowed if $U = 0$. In that case, however, equations $19, 20, 21$ would follow immediately from the first, third and sixth of the preceding equations.

Any of these equations gives U much more easily than [14] does. — It also follows that however $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ are chosen (which can be done in infinitely many ways), both T and U retain their respective values.

Now multiplying equation 18 by α, 19 by 2β, and 20 by $-\alpha$, and adding gives

$$2\alpha eT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m$$

Similarly, from $\beta[18] + \beta[20] - 2\alpha[21]$ we get

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m$$

Further, from $\gamma[18] + 2\delta[19] - \gamma[20]$ we get

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m$$

Finally, from $\delta[18] + \delta[20] - 2\gamma[21]$ we get

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m$$

Substituting in these formulas the values of a, b, c from $1, 3, 5$ gives

$$\begin{aligned}
\alpha' m &= \alpha T - (\alpha B + \gamma C)U \\
\beta' m &= \beta T - (\beta B + \delta C)U \\
\gamma' m &= \gamma T + (\alpha A + \gamma B)U \\
\delta' m &= \delta T + (\beta A + \delta B)U^{*)}
\end{aligned}$$

The preceding analysis shows that there is no transformation of the form F into f similar to the given one that is not included in the formula

$$\begin{aligned}
X &= \tfrac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \tfrac{1}{m}(\beta t - (\beta B + \delta C)u)y \\
Y &= \tfrac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \tfrac{1}{m}(\delta t + (\beta A + \delta B)u)y \quad \ldots \quad \text{(I)}
\end{aligned}$$

where t, u stand for all integers satisfying the equation $tt - Duu = mm$. We cannot yet conclude that all values of t, u satisfying that equation give suitable transformations when substituted into formula (I). But:

1. The form F always changes, under a substitution coming from any such values of t, u, into the form f. This is easily confirmed by expansion using equations $1, 3, 5$ and the equation $tt - Duu = mm$. We omit the calculation for brevity; it is longer than it is difficult.

*) From this we easily derive

$$\begin{aligned}
AeU &= (\delta\gamma' - \gamma\delta')m \\
2BeU &= (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m \\
CeU &= (\beta\alpha' - \alpha\beta')m
\end{aligned}$$

2. Every transformation derived from the formula is similar to the given one. For

$$\begin{aligned}&\tfrac{1}{m}(\alpha t-(\alpha B+\gamma C)u)\times\tfrac{1}{m}(\delta t+(\beta A+\delta B)u)\\&\quad-\tfrac{1}{m}(\beta t-(\beta B+\delta C)u)\times\tfrac{1}{m}(\gamma t+(\alpha A+\gamma B)u)\\&\quad=\tfrac{1}{mm}(\alpha\delta-\beta\gamma)(tt-Duu)=\alpha\delta-\beta\gamma\end{aligned}$$

3. If the forms F, f have unequal determinants, formula (I) may for some values of t, u give substitutions involving *fractions*, which must therefore be rejected. All the others will be suitable transformations, and there will be no others beyond them.

4. If, however, the forms F, f have the same determinant and so are *equivalent*, formula (I) will give no transformations involving fractions and will therefore give the complete solution of the problem in this case. We prove this as follows.

The theorem of the preceding article shows that in this case m is also a common divisor of the numbers $A, 2B, C$. Since $tt - Duu = mm$, we have $tt - BBuu = mm - ACuu$, so $tt - BBuu$ is divisible by mm. Then certainly $4tt - 4BBuu$ is also divisible by it, and (because $2B$ is divisible by m) so is $4tt$ by mm, and therefore $2t$ by m. Thus $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ are integers, and, since their difference $\frac{4}{m}Bu$ is even, they are either both even or both odd. If both were odd, their product would also be odd. But as four times the number $\frac{1}{mm}(tt - BBuu)$, which we have just shown to be an integer, this product is necessarily even. So that case is impossible, and $\frac{2}{m}(t+Bu)$, $\frac{2}{m}(t-Bu)$ are always even, giving integers $\frac{1}{m}(t+Bu)$, $\frac{1}{m}(t-Bu)$. It follows without difficulty that all four coefficients in (I) are always integers. *Q.E.D.*

It follows that once all solutions of the equation $tt - Duu = mm$ are known, all transformations of the form (A, B, C) into (a, b, c) similar to the given transformation can be derived from them. We will show later how to find those solutions. Here we note only that their number is always finite when D is negative, or positive and a square; it is infinite when D is positive and not a square. In the latter case, if also the equality $D = d$ does not hold (point 3^0 above), one would also have to investigate how to distinguish in advance the values of t, u that give substitutions free of fractions from those that give fractional substitutions. But for this case we will give another method below, free of this drawback (Article 214).

Example. The form $xx + 2yy$ changes under the proper substitution $x = 2x' + 7y'$, $y = x' + 5y'$ into the form $(6, 24, 99)$. We want *all* proper transformations of the former form into the latter. Here $D = -2$, $m = 3$, so the equation to solve is $tt + 2uu = 9$. It is satisfied in six different ways, namely by putting $t = 3, -3, 1, -1, 1, -1$; $u = 0, 0, 2, 2, -2, -2$ respectively. The third and sixth solutions give fractional substitutions and must therefore be rejected. The others give four substitutions:

$$x=\begin{cases}2x'+7y'\\-2x'-7y'\\-2x'-9y'\\2x'+9y'\end{cases}\qquad y=\begin{cases}x'+5y'\\-x'-5y'\\x'+3y'\\-x'-3y'\end{cases}$$

(the first of which is the given one).

Ambiguous forms.

163.

We have already mentioned in passing that a form F may contain another form F' both properly and improperly. This clearly happens if between the forms F, F' we can place another form G so that F contains G and G contains F', and the form G is improperly equivalent to itself. For suppose F contains G properly or improperly. Since G contains G improperly, F also contains G improperly or properly, respectively, and thus in either case both properly and improperly (Article 159). It follows in the same way that however G is assumed to contain F', F must always contain F' both properly and improperly. — That forms improperly equivalent to themselves exist can be seen from the most obvious case, where the middle term of the form $= 0$. Such a form is its own opposite (Article 159) and so is improperly equivalent to itself. More generally, every form (a, b, c) in which $2b$ is divisible by a has this property. For the form (c, b, a) is its neighbor on the left (Article 160), and so is properly equivalent to it. But by Article 159, (c, b, a) is improperly equivalent to the form (a, b, c), so (a, b, c) is improperly equivalent to itself. We will call forms (a, b, c) in which $2b$ is divisible by a *ambiguous*. We therefore have the following theorem:

A form F contains another form F' both properly and improperly if an ambiguous form can be found that is contained in F and contains F'. But this proposition also has a converse, namely:

Theorem on the case where one form is contained in another both properly and improperly.

164.

Theorem. *If the form*

$$Axx + 2Bxy + Cyy \quad \ldots\ldots \quad (F)$$

contains the form

$$A'x'x' + 2B'x'y' + C'y'y' \quad \ldots\ldots \quad (F')$$

both properly and improperly, an ambiguous form can be found that is contained in F and contains the form F'.

Suppose the form F changes into the form F' both under the substitution

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

and under the following dissimilar substitution:

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

Denoting the numbers $\alpha\delta - \beta\gamma$, $\alpha'\delta' - \beta'\gamma'$ by e, e', we have $B'B' - A'C' = ee(BB - AC) = e'e'(BB - AC)$, and so $ee = e'e'$. Since by hypothesis e, e' have opposite signs, $e = -e'$, or $e + e' = 0$. It is now clear that if, in F', we substitute for x' the

expression $\delta' x'' - \beta' y''$, and make the corresponding replacement $y', -\gamma' x'' + \alpha' y''$, the same form results as when we write in F

$$\begin{aligned}
\textit{either } 1) \text{ for } x \quad & \alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'') \\
\textit{that is} \quad & (\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y'' \\
\text{and for } y \quad & \gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'') \\
\textit{that is} \quad & (\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y'' \\
\textit{or } 2) \text{ for } x \quad & \alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'') \quad \textit{that is} \quad e' x'' \\
\text{and for } y \quad & \gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'') \quad \textit{that is} \quad e' y''
\end{aligned}$$

Thus, denoting the numbers $\alpha\delta' - \beta\gamma',\ \beta\alpha' - \alpha\beta',\ \gamma\delta' - \delta\gamma',\ \delta\alpha' - \gamma\beta'$ by a, b, c, d, the form F changes under the two substitutions

$$x = ax'' + by'', \quad y = cx'' + dy''; \qquad x = e'x'', \quad y = e'y''$$

into the same form. This gives the following three equations:

$$\begin{aligned}
Aaa + 2Bac + Ccc &= Ae'e' \quad \ldots\ldots\ldots \quad [1] \\
Aab + B(ad + bc) + Ccd &= Be'e' \quad \ldots\ldots \quad [2] \\
Abb + 2Bbd + Cdd &= Ce'e' \quad \ldots\ldots\ldots \quad [3]
\end{aligned}$$

From the values of a, b, c, d, however, we find

$$ad - bc = ee' = -ee = -e'e' \quad \ldots\ldots \quad [4]$$

Then from $d[1] - c[2]$ we get

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'e'$$

and so

$$A(a + d) = 0$$

Further, from $(a + d)[2] - b[1] - c[3]$ we get

$$(Ab + B(a + d) + Cc)(ad - bc) = (-Ab + B(a + d) - Cc)e'e'$$

and so

$$B(a + d) = 0$$

Finally, from $a[3] - b[2]$ we get

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)e'e'$$

and so

$$C(a + d) = 0$$

Since A, B, C cannot all be $= 0$, we must have $a + d = 0$, or $a = -d$.

From $a[2] - b[1]$ we get

$$(Ba + Cc)(ad - bc) = (Ba - Ab)e'e'$$

and thus

$$Ab - 2Ba - Cc = 0 \quad \ldots\ldots\ldots \quad [5]$$

The equations $e + e' = 0$, $a + d = 0$, or

$$\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma' = 0, \quad \alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha' = 0$$

give $(\alpha + \alpha')(\delta + \delta') = (\beta + \beta')(\gamma + \gamma')$, or

$$(\alpha + \alpha') : (\gamma + \gamma') = (\beta + \beta') : (\delta + \delta')$$

Let this ratio[*)] be written in lowest terms as $m : n$, so that m, n are relatively prime, and choose μ, ν so that $\mu m + \nu n = 1$. Further, let r be the greatest common divisor of the numbers a, b, c. Its square therefore divides $aa + bc$, or $bc - ad$, or ee, so r also divides e. With these choices, suppose the form F changes under the substitution

$$x = mt + \frac{\nu e}{r}u, \qquad y = nt - \frac{\mu e}{r}u$$

into the form $Mtt + 2Ntu + Puu$, (G). This form will be ambiguous and will contain the form F'.

Proof. I. To show that the form G is ambiguous, we will prove that

$$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr$$

Since r divides a, b, c, the number $\frac{1}{r}(b\mu\mu - 2a\mu\nu - c\nu\nu)$ is an integer, and so $2N$ is a multiple of M. Now

$$M = Amm + 2Bmn + Cnn,$$
$$Nr = (Am\nu - B(m\mu - n\nu) - Cn\mu)e \quad \ldots \quad [6]$$

Further, expansion easily confirms that

$$\begin{aligned} 2e + 2a &= e - e' + a - d \\ &= (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma') \end{aligned}$$

$$2b = (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta')$$

Since $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$, this gives

[*)] If all of $\alpha + \alpha'$, $\gamma + \gamma'$, $\beta + \beta'$, $\delta + \delta'$ were $= 0$, the ratio would be indeterminate, and the method would not apply. But a little thought shows that this is inconsistent with our assumptions. For we would have $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$, that is, $e = e'$, and thus, since $e = -e'$, $e = e' = 0$. Then $B'B' - A'C'$, that is, the determinant of the form F', would also become $= 0$. We have excluded such forms entirely.

$$m(2e + 2a) = -2nb \quad \text{or}$$

$$me + ma + nb = 0 \quad \ldots\ldots\ldots \quad [7]$$

Similarly,

$$\begin{aligned} 2e - 2a &= e - e' - a + d \\ &= (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma') \end{aligned}$$

$$2c = (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta')$$

and so $n(2e - 2a) = -2mc$, or

$$ne - na + mc = 0 \quad \ldots\ldots\ldots \quad [8]$$

Now add to $mm(b\mu\mu - 2a\mu\nu - c\nu\nu)$ the expression

$$\begin{gathered} (1 - m\mu - n\nu)(m\nu(e - a) + (m\mu + 1)b) \\ +(me + ma + nb)(m\mu\nu + \nu) + (ne - na + mc)m\nu\nu \end{gathered}$$

which clearly $= 0$, because

$$1 - \mu m - \nu u = 0, \quad me + ma + nb = 0, \quad ne - na + mc = 0$$

Expanding the products and removing the terms that cancel gives $2m\nu e + b$. So

$$mm(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2m\nu e + b \quad \ldots\ldots \quad [9]$$

Similarly, adding to $mn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ the following:

$$\begin{gathered} (1 - m\mu - n\nu)((n\nu - m\mu)e - (1 + m\mu + n\nu)a) \\ -(me + ma + nb)m\mu\mu + (ne - na + mc)n\nu\nu \end{gathered}$$

gives

$$mn(b\mu\mu - 2a\mu\nu - c\nu\nu) = (n\nu - m\mu)e - a \quad \ldots\ldots [10]$$

Finally, adding to $nn(b\mu\mu - 2a\mu\nu - c\nu\nu)$ the expression

$$\begin{gathered} (m\mu + n\nu - 1)(n\mu(e + a) + (n\nu + 1)c) \\ -(me + ma + nb)n\mu\mu - (ne - na + mc)(n\mu\nu + \mu) \end{gathered}$$

gives

$$nn(b\mu\mu - 2a\mu\nu - c\nu\nu) = -2n\mu e - c \quad \ldots\ldots [11]$$

Now from 9, 10, 11, we derive

$$\begin{gathered} (Amm + 2Bmn + Cnn)(b\mu\mu - 2a\mu\nu - c\nu\nu) \\ = 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc \end{gathered}$$

or, because of [6],,

$$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr. \quad Q.\ E.\ D.$$

II. To prove that the form G contains the form F', we will show *first* that G changes into F' on putting

$$t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y',$$
$$u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y' \ \ldots\ (S)$$

and *second* that $\frac{r}{e}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ are integers.

1. Since F changes into G on putting

$$x = mt + \frac{\nu e}{r}u, \quad y = nt - \frac{\mu e}{r}u$$

the form G changes under substitution (S) into the same form as F does on putting

$$x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') + \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

that is, $= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y'$, or $= \alpha x' + \beta y'$,
and

$$y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

that is, $= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y'$, or $= \gamma x' + \delta y'$.

But this substitution changes F into F', so substitution (S) also changes G into F'.

2. From the values of e, b, d we find $\alpha' e + \gamma b - \alpha d = 0$, or, because $d = -a$, $n\alpha' e + n\alpha a + n\gamma b = 0$. Then [7] gives $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$, or

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e \quad \ldots\ldots\ [12]$$

Further, $\alpha n b = -\alpha m(e + a)$, $\gamma m b = -m(\alpha' e + \alpha a)$, and so

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me \quad \ldots\ldots\ [13]$$

Finally, $\gamma' e - \gamma a + \alpha c = 0$. Multiplying by n and substituting for na its value from [8] gives

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne \quad \ldots\ldots\ [14]$$

Similarly, we derive $\beta' e + \delta b - \beta d = 0$, or $n\beta' e + n\delta b + n\beta a = 0$, and therefore, by [7],, $n\beta' e + n\beta a = m\delta e + m\delta a$, or

$$(n\beta - m\delta)a = (m\delta - n\beta')e \quad \ldots\ldots\ [15]$$

Further, $\beta n b = -\beta m(e + a)$, $\delta m b = -m(\beta' e + \beta a)$, and so

$$(n\beta - m\delta)b = (\beta' - \beta)me \quad \ldots\ldots\ldots [16]$$

Finally, $\delta e - \delta a + \beta c = 0$. Multiplying by n and substituting for na its value from [8] gives

$$(n\beta - m\delta)c = (\delta - \delta')ne \quad \ldots\ldots\ldots [17]$$

Now, since the greatest common divisor of the numbers a, b, c is r, integers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ can be chosen so that

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

Then 12, 13, 14 and 15, 16, 17 give

$$\begin{aligned} &\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n \\ &\qquad = \frac{r}{e}(n\alpha - m\gamma) \\ &\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n \\ &\qquad = \frac{r}{e}(n\beta - m\delta) \end{aligned}$$

so $\frac{r}{e}(n\alpha - n\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ are integers. *Q. E. D.*

165.

Example. The form $3xx+14xy-4yy$ changes into the form $-12x'x'-18x'y'+39y'y'$ both properly, on putting

$$x = 4x' + 11y', \quad y = -x' - 2y'$$

and improperly, on putting

$$x = -74x' + 89y', \quad y = 15x' - 18y'$$

Here $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ are -70, 100, 14, -20, and $-70 : 14 = 100 : -20 = 5 : -1$. So we put $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. The numbers a, b, c are found to be -237, -1170, 48, whose greatest common divisor $= 3 = r$; finally, $e = 3$. Thus transformation (S) is $x = 5t - u$, $y = -t$. It changes the form $(3, 7, -4)$ into the ambiguous form $tt - 16tu + 3uu$.

If the forms F, F' are equivalent, the form G, contained in F, is also contained in F'. But since it also contains that same form, it is equivalent to it, and so also to the form F. In this case, therefore, the theorem can be stated as follows:

If F, F' are both properly and improperly equivalent, an ambiguous form equivalent to both can be found. — In this case $e = \pm 1$, so $r.$, which divides e, must also be $= 1$.

Let this suffice for the transformation of forms in general. We now turn to *representations.*

General results on representations of numbers by forms and their connection with transformations.

166.

If the form F contains the form F', every number that can be represented by F' can also be represented by F.

Let the indeterminates of the forms F, F' be $x, y; x', y'$ respectively. Suppose the number M is represented by F' on putting $x' = m$, $y' = n$, and that the form F changes into F' under the substitution

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

Then clearly, on putting

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

F takes the value M.

If M can be represented in several ways by the form F', for example also on putting $x' = m'$, $y' = n'$, several representations of M by F follow. For if both

$$\alpha m + \beta n = \alpha m' + \beta n' \quad \text{and} \quad \gamma m + \delta n = \gamma m' + \delta n'$$

we would have either $\alpha\delta - \beta\gamma = 0$, making the determinant of the form $F = 0$, contrary to hypothesis, or $m = m'$, $n = n'$. So M can be represented in at least as many different ways by F as by F'.

Thus, if both F contains F' and F' contains F, *that is*, if F, F' are equivalent, and the number M can be represented by either form, it can also be represented by the other, and in just as many different ways by one as by the other.

Finally, we note that in this case the greatest common divisor of the numbers m, n equals the greatest common divisor of $\alpha m + \beta n$, $\gamma m + \delta n$. Let the former $= \Delta$, and choose the numbers μ, ν so that $\mu m + \nu n = \Delta$. Then

$$\begin{aligned}(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n)\\ = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta\end{aligned}$$

So the greatest common divisor of $\alpha m + \beta n$, $\gamma m + \delta n$ divides Δ. But Δ also divides it, since it clearly divides $\alpha m + \beta n$, $\gamma m + \delta n$. The greatest common divisor must therefore be $= \Delta$. — Thus, if m, n are relatively prime, $\alpha m + \beta n$. $\gamma m + \delta n$ are also relatively prime.

167.

THEOREM. *Suppose the forms*

$$axx + 2bxy + cyy \quad \ldots\ldots (F)$$

$$a'x'x' + 2b'x'y' + c'y'y' \quad \ldots\ldots (F')$$

are equivalent, their determinant $= D$*, and the latter changes into the former on putting*

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

Suppose also that the number M *is represented by* F *on putting* $x = m$*,* $y = n$*, and so by* F' *on putting*

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

with m *relatively prime to* n*, and therefore also* m' *to* n'*. Then the two representations belong either to the same value of the expression* $\sqrt{D}(\text{mod. } M)$ *or to opposite values, according as the transformation of the form* F' *into* F *is proper or improper.*

Proof. Choose the numbers μ, ν so that $\mu m + \nu n = 1$, and put

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

These are integers because $\alpha\delta - \gamma\beta = \pm 1$. Then

$$\mu' m' + \nu' n' = 1. \quad \text{(See the end of the preceding article.)}$$

Further, put

$$\mu(bm + cn) - \nu(am + bn) = V,$$
$$\mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$$

Then V, V' are values of the expression $\sqrt{D}(\text{mod. } M)$ to which the first and second representations belong. If in V' we substitute the values of μ', ν', m', n', and in V substitute

$$\begin{array}{lll} \text{for} & a, & a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma \\ \text{for} & b, & a'a\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta \\ \text{for} & c, & a'\beta\beta + 2b'\beta\delta + c'\delta\delta \end{array}$$

expansion gives $V = V'(\alpha\delta - \beta\gamma)$.

So either $V = V'$ or $V = -V'$, according as $\alpha\delta - \beta\gamma = +1$ or $= -1$. *That is*, the representations belong to the same value of the expression $\sqrt{D}(\text{mod. } M)$ or to opposite values, according as the transformation of the form F' into F is proper or improper. *Q. E. D.*

Thus, if several representations of the number M by the form (a, b, c), using relatively prime values of the indeterminates x, y, belong to *different* values of the

expression $\sqrt{D}(\text{mod. } M)$, the corresponding representations by the form (a', b', c') belong to those same respective values. If there is no representation of the number M by a form belonging to a particular value, there is also none belonging to this value by an equivalent form.

168.

THEOREM. *If the number M is represented by the form $axx+2bxy+cyy$ by assigning to x, y relatively prime values m, n, and the value of the expression $\sqrt{D}(\text{mod. } M)$ to which this representation belongs is N, then the forms (a, b, c), $(M, N, \frac{NN-D}{M})$ are properly equivalent.*

Proof. Article 155 shows that integers μ, ν can be found so that

$$m\mu + n\nu = 1, \quad \mu(bm + cn) - \nu(am + bn) = N$$

Then the form (a, b, c), under the substitution $x = mx' - \nu y'$, $y = nx' + \mu y'$, which is clearly proper, changes into a form whose determinant $= D(m\mu + n\nu)^2$, *that is*, $= D$, and so into an equivalent form. If we write this form $= (M', N', \frac{N'N'-D}{M'})$, we have

$$M' = amm + 2bmn + cnn = M,$$
$$N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N$$

So the form into which (a, b, c) changes under that transformation is $(M, N, \frac{NN-D}{M})$. *Q. E. D.*

The equations

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

also give

$$\mu = \frac{nN + ma + nb}{amm + 2bmn + cnn} = \frac{nN + ma + nb}{M},$$
$$\nu = \frac{mb + nc - mN}{M}$$

so these numbers are integers.

We must also note that this proposition does not apply if $M = 0$, since the term $\frac{NN-D}{M}$ is then indeterminate*).

169.

If we have several representations of the number M by (a, b, c) belonging to the same value of the expression $\sqrt{D}(\text{mod. } M)$, N (always assuming the values of x, y to be relatively prime), several proper transformations of the form $(a, b, c)..(F)$ into $(M.\ N, \frac{NN-D}{M})..(G)$ can also be derived from them. For if such a representation also comes from the values $x = m'$, $y = n'$, then (F) also changes under the substitution

*)In this case, if we wish to extend our wording to it, saying that N is a value of the expression $\sqrt{D}(\text{mod. } M)$, or that $NN \equiv D(\text{mod. } M)$, means that $NN - D$ is a multiple of M, and so $= 0$.

$$x = m'x' + \frac{m'N - m'b - n'c}{M}y',$$
$$y = n'x' + \frac{n'N + m'a + n'b}{M}y'$$

into (G). Conversely, every proper transformation of the form (F) into (G) gives a representation of the number M by the form (F) belonging to the value N. For if (F) changes into (G) on putting $x = mx' - \nu y'$, $y = nx' + \mu y'$, then M is represented by (F) on putting $x = m$, $y = n$. Since here $m\mu + n\nu = 1$, the value of the expression $\sqrt{D}(\mathrm{mod.}\, M)$ to which the representation belongs is $\mu(bm+cn) - \nu(am+bn)$, *that is*, N. Several different proper transformations give just as many different representations belonging to N*). — It follows easily that once all proper transformations of the form (F) into (G) are known, they give all representations of M by (F) belonging to the value N. So the problem of finding representations of a given number by a given form, in which the indeterminates have relatively prime values, has been reduced to finding all proper transformations of that form into a given equivalent form.

Applying the results of Article 162, we easily conclude: if one representation of the number M by the form (F) belonging to the value N is $x = \alpha$, $y = \gamma$, then the general formula including all representations of the same number by the form (F) belonging to the value N is

$$x = \frac{\alpha t - (\alpha b + \gamma c)u}{m}, \quad y = \frac{\gamma t + (\alpha a + \gamma b)u}{m}$$

where m is the greatest common divisor of the numbers $a, 2b, c$, and t, u stand for all numbers satisfying the equation $tt - Duu = mm$.

170.

If the form (a, b, c) is equivalent to an ambiguous form, and so is both properly and improperly equivalent to the form $(M, N, \frac{NN-D}{M})$, or properly equivalent both to the form $(M, N, \frac{NN-D}{M})$ and to $(M, -N, \frac{NN-D}{M})$, there are representations of the number M by the form (F) belonging both to the value N and to the value $-N$. Conversely, if several representations of the number M by the same form (F) belong to *opposite* values of the expression $\sqrt{D}(\mathrm{mod.}\, M)$, $N, -N$, then the form (F) is both properly and improperly equivalent to the form (G), and an ambiguous form equivalent to (F) can be found.

*) If two different proper transformations are assumed to give the same representation, they must have the following form:

1) $x = mx' - \nu y', \quad y = nx' + \mu y';$
2) $x = mx' - \nu' y', \quad y = nx' + \mu' x'.$

But the two equations

$$m\mu + n\nu = m\mu' + n\nu',$$
$$\mu(mb + nc) - \nu(ma + nb) = \mu'(mb + nc) - \nu'(ma + nb),$$

easily give either $M = 0$ or $\mu = \mu'$, $\nu = \nu'$. We have already excluded $M = 0$.

Let these general results on representations suffice here. We will discuss representations in which the indeterminates do not have relatively prime values below. As for other properties, forms with negative determinant need a completely different treatment from forms with positive determinant, so we will now consider them separately. We begin with the former, as the easier ones.

Forms with negative determinant.

171.

PROBLEM. *Given any form (a, b, a') with negative determinant $= -D$, where D denotes a positive number, find a properly equivalent form (A, B, C) in which A is no greater than $\sqrt{\frac{4}{3}}D$, C, and no smaller than $2B$.*

Solution. We assume that the given form does not satisfy all three conditions at once; otherwise there would be no need to look for another form. Let b' be the absolutely least residue of the number $-b$ modulo a'[*)], and let $a'' = \frac{b'b'+D}{a'}$, which is an integer because $b'b' \equiv bb$, $b'b' + D \equiv bb + D \equiv aa' \equiv 0 (\mathrm{mod.}\, a')$. Now if $a'' < a'$, again let b'' be the absolutely least residue of $-b'$ modulo a'', and let $a''' = \frac{b''b''+D}{a''}$. If again $a''' < a''$, once more let b''' be the absolutely least residue of $-b''$ modulo a''' and let $a'''' = \frac{b'''b'''+D}{a'''}$. Continue this operation until the sequence a', a'', a''', a'''' etc. reaches a term a^{m+1} no smaller than its predecessor a^m. This must eventually happen, since otherwise we would have an infinite sequence of integers that keep decreasing. Then the form (a^m, b^m, a^{m+1}) satisfies all the conditions.

Proof. I. In the sequence of forms (a, b, a'), (a', b', a''), (a'', b'', a''') etc., each is a neighbor of its predecessor, so the last is properly equivalent to the first (Articles 159, 160). II. Since b^m is the absolutely least residue of $-b^{m-1}$ modulo a^m, it is no greater than $\frac{1}{2}a^m$ (Article 4).

III. Since $a^m a^{m+1} = D + b^m b^m$, and a^{m+1} is not $< a^m$, $a^m a^m$ is not $> D + b^m b^m$. Since b^m is not $> \frac{1}{2}a^m$, $a^m a^m$ is not $> D + \frac{1}{4}a^m a^m$, and $\frac{3}{4}a^m a^m$ is not $> D$; finally, a^m is *not* $> \sqrt{\frac{4}{3}}D$.

Example. Let the given form be $(304, 217, 155)$, whose determinant $= -31$. Here we find the sequence of forms:

$$(304, 217, 155),\ (155, -62, 25),\ (25, 12, 7),\ (7, 2, 5),\ (5, -2, 7).$$

The last is the one we want. — In the same way, for the form $(121, 49, 20)$, whose determinant $= -19$, we find the equivalent forms $(20, -9, 5)$, $(5, -1, 4)$, $(4, 1, 5)$; so $(4, 1, 5)$ is the form we want.

We will call forms (A, B, C) with negative determinant, in which A is no greater than $\sqrt{\frac{4}{3}}D, C$ and no smaller than $2B$, *reduced forms.* So for any form with negative determinant, a properly equivalent reduced form can be found.

[*)] Notice that if, in a form (a, b, a'), the first or last term a or a' is $= 0$, its determinant is a positive square, so this cannot happen in the present case. — For a similar reason, the outer terms a, a' of a form with negative determinant cannot have opposite signs.

172.

PROBLEM. *Find the conditions under which two nonidentical reduced forms with the same determinant $-D$, (a,b,c), (a',b',c'), can be properly equivalent.*

Solution. We may assume that a' is not $> a$, and that the form $axx + 2bxy + cyy$ changes into $a'x'x' + 2b'x'y' + c'y'y'$ under the proper substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Then we have the equations

$$\begin{aligned} a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a' \quad & \ldots\ldots\ldots [1] \\ a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b' \quad & \ldots\ldots\ldots [2] \\ \alpha\delta - \beta\gamma = 1 \quad & \ldots\ldots\ldots [3] \end{aligned}$$

From [1] we get $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$, so aa' is positive. Since $ac = D + bb$, $a'c' = D + b'b'$, ac and $a'c'$ are also positive; so a, a', c, c' all have the same sign. But both a and a' are not $> \sqrt{\frac{4}{3}}D$, so aa' is not $> \sqrt{\frac{4}{3}}D$; still less, then, can $D\gamma\gamma$ $(= aa' - (a\alpha + b\gamma)^2)$ be greater than $\frac{4}{3}D$. Thus γ is either $= 0$ or $= \pm 1$.

I. If $\gamma = 0$, [3] gives either $\alpha = 1. \delta = 1$ or $\alpha = -1$, $\delta = -1$. In both cases [1] gives $a' = a$, and [2] gives $b' - b = \pm\beta a$. But b is not $> \frac{1}{2}a$, and b' is not $> \frac{1}{2}a'$, so it is also not $> \frac{1}{2}a$. Thus the equation $b' - b = \pm\beta a$ can hold only if

either $b = b'$, which would give $c' = \frac{b'b'+D}{a'} = \frac{bb+D}{a} = c$, making the forms (a,b,c), (a',b',c') identical, against our assumption;

or $b = -b' = \pm\frac{1}{2}a$. In this case too, $c' = c$, and the form (a',b',c') is $(a,-b,c)$, *that is*, the opposite of the form (a,b,c). It is also clear that these forms are ambiguous, since $2b = \pm a$.

II. If $\gamma = \pm 1$, [1] gives $a\alpha\alpha + c - a' = \pm 2b\alpha$. But c is no smaller than a, so it is no smaller than a'. Thus $a\alpha\alpha + c - a'$, or $2b\alpha$, is certainly no smaller than $a\alpha\alpha$. Since $2b$ is no greater than a, α is no smaller than $\alpha\alpha$; so necessarily either $\alpha = 0$ or $= \pm 1$.

1) If $\alpha = 0$, [1] gives $a' = c$, and since a is neither greater than c nor smaller than a', necessarily $a' = a = c$. Further, [3] gives $\beta\gamma = -1$, so [2] gives $b + b' = \pm\delta c = \pm\delta a$. From this, as in (I), we get

either $b = b'$, in which case the forms (a,b,c), (a',b',c') would be identical, against our assumption;

or $b = -b'$, in which case the forms (a,b,c), (a',b',c') are opposite.

2) If $\alpha = \pm 1$, [1] gives $\pm 2b = a + c - a'$. So, since a is not smaller and $c < a'$ does not hold, $2b$ is not $< a$ and not $< c$. But $2b$ is also not $> a$ or $> c$, so necessarily $\pm 2b = a = c$, and from the equation $\pm 2b = a + c - a'$, also $= a'$. Thus [2] gives

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

or, since $\alpha\delta - \beta\gamma = 1$,

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma)$$

so necessarily, as before,

either $b = b'$, making the forms (a,b,c), (a',b',c') identical, against our assumption;

or $b = -b'$, so those forms are opposite. In this case too, since $a = \pm 2b$, the forms are ambiguous.

From all this we conclude that the forms (a, b, c), (a', b', c') can be properly equivalent only if they are opposite and, at the same time, *either* ambiguous *or* $a = c = a' = c'$. That the forms (a, b, c), (a', b', c') are properly equivalent in these cases could also have been seen easily in advance. For opposite forms must be improperly equivalent, and if they are also ambiguous, they must be properly equivalent too. If $a = c$, the form $(\frac{D+(a-b)^2}{a}, a - b, a)$ is a neighbor of the form (a, b, c) and so equivalent to it. But since $D + bb = ac = aa$, we have $\frac{D+(a-b)^2}{a} = 2a - 2b$, and the form $(2a - 2b, a - b, a)$ is ambiguous; so (a, b, c) is properly equivalent to its opposite too.

We can now decide just as easily when two reduced forms (a, b, c), (a', b', c') that are not opposite can be improperly equivalent. They are improperly equivalent if (a, b, c), $(a', -b', c')$, which are not identical, are properly equivalent, and conversely. Thus the condition for *the former* to be improperly equivalent is that they are identical and, in addition, either ambiguous or $a = c$. — Reduced forms that are neither identical nor opposite can be neither properly nor improperly equivalent.

173.

Problem. *Given two forms F and F' with the same negative determinant, determine whether they are equivalent.*

Solution. Find two reduced forms f, f' properly equivalent to the forms F, F', respectively. If the forms f, f' are properly equivalent, improperly equivalent, or equivalent in both ways, so are F, F'. If f, f' are not equivalent in any way, neither are F, F'.

The preceding article gives four possible cases:

1) If f, f' are neither identical nor opposite, F, F' are not equivalent in any way.

2) If f, f' are *first* either identical or opposite, and *second* either ambiguous or have equal outer terms, F, F' are both properly and improperly equivalent.

3) If f, f' are identical, but neither ambiguous nor have equal outer terms, F, F' are only properly equivalent.

4) If f, f' are opposite, but neither ambiguous nor have equal outer terms, F, F' are only improperly equivalent.

Example. For the forms $(41, 35, 30)$, $(7, 18, 47)$, whose determinant $= -5$, we find the equivalent reduced forms $(1, 0, 5)$, $(2, 1, 3)$; so the given forms are not equivalent in any way. — But the forms $(23, 38, 63)$, $(15, 20, 27)$ have the same equivalent reduced form $(2, 1, 3)$. Since it is also ambiguous, the forms $(23, 38, 63)$, $(15, 20, 27)$ are both properly and improperly equivalent. — For the forms $(37, 53, 78)$, $(53, 73, 102)$, the equivalent reduced forms are $(9, 2, 9)$, $(9, -2, 9)$. Since the reduced forms are opposite and their outer terms are equal, the given forms are both properly and improperly equivalent.

174.

The number of all reduced forms with a given determinant $-D$ is always finite and fairly small in relation to the number D. The forms themselves can be found in two ways. Denote the reduced forms with determinant $-D$ generally by (a, b, c); we then have to determine all the values of a, b, c.

First method. For a, take all numbers, both positive and negative, no greater than $\sqrt{\frac{4}{3}D}$, for which $-D$ is a quadratic residue. For each a, let b successively equal all values of the expression $\sqrt{-D}$ (mod. a) no greater than $\frac{1}{2}a$, taken both positively and negatively. For c, given each determined pair of values of a, b, put $= \frac{D+bb}{a}$. Discard any forms produced this way in which $c < a$; the others are clearly reduced.

Second method. For b, take all numbers, both positive and negative, no greater than $\frac{1}{2}\sqrt{\frac{4}{3}D}$, or $\sqrt{\frac{1}{3}D}$. For each b, factor $bb + D$ in every possible way into two factors (also taking differences of sign into account), both no smaller than $2b$. Put one factor—the smaller one when they are unequal—$= a$, and the other $= c$. Since a is not $> \sqrt{\frac{4}{3}D}$, all forms obtained this way are clearly reduced. — Finally, it is clear that no reduced form can fail to be found by either method.

Example. Let $D = 85$. Here the bound on the values of a is $\sqrt{\frac{340}{3}}$, which lies between 10 and 11. The numbers between 1 and 10 (inclusive) for which -85 is a residue are $1, 2, 5, 10$. This gives twelve forms:

$$(1, 0, 85),\ (2, 1, 43),\ (2, -1, 43),\ (5, 0, 17),$$
$$(10, 5, 11),\ (10. -5, 11);\ (-1, 0, -85),\ (-2, 1, -43),$$
$$(-2, -1, -43).\ (-5, 0, -17),\ (-10, 5, -11,\ (-10, -5, -11).$$

The other method gives, for the values of b, the bound $\sqrt{\frac{85}{3}}$, which lies between 5 and 6. For $b = 0$, we get the forms

$$(1, 0, 85),\ (-1, 0, -85),\ (5, 0, 17),\ (-5, 0, -17),$$

and for $b = \pm 1$, these: $(2, \pm 1, 43)$, $(-2, \pm 1, -43)$.

For $b = \pm 2$, there are none, since 89 cannot be factored into two factors both not < 4. The same holds for ± 3, ± 4. Finally, for $b = \pm 5$, we get

$$(10, \pm 5, 11),\ (-10, \pm 5. -11).$$

175.

From all reduced forms with a given determinant, discard one of each pair of forms that, though not identical, are properly equivalent. The remaining forms have this notable property: every form with the same determinant is properly equivalent to one of them, and to only one (otherwise some of them would be properly equivalent to one another). Thus *all forms with the same determinant can be divided into as many classes as there are forms remaining*, by putting forms properly equivalent to the same reduced form into the same class. For $D = 85$, for example, the remaining forms are

$$(1, 0, 85),\ (2, 1, 43),\ (5, 0, 17),\ (10, 5, 11),$$
$$(-1, 0. -84),\ (-2, 1, -43).\ (-5, 0, -17),\ (-10, 5, -11)$$

so all forms with determinant -85 can be divided into eight classes, according as they are properly equivalent to the first form, the second, etc. Clearly, forms in the same class are properly equivalent, and forms from different classes cannot be properly equivalent. We will discuss this subject of classifying forms much more fully below. Here we add just one observation. We showed above that if the determinant of the form (a, b, c) is negative $= -D$, a and c have the same sign (since $ac = bb + D$, which is positive). In the same way, it is easy to see that if the forms (a, b, c), (a', b', c') are equivalent, all of a, c, a', c' have the same sign. For if the first changes into the second under the substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, then $a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a'$, giving $aa' = (a\alpha + b\beta)^2 + D\gamma\gamma$, which is certainly nonnegative. Since a cannot be zero and $a' = 0$ cannot hold, aa' is positive, so a, a' have the same sign.

This makes it clear that forms whose outer terms are positive are completely separate from those whose outer terms are negative. It is enough to consider just the reduced forms with positive outer terms, since the others are equal in number and come from them by giving the outer terms opposite signs. The same holds for the forms to be discarded from the reduced forms and those to be retained.

176.

Here, then, is a table of forms for certain negative determinants, according to which all other forms with the same determinant can be divided into classes. In line with the observation in the preceding article, we give only half of them, those with positive outer terms.

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	$(1, 0, 12)$, $(2, 0, 6)$, $(3, 0, 4)$, $(4, 2, 4)$.

There would be no need to continue this table further here, since below we will show how to arrange it much more usefully.

So every form with determinant -1 is properly equivalent to the form $xx + yy$ if its outer terms are positive, or to $-xx - yy$ if they are negative; every form with determinant -2 whose outer terms are positive is properly equivalent to the form $xx + 2yy$, etc.; every form with determinant -11 whose outer terms are positive, to one of $xx + 11yy$, $2xx + 2xy + 6yy$, $3xx + 2xy + 4yy$, $3xx - 2xy + 4yy$, etc.

177.

PROBLEM. *Given a sequence of forms, each a right neighbor of its predecessor, find a proper transformation of the first into any form in the sequence.*

Solution. Let the forms be $(a,b,a') = F$; $(a',b',a'') = F'$; $(a'',b'',a''') = F''$; $(a''',b''',a'''') = F'''$ etc. Denote $\frac{b+b'}{a'}$, $\frac{b'+b''}{a''}$, $\frac{b''+b'''}{a'''}$ etc. by h', h'', h''' etc., respectively. Let the indeterminates of the forms F, F', F'' etc. be x, y; x', y'; x'', y'' etc. Suppose F changes

into F'	for	$x = \alpha' x' + \beta' y'$,	$y = \gamma' x' + \delta' y'$
F''	...	$x = \alpha'' x'' + \beta'' y''$,	$y = \gamma'' x'' + \delta'' y''$
F'''	...	$x = \alpha''' x''' + \beta''' y'''$,	$y = \gamma''' x''' + \delta''' y'''$
		etc.	

Then since F changes into F' for $x = -y'$, $y = x' + h'y'$
F' into F'' for $x' = -y''$, $y' = x'' + h''y''$
F'' into F''' for $x'' = -y'''$, $y'' = x''' + h'''y'''$ etc. (Article 160)

we easily obtain the following algorithm (Article 159):

$\alpha' = 0$	$\beta' = -1$	$\gamma' = 1$	$\delta' = h'$
$\alpha'' = \beta'$	$\beta'' = h''\beta' - \alpha'$	$\gamma'' = \delta'$	$\delta'' = h''\delta' - \gamma'$
$\alpha''' = \beta''$	$\beta''' = h'''\beta'' - \alpha''$	$\gamma''' = \delta''$	$\delta''' = h'''\delta'' - \gamma''$
$\alpha'''' = \beta'''$	$\beta'''' = h''''\beta''' - \alpha'''$	$\gamma'''' = \delta'''$	$\delta'''' = h''''\delta''' - \gamma'''$
	etc.		

or

$\alpha' = 0$	$\beta' = -1$	$\gamma' = 1$	$\delta' = h'$
$\alpha'' = \beta'$	$\beta'' = h''\beta'$	$\gamma'' = \delta'$	$\delta'' = h''\delta' - 1$
$\alpha''' = \beta''$	$\beta''' = h'''\beta'' - \beta'$	$\gamma''' = \delta''$	$\delta''' = h'''\delta'' - \delta'$
$\alpha'''' = \beta'''$	$\beta'''' = h''''\beta''' - \beta''$	$\gamma'''' = \delta'''$	$\delta'''' = h''''\delta''' - \delta''$
	etc.		

That all these transformations are proper follows easily both from their construction and from Article 159.

This very simple algorithm is convenient for calculation and is analogous to the algorithm given in Article 27; it can also be reduced to that algorithm*). This solution is not restricted to forms with negative determinant: it applies to all cases, provided none of the numbers a', a'', a''' etc. is $= 0$.

*)In the notation of Article 27, we have $\beta^n = \pm[-h'', h''', -h'''' \ldots \pm h^n]$, where the alternative signs must be $--$; $-+$; $+-$; $++$, according as n has the form $4k+0$; 1; 2; 3, and

$$\delta^n = \pm[h', -h'', h''' \ldots . \pm h^n]$$

where the alternative signs must be $+-$; $++$; $--$; $-+$, according as n has the form $4k+0$; 1; 2; 3. But to keep this brief, we cannot develop this further; anyone can easily confirm it for themselves.

178.

PROBLEM. *Given two properly equivalent forms F, f with the same negative determinant, find a proper transformation of one into the other.*

Solution. Suppose the form F is (A, B, A'), and that the method of Article 171 has given the sequence of forms (A', B', A''), (A'', B'', A''') etc. up to (A^m, B^m, A^{m+1}), which is reduced. Similarly, suppose f is (a, b, a'), and the same method has given the sequence (a', b', a''), (a'', b'', a''') up to (a^n, b^n, a^{n+1}), which is reduced. There are then two possible cases.

I. The forms (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) are either identical, or opposite and also ambiguous. Then the forms (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$ are neighbors (where A^{m-1} denotes the next-to-last term of the sequence $A, A', A'' \dots A^m$, and B^{m-1}, a^{n-1}, b^{n-1} have similar meanings). For $A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ or } A^m}$, giving $B^{m-1} - b^{n-1} \equiv b^n - B^m$ and so $\equiv 0$ if the forms (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) are identical, and $\equiv 2b^n$, so $\equiv 0$, if they are opposite and ambiguous. Thus, in the sequence of forms

$$(A, B, A'),\ (A', B', A'') \dots (A^{m-1}, B^{m-1}, A^m),$$
$$(a^n, -b^{n-1}, a^{n-1}),\ (a^{n-1}, -b^{n-2}, a^{n-2}) \dots (a', -b, a),\ (a, b, a')$$

each form is a neighbor of its predecessor. By the preceding article, we can therefore find a proper transformation of the first, F, into the last, f.

II. The forms (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) are not identical but opposite, and also $A^m = A^{m+1} = a^n = a^{n+1}$. Then the sequence of forms

$$(A, B, A'),\ (A', B', A'') \dots (A^m, B^m, A^{m+1}),$$
$$(a^n, -b^{n-1}, a^{n-1}),\ (a^{n-1}, -b^{n-2}, a^{n-2}) \dots (a', -b, a),\ (a, b, a')$$

has the same property. For $A^{m+1} = a^n$, and $B^m - b^{n-1} = -(b^n + b^{n-1})$ is divisible by a^n. So the preceding article gives a proper transformation of the first form F into the last f.

Example. For the forms $(23.\,38, 63)$, $(15, 20, 27)$, we have the sequence

$$(23, 38, 63).\ (63, 25, 10),\ (10, 5, 3),\ (3, 1.\,2),$$
$$(2.\,-7, 27),\ (27, -20, 15),\ (15, 20, 27)$$

so

$$h' = 1, \quad h'' = 3, \quad h''' = 2, \quad h'''' = -3, \quad h''''' = -1, \quad h'''''' = 0.$$

This gives the following transformation of the form $23xx + 76xy + 63yy$ into $15tt + 40tu + 27uu$: $x = -13t - 18u$, $y = 8t + 11u$.

This solution easily gives the solution of the problem: *If the forms F, f are improperly equivalent, find an improper transformation of the form F into f.* For let $f = att + 2btu + a'uu$; then the opposite form $app - 2bpq + a'qq$ is properly equivalent to the form F. Find a proper transformation of the form F into that form, $x = \alpha p + \beta q$, $y = \gamma p + \delta q$. Clearly F changes into f on putting $x = \alpha t - \beta u$, $y = \gamma t - \delta u$, and this transformation is improper.

So if the forms F, f are both properly and improperly equivalent, we can find both a proper and an improper transformation.

179.

PROBLEM. *If the forms F, f are equivalent, find all transformations of the form F into f.*

Solution. If the forms F, f are equivalent in only one way, *that is*, only properly or only improperly, use the preceding article to find one transformation of the form F into f. Clearly there can be no other transformations except those similar to this one. If the forms F, f are both properly and improperly equivalent, find two transformations, one proper and the other improper. Now take the form $F = (A, B, C)$, with $BB - AC = -D$, and let the greatest common divisor of the numbers $A, 2B, C$ be $= m$. Article 162 shows that, in the first case, all transformations of the form F into f can be derived from one transformation; in the second, all proper transformations can be derived from the proper one and all improper transformations from the improper one, provided we have all solutions of the equation $tt + Duu = mm$. Once these have been found, the problem is solved.

But we have $D = AC - BB$, $4D = 4AC - 4BB$, so $\frac{4D}{mm} = 4\frac{AC}{mm} - (\frac{2B}{m})^2$ is an integer. Now if

1) $\frac{4D}{mm} > 4$, we have $D > mm$. So in $tt + Duu = mm$, u must be $= 0$, and t can have no values other than $+m$ and $-m$. Thus, if F, f are equivalent in only one way and one transformation is

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

there can be no others except this one, which comes from $t = m$ (Article 162), and

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

If F, f are both properly and improperly equivalent, and we have a proper transformation

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

and an improper one

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

there is no other proper transformation except the former (from $t = m$) and

$$x = -\alpha x' - \beta y', \ y = -\gamma x' - \delta y' \text{ (from } t = -m)$$

and likewise no improper transformation except

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y';$$
$$\text{and } x = -\alpha' x' - \beta' y', \quad y' = -\gamma' x' - \delta' y'$$

2) If $\frac{4D}{mm} = 4$, or $D = mm$, the equation $tt + Duu = mm$ has four solutions $t, u; = m, 0; \ -m, 0; \ 0, 1; \ 0, -1$. So if F, f are equivalent in only one way and one transformation is

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

there are exactly *four* transformations,

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

$$x = \mp\frac{\alpha B + \gamma C}{m}x' \mp \frac{\beta B + \delta C}{m}y',$$
$$y = \pm\frac{\alpha A + \gamma B}{m}x' \pm \frac{\beta A + \delta B}{m}y'$$

If F, f are equivalent in two ways, or there is another transformation dissimilar to the given one, this also gives four transformations dissimilar to the former four, making *eight* transformations. — It is also easy to prove that in this case F, f really are always equivalent in both ways. For since $D = mm = AC - BB$, m divides B too. The form $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ has determinant $= -1$, so it is equivalent to the form $(1, 0, 1)$ or to $(-1, 0, -1)$. It is easy to see that the same transformation that changes $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ into $(\pm 1, 0, \pm 1)$ changes the form (A, B, C) into $(\pm m, 0, \pm m)$, which is ambiguous. So the form (A, B, C), being equivalent to an ambiguous form, is both properly and improperly equivalent to every form equivalent to it.

3) If $\frac{4D}{mm} = 3$, or $4D = 3mm$, m is even, and all solutions of the equation $tt + Duu = mm$ are these six:

$$t, u; = m, 0;\ -m, 0;\ \tfrac{1}{2}m, 1;\ -\tfrac{1}{2}m, -1;\ \tfrac{1}{2}m, -1;\ -\tfrac{1}{2}m, 1$$

So if we have two dissimilar transformations of the form F into f,

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

we have twelve transformations, namely six similar to the first,

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \pm(\tfrac{1}{2}\alpha - \tfrac{\alpha B + \gamma C}{m})x' \pm (\tfrac{1}{2}\beta - \tfrac{\beta B + \delta C}{m})y'$$
$$y = \pm(\tfrac{1}{2}\gamma + \tfrac{\alpha A + \gamma B}{m})x' \pm (\tfrac{1}{2}\delta + \tfrac{\beta A + \delta B}{m})y'$$
$$x = \pm(\tfrac{1}{2}\alpha + \tfrac{\alpha B + \gamma C}{m})x' \pm (\tfrac{1}{2}\beta + \tfrac{\beta B + \delta C}{m})y'$$
$$y = \pm(\tfrac{1}{2}\gamma - \tfrac{\alpha A + \gamma B}{m})x' \pm (\tfrac{1}{2}\delta - \tfrac{\beta A + \delta B}{m})y'$$

and six similar to the second, obtained from these by replacing α, β, γ, δ with α', β', γ', δ'.

That in this case F, f are always equivalent in both ways is proved as follows. The form $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ has determinant $= -\frac{4D}{mm} = -3$, so this form (Article 176) is equivalent either to the form $(\pm 1, 0, \pm 3)$ or to $(\pm 2, \pm 1, \pm 2)$. From this it is easy to see that the form (A, B, C) is equivalent either to the form $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ or to $(\pm m, \frac{1}{2}m, \pm m)$*), both of which are ambiguous, and so is equivalent in both ways to every equivalent form.

4) If we assume $\frac{4D}{mm} = 2$, we get $(\frac{2B}{m})^2 = 4\frac{AC}{mm} - 2$, and so $\equiv 2 \pmod 4$. But no square can be $\equiv 2 \pmod 4$, so this case cannot occur.

5) Assuming $\frac{4D}{mm} = 1$, we get $(\frac{2B}{m})^2 = 4\frac{AC}{mm} - 1 \equiv -1 \pmod 4$. Since this is impossible, this case cannot occur either.

Since D is neither $= 0$ nor negative, no cases other than those listed are possible.

*) It can be proved that the form (A, B, C) is necessarily equivalent to the latter, but this is not needed here.

180.

PROBLEM. *Find all representations of a given number M by the form $axx+2bxy+cyy\ldots F$ with negative determinant $-D$, in which x, y take relatively prime values.*

Solution. Article 154 shows that M cannot be represented in the required way unless $-D$ is a quadratic residue of M. First find all distinct (*that is*, incongruent) values of the expression $\sqrt{-D}$ (mod. M), say $N, -N, N', -N', N'', -N''$ etc. To make the calculation simpler, all N, N' etc. can be chosen so that they are not $> \frac{1}{2}M$. Since each representation must belong to one of these values, consider each value separately.

If the forms $F, (M, N, \frac{D+NN}{M})$ are not properly equivalent, there can be no representation of M belonging to the value N (Article 168). If they are, find a proper transformation of the form F into

$$Mx'x' + 2Nx'y' + \frac{D+NN}{M}y'y'$$

say

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

Then $x = \alpha, y = \gamma$ is a representation of the number M by F belonging to N. Let the greatest common divisor of the numbers $A, 2B, C, = m$. We distinguish three cases (preceding article):

1) If $\frac{4D}{mm} > 4$, there are no representations belonging to N other than these *two*: $x = \alpha, y = \gamma$; $x = -\alpha, y = -\gamma$ (Articles 169, 179).

2) If $\frac{4D}{mm} = 4$, there are *four* representations

$$x = \pm\alpha, \quad y = \pm\gamma; \quad x = \mp\frac{\alpha B + \gamma C}{m}, \quad y = \pm\frac{\alpha A + \gamma B}{m}$$

3) If $\frac{4D}{mm} = 3$, there are *six* representations

$$\begin{array}{ll} x = \pm\alpha, & y = \pm\gamma; \\ x = \pm(\frac{1}{2}\alpha - \frac{\alpha B+\gamma C}{m}), & y = \pm(\frac{1}{2}\gamma + \frac{\alpha A+\gamma B}{m}) \\ x = \pm(\frac{1}{2}\alpha + \frac{\alpha B+\gamma C}{m}), & y = \pm(\frac{1}{2}\gamma - \frac{\alpha A+\gamma B}{m}) \end{array}$$

Representations belonging to the values $-N.N', -N'$ etc. must be found in the same way.

181.

Finding the representations of the number M by the form F in which x, y take values that are not relatively prime can easily be reduced to the case already considered. Suppose such a representation is obtained on putting $x = \mu e, y = \mu f$, where μ is the greatest common divisor of $\mu e, \mu f$, that is, e, f are relatively prime. Then $M = \mu\mu(Aee + 2Bef + Cff)$, which is therefore divisible by $\mu\mu$. The substitution $x = e, y = f$ is a representation of the number $\frac{M}{\mu\mu}$ by the form F in which x, y take relatively prime values. So if M is divisible by no square (other than 1), *for example*, if it is prime, there are no such representations of M. If M has square divisors, let them be $\mu\mu, \nu\nu, \pi\pi$ etc. First find all representations of the number $\frac{M}{\mu\mu}$ by the form (A, B, C) in which x, y take relatively prime values. Multiplying these values by μ gives all representations of M in which the greatest common divisor of the numbers x, y is μ. Similarly, all representations of $\frac{M}{\nu\nu}$ in which the values of x, y are relatively prime give all representations of M in which the greatest common divisor of the values of x, y is ν, etc.

So the preceding rules find all representations of a given number by a given form with negative determinant.

Special applications to writing numbers as sums of two squares, a square and twice a square, a square and three times a square.

182.

We turn to some special cases, both for their remarkable elegance and for the sustained attention the distinguished Euler gave them, which has earned them something of the status of classics.

I. A number can be represented by the form $xx + yy$ with x relatively prime to y (or written as a sum of two relatively prime squares) only if -1 is a quadratic residue of it. Conversely, every such number, taken positively, can be represented. Let M be such a number, and let all values of the expression $\sqrt{-1}$ (mod. M) be $N, -N, N', -N', N'', -N''$ etc. Then, by Article 176, the form $(M, N, \frac{NN+1}{M})$ is properly equivalent to the form $(1, 0, 1)$. Let a proper transformation of the latter into the former be $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. The representations of the number M by the form $xx + yy$ belonging to N are then these four[*)]: $x = \pm\alpha, y = \pm\gamma$; $x = \mp\gamma, y = \pm\alpha$.

Since the form $(1, 0, 1)$ is ambiguous, the form $(M, -N, \frac{NN+1}{M})$ is clearly also properly equivalent to it, and the former changes properly into the latter on putting $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. This gives four representations of M belonging to $-N$: $x = \pm\alpha, y = \mp\gamma$; $x = \pm\gamma, y = \pm\alpha$. So there are eight representations of M, half belonging to N and half to $-N$. But all these give only *one* decomposition of the number M into two squares, $M = \alpha\alpha + \gamma\gamma$, if we consider only the squares themselves, without regard to their order or the signs of their roots.

So if there are no values of the expression $\sqrt{-1}$ (mod. M) other than N and $-N$, as happens, *for example*, when M is prime, M can be written as a sum of two relatively prime squares in only one way. Now -1 is a quadratic residue of every prime of the form $4n + 1$ (Article 108), and a prime clearly cannot be written as a sum of two squares that are not relatively prime. We therefore have the theorem:

Every prime of the form $4n + 1$ can be written as a sum of two squares, in only one way.

$$1 = 0 + 1, \quad 5 = 1 + 4, \quad 13 = 4 + 9, \quad 17 = 1 + 16,$$
$$29 = 4 + 25, \quad 37 = 1 + 36, \quad 41 = 16 + 25, \quad 53 = 4 + 49,$$
$$61 = 25 + 36, \quad 73 = 9 + 64, \quad 89 = 25 + 64, \quad 97 = 16 + 81 \quad \text{etc.}$$

This very elegant theorem was already known to Fermat, but was first proved by the distinguished Euler, *Comm. nov. Petr. Vol.* V, *for the years* 1754, 1755, *p.* 3 ff. *Vol.* IV contains a paper on the same subject, *p.* 3 ff., but he had not yet completed the matter there; see especially Article 27.

So if a number of the form $4n + 1$ can be written as a sum of two squares either in several ways or in no way, it is certainly not prime.

[*)] This case is clearly covered by (2) of Article 180.

Conversely, if the expression $\sqrt{-1}$ (mod. M) has values other than N and $-N$, there are further representations of M belonging to them. In this case, then, M can be written as a sum of two squares in several ways, *for example*, $65 = 1+64 = 16+49$, $221 = 25 + 196 = 100 + 121$.

The remaining representations, in which x, y take values that are not relatively prime, can easily be found by our general method. We only note that if a number has factors of the form $4n+3$ that cannot be removed by dividing by any square (which happens if one or more such factors has an *odd exponent*), it cannot be written as a sum of two squares in any way[*)].

II. The form $xx + 2yy$ cannot represent a number for which -2 is a nonresidue with x relatively prime to y; every other number can be represented. Let -2 be a residue of the number M, and N a value of the expression $\sqrt{-2}$ (mod. M). Then, by Article 176, the forms $(1, 0, 2)$, $(M, N, \frac{NN+2}{M})$ are properly equivalent. Let the first change properly into the second on putting $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Then $x = \alpha, y = \gamma$ is a representation of the number M belonging to N. Except this one and $x = -\alpha, y = -\gamma$, no others belong to N (Article 180).

As above, we see that the representations $x = \pm\alpha, y = \mp\gamma$ belong to the value $-N$. All four representations give just one decomposition of M into a square and twice a square. If there are no values other than N and $-N$ of the expression $\sqrt{-2}$ (mod. M), there are no other decompositions. With the propositions of Article 116, this easily gives the theorem:

Every prime of the form $8n+1$ *or* $8n+3$ *can be written as a square plus twice a square, in only one way.*

$$1 = 1 + 0, \quad 3 = 1 + 2, \quad 11 = 9 + 2, \quad 17 = 9 + 8,$$
$$19 = 1 + 18, \quad 41 = 9 + 32. \quad 43 = 25 + 18, \quad 59 = 9 + 50,$$
$$67 = 49 + 18, \quad 73 = 1 + 72, \quad 83 = 81 + 2,$$
$$89 = 81 + 8, \quad 97 = 25 + 72 \quad \text{etc.}$$

Fermat also knew this theorem, like several similar ones, but the distinguished La Grange first gave a proof, *Suite des recherches d'Arithmétique*, Nouv. Mém. de l'Ac. de Berlin 1775, p. 323 ff. The distinguished Euler had already settled many points on this subject, *Specimen de usu observationum in mathesi pura*, Comm. nov. Petr. Vol. VI, p. 185 ff. But a complete proof of the theorem always eluded his efforts, p. 220. Compare also the paper in Vol. VIII (for the years 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, near the end.

[*)] If the number $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$, where a, b, c etc. are distinct primes of the form $4n+1$, and S is the product of all prime factors of M of the form $4n+3$ (every positive number can be put in this form by taking $\mu = 0$ when M is odd, and $S = 1$ when M has no factors of the form $4n+3$), then M can be written as a sum of two squares in *no way* if S is not a square. If S is a square, there are $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ etc. decompositions of M when at least one of the numbers α, β, γ etc. is odd, or $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ etc. $+\frac{1}{2}$ when all α, β, γ etc. are even (considering only the squares themselves). Anyone with some practice in combinatorics can derive the proof of this theorem from our general theory without much difficulty. We cannot dwell on it here, any more than on other *special cases*. Compare Article 105.

III. A similar method proves that every number of which -3 is a quadratic residue can be represented either by the form $xx+3yy$ or by $2xx+2xy+2yy$, with the value of x relatively prime to the value of y. Since -3 is a residue of all primes of the form $3n+1$ (Article 119), and the form $2xx+2xy+2yy$ clearly represents only *even* numbers, we have, as above, the theorem:

Every prime of the form $3n+1$ *can be written as a square plus three times a square, in only one way.*

$$1 = 1 + 0, \quad 7 = 4 + 3, \quad 13 = 1 + 12, \quad 19 = 16 + 3,$$
$$31 = 4 + 27, \quad 37 = 25 + 12, \quad 43 = 16 + 27, \quad 61 = 49 + 12,$$
$$67 = 64 + 3, \quad 73 = 25 + 48 \quad \text{etc.}$$

The distinguished Euler first gave a proof of this theorem in the paper just cited, *Comm. nov. Petr. Vol.* VIII, *p.* 105 ff.

We could proceed further in the same way and, *for example*, show that every prime of the form $20n+1$, $20n+3$, $20n+7$, or $20n+9$ (of which -5 is a residue) can be represented by one of the forms $xx+5yy$, $2xx+2xy+3yy$: primes of the forms $20n+1$ and $20n+9$ by the first, primes of the forms $20n+3, 20n+7$ by the second. Also, twice a prime of the forms $20n+1, 20n+9$ can be represented by the form $2xx+2xy+3yy$, and twice a prime of the forms $20n+3, 20n+7$ by the form $xx+5yy$. But anyone can derive this proposition and infinitely many other special ones for themselves from the preceding results and those to be given below. — So we turn to *forms with positive determinant.* Since their nature is quite different according as the determinant is a square or not a square, we first exclude forms with square determinant here and will consider them separately later.

Forms with positive nonsquare determinant.

183.

PROBLEM. *Given any form (a, b, a') with positive nonsquare determinant $= D$, find a properly equivalent form (A, B, C) in which B is positive and $< \sqrt{D}$, and A, if positive, or $-A$, if A is negative, lies between $\sqrt{D} + B$ and $\sqrt{D} - B$.*

Solution. We assume the given form does not yet satisfy both conditions; otherwise there would be no need to look for another form. We also note that in a form with *nonsquare* determinant, the first or last term cannot be $= 0$ (Article 171, note). Let $b' \equiv -b \pmod{a'}$, lying between the bounds $\sqrt{D}$ and $\sqrt{D} \mp a'$ (taking the upper sign when a' is positive and the lower when it is negative). That this is possible is easily proved as in Article 3. Put $\frac{b'b'-D}{a'} = a''$, which is an integer because $b'b' - D \equiv bb - D \equiv aa' \equiv 0 \pmod{a'}$. Now if $a'' < a'$, again let $b'' \equiv -b' \pmod{a''}$, lying between $\sqrt{D}$ and $\sqrt{D} \mp a''$ (according as a'' is positive or negative), and $\frac{b''b''-D}{a''} = a'''$. If again $a''' < a''$, once more let $b''' \equiv -b'' \pmod{a'''}$, lying between $\sqrt{D}$ and $\sqrt{D} \mp a'''$, and $\frac{b'''b'''-D}{a'''} = a''''$. Continue this operation until the sequence a', a'', a''', a'''' etc. reaches a term a^{m+1} no smaller than its predecessor a^m. This must eventually happen, since otherwise we would have an infinite sequence of integers that keep decreasing. Then, on putting $a^m = A$, $b^m = B$, $a^{m+1} = C$, the form (A, B, C) satisfies all the conditions.

Proof. I. In the sequence of forms (a, b, a'), (a', b', a''), (a'', b'', a''') etc., each is a neighbor of its predecessor; so the last, (A, B, C), is properly equivalent to the first, (a, b, a').

II. Since B lies between $\sqrt{D}$ and $\sqrt{D} \mp A$ (always taking the upper sign when A is positive and the lower when A is negative), putting $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$ clearly makes p, q positive. It is easy to confirm that $qq + 2pq + 2p\sqrt{D} = D + AA - BB$; so $D + AA - BB$ is a positive number, which we put $= r$. Then, since $D = BB - AC$, we get $r = AA - AC$, so $AA - AC$ is positive. But by assumption A is no greater than C, so this clearly requires AC to be negative, making the signs of A, C opposite. This gives $BB = D + AC < D$, and so $B < \sqrt{D}$.

III. Further, since $-AC = D - BB$, we have $AC < D$, and so (since A is not $> C$) $A < \sqrt{D}$. Thus $\sqrt{D} \mp A$ is positive, as is B, which lies between $\sqrt{D}$ and $\sqrt{D} \mp A$.

IV. So $\sqrt{D} + B \mp A$ is certainly positive. Since $\sqrt{D} - B \mp A = -q$ is negative, $\pm A$ lies between $\sqrt{D} + B$ and $\sqrt{D} - B$. *Q. E. D.*

Example. Let the given form be $(67, 97, 140)$, whose determinant $= 29$. Here we find the sequence of forms $(67, 97, 140)$, $(140, -97, 67)$, $(67, -37, 20)$, $(20, -3, -1)$, $(-1, 5, 4)$. The last is the one we want.

We will call forms (A, B, C) with positive nonsquare determinant D, in which A, taken positively, lies between $\sqrt{D} + B$ and $\sqrt{D} - B$, while B is positive and $< \sqrt{D}$, *reduced forms*. Reduced forms with positive nonsquare determinant thus differ somewhat from reduced forms with negative determinant. But because of the close analogy between them, we did not want to introduce different names.

184.

If we could recognize the equivalence of two *reduced* forms with positive determinant as easily as for forms with negative determinant (Article 172), we could decide without difficulty whether two *arbitrary* forms with the same positive determinant are equivalent. But the situation here is quite different: many reduced forms can be equivalent to one another. Before taking up this problem, we must look more deeply into the nature of reduced forms (with positive nonsquare determinant, which is always understood here).

1) If (a, b, c) is a reduced form, a and c have opposite signs. For putting the determinant of the form $= D$, we have $ac = bb - D$, which is negative because $b < \sqrt{D}$.

2) The number c, like a, taken positively, lies between $\sqrt{D} + b$ and $\sqrt{D} - b$. For $-c = \frac{D-bb}{a}$, so, disregarding the sign, c lies between $\frac{D-bb}{\sqrt{D}+b}$ and $\frac{D-bb}{\sqrt{D}-b}$, *that is*, between $\sqrt{D} - b$ and $\sqrt{D} + b$.

3) So (c, b, a) is also a reduced form.

4) Both a and c are $< 2\sqrt{D}$. Each is $< \sqrt{D} + b$, so also $< 2\sqrt{D}$.

5) The number b lies between $\sqrt{D}$ and $\sqrt{D} \mp a$ (taking the upper sign when a is positive and the lower when it is negative). Since $\pm a$ lies between $\sqrt{D} + b$ and $\sqrt{D} - b$, $\pm a - (\sqrt{D} - b)$, or $b - (\sqrt{D} \mp a)$, is positive. But $b - \sqrt{D}$ is negative, so b lies between $\sqrt{D}$ and $\sqrt{D} \mp a$. — Exactly the same argument shows that b lies between $\sqrt{D}$ and $\sqrt{D} \mp c$ (according as c is positive or negative).

6) *Every reduced form* (a, b, c) *has exactly one reduced neighbor on each side.*

Put $a' = c$, $b' \equiv -b$ (mod. a'), lying between $\sqrt{D}$ and $\sqrt{D} \mp a'$[*)], and $c' = \frac{b'b'-D}{a'}$. Then the form (a', b', c') is a right neighbor of the form (a, b, c). It is also clear that any reduced right neighbor of the form (a, b, c) must be this (a', b', c'). That it really is reduced is proved as follows.

A) On putting

$$\sqrt{D} + b \mp a' = p, \quad \pm a' - (\sqrt{D} - b) = q, \quad \sqrt{D} - b = r$$

these p, q, r are positive, by (2) above and the definition of a reduced form. Further, put

$$b' - (\sqrt{D} \mp a) = q', \quad \sqrt{D} - b' = r'$$

Then q', r' are positive, since b' lies between $\sqrt{D}$ and $\sqrt{D} \mp a'$. Finally, let $b + b' = \pm ma$; then m is an integer. Clearly $p + q' = b + b'$, so $b + b'$, or $\pm ma'$, is positive, and therefore so is m. Thus $m - 1$ is certainly nonnegative. Further, we get

$$r + q' \pm ma' = 2b' \pm a', \quad \text{or} \quad 2b' = r + q' \pm (m - 1)a'$$

so $2b'$ and b' must be positive. Since $b' + r' = \sqrt{D}$, we have $b' < \sqrt{D}$.

[*)] Where there are alternative signs, the upper sign always applies when a' is positive and the lower when a' is negative.

B) Further, we get

$$r \pm ma' = \sqrt{D} + b', \quad \text{or} \quad r \pm (m-1)a' = \sqrt{D} + b' \mp a'$$

so $\sqrt{D} + b' \mp a'$ is positive. From this, and since $\pm a' - (\sqrt{D} - b') = q'$, and so is positive, $\pm a'$ lies between $\sqrt{D} + b'$ and $\sqrt{D} - b'$. — Thus (a', b', c') is a reduced form.

The same argument proves that if we put $'c = a$, $'b \equiv -b \pmod{'c}$, lying between $\sqrt{D}$ and $\sqrt{D} \pm 'c$, and $'a = \frac{'b'b - D}{'c}$, the form $('a, 'b, 'c)$ is reduced. Clearly this form is a left neighbor of the form (a, b, c), and no reduced form other than $('a, 'b, 'c)$ can have this property.

Example. The reduced form $(5, 11, -14)$, whose determinant $= 191$, has the reduced right neighbor $(-14, 3, 13)$ and the left neighbor $(-22, 9, 5)$.

7) If the reduced form (a, b, c) has the reduced right neighbor (a', b', c'), the reduced form (c, b, a) has the left neighbor (c', b', a'). If the reduced form (a, b, c) has the left neighbor $('a, 'b, 'c)$, the reduced form (c, b, a) has the reduced right neighbor $('c, 'b, 'a)$. The forms $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b', -c')$ are also reduced, with the second a right neighbor of the first, and the third of the second; or the first a left neighbor of the second, and the second of the third. The same holds for the three forms $(-c', b', -a')$, $(-c, b, -a)$, $(-'c, 'b, -'a)$. These facts are so clear that no further discussion is needed.

185.

The number of all reduced forms with a given determinant D is always finite, and the forms themselves can be found in two ways. Let us denote all reduced forms with determinant D in general by (a, b, c), so that we have to determine all the values of a, b, c.

First method. For a, take all numbers (both positive and negative) less than $2\sqrt{D}$ for which D is a quadratic residue. For each a, set b equal to all positive values of the expression $\sqrt{D}$ (mod. a) lying between $\sqrt{D}$ and $\sqrt{D} \mp a$; and c is to be set, for each pair of determined values of a, b, $= \frac{bb-D}{a}$. Any forms obtained this way in which $\pm a$ lies outside the interval between $\sqrt{D} + b$ and $\sqrt{D} - b$ must be discarded.

Second method. For b, take all positive numbers less than $\sqrt{D}$. For each b, factor $bb - D$ in every possible way into two factors which, disregarding their signs, lie between $\sqrt{D} + b$ and $\sqrt{D} - b$, and set one $= a$ and the other $= c$. Each factorization clearly gives two forms, since each factor must be set both $= a$ and $= c$.

Example. Let $D = 79$; then there are twenty-two values of a: ∓ 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15. These give nineteen forms:

$$\begin{gathered}(1, 8, -15), \quad (2, 7, -15), \quad (3, 8, -5), \quad (3, 7, -10), \\ (5, 8, -3), \quad (5, 7, -6), \quad (6, 7, -5), \quad (6, 5, -9), \\ (7, 4, -9), \quad (7, 3, -10), \quad (9, 5, -6), \quad (9, 4, -7), \\ (10, 7, -3), \quad (10, 3, -7), \quad (13, 1, -6), \quad (14, 3, -5), \\ (15, 8, -1), \quad (15, 7, -2), \quad (15, 2, -5)\end{gathered}$$

and just as many others obtained from them by changing the signs of the outer terms, namely $(-1, 8, 15)$, $(-2, 7, 15)$, etc., making thirty-eight in all. But six of these, $(\pm 13, 1, \mp 6)$, $(\pm 14, 3, \mp 5)$, $(\pm 15, 2, \mp 5)$, must be discarded; the remaining thirty-two include all the reduced forms. The second method gives the same forms in the following order[*)]:

$$\begin{gathered}(\pm 7, 3, \mp 10), \quad (\pm 10, 3, \mp 7), \quad \pm 7, 4, \mp 9), \quad (\pm 9, 4, \mp 7), \\ (\pm 6, 5, \mp 9), \quad (\pm 9, 5, \mp 6), \quad (\pm 2, 7, \mp 15), \quad (\pm 3, 7, \mp 10), \\ (\pm 5, 7, \mp 6), \quad (\pm 6, 7, \mp 5), \quad (\pm 10, 7, \mp 3), \quad (\pm 15, 7, \mp 2), \\ (\pm 1, 8, \mp 15), \quad (\pm 3, 8, \mp 5), \quad (\pm 5, 8, \mp 3), \quad (\pm 15, 8, \mp 1).\end{gathered}$$

[*)] For $b = 1$, -78 cannot be factored into two factors which, disregarding their signs, lie between $\sqrt{79} + 1$ and $\sqrt{79} - 1$. So this value must be skipped, and for the same reason so must the values 2 and 6.

186.

Let F be a reduced form with determinant D, and let F' be its reduced right neighbor; let F'' in turn be the reduced right neighbor of this form, F''' the reduced right neighbor of F'', and so on. All the forms F', F'', F''' etc. are then completely determined, and are properly equivalent both to one another and to F. But since the number of all reduced forms with a given determinant is finite, the forms in the infinite sequence F, F', F'' etc. cannot all be different. Suppose F^m and F^{m+n} are identical. Then F^{m-1}, F^{m+n-1} are reduced left neighbors of the same reduced form, and so are identical; in the same way F^{m-2} and F^{m+n-2} etc., and finally F and F^n, are identical. So if the sequence F, F', F'' etc. is continued far enough, the first form F must eventually recur. If we suppose that F^n is the first form identical to F, or that all $F', F'' \ldots . F^{n-1}$ are different from F, we easily see that all the forms $F, F', F'' \ldots . F^{n-1}$ are different. We will call this collection of forms the *period of the form* F. If the sequence is continued beyond the last form of the period, the same forms F, F', F'' etc. appear again, and the whole infinite sequence F, F', F'' etc. consists of this period of F repeated infinitely often.

The sequence F, F', F'' etc. can also be continued backwards by placing before F the reduced form $'F$, its left neighbor; before this, the reduced form $''F$, its left neighbor, and so on. This gives a sequence of forms infinite *in both directions*:

$$\ldots .{}'''F,\ {}''F,\ {}'F,\ F,\ F',\ F'',\ F''' \ldots .$$

We easily see that $'F$ is identical to F^{n-1}, $''F$ to F^{n-2}, etc., so the sequence on the left also consists of the period of F repeated infinitely often.

If we assign to the forms F, F', F'' etc., $'F$, $''F$ etc. the indices 0, 1, 2 etc., -1, -2 etc., and in general to F^m the index m and to ${}^mF$ the index $-m$, then clearly *any two forms of the sequence are identical or different according as their indices are congruent or incongruent modulo* n.

Example. The period of the form $(3, 8, -5)$, with determinant $= 79$, is found to be $3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$. After the last, $(3, 8, -5)$ appears again. So here $n = 6$.

187.

Here are some general observations about these periods.

1) If the forms F, F', F'' etc.; $'F, ''F, '''F$ etc. are written as

$$\begin{array}{c} a, b, -a'), \quad (-a', b', a''), \quad (a'', b'', -a''') \text{ etc.;} \\ (-'a, 'b, a), \quad (''a, ''b, -'a), \quad (-'''a, '''b, ''a) \end{array}$$

then all a, a', a'', a''' etc., $'a, ''a, '''a$ etc. have *the same sign* (Article 184, 1), while all b, b', b'' etc., $'b, ''b$ etc. are positive.

2) This shows that the number n (the number of forms making up the period of F) is always *even*. For the first term of any form F^m in this period clearly has the same sign as the first term a of F if m is even, and the opposite sign if m is odd. Since F^n and F are identical, n must be even.

3) By Article 184, 6, the algorithm for finding the numbers b', b'', b''' etc., a'', a''' etc. is as follows:

$$\begin{array}{llll} b' \equiv -b \text{ (mod. } a') & \text{between } \sqrt{D} \text{ and } \sqrt{D} \mp a'; & a'' = \dfrac{D - b'b'}{a'} \\ b'' \equiv -b' \text{ (mod. } a'') & \ldots\ldots\ldots \quad \sqrt{D} \mp a''; & a''' = \dfrac{D - b''b''}{a''} \\ b''' \equiv -b'' \text{ (mod. } a''') & \ldots\ldots\ldots \quad \sqrt{D} \mp a'''; & a'''' = \dfrac{D - b'''b'''}{a'''} \end{array}$$

etc.

In the second column we take the upper or lower signs according as a, a', a'' etc. are positive or negative. Instead of the formulas in the third column, we may also use the following, which are more convenient when D is large:

$$\begin{aligned} a'' &= \frac{b + b'}{a'}(b - b') + a \\ a''' &= \frac{b' + b''}{a''}(b' - b'') + a' \\ a'''' &= \frac{b'' + b'''}{a'''}(b'' - b''') + a'' \end{aligned}$$

etc.

4) Any form F^m contained in the period of F has essentially the same period as F. Its period is $F^m, F^{m+1} \ldots . F^{n-1}, F, F' \ldots . F^{m-1}$, containing the same forms in the same order as the period of F, and differing from it only in where it begins and ends.

5) So all reduced forms with the same determinant D can be *distributed* into periods. Take any one of these forms, F, and find its period $F, F', F'' \ldots . F^{n-1}$, which we will denote by P. If this does not yet include all reduced forms with determinant D, let G be one not contained in it, and Q its period. Then P and Q clearly cannot have a form in common; otherwise G would also have to be contained in P, and the periods would coincide entirely. If P and Q do not yet exhaust all reduced forms, one of the missing forms, H, supplies a third period R, having no form in common with either P or Q. We can continue this way until all the reduced forms are exhausted. For *example*, all reduced forms with determinant 79 are distributed into six periods:

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) Let us call forms made up of the same terms in reverse order, such as $(a, b, -a')$, $(-a', b, a)$, *associated forms*. By Article 184, 7 we easily see that if the period of the reduced form F is $F, F', F'' \ldots . F^{n-1}$, if F has the associated form f, and if the forms $F^{n-1}, F^{n-2} \ldots . F'', F'$ have the respective associated forms $f', f'' \ldots . f^{n-2}, f^{n-1}$, then the period of f is $f, f', f'' \ldots . f^{n-2}, f^{n-1}$. So it consists of just as many forms as the period of F. We will call the periods of associated forms *associated periods*. In our example, periods III and VI are associated, as are IV and V.

7) But the form f may itself occur in the period of its associated form F, as in periods I and II of our example. Then the period of F agrees with that of f, or *the period of F is associated with itself*. Whenever this happens, two ambiguous forms occur in this period. Suppose the period of F consists of $2n$ forms, or that F and F^{2n} are identical; and let $2m+1$ be the index of f in the period of F[*)], so that F^{2m+1} and F are associated. Then F' and F^{2m} are also associated, as are F'' and F^{2m-1} etc., and so also F^m and F^{m+1}. Let $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Then $b^m + b^{m+1} \equiv 0 \pmod{a^{m+1}}$; but by the definition of associated forms, $b^m = b^{m+1}$, and so $2b^{m+1} \equiv 0 \pmod{a^{m+1}}$, or the form F^{m+1} is ambiguous. — In the same way F^{2m+1} and F^{2n} are associated; so are F^{2m+2} and F^{2n-1}, F^{2m+3} and F^{2n-2} etc., and finally F^{m+n} and F^{m+n+1}. The latter is ambiguous, as a similar argument easily proves. But $m+1$ and $m+n+1$ are incongruent modulo $2n$, so the forms F^{m+1} and F^{m+n+1} are not identical (Article 186, where n denotes what $2n$ denotes here). Thus in I the ambiguous forms are $(1, 8, -15)$, $(2, 7, -15)$, and in II they are $(-1, 8, 15)$, $(-2, 7, 15)$.

8) Conversely, *every period containing an ambiguous form is associated with itself.* For if F^m is a reduced ambiguous form, we easily see that its associated form (which is also reduced) is also its left neighbor, *that is*, F^{m-1} and F^m are associated. But then the whole period is associated with itself. — This shows that *a period cannot contain exactly one ambiguous form.*

9) But *it cannot contain more than two either.* Suppose the period of F, consisting of $2n$ forms, contains three ambiguous forms F^λ, F^μ, F^ν, with respective indices λ, μ, ν, so that λ, μ, ν are distinct numbers lying between 0 and $2n-1$ inclusive. Then the forms $F^{\lambda-1}$ and F^λ are associated; so are $F^{\lambda-2}$ and $F^{\lambda+1}$ etc., and finally F and $F^{2\lambda-1}$. For the same reason F and $F^{2\mu-1}$ are associated, as are F and $F^{2\nu-1}$. So $F^{2\lambda-1}$, $F^{2\mu-1}$, $F^{2\nu-1}$ are identical, and the indices $2\lambda-1$, $2\mu-1$, $2\nu-1$ are congruent modulo $2n$, and consequently $\lambda \equiv \mu \equiv \nu \pmod{n}$. *This is absurd*, since between 0 and $2n-1$ there clearly cannot lie three distinct numbers congruent modulo n.

[*)] This index must be odd, since the first terms of the forms F, f clearly have opposite signs (*see above*, 2).

188.

Since all forms in the same period are properly equivalent, the question arises whether forms in different periods can also be properly equivalent. But before showing that *this is impossible*, we must discuss some points about transformations of reduced forms.

Since we will often be dealing with transformations of forms in what follows, from now on we will always use the following abbreviated notation to keep the writing as short as possible. If a form $LXX+2MXY+NYY$ is transformed by the substitution $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$ into the form $lxx + 2mxy + nyy$, we will simply say that (L, M, N) is transformed into (l, m, n) by the substitution $\alpha, \beta, \gamma, \delta$. This way we will not need separate symbols for the indeterminates of each form under consideration. — But clearly the *first* indeterminate must be carefully distinguished from the *second* in every form.

Let the reduced form $(a, b, -a') \dots f$ with determinant D be given. As in Article 186, form the sequence of reduced forms infinite in both directions, $\dots .{}''f, {}'f, f, f', f'' \dots$, and let

$$f' = (-a', b', a''), \quad f'' = (a'', b'', -a''') \quad \text{etc.}$$
$${}'f = (-{}'a, {}'b, a), \quad {}''f = ({}''a, {}''b, -{}'a) \quad \text{etc.}$$

Set

$$\frac{b+b'}{-a'} = h', \quad \frac{b'+b''}{a''} = h'', \quad \frac{b''+b'''}{-a'''} = h''' \quad \text{etc.}$$
$$\frac{{}'b+b}{a} = h, \quad \frac{{}''b+{}'b}{-{}'a} = {}'h, \quad \frac{{}'''b+{}''b}{{}''a} = {}''h \quad \text{etc.}$$

Then clearly, if (as in Article 177) the numbers $\alpha', \alpha'', \alpha'''$ etc., $\beta', \beta'', \beta'''$ etc., and so on are formed by the following algorithm

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta & \delta'' = h''\delta' - 1 \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' \end{array}$$
etc.

f will be transformed

$$\begin{array}{llll} \text{into} & f' & \text{by the substitution} & \alpha',\ \beta',\ \gamma',\ \delta' \\ & f'' & \dots\dots\dots & \alpha'',\ \beta'',\ \gamma'',\ \delta'' \\ & f''' & \dots\dots\dots & \alpha''',\ \beta''',\ \gamma''',\ \delta''' \end{array}$$

etc.

and all these transformations will be proper.

Since $'f$ goes into f by the proper substitution $0, -1, 1, h$ (Article 158), f goes into $'f$ by the proper substitution $h, 1, -1, 0$. For a similar reason $'f$ goes into $''f$ by the proper substitution $'h, 1, -1, 0$; $''f$ into $'''f$ by the proper substitution $''h, 1, -1, 0$, and so on. From Article 159, in the same way as in Article 177, we conclude that if the numbers $'\alpha, ''\alpha, '''\alpha$ etc., $'\beta, ''\beta, '''\beta$ etc., and so on are formed by the following algorithm

$$\begin{array}{llll} '\alpha = h & '\beta = 1 & '\gamma = -1 & '\delta = 0 \\ ''\alpha = 'h'\alpha - 1 & ''\beta = '\alpha & ''\gamma = 'h'\gamma & ''\delta = '\gamma \\ '''\alpha = ''h''\alpha - '\alpha & '''\beta = ''\alpha & '''\gamma = ''h''\gamma - '\gamma & '''\delta = ''\gamma \\ ''''\alpha = '''h'''\alpha - ''\alpha & ''''\beta = '''\alpha & ''''\gamma = '''h'''\gamma - ''\gamma & ''''\delta = '''\gamma \end{array}$$

etc.

f will be transformed

$$\begin{array}{llll} \text{into} & 'f & \text{by the substitution} & '\alpha,\ '\beta,\ '\gamma,\ '\delta \\ & ''f & \ldots\ldots\ldots & ''\alpha,\ ''\beta,\ ''\gamma,\ ''\delta \\ & '''f & \ldots\ldots\ldots & '''\alpha,\ '''\beta,\ '''\gamma,\ '''\delta \end{array}$$

etc.

and all these transformations will be proper.

If we set $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$, these numbers will have the same relation to the form f as $\alpha', \beta', \gamma', \delta'$ have to f', $\alpha'', \beta'', \gamma'', \delta''$ to f'' etc., $'\alpha, '\beta, '\gamma, '\delta$ to $'f$ etc. Namely, the substitution $\alpha, \beta, \gamma, \delta$ takes the form f into f. The infinite sequences $\alpha', \alpha'', \alpha'''$ etc., $'\alpha, ''\alpha, '''\alpha$ etc. join together by inserting the term α so that they can be regarded as one continuous sequence, infinite in both directions and following the same law throughout: $\ldots '''\alpha, ''\alpha, '\alpha, \alpha, \alpha', \alpha'', \alpha''' \ldots$. The law of this sequence is

$$'''\alpha + '\alpha = ''h''\alpha, \quad ''\alpha + \alpha = 'h'\alpha, \quad '\alpha + \alpha' = h\alpha,$$
$$\alpha + \alpha'' = h'\alpha', \quad \alpha' + \alpha''' = h''\alpha'' \text{ etc.}$$

or, in general (if we take a negative index written on the right to mean the same as a positive one on the left),

$$\alpha^{m-1} + \alpha^{m+1} = h^m \alpha^m$$

Similarly the sequence $\ldots ''\beta, '\beta, \beta, \beta', \beta'' \ldots$ is continuous, with the law

$$\beta^{m-1} + \beta^{m+1} = h^{m+1} \beta^m$$

and is essentially identical to the preceding sequence, with all its terms moved one place: $''\beta = '\alpha$, $'\beta = \alpha$, $\beta = \alpha'$ etc. The law of the continuous sequence $\ldots . ''\gamma, '\gamma, \gamma, \gamma', \gamma'' \ldots .$ is

$$\gamma^{m-1} + \gamma^{m+1} = h^m \gamma^m$$

and the law of $\ldots ''\delta, '\delta, \delta, \delta', \delta'' \ldots$ is

$$\delta^{m-1} + \delta^{m+1} = h^{m+1} \delta^m$$

and in addition, in general, $\delta^m = \gamma^{m+1}$.

Example. Let the given form f be $(3, 8, -5)$. It will be transformed

into the form		by the 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''''''''	$(-5, 7, 6)$	$-45,\ +143,\ -152,\ +483$

etc.

189.

The following points about this algorithm should be noted.

1) All a, a', a'' etc., $'a, ''a$ etc. have the same sign; all b, b', b'' etc., $'b, ''b$ etc. are positive. In the sequence $\ldots ''h, 'h, h, h', h'' \ldots$ the signs alternate: if all a, a' etc. are positive, h^m or ${}^m h$ is positive when m is even and negative when m is odd; but if a, a' etc. are negative, h^m or ${}^m h$ is negative for even m and positive for odd.

2) If a is positive, and so h' negative, h'' positive, etc., then $\alpha'' = -1$ is negative, $\alpha''' = h''\alpha''$ negative and $> \alpha''$ (or $= \alpha''$ if $h'' = 1$); $\alpha'''' = h'''\alpha''' - \alpha''$ positive and $> \alpha'''$ (since $h'''\alpha'''$ is positive and α'' negative); $\alpha''''' = h''''\alpha'''' - \alpha'''$ positive and $> \alpha''''$ (since $h''''\alpha''''$ is positive), and so on. We easily conclude that the sequence $\alpha', \alpha'', \alpha'''$ etc. grows without bound, and that two positive signs are always followed by two negative ones, so that α^m has the sign $+, +, -, -$ according as $m \equiv 0, 1, 2, 3 \pmod 4$. If a is negative, a similar argument gives α'' negative, α''' positive and either $>$ or $= \alpha''$; α'''' positive and $> \alpha'''$; α''''' negative and $> \alpha''''$, and so on, so that the sequence $\alpha', \alpha'', \alpha'''$ etc. keeps growing, and the term α^m has the sign $+, -, -, +$ according as $m \equiv 0, 1, 2, 3 \pmod 4$.

3) In this way we find that all four infinite sequences $\alpha', \alpha'', \alpha'''$ etc., $\gamma, \gamma', \gamma''$ etc.; $\alpha', \alpha, {}'\alpha, {}''\alpha$ etc.; $\gamma, {}'\gamma, {}''\gamma$ etc. keep growing, and so do the following sequences identical to them: β, β', β'' etc.; ${}'\delta, \delta, \delta', \delta''$ etc.; $\beta, {}'\beta, {}''\beta$ etc.; ${}'\delta, {}''\delta$ etc. According as $m \equiv 0, 1, 2, 3 \pmod 4$, the signs are

$$\begin{array}{llll} \text{of } \alpha^m, & + \pm - \mp; & \text{of } \beta^m, & \pm - \mp + \\ \text{of } \gamma^m, & \pm + \mp -; & \text{of } \delta^m, & + \mp - \pm \\ \text{of } {}^m\alpha, & + \pm - \mp; & \text{of } {}^m\beta, & \mp + \pm - \\ \text{of } {}^m\gamma, & \mp - \pm +; & \text{of } {}^m\delta, & + \mp - \pm \end{array}$$

with the upper signs applying when a is positive and the lower when a is negative. Keep the following property especially in mind: if m denotes any positive index, α^m and γ^m have the same sign when a is positive. Opposite signs when a is negative, and similarly for β^m and δ^m; conversely, ${}^m\alpha$ and ${}^m\gamma$, or ${}^m\beta$ and ${}^m\delta$, have the same sign when a is negative and opposite signs when a is positive.

4) In the notation of Article 27, the magnitude of α^m etc. can be expressed conveniently as follows. Set

$$\begin{array}{cccc} \mp h' = k', & \pm h'' = k'', & \mp h''' = k''' \text{ etc.} \\ \pm h = k, & \mp' h = {}'k, & \pm'' h = {}''k \text{ etc.} \end{array}$$

so that all k', k'' etc., $k, {}'k$ etc. are positive numbers:

$$\begin{array}{ll} \alpha^m = \pm[k'', k''', k'''' \ldots . k^{m-1}]; & \beta^m = \pm[k'', k''', k'''' \ldots k^m] \\ \gamma^m = \pm[k', k'', k''' \ldots . k^{m-1}]; & \delta^m = \pm[k', k'', k''' \ldots . k^m] \\ {}^m\alpha = \pm[k, {}'k, {}''k \ldots . {}^{m-1}k]; & {}^m\beta = \pm[k, {}'k, {}''k \ldots . {}^{m-2}k] \\ {}^m\gamma = \pm[{}'k, {}''k \ldots . {}^{m-1}k]; & {}^m\delta = \pm[{}'k, {}''k \ldots . {}^{m-2}k] \end{array}$$

The *signs*, however, must be determined by the rules just given. With these formulas, whose proof we omit because it is easy, the calculation can always be carried out very quickly.

190.

Lemma. *Let m, μ, m', n, ν, n' denote any integers, but with none of the last three $= 0$. I say that if $\frac{\mu}{\nu}$ lies strictly between $\frac{m}{n}$ and $\frac{m'}{n'}$, and $mn' - nm' = \mp 1$, the denominator ν is greater than n and n'.*

Proof. Clearly $\mu nn'$ lies between $\nu mn'$ and $\nu nm'$, and so differs from either bound by less than the bounds differ from each other; *that is*, $\nu mn' - \nu nm' > \mu nn' - \nu mn'$ and $> \mu nn' - \nu nm'$, or $\nu > n'(\mu n - \nu m)$ and $> n(\mu n' - \nu m')$. Since $\mu n - \nu m$ is certainly not $= 0$ (otherwise $\frac{\mu}{\nu} = \frac{m}{n}$, contrary to the hypothesis), nor is $\mu n' - \nu m' = 0$ (for a similar reason), but each is at least $= 1$, it follows that $\nu > n'$ and $> n$. *Q. E. D.*

So ν clearly cannot be $= 1$; *that is*, if $mn' - nm' = \pm 1$, no integer can lie between the fractions $\frac{m}{n}$, $\frac{m'}{n'}$. In particular, zero cannot lie between them, *that is*, these fractions cannot have opposite signs.

191.

THEOREM. *If a reduced form $(a, b, -a')$ with determinant D goes by the substitution $\alpha, \beta, \gamma, \delta$ into the reduced form $(A, B, -A')$ with the same determinant, then,* first, $\frac{\pm\sqrt{D}-b}{a}$ *lies between* $\frac{\alpha}{\gamma}$ *and* $\frac{\beta}{\delta}$ *(provided neither* γ *nor* $\delta = 0$*, that is, both bounds are finite), taking the upper sign when neither bound has the sign opposite to that of* a *(or, more clearly, when either both have the coefficient's sign, or one has that sign and the other is* $= 0$*), and the lower sign when neither has the same sign as* a*;* second, $\frac{\pm\sqrt{D}+b}{a'}$ *lies between* $\frac{\gamma}{\alpha}$ *and* $\frac{\delta}{\beta}$ *(provided neither* α *nor* $\beta = 0$*), taking the upper sign when neither bound has the sign opposite to that of* a' *(or* a*), and the lower sign when neither has the same sign as* a'[*)]*.*

Proof. We have the equations

$$\begin{aligned} a\alpha\alpha + 2b\alpha\gamma - a'\gamma\gamma &= A \qquad \ldots\ldots\ldots \quad [1] \\ a\beta\beta + 2b\beta\delta - a'\delta\delta &= -A' \qquad \ldots\ldots\ldots \quad [2] \end{aligned}$$

From these we obtain

$$\begin{aligned} \frac{\alpha}{\gamma} &= \frac{\pm\sqrt{\left(D + \frac{aA}{\gamma\gamma}\right)} - b}{a} \qquad \ldots\ldots\ldots \quad [3] \\ \frac{\beta}{\delta} &= \frac{\pm\sqrt{\left(D - \frac{aA'}{\delta\delta}\right)} - b}{a} \qquad \ldots\ldots\ldots \quad [4] \end{aligned}$$

$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{\left(D - \frac{a'A}{\alpha\alpha}\right)} + b}{a'} \qquad \ldots\ldots\ldots \quad [5]$$

$$\frac{\delta}{\beta} = \frac{\pm\sqrt{\left(D + \frac{a'A'}{\beta\beta}\right)} + b}{a'} \qquad \ldots\ldots\ldots \quad [6]$$

Equation 3, 4. 5, 6 must be discarded if $\gamma, \delta, \alpha, \beta$ respectively $= 0$. — But it remains uncertain which *signs* to give the radical quantities. We decide this as follows.

In [3] and [4] the upper signs must clearly be taken when neither $\frac{\alpha}{\gamma}$ nor $\frac{\beta}{\delta}$ has the sign opposite to that of a, since taking the lower sign would make $\frac{a\alpha}{\gamma}$ and $\frac{a\beta}{\delta}$ negative quantities. But A and A' have the same sign, so $\sqrt{D}$ falls between $\sqrt{\left(D + \frac{aA}{\gamma\gamma}\right)}$ and $\sqrt{\left(D - \frac{aA'}{\delta\delta}\right)}$, and therefore in this case $\frac{\sqrt{D}-b}{a}$ lies between $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$. So the first part of the theorem is proved for the first case.

In the same way we see that in [5] and [6] the lower signs must be taken when neither $\frac{\gamma}{\alpha}$ nor $\frac{\delta}{\beta}$ has the same sign as a' or a, since taking the upper sign would necessarily make $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\beta}$ positive quantities. It follows at once that in this case $\frac{-\sqrt{D}+b}{a'}$ lies between $\frac{\gamma}{\alpha}$ and $\frac{\delta}{\beta}$. So the second part of the theorem is also proved for the second case. If it could be shown just as easily that in [3] and [4] the lower signs must be taken when neither of the quantities $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ has the same sign as a, and in [5] and [6] the upper signs when neither $\frac{\gamma}{\alpha}$ nor $\frac{\delta}{\beta}$ has the opposite sign, it would follow in

[*)] Other cases clearly cannot occur, since by the preceding article, because $\alpha\delta - \beta\gamma = \pm 1$, the two bounds can neither have opposite signs nor both be $= 0$.

the same way that in the former case $\frac{-\sqrt{D}-b}{a}$ lies between $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$, and in the latter $\frac{\sqrt{D}+b}{a'}$ between $\frac{\gamma}{\alpha}$ and $\frac{\delta}{\beta}$. The first part of the theorem would then also be proved for the second case, and the second part for the first. But although this is not difficult, it cannot be done without some detours. We prefer the following method.

When none of the numbers $\alpha, \beta.\gamma, \delta = 0$, $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$ have the same signs as $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$. So when neither of these quantities has the same sign as a' or a, and therefore $\frac{-\sqrt{D}+b}{a'}$ falls between $\frac{\gamma}{\alpha}$ and $\frac{\delta}{\beta}$, neither of the quantities $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ has the same sign as a, and $\frac{a'}{-\sqrt{D}+b} = \frac{-\sqrt{D}-b}{a}$ (because $aa' = D - bb$) falls between $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$. Thus, provided neither α nor $\beta = 0$, the first part of the theorem is also proved for the second case (for the condition that neither γ nor $\delta = 0$ is already included in the theorem itself). Similarly, when none of the numbers $\alpha, \beta, \gamma, \delta = 0$, and neither $\frac{\alpha}{\gamma}$ nor $\frac{\beta}{\delta}$ has the sign opposite to that of a or a', so that $\frac{\sqrt{D}-b}{a'}$ lies between $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$, then $\frac{\gamma}{\alpha}$ and $\frac{\delta}{\beta}$ also do not have the sign opposite to that of a', and $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ falls between $\frac{\gamma}{\alpha}$ and $\frac{\delta}{\beta}$. Thus, provided neither γ nor $\delta = 0$, the second part of the theorem is also proved for the second case.

It would therefore remain only to prove that the first part of the theorem also holds in the second case if either of the numbers α, β is $= 0$, and the second part in the first case if either γ or $\delta = 0$. But *all these cases are impossible*. For the *first* part of the theorem, suppose that neither γ nor $\delta = 0$, that $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ do not have the same sign as a, and that 1) $\alpha = 0$. Then the equation $\alpha\delta - \beta\gamma = \pm 1$ gives $\beta = \pm 1$, $\gamma = \pm 1$. From [1] we get $A = -a'$, so A and a', and therefore also a and A', have opposite signs, giving $\sqrt{\left(D - \frac{aA'}{\delta\delta}\right)} > \sqrt{D} > b$. In [4] the lower sign must therefore be taken, since with the upper sign $\frac{\beta}{\delta}$ would clearly acquire the same sign as a. So $\frac{\beta}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$ (because $a < \sqrt{D} + b$ by the definition of a reduced form), *which is absurd*, since $\beta = \pm 1$ and δ is not $= 0$. — 2) Let $\beta = 0$. Then the equation $\alpha\delta - \beta\gamma = \pm 1$ gives $\alpha = \pm 1$, $\delta = \pm 1$. From [2] we get $-A' = -a'$, so a' and a and A have the same sign, giving $\sqrt{\left(D + \frac{aA}{\alpha\alpha}\right)} > \sqrt{D} > b$. In [3] the lower sign must therefore be taken, since with the upper sign $\frac{\alpha}{\gamma}$ would acquire the same sign as a. So $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, *which is absurd* for the same reason as before. — For the *second* part, suppose that neither α nor $\beta = 0$, that $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$ do not have the sign opposite to that of a', and that 1) $\gamma = 0$. The equation $\alpha\delta - \beta\gamma = \pm 1$ gives $\alpha = \pm 1$, $\delta = \pm 1$. From [1] we get $A = a$, so a' and A' have the same sign, giving $\sqrt{\left(D + \frac{a'A'}{\beta\beta}\right)} > \sqrt{D} > b$. In [6] the upper sign must therefore be taken, since with the lower sign $\frac{\delta}{\beta}$ would acquire the sign opposite to that of a'. Thus $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$, *which is absurd*, since $\delta = \pm 1$ and β is not $= 0$. Finally, 2) if $\delta = 0$, then $\alpha\delta - \beta\gamma = \pm 1$ gives $\beta = \pm 1$, $\gamma = \pm 1$, and therefore from [2], $-A' = a$. This gives $\sqrt{\left(D - \frac{a'A}{\alpha\alpha}\right)} > \sqrt{D} > b$, so in [5] the upper sign must be taken. Thus $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, *which is absurd*. — So the theorem is proved in its full scope.

Since the difference between $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$ is $= \frac{1}{\gamma\delta}$, the difference between $\frac{\pm\sqrt{D}-b}{a}$ and $\frac{\alpha}{\gamma}$ or $\frac{\beta}{\delta}$ is $< \frac{1}{\gamma\delta}$; and between $\frac{\pm\sqrt{D}-b}{a}$ and $\frac{\alpha}{\gamma}$, or between that quantity and $\frac{\beta}{\delta}$, no fraction can lie whose denominator is not greater than γ or δ (*the preceding lemma*). — In the same way the difference of the quantity $\frac{\pm\sqrt{D}+b}{a}$ from the fraction $\frac{\gamma}{\alpha}$ or $\frac{\delta}{\beta}$ is less than $\frac{1}{\alpha\beta}$, and between that quantity and either of these fractions no fraction can lie whose denominator is not greater than α and β.

192.

Applying the preceding theorem to the algorithm of Article 188 shows that the quantity $\frac{\sqrt{D}-b}{a}$, which we will denote by L, lies between $\frac{\alpha'}{\gamma'}$ and $\frac{\beta'}{\delta'}$, between $\frac{\alpha''}{\gamma''}$ and $\frac{\beta''}{\delta''}$, between $\frac{\alpha'''}{\gamma'''}$ and $\frac{\beta'''}{\delta'''}$, etc. (for it follows easily from the end of Article 189, 3 that none of these bounds has the sign opposite to that of a, so the radical quantity $\sqrt{D}$ must be given the positive sign), or between $\frac{\alpha'}{\gamma'}$ and $\frac{\alpha''}{\gamma''}$, between $\frac{\alpha''}{\gamma''}$ and $\frac{\alpha'''}{\gamma'''}$, etc. Thus all the fractions $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha'''''}{\gamma'''''}$ etc. lie on the same side of L, and all $\frac{\alpha''}{\gamma''}$, $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha''''''}{\gamma''''''}$ etc. on the other side. But since $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ lies *outside* the interval between $\frac{\alpha'''}{\gamma'''}$ and L, and for a similar reason $\frac{\alpha''}{\gamma''}$ outside L and $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha'''}{\gamma'''}$ outside L and $\frac{\alpha'''''}{\gamma'''''}$, etc. So these quantities clearly lie in the following order:

$$\frac{\alpha'}{\gamma'},\ \frac{\alpha'''}{\gamma'''},\ \frac{\alpha'''''}{\gamma'''''} \ldots L \ldots \frac{\alpha''''''}{\gamma''''''},\ \frac{\alpha''''}{\gamma''''},\ \frac{\alpha''}{\gamma''}$$

The difference between $\frac{\alpha'}{\gamma'}$ and L is less than the difference between $\frac{\alpha'}{\gamma'}$ and $\frac{\alpha''}{\gamma''}$, *that is*, $< \frac{1}{\gamma'\gamma''}$, and similarly the difference between $\frac{\alpha''}{\gamma''}$ and L is $< \frac{1}{\gamma''\gamma'''}$, etc. So the fractions $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ etc. keep approaching the limit L more closely, and since $\gamma', \gamma'', \gamma'''$ keep growing without bound, the difference between the fractions and the limit can be made smaller than any given quantity.

By Article 189, none of the quantities $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$ etc. has the same sign as a. An argument entirely similar to the preceding one therefore shows that these quantities and $\frac{-\sqrt{D}+b}{a'}$, which we will denote by L', lie in the following order:

$$\frac{\gamma}{\alpha},\ \frac{''\gamma}{''\alpha},\ \frac{''''\gamma}{''''\alpha} \ldots\ldots L' \ldots\ldots \frac{''''''\gamma}{''''''\alpha},\ \frac{'''\gamma}{'''\alpha},\ \frac{'\gamma}{'\alpha}$$

The difference between $\frac{\gamma}{\alpha}$ and L' is less than $\frac{1}{'\alpha\alpha}$, the difference between $\frac{'\gamma}{'\alpha}$ and L' less than $\frac{1}{''\alpha'\alpha}$, etc. So the fractions $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$ etc. keep approaching L' more closely, and the difference can be made smaller than any given quantity.

In the *example* of Article 188 we have $L = \frac{\sqrt{79}-8}{3} = 0{,}2960648$, and the approximating fractions are $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{5}{17}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$, etc. Now $\frac{143}{483} = 0{,}2960662$. — There we also have $L' = \frac{-\sqrt{79}+8}{5} = -0{,}1776388$, and the approximating fractions are $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$, $-\frac{8}{45}$, $-\frac{27}{152}$, $-\frac{143}{805}$, etc. But $\frac{143}{805} = 0{,}1776397$.

193.

THEOREM. *If the reduced forms f, F are properly equivalent, one is contained in the period of the other.*

Let $f = (a, b, -a')$, $F = (A, B, -A')$, let the determinant of these forms be D, and let the former pass into the latter by the proper substitution $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$. I then claim that if we find the period of the form f and work out the sequence, infinite in both directions, of reduced forms and transformations of f into them, as in Article 188, *either* $+\mathfrak{A}$ equals some term of the sequence $\ldots''\alpha, '\alpha, \alpha, \alpha', \alpha'' \ldots$, and, on setting this term $= \alpha^m$, $+\mathfrak{B}$ is $= \beta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$; *or* $-\mathfrak{A}$ equals some term α^m, and $-\mathfrak{B}, -\mathfrak{C}, -\mathfrak{D}$ are respectively $= \beta^m, \gamma^m, \delta^m$ (where m may also denote a negative index). In either case F is clearly identical to f^m.

Proof. I. We have the four equations

$$a\mathfrak{A}\mathfrak{A} + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}\mathfrak{C} = A \quad \ldots\ldots \qquad [1]$$

$$a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B \quad \ldots\ldots \qquad [2]$$

$$a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D} = -A' \quad \ldots\ldots \qquad [3]$$

$$\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1 \quad \ldots\ldots\ldots \qquad [4]$$

We *first* consider the case where one of the numbers $\mathfrak{A}\ \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$.

1° If $\mathfrak{A} = 0$, [4] gives $\mathfrak{B}\mathfrak{C} = -1$, so $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Then [1] gives $-a' = A$, and [2] gives $-b \pm a'\mathfrak{D} = B$, or $B \equiv -b \pmod{a' \text{ or } A}$. It follows that the form $(A, B, -A')$ is a right neighbor of the form $(a, b, -a')$. Since the former is reduced, it must be identical to f'. So $B = b'$, and [2] therefore gives $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; since $\frac{b+b'}{-a'} = h'$, we get $\mathfrak{D} = \mp h'$. We conclude that $\mp\mathfrak{A}, \mp\mathfrak{B}, \mp\mathfrak{C}, \mp\mathfrak{D}$ are respectively $= 0, -1, +1, h'$, or $= \alpha', \beta', \gamma', \delta'$.

2° If $\mathfrak{B} = 0$, [4] gives $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; [3] gives $a' = A'$; and [2] gives $b \mp a'\mathfrak{C} = B$, or $b \equiv B \pmod{a'}$. Since both f and F are reduced forms, both b and B lie between $\sqrt{D}$ and $\sqrt{D} \mp a'$ (according as a' is positive or negative, Article 185, 5). So we must have $b = B$ and $\mathfrak{C} = 0$. Thus the forms f, F are identical, and $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D} = 1, 0, 0, 1 = \alpha, \beta, \gamma\ \delta$ respectively.

3° If $\mathfrak{C} = 0$, [4] gives $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; [1] gives $a = A$; and [2] gives $\pm a\mathfrak{B} + b = B$, or $b \equiv B \pmod{a}$. But both b and B lie between $\sqrt{D}$ and $\sqrt{D} \mp a$, so we must have $B = b$ and $\mathfrak{B} = 0$. This case therefore does not differ from the preceding one.

4° If $\mathfrak{D} = 0$, [4] gives $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; [3] gives $a = -A'$; and [2] gives $\pm a\mathfrak{A} - b = B$, or $B \equiv -b \pmod{a}$. So F is a left neighbor of f, and is therefore identical to the form $'f$. Since $\frac{'b+b}{a} = h$ and $B = 'b$, we get $\pm\mathfrak{A} = h$. We conclude that $\pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{C}, \pm\mathfrak{D}$ are respectively $= h, 1, -1, 0, = '\alpha, '\beta, '\gamma, '\delta$.

It remains to consider the case where none of the numbers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$. By the lemma in Article 190, the quantities $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$, $\frac{\mathfrak{D}}{\mathfrak{B}}$ then have the same sign. This gives two cases, since this sign can either agree with the sign of a, a', or be opposite to it.

II. If $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ have the same sign as a, the quantity $\frac{\sqrt{D}-b}{a}$ (which we will denote by L) lies between these fractions (Article 191). We will now prove that $\frac{\mathfrak{A}}{\mathfrak{C}}$ equals one of the fractions $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha''''}{\gamma''''}$ etc., and $\frac{\mathfrak{B}}{\mathfrak{D}}$ equals the next one: namely, if $\frac{\mathfrak{A}}{\mathfrak{C}}$ is $= \frac{\alpha^m}{\gamma^m}$, then $\frac{\mathfrak{B}}{\mathfrak{D}}$ is $= \frac{\alpha^{m+1}}{\gamma^{m+1}}$. In the preceding article we showed that the quantities $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ etc.

(which we will denote briefly by (1), (2), (3) etc.), together with L, have the following order (I): $(1), (3), (5) \ldots L \ldots (6), (4), (2)$. The first of these quantities is $= 0$ (since $\alpha' = 0$); all the others have the same sign as L, or a. But by hypothesis $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ (for which we will write $\mathfrak{M}, \mathfrak{N}$) have the same sign. Clearly, then, these quantities lie to the right of (1) (or, if you prefer, on the same side as L); and since L lies between them, one lies to the right of L and the other to its left. It is easy to show that $\mathfrak{M}$ cannot lie to the right of (2), for otherwise $\mathfrak{N}$ would lie between (1) and L. It would follow *first* that (2) lies between $\mathfrak{M}$ and $\mathfrak{N}$, so the denominator of the fraction (2) is greater than that of $\mathfrak{N}$ (Article 190); and *second* that $\mathfrak{N}$ lies between (1) and (2), so the denominator of $\mathfrak{N}$ is greater than that of (2). *This is a contradiction.*

Let us suppose that $\mathfrak{M}$ equals none of the fractions (2), (3), (4) etc., and see what follows. If the fraction $\mathfrak{M}$ lies to the left of L, it must clearly lie either between (1) and (3), or between (3) and (5), or between (5) and (7), and so on (since L is irrational, and is therefore certainly unequal to $\mathfrak{M}$, while the fractions (1), (3), (5) etc. can come closer to L than any given quantity unequal to L). If, however, $\mathfrak{M}$ lies to the right of L, it must lie either between (2) and (4), or between (4) and (6), or between (6) and (8), and so on. So let $\mathfrak{M}$ lie between (m) and $(m+2)$. The quantities $\mathfrak{M}, (m), (m+1), (m+2), L$ clearly lie in the following order:

$$(\text{II})^{*)}: \qquad (m),\ (\mathfrak{M}),\ (m+2),\ L,\ (m+1)$$

We must then have $\mathfrak{N} = (m+1)$. For $\mathfrak{N}$ lies to the right of L. If it also lay to the right of $(m+1)$, then $(m+1)$ would lie between $\mathfrak{M}$ and $\mathfrak{N}$, giving $\gamma^{m+1} > \mathfrak{C}$, while $\mathfrak{M}$ would lie between (m) and $(m+1)$, giving $\mathfrak{C} > \gamma^{m+1}$ (Article 190), *a contradiction.* If, on the other hand, $\mathfrak{N}$ lay to the left of $(m+1)$, or between $(m+2)$ and $(m+1)$, we would have $\mathfrak{D} > \gamma^{m+2}$; and since $(m+2)$ lies between $\mathfrak{M}$ and $\mathfrak{N}$, we would have $\gamma^{m+2} > \mathfrak{D}$, *a contradiction.* So $\mathfrak{N} = (m+1)$, or $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}} = \frac{\beta^m}{\delta^m}$.

Since $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, $\mathfrak{B}$ is relatively prime to $\mathfrak{D}$, and for the same reason β^m is relatively prime to δ^m. We can thus easily see that the equation $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\beta^m}{\delta^m}$ can hold only if either $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$, or $\mathfrak{B} = -\beta^m$, $\mathfrak{D} = -\delta^m$. Now the form f is transformed by the proper substitution $\alpha^m, \beta^m, \gamma^m, \delta^m$ into the form f^m, which is $(\pm a^m, b^m, \mp a^{m+1})$, so we have the equations

$$a\alpha^m\alpha^m + 2b\alpha^m\gamma^m - a'\gamma^m\gamma^m = \pm a^m \quad \ldots\ldots \qquad [5]$$

$$a\alpha^m\beta^m + b(\alpha^m\delta^m + \beta^m\gamma^m) - a'\gamma^m\delta^m = b^m \quad \ldots. \qquad [6]$$

$$a\beta^m\beta^m + 2b\beta^m\delta^m - a'\delta^m\delta^m = \mp a^{m+1} \quad \ldots\ldots \qquad [7]$$

$$\alpha^m\delta^m - \beta^m\gamma^m = 1 \quad \ldots\ldots\ldots \qquad [8]$$

These give (from equations 7 and 3) $\mp a^{m+1} = -A'$. Further, multiplying equation [2] by $\alpha^m\delta^m - \beta^m\gamma^m$ and equation [6] by $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C}$, and subtracting, we readily

*)It makes no difference here whether the order in (II) is the same as that in (I) or the reverse; *i.e.*, whether (m) also lies to the left of L in (I), or to its right.

confirm by expansion that

$$\begin{aligned} B - b^m = (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)\big(a\mathfrak{B}\beta^m \\ + b(\mathfrak{D}\beta^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m\big) \\ + (\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)\big(a\mathfrak{A}\alpha^m \\ + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m\big) \quad .. \end{aligned} \tag{9}$$

or, since either $\beta^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$ or $\beta^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$,

$$\begin{aligned} B - b^m &= \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D}) \\ &= \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A' \end{aligned}$$

Thus $B \equiv b^m \pmod{A'}$. But both B and b^m lie between $\sqrt{D}$ and $\sqrt{D} \mp A'$, so we must have $B = b^m$, and therefore $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$, or $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$, *i.e.*, $\mathfrak{M} = (m)$.

In this way, from the assumption that $\mathfrak{M}$ equals none of the quantities (2), (3), (4) etc., we have deduced that it really does equal one of them. If, however, we assume from the start that $\mathfrak{M} = (m)$, we clearly have either $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$, or $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. In either case [1] and [5] give $A = \pm a^m$, and [9] gives $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)A$, or $B \equiv b^m \pmod{A}$. As above, we conclude that $B = b^m$, and hence $\mathfrak{B}\delta^m = \mathfrak{D}\beta^m$. Since $\mathfrak{B}$ is relatively prime to $\mathfrak{D}$, and β^m to δ^m, we have either $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ or $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$; so [7] gives $-A' = \mp a^{m+1}$. The forms F, f^m are therefore identical. Using the equation $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^m\delta^m - \beta^m\gamma^m$, it is easy to prove that we must take $+\mathfrak{B} = \beta^m$, $+\mathfrak{D} = \delta^m$ when $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$; but $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = -\delta^m$ when $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. *This proves the claim.*

III. If the sign of the quantities $\frac{\mathfrak{A}}{\mathfrak{C}}$ etc. is opposite to that of a, the proof is so similar to the preceding one that it is enough to indicate its main points. The quantity $\frac{-\sqrt{D}+b}{a'}$ lies between $\frac{\mathfrak{C}}{\mathfrak{A}}$ and $\frac{\mathfrak{D}}{\mathfrak{B}}$. The fraction $\frac{\mathfrak{D}}{\mathfrak{B}}$ equals one of the fractions

$$\frac{'\delta}{'\beta},\ \frac{''\delta}{''\beta},\ \frac{'''\delta}{'''\beta} \text{ etc.} \quad ..... \tag{I}$$

$$\text{when this is } = \frac{{}^m\delta}{{}^m\beta}, \qquad \frac{\mathfrak{C}}{\mathfrak{A}} \text{ is } = \frac{{}^m\gamma}{{}^m\alpha} \quad ..... \tag{II}$$

We prove (I) as follows. If we suppose that $\frac{\mathfrak{D}}{\mathfrak{B}}$ equals none of those fractions, it must lie between two of them, $\frac{{}^m\delta}{{}^m\beta}$ and $\frac{{}^{m+2}\delta}{{}^{m+2}\beta}$. From this, just as above, we deduce that we must have

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{m+1}\delta}{{}^{m+1}\beta} = \frac{{}^m\gamma}{{}^m\alpha}$$

and either $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$, or $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. But f passes by the proper substitution ${}^m\alpha, {}^m\beta, {}^m\gamma, {}^m\delta$ into the form

$${}^m f = (\pm {}^m a, {}^m b, \mp {}^{m-1} a)$$

This gives three equations. Combining them with equations 1, 2, 3, 4 and with ${}^m\alpha^m\delta - {}^m\beta^m\gamma = 1$, we deduce, as above, that the first term A of the form F equals

the first term of ${}^m f$, and that the middle term of the former is congruent to that of the latter modulo A. Since both forms are reduced, and the middle term of each therefore lies between $\sqrt{D}$ and $\sqrt{D} \mp A$, it follows that these middle terms are equal; from this we deduce $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$. So here the truth of assertion (I) has been derived from the assumption that it is false.

But if we assume $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$, then, in just the same way and by the same equations, we prove that $\frac{{}^m\gamma}{{}^m\beta} = \frac{\mathfrak{C}}{\mathfrak{A}}$ also holds, as stated in (II). Using the equations $\mathfrak{AD} - \mathfrak{BC} = 1$, ${}^m\alpha\,{}^m\delta - {}^m\beta\,{}^m\gamma = 1$, we then deduce that either

$$\mathfrak{A} = {}^m\alpha,\ \mathfrak{B} = {}^m\beta,\ \mathfrak{C} = {}^m\gamma,\ \mathfrak{D} = {}^m\delta$$

or

$$-\mathfrak{A} = {}^m\alpha,\ -\mathfrak{B} = {}^m\beta,\ -\mathfrak{C} = {}^m\gamma,\ -\mathfrak{D} = {}^m\delta$$

and that the forms F, ${}^m f$ are identical. *This proves the claim.*

194.

Since the forms we called associated above (Article 187, 6) are always improperly equivalent (Article 159), it is clear that if the reduced forms F, f are improperly equivalent, and F has the associated form G, then f, G are properly equivalent, so G is contained in the period of f. Thus if the forms F, f are both properly and improperly equivalent, both F and G must occur in the period of f. This period is therefore associated with itself and contains two ambiguous forms (Article 187, 7). This gives a fine confirmation of the theorem in Article 165, which already assured us that there is an ambiguous form equivalent to F, f.

195.

PROBLEM. *Given any two forms Φ, φ with the same determinant, decide whether or not they are equivalent.*

Solution. Find two reduced forms F, f properly equivalent to the given forms Φ, φ respectively (Article 183). According as these are equivalent only properly, only improperly, in both ways, or in neither, the given forms will likewise be equivalent only properly, only improperly, in both ways, or in neither. Work out the period of either reduced form, *e.g.*, that of f. If F occurs in this period but the form associated with F does not, we clearly have the *first* case; if this associated form occurs but F itself does not, the *second*; if both occur, the *third*; if neither, the *fourth*.

Example. Let the given forms be $(129, 92, 65)$, $(42, 59, 81)$, with determinant 79. We find the reduced forms $(10, 7, -3)$, $(5, 8, -3)$ properly equivalent to them. The period of the former is $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 7, -6)$, $(-6, 5, 9)$, $(9, 4. -7)$, $(-7, 3, 10)$. Since the form $(5, 8, -3)$ itself does not occur in this period, but its associated form $(-3, 8, 5)$ does, we conclude that the given forms are equivalent only improperly.

If all the reduced forms with a given determinant are divided into periods P, Q, R etc., as above (Article 187, 5), and we choose any one form from each period (from P F, from Q G, from R H etc.), no two of these forms F, G, H etc. can be properly equivalent. But every other form with the same determinant is properly equivalent to one of these, and to *only one*. Clearly, then, *all forms with this determinant can be divided into as many classes as there are periods*, by putting those properly equivalent to F in the first class, those properly equivalent to G in the second, and so on. In this way all forms in the same class will be properly equivalent, while forms in different classes cannot be properly equivalent. But we will not dwell on this subject here, since we will discuss it more fully below.

196.

PROBLEM. *Given two properly equivalent forms Φ, φ, find a proper transformation of one into the other.*

Solution. By the method in Article 183 we can find two sequences of forms

$$\Phi, \Phi', \Phi'' \ldots \Phi^n \quad \text{and} \quad \varphi, \varphi', \varphi'' \ldots \varphi^\nu$$

such that each form is properly equivalent to its predecessor, and the last forms Φ^n, φ^ν are reduced. Since Φ, φ are assumed properly equivalent, Φ^n must be contained in the period of φ^ν. Let $\varphi^\nu = f$, and let its period as far as Φ^n be

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

so that Φ^n has index m in this period. Denote the forms opposite to the associated forms of

$$\Phi,\ \Phi',\ \Phi'' \dots \Phi^n \quad \text{by } \Psi,\ \Psi',\ \Psi'' \dots \Psi^n \text{ respectively}^{*)}.$$

Then in the sequence

$$\varphi,\ \varphi',\ \varphi'' \dots f,\ f',\ f'' \dots f^{m-1},\ \Psi^{n-1},\ \Psi^{n-2} \dots \Psi,\ \Phi$$

each form is a right neighbor of its predecessor. So by Article 177 we can find a proper transformation of the first form φ into the last Φ. This is easy to see for the other forms in the sequence; for f^{m-1}, Ψ^{n-1}, it is proved as follows. Let

$$f^{m-1} = (g, h, i); \quad f^m \text{ or } \Phi^n = (g', h', i');$$
$$\Phi^{n-1} = (g'', h'', i'')$$

The form (g', h', i') is a right neighbor both of (g, h, i) and of (g'', h'', i''); hence $i = g' = i''$ and $-h \equiv h' \equiv -h''$ (mod. i or g' or i''). It follows that the form $(i'', -h'', g'')$, *i.e.*, Ψ^{n-1}, is a right neighbor of (g, h, i), *i.e.*, f^{m-1}.

If the forms Φ, φ are improperly equivalent, φ is properly equivalent to the form opposite to Φ. So we can find a proper transformation of φ into the form opposite to Φ. If this is given by the substitution $\alpha, \beta, \gamma, \delta$, it is easy to see that φ is improperly transformed into Φ itself by the substitution $\alpha, -\beta, \gamma, -\delta$.

This also shows that if the forms Φ, φ are both properly and improperly equivalent, we can find *two* transformations, one proper and one improper.

Example. We seek an improper transformation of the form $(129, 92, 65)$ into $(42, 59, 81)$, which we found in the preceding article to be improperly equivalent to it. We must therefore first find a proper transformation of $(129, 92, 65)$ into $(42, -59, 81)$. For this purpose we work out the sequence of forms $(129, 92, 65)$, $(65, -27, 10)$, $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 22, 81)$, $(81, 59, 42)$, $(42, -59, 81)$. From this we derive the proper transformation $-47, 56, 73, -87$, which takes $(129, 92, 65)$ into $(42, -59, 81)$; so the improper transformation $-47, -56, 73, 87$ takes it into $(42, 59, 81)$.

*)Thus Ψ is obtained from Φ by interchanging the first and last terms and giving the middle term the opposite sign; similarly for the others.

197.

If we have one transformation of a form $(a,b,c)\ldots\varphi$ into an equivalent form Φ, we can derive from it *all* similar transformations of φ into Φ, provided we can find all the solutions of the indeterminate equation $tt - Duu = mm$, where D denotes the determinant of the forms Φ, φ, and m the greatest common divisor of $a, 2b, c$ (Article 162). Having already solved this problem above for a negative value of D, we will now tackle it for a positive value. Clearly, any value of t satisfying the equation still satisfies it when its sign is reversed, and the same is true of any value of u. So it is enough to find all *positive* values of t, u, and each solution in positive values will stand for four solutions. We will do this by showing *first* how to find the *smallest* values of t, u (apart from the obvious ones $t = m,\ u = 0$), and *then* how to derive all the others from them.

198.

PROBLEM. *Find the smallest numbers t, u satisfying the indeterminate equation $tt - Duu = mm$, given a form (M, N, P) whose determinant is D and for which $M, 2N, P$ have greatest common divisor n.*

Solution. Choose any reduced form $(a, b, -a')\ldots f$ with determinant D, in which $a, 2b, a'$ have greatest common divisor m. Such a form clearly exists, since we can find a reduced form equivalent to (M, N, P), which by Article 161 has this property. But for our present purpose we can use any reduced form satisfying this condition. Work out the period of f, which we will suppose consists of n forms. Retaining all the notation used in Article 188, f^n is $(+a^n, b^n, -a^{n+1})$, since n is even; and f passes into this form by the proper substitution $\alpha^n, \beta^n, \gamma^n, \delta^n$. But f and f^n are identical, so f also passes into f^n by the proper substitution $1, 0, 0, 1$. From these two similar transformations of f into f^n, Article 162 gives a solution of $tt - Duu = mm$ *in integers*, namely $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (equation 18, Article 162), $u = \frac{\gamma^n m}{a}$ (equation 19)*). Denote these values by T, U, taking them positive if they are not already so. These T, U will be the smallest values of t, u, apart from $t = m,\ u = 0$ (from which they must differ, since γ^n clearly cannot be $= 0$).

For suppose there are still smaller values of t, u, say $\mathfrak{t}, \mathfrak{u}$, which are positive, with $\mathfrak{u}$ not $= 0$. Then by Article 162 the form f is transformed by the proper substitution $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u}),\ \frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$ into a form identical to itself. By Article 193, II, *either* $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ *or* $-\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ must equal one of the numbers $\alpha'', \alpha''', \alpha''''$ etc., say $= \alpha^\mu$ (for since $\mathfrak{tt} = D\mathfrak{uu} + mm = bb\mathfrak{uu} + aa'\mathfrak{uu} + mm$, we have $\mathfrak{tt} > bb\mathfrak{uu}$, so $\mathfrak{t} - b\mathfrak{u}$ is positive; hence the fraction $\frac{\mathfrak{t} - b\mathfrak{u}}{a\mathfrak{u}}$, corresponding to $\frac{\mathfrak{A}}{\mathfrak{C}}$ in Article 193, has the same sign as a or a'). In the first case $\frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$, and in the second the same quantities with their signs reversed, are respectively $= \beta^\mu, \gamma^\mu, \delta^\mu$. But since $\mathfrak{u} < U$, *i.e.*, $\mathfrak{u} < \frac{\gamma^n m}{a}$ and > 0, we have $\gamma^\mu < \gamma^n$ and > 0. Since the sequence $\gamma, \gamma', \gamma''$ etc. increases continually, μ must lie strictly between 0 and n. But the corresponding form f^μ is identical to f, *a contradiction*, since all the forms f, f', f'' etc. as far as

*) In Article 162 we had $\alpha, \beta, \gamma, \delta$; $\alpha', \beta', \gamma', \delta'$;
here we have $1, 0, 0, 1$; $\alpha^n, \beta^n, \gamma^n, \delta^n$;
A, B, C; a, b, c; e,
$a, b, -a'$; $a, b, -a'$; 1.

f^{n-1} are assumed distinct. We conclude that the smallest values of t, u (apart from $m, 0$) are T, U.

Example. If $D = 79,\ m = 1$, we can use the form $(3, 8, -5)$, for which $n = 6$ and $\alpha^n = -8,\ \gamma^n = -27,\ \delta^n = -152$ (Article 188). This gives $T = 80,\ U = 9$, the smallest values of t, u satisfying $tt - 79uu = 1$.

199.

For practical use we can obtain still more convenient formulas. We have $2b\gamma^n = -a(\alpha^n - \delta^n)$, which follows easily from Article 162 by multiplying equation [19] by $2b$ and [20] by a, and changing the notation used there to our present notation. This gives $\alpha^n + \delta^n = 2\delta^n - \frac{2b}{a}\gamma^n$, so

$$\pm T = m\left(\delta^n - \frac{b}{a}\gamma^n\right), \quad \pm U = \frac{\gamma^n m}{a}$$

By a similar method we obtain

$$\pm T = m\left(\alpha^n + \frac{b}{a'}\beta^n\right), \quad \pm U = \frac{\beta^n m}{a'}$$

Both sets of formulas are very convenient, since $\gamma^n = \delta^{n-1},\ \alpha^n = \beta^{n-1}$. If we use the latter, it is enough to calculate just the sequence $\beta', \beta'', \beta''' \ldots \beta^n$; if we prefer the former, just the sequence $\delta', \delta'', \delta'''$ etc. Further, Article 189, 3 easily shows that, since n is necessarily even, α^n and $\frac{b}{a'}\beta^n$ have the same sign, as do δ^n and $\frac{b}{a}\gamma^n$. So in the first formula for T we must take the absolute difference, and in the second the absolute sum; we need not consider the signs at all. Returning to the notation used in Article 189, 4, the first formula gives

$$T = m[k', k'', k'''. \ldots k^n] - \frac{mb}{a}[k', k'', k'''. \ldots k^{n-1}],$$
$$U = \frac{m}{a}[k', k'', k'''. \ldots k^{n-1}]$$

and the second

$$T = m[k'', k'''. \ldots k^{n-1}] + \frac{mb}{a'}[k'', k'''. \ldots k^n],$$
$$U = \frac{m}{a'}[k'', k'''. \ldots k^n]$$

where the value of T can also be written $m\left[k'', k'''. \ldots k^n, \frac{b}{a'}\right]$.

Example. For $D = 61,\ m = 2$ we can use the form $(2, 7, -6)$, for which we find $n = 6$, and $k', k'', k''', k'''', k''''', k'''''' = 2, 2, 7, 2, 2, 7$. This gives

$$T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2]$$
$$= 2888 - 1365 = 1523$$

from the first formula; the second gives the same result:

$$T = 2[2, 7, 2, 2] + \tfrac{7}{3}[2, 7, 2, 2.7]$$
$$U \text{ is } = [2, 2, 7, 2, 2] = \tfrac{1}{3}[2, 7, 2, 2, 7] = 195.$$

There are other ways to shorten the calculation, but to keep this account brief we cannot discuss them more fully here.

200.

To obtain *all* values of t, u from the smallest ones, we write the equation $TT - DUU = mm$ as

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right) = 1$$

which also gives

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = 1 \quad \ldots\ldots \qquad [1]$$

where e denotes any number. For brevity, we will generally denote the values of the quantities

$$\frac{m}{2}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e + \frac{m}{2}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e,$$
$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e - \frac{m}{2\sqrt{D}}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e \text{ *)}$$

by t^e, u^e respectively: *i.e.*, their values for $e = 0$ by t^0, u^0 (which are $m, 0$); for $e = 1$ by t', u' (which are T, U); for $e = 2$ by t'', u''; for $t = 3$ by t''', u''' etc. — We will prove that if e takes all nonnegative integers, *i.e.*, 0 and all positive integers from 1 to ∞, these expressions give all positive values of t, u: namely, I) all values of these expressions are indeed values of t, u; II) all these values are integers; III) there are no positive values of t, u not contained in these formulas.

I. Substituting the values of t^e, u^e, we readily confirm, using equation [1], that

$$(t^e + u^e\sqrt{D})(t^e - u^e\sqrt{D}) = mm, \quad i.e. \quad t^e t^e - Du^e u^e = mm$$

II. In the same way we easily confirm that, in general,

$$t^{e+1} + t^{e-1} = \frac{2T}{m}t^e, \quad u^{e+1} + u^{e-1} = \frac{2T}{m}u^e$$

The two sequences t^0, t', t'', t''' etc., u^0, u', u'', u''' etc. therefore satisfy recurrence relations, both with coefficients $\frac{2T}{m}, -1$, namely

$$t'' = \frac{2T}{m}t' - t^0, \quad t''' = \frac{2T}{m}t'' - t' \text{ etc.}, \quad u'' = \frac{2T}{m}u' \text{ etc.}$$

Now by hypothesis there is a form (M, N, P) with determinant D, in which $M, 2N, P$ are divisible by m. So

$$TT = (NN - MP)UU + mm$$

and $4TT$ is clearly divisible by mm. Thus $\frac{2T}{m}$ is an integer, and a positive one. But we have $t^0 = m,\ t' = T,\ u^0 = 0,\ u' = U$, all integers, so all of t'', t''' etc., u'', u''' etc. are integers too. Further, since $TT > mm$, all of t^0, t', t'', t''' etc. are clearly positive and increase continually without bound, as do all of u^0, u', u'', u''' etc.

*) Only in these four expressions and in equation [1] does e denote the *exponent* of a power; elsewhere superscript letters always denote an *index*.

III. Suppose there are other positive values of t, u not contained in the sequences t^0, t', t'' etc., u^0, u', u'' etc., say $\mathfrak{T}, \mathfrak{U}$. Since the sequence u^0, u' etc. increases from 0 without bound, $\mathfrak{U}$ must clearly lie between two consecutive terms, u^n and u^{n+1}, so that $\mathfrak{U} > u^n$ and $\mathfrak{U} < u^{n+1}$. To show that this assumption is absurd, we observe the following.

1° The equation $tt - Duu = mm$ is also satisfied by taking

$$t = \frac{1}{m}(\mathfrak{T}t^n - D\mathfrak{U}u^n), \quad u = \frac{1}{m}(\mathfrak{U}t^n - \mathfrak{T}u^n).$$

This is readily confirmed by substitution. We show as follows that these values, which we will briefly denote by $= \tau, \upsilon$, are always *integers*. If (M, N, P) is a form with determinant D, and m is a common divisor of $M, 2N, P$, then both $\mathfrak{T} + N\mathfrak{U}$ and $t^n + Nu^n$ are divisible by m, and so is $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$, or $\mathfrak{U}t^n - \mathfrak{T}u^n$. Thus υ is an integer, and so is τ, since $\tau\tau = D\upsilon\upsilon + mm$.

2° Clearly υ cannot be $= 0$, for this would give

$$\mathfrak{U}\mathfrak{U}t^n t^n = \mathfrak{T}\mathfrak{T}u^n u^n$$

or

$$\mathfrak{U}\mathfrak{U}(Du^n u^n + mm) = u^n u^n(D\mathfrak{U}\mathfrak{U} + mm)$$

or $\mathfrak{U}\mathfrak{U} = u^n u^n$, contrary to the hypothesis $\mathfrak{U} > u^n$. So, since apart from 0 the smallest value of u is U, υ is certainly no smaller than U.

3° From the values of $t^n, t^{n+1}, u^n, u^{n+1}$ we easily confirm that

$$mU = u^{n+1}t^n - t^{n+1}u^n.$$

So $\mathfrak{U}t^n - \mathfrak{T}u^n$ is certainly no smaller than $u^{n+1}t^n - t^{n+1}u^n$.

4° Now the equation $\mathfrak{T}\mathfrak{T} - D\mathfrak{U}\mathfrak{U} = mm$ gives

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{\left(D + \frac{mm}{\mathfrak{U}\mathfrak{U}}\right)}$$

and similarly

$$\frac{t^{n+1}}{u^{n+1}} = \sqrt{\left(D + \frac{mm}{u^{n+1}u^{n+1}}\right)}$$

from which we easily deduce $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{n+1}}{u^{n+1}}$. This and the conclusion in 3° give

$$(\mathfrak{U}t^n - \mathfrak{T}u^n)\left(t^n + u^n\frac{\mathfrak{T}}{\mathfrak{U}}\right) > (u^{n+1}t^n - t^{n+1}u^n)\left(t^n + u^n\frac{t^{n+1}}{u^{n+1}}\right)$$

or, expanding and substituting for $\mathfrak{T}\mathfrak{T}$, $t^n t^n$, $t^{n+1}t^{n+1}$ their values $D\mathfrak{U}\mathfrak{U} + mm$, $Du^n u^n + mm$, $Du^{n+1}u^{n+1} + mm$,

$$\frac{1}{\mathfrak{U}}(\mathfrak{U}\mathfrak{U} - u^n u^n) > \frac{1}{u^{n+1}}(u^{n+1}u^{n+1} - u^n u^n)$$

Since both quantities are clearly positive, rearrangement gives $\mathfrak{U}+\frac{u^n u^n}{u^{n+1}} > u^{n+1}+\frac{u^n u^n}{\mathfrak{U}}$, *a contradiction*, because the first part of the first quantity is *smaller* than the first part of the second quantity, and its second part is also smaller than the second part of the other. So the assumption cannot hold, and the sequences t^0, t', t'' etc., u^0, u', u'' etc. give all positive values of t, u.

Example. For $D = 61,\ m = 2$ we found the smallest positive values of t, u to be $1523, 195$. So *all* positive values are given by the formulas

$$t = \left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e + \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e$$
$$u = \frac{1}{\sqrt{61}}\left(\left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e - \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e\right)$$

We find

$$t^0 = 2, \quad t' = 1523,$$
$$t'' = 1523t' - t^0 = 2319527,$$
$$t''' = 1523t'' - t' = 3532618098 \text{ etc.}$$
$$u^0 = 0, \quad u' = 195,$$
$$u'' = 1523u' - u^0 = 296985,$$
$$u''' = 1523u'' - u' = 452307960 \text{ etc.}$$

201.

We add the following observations on the problem treated in the preceding articles.

1) We have shown how to solve $tt - Duu = mm$ in every case where m is the greatest common divisor of three numbers $M, 2N, P$ such that $NN - MP = D$. It is worth finding all numbers that can be such divisors, or all values of m for a given value of D. Put $D = nnD'$, with D' entirely free of square factors. We obtain this by taking nn to be the largest square dividing D; if D itself already has no square factor, we must put $n = 1$. I then claim the following.

First, if D' has the form $4k+1$, every divisor of $2n$ is a value of m, and conversely. For if g divides $2n$, we have the form $\left(g, n, \frac{nn(1-D')}{g}\right)$, with determinant D, in which $g, 2n, \frac{nn(D'-1)}{g}$ clearly have greatest common divisor g (for $\frac{nn(D'-1)}{gg} = \frac{4nn}{gg} \cdot \frac{D'-1}{4}$ is clearly an integer). Conversely, suppose g is a value of m, namely the greatest common divisor of $M, 2N, P$, with $NN - MP = D$. Clearly $4D$, or $4nnD'$, is divisible by gg. It follows that $2n$ must be divisible by g. For if g did not divide $2n$, then g and $2n$ would have a greatest common divisor smaller than g. Putting this $= \delta$, and $2n = \delta n'$, $g = \delta g'$, we would have $n'n'D'$ divisible by $g'g'$, n' relatively prime to g', and therefore $n'n'$ to $g'g'$, so D' would also be divisible by $g'g'$, contrary to the hypothesis that D' has no square factor.

Second, if D' has the form $4k+2$ or $4k+3$, every divisor of n is a value of m, and conversely every value of m divides n. For if g divides n, we have the form $\left(g, 0, -\frac{nnD'}{g}\right)$, whose determinant $= D$, and in which $g, 0, \frac{nnD'}{g}$ clearly have greatest common divisor g. — Conversely, suppose g is a value of m, namely the greatest common divisor of $M, 2N, P$, with $NN - MP = D$. As above, g divides $2n$, or $\frac{2n}{g}$ is an integer. If this quotient were odd, the square $\frac{4nn}{gg}$ would be $\equiv 1 \pmod 4$, so $\frac{4nnD'}{gg}$ would be either $\equiv 2$ or $\equiv 3 \pmod 4$. But $\frac{4nnD'}{gg} = \frac{4D}{gg} = \frac{4NN}{gg} - \frac{4MP}{gg} \equiv \frac{4NN}{gg} \pmod 4$, so $\frac{4NN}{gg}$ would be either $\equiv 2$ or $\equiv 3 \pmod 4$, *a contradiction*, since every square must be congruent to zero or one modulo 4. So the quotient $\frac{2n}{g}$ must be even, and $\frac{n}{g}$ an integer, or g a divisor of n.

Thus 1 is always a value of m, or the equation $tt - Duu = 1$ can be solved by the preceding method for every positive nonsquare value of D; and 2 is a value of m exactly when D has either the form $4k$ or $4k+1$.

2) If m is greater than 2 but is an admissible number, solving $tt - Duu = mm$ can be reduced to solving a similar equation in which m is either 1 or 2. Put $D = nnD'$ as before. If m divides n, then mm divides D. If the smallest values of p, q in $pp - \frac{D}{mm}qq = 1$ are $p = P$, $q = Q$, the smallest values of t, u in $tt - Duu = mm$ are $t = mP$, $u = Q$. — But if m does not divide n, it at least divides $2n$ and is certainly even, while $\frac{4D}{mm}$ is an integer. If we then find that the smallest values of p, q in $pp - \frac{4D}{mm}qq = 4$ are $p = P$, $q = Q$, the smallest values of t, u in $tt - Duu = mm$ are $t = \frac{m}{2}P$, $u = Q$. — In both cases this method clearly derives not only from the smallest values of p, q the smallest values of t, u, but from *all* values of the former *all* values of the latter.

3) Let t^0, u^0; t', u'; t'', u'' etc. denote all positive values of t, u in $tt - Duu = mm$ (as in the preceding article). Suppose some values in this sequence are congruent to

its first values modulo any given r, say $t^\rho \equiv t$ (or $\equiv m$), $u^\rho \equiv u^0$, or $\equiv 0$ (mod. r), and at the same time the next values are congruent to the second values, say

$$t^{\rho+1} \equiv t', \quad u^{\rho+1} \equiv u' \pmod{r}$$

Then we also have

$$t^{\rho+2} \equiv t'', \quad u^{\rho+2} \equiv u''; \quad t^{\rho+3} \equiv t''', \quad u^{\rho+3} \equiv u''' \text{ etc.}$$

This follows easily because both sequences t^0, t', t'' etc., u^0, u', u'' etc. satisfy recurrence relations: since

$$t'' = \frac{2T}{m}t' - t^0, \quad t^{\rho+2} = \frac{2T}{m}t^{\rho+1} - t^\rho$$

we have

$$t'' \equiv t^{\rho+2}$$

and similarly for the others. — It follows that, in general,

$$t^{h+\rho} \equiv t^h, \quad u^{h+\rho} \equiv u^h \pmod{r}$$

where h denotes any number; and, more generally still, if

$$\mu \equiv \nu \pmod{\rho}, \quad \text{then } t^\mu \equiv t^\nu, \quad u^\mu \equiv u^\nu \pmod{r}.$$

4) We can always satisfy the conditions required in the preceding observation: we can always find an index ρ (for any given modulus r) such that

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u'$$

To prove this we observe the following.

First, we can always satisfy the third condition. The criteria given in (1) readily show that $pp - rrDqq = mm$ is also solvable. If the smallest positive values of p, q (apart from $m, 0$) are P, Q, the values of t, u clearly include $t = P$, $u = rQ$. So P, rQ occur in the sequences t^0, t' etc., u^0, u' etc.; and if $P = t^\lambda$, $rQ = u^\lambda$, then $u^\lambda \equiv 0 \equiv u^0 \pmod{r}$. It is also easy to see that between u^0 and u^λ no term is congruent to u^0 modulo r.

Second, if the other three conditions also hold, namely if $u^{\lambda+1} \equiv u'$, $t^\lambda \equiv t^0$, $t^{\lambda+1} \equiv t'$ as well, we clearly need only put $\rho = \lambda$. If, however, one or another of these conditions fails, I claim that we can certainly put $\rho = 2\lambda$. For equation [1] and the general formulas for t^e, u^e in the preceding article give

$$t^{2\lambda} = \frac{1}{m}(t^\lambda t^\lambda + Du^\lambda u^\lambda) = \frac{1}{m}(mm + 2Du^\lambda u^\lambda)$$

and therefore

$$\frac{t^{2\lambda} - t^0}{r} = \frac{2Du^\lambda u^\lambda}{mr}$$

This quantity is an integer, since by hypothesis r divides u^λ, and mm divides $4D$, so all the more m divides $2D$. — Further, $u^{2\lambda} = \frac{2}{m} t^\lambda u^\lambda$, and since

$$4t^\lambda t^\lambda = 4Du^\lambda u^\lambda + 4mm$$

which is therefore divisible by mm, $2t^\lambda$ is divisible by m, so $u^{2\lambda}$ is divisible by r, or

$$u^{2\lambda} \equiv u^0 \pmod{r}$$

Third, we find

$$t^{2\lambda+1} = t' + \frac{2Du^\lambda u^{\lambda+1}}{m}$$

and since $\frac{2Du^\lambda}{mr}$ is an integer for the same reason, we have

$$t^{2\lambda+1} \equiv t' \pmod{r}$$

Finally, we find

$$u^{2\lambda+1} = u' + \frac{2t^{\lambda+1}u^\lambda}{m}$$

and since $2t^{\lambda+1}$ is divisible by m, and u^λ by r, we have

$$u^{2\lambda+1} \equiv u' \pmod{r}. \quad \textit{This proves the claim.}$$

We will see the use of the last two observations in what follows.

202.

The special case of the problem, solving $tt - Duu = 1$, was already studied by the mathematicians of the preceding century. The very perceptive Fermat proposed this problem to the English analysts. Wallis names Brounker as the inventor of the solution he gives in *Alg. Cap.* 98, *Opp. T.* II *p.* 418 ff.; Ozanam names Fermat; and finally the distinguished Euler, who treats it in *Comm. Petr.* VI *p.* 175, *Comm. nov.* XI *p.* 28[*)], *Algebra P.* II *p.* 226, *Opusc. An.* I *p.* 310, names Pell. This is why some authors have called the problem *Pell's problem.* All these solutions agree in substance with the one we obtain by choosing in Article 198 the reduced form in which $a = 1$. But no one before the distinguished La Grange rigorously[*)] proved that the operation they prescribe must eventually *terminate*, or that the problem is always *actually solvable*: *Mélanges de la Soc. de Turin T.* IV *p.* 19, and more neatly in *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. This investigation also appears in the *supplements to Euler's Algebra*, already cited several times. Our method, however (based on entirely different principles and not restricted to $m = 1$), usually offers several ways to reach the solution, since in Article 198 we can start from any other reduced form $(a, b, -a')$.

[*)] In this paper the algorithm we presented in Article 27 is expressed in similar notation, which we neglected to mention there.

[*)] What Wallis offers for this purpose at the cited place, pp. 427, 428, carries no weight. His false reasoning consists in assuming, on p. 428, line 4, that for a given quantity p we can find integers a, z such that $\frac{z}{a}$ is smaller than p, with a shortfall smaller than the *specified* one. This is certainly true when the *specified* shortfall is *a given quantity*, but not when it depends on a and z, and so is variable, as happens in the present case.

203.

PROBLEM. *If the forms Φ, φ are equivalent, give all transformations of one into the other.*

Solution. When these forms are equivalent in only one way (*i.e.*, either only properly or only improperly), find by Article 196 one transformation of φ into Φ, say $\alpha, \beta, \gamma, \delta$. Clearly no transformations other than those similar to this one can exist. But when φ, Φ are both properly and improperly equivalent, find two dissimilar transformations, *i.e.*, one proper and one improper, say $\alpha, \beta, \gamma, \delta$ and $\alpha', \beta', \gamma', \delta'$. Every other transformation will be similar to one or the other. So let the form φ be (a, b, c), its determinant $= D$, the greatest common divisor of $a, 2b, c$ be m (as throughout the preceding discussion), and let t, u range over all numbers satisfying $tt - Duu = mm$. In the first case all transformations of φ into Φ are contained in the first of the following formulas, I; in the second case, either in the first, I, or in the second, II.

$$\begin{array}{lll} \text{I} \ldots\ldots\ldots & \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u), & \frac{1}{m}(\beta t - (\beta b + \delta c)u) \\ & \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u), & \frac{1}{m}(\delta t + (\beta a + \delta b)u) \\ \text{II} \ldots\ldots\ldots & \frac{1}{m}(\alpha' t - (\alpha' b + \gamma' c)u), & \frac{1}{m}(\beta' t - (\beta' b + \delta' c)u) \\ & \frac{1}{m}(\gamma' t + (\alpha' a + \gamma' b)u), & \frac{1}{m}(\delta' t + (\beta' a + \delta' b)u) \end{array}$$

Example. - We seek all transformations of $(129, 92, 65)$ into $(42, 59, 81)$. In Article 195 we found that these are equivalent only improperly, and in the next article we obtained the improper transformation $-47, -56, 73, 87$ of the former into the latter. So all transformations of $(129, 92, 65)$ into $(42, 59, 81)$ are given by the formula

$$-(47t + 421u), \quad -(56t + 503u). \quad 73t + 653u, \quad 87t + 780u$$

where t, u range over all numbers satisfying $tt - 79uu = 1$. These are given by

$$\begin{aligned} \pm t &= \tfrac{1}{2}\big((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e\big) \\ \pm u &= \tfrac{1}{2\sqrt{79}}\big((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e\big) \end{aligned}$$

where e takes all nonnegative integers.

204.

Clearly, the general formula giving all transformations becomes *simpler* as the initial transformation from which it is derived becomes simpler. Since we can choose which transformation to start from, we can often make the general formula simpler by deriving a simpler transformation from the formula first found, giving t, u particular values, and then forming another formula from it. For *example*, putting $t = 80$, $u = -9$ in the formula found in the preceding article's example gives a simpler transformation than the one we started from, namely $29, 47, -37, -60$. From this we derive the general formula $29t - 263u$, $47t - 424u$, $-37t + 337u$, $-60t + 543u$. So once we have obtained a general formula by the preceding rules, we can try giving t, u particular values $\pm t', \pm u'$; $\pm t'', \pm u''$ etc., to see whether we get a simpler

transformation than the one from which the formula was derived. If so, we can derive a simpler formula from that transformation. — Some freedom remains in judging simplicity. If it were worth the effort, we could put this on a fixed footing, and also assign *bounds* in the sequence t', u'; t'', u'' etc. beyond which the transformations become continually less simple. We would then need to try only those within the bounds, without going further. But with the methods we have given, the simplest transformation usually appears either at once or on taking t, u to have the values $\pm t', \pm u'$. So to keep this account brief, we leave out this investigation.

205.

PROBLEM. *Find all representations of a given number M by a given formula $axx + 2bxy + cyy$, with positive nonsquare determinant $= D$.*

Solution. First we observe that finding representations in values of x, y that are not relatively prime can be reduced to the case of relatively prime values of the indeterminates, in exactly the same way as above for forms with negative determinant (Article 181). So it would be unnecessary to repeat this here. For representations in relatively prime values of x, y to be possible, D must be a quadratic residue of M. If all values of the expression $\sqrt{D} \pmod{M}$ are $N, -N, N', -N', N'', -N''$ etc. (which we may take so that none is $> \frac{1}{2}M$), every representation of M by the given form belongs to one of these values. We must therefore first find these values, and then investigate the representations belonging to each in turn. There are no representations belonging to N unless the forms (a, b, c) and $(M, N, \frac{NN-D}{M})$ are properly equivalent. If they are, find any proper transformation of the former into the latter, say $\alpha, \beta, \gamma, \delta$. We then have the representation of M by (a, b, c) belonging to N, namely $x = \alpha$, $y = \gamma$, and all representations belonging to this value are given by

$$x = \tfrac{1}{m}\big(\alpha t - (\alpha b + \gamma c)u\big), \qquad y = \tfrac{1}{m}\big(\gamma t + (\alpha a + \gamma b)u\big)$$

where m denotes the greatest common divisor of $a, 2b, c$, and t, u range over all numbers satisfying $tt - Duu = mm$. — Clearly this general formula becomes simpler as the transformation $\alpha, \beta, \gamma, \delta$ from which it is derived becomes simpler. So it is useful first to find the simplest transformation of (a, b, c) into $(M, N, \frac{NN-D}{M})$, as in the preceding article, and derive the formula from it. — In exactly the same way, general formulas give the representations belonging to the remaining values $-N, N', -N'$ etc., if there are any.

Example. We seek all representations of 585 by the formula $42xx + 62xy + 21yy$. For representations in values of x, y that are not relatively prime, it is immediately clear that the only possible ones have greatest common divisor of x, y equal to 3, since 585 is divisible by only one square, 9. So once we have found all representations of $\frac{585}{9}$, *i.e.*, 65, by the form $42x'x' + 62x'y' + 21y'y'$, in which x' is relatively prime to y', all representations of 585 by $42xx + 62xy + 21yy$ in which x is not relatively prime to y follow by putting $x = 3x'$, $y = 3y'$. The values of $\sqrt{79} \pmod{65}$ are $\pm 12, \pm 27$. A representation of 65 belonging to -12 is $x' = 2$, $y' = -1$. So all representations of 65 belonging to this value are given by $x' = 2t - 41u$, $y' = -t + 53u$, and all representations of 585 arising *from these* by $x = 6t - 123u$, $y = -3t + 159u$. In the same way we find the general formula giving all representations of 65 belonging

to $+12$, namely $x' = 22t - 199u$, $y' = -23t + 211u$; and the formula containing all representations of 585 arising from these, $x = 66t - 597u$, $y' = -69t + 633u$. For the values $+27$ and -27, however, there is no representation of 65. — To find the representations of 585 in relatively prime values of x, y, we must first find the values of $\sqrt{79}$ (mod. 585), which are $\pm 77, \pm 103, \pm 157, \pm 248$. No representation is found to belong to $\pm 77, \pm 103, \pm 248$. But to -157 belongs the representation $x = 3$, $y = 1$, from which we derive the general formula giving all representations belonging to this value, $x = 3t - 114u$, $y = t + 157u$. Similarly, we find the representation belonging to $+157$, namely $x = 83$, $y = -87$, and the formula containing all similar representations, $x = 83t - 746u$, $y = -87t + 789u$. So we have four general formulas containing all representations of 585 by $42xx + 62xy + 21yy$:

$$\begin{aligned} x &= 6t - 123u & y &= -3t + 159u \\ x &= 66t - 597u & y &= -69t + 633u \\ x &= 3t - 114u & y &= t + 157u \\ x &= 83t - 746u & y &= -87t + 789u \end{aligned}$$

where t, u range over all integers satisfying $tt - 79uu = 1$.

To keep this account brief, we will not dwell on special applications of the preceding investigations into forms with positive nonsquare determinant. Anyone can work these out without difficulty, along the lines of Articles 176, 182. We turn at once to forms with positive square determinant, the only ones left to consider.

Forms with square determinant.

206.

PROBLEM. *Given a form (a, b, c) with square determinant hh, where h denotes its positive root, find a properly equivalent form (A, B, C) in which A lies between 0 and $2h - 1$, inclusive, $B = h$, and $C = 0$.*

Solution. I. Since $hh = bb - ac$, we have $(h - b) : a = c : -(h + b)$. Let $\beta : \delta$ be an equal ratio, with β relatively prime to δ, and determine α, γ so that $\alpha\delta - \beta\gamma = 1$, which is possible. Let the substitution $\alpha, \beta, \gamma, \delta$ take (a, b, c) into (a', b', c'), which is therefore properly equivalent to it. We have

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ &= (h - b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h + b)\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \\ c' &= a\beta\beta + 2b\beta\delta + c\delta\delta \\ &= (h - b)\beta\delta + 2b\beta\delta - (h + b)\beta\delta = 0 \end{aligned}$$

So if a' also already lies between 0 and $2h - 1$, the form (a', b', c') satisfies all the conditions.

II. But if a' lies outside the bounds 0 and $2h-1$, let A be the least positive residue of a' modulo $2h$, which clearly lies between these bounds, and put $A-a' = 2hk$. Then the form (a', b', c'), *i.e.*, $(a', h, 0)$, passes by the substitution $1, 0, k, 1$ into $(A, h, 0)$, which is properly equivalent to (a', b', c'), (a, b, c) and satisfies all the conditions. — Clearly the form (a, b, c) passes into $(A, h, 0)$ by the substitution $\alpha + \beta k, \beta, \gamma + \delta k, \delta$.

Example. Let the given form be $(27, 15, 8)$, with determinant $= 9$. Here $h = 3$; the ratio in smallest terms equal to $-12 : 27 = 8 : -18$ is $4 : -9$. So putting $\beta = 4$, $\delta = -9$, $\alpha = -1$, $\gamma = 2$, the form (a', b', c') becomes $(-1, 3, 0)$, which passes into $(5, 3, 0)$ by the substitution $1, 0, 1, 1$. This is therefore the required form, and the given form passes into it by the proper substitution $3, 4, -7, -9$.

We will call such forms (A, B, C), in which $C = 0$, $B = h$, and A lies between 0 and $2h - 1$, *reduced forms*. They must therefore be carefully distinguished from reduced forms with negative determinant or positive nonsquare determinant.

207.

THEOREM. *Two reduced forms $(a, h, 0)$, $(a', h, 0)$ that are not identical cannot be properly equivalent.*

Proof. Suppose they are properly equivalent, and let the former pass into the latter by the proper substitution $\alpha, \beta, \gamma, \delta$. We then have four equations:

$$\begin{aligned} a\alpha\alpha + 2h\alpha\gamma &= a' && \ldots\ldots\ldots [1] \\ a\alpha\beta + h(\alpha\delta + \beta\gamma) &= h && \ldots\ldots\ldots [2] \\ a\beta\beta + 2h\beta\delta &= 0 && \ldots\ldots\ldots [3] \\ \alpha\delta - \beta\gamma &= 1 && \ldots\ldots\ldots [4] \end{aligned}$$

Multiplying the second equation by β, the third by α, and subtracting gives $-h(\alpha\delta - \beta\gamma)\beta = \beta h$, or, by [4], $-\beta h = \beta h$, so we must have $\beta = 0$. Thus [4] gives $\alpha\delta = 1$

and $\alpha = \pm 1$. Then [1] gives $a \pm 2\gamma h = a'$. This equation cannot hold unless $\gamma = 0$ (since by hypothesis both a and a' lie between 0 and $2h - 1$), *i.e.*, unless $a = a'$, or the forms $(a, h, 0)$, $(a', h, 0)$ are identical, contrary to the hypothesis.

We can therefore easily solve the following problems, which caused much greater difficulty for nonsquare determinants.

I. *Given two forms F, F' with the same square determinant, determine whether they are properly equivalent.* Find two reduced forms properly equivalent to F, F' respectively. If they are identical, the given forms are properly equivalent; otherwise they are not.

II. *Under the same assumptions, determine whether they are improperly equivalent.* Let the form opposite to one of the given forms, *e.g.*, F, be G. If it is properly equivalent to F', then F and F' are improperly equivalent, and conversely.

208.

PROBLEM. *Given two properly equivalent forms F, F' with determinant hh, find a proper transformation of one into the other.*

Solution. Let F be properly equivalent to a reduced form Φ, which, by hypothesis, is therefore also properly equivalent to F'. By Article 206, find a proper transformation of F into Φ, say $\alpha, \beta, \gamma, \delta$, and also a proper transformation of F' into Φ, say $\alpha', \beta', \gamma', \delta'$. Then Φ passes into F' by the proper substitution $\delta', -\beta', -\gamma', \alpha'$, and so F passes into F' by the proper substitution

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

It is useful to develop another formula for this transformation of F into F', for which we need not even know the reduced form Φ itself. Let

$$F \text{ be } (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0)$$

Since the ratio in smallest terms equal to $h - b : a$ or $c : -(h + b)$ is $\beta : \delta$, we easily see that $\frac{h-b}{\beta} = \frac{a}{\delta}$ is an *integer*; call it f. Likewise, $\frac{c}{\beta} = \frac{-h-b}{\delta}$ is an integer; put it $= g$. We have

$$A = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma \quad \text{so}$$
$$\beta A = a\alpha\alpha\beta + 2b\alpha\beta\gamma + c\beta\gamma\gamma$$

or, substituting for $a\beta$ the value $\delta(h - b)$, and for c the value βg,

$$\beta A = \alpha\alpha\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta\beta\gamma\gamma g$$

or, since $b = -h - \delta g$,

$$\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$$

Similarly,

$$\begin{aligned}\delta A &= a\alpha\alpha\delta + 2b\alpha\gamma\delta + c\gamma\gamma\delta \\ &= \alpha\alpha\delta\delta f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma\gamma h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f\end{aligned}$$

So

$$\alpha = \tfrac{\beta A - g}{2h}, \qquad \gamma = \tfrac{\delta A - f}{2h}$$

In exactly the same way, putting

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \qquad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g'$$

gives

$$\alpha' = \tfrac{\beta' A - g'}{2h}, \qquad \gamma' = \tfrac{\delta' A - f'}{2h}$$

Substituting these values of $\alpha, \gamma, \alpha', \gamma'$ into the formula just given for the transformation of F into F' turns it into

$$\tfrac{\beta f' - \delta' g}{2h}, \quad \tfrac{\beta' g - \beta g'}{2h}, \quad \tfrac{\delta f' - \delta' f}{2h}, \quad \tfrac{\beta' f - \delta g'}{2h}$$

from which A has disappeared entirely.

If two improperly equivalent forms F, F' are given and we seek an improper transformation of one into the other, let G be the form opposite to F, and let a proper transformation of G into F' be $\alpha, \beta, \gamma.\ \delta$. Then clearly $\alpha, \beta, -\gamma, -\delta$ is an improper transformation of F into F'.

Finally, if the given forms are both properly and improperly equivalent, we can clearly find two transformations in this way, one proper and one improper.

209.

All that remains is to show how to derive all the other similar transformations from one transformation. This depends on solving the indeterminate equation $tt - hhuu = mm$, where m denotes the greatest common divisor of $a, 2b, c$, if (a, b, c) is either of the equivalent forms. But this equation can always be solved in only two ways: either put $t = m$, $u = 0$, or $t = -m$, $u = 0$. For suppose there is another solution $t = T$, $u = U$, with U not $= 0$. Since mm certainly divides $4hh$, we have $\frac{4TT}{mm} = \frac{4hhUU}{mm} + 4$, and both $\frac{4TT}{mm}$ and $\frac{4hhUU}{mm}$ are integer squares. But we easily see that 4 cannot be the difference of two integer squares unless the smaller square is 0, *i.e.*, $U = 0$, contrary to the hypothesis. — So if F passes into F' by the substitution $\alpha, \beta, \gamma, \delta$, there is no other transformation similar to this one except $-\alpha, -\beta, -\gamma, -\delta$. If two forms are equivalent only properly, or only improperly, there are therefore only *two* transformations. If they are both properly and improperly equivalent, there are *four*, namely two proper and two improper.

210.

THEOREM. *If two reduced forms $(a, h, 0)$, $(a', h, 0)$ are improperly equivalent, then $aa' \equiv mm\ (mod.\, 2mh)$, where m denotes the greatest common divisor of $a, 2h$ or $a', 2h$. Conversely, if $a, 2h$; $a', 2h$ have the same greatest common divisor m and $aa' \equiv mm\ (mod.\, 2mh)$, then the forms $(a, h, 0)$, $(a', h, 0)$ are improperly equivalent.*

Proof. I. Let $(a, h, 0)$ pass into $(a', h, 0)$ by the improper substitution $\alpha, \beta, \gamma, \delta$, so that we have four equations:

$$a\alpha\alpha + 2h\alpha\gamma = a' \quad \ldots\ldots\ldots\ldots [1]$$
$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad \ldots\ldots\ldots\ldots [2]$$
$$a\beta\beta + 2h\beta\delta = 0 \quad \ldots\ldots\ldots\ldots [3]$$
$$\alpha\delta - \beta\gamma = -1 \quad \ldots\ldots\ldots\ldots [4]$$

Multiplying [4] by h and subtracting it from [2], which we write as $[2] - h[4]$, gives

$$(a\alpha + 2h\gamma)\beta = 2h \quad \ldots\ldots\ldots\ldots [5]$$

Similarly, from $\gamma\delta[2] - \gamma\gamma[3] - (a + a\beta\gamma + h\gamma\delta)[4]$, after removing the terms that cancel, we get

$$-a\alpha\delta = a + 2h\gamma\delta, \quad \text{or} \quad -(a\alpha + 2h\gamma)\delta = a \quad \ldots [6]$$

Finally, we get $a[1] \ldots a\alpha(a\alpha + 2h\gamma) = aa'$, or

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

or

$$(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)} \quad \ldots\ldots [7]$$

Now [5] and [6] show that $a\alpha+2h\gamma$ divides $2h$ and a, and therefore also m, the greatest common divisor of $a, 2h$. But clearly m also divides $a\alpha + 2h\gamma$. So $a\alpha + 2h\gamma$ must be either $= +m$ or $= -m$. It follows at once from [7] that $mm \equiv aa' \pmod{2mh}$. *This proves the claim.*

II. If $a, 2h$; $a', 2h$ have the same greatest common divisor m and, in addition, $aa' \equiv mm \pmod{2mh}$, then $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa'-mm}{2mh}$ are integers. It is easy to check that $(a, h, 0)$ passes into $(a', h, 0)$ by the substitution $-\frac{a'}{m}, -\frac{2h}{m}, \frac{aa'-mm}{2mh}, \frac{a}{m}$, and that this transformation is improper. So these forms are improperly equivalent. *This proves the claim.*

From this we can also decide at once whether a given reduced form $(a, h, 0)$ is improperly equivalent to itself. If $a, 2h$ have greatest common divisor m, the required condition is $aa \equiv mm \pmod{2mh}$.

211.

We obtain all reduced forms with given determinant hh by substituting in the indefinite form $(A, h, 0)$, for A, all numbers from 0 to $2h - 1$, inclusive. So there are $2h$ of them. Clearly all forms with determinant hh can be divided into that many *classes*, and these have the same properties we discussed above (Articles 175, 195) for classes of forms with negative determinant and positive nonsquare determinant. For example, all forms with determinant 25 divide into ten classes, which can be distinguished by the reduced form in each. These reduced forms are $(0, 5, 0)$, $(1, 5, 0)$, $(2, 5, 0)$, $(5, 5, 0)$, $(8, 5, 0)$, $(9, 5, 0)$, which are also improperly equivalent to themselves; $(3, 5, 0)$, to which $(7, 5, 0)$ is improperly equivalent; and $(4, 5, 0)$, to which $(6, 5, 0)$ is improperly equivalent.

212.

PROBLEM. *Find all representations of a given number M by a given form $axx + 2bxy + cyy$ with determinant hh.*

We can solve this problem from the principles of Article 168 in exactly the same way as we showed above (Articles 180, 181, 205) for forms with negative determinant and positive nonsquare determinant. Since this involves no difficulty, it would be unnecessary to repeat it here. It is useful, however, to derive the solution from another principle specific to the present case.

Putting, as in Articles 206, 208,

$$h - b : a = c : -(h + b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g$$

we can easily prove that the given form is the product of the factors $\delta x - \beta y$ and $fx - gy$. So every representation of M by the given form gives a factorization of M into two factors. If all divisors of M are d, d', d'' etc. (including 1 and M, and taking each *twice*, both positively and negatively), we clearly obtain all representations of M by putting in turn

$$\delta x - \beta y = d, \qquad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \qquad fx - gy = \frac{M}{d'} \quad \text{etc.}$$

finding the values of x, y from these equations, and discarding the representations in which x or y has a fractional value. From the first two equations we clearly get

$$x = \tfrac{\beta M - gdd}{(\beta f - \delta g)d} \quad \text{and} \quad y = \tfrac{\delta M - fdd}{(\beta f - \delta g)d}$$

These values are always *determinate*, since $\beta f - \delta g = 2h$, so the numerator is certainly not $= 0$. — We could have solved the other problems from the same principle, namely that every form with square determinant factors into two factors. But here too we preferred to use a method analogous to the one given above for forms with nonsquare determinant.

Example. We seek all representations of 12 by $3xx + 4xy - 7yy$. This factors into $x - y$ and $3x + 7y$. All divisors of 12 are $\pm 1, 2, 3, 4, 6, 12$. Putting $x - y = 1$, $3x + 7y = 12$ gives $x = \frac{19}{10}$, $y = \frac{9}{10}$, which we must discard because they are fractional. In the same way the divisors $-1, \pm 3, \pm 4, \pm 6, \pm 12$ give unusable values. But the divisor $+2$ gives $x = 2, y = 0$, and -2 gives $x = -2$, $y = 0$. So there are no representations beyond these two.

This method cannot be used if $M = 0$. In that case all values of x, y must clearly satisfy either $\delta x - \beta y = 0$ or $fx - gy = 0$. All solutions of the first equation are contained in the formula $x = \beta z$, $y = \delta z$, where z ranges over all integers (since, as assumed, β, δ are relatively prime). Similarly, putting the greatest common divisor of $f, g = m$, all solutions of the second equation are given by $x = \frac{gz}{m}, y = \frac{hz}{m}$. These two general formulas therefore contain all representations of M in this case.

* * *

In the preceding discussion we have set out everything needed to recognize equivalence, find all transformations of forms, and find all representations of given numbers by given forms, so that there seems to be nothing more to ask for. All that remains is to show, given two forms that cannot be equivalent because their *determinants are unequal*, how to decide whether one is contained in the other and, if so, how to find all transformations of the former into the latter.

Forms contained in others but not equivalent to them.

213.

Above, in Articles 157, 158, we showed that if a form f with determinant D contains a form F with determinant E and passes into it by the substitution $\alpha, \beta, \gamma, \delta$, then $E = (\alpha\delta - \beta\gamma)^2 D$. If $\alpha\delta - \beta\gamma = \pm 1$, the form f not only contains F but is equivalent to it. So if f contains F without being equivalent to it, the quotient $\frac{E}{D}$ is an integer greater than 1. The problem we must now solve is therefore *to decide whether a given form f with determinant D contains a given form F with determinant Dee*, where e is assumed to be a positive number greater than 1. We will do this by showing how to give a finite collection of forms contained in f, such that F, if contained in f, must be equivalent to one of them.

I. Let all the positive divisors of e (including 1 and e) be m, m', m'' etc., and let $e = mn = m'n' = m''n''$ etc. For brevity, denote the form into which f passes by the proper substitution $m.0, 0, n$ by $(m; 0)$, the form into which f passes by the proper substitution $m, 1, 0, n$ by $(m; 1)$, etc., and generally the form into which f passes by the proper substitution $m, k, 0, n$ by $(m; k)$. Similarly, let f pass by the proper substitution $m', 0, 0, n'$ into $(m'; 0)$, by $m', 1, 0, n'$ into $(m'; 1)$, etc., by $m'', 0, 0, n''$ into $(m''; 0)$, and so on. All these forms are properly contained in f, and each has determinant $= Dee$. Denote the collection of all forms $(m; 0)$, $(m; 1)$, $(m; 2) \ldots (m; m-1)$, $(m'; 0)$, $(m'; 1) \ldots (m'; m'-1)$; $(m''; 0)$ etc., whose number is $m + m' + m'' +$ etc. and which are easily seen to be all distinct, by Ω.

For *example*, if the form f is $(2, 5, 7)$ and $e = 5$, then Ω contains the following six forms: $(1; 0)$, $(5; 0)$, $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$. Written out, these are $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$.

II. I now claim that if a form F with determinant Dee is properly contained in f, it must be properly equivalent to one of the forms Ω. Suppose f passes into F by the proper substitution $\alpha, \beta, \gamma, \delta$. Then $\alpha\delta - \beta\gamma = e$. Let the greatest common divisor of γ, δ (which cannot both be 0), taken positively, be $= n$, and let $\frac{e}{n} = m$, which is clearly an integer. Choose g, h so that $\gamma g + \delta h = n$, and finally let k be the least positive residue of $\alpha g + \beta h$ modulo m. Then $(m; k)$, which clearly belongs to Ω, is properly equivalent to F, and passes into it by the proper substitution

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

For *first*, these four numbers are clearly integers; *second*, it is easy to check that the substitution is proper; *third*, the form into which $(m; k)$ passes by this substitution is clearly the same as the one into which f*) passes by the substitution

$$m\left(\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h\right) + \frac{k\gamma}{n}, \quad m\left(\frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g\right) + \frac{k\delta}{n}, \quad \gamma, \quad \delta$$

or, since $mn = e = \alpha\delta - \beta\gamma$, and therefore $\beta\gamma + mn = \alpha\delta$, $\alpha\delta - mn = \beta\gamma$, by

$$\frac{1}{n}(\alpha\gamma g + \alpha\delta h), \quad \frac{1}{n}(\beta\gamma g + \beta\delta h), \quad \gamma, \quad \delta$$

*) Since it passes by the substitution $m, k, 0, n$ into $(m; k)$. See Article 159.

or finally, since $\gamma g + \delta h = n$, by $\alpha, \beta, \gamma, \delta$, *i.e.*, by hypothesis, into F. So $(m; k)$ and F are properly equivalent. *This proves the claim.*

We can therefore always decide whether a given form f with determinant D properly contains a form F with determinant Dee. To decide whether f improperly contains F, we need only investigate whether the form opposite to F is properly contained in f (Article 159).

214.

PROBLEM. *Given two forms, f with determinant D and F with determinant Dee, the former properly containing the latter, give all proper transformations of f into F.*

Solution. Let Ω denote the same collection of forms as in the preceding article. Select from it all forms to which F is properly equivalent; let them be Φ, Φ', Φ'' etc. Each of these forms gives proper transformations of f into F in the following way, different forms giving different transformations (*i.e.*, each gives distinct ones), and all together giving all of them (*i.e.*, there is no proper transformation of f into F that is not supplied by one of the forms Φ, Φ' etc.). Since the method is the same for all forms Φ, Φ' etc., we will discuss just one.

Let Φ be $(M; K)$, and $e = MN$, so that f passes into Φ by the proper substitution $M, K, 0, N$. Further, let all proper transformations of Φ into F be denoted by $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$. Then clearly f passes into Φ by the proper substitution $M\mathfrak{a} + K\mathfrak{c}, M\mathfrak{b} + K\mathfrak{d}, N\mathfrak{c}, N\mathfrak{d}$. In this way every proper transformation of Φ into F gives a proper transformation of f into F. — Treat the remaining forms Φ', Φ'' etc. in the same way: each of their proper transformations into F gives a proper transformation of f into F.

To see that this solution is complete in every respect, we must show:

I. *This gives all possible proper transformations of f into F.* Let any proper transformation of f into F be $\alpha, \beta, \gamma, \delta$. As in II of the preceding article, let n be the greatest common divisor of γ, δ, and determine m, g, h, k as there. Then $(m; k)$ is among the forms Φ, Φ' etc., and

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

is one of its proper transformations into F. From this the rule just given produces the transformation $\alpha, \beta, \gamma, \delta$. All this was proved in the preceding article.

II. *All transformations obtained in this way are distinct; none is obtained twice.* It is easy to see that different transformations of the same form Φ or Φ' etc. into F cannot produce the same transformation of f into F. To prove that different forms, *e.g.*, Φ and Φ', also cannot give the same transformation, we argue as follows. Suppose the proper transformation $\alpha, \beta, \gamma, \delta$ of f into F is obtained *both* from the proper transformation $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ of Φ into F *and* from the proper transformation $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \mathfrak{d}'$ of Φ' into F. Let $\Phi = (M; K)$, $\Phi' = (M'; K')$, $e = MN = M'N'$. Then we have the equations

$$\begin{aligned}
\alpha &= M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' && \ldots\ldots [1]\\
\beta &= M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}' && \ldots\ldots [2]\\
\gamma &= N\mathfrak{c} = N'\mathfrak{c}' && \ldots\ldots\ldots [3]\\
\delta &= N\mathfrak{d} = N'\mathfrak{d}' && \ldots\ldots\ldots [4]\\
\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} &= \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1 && \ldots\ldots\ldots [5]
\end{aligned}$$

From $\mathfrak{a}[4] - \mathfrak{b}[3]$, with the help of equation [5], we get $N = N'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}')$, so N' divides N. Similarly, $\mathfrak{a}'[4] - \mathfrak{b}'[3]$ gives $N(\mathfrak{a}'\mathfrak{d} - \mathfrak{b}'\mathfrak{c}) = N'$, so N divides N'. Since both N and N' are assumed positive, we must have $N = N'$ and $M = M'$, and then [3] and [4] give $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{d} = \mathfrak{d}'$. Further, $\mathfrak{a}[2] - \mathfrak{b}[1]$ gives

$$K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$$

so $K \equiv K' \pmod{M}$. This can hold only if $K = K'$, since both K and K' lie between 0 and $M - 1$. So the forms Φ, Φ' are not distinct, contrary to the hypothesis.

Clearly, if D is negative or a positive square, this method lets us actually find all proper transformations of f into F. But if D is positive and nonsquare, we can give general formulas containing all proper transformations, of which there are infinitely many.

Finally, if F is improperly contained in f, the method given lets us easily obtain all improper transformations of the former into the latter. Namely, suppose $\alpha, \beta, \gamma, \delta$ denote all proper transformations of f into the form opposite to F. Then all improper transformations of f into F are given by $\alpha, -\beta, \gamma, -\delta$.

Example. We seek all transformations of $(2, 5, 7)$ into $(275, 0, -1)$, which is both properly and improperly contained in the former. We gave the collection Ω for this case in the preceding article. Investigation shows that both $(5; 1)$ and $(5; 4)$ are properly equivalent to $(275, 0, -1)$. By the theory developed above, all proper transformations of $(5; 1)$, *i.e.*, $(50, 35, 19)$, into $(275, 0, -1)$ are found to be contained in the general formula

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u$$

where t, u range over all integers satisfying $tt - 275uu = 1$. So all proper transformations of $(2, 5, 7)$ into $(275, 0, -1)$ arising from these are contained in the general formula

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u$$

Similarly, all proper transformations of $(5, 4)$, *i.e.*, $(50, 65, 79)$, into $(275, 0, -1)$ are contained in the general formula

$$14t + 275u, \quad t + 14u, \quad -15t - 275u, \quad -t - 15u$$

and so all proper transformations of $(2, 5, 7)$ into $(275, 0, -1)$ arising from these are contained in

$$10t + 275u, \quad t + 10u, \quad -15t - 275u, \quad -t - 15u$$

These two formulas therefore contain all the required proper transformations*). — In the same way we find that all improper transformations of $(2, 5, 7)$ into $(275, 0, -1)$ are contained in the following two formulas:

$$\text{(I)} \ \ldots \quad 65t - 1100u, \quad 4t - 65u, \quad -15t + 275u, \quad -t + 15u$$

and

$$\text{(II)} \ \ldots \quad 10t + 275u, \quad -t - 10u, \quad -15t - 275u, \quad t + 15u$$

*) All proper transformations are given more elegantly by the formula

$$10t + 55u, \quad t + 2u, \quad -15t - 55u, \quad -t - 3u$$

where t, u range over all integers satisfying $tt - 11uu = 1$.

Forms with determinant 0.

215.

So far we have excluded forms with determinant 0 from all our investigations. We must add a few things about them to make our theory complete in every respect. We have proved generally that if a form with determinant D contains a form with determinant D', then D' is a multiple of D. So a form with determinant $= 0$ clearly cannot contain any form whose determinant is not also $= 0$. Only two problems therefore remain: 1° *given two forms f, F, the latter with determinant 0, decide whether the former contains the latter, and if it does, give all transformations of the former into the latter;* 2° *find all representations of a given number by a given form with determinant 0.* The first problem requires one method when the determinant of the first form f is also 0, and another when it is not 0. We will now set all this out.

I. First we observe that every form $axx + 2bxy + cyy$ with determinant $bb - ac = 0$ can be written as $m(gx + hy)^2$, where g, h are relatively prime and m is an integer. For let m be the greatest common divisor of a, c, taken with the same sign as these numbers themselves (we easily see that they cannot have opposite signs). Then $\frac{a}{m}, \frac{c}{m}$ are relatively prime nonnegative integers; their product is $= \frac{bb}{mm}$, *i.e.*, a square, so they themselves are squares (Article 21). Let $\frac{a}{m} = gg$, $\frac{c}{m} = hh$. Then g, h are also relatively prime, $gghh = \frac{bb}{mm}$, and $gh = \pm\frac{b}{m}$. Clearly, then,

$$m(gx \pm hy)^2 = axx + 2bxy + cyy$$

Now let two forms f, F be given, both with determinant 0, and let

$$f = m(gx + hy)^2, \quad F = M(GX + HY)^2$$

where g is relatively prime to h, and G to H. I claim that if f contains F, then m either equals M or at least divides M, and the quotient is a square. Conversely, if $\frac{M}{m}$ is an integer square, F is contained in f. For suppose f passes by the substitution

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

into F. Then

$$\frac{M}{m}(GX + HY)^2 = ((\alpha g + \gamma h)X + (\beta g + \delta h)Y)^2$$

from which we easily get that $\frac{M}{m}$ is a square. Put it $= ee$. Then

$$e(GX + HY) = \pm((\alpha g + \gamma h)X + (\beta g + \delta h)Y), \quad \textit{i.e.}$$

$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h$$

So if $\mathfrak{G}, \mathfrak{H}$ are chosen so that $\mathfrak{G}G + \mathfrak{H}H = 1$, we have

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h), \quad \text{so an } \textit{integer.} \quad \textit{Q.E.D.}$$

Conversely, suppose $\frac{M}{m}$ is an integer square $= ee$. Then f contains F. Namely, we can choose integers $\alpha, \beta, \gamma, \delta$ so that

$$\alpha g + \gamma h = \pm eG, \quad \beta g + \delta h = \pm eH$$

For choose integers $\mathfrak{g}, \mathfrak{h}$ so that $\mathfrak{g}g + \mathfrak{h}h = 1$. We satisfy these equations by putting

$$\begin{aligned} \alpha &= \pm eG\mathfrak{g} + hz, \qquad & \gamma &= \pm eG\mathfrak{h} - gz \\ \beta &= \pm eH\mathfrak{g} + hz', \qquad & \delta &= \pm eH\mathfrak{h} - gz' \end{aligned}$$

whatever integer values we give z, z'. So F is contained in f. *This proves the claim.* We also easily see that these formulas give all possible values of $\alpha, \beta, \gamma, \delta$, *i.e.*, all transformations of f into F, if z, z' range over all integers.

II. Given two forms $f = axx + 2bxy + cyy$ with determinant not $= 0$, and $F = M(GX + HY)^2$ with determinant $= 0$ (where, as before, G, H are relatively prime), I claim *first* that if f contains F, then M can be represented by f; *second*, if M can be represented by f, then F is contained in f; *third*, if in this case all representations of M by f are given by $x = \xi, y = \upsilon$, then all transformations of f into F are given by $G\xi, H\zeta, G\upsilon, H\upsilon$. We prove all this as follows.

1° Suppose f passes into F by the substitution $\alpha, \beta, \gamma, \delta$, and choose $\mathfrak{G}, \mathfrak{H}$ so that $\mathfrak{G}G + \mathfrak{H}H = 1$. Clearly, putting $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$ makes the value of f equal to M, so M is representable by f.

2° Suppose $a\xi\xi + 2b\xi\upsilon + c\upsilon\upsilon = M$. Clearly, by the substitution $G\xi, H\xi, G\upsilon, H\upsilon$, the form f passes into F. To see that

3° in this case the substitution $G\xi, H\zeta, G\upsilon, H\upsilon$ gives *all* transformations of f into F, if ξ, υ give all values of x, y that make $f = M$, we argue as follows. Let $\alpha, \beta, \gamma, \delta$ be any transformation of f into F, and, as before, $\mathfrak{G}G + \mathfrak{H}H = 1$. Among the values of x, y are then

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H}, \quad y = \gamma\mathfrak{G} + \delta\mathfrak{H}$$

which give the substitution

$$G(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad H(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad G(\gamma\mathfrak{G} + \delta\mathfrak{H}), \quad H(\gamma\mathfrak{G} + \delta\mathfrak{H})$$

or

$$\begin{aligned} &\alpha + \mathfrak{H}(\beta G - \alpha H), \qquad &&\beta + \mathfrak{G}(\alpha H - \beta G) \\ &\gamma + \mathfrak{H}(\delta G - \gamma H), \qquad &&\delta + \mathfrak{G}(\gamma H - \delta G) \end{aligned}$$

But since

$$\begin{aligned} a(\alpha X + \beta Y)^2 + 2b(\alpha X + \beta Y)(\gamma X + \delta Y) \\ + c(\gamma X + \delta Y)^2 = M(GX + HY)^2 \end{aligned}$$

we have

$$\begin{aligned} a(\alpha\delta - \beta\gamma)^2 &= M(\delta G - \gamma H)^2 \\ c(\beta\gamma - \alpha\delta)^2 &= M(\beta G - \alpha H)^2 \end{aligned}$$

and therefore (since the determinant of f, multiplied by $(\alpha\delta - \beta\gamma)^2$, equals the determinant of F, *i.e.*, $= 0$, so that also $\alpha\delta - \beta\gamma = 0$),

$$\delta G - \gamma H = 0, \quad \beta G - \alpha H = 0$$

The substitution thus becomes $\alpha, \beta, \gamma, \delta$, which shows that the formula given supplies *all* transformations of f into F.

III. It remains to show how to give all representations of a given number by a given form with determinant 0. Let the form be $m(gx + hy)^2$. Clearly the number must be divisible by m, and the quotient must be a square. If we put the given number $= mee$, then for the same values of x, y that make $m(gx + hy)^2 = mee$, clearly $gx + hy$ is either $= +e$ or $= -e$. So we obtain all representations by finding all integer solutions of the linear equations $gx + hy = e$, $gx + hy = -e$. These are known to be solvable, since g, h are relatively prime, as assumed. Namely, if we choose $\mathfrak{g}, \mathfrak{h}$ so that $\mathfrak{g}g + \mathfrak{h}h = 1$, we satisfy the first equation by putting $x = \mathfrak{g}e + hz$, $y = \mathfrak{h}e - gz$, and the second by putting $x = -\mathfrak{g}e + hz$, $y = -\mathfrak{h}e - gz$, where z is any integer. These formulas give *all* integer values of x, y if z ranges over all integers.

General solution in integers of all indeterminate equations of the second degree in two unknowns.

As a finishing touch to these investigations, we add

216.

PROBLEM. *Find all integer solutions of the general*[*)] *indeterminate equation of the second degree in two unknowns*

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

(where a, b, c etc. are any given integers).

Solution. In place of the unknowns x, y, introduce

$$p = (bb - ac)x + be - cd \quad \text{and} \quad q = (bb - ac)y + bd - ae$$

which are clearly always integers when x, y are integers. This gives the equation

$$app + 2bpq + cqq + f(bb - ac)^2 + (bb - ac)(aee - 2bde + cdd) = 0$$

or, putting for brevity

$$f(bb - ac)^2 + (bb - ac)(aee - 2bde + cdd) = -M$$

the equation

$$app + 2bpq + cqq = M$$

We have already shown how to find all solutions of this equation, *i.e.*, all representations of M by (a, b, c). From each set of values of p, q, determine the corresponding values of x, y by the equations

$$x = \frac{p + cd - be}{bb - ac}, \quad y = \frac{q + ae - bd}{bb - ac}$$

We easily see that all these values satisfy the given equation, and that no integer values of x, y are missed by this method. So if we discard the fractional values from all the values of x, y obtained in this way, all the required solutions remain.

We make the following observations about this solution.

1° If either M cannot be represented by (a, b, c), or no representation gives *integer* values of x, y, then the equation has no integer solution.

2° If the determinant of (a, b, c), *i.e.*, $bb - ac$, is negative, or is a positive square and at the same time M is not $= 0$, the number of representations of M by (a, b, c) is finite. So the number of all solutions of the given equation, if there are any, is also finite.

3° If $bb - ac$ is positive and nonsquare, or is a square and at the same time $M = 0$, then M, if it can be represented at all, can be represented in *infinitely many different ways* by (a, b, c). But it is impossible to find all these representations *themselves* and

[*)] If an equation is given whose second, fourth or fifth coefficient is not even, multiplying it by 2 gives it the form assumed here.

try whether they give integer or fractional values of x, y. So we need a rule that lets us be *certain* when no representation at all can give integer values of x, y (for however many representations we *try* in this case, without such a rule we would never reach certainty). If some representations give integer values of x, y and others fractional values, we must show how to distinguish the latter from the former in advance, in general.

4° If $bb - ac = 0$, the values of x, y cannot be determined at all by the preceding formulas. So we must find a *special method* for this case.

217.

For the case where $bb - ac$ is a positive nonsquare number, we showed above that all representations of the number M by the form $app + 2bpq + cqq$ (if there are any at all) can be given by one or more formulas such as

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

where $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ denote given integers, m the greatest common divisor of the numbers $a, 2b, c$, and finally t, u range over all integers satisfying the equation $tt-(bb-ac)uu = mm$. Since all values of t, u can be taken both positively and negatively, we can replace each of those formulas by *four* others:

$$\begin{array}{ll} p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), & q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \\ p = \tfrac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), & q = \tfrac{1}{m}(\mathfrak{C}t - \mathfrak{D}u) \end{array}$$

$$\begin{array}{ll} p = \tfrac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), & q = \tfrac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u) \\ p = -\tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), & q = -\tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \end{array}$$

The total number of formulas is now four times as large as before, while t and u no longer stand for all numbers satisfying the equation $tt - (bb - ac)uu = mm$, but only the positive ones. We must therefore consider each of these forms separately and determine which values of t, u give integer values of x, y.

The formula

$$p = \tfrac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \tfrac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \qquad \ldots . \; [1]$$

gives the following values of x, y:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(bb - ac)}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(bb - ac)}$$

But we showed above that all (positive) values of t form a recurrent sequence t^0, t', t'' etc., and that the corresponding values of u likewise form a recurrent sequence u^0, u', u'' etc.; also, that we can specify a number ρ such that, for any given modulus,

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad t^{\rho+2} \equiv t'' \text{ etc.}, \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u' \text{ etc.}$$

We take the number $m(bb - ac)$ as this modulus. For brevity, we denote the values of x, y obtained by setting $t = t^0$, $u = u^0$, to which we assign the index 0, by x^0, y^0; similarly, those obtained by setting $t = t'$, $u = u'$, by x', y', to which we assign the index 1, etc. It is then easy to see that if x^h, y^h are integers and ρ is correctly determined, then $x^{h+\rho}, y^{h+\rho}$, as well as $x^{h+2\rho}, y^{h+2\rho}$ and, in general, $x^{h+k\rho}, y^{h+k\rho}$, will also be integers. Conversely, if x^h or y^h is fractional, then $x^{h+k\rho}$ or $y^{h+k\rho}$, respectively, will also be fractional. We readily conclude that if we work out the values of x, y with indices $0, 1, 2 \ldots . \rho - 1$, and for none of these indices are *both* x *and* y integers, then there is no index at all for which both x and y take integer values. In that case, no integer values of x, y can be derived from formula [1]. But if

some of those indices, say μ, μ', μ'' etc., correspond to integer values of x, y, then all integer values of x, y that can be obtained from formula [1] are those whose indices are contained in one of the formulas $\mu + k\rho$, $\mu' + k\rho$, $\mu'' + k\rho$ etc., where k ranges over all positive integers, including zero.

The remaining formulas containing the values of p, q must be treated in exactly the same way. If none of these formulas were to yield integer values of x, y, the proposed equation could not be solved in integers at all. Whenever it is in fact solvable, however, all its integer solutions can be given by the rules set out above.

218.

When $bb - ac$ is a square number and $M = 0$, all values of p, q are contained in two formulas of the kind $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, where z ranges over all integers, while $\mathfrak{A}, \mathfrak{B}, \mathfrak{A}', \mathfrak{B}'$ are given integers, the first and second being relatively prime, and likewise the third and fourth (Article 212). Thus all integer values of x, y arising from the first formula are contained in formula [1]

$$x = \frac{\mathfrak{A}z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{bb - ac}$$

and all the remaining ones arising from the second formula in this formula [2]:

$$x = \frac{\mathfrak{A}'z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{bb - ac}$$

But since either formula can also give fractional values (unless $bb - ac = 1$), we must separate, in each formula, the values of z that make both x and y integers from the others. It is enough, however, to consider the first formula alone, since exactly the same method applies to the other.

Since $\mathfrak{A}$, $\mathfrak{B}$ are relatively prime, we can determine two numbers $\mathfrak{a}$, $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$. This gives

$$(\mathfrak{a}x + \mathfrak{b}y)(bb - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$$

so it is immediately clear that all values of z capable of producing integer values of x, y must be congruent to the number $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ modulo $bb - ac$, or be contained in the formula $(bb - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$, where z' ranges over all integers. From this we easily obtain, in place of formula [1], the following:

$$x = \mathfrak{A}z' + \mathfrak{b} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$
$$y = \mathfrak{B}z' - \mathfrak{a} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$

It clearly gives, either for all values of z' or for none, integer values of x, y. The first case always occurs when $\mathfrak{A}(bd - ae)$ and $\mathfrak{B}(be - cd)$ are congruent modulo $bb - ac$, and the second when they are incongruent. — Formula [2] must be treated in exactly the same way, separating its integer solutions (if it can give any) from the others.

219.

When $bb - ac = 0$, the form $axx + 2bxy + cyy$ can be written as $m(\alpha x + \beta y)^2$, where m, α, β are integers (Article 215). Set $\alpha x + \beta y = z$; the proposed equation becomes

$$mzz + 2dx + 2ey + f = 0$$

and from this and $z = \alpha x + \beta y$ we obtain

$$x = \frac{\beta mzz + 2ez + \beta f}{2\alpha e - 2\beta d}, \quad y = \frac{\alpha mzz + 2dz + \alpha f}{2\beta d - 2\alpha e}$$

It is now clear that, unless $\alpha e = \beta d$ (a case we will consider separately in a moment), the values of x, y derived from these formulas by giving z any value satisfy the proposed equation. It remains only to show how to determine the values of z that give integer values of x, y.

Since $\alpha x + \beta y = z$, only *integer* values can be taken for z. Moreover, if some value of z makes both x and y integers, all values of z congruent to it modulo $2\alpha e - 2\beta d$ clearly also produce integer values. So substitute for z all integers from 0 to $2\alpha e - 2\beta d - 1$ (when $\alpha e - \beta d$ is positive) or to $2\beta d - 2\alpha e - 1$ (when $\alpha e - \beta d$ is negative), inclusive. If none of these values makes both x and y integers, then no value of z at all will produce integer values of x, y, and the proposed equation cannot be solved in integers. But if some of those values of z give integer values of x, y, say ζ, ζ', ζ'' etc. (which can also be found by solving quadratic congruences using the principles of Section IV), *all* solutions follow by setting $z = (2\alpha e - 2\beta d)v + \zeta$, $z = (2\alpha e - 2\beta d)v + \zeta'$ etc., where v ranges over all integers.

220.

For the excluded case where $\alpha e = \beta d$, we must find a separate method. Suppose α, β are relatively prime, as Article 215, I shows we may assume. Then $\frac{d}{\alpha} = \frac{e}{\beta}$ is an integer (Article 19), which we set $= h$. The proposed equation now takes the form

$$(m\alpha x + m\beta y + h)^2 - hh + mf = 0$$

and so clearly has no rational solution unless $hh - mf$ is a square number. Let $hh - mf = kk$; the following two equations are clearly equivalent to the proposed equation:

$$m\alpha x + m\beta y + h + k = 0, \quad \text{and} \quad m\alpha x + m\beta y + h - k = 0$$

i.e., every solution of the proposed equation also satisfies one or the other of these equations, and conversely. The first equation clearly cannot be solved in integers unless $h + k$ is divisible by m, and similarly the second admits no integer solution unless $h - k$ is divisible by m. These conditions also suffice for the solvability of each equation (since α, β are assumed relatively prime), and all the solutions can be given by the known rules.

221.

We illustrate the case considered in Article 217 (since it is the most difficult of all) by an example. Let the proposed equation be $xx + 8xy + yy + 2x - 4y + 1 = 0$. From this, by first introducing the other unknowns $p = 15x - 9$. $q = 15y + 6$, we derive the equation $pp + 8pq + qq = -540$. All its integer solutions are found to be contained in the following four formulas:

$$\begin{aligned} p &= 6t, \quad & q &= -24t - 90u \\ p &= 6t, \quad & q &= -24t + 90u \\ p &= -6t, \quad & q &= 24t - 90u \\ p &= -6t, \quad & q &= 24t + 90u \end{aligned}$$

where t, u range over all positive integers satisfying the equation $tt - 15uu = 1$, which are contained in the formula

$$\begin{aligned} t &= \tfrac{1}{2}\big((4 + \sqrt{15})^n + (4 - \sqrt{15})^n\big) \\ u &= \frac{1}{2\sqrt{15}}\big((4 + \sqrt{15})^n - (4 - \sqrt{15})^n\big) \end{aligned}$$

when n ranges over all positive integers (including zero). Thus all values of x, y are contained in the following formulas:

$$\begin{aligned} x &= \tfrac{1}{5}(2t + 3), \quad & y &= -\tfrac{1}{5}(8t + 30u + 2) \\ x &= \tfrac{1}{5}(2t + 3), \quad & y &= -\tfrac{1}{5}(8t - 30u + 2) \\ x &= \tfrac{1}{5}(-2t + 3), \quad & y &= \tfrac{1}{5}(8t - 30u - 2) \\ x &= \tfrac{1}{5}(-2t + 3), \quad & y &= \tfrac{1}{5}(8t + 30u - 2) \end{aligned}$$

Applying our rules correctly, we find that to obtain *integer* values, the first and second formulas require those values of t, u that arise from an *even* index n; the third and fourth require those obtained from an *odd* n. — The simplest solutions are $x = 1, -1, -1$; $y = -2, 0, 12$, respectively.

We should also note that the solution of the problem explained in the preceding articles can usually be shortened by various devices, especially in excluding unusable solutions, *i.e.*, those involving fractions. But to avoid going on too long, we have had to pass over these here.

Historical remarks.

222.

Since several of the matters we have discussed so far have also been considered by other mathematicians, we cannot pass over their contributions in silence. The distinguished La Grange made general investigations into the *equivalence of forms*, *Nouv. Mém. de l'Ac. de Berlin,* 1773 *p.* 263 and 1775 *p.* 323 ff. In particular, he showed that for any given determinant there is a finite number of forms such that every form with that determinant is equivalent to one of them, and so all forms with a given determinant can be divided into classes. Later, the celebrated Le Gendre discovered several elegant properties of this classification, mostly by induction from observed cases; we will give these below and support them with proofs. But no one had yet reached the distinction between proper and improper equivalence, whose usefulness is most apparent in the finer investigations.

The distinguished La Grange was the first to solve completely the famous problem explained in Article 216 ff., *Hist. de l'Ac. de Berlin,* 1767 *p.* 165 and 1768 *p.* 181 ff. A solution (but a less complete one) also appears in the *Suppl. ad Euleri Algebram*, already cited several times. Earlier, the distinguished Euler had tackled the same subject, *Comm. Petr. T.* VI *p.* 175; *Comm. Nov. T.* IX *p.* 3; *Ibid. T.* XVIII *p.* 185 ff. But he always restricted his investigation to deriving other solutions from some solution he assumes already known; moreover, his methods can provide *all* solutions in only a few cases (see La Grange, *Hist. de l'Ac. de Berlin* 1767, *p.* 237). Since the last of these three papers is later than La Grange's solution, which covers the problem in full generality and leaves nothing to be desired in this respect, Euler seems not yet to have known that solution at the time (Volume XVIII of the Commentaries belongs to the year 1773 and was published in 1774). Our solution, however (like everything else we have given so far in this section), rests on entirely different principles.

The relevant results given by others, Diophantus, Fermat, etc., concern very special cases. Since we have already mentioned above those that seemed particularly worth recording, we will refrain from listing everything individually.

* *
*

What we have set out so far about forms of the second degree should be regarded only as the first elements of this theory. As we pursued this investigation more closely, a vast field opened up before us; in what follows we will select from it those matters that seem especially worth attention. For this subject is so fertile that, for brevity, we must pass over in silence many other things we have already managed to discover; far more, without doubt, still lie hidden and await new efforts. At the start of these investigations, we should note at once that forms with determinant 0 are excluded unless we state otherwise.

FURTHER INVESTIGATIONS INTO FORMS.

Division of forms with a given determinant into classes.

223.

We have already shown above (Articles 175, 195, 211) that for any given integer D (positive or negative), we can specify a finite number of forms F, F', F'' etc. with determinant D, such that every form with determinant D is properly equivalent to one, and only one, of them. Thus all forms with determinant D (of which there are infinitely many) can be *classified* according to those forms: the collection of all forms properly equivalent to F makes up the first class; those properly equivalent to F' make up the second, etc.

From each class of forms with a given determinant D, we can choose a form and regard it as a *representative form* of the whole class. In itself, the choice of form from each class is entirely arbitrary, but we should always prefer one that seems to surpass the others in *simplicity*. The simplicity of a form (a, b, c) must clearly be judged from the size of the numbers a, b, c, and we may rightly call a form (a', b', c') less simple than (a, b, c) if $a' > a$, $b' > b$, $c' > c$. But this does not settle the matter completely: for *example*, it remains our choice which of the forms $(17, 0, -45)$, $(5, 0, -153)$ we prefer to call simpler. Usually, however, it will be useful to follow this rule:

I. When the determinant D is negative, take the reduced forms contained in the individual classes as their representative forms. If two reduced forms occur in the same class (which will be opposite, Article 172), take the one whose middle term is positive.

II. When the determinant D is positive and nonsquare, work out the period of a reduced form contained in the proposed class. This period will contain either two ambiguous forms or none (Article 187).

1) In the first case, let the ambiguous forms be (A, B, C), (A', B', C'); let the least residues of the numbers B, B' modulo A, A' be M, M', respectively (these can be taken positively unless they are $= 0$); finally, let $\frac{D-MM}{A} = N$, $\frac{D-M'M'}{A'} = N'$. With this done, take whichever of the forms $(A, M, -N)$, $(A', M', -N')$ seems simplest as the representative form. In deciding this, prefer a form whose middle term is $= 0$. If the middle term is 0 in both or in neither, prefer the form with the smaller first term; and when the first terms are equal in size but opposite in sign, prefer the positive sign to the negative.

2) If there is no ambiguous form in the whole period, choose from all the forms of the period the one with the smallest first term, disregarding its sign. If two forms occur in the same period with the same first term positive in one and negative in the other, prefer the former to the latter. Let this form be (A, B, C), and derive from it, in the same way as in the preceding case, another form $(A, M, -N)$ (namely, by taking M to be the absolutely least residue of B modulo A, and setting $N = \frac{D-MM}{A}$). Take this last form as the representative.

If the same smallest first term A happens to be shared by several forms of the period, treat all these forms in the way prescribed, and take as representative the resulting form whose middle term is as small as possible.

Thus, for *example*, for $D = 305$ we have, among others, the period $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$. From it we first choose the form $(7, 16, -7)$, and then derive from this the representative form $(7, 2, -43)$.

III. When the determinant is a positive square $= kk$, find the reduced form $(A, k, 0)$ contained in the proposed class. If $A < k$ or $= k$, take this form itself as the representative. But if $A > k$, take in its place the form $(A - 2k, k, 0)$, whose first term will be negative but smaller than k.

Example. In this way all forms with determinant -235 are divided into sixteen classes, whose representatives are $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$, and eight others differing from the preceding ones only in the signs of their outer terms: $(-1, 0, -235)$, $(-2, 1, -118)$ etc.

All forms with determinant 79 fall into six classes, whose representatives are $(1, 0, -79)$, $(3. 1, -26)$, $(3, -1, -26)$, $(-1, 0. 79)$, $(-3, 1, 26)$, $-3. -1, 26)$.

224.

This classification therefore separates properly equivalent forms completely from the others. Two forms with the same determinant D, if they belong to the same class, will be properly equivalent. Any number representable by one can also be represented by the other; and if a number M can be represented by the first form with relatively prime values of the indeterminates, the same number can be represented by the other form in the same way, with both representations belonging to the same value of the expression $\sqrt{D}$ (mod. M). But if two forms belong to different classes, they will not be properly equivalent. From the representability of a given number by one, we cannot infer its representability by the other. On the contrary, if the number M can be represented by one with relatively prime values of the indeterminates, we are immediately certain that there is no similar representation of the same number by the other form belonging to the same value of the expression $\sqrt{D}$(mod. M) (see Articles 167, 168).

On the other hand, two forms F, F' from different classes K, K' can indeed be improperly equivalent. In this case, *every* form from one class will be improperly equivalent to *every* form from the other. Every form from K will have its opposite in K', and the classes K, K' themselves will be called *opposite*. Thus in the first example of the preceding article, the third class of forms with determinant -235 is opposite to the fourth, and the seventh to the eighth; in the second example, the second class is opposite to the third, and the fifth to the sixth. So, given any two forms from opposite classes, every number M representable by one is also representable by the other. If one representation uses relatively prime values of the indeterminates, the other can do so too, but these two representations belong to opposite values of the expression $\sqrt{D}$ (mod. M). — The rules given above for choosing representative forms are arranged so that opposite classes always receive opposite representative forms.

Finally, there are also classes *opposite to themselves*. If a form and its opposite belong to the same class, it is easy to see that all forms in this class are both properly and improperly equivalent to one another and have their opposites in the same class. Every class containing an ambiguous form has this property; conversely, every class

opposite to itself necessarily contains an ambiguous form (Articles 163, 165), and so is called an *ambiguous class*. Thus among the classes of forms with determinant -235 there are eight ambiguous ones, represented by $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$; among the classes of forms with determinant 79 there are two, represented by $(1, 0, -79)$, $(-1, 0, 79)$. — If the representative forms have been determined by our rules, the ambiguous classes can easily be recognized from them. For a positive nonsquare determinant, an ambiguous class certainly receives an ambiguous representative form (Article 194). For a negative determinant, the representative form of an ambiguous class is either itself ambiguous or has equal outer terms (Article 172). Finally, for a positive square determinant, Article 210 makes it easy to decide whether the representative form is improperly equivalent to itself, and thus whether the class it represents is ambiguous.

225.

We have already shown above (Article 175) that in a form (a, b, c) with negative determinant, the outer terms have the same sign, both as each other and as the outer terms of any equivalent form. If a, c are positive, we call the form (a, b, c) *positive*. We also call the whole class containing (a, b, c), which consists only of positive forms, a *positive class*. Conversely, (a, b, c) will be a *negative form*, contained in a *negative class*, if a, c are negative. Negative numbers cannot be represented by a positive form, nor positive numbers by a negative form. If the form (a, b, c) represents a positive class, the form $(-a, b, -c)$ represents a negative class. It follows that there are as many positive classes as negative ones, and that once the former have been specified, the latter are also known. Thus in investigating forms with negative determinant, it is usually enough to consider the positive classes, whose properties transfer easily to the negative classes.

This distinction applies only to forms with negative determinant. Forms with positive determinant can represent both positive and negative numbers without distinction; indeed, two forms such as (a, b, c), $(-a, b, -c)$ quite often belong to the same class in this case.

Division of classes into orders.

226.

We call a form (a, b, c) *primitive* if the numbers a, b, c share no nontrivial divisor; otherwise it is called *derived*. More precisely, if the greatest common divisor of the numbers a, b, c is set $= m$, the form (a, b, c) is *derived from the primitive form* $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$. This definition immediately shows that all forms whose determinant is divisible by no square (except 1) must be primitive. Further, Article 161 shows that if a given class of forms with determinant D contains a primitive form, all forms of this class are primitive; in that case the class itself is called *primitive*. It is also clear that if a form F with determinant D is derived from a primitive form f with determinant $\frac{D}{mm}$, and the classes containing the forms F, f are K, k, respectively, then all forms in the class K are derived from the primitive class k. In this case we therefore call the class K itself *derived from the primitive class* k.

If (a, b, c) is a primitive form, but a, c are not both even (*i.e.*, both are odd, or at least one is), it is easy to see that not only a, b, c, but also a, $2b$, c share no nontrivial divisor. In this case the form (a, b, c) is called *properly primitive*, or simply a *proper form*. But if (a, b, c) is a primitive form and the numbers a, c are both even, the numbers a, $2b$, c clearly have the common divisor 2 (which is also their greatest common divisor), and (a, b, c) is called an *improperly primitive form*, or simply an *improper form*[*)]. In this case b must be odd (otherwise (a, b, c) would not be primitive); so $bb \equiv 1 \pmod 4$, and since ac is divisible by 4, the determinant $bb - ac \equiv 1 \pmod 4$. Improper forms therefore occur only for a determinant of the form $4n+1$ if positive, or of the form $-(4n+3)$ if negative. — Article 161 also makes it clear that if a given class contains a properly primitive form, all forms of this class are properly primitive; conversely, a class containing an improperly primitive form consists only of improperly primitive forms. Thus in the first case the class itself is called *properly primitive*, or simply *proper*; in the second, *improperly primitive*, or *improper*. For *example*, among the positive classes of forms with determinant -235, six are proper, namely those represented by $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$, and there are just as many among the negative classes; two in each group are improper. — The classes of forms with determinant 79 (a number of the form $4n + 3$) are all proper.

If a form (a, b, c) is derived, specifically from the primitive form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, the latter can be either properly or improperly primitive. In the first case m is also the greatest common divisor of the numbers a, $2b$, c; in the second their greatest common divisor is $2m$. This explains the distinction between a *form derived from a properly primitive form* and a *form derived from an improperly primitive form*; and also (since by Article 161 all forms in the same class behave alike in this respect) between a *class derived from a properly primitive class* and a *class derived from an improperly primitive class*.

[*)] We chose the terms *properly* and *improperly* here because no more suitable ones came to mind. We mention this so that no one will look for a hidden connection between this meaning and the one we have used since Article 157: there is none. In any case, there is certainly no need to fear ambiguity here.

These distinctions give us a first foundation for dividing all classes of forms with a given determinant into different *orders*. We place two classes represented by the forms (a, b, c), (a', b', c') in the *same order* if *both* the numbers a, b, c have the same greatest common divisor as a', b', c', *and* a, $2b$, c have the same greatest common divisor as a', $2b'$, c'. If either or both of these conditions fail, the classes belong to *different orders*. It follows at once that all properly primitive classes form one order, and all improperly primitive classes another. If mm is a square dividing the determinant D, the classes derived from properly primitive classes with determinant $\frac{D}{mm}$ form a separate order, and those derived from improperly primitive classes with determinant $\frac{D}{mm}$ another, etc. If D is divisible by no square (except 1), there are no orders of derived classes. Thus there is either just one order (when $D \equiv 2$ or 3 modulo 4), namely the order of properly primitive classes, or two (when $D \equiv 1$ (mod. 4)), namely the order of properly primitive classes and the order of improperly primitive classes. The principles of combinatorics readily give the following general rule. Suppose $D = D'2^{2\mu}a^{2\alpha}b^{2\beta}c^{2\gamma}\ldots$, where D' has no square factor and a, b, c etc. are distinct odd primes (any number can be put in this form by setting $\mu = 0$ when D is not divisible by 4, and setting α, β, γ etc. all $= 0$, or, equivalently, omitting the factors $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$ etc., when D is divisible by no odd square). Then there are either

$$(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1)\ldots$$

orders, namely when $D' \equiv 2$ or 3 (mod. 4), or

$$(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1)\ldots$$

orders when $D' \equiv 1$ (mod. 4). But we omit the proof of this rule, since it is neither difficult nor particularly necessary here.

Example 1. For $D = 45 = 5.3^2$ there are six classes, represented by $(1, 0, -45)$, $(-1.0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3.0, -15)$, $(6, 3, -6)$. They are divided into four orders: Order I contains the two proper classes represented by $(1, 0, -45)$, $(-1, 0, 45)$; Order II contains the two improper classes, represented by $(2, 1, -22)$, $(-2, 1, 22)$; Order III contains one class derived from a proper class with determinant 5, namely the one represented by $(3, 0, -15)$; Order IV consists of one class derived from an improper class with determinant 5, namely the one represented by $(6, 3, -6)$.

Example 2. The positive classes with determinant $-99 = -11.3^2$ are divided into four orders. Order I comprises the following properly primitive classes*): $(1, 0, 99)$, $(4, 1, 25)$. $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; Order II contains the improper classes $(2, 1, 50)$, $(10, 1, 10)$; Order III, the classes derived from proper classes with determinant -11, $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; Order IV, the single class derived from an improper class with determinant -11, $(6, 3, 18)$. — The negative classes with this determinant can be divided into orders in exactly the same way.

We note that *opposite classes always belong to the same order*; the reason for this theorem is easy to see.

*) For brevity, we use representative forms in place of the classes they represent.

227.

Among these different orders, the order of properly primitive classes especially deserves the closest attention. Each derived class comes from a certain primitive class (with a smaller determinant), and considering the latter usually gives what concerns the former directly. Below we will show that every improperly primitive class is, in a similar way, associated, so to speak, with either a single properly primitive class or three (with the same determinant). Further, for negative determinants we may pass over the negative classes, since a certain positive class always corresponds to each of them. To understand the nature of properly primitive classes more deeply, we will first explain a certain essential distinction by which the whole order of proper classes can be subdivided into several *genera*. Since we have not yet touched on this very important subject, we must take it up from the beginning.

Division of orders into genera.

228.

THEOREM. *Any properly primitive form F represents infinitely many numbers not divisible by any given prime p.*

Proof. If the form $F = axx + 2bxy + cyy$, clearly p cannot divide all three numbers a, $2b$, c at once. Now if a is not divisible by p, it is clear that taking for x any number not divisible by p, and for y a number divisible by p, makes the value of the form F not divisible by p. If c is not divisible by p, the same result follows by giving x a divisible value and y a nondivisible one. Finally, if both a and c are divisible by p, so that $2b$ is not, the form F takes a value not divisible by p when both x and y are given any values not divisible by p. *Q.E.D.*

The theorem clearly also holds for *improperly primitive* forms, provided $p = 2$ does not hold.

Since several conditions of this kind can hold at once, with the same number divisible by certain given primes and not divisible by others (see Article 32), it is easy to see that the numbers x, y can be chosen in infinitely many ways so that the primitive form $axx + 2bxy + cyy$ takes a value not divisible by any number of given primes. Only 2 must be excluded from those primes when the form is improperly primitive. Thus we can state the theorem more generally as follows: *Any primitive form represents infinitely many numbers relatively prime to any given number (which must be odd when the form is improperly primitive).*

229.

THEOREM. *Let F be a primitive form with determinant D, and p a prime dividing D. Then the numbers not divisible by p that can be represented by the form F agree in this respect: either they are all quadratic residues of p, or they are all nonresidues.*

Proof. Let $F = (a, b, c)$; let m, m' be any two numbers not divisible by p that can be represented by the form F, namely

$$m = agg + 2bgh + chh, \qquad m' = ag'g' + 2bg'h' + ch'h'$$

Then

$$mm' = (agg' + b(gh' + hg') + chh')^2 - D(gh' - hg')^2$$

so mm' is congruent to a square modulo D, and therefore also modulo p, *i.e.*, mm' is a quadratic residue of p. It follows that either both m, m' are quadratic residues of p, or both are nonresidues. *Q.E.D.*

Similarly, when the determinant D is divisible by 4, we prove that all odd numbers representable by F are either all $\equiv 1$. or all $\equiv 3$ (mod. 4). For in this case the product of two such numbers is always a quadratic residue of 4, and so $\equiv 1$ (mod. 4); hence either both are $\equiv 1$, or both $\equiv 3$.

Finally, when D is divisible by 8, the product of any two odd numbers representable by F is a quadratic residue of 8, and therefore $\equiv 1$ (mod. 8). Thus in this case the odd numbers representable by F are either all $\equiv 1$, or all $\equiv 3$, or all $\equiv 5$, or all $\equiv 7$ (mod. 8).

Thus, for *example*, since the form $(10, 3, 17)$ represents the number 10, which is a nonresidue of 7, all numbers not divisible by 7 that this form represents are nonresidues of 7. — Since -3 is representable by the form $(-3, 1, 49)$ and modulo 4 is $\equiv 1$, all odd numbers representable by this form behave in the same way.

If it were needed for our present purpose, we could easily prove that the numbers representable by the form F have no such fixed relation to any prime not dividing D: both residues and nonresidues of any prime not dividing D can be represented by the form F without distinction. For the numbers 4 and 8, on the other hand, something similar also holds in other cases, which we cannot pass over.

I. *When the determinant D of the primitive form F is $\equiv 3$ (mod. 4), the odd numbers representable by the form F are either all $\equiv 1$, or all $\equiv 3$ (mod. 4).* For if m, m' are two numbers representable by F, their product mm' can be put in the form $pp - Dqq$ as above. If both m, m' are odd, one of the numbers p, q must be even and the other odd, so one of the squares pp, qq is $\equiv 0$ and the other $\equiv 1$ (mod. 4). It follows easily that $pp - Dqq$ is certainly $\equiv 1$ (mod. 4), and so either both m, m' are $\equiv 1$, or both $\equiv 3$ (mod. 4). For *example*, the form $(10, 3, 17)$ cannot represent odd numbers other than those of the form $4n + 1$.

II. *When the determinant D of the primitive form F is $\equiv 2$ (mod. 8), the odd numbers representable by the form F are either partly $\equiv 1$ and partly $\equiv 7$, or partly $\equiv 3$ and partly $\equiv 5$ (mod. 8).* For let m, m' be two odd numbers representable by F, so that their product mm' can be put in the form $pp - Dqq$. Since both m, m' are odd, p must be odd (because D is even), and so $pp \equiv 1$ (mod. 8); but qq is either $\equiv 0$, $\equiv 1$, or $\equiv 4$, and therefore Dqq is either $\equiv 0$ or $\equiv 2$. Hence $mm' = pp - Dqq$ is either $\equiv 1$ or $\equiv 7$ (mod. 8). Thus if m is either $\equiv 1$ or $\equiv 7$, m' is also either $\equiv 1$ or $\equiv 7$; but if m is either $\equiv 3$ or $\equiv 5$, m' is also either $\equiv 3$ or $\equiv 5$. For *example*, all odd numbers representable by the form $(3, 1, 5)$ are either $\equiv 3$ or $\equiv 5$ (mod. 8), and no numbers of the form $8n + 1$ or $8n + 7$ can be represented by that form.

III. *When the determinant D of the primitive form F is $\equiv 6$ (mod. 8), this form can represent odd numbers only in the two cases $\equiv 1$ and $\equiv 3$ (mod. 8), or only in the two cases $\equiv 5$ and $\equiv 7$ (mod. 8).* Anyone can easily work out a proof entirely similar to the preceding one (in II). — Thus, for *example*, the only odd numbers representable by the form $(5, 1, 7)$ are those either $\equiv 5$ or $\equiv 7$ (mod. 8).

230.

Thus all numbers representable by a given primitive form F with determinant D have a fixed relation to each prime divisor of D (by which they themselves are not divisible). The odd numbers representable by F also have, in certain cases, a fixed relation to the numbers 4 and 8: namely to 4 whenever D is either $\equiv 0$ or $\equiv 3$ (mod. 4), and to 8 whenever D is either $\equiv 0$, $\equiv 2$, or $\equiv 6$ (mod. 8)[*)]. We call such a relation to each of these numbers a *character*, or an *individual character*, of the form F, and express it as follows. When only quadratic residues of the prime p can be represented by the form F, we assign it the character Rp, and in the opposite case the character Np. Similarly, we write $1, 4$ when the form F cannot represent any odd numbers except those that are $\equiv 1$ (mod. 4). This makes it immediately clear which characters the signs $3, 4$; $1, 8$; $3, 8$; $5, 8$; $7, 8$ express. Finally, to forms that represent only odd numbers that modulo 8 are either $\equiv 1$ or $\equiv 7$, we assign the character 1 *and* $7, 8$. The meaning of the characters 3 *and* $5, 8$; 1 *and* $3, 8$; 5 *and* $7, 8$ then follows by itself.

The individual characters of a given primitive form (a, b, c) with determinant D can always be found from at least one of the numbers a, c (both of which are clearly representable by that form). For whenever p is a prime divisor of D, at least one of the numbers a, c is certainly not divisible by p. If both were divisible by p, then p would also divide $bb(= D + ac)$. and therefore b as well; *i.e.*, the form (a, b, c) would not be primitive. Similarly, whenever the form (a, b, c) has a fixed relation to the number 4 or 8, at least one of the numbers a, c is certainly odd, and this determines that relation. For *example*, the character of the form $(7, 0, 23)$ with respect to the number 23 follows from the number 7 and is $N23$; the character of the same form with respect to 7 is obtained from the number 23, namely $R7$; finally, this form's character with respect to 4, namely $3, 4$, can be found from either 7 or 23.

Since all numbers representable by a form F in a class K are also representable by every other form of that class, each character of the form F clearly also belongs to all the other forms in this class. We may therefore regard them as characters of the whole class. Thus the individual characters of any given primitive class are found from its representative form. Opposite classes always have all their characters in common.

[*)] For determinants divisible by 8, the relation to the number 4 can be left out, since in this case it is already contained in the relation to 8.

231.

The collection of *all* individual characters of a given form or class makes up the complete character of that form or class. For *example*, the complete character of the form $(10, 3, 17)$, or of the whole class it represents, is $1, 4;\ N7;\ N23$. Similarly, the complete character of the form $(7, 1, -17)$ is $7, 8;\ R3;\ N5$, since the individual character $3, 4$ is left out in this case because it is already contained in the character $7, 8$. — On this basis we subdivide the whole order of properly primitive classes (positive ones when the determinant is negative) with a given determinant into several different *genera*: classes with the same complete character belong to the same genus, and classes with different complete characters to different genera. We assign each genus the complete character of the classes it contains. Thus, for *example*, for the determinant -161 there are sixteen positive properly primitive classes. They are divided into four genera as follows:

Character	Representative forms of the classes
$1, 4;\ R7;\ R23$	$(1, 0, 161)$, $(2, 1, 81)$, $(9, 1, 18)$, $(9, -1, 18)$
$1, 4;\ N7;\ N23$	$(5, 2, 33)$, $(5, -2, 33)$, $(10, 3, 17)$, $(10, -3, 17)$
$3, 4;\ R7;\ N23$	$(7, 0, 23)$, $(11, 2, 15)$, $(11, -2, 15)$, $(14, 7, 15)$
$3, 4;\ N7;\ R23$	$(3, 1, 54)$, $(3, -1, 54)$, $(6, 1, 27)$, $(6, -1, 27)$

For the number of different complete characters possible in principle, keep the following in mind.

I. When the determinant D is divisible by 8, four different individual characters are possible with respect to 8; the number 4 gives no separate character (note to the preceding article). In addition, each odd prime divisor of D gives two characters. So if there are m of these divisors, there are altogether 2^{m+2} different complete characters (setting $m = 0$ whenever D is a power of two).

II. When the determinant D is not divisible by 8, but is divisible by 4 and also by m odd primes, there are altogether 2^{m+1} different complete characters.

III. When the determinant D is even but not divisible by 4, it is either $\equiv 2 \pmod 8$ or $\equiv 6$. In the first case there are two individual characters with respect to 8, namely 1 *and* $7, 8$ and 3 *and* $5, 8$; in the second case there are just as many. Thus, setting the number of odd prime divisors of $D = m$, there are altogether 2^{m+1} different complete characters.

IV. When D is odd, it is either $\equiv 1$ or $\equiv 3 \pmod 4$. In the latter case there are two different characters with respect to 4, whereas in the former case no such relation enters the complete character. Thus, with m denoting the same thing as before, there are 2^m different complete characters in the former case and 2^{m+1} in the latter.

But we must take care to note that this by no means implies that as many genera actually exist as there are different characters possible in principle. In our example, only half of these actually correspond to classes or genera. There are no positive classes with the characters $1, 4;\ R7;\ N23$ or $1, 4;\ N7;\ R23$; or $3, 4;\ R7;\ R23$ or $3, 4;\ N7;\ N23$. We will discuss this very important subject more fully below.

From now on we call the form $(1, 0, -D)$, which is undoubtedly the simplest of all forms with determinant D, the *principal form*. The whole class containing it is called

the *principal class*, and the whole genus containing the principal class, the *principal genus*. We must therefore distinguish carefully between the principal form, a form in the principal class, and a form in the principal genus; likewise between the principal class and a class in the principal genus. We always use these names even if, for some determinant, there are no classes other than the principal class, or no genera other than the principal genus. This happens, for *example*, quite often when D is a positive prime of the form $4n + 1$.

232.

Although our discussion of the characters of forms was introduced primarily to subdivide the *positive properly primitive* order, nothing prevents us from applying the same ideas to negative forms and classes, or to improperly primitive ones. The positive improperly primitive order, the negative properly primitive order, and the negative improperly primitive order can all be subdivided into genera by the same principle. Thus, for *example*, after the properly primitive order of forms with determinant 145 has been divided into the following two genera,

$R5,\ R29$	$(1,0,-145),\ (5,0,-29)$
$N5,\ N29$	$(3,1,-48),\ (3,-1,-48)$

the improperly primitive order can likewise be divided into two genera:

$R5,\ R29$	$(4,1,-36),\ (4,-1,-36)$
$N5,\ N29$	$(2,1,-72),\ (10,5,-12)$

Or, just as the positive classes of forms with determinant -129 are divided into four genera,

$1,4;\ R3;\ R43$	$(1,0,129),\ (10,1,13),\ (10,-1,13)$
$1,4;\ N3;\ N43$	$(2,1,65),\ (5,1,26),\ (5,-1.\,26)$
$3,4;\ R3;\ N43$	$(3,0,43),\ (7,2,19),\ (7,-2,19)$
$3,4;\ N3;\ R43$	$(6,3,23),\ (11,5,14),\ (11,-5,14)$

the negative classes also fall into four orders:

$3,4;\ N3;\ N43$	$(-1,0,-129),\ (-10,1,-13),\ (-10,-1,-13)$
$3,4;\ R3;\ R43$	$(-2,1,-65),\ (-5,1,-26),\ (-5,-1,-26)$
$1,4;\ N3;\ R43$	$(-3,0,-43),\ (-7,2,-19),\ (-7,-2,-19)$
$1,4;\ R3;\ N43$	$(-6,3,-23),\ (-11,5,-14),\ (-11,-5,-14)$

But since the system of negative classes is always so similar to that of positive classes, it will usually seem unnecessary to construct it separately. Below we will show how to reduce the improperly primitive order to the properly primitive one.

Finally, no new rules are needed for subdividing derived orders. Every derived order comes from a primitive order (with a smaller determinant), and its individual classes correspond naturally to the individual classes of the latter. So the subdivision of the derived order can clearly be obtained from that of the primitive order.

233.

If a (primitive) form $F = (a, b, c)$ is such that two numbers g, h can be found with $gg \equiv a$, $gh \equiv b$, $hh \equiv c$ for a given modulus m, we will call this form a quadratic residue of the number m, and $gx + hy$ a value of the expression $\sqrt{}(axx + 2bxy + cyy)$(mod. m), or, more briefly, (g, h) a value of the expression $\sqrt{}(a, b, c)$ or $\sqrt{}F$(mod. m). More generally, if a multiplier M, relatively prime to the modulus m, is such that we can have

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \pmod{m}$$

we will call $M \times (a, b, c)$ or MF a quadratic residue of m, and (g, h) a value of the expression $\sqrt{}M(a, b, c)$ or $\sqrt{}MF$(mod. m). For *example*, the form $(3, 1, 54)$ is a quadratic residue of 23, and $(7, 10)$ is a value of the expression $\sqrt{}(3, 1, 54)$(mod. 23); similarly, $(2, -4)$ is a value of the expression $\sqrt{}5(10, 3, 17)$(mod. 23). We will show the use of these definitions below; here we note the following propositions:

I. If $M(a, b, c)$ is a quadratic residue of the number m, this number divides the determinant of the form (a, b, c). For if (g, h) is a value of the expression $\sqrt{}M(a, b, c)$ (mod. m), or

$$gg \equiv aM, \quad gh \equiv bM, \quad hh \equiv cM \pmod{m}$$

then $bbMM - acMM \equiv 0$, or $(bb - ac)MM$ is divisible by m. But since M is assumed relatively prime to m, $bb - ac$ is also divisible by m.

II. If $M(a, b, c)$ is a quadratic residue of m, and m is either a prime number or a power of a prime number, say $= p^\mu$, the individual character of the form (a, b, c) with respect to the number p is either Rp or Np, according as M is a residue or a nonresidue of p. This follows at once because both aM and cM are residues of m, or of p, and at least one of the numbers a, c is not divisible by p (Article 230).

Similarly, if (with the other conditions unchanged) $m = 4$, either $1, 4$ or $3, 4$ is the individual character of the form (a, b, c), according as $M \equiv 1$ or $\equiv 3$; a similar result holds for $m = 8$ or a higher power of the number 2. The individual character is $1, 8$; $3, 8$; $5, 8$; $7, 8$ for the form (a, b, c), according as $M \equiv 1$; 3; 5; 7 (mod. 8), respectively.

III. Conversely, if m is a prime number or a power of an odd prime number $= p^\mu$, dividing the determinant $bb - ac$, and M is either a residue or a nonresidue of p, according as the character of the form (a, b, c) with respect to p is Rp or Np, respectively, then $M(a, b, c)$ is a quadratic residue of m. For when a is not divisible by p, aM is a residue of p and therefore also of m; so if g is a value of the expression $\sqrt{}aM$ (mod. m), and h a value of the expression $\frac{bg}{a}$ (mod. m), we have $gg \equiv aM$; $ah \equiv bg$, and so

$$agh \equiv bgg \equiv abM \quad \text{and} \quad gh \equiv bM$$

and finally

$$ahh \equiv bgh \equiv bbM \equiv bbM - (bb - ac)M \equiv acM$$

and so $hh \equiv cM$, *i.e.*, (g, h) is a value of the expression $\sqrt{}M(a, b, c)$. But when a is divisible by m, c certainly is not; it is then easy to see that the same result follows

if we take for h a value of the expression $\sqrt{cM}$ (mod. m). For g we take a value of the expression $\frac{bh}{c}$ (mod. m).

Similarly, we prove that if we have $m = 4$ and this number divides $bb - ac$, and we take the number M either $\equiv 1$ or $\equiv 3$, according as $1, 4$ or $3, 4$ is the individual character of the form (a, b, c), then $M(a, b, c)$ is a quadratic residue of m. Likewise, if we have $m = 8$ or a higher power of 2, by which $bb - ac$ is divisible, and we take M to be $\equiv 1;\ 3;\ 5;\ 7$ (mod. 8), as the individual character of the form (a, b, c) with respect to the number 8 requires, then $M(a, b, c)$ is a quadratic residue of m.

IV. If the determinant of the form (a, b, c) is given by $= D$, and $M(a, b, c)$ is a quadratic residue of D, all the individual characters of the form (a, b, c), both with respect to each odd prime divisor of D and with respect to the number 4 or the number 8 (if they divide D), can be read off at once from the number M. For *example*, since $3(20, 10, 27)$ is a quadratic residue of 440, namely $(150, 9)$ is a value of the expression $\sqrt{3(20, 10, 27)}$ modulo 440, and $3N5$, $3R11$, the characters of the form $(20, 10, 27)$ are $3, 8;\ N5;\ R11$. Only the individual characters with respect to the numbers 4 and 8, whenever these do not divide the determinant, have no necessary connection with the number M

V. Conversely, if the number M, relatively prime to D, contains all the individual characters of the form (a, b, c) (except the characters with respect to the numbers $4, 8$, when these do not divide D), then $M(a, b, c)$ is a quadratic residue of D. For III shows that if D is put in the form $\pm A^\alpha B^\beta D^\gamma \ldots$, where A, B, C, etc. are distinct prime numbers, then $M(a, b, c)$ is a quadratic residue of each of A^α, B^β, C^γ, etc. So if a value of the expression $\sqrt{M(a, b, c)}$ modulo A^α is $(\mathfrak{A}, \mathfrak{A}')$; modulo B^β, $(\mathfrak{B}, \mathfrak{B}')$; modulo C^γ, $(\mathfrak{C}, \mathfrak{C}')$, etc., and the numbers g, h are determined so that $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc.; $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$, etc., for the moduli A^α, B^β, C^γ, etc., respectively (Article 32), we readily see that $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ for all the moduli A^α, B^β, C^γ, etc., and therefore also for the modulus D, which is their product.

VI. For these reasons, numbers such as M will be called *characteristic numbers* of the form (a, b, c). By V, several such numbers can be found without difficulty as soon as all the individual characters of this form are known; the simplest ones, however, are usually found most easily by trial. Clearly, if M is a characteristic number of a given primitive form with determinant D, all numbers congruent to M modulo D are characteristic numbers of the same form; forms in the same class, or even in different classes of the same genus, have the same characteristic numbers, so any characteristic number of a given form can also be assigned to the whole class and genus; finally, 1 is always a characteristic number of the principal form, class and genus, or every form of the principal genus is a residue of its own determinant.

VII. If (g, h) is a value of the expression $\sqrt{M(a, b, c)}$ (mod. m), and $g' \equiv g$, $h' \equiv h$ (mod. m), then (g', h') is also a value of the same expression. Such values can be regarded as *equivalent*; but if (g, h), (g', h') are values of the same expression $\sqrt{M(a, b, c)}$, and we do not have both $g' \equiv g$, $h' \equiv h$ (mod. m), they must be counted as *distinct*. Clearly, whenever (g, h) is a value of such an expression, $(-g, -h)$ is one too, and it is easy to prove that these values are always distinct unless $m = 2$. It is just as easy to prove that the expression $\sqrt{M(a, b, c)}$ (mod. m) cannot have more distinct values than two such (opposite) ones when m is either an odd prime number, a power

of an odd prime number, or $= 4$; but when m is $= 8$ or a higher power of the number 2, there are exactly four. From this, using VI, we easily deduce that if the determinant D of the form (a, b, c) is $= \pm 2^\mu A^\alpha B^\beta \ldots$, where A, B, etc. denote distinct odd prime numbers whose number is given by $= n$, and M is a characteristic number of this form, there are exactly 2^n, 2^{n+1} or 2^{n+2} distinct values of the expression $\sqrt{M}(a, b, c)$ (mod. D), according as μ is < 2, $= 2$ or > 2. For *example*, there are sixteen values of the expression $\sqrt{7}(12, 6, -17)$ (mod. 240), namely $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. We omit a fuller proof for brevity, since it is not particularly needed for what follows.

VIII. Finally, we observe that if two equivalent forms (a, b, c), (a', b', c') have determinant D and characteristic number M, and the first passes into the second by the substitution $\alpha, \beta, \gamma, \delta$, then any value of the expression $\sqrt{M}(a, b, c)$, such as (g, h), gives a value of the expression $\sqrt{M}(a', b', c')$, namely $(\alpha g + \gamma h, \beta g + \delta h)$. Anyone can work out the proof without difficulty.

Composition of forms.

234.

Having discussed the division of forms into classes, genera and orders, and explained the general properties that follow directly from these distinctions, we turn to another very important subject, which no one has yet considered: the *composition* of forms. At the start of this investigation, we insert the following lemma at once, so that we will not later have to interrupt the continuous sequence of proofs.

LEMMA. *Suppose we have four sequences of integers*

$$\begin{array}{ll} a, a', a'' \ldots a^n; & b, b', b'' \ldots b^n; \\ c, c', c'' \ldots c^n; & d, d', d'' \ldots d^n \end{array}$$

with equally many terms (say $n + 1$), such that

$$cd' - dc', \quad cd'' - dc'' \text{ etc.}, \quad c'd'' - d'c'' \text{ etc. etc.}$$

are respectively

$$= k(ab' - ba'), \quad k(ab'' - ba'') \text{ etc.}, \quad k(a'b'' - b'a'') \text{ etc. etc.}$$

or, in general,

$$c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$$

where k denotes a given integer; λ, μ are any two distinct integers between 0 and n inclusive, the larger being μ[*]*; suppose also that all the $a^\lambda b^\mu - b^\lambda a^\mu$ have no common divisor. Then four integers $\alpha, \beta, \gamma, \delta$ can be found such that*

$$\begin{array}{lll} \alpha a + \beta b = c, & \alpha a' + \beta b' = c', & \alpha a'' + \beta b'' = c'' \text{ etc.} \\ \gamma a + \delta b = d, & \gamma a' + \delta b' = d', & \gamma a'' + \delta b'' = d'' \text{ etc.} \end{array}$$

[*] We regard a as a^0, b as b^0, etc. — The same equation clearly also holds when $\lambda = \mu$ or $\lambda > \mu$.

or, in general,

$$\alpha a^\nu + \beta b^\nu = c^\nu, \quad \gamma a^\nu + \delta b^\nu = a^\nu$$

and then we have

$$\alpha\delta - \beta\gamma = k$$

Since by hypothesis the numbers $ab' - ba'$, $ab'' - ba''$, etc., $a'b'' - b'a''$, etc. (of which there are $= \frac{1}{2}(n+1)n$) have no common divisor, we can find as many other integers such that, when the former are multiplied by these respectively, the sum of the products is $= 1$ (Article 40). Denote these multipliers by $(0,1)$, $(0,2)$, etc., $(1,2)$, etc., or, in general, denote the multiplier of $a^\lambda b^\mu - b^\lambda a^\mu$ by (λ,μ), so that

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

(By the letter Σ we mean the sum of all values of the expression that follows it, obtained by giving λ, μ all distinct values between 0 and n, with $\mu > \lambda$). Now if we set

$$\Sigma(\lambda,\mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha, \quad \Sigma(\lambda,\mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta$$
$$\Sigma(\lambda,\mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma, \quad \Sigma(\lambda,\mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta$$

these $\alpha, \beta, \gamma.\delta$ have the required properties.

Proof. I. If ν denotes any integer between 0 and n, we have

$$\begin{aligned}
\alpha a^\nu + \beta b^\nu &= \Sigma(\lambda,\mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu) \\
&= \frac{1}{k}\Sigma(\lambda,\mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu) \\
&= \frac{1}{k}c^\nu\Sigma(\lambda,\mu)(c^\lambda d^\mu - d^\lambda c^\mu) \\
&= c^\nu\Sigma(\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu
\end{aligned}$$

And a similar calculation gives

$$\gamma a^\nu + \delta b^\nu = d^\nu. \qquad \textit{Q. E. P.}$$

II. Since we therefore have

$$c^\lambda = \alpha a^\lambda + \beta b^\lambda, \quad c^\mu = \alpha a^\mu + \beta b^\mu$$

we get

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$$

and similarly

$$a^\lambda c^\mu - c^\lambda a^\mu = \beta(a^\lambda b^\mu - b^\lambda a^\mu)$$
$$d^\lambda b^\mu - b^\lambda d^\mu = \gamma(a^\lambda b^\mu - b^\lambda a^\mu)$$
$$a^\lambda d^\mu - d^\lambda a^\mu = \delta(a^\lambda b^\mu - b^\lambda a^\mu)$$

From these formulas the values of $\alpha, \beta, \gamma, \delta$ can be found much more easily, provided we choose λ, μ so that $a^\lambda b^\mu - b^\lambda a^\mu$ is not $= 0$. This is certainly possible, because by hypothesis all the $a^\lambda b^\mu - b^\lambda a^\mu$ have no common divisor, and so they cannot *all* be

$= 0$. — From the same equations, multiplying the first by the fourth and the second by the third, and subtracting, we obtain

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$$

and so necessarily

$$\alpha\delta - \beta\gamma = k. \qquad \textit{Q. E. S.}$$

235.

If the form

$$AXX + 2BXY + CYY \ldots F$$

passes into the product of two forms

$$axx + 2bxy + cyy \ldots f, \quad \text{and} \quad a'x'x' + 2b'x'y' + c'y'y' \ldots f'$$

by a substitution of the kind

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

(which, for brevity, we will always express below as follows: If F passes into ff' by the substitution p, p', p'', p'''; q, q', q'', q'''*), we will simply say that the form F is *transformable* into ff'; if, in addition, this transformation is such that the six numbers

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''',$$
$$p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

have no common divisor, we will call the form F *composed* of the forms f, f'.

We begin this investigation with the most general assumption, that the form F passes into ff' by the substitution p, p', p'', p'''; q, q', q'', q''', and work out what follows from it. This assumption is clearly exactly equivalent to the following nine equations (*i.e.*, as soon as these equations hold, F passes into ff' by the stated substitution, and conversely):

$$App + 2Bpq + Cqq = aa' \quad \ldots \quad [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac' \quad \ldots \quad [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca' \quad \ldots \quad [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc' \quad \ldots \quad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \quad \ldots \quad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \quad \ldots \quad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \quad \ldots \quad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \quad \ldots \quad [8]$$
$$\begin{aligned} A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') \\ + C(qq''' + q'q'') \end{aligned} = 2bb' \quad \ldots \quad [9]$$

Let the determinants of the forms F, f, f' be D, d, d', respectively; let the greatest common divisors of the numbers $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ be M, m, m', respectively (all taken positively). Further, determine six integers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ so that

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \qquad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$$

*) In this notation, then, careful attention must be paid both to the order of the coefficients p, p', etc., and to that of the forms f, f'. It is easy to see that if the order of the forms f, f' is reversed, so that the first becomes the second, the coefficients p', q' must be exchanged with p'', q'', while each of the others stays in its place.

Finally, denote the numbers

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''',$$
$$p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

by P, Q, R, S, T, U, respectively, and let their greatest common divisor, taken positively, be $= k$. — Now, setting

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \quad \ldots . \qquad [10]$$

we obtain from equation 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \quad \ldots . \qquad [11]$$

From these eleven equations $1 \ldots 11$ we derive the following new ones[*]:

$$DPP = d'aa \quad \ldots\ldots\ldots\ldots . \qquad [12]$$
$$DP(R-S) = 2d'ab \quad \ldots\ldots\ldots\ldots . \qquad [13]$$
$$DPU = d'ac - (\Delta\Delta - dd') \quad \ldots\ldots . \qquad [14]$$
$$D(R-S)^2 = 4d'bb + 2(\Delta\Delta - dd') \quad \ldots\ldots . \qquad [15]$$
$$D(R-S)U = 2d'bc \quad \ldots\ldots\ldots\ldots . \qquad [16]$$
$$DUU = d'cc \quad \ldots\ldots\ldots\ldots . \qquad [17]$$
$$DQQ = da'a' \quad \ldots\ldots\ldots\ldots . \qquad [18]$$
$$DQ(R+S) = 2da'b' \quad \ldots\ldots\ldots\ldots . \qquad [19]$$
$$DQT = da'c' - (\Delta\Delta - dd') \quad \ldots\ldots . \qquad [20]$$
$$D(R+S)^2 = 4db'b' + 2(\Delta\Delta - dd') \quad \ldots\ldots . \qquad [21]$$
$$D(R+S)T = 2db'c' \quad \ldots\ldots\ldots\ldots . \qquad [22]$$
$$DTT = dc'c' \quad \ldots\ldots\ldots\ldots . \qquad [23]$$

From these we in turn deduce the following two:

$$0 = 2d'aa(\Delta\Delta - dd')$$
$$0 = (\Delta\Delta - dd')^2 - 2d'ac(\Delta\Delta - dd')$$

namely, the first from $12.15 - 13.13$, the second from $14.14 - 12.17$; from this it is easy to see that necessarily $\Delta\Delta - dd' = 0$, whether $a = 0$ or not $= 0$[*]. So we will suppose that in equations $14, 15, 20, 21$, $\Delta\Delta - dd'$ is removed from the right sides.

[*] These equations arise as follows: 12 from $5.5 - 1.2$; 13 from $5.9 - 1.7 - 2.6$; 14 from $10.11 - 6.7$; 15 from $5.8 + 5.8 + 10.10 + 11.11 - 1.4 - 2.3 - 6.7 - 6.7$; 16 from $8.9 - 3.7 - 4.6$; 17 from $8.8 - 3.4$. The other six are derived in the same way, if we exchange equations $2, 5, 7$ with equations $3, 6, 8$, respectively, and keep the remaining ones $1, 4, 9, 10, 11$ in the same positions throughout; thus 18 comes from $6.6 - 1.3$, etc.

[*] This derivation of the equation $\Delta\Delta = dd'$ is enough for our present purpose; otherwise we could give a more elegant analysis, but one too long for this place, by directly deriving from equations $1 \ldots 11$ the equation $0 = (\Delta\Delta - dd')^2$.

Now, setting

$$\mathfrak{A}P + \mathfrak{B}(R-S) + \mathfrak{C}U = mn'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R+S) + \mathfrak{C}'T = m'n$$

(where we must carefully note that n, n' can also be fractions, although $mn', m'n$ are necessarily integers), we readily deduce from equations 12 . . . 17

$$Dmmn'n' = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'mm$$

and similarly from equations 18 . . . 23

$$Dm'm'nn = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'm'$$

Thus $d = Dnn$, $d' = Dn'n'$, and we obtain the FIRST CONCLUSION: *The determinants of the forms F, f, f' necessarily have the ratios of squares to one another;* and the SECOND: *D always divides the numbers $dm'm', d'mm$.* So D, d, d' clearly have the same sign, and no form can be transformable into the product ff' if its determinant is greater than the greatest common divisor of the numbers $dm'm', d'mm$.

Multiply equations $12, 13, 14$ by $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, respectively; likewise multiply equations $13, 15, 16$, and $14, 16, 17$, by the same numbers; add each three products, and divide the sum by Dmn', replacing d' by $Dn'n'$. We then get

$$P = an', \quad R - S = 2bn', \quad U = cn'$$

Similarly, multiplying equations $18, 19, 20$, as well as $19, 21, 22$ and $20, 22, 23$, by $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$, respectively, we obtain

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n$$

This gives the THIRD CONCLUSION: *The numbers $a, 2b, c$ are proportional to the numbers $P, R-S, U$, and if their ratio to the latter is put as 1 to n', then n' is a square root of $\frac{d'}{D}$; similarly, the numbers $a', 2b', c'$ have the same ratio to $Q, R+S, T$, and if this is put as 1 to n, then n is a square root of $\frac{d}{D}$.*

The quantities n, n', however, may be either positive or negative square roots of $\frac{d}{D}, \frac{d'}{D}$. This gives us a distinction that may seem fruitless at first, but whose use will become clear enough below. Namely, in the transformation of the form F into ff', we will say that the form f is taken *directly* when n is positive, and *inversely* when n is negative; similarly, f' is taken directly or inversely according as n' is positive or negative. If we also require that k be $= 1$, the form F will be said to be composed *either* directly of both forms f, f', *or* inversely of both, *or* directly of f and inversely of f', *or* inversely of f and directly of f', according as n, n' are both positive, both negative, the first positive and the second negative, or the first negative and the second positive. Anyone will readily understand that these relations do not depend on the order in which the forms f, f' are placed (see the first note to this article).

We further observe that the greatest common divisor of the numbers P, Q, R, S, T, U, namely k, divides the numbers $mn', m'n$ (as is clear from the values established above), and so the square kk divides $mmn'n', m'm'nn$, and Dkk divides

$d'mm, dm'm'$. Conversely, every common divisor of $mn', m'n$ also divides k. For let e be such a divisor; it clearly also divides the numbers $an', 2bn', cn', a'n, 2b'n, c'n$, *i.e.*, the numbers $P, R-S, U, Q, R+S, T$, and therefore also $2R$ and $2S$. Now if $\frac{2R}{e}$ were odd, $\frac{2S}{e}$ would have to be odd too (since their sum and difference are even), and so their product would also be odd. But this product is $= \frac{4}{ee}(b'b'nn - bbn'n') = \frac{4}{ee}(d'nn + a'c'nn - dn'n' - acn'n') = \frac{4}{ee}(a'c'nn - acn'n')$ and is therefore even, since e divides $a'n, c'n, an', cn'$. So $\frac{2R}{e}$ is necessarily even, and therefore R, as well as S, is divisible by e. Since e thus divides all six numbers P, Q, R, S, T, U, it also divides their greatest common divisor k. *Q. E. D.* — We conclude that k is the greatest common divisor of the numbers $mn', m'n$; from this it is easy to see that *Dkk is the greatest common divisor of the numbers $dm'm', d'mm$.* This is the FOURTH CONCLUSION. So whenever F is composed of f and f', D is clearly the greatest common divisor of the numbers $dm'n', d'mm$, and conversely; this property could also have been adopted as the definition of a composed form. Thus a form composed of the forms f, f' has the greatest possible determinant among all forms transformable into the product ff'.

Before we can proceed further, we must first determine more precisely the value of Δ, which we have shown to be $= \sqrt{dd'} = \sqrt{DDnnn'n'}$, but whose *sign* has not yet been determined by this. For this purpose, from the fundamental equations 1—11 we derive $DPQ = \Delta aa'$ (this equation comes from $5.6 - 1.11$), and so $Daa'nn' = \Delta aa'$, from which, unless one of the numbers a, a' is $= 0$, we get $\Delta = Dnn'$. But in exactly the same way, eight other equations can be derived from the fundamental equations, in which Dnn' on the left and Δ on the right are multiplied by $2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc'$*). From this we easily conclude, since neither all of $a, 2b, c$ nor all of $a', 2b', c'$ can be $= 0$, that in all cases $\Delta = Dnn'$, and therefore Δ has the same sign as D, d, d', or the opposite sign, according as n, n' have the same or different signs.

We further observe that the numbers $aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc', 2bb' + 2\Delta, 2bb' - 2\Delta$ are all divisible by mm'. This is evident for the first nine; for the other two, it can be proved in the same way as we showed above that R and S are divisible by e. Namely, $4bb'+4\Delta$ and $4bb'-4\Delta$ are clearly divisible by mm' (since $4\Delta = \sqrt{16dd'}$, and $4d$ is divisible by mm, $4d'$ by $m'm'$, and therefore $16dd'$ by $mmm'm'$ and 4Δ by mm'), and the difference of the quotients is even; their product is easily shown to be even, so each quotient is even, and $2bb' + 2\Delta, 2bb' - 2\Delta$ are divisible by mm'.

The following six equations are now easily deduced from the eleven fundamental equations:

$$\begin{aligned}
APP &= aa'q'q' - 2ab'qq' + ac'qq \\
AQQ &= aa'q''q'' - 2ba'qq'' + ca'qq \\
ARR &= aa'q'''q''' - 2(bb' + \Delta)qq''' + cc'qq \\
ASS &= ac'q''q'' - 2(bb' - \Delta)q'q'' + ca'q'q' \\
ATT &= ac'q'''q''' - 2bc'q'q''' + cc'q'q' \\
AUU &= ca'q'''q''' - 2cb'q''q''' + cc'q''q''
\end{aligned}$$

It follows that all of APP, AQQ, etc. are divisible by mm', and from this, since

*) For brevity we must leave out the analysis, which readers can easily find for themselves.

kk is the greatest common divisor of the numbers PP, QQ, RR, etc., it is easy to deduce that Akk is also divisible by mm'. If we substitute for $a, 2b, c$, $a', 2b', c'$ their values $\frac{P}{n'}$, etc., or $\frac{1}{n'}(pq' - qp')$, etc., these become six other equations, in which the right sides are products of the quantity $\frac{1}{nn'}(q'q'' - qq''')$ with PP, QQ, RR, etc. We leave this very easy calculation to the readers. It follows (since not all of PP, QQ, etc. can be $= 0$) that $Ann' = q'q'' - qq'''$.

Similarly, six other equations are derived from the fundamental equations, differing from the previous ones only in that A is everywhere replaced by C, and q, q', q'', q''' by p, p', p'', p''', respectively. We do not write them down, for brevity. In the same way it follows that Ckk is divisible by mm' and that $Cnn' = p'p'' - pp'''$.

Finally, the same source gives these six equations:

$$\begin{aligned}
BPP &= -aa'p'q' + ab'(pq' + qp') - ac'pq \\
BQQ &= -aa'p''q'' + ba'(pq'' + qp'') - ca'pq \\
BRR &= -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq \\
BSS &= -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q' \\
BTT &= -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q' \\
BUU &= -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q''
\end{aligned}$$

from which we conclude, just as before, that $2Bkk$ is divisible by mm' and that $2Bnn' = pq''' + qp''' - p'q'' - q'p''$.

Since $Akk, 2Bkk, Ckk$ are therefore divisible by mm', we readily see that Mkk must also be divisible by mm'. But the fundamental equations show that M divides $aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc'$, and therefore also $am', 2bm', cm'$ (the greatest common divisors of the first, middle and last three, respectively); finally, it also divides mm', their greatest common divisor. So in the case where the form F is composed of the forms f, f', or $k = 1$, we necessarily have $M = mm'$. This is the FIFTH CONCLUSION.

If the greatest common divisor of the numbers A, B, C is $\mathfrak{M}$, it is either $= M$ (when the form F is properly primitive or derived from a properly primitive form) or $= \frac{1}{2}M$ (when F is improperly primitive or derived from an improperly primitive form); similarly, if we denote the greatest common divisors of the numbers a, b, c; a', b', c' by $\mathfrak{m}, \mathfrak{m}'$, respectively, then $\mathfrak{m}$ is either $= m$ or $\frac{1}{2}m$, and $\mathfrak{m}'$ either $= m'$ or $= \frac{1}{2}m'$. Now clearly $\mathfrak{m}\mathfrak{m}$ divides d', $\mathfrak{m}'\mathfrak{m}'$ divides d', and therefore $\mathfrak{m}\mathfrak{m}\mathfrak{m}'\mathfrak{m}'$ divides dd' or $\Delta\Delta$, and $\mathfrak{m}\mathfrak{m}'$ divides Δ. From the last six equations for BPP, etc. it then follows that $\mathfrak{m}\mathfrak{m}'$ divides Bkk and so (since it also divides Akk, Ckk) also $\mathfrak{M}kk$. Thus whenever F is composed of f, f', $\mathfrak{m}\mathfrak{m}'$ divides $\mathfrak{M}$. So when, in this case, both f, f' are properly primitive or derived from properly primitive forms, or $\mathfrak{m}\mathfrak{m}' = mm' = M$, we have $\mathfrak{M} = M$, or F is a similar form. But when, under the same assumption, either both f, f' or at least one of them is improperly primitive or derived from an improperly primitive form, for *example* the form f, the fundamental equations show that $aa', 2ab', ac', ba', 2bb', bc', ca', 2cb', cc'$ are divisible by $\mathfrak{M}$, and therefore also am', bm', cm', and consequently $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$ too. So in this case we necessarily have $\mathfrak{M} = \frac{1}{2}M$, or the form F is also improperly primitive or derived from an improperly primitive form. These give the SIXTH CONCLUSION.

Finally, we observe that if the nine equations

$$\begin{gathered} an' = P, \quad 2bn' = R - S, \quad cn' = U \\ a'n = Q, \quad 2b'n = R + S, \quad c'n = T \\ Ann' = q'q'' - qq''', \\ 2Bnn' = pq''' + qp''' - p'q'' - q'p'', \\ Cnn' = p'p'' - pp''' \end{gathered}$$

(which we will denote by Ω, since we will often need to return to them below) are *assumed* to hold, even treating n, n' as unknowns, but neither being $= 0$, substitution readily confirms that the fundamental equations $1 \ldots 9$ are necessarily true as well, or that the form (A, B, C) passes by the substitution p, p', p'', p'''; q, q', q'', q''' into the product of the forms $(a, b, c)(a', b', c')$; and also that

$$bb - ac = nn(BB - AC), \quad b'b' - a'c' = n'n'(BB - AC)$$

We leave to the readers' efforts the calculation, which would be too long to include here.

236.

PROBLEM. *Given two forms whose determinants are either equal or at least have the ratio of squares to one another, find a form composed of them.*

Solution. Let the forms to be composed be $(a,b,c)\dots f$, $(a',b',c')\dots f'$; let their determinants be d,d'; let the greatest common divisors of the numbers $a,2b,c$; $a',2b',c'$ be m,m', respectively; let the greatest common divisor of the numbers $dm'm', d'mm$, taken with the same sign as d,d', be D. Then $\frac{dm'm'}{D}, \frac{d'mm}{D}$ are positive, relatively prime numbers whose product is a square; so they are themselves squares (Article 21). Thus $\sqrt{\frac{d}{D}}, \sqrt{\frac{d'}{D}}$ are rational quantities, which we put $= n, n'$, taking for n the positive or negative value according as the form f is to enter the composition directly or inversely; similarly, we determine the sign of n' from the way in which f' is to enter the composition. Thus $mn', m'n$ are relatively prime integers; but n and n' may also be fractions. Having done this, we observe that $an', cn', a'n, c'n, bn'+b'n, bn'-b'n$ are integers. This is evident for the first four (since $an' = \frac{a}{m}mn'$, etc.); for the other two, it is proved in the same way as we proved in the preceding article that R and S are divisible by e.

Now take any four integers $\mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$, with only the condition that the four quantities on the left in the following equation (I) are not all $= 0$ at once, and put

$$\begin{aligned}
\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn'+b'n) &= \mu q \qquad \dots\dots \qquad \text{(I)}\\
-\mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}''(bn'-b'n) &= \mu q'\\
\mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn'-b'n) &= \mu q''\\
-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn'+b'n) &= \mu q'''
\end{aligned}$$

so that q, q', q'', q''' are integers with no common divisor. We achieve this by taking for μ the greatest common divisor of the four numbers on the left in these equations. Then, by Article 40, four integers $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ can be found such that

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

Now determine the numbers p, p', p'', p''' by the following equations:

$$\begin{aligned}
\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn'+b'n) &= p \qquad \dots\dots \qquad \text{(II)}\\
-\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn'-b'n) &= p'\\
\mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn'-b'n) &= p''\\
-\mathfrak{P}''cn' - \mathfrak{P}'c'n - \mathfrak{P}(bn'+b'n) &= p'''
\end{aligned}$$

Finally, put

$$\begin{aligned}
q'q'' - qq''' &= Ann',\\
pq''' + qp''' - p'q'' - q'p'' &= 2Bnn',\\
p'p'' - pp''' &= Cnn'
\end{aligned}$$

Then A, B, C are integers, and the form $(A,B,C)\dots F$ is composed of the forms f, f'.

Proof. I. From equations I, the following four equations are confirmed without difficulty:

$$\begin{aligned} 0 &= q'cn' - q''c'n - q'''(bn' - b'n) \qquad \ldots\ldots \qquad \text{(III)} \\ 0 &= qcn' + q'''a'n - q''(bn' + b'n) \\ 0 &= q'''an' + qc'n - q'(bn' + b'n) \\ 0 &= q''an' - q'a'n - q(bn' - b'n) \end{aligned}$$

II. Now suppose that the integers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \mathfrak{N}, \mathfrak{N}'$ have been determined so that

$$\begin{aligned} \mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m \\ \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m' \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1 \end{aligned}$$

Then we have

$$\begin{aligned} &\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' \\ &\qquad + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1 \end{aligned}$$

From this and equations (III), we readily confirm that if we put

$$\begin{aligned} -q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q} \\ q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}' \\ -q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'' \\ q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}''' \end{aligned}$$

we have

$$\begin{aligned} \mathfrak{q}'an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) &= q \qquad \ldots\ldots \qquad \text{(IV)} \\ -\mathfrak{q}an' + \mathfrak{q}'''c'n - \mathfrak{q}''(bn' - b'n) &= q' \\ \mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) &= q'' \\ -\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) &= q''' \end{aligned}$$

Whenever $\mu = 1$, these equations are unnecessary; in their place we can keep equations (I), to which they are entirely analogous. If we now work out from equations II, IV the values of $Ann', 2Bnn', Cnn'$ (*i.e.*, of the numbers $q'q'' - qq'''$, etc.), and remove the terms that cancel one another, we find that the terms of each are products of integers either with nn', with $dn'n'$, or with $d'nn$, and that all the terms making up $2Bnn'$ also contain the factor 2. From this (since $dn'n' = d'nn$, and so $\frac{dn'n'}{nn'} = \frac{d'nn}{nn'} = \sqrt{dd'}$ are integers) we conclude that A, B, C are integers. *Q. E. P.*

III. Substituting from equations (II) the values of p, p', p'', p''', we readily verify, with the help of equations (III) and of

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

that

$$\begin{aligned} pq' - qp' &= an', \\ pq''' - qp''' - p'q'' + q'p'' &= 2bn', \\ p''q''' - q''p''' &= cn' \\ pq'' - qp'' &= a'n, \\ pq''' - qp''' + p'q'' - q'p'' &= 2b'n, \\ p'q''' - q'p''' &= c'n \end{aligned}$$

These equations are identical to the first six (Ω) of the preceding article; the other three already hold by hypothesis. So (*at the end of the same article*) the form F passes into ff' by the substitution p, p', p'', p'''; $q, q', q''\, q'''$; its determinant is $= D$, or equal to the greatest common divisor of the numbers $dm'm', d'mm$, and therefore, by the fourth conclusion of the preceding article, F is composed of f, f'. *Q. E. S.* Finally, it is easy to see that F is composed of f, f' *in the way* required, since the signs of the quantities n, n' were determined correctly from the start.

237.

THEOREM. *If a form F is transformable into the product of two forms f, f', and the form f' contains the form f'', then F is also transformable into the product of the forms f, f''.*

Proof. Keep all the notation of Article 235 for the forms F, f, f'; let the form f'' be $= (a'', b'', c'')$, and let f' pass into f'' by the substitution $\alpha. \beta, \gamma, \delta$. Then it is easy to see that F passes into ff'' by the substitution

$$\begin{array}{cccc} \alpha p + \gamma p', & \beta p + \delta p', & \alpha p'' + \gamma p''', & \beta p'' + \delta p''' \\ \alpha q + \gamma q', & \beta q + \delta q', & \alpha q'' + \gamma q''', & \beta q'' + \delta q''' \end{array} \qquad \textit{Q. E. D.}$$

For brevity, put the coefficients

$$\begin{array}{c} \alpha p + \gamma p', \quad \beta p + \delta p' \text{ etc.} \\ = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \quad \mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}''' \end{array}$$

and the number $\alpha\delta - \beta\gamma = e$; from equations Ω of Article 235 we readily verify that

$$\begin{aligned} \mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' &= an'e \\ \mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' &= 2bn'e \\ \mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' &= cn'e \\ \mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' &= \alpha\alpha a'n + 2\alpha\gamma b'n + \gamma\gamma c'n = a''n \\ \mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2b''n \\ \mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' &= c''n \\ \mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' &= Ann'e \\ \mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2Bnn'e \\ \mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e \end{aligned}$$

Now, denoting the determinant of the form f'' by d'', we have that e is a square root of $\frac{d''}{d'}$, positive or negative according as the form f' contains the form f'' properly or improperly. So $n'e$ is a square root of $\frac{d''}{D}$. Thus the preceding nine equations are clearly entirely analogous to equations Ω of Article 235, and the form f is taken in the transformation of the form F into ff'' in the same way as in the transformation of the form F into ff'; but the form f'' is taken in the former either in the same way as f' in the latter, or in the opposite way, according as f' contains f'' properly or improperly.

238.

THEOREM. *If a form F is contained in a form F' and is transformable into the product of the forms f, f', then the form F' is also transformable into the same product.*

Proof. Keeping the same notation as above for the forms F, f, f', and supposing that the form F' passes into F by the substitution $\alpha, \beta, \gamma, \delta$, we readily see that F', by the substitution

$$\begin{array}{cccc} \alpha p + \beta q, & \alpha p' + \beta q', & \alpha p'' + \beta q'', & \alpha p''' + \beta q''' \\ \gamma p + \delta q, & \gamma p' + \delta q', & \gamma p'' + \delta q'', & \gamma p''' + \delta q''' \end{array}$$

becomes the same as F does by the substitution p, p', p'', p'''; q, q', q'', q''', and therefore F' passes into ff' by that substitution. *Q. E. D.*

Further, a calculation like the one in the preceding article readily confirms that F' is transformable into ff' in the same way as F, when F' contains F properly; but when F is improperly contained in F', the transformations of the form F into ff' and of the form F' into ff' are opposite with respect to each of the forms f, f': namely, whichever of these forms enters one transformation directly is taken inversely in the other.

Combining this theorem with the theorem of the preceding article gives the following more general one: *If a form F is transformable into the product ff', and the forms f, f' contain the forms g, g', respectively, while the form F is contained in the form G, then G is transformable into the product gg'.* For by the theorem of this article, G is transformable into ff', then by the theorem of the preceding article into fg', and by the same theorem also into gg'. Further, if all three forms f, f', G contain the forms g, g', F properly, then G is clearly transformable into gg' in the same way with respect to the forms g, g' as F into ff' with respect to the forms f, f'; the same happens if all three containments are improper. Finally, it is just as easy to determine *how* G is transformable into gg' if one of these containments differs from the other two.

If the forms F, f, f' are equivalent to the forms G, g, g', respectively, the latter have the same determinants as the former, and for the forms f, f', the numbers m, m' are the same for the forms g, g' (Article 161). From this, by the fourth conclusion of Article 235, we deduce without difficulty that in this case G is *composed* of g, g' if F is composed of f, f'. Also, the form g enters the former composition in the same way as f enters the latter, when F is equivalent to G in the same way as f to g, and conversely; similarly, g' is taken in the former composition in the same or the opposite way as f' in the latter, according as the equivalence of the forms f', g' is of the same or a different kind as the equivalence of the forms F, G.

239.

THEOREM. *If a form F is composed of the forms f, f', then every other form transformable into the product ff' in the same way as F contains F properly.*

Proof. Keeping all the notation of Article 235 for F, f, f', equations Ω hold here too. Suppose the form $F' = (A', B', C')$, whose determinant is $= D'$, passes into the product ff' by the substitution $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''$; $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \mathfrak{q}'''$, and denote the numbers

$$\begin{array}{ccc} \mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', & \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', & \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}'''. \\ \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', & \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', & \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''' \end{array}$$

by

$$P', Q', R', S', T', U'$$

respectively. Then we have nine equations entirely analogous to Ω, namely

$$\begin{gathered}
P' = a\mathfrak{n}', \quad R' - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}' \\
Q' = a'\mathfrak{n}, \quad R' + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n} \\
\mathfrak{q}'\mathfrak{q}'' - \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}', \\
\mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \\
\mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}'
\end{gathered}$$

which we will denote by Ω'. Here the quantities $\mathfrak{n}, \mathfrak{n}'$ are square roots of $\frac{d}{D'}, \frac{d'}{D'}$, taken with the same signs as n, n', respectively; so if the positive square root of $\frac{D}{D'}$ (which is an integer) is put $= k$, then $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. From this and the first six equations in Ω and Ω', we clearly have

$$\begin{gathered}
P' = kP, \quad Q' = kQ, \quad R' = kR \\
S' = kS, \quad T' = kT, \quad U' = kU
\end{gathered}$$

So by the lemma of Article 234, four integers $\alpha, \beta, \gamma, \delta$ can be determined such that

$$\begin{gathered}
\alpha p + \beta q = \mathfrak{p}. \qquad \gamma p + \delta q = \mathfrak{q} \\
\alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}' \text{ etc.}
\end{gathered}$$

and

$$\alpha\delta - \beta\gamma = k$$

Substituting these values of $\mathfrak{p}, \mathfrak{q}, \mathfrak{p}', \mathfrak{q}'$, etc. into the last three equations Ω', we readily verify, with the help of the equations $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ and the last three of Ω, that

$$\begin{gathered}
A'\alpha\alpha + 2B'\alpha\gamma + C'\gamma\gamma = A \\
A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B \\
A'\beta\beta + 2B'\beta\delta + C'\delta\delta = C
\end{gathered}$$

Thus the form F' passes by the substitution $\alpha, \beta, \gamma, \delta$ (which is proper, since $\alpha\delta - \beta\gamma = k$ is positive) into F, *i.e.*, it contains the form F properly. *Q. E. D.*

So if F' is also composed of the forms f, f' (in the same way as F is composed of them), the forms F, F' have the same determinant, and are therefore properly equivalent. More generally, if a form G is composed of the forms g, g' in the same way as F of f, f', respectively, and the forms g, g' are properly equivalent to f, f', then the forms F, G are properly equivalent.

Since the case in which both forms enter the composition directly is the simplest, and the others are easily reduced to it, we will consider only this case below. Thus whenever a form is simply said to be composed of two others, we must always understand that it is properly composed of each of them[*)]. The same restriction will apply whenever a form is said to be transformable into the product of two others.

[*)] Similarly, in the composition of ratios (which has a close analogy with the composition of forms), it is usually understood that the ratios to be composed are to be taken directly, unless the opposite is stated.

240.

THEOREM. *Suppose that from the forms f, f' the form F is composed; from F and f'' the form $\mathfrak{F}$; from f, f'' the form F'; and from F' and f' the form $\mathfrak{F}'$. Then the forms $\mathfrak{F}, \mathfrak{F}'$ are properly equivalent.*

Proof. I. Let

$$\begin{aligned} f &= axx + 2bxy + cyy \\ f' &= a'x'x' + 2b'x'y' + c'y'y' \\ f'' &= a''x''x'' + 2b''x''y'' + c''y''y'' \\ F &= AXX + 2BXY + CYY \\ F' &= A'X'X' + 2B'X'Y' + C'Y'Y' \\ \mathfrak{F} &= \mathfrak{A}\mathfrak{X}\mathfrak{X} + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}\mathfrak{Y} \\ \mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'\mathfrak{X}' + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'\mathfrak{Y}' \end{aligned}$$

and let the determinants of these seven forms be $d, d', d'', D, D', \mathfrak{D}, \mathfrak{D}'$, respectively. All have the same sign and the ratios of squares to one another. Further, let m be the greatest common divisor of the numbers $a, 2b, c$, and let m', m'', M have similar meanings for the forms $f', f''; F$. Then, by the fourth conclusion of Article 235, D is the greatest common divisor of the numbers $dm'm', d'mm$, and therefore $Dm''m''$ of the numbers $dm'm'm''m'', d'mmm''m''$; $M = mm'$; $\mathfrak{D}$ is the greatest common divisor of the numbers $Dm''m''$, $d''MM$, or of the numbers $Dm''m'', d''mmm'm'$. It follows that $\mathfrak{D}$ is the greatest common divisor of the three numbers $dm'm'm''m'', d'mmm''m'', d''mmm'm'$; but by a similar argument $\mathfrak{D}'$ is the greatest common divisor of the same three numbers. So, since $\mathfrak{D}, \mathfrak{D}'$ have the same sign, we have $\mathfrak{D} = \mathfrak{D}'$, or the forms $\mathfrak{F}, \mathfrak{F}'$ have the same determinant.

II. Now let F pass into ff' by the substitution

$$\begin{aligned} X &= pxx' + p'xy' + p''yx' + p'''yy' \\ Y &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned}$$

and $\mathfrak{F}$ into Ff'' by the substitution

$$\begin{aligned} \mathfrak{X} &= \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy'' \\ \mathfrak{Y} &= \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy'' \end{aligned}$$

and denote the positive square roots of $\frac{d}{D}, \frac{d'}{D}, \frac{D}{\mathfrak{D}}, \frac{d''}{\mathfrak{D}}$ by $n, n', \mathfrak{N}, \mathfrak{n}''$. Then, by Article 235, we have eighteen equations, half belonging to the transformation of the form F into ff', the other half to that of the form $\mathfrak{F}$ into Ff''. The first is $pq' - qp' = an'$; the others can easily be formed on its model, and we omit them here for brevity. The quantities $n, n', \mathfrak{N}, \mathfrak{n}''$, however, are rational, but not necessarily integers.

III. Substituting the values of X, Y into those of $\mathfrak{X}, \mathfrak{Y}$ gives a substitution of the following kind:

$$\begin{aligned} \mathfrak{X} = {} & (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' \\ & + (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y'' \\ \mathfrak{Y} = {} & (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' \\ & + (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y'' \end{aligned}$$

by which $\mathfrak{F}$ clearly passes into the product $ff'f''$. The coefficient (1) is $= p\mathfrak{p}+q\mathfrak{p}''$; we do not give the values of the other fifteen, since anyone can work them out without difficulty. Denote the number $(1)(10)-(2)(9)$ by $(1,2)$, the number $(1)(11)-(3)(9)$ by $(1,3)$, and, in general, $(g)(8+h)-(h)(8+g)$ by (g,h), supposing g,h to be distinct integers between 1 and 16, the larger being h*); in this way we have twenty-eight symbols in all. Now, denoting the positive square roots of $\frac{d}{\mathfrak{D}}, \frac{d'}{\mathfrak{D}}$ by $\mathfrak{n},\mathfrak{n}'$ (which are $= n\mathfrak{N}, n'\mathfrak{N}$), we derive the following 28 equations:

$$
\begin{aligned}
(1,2) &= aa'\mathfrak{n}'' \\
(1,3) &= aa''\mathfrak{n}' \\
(1,4) &= ab'\mathfrak{n}'' + ab''\mathfrak{n}' \\
(1,5) &= a'a''\mathfrak{n} \\
(1,6) &= a'b\mathfrak{n}'' + a'b''\mathfrak{n} \\
(1,7) &= a''b\mathfrak{n}' + a''b'\mathfrak{n} \\
(1,8) &= bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'', \\
(2,3) &= ab''\mathfrak{n}' - ab'\mathfrak{n}'' \\
(2,4) &= ac''\mathfrak{n}' \\
(2,5) &= a'b''\mathfrak{n} - a'b\mathfrak{n}'' \\
(2,6) &= a'c''\mathfrak{n} \\
(2,7) &= bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'', \\
(2,8) &= bc''\mathfrak{n}' + b'c''\mathfrak{n} \\
(3,4) &= ac'\mathfrak{n}'' \\
(3,5) &= a''b'\mathfrak{n} - a''b\mathfrak{n}' \\
(3,6) &= bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(3,7) &= a''c'\mathfrak{n} \\
(3,8) &= bc'\mathfrak{n}'' + b''c\mathfrak{n} \\
(4,5) &= b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(4,6) &= b'c''\mathfrak{n} - bc''\mathfrak{n}' \\
(4,7) &= b''c'\mathfrak{n} - bc'\mathfrak{n}'' \\
(4,8) &= c'c''\mathfrak{n} \\
(5,6) &= ca'\mathfrak{n}'' \\
(5,7) &= ca''\mathfrak{n}' \\
(5,8) &= b'c\mathfrak{n}'' + b''c\mathfrak{n}' \\
(6,7) &= b''c\mathfrak{n}' - b'c\mathfrak{n}'' \\
(6,8) &= cc''\mathfrak{n}' \\
(7,8) &= cc'\mathfrak{n}''
\end{aligned}
$$

*)The present meaning of these symbols must not be confused with the meaning they had in Article 234; for the numbers expressed by them *here* correspond exactly to those which, in Article 234, were multiplied by the numbers denoted *there* by similar symbols.

which we will denote by Φ, and nine others:

$$\begin{aligned}
(10)(11) - (9)(12) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(12) - (2)(11) - (3)(10) + (4)(9) &= 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(2)(3) - (1)(4) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
-(9)(16) + (10)(15) + (11)(14) - (12)(13) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(16) - (2)(15) - (3)(14) + (4)(13)\{ & \\
+(5)(12) - (6)(11) - (7)(10) + (8)(9)\} &= 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
-(1)(8) + (2)(7) + (3)(6) - (4)(5) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
(14)(15) - (13)(16) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(5)(16) - (6)(15) - (7)(14) + (8)(13) &= 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(6)(7) - (5)(8) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}
\end{aligned}$$

which we will denote by Ψ[*)].

IV. Deriving the origin of all these 37 equations would take too long. It will be enough to verify a few, on whose model the others can be proved without much difficulty.

1) We have

$$\begin{aligned}
(1,2) &= (1)(10) - (2)(9) \\
&= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp \\
&\quad + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' + \mathfrak{q}'\mathfrak{p}'')pq \\
&\quad + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq \\
&= \mathfrak{n}''(App + 2Bpq + Cqq) = \mathfrak{n}''aa'
\end{aligned}$$

which is the first equation.

2) We obtain

$$\begin{aligned}
(1,3) &= (1)(11) - (3)(9) \\
&= (\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'')(pq' - qp') \\
&= a''\mathfrak{N}an' = aa''\mathfrak{n}'
\end{aligned}$$

the second equation.

[*)] We should note that 18 other equations like these Ψ can be derived, with the factors a, $2b$, c on the right replaced by a', $2b'$, c'; a'', $2b''$, c''. But we omit them, since they are not needed for our purpose.

3) We have

$$\begin{aligned}(1,8) &= (1)(16) - (8)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp'''\\ &\quad + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''')pq'''\\ &\quad - (\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'')qp'''\\ &\quad + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq'''\\ &= \mathfrak{n}''(App''' + B(pq''' + qp''') + Cqq''')\\ &\quad + b''\mathfrak{N}(pq''' - qp''')\\ &= \mathfrak{n}''(bb' + \sqrt{}dd') + b''\mathfrak{N}(b'n + bn')^{*)}\\ &= \mathfrak{n}''bb' + \mathfrak{n}'bb'' + \mathfrak{n}b'b'' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''\end{aligned}$$

the eighth equation in Φ. We leave the remaining equations for the readers to verify.

V. It follows from equations Φ that the twenty-eight numbers $(1,2)$, $(1,3)$, etc. have no common divisor, as follows. First we observe that the twenty-seven products of three factors, whose first factor is either $\mathfrak{n}$, second one of the numbers a', $2b'$, c', and third one of the numbers a'', $2b''$, c''; or whose first is $\mathfrak{n}'$, second one of the numbers a, $2b$, c, and third one of the numbers a'', $2b''$, c''; or, finally, whose first is $\mathfrak{n}''$, second one of the numbers a, $2b$, c, and third one of the numbers a', $2b'$, c'—each of these twenty-seven products, by equations Φ, equals either one of the twenty-eight numbers $(1,2)$, $(1,3)$, etc., or a sum or difference of several of them (for *example*, $\mathfrak{n}a'a'' = (1,5)$, $2\mathfrak{n}a'b'' = (1,6) + (2,5)$, $4\mathfrak{n}b'b'' = (1,8) + (2,7) + (3,6) + (4,5)$, and so on). So if these numbers had a common divisor, it would necessarily divide all those products as well. From this, with the help of Article 40 and the method often used above, we readily deduce that the same divisor must also divide the numbers $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$, and therefore their squares, which are $\frac{dm'm'm''m''}{\mathfrak{D}}$, $\frac{d'mmm''m''}{\mathfrak{D}}$, $\frac{d''mmm'm'}{\mathfrak{D}}$, would be divisible by its square, *which is absurd*, since by I the greatest common divisor of the three numerators is $\mathfrak{D}$, and therefore the squares themselves can have no common divisor.

VI. All this concerns the transformation of the form $\mathfrak{F}$ into $ff'f''$, and was derived from the transformations of the form F into ff' and of the form $\mathfrak{F}$ into Ff''. But in exactly the same way, from the transformations of the form F' into ff'' and of the form $\mathfrak{F}'$ into $F'f'$, we derive a transformation of the form $\mathfrak{F}'$ into $ff'f''$ of the following kind:

$$\begin{aligned}\mathfrak{X}' &= (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \text{etc.}\\ \mathfrak{Y}' &= (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \text{etc.}\end{aligned}$$

(denoting all coefficients as in the transformation of the form $\mathfrak{F}$ into $ff'f''$, and adding a prime to each to distinguish them). From this, as before, we derive 28 equations analogous to Φ, which we will denote by Φ', and nine others analogous to Ψ, which we will denote by Ψ'. Namely, denoting

$$(1)'(10)' - (2)'(9)' \text{ by } (1,2)', \quad (1)'(11)' - (3)'(9)' \text{ by } (1,3)'$$

*)This follows from equation 10 of Article 235 and what follows it. The radical quantity $\sqrt{}dd'$ becomes $= Dnn' = \mathfrak{D}nn'\mathfrak{M}\mathfrak{M} = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

the equations Φ' are

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

and the equations Ψ' are

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

(For brevity we leave the fuller working to the readers; those familiar with the subject will find that a new calculation is not even necessary, and that the first analysis is easily carried over by analogy.) With this done, from Φ and Φ' we immediately have

$$(1,2) = (1,2)', \quad (1,3) = (1,3)', \quad (1,4) = (1,4)', \quad (2,3) = (2,3)', \quad \text{etc.}$$

From this, and because all of $(1,2)$, $(1,3)$, $(2,3)$, etc. have no common divisor (by V), the lemma of Article 234 shows that four integers α, β, γ, δ can be determined such that

$$\begin{aligned}
\alpha(1)' + \beta(9)' &= (1), \\
\alpha(2)' + \beta(10)' &= (2), \\
\alpha(3)' + \beta(11)' &= (3), \quad \text{etc.} \\
\gamma(1)' + \delta(9)' &= (9), \\
\gamma(2)' + \delta(10)' &= (10), \\
\gamma(3)' + \delta(11)' &= (11), \quad \text{etc.}
\end{aligned}$$

and $\alpha\delta - \beta\gamma = 1$.

VII. From this, substituting from the first three equations Ψ the values of $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$, and from the first three equations Ψ' the values of $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$, we readily verify that

$$\begin{aligned}
a(\mathfrak{A}\alpha\alpha + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma\gamma) &= a\mathfrak{A}' \\
a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}' \\
a(\mathfrak{A}\beta\beta + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta\delta) &= a\mathfrak{C}'
\end{aligned}$$

Unless $a = 0$, it clearly follows that the form $\mathfrak{F}$ passes into $\mathfrak{F}'$ by the proper substitution α, β, γ, δ. — But using the next three equations in place of the first three in Ψ and Ψ', we readily verify three equations entirely analogous to those just given, with the factor a everywhere replaced by b. So the same conclusion clearly still holds, provided we do not have $b = 0$. Finally, using the last three equations Ψ, Ψ', we find in the same way that the conclusion is true unless $c = 0$. Therefore, since certainly not all of a, b, c can be $= 0$ at once, the form $\mathfrak{F}$ necessarily passes by the substitution α, β, γ, δ into $\mathfrak{F}'$, and so is properly equivalent to this form. *Q. E. D.*

241.

We will call a form such as $\mathfrak{F}$ or $\mathfrak{F}'$, obtained by composing one of three given forms with the form composed of the other two, *composed of these three forms*. The preceding article shows that the order in which the three forms are composed makes no difference. Similarly, given any number of forms f, f', f'', f''', etc. (whose determinants must have the ratios of squares to one another), if we compose the form f with f', the resulting form with f'', the next result with f''', etc., the form obtained at the end of this operation is said to be composed *of all the forms* f, f', f'', f''', etc. It is easy to prove that here too the order of composition is arbitrary; *i.e.*, whatever the order in which these forms are composed, the forms resulting from the composition are always properly equivalent. — Further, if the forms f, f', f'', etc. are properly equivalent to the forms g, g', g'', etc., respectively, then the form composed of the latter is clearly properly equivalent to that composed of the former.

242.

The preceding propositions cover the composition of forms in its full generality. We now move on to more particular applications, with which we did not want to interrupt their sequence. First we return to the problem of Article 236, restricting it by the following conditions: *first*, the forms to be composed have the same determinant, that is, $d = d'$; *second*, m. m' are coprime; *third*, the required form is composed directly from each of f, f'. Then mm, $m'm'$ are also coprime, so the greatest common divisor of $dm'm'$, $d'mm$, *that is,* D, becomes $= d = d'$, and $n = n' = 1$. We set the four quantities $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, which can be chosen at will, equal to $= -1$, 0, 0, 0 respectively. This is always allowed except in the single case where a, a', $b+b'$ are all $= 0$, which we therefore leave aside here. Clearly this case can occur only for forms whose determinant is a positive square. It is then clear that μ becomes the greatest common divisor of a, a', $b + b'$; the numbers $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ must be chosen so that

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$$

while $\mathfrak{P}$ itself is entirely arbitrary. Substituting their values for p, q, p', q' etc. in the cited passage gives

$$A = \frac{aa'}{\mu\mu},$$
$$B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

and C can be determined from the equation $AC = BB - D$, unless a is zero and $a' = 0$ also holds.

In this solution, then, the value of A does not depend on the values of $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (which can be determined in infinitely many different ways). But B takes different values when these numbers are assigned different values, and it is worth investigating how all the values of B are connected. To this end we observe:

I. However $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ are determined, the resulting values of B are all congruent modulo A. Suppose that setting

$$\mathfrak{P} = \mathfrak{p},$$
$$\mathfrak{P}' = \mathfrak{p}',$$
$$\mathfrak{P}'' = \mathfrak{p}'',$$
$$\mathfrak{P}''' = \mathfrak{p}''',$$
$$\text{gives } B = \mathfrak{B}$$

but setting

$$\mathfrak{P} = \mathfrak{p} + \mathfrak{d},$$
$$\mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}',$$
$$\mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}''.$$
$$\mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}''',$$
$$\text{gives } B = \mathfrak{B} + \mathfrak{D}$$

Then

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0,$$
$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb'+D)\mathfrak{d}''' = \mu\mathfrak{D}$$

Multiply the first side of the latter equation by $a\mathfrak{p}' + a'\mathfrak{p}'' + (b+b')\mathfrak{p}'''$, the second by μ, and subtract from the first product the quantity

$$(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (bb'+D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''')$$

which, by the former equation, is clearly $= 0$. Expanding and cancelling the terms that cancel each other gives

$$\begin{aligned} aa'(&\mu\mathfrak{d} \\ &+ ((b'-b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' \\ &+ ((b-b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' \\ &- (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}''') = \mu\mu\mathfrak{D} \end{aligned}$$

so clearly $\mu\mu\mathfrak{D}$ is divisible by aa', or $\mathfrak{D}$ by $\frac{aa'}{\mu\mu}$, *that is,* by A, and

$$\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D} \pmod{A}$$

II. If the values $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ $\mathfrak{p}'''$ of $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ give $B = \mathfrak{B}$, other values of these numbers can be found that give B any specified value congruent to $\mathfrak{B}$ modulo A, say $\mathfrak{B} + kA$. First we observe that the four numbers μ, c, c', $b-b'$ cannot have a common divisor. For if they had one, it would divide the six numbers a, a', $b+b'$, c, c', $b-b'$, and therefore both a, $2b$, c and a', $2b'$, c', and consequently also m, m', which are coprime by hypothesis. We can therefore assign four integers h, h', h'', h''' so that

$$h\mu + h'c + h''c' + h'''(b-b') = 1$$

Having done this, if we set

$$\begin{aligned} kh &= \mathfrak{d}, \\ k(h''(b+b') - h'''a') &= \mu\mathfrak{d}' \\ k(h'(b+b') + h'''a) &= \mu\mathfrak{d}'', \\ -k(h'a' + h''a) &= \mu\mathfrak{d}''' \end{aligned}$$

it is clear that $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$, $\mathfrak{d}'''$ are integers. Further, we easily confirm that

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0$$

$$\begin{aligned} aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb'+D)\mathfrak{d}''' &\\ = \frac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b-b')h''') &\\ = \mu kA & \end{aligned}$$

The former equation shows that $\mathfrak{p}+\mathfrak{d}$, $\mathfrak{p}'+\mathfrak{d}'$, $\mathfrak{p}''+\mathfrak{d}''$, $\mathfrak{p}'''+\mathfrak{d}'''$ are also values of $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$; the latter shows that these values produce $B = \mathfrak{B} + kA$. *Q. E. D.* — It is clear from this that B can always be determined so that it lies between 0 and $A-1$ inclusive if A is positive, or between 0 and $-A-1$ if A is negative.

243.

From the equations

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b+b') = \mu,$$
$$B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb'+D))$$

we obtain

$$B = b + \frac{a}{\mu}(\mathfrak{P}a' + \mathfrak{P}'(b'-b) - \mathfrak{P}'''c)$$
$$= b' + \frac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b-b') - \mathfrak{P}'''c')$$

so

$$B \equiv b \text{ (mod. } \tfrac{a}{\mu}) \quad \text{and} \quad B \equiv b' \text{ (mod. } \tfrac{a'}{\mu})$$

Whenever $\frac{a}{\mu}$, $\frac{a'}{\mu}$ are coprime, there is only one number between 0 and $A-1$ (or between 0 and $-A-1$ when A is negative) that modulo $\frac{a}{\mu}$ is $\equiv b$, and is $\equiv b'$ modulo $\frac{a'}{\mu}$. If we set this number $= B$ and $\frac{BB-D}{A} = C$, it is clear that (A,B,C) is composed from the forms (a,b,c), (a',b',c'). In this case, then, to find the composite form we no longer need to consider the numbers $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$*). Thus, *for example,* if we seek a form composed from $(10,3,11)$, $(15,2,7)$, then a, a', $b+b'$ are respectively $= 10, 15, 5$; $\mu = 5$; so $A = 6$; $B \equiv 3$ (mod. 2) and $\equiv 2$ (mod. 3), giving $B = 5$ and $(6,5,21)$ as the required form. — The condition that $\frac{a}{\mu}$, $\frac{a'}{\mu}$ are coprime is entirely equivalent to the condition that the two numbers a, a' have no greater common divisor than the three a, a', $b+b'$; or, what comes to the same thing, that the greatest common divisor of a, a' also divides $b+b'$. The following particular cases should especially be noted:

1) Given two forms (a,b,c), (a',b',c') of the same determinant D, such that the greatest common divisor of a, $2b$, c is coprime to the greatest common divisor of a', $2b'$, c', and a is coprime to a', the form (A,B,C) composed from them is found by setting $A = aa'$, $B \equiv b$ (mod. a) and $\equiv b'$ (mod. a'), $C = \frac{BB-D}{A}$. This case always applies when one of the forms to be composed is the principal form, say $a = 1$, $b = 0$, $c = -D$. Then $A = a'$, and B can be set $= b'$, giving $C = c'$; so *the form composed from the principal form and any other form of the same determinant is that other form itself.*

2) If two *opposite*, properly primitive forms, say (a,b,c) and $(a,-b,c)$, are to be composed, then $\mu = a$. It is easy to see from this that the principal form $(1,0,-D)$ is composed from them.

3) Given any number of properly primitive forms (a,b,c), (a',b',c'), (a'',b'',c'') etc. of the same determinant D, whose leading coefficients a, a', a'' etc. are pairwise coprime, the form (A,B,C) composed from all of them is found. Set A equal to the product of all a, a', a'' etc.; B congruent to b, b', b'' etc. modulo a, a', a'' etc.

*) This can always be done by using the congruences

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b+b')B}{\mu} \equiv \frac{bb'+D}{\mu} \text{ (mod. } A)$$

respectively; $C = \frac{BB-D}{A}$. For it is easy to see that from the two forms (a, b, c), (a', b', c') the form $(aa', B, \frac{BB-D}{aa'})$ is composed; from this and (a'', b'', c'') the form $(aa'a'', B, \frac{BB-D}{aa'a''})$ etc. — Conversely:

4) Given a properly primitive form (A, B, C) of determinant D, resolve the coefficient A into any number of pairwise coprime factors a, a', a'' etc.; choose numbers b, b', b'' etc. equal to B, or at least congruent to it modulo a, a', a'' etc. respectively, and set $ac = bb - D$, $a'c' = b'b' - D$, $a''c'' = b''b'' - D$ etc. Then the form (A, B, C) is composed from the forms (a, b, c), $(a'\ b'\ c')$, $(a''\ b''\ c'')$, or is *resolvable into these forms*. It is proved without difficulty that the same proposition still holds even if the form (A, B, C) is improperly primitive or derived. In this way, then, any form can be resolved into others of the same determinant whose leading coefficients are all either primes or powers of primes. Such a resolution can often be usefully applied when one form is to be composed from several given forms. Thus, *for example,* if we seek the form composed from $(3, 1, 134)$, $(10, 3, 41)$, $(15, 2, 27)$, resolve the second into $(2, 1, 201)$, $(5, -2, 81)$, and the third into $(3, -1, 134)$, $(5, 2, 81)$. Clearly the form composed from the five forms $(3, 1, 134)$, $(2, 1, 201)$, $(5, -2, 81)$, $(3, -1, 134)$, $(5, 2, 81)$, in whatever order they are taken, is also composed from the three given forms. But composing the first with the fourth gives the principal form $(1, 0, 401)$; composing the third with the fifth gives the same form; so composing all of them gives the form $(2, 1, 201)$.

5) Since the method is useful, it is worth explaining it further. The preceding observation shows that the problem of composing any number of given properly primitive forms of the same determinant can be reduced to composing forms whose leading coefficients are powers of primes (for a prime can be regarded as the first power of itself). We should therefore consider especially the case where two properly primitive forms (a, b, c), (a', b', c') are to be composed, in which a and a' are powers of the *same* prime. Let $a = h^{\varkappa}$, $a' = h^{\lambda}$, where h denotes a prime, and suppose, as we may, that $\varkappa$ is not less than λ. Then h^{λ} is the greatest common divisor of a, a'. If it also divides $b + b'$, we have the case considered at the beginning of this article, and (A, B, C) is composed from the given forms if we set $A = h^{\varkappa-\lambda}$, $B \equiv b$ (mod. $h^{\varkappa-\lambda}$) and $\equiv b'$ (mod. 1), where the latter condition can clearly be omitted; $C = \frac{BB-D}{A}$. But if h^{λ} does not divide $b + b'$, the greatest common divisor of these numbers must itself be a power of h. Let it be $= h^{\nu}$; then $\nu < \lambda$ (we must set $\nu = 0$. if h^{λ} and $b + b'$ happen to be coprime). If, then, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ are determined so that

$$\mathfrak{P}'h^{\varkappa} + \mathfrak{P}''h^{\lambda} + \mathfrak{P}'''(b + b') = h^{\nu}$$

while $\mathfrak{P}$ is chosen at will, the form (A, B, C) is composed from the given forms if we set

$$A = h^{\varkappa+\lambda-2\nu},$$
$$B = b + h^{\varkappa-\nu}(\mathfrak{P}h^{\lambda} - \mathfrak{P}'(b - b') - \mathfrak{P}'''c),$$
$$C = \frac{BB - D}{A}$$

But it is easy to see that in this case $\mathfrak{P}'$ can also be chosen at will. So setting $\mathfrak{P} = \mathfrak{P}' = 0$ gives

$$B = b - \mathfrak{P}'''ch^{\varkappa-\nu}$$

or, in general,

$$B = kA + b - \mathfrak{P}''' ch^{\varkappa-\nu}$$

where k denotes an arbitrary number (preceding article). Only $\mathfrak{P}'''$ enters this very simple formula; it is a value of the expression $\frac{h^\nu}{b+b'}$ (mod. h^λ)*). If, *for example,* we seek the form composed from $(16, 3, 19)$ and $(8, 1, 37)$, then $h = 2$, $\varkappa = 4$, $\lambda = 3$, $\nu = 2$. So $A = 8$, and $\mathfrak{P}'''$ is a value of the expression $\frac{4}{4}$ (mod. 8), such as 1, giving $B = 8k - 73$. Thus, setting $k = 9$ gives $B = -1$ and $C = 37$, or $(8, -1, 37)$ as the required form.

Given, then, any number of forms whose leading coefficients are all powers of primes, we must check whether some of their leading coefficients are powers of the *same* prime and compose these with each other using the rule just given. This produces forms whose leading coefficients are still powers of primes, but of entirely different primes; the form composed from them can therefore be determined by the third observation. *For example,* given the forms $(3, 1, 47)$, $(4, 0, 35)$, $(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$, $(16, 6, 11)$, the first and fifth give the form $(27, 7, 7)$; the second and fourth give $(16, -6, 11)$, and this and the sixth give $(1, 0, 140)$, which can be left out. This leaves $(5, 0, 28)$, $(27, 7, 7)$, which produce $(135, -20, 4)$; in its place we can take the properly equivalent $(4, 0, 35)$. This, then, is the result of composing the six given forms.

Other useful practical methods can also be drawn from this source. But to avoid going on too long, we leave out a fuller treatment of this matter and move on to more difficult things.

*) or of the expression $\frac{1}{\frac{b+b'}{h^\nu}}$ (mod. $h^{\lambda-\nu}$), giving $B \equiv b - \frac{ch^{\varkappa-\nu}}{\frac{b+b'}{h^\nu}} \equiv \frac{(D+bb'):h^\nu}{(b+b'):h^\nu}$ (mod. A)

244.

If a form f can represent the number a, a form f' the number a', and the form F can be transformed into ff', it is easy to see that the product aa' can be represented by the form F. It follows at once that, when the determinants of these forms are negative, the form F is positive if f, f' are both positive or both negative; by contrast, F is negative if one of the forms f, f' is positive and the other negative. Let us focus especially on the case considered in the preceding article, where F is composed from f, f'. Also, f, f' and F have the same determinant D. Suppose further that the representations of the numbers a, a' by the forms f, f' use coprime values of the indeterminates, and that the former belongs to the value b of the expression $\sqrt{D}$ (mod. a), the latter to the value b' of the expression $\sqrt{D}$ (mod. a'), and set $bb - D = ac$, $b'b' - D = a'c'$. Then, by Article 168, the forms (a, b, c), (a', b', c') are properly equivalent to the forms f, f', so F is also composed from those two forms. But the form (A, B, C) is composed from the same forms if, denoting the greatest common divisor of a, a', $b + b'$ by $= \mu$, we set $A = \frac{aa'}{\mu\mu}$, $B \equiv b$ and b' modulo $\frac{a}{\mu}$, $\frac{a'}{\mu}$. respectively, $AC = BB - D$; so this form is properly equivalent to the form F. Now the form $Axx + 2Bxy + Cyy$ represents the number aa' on setting $x = \mu$, $y = 0$, the greatest common divisor of these values being μ. Thus aa' can also be represented by the form F so that the values of the indeterminates have greatest common divisor μ (Article 166). Whenever $\mu = 1$, therefore, aa' can be represented by the form F by assigning coprime values to the indeterminates, and this representation belongs to the value B of the expression $\sqrt{D}$ (modulo aa') that is congruent to b, b' modulo a, a' respectively. The condition $\mu = 1$ always holds when a, a' are coprime; more generally, when the greatest common divisor of a, a' is coprime to $b + b'$.

Composition of orders.

245.

THEOREM. *If the form f belongs to the same order as g, and likewise f' to the same order as g', the form F composed from f, f' has the same determinant and belongs to the same order as the form G composed from g, g'.*

Proof. Let the forms be $f, f', F = (a, b, c)$, (a', b', c'), (A, B, C) respectively, and their determinants $= d, d', D$. Further, let the greatest common divisor of $a, 2b, c$ be $= m$, and the greatest common divisor of a, b, c be $= \mathfrak{m}$; let m', $\mathfrak{m}'$ have similar meanings for the form f', and M, $\mathfrak{M}$ for the form F. Then the order of the form f is determined by the numbers $d, m, \mathfrak{m}$, so the same numbers also apply to the form g. Likewise, the numbers $d', m', \mathfrak{m}'$ are the same for the form g' as for the form f'. Now, by Article 235, the numbers $D, M, \mathfrak{M}$ are determined by $d, d', m, m', \mathfrak{m}, \mathfrak{m}'$: namely, D is the greatest common divisor of $dm'm'$, $d'mm$; $M = mm'$; and $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (if both $m = \mathfrak{m}$, $m' = \mathfrak{m}'$) or $= 2\mathfrak{m}\mathfrak{m}'$ (if $m = 2\mathfrak{m}$ or $m' = 2\mathfrak{m}'$). These properties of $D, M, \mathfrak{M}$ follow from the fact that F is composed from f, f', so it is easy to see that D, M and $\mathfrak{M}$ also apply to the form G, and therefore G belongs to the same order as F. *Q. E. D.*

For this reason, we call the order containing the form F composed from the orders containing the forms f, f'. Thus, *for example,* two properly primitive orders always

give an order of the same kind; a properly primitive and an improperly primitive order give an improperly primitive order. — A similar meaning is intended when an order is said to be composed from several other orders.

Composition of genera.

246.

PROBLEM. *Given any two primitive forms f, f', whose composition gives F, determine from the genera to which f, f' belong the genus to which F belongs.*

Solution. I. First consider the case where at least one of the forms f, f', say the first, is properly primitive, and denote the determinants of the forms f, f', F by d, d', D. Then D is the greatest common divisor of $dm'm'$, d', where m' is either 1 or 2, according as the form f' is properly or improperly primitive; F belongs to the properly primitive order in the former case and to the improperly primitive order in the latter. Now the genus of the form F is determined by its individual characters, with respect both to each odd prime divisor of D and, in certain cases, to the numbers 4 or 8. We must therefore determine each of these.

1°. If p is any odd prime divisor of D, it must also divide d, d', so the relations of the forms f, f' to p also occur among their characters. Now if f can represent the number a, and f' the number a', the product aa' can be represented by F. So if both f and f' can represent quadratic residues modulo p (not divisible by p), F can also represent quadratic residues modulo p; *that is,* if both f, f' have the character Rp, the form F has the same character. Likewise F has the character Rp if both f, f' have the character Np; by contrast, F has the character Np if one of the forms f, f' has Rp and the other Np.

2°. If the complete character of the form F includes a relation to the number 4, such a relation must also occur among the characters of the forms f, f'. For this happens only when D is $\equiv 0$ or $\equiv 3$ (modulo 4). When D is divisible by 4, both $dm'm'$ and d' are also divisible by 4. It follows at once that f' cannot be improperly primitive, and therefore $m' = 1$; thus both d and d' are divisible by 4, and the character of each includes a relation to 4. When $D \equiv 3$ (modulo 4), D divides d, d'; the quotients are squares, so d, d' must also be either $\equiv 0$ or $\equiv 3$ (modulo 4), and among the characters of f, f' a relation to 4 occurs. It follows, just as in (1°), that the form F has the character $1, 4$ if either both f, f' have $1, 4$ or both have $3, 4$; by contrast, the form F has the character $3, 4$ if one of the forms f, f' has $1, 4$ and the other $3, 4$.

3°. When D is divisible by 8, d' is too; so f' is certainly properly primitive, $m' = 1$, and d is also divisible by 8. Thus among the characters of the form F, one of the characters $1, 8$; $3, 8$; $5, 8$; $7, 8$ can occur only if the characters of both forms f, f' also include such a relation to 8. As before, we easily confirm that the form F has the character $1, 8$ if f and f' have the same character with respect to 8; the form F has the character $3, 8$ if one of the forms f, f' has $1, 8$ and the other $3, 8$, or one has $5, 8$ and the other $7, 8$; F has $5, 8$ if f, f' have $1, 8$ and $5, 8$, or $3, 8$ and $7, 8$; F has $.7, 8$ if f and f' have either $1, 8$ and $7, 8$, or $3, 8$ and $5, 8$.

4°. When $D \equiv 2$ (modulo 8), d' is either $\equiv 0$ or $\equiv 2$ (modulo 8), so $m' = 1$, and therefore d is also either $\equiv 0$ or $\equiv 2$ (modulo 8). But d, d' cannot both be divisible by 8, since D is their *greatest* common divisor. Thus one of the characters 1 *and* $7, 8$; 3 *and* $5, 8$ can be assigned to the form F only when either both forms f, f' have one of those characters, or one has one of them and the other one of the characters $1, 8$;

$3,8$; $5,8$; $7,8$. It is easy to deduce that the character of the form F is determined by the following table, where the character in the margin belongs to one of the forms f, f' and the character at the top to the other:

	1 *and* $7,8$ or $1,8$ or $7,8$	3 *and* $5,8$ or $3,8$ or $5,8$
1 *and* $7,8$	1 *and* $7,8$	3 *and* $5,8$
3 *and* $5,8$	3 *and* $5,8$	1 *and* 7.8

5°. In the same way we prove that the form F cannot be assigned either of the characters 1 *and* $3,8$; 5 *and* $7,8$ unless at least one of the forms f, f' also has one of those characters and the other either one of them or one of the characters $1,8$; $3,8$; $5,8$; $7,8$. The character of the form F is determined by the following table, whose margin and top give the characters of the forms f, f':

	1 *and* $3,8$ or $1,8$ or $3,8$	5 *and* $7,8$ or $5,8$ or $7,8$
1 *and* $3,8$	1 *and* $3,8$	5 *and* $7,8$
5 *and* $7,8$	5 *and* $7,8$	1 *and* 3.8

II. If both forms f, f' are improperly primitive, D is the greatest common divisor of $4d$. $4d'$, or $\frac{1}{4}D$ is the greatest common divisor of d. d'. It follows easily that d, d' and $\frac{1}{4}D$ are all $\equiv 1$ (modulo 4). Setting $F = (A, B, C)$, the greatest common divisor of A, B, C is $= 2$. and the greatest common divisor of $A, 2B, C$ is 4. Thus F is a form derived from the improperly primitive form $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, whose determinant is $\frac{1}{4}D$ and whose genus determines the genus of the form F. As that form is improperly primitive, its character includes no relations to 4 or 8, only relations to the individual odd prime divisors of $\frac{1}{4}D$. Now all these divisors clearly also divide d, d', and half of any product of two factors. one representable by f and the other by f', can be represented by the form $(\frac{1}{2}A. \frac{1}{2}B, \frac{1}{2}C)$. It is therefore easy to see that the character of this form with respect to any odd prime p dividing $\frac{1}{4}D$ is Rp, *both* if $2Rp$ and the forms f, f' have the same character with respect to p. *and* if $2Np$ and the characters of the forms f, f' with respect to p are opposite; by contrast, the character of that form is Np, *both* if f, f' have the same character with respect to p and $2Np$, *and* if f, f' have opposite characters and $2Rp$.

247.

The solution of the preceding problem shows that if g is a primitive form of the same order and genus as f, and g' a primitive form of the same order and genus as f', the form composed from g and g' belongs to the same genus as the form composed from f and f'. This gives the meaning of a *genus composed* from two other genera (or even more). Further, the same solution shows that if f, f' have the same determinant, f is a form of the principal genus and F is composed from f and f', then F belongs to the same genus as f'. So the principal genus can always be left out when composing it with other genera of the same determinant. But if, with the other conditions unchanged, f does not belong to the principal genus and f' is a primitive form, F certainly belongs to a different genus from f'. Finally, if f, f' are properly primitive forms of the same genus, F belongs to the principal genus; but if f, f' are both properly primitive with the same determinant but of different genera, F cannot belong to the principal genus. Thus, when any properly primitive form is composed *with itself*, the resulting form, which is also properly primitive with the same determinant, must belong to the principal genus.

248.

Problem. *Given any two forms f, f', from which F is composed, determine from the genera of the forms f, f' the genus of the form F.*

Solution. Let $f = (a, b, c)$, $f' = (a', b', c')$, $F = (A, B, C)$, and let $\mathfrak{m}$ be the greatest common divisor of a, b, c, and $\mathfrak{m}'$ the greatest common divisor of a', b', c', so that f, f' are derived from the primitive forms $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$, $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$, which we denote by $\mathfrak{f}$, $\mathfrak{f}'$ respectively. Now, if at least one of the forms $\mathfrak{f}$, $\mathfrak{f}'$ is properly primitive, the greatest common divisor of A, B, C is $\mathfrak{m}\mathfrak{m}'$, so F is derived from the primitive form $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}) \ldots \mathfrak{F}$; thus the genus of the form F depends on the genus of the form $\mathfrak{F}$. But it is easy to see that $\mathfrak{F}$ is transformed into $\mathfrak{f}\mathfrak{f}'$ by the same substitution that transforms F into ff', so $\mathfrak{F}$ is composed from $\mathfrak{f}$, $\mathfrak{f}'$, and its genus can be determined by the problem of Article 246. — But if both $\mathfrak{f}$, $\mathfrak{f}'$ are improperly primitive, the greatest common divisor of A, B, C is $2\mathfrak{m}\mathfrak{m}'$, and the form $\mathfrak{F}$ is still composed from $\mathfrak{f}$, $\mathfrak{f}'$ and is clearly derived from the properly primitive form $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$. The genus of this form can therefore be determined by Article 246; and since F is derived from the same form, its genus follows at once.

This solution shows that the theorem set out in the preceding article for primitive forms, namely *if f', g' belong to the same genera as f, g respectively, the form composed from f', g' belongs to the same genus as the form composed from f, g*, holds in general for any forms.

Composition of classes.

249.

THEOREM. *If the forms f, f' belong to the same orders, genera and classes as g, g' respectively, the form composed from f and f' belongs to the same class as the form composed from g and g'.*

This theorem, whose truth follows at once from Article 239, gives the meaning of a *class composed from two given classes*, or even *from several*.

If any class K is composed with the principal class, the class K itself results; that is, the principal class can be left out when composing it with other classes of the same determinant. Composing two opposite properly primitive classes always gives the principal class of the same determinant (see Article 243). Since every ambiguous class is opposite to itself, composing any properly primitive ambiguous class with itself gives the principal class of the same determinant.

The converse of the last proposition also holds: namely, *if composing a properly primitive class K with itself gives the principal class H of the same determinant, K must be an ambiguous class.* For if K' is the class opposite to K, the three classes K, K, K' give the same composite class as H and K'. The former give K (since K and K' produce H, and this with K gives K itself), the latter K'; so K coincides with K' and is therefore an ambiguous class.

The following proposition should also be noted: *If the classes K, L are opposite to the classes K', L' respectively, the class composed from K and L is opposite to the class composed from K' and L'.* Let the forms f, g, f', g' belong to the classes K, L, K', L' respectively; let the form F be composed from f, g, and F' from f', g'. Since f' is improperly equivalent to f, and g' to g, while F is composed directly from each of f, g, F is also composed from f', g', but inversely from each. So any form improperly equivalent to F is composed directly from f', g' and is therefore properly equivalent to F' (Articles 238, 239). Thus F, F' are improperly equivalent, and the classes to which they belong are opposite.

It follows that if an ambiguous class K is composed with an ambiguous class L. an ambiguous class always results. For it is opposite to the class composed from the classes opposite to K, L, and therefore to itself, since these classes are opposite to themselves.

Finally, we observe that, given any two classes K, L of the same determinant, the first of which is properly primitive, we can always find a class M of the same determinant whose composition with K gives L. Clearly we achieve this by taking for M the class composed from L and the class opposite to K. It is also very easy to see that this is the only class with this property; that is, distinct classes of the same determinant, composed with the same properly primitive class, produce distinct classes.

Composition of classes can conveniently be denoted by the addition sign $+$, just as identity of classes is denoted by the equality sign. With these signs the proposition just given can be expressed as follows. If K' is the class opposite to K, $K + K'$ is the principal class of the same determinant, so $K + K' + L = L$; setting $K' + L = M$ therefore gives $K + M = L$, as required. But if, besides M, there were another M with

the same property, that is, $K + M' = L$, we would have $K + K' + M' = L + K' = M$, giving $M' = M$. — If several identical classes are composed, we can indicate this, as in multiplication, by putting their number before them, so that $2K$ means the same as $K + K$, $3K$ the same as $K + K + K$ etc. The same signs could also be applied to forms, so that $(a, b, c) + (a', b', c')$ would denote a form composed from (a, b, c), (a', b', c'). But to avoid even the appearance of ambiguity, we prefer not to use this abbreviation, especially since we have already assigned a particular meaning to a sign such as $\surd M(a, b, c)$. — We say that the class $2K$ arises by *doubling* the class K, the class $3K$ by *tripling*, and so on.

250.

If D is a number divisible by mm (where we suppose m positive), there is an order of forms of determinant D derived from the properly primitive order of determinant $\frac{D}{mm}$ (or *two* when D is negative, namely a positive and a negative order). Clearly the form $(m, 0, -\frac{D}{m})$ belongs to that order, namely the positive one, and may rightly be regarded as its *simplest form* (just as $(-m, 0, \frac{D}{m})$ is the simplest in the negative order when D is negative). If also $\frac{D}{mm} \equiv 1$ (modulo 4), there is an order of forms of determinant D derived from the improperly primitive order of determinant $\frac{D}{mm}$. Clearly the form $(2m, m, \frac{mm-D}{2m})$ belongs to it and is regarded as its simplest form. (When D is negative there are again two orders, and in the negative order the form $(-2m, -m, \frac{D-mm}{2m})$ is regarded as the simplest.) Thus, *for example,* if we also include the case where $m = 1$, in the four orders of forms of determinant 45 the simplest forms are $(1, 0, -45)$, $(2, 1, -22)$. $(3, 0, -15)$, $(6, 3, -6)$. With this understood, we have the following

Problem. *Given any form F of the order O, find a properly primitive (positive) form of the same determinant whose composition with the simplest form in O gives F.*

Solution. Let the form $F = (ma, mb, mc)$ be derived from the primitive form $f = (a, b, c)$, whose determinant is $= d$, and suppose *first* that f is properly primitive. First we observe that if a is not coprime to $2dm$, there are certainly other forms properly equivalent to (a, b, c) whose leading coefficients have this property. For by Article 228 that form represents numbers coprime to $2dm$. Let $a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$ be such a number, and suppose, as we may, that α, γ are coprime. Then choose β, δ so that $\alpha\delta - \beta\gamma = 1$, and transform f by the substitution $\alpha, \beta, \gamma, \delta$ into the form (a', b', c'), which is properly equivalent to it and has the required property. Since F and $(a'm, b'm, c'm)$ are also properly equivalent, we easily see that it is enough to consider the case where a is coprime to $2dm$. Then (a, bm, cmm) is a properly primitive form (for if $a, 2bm, cmm$ had a common divisor, it would also divide $2dm = 2bbm - 2acm$) of the same determinant as F. It is easily confirmed that F is transformed into the product of the form $(m, 0, -dm)$, which, unless F is a negative form, is the simplest in the order O, and (a, bm, cmm), by the substitution $1, 0, -b, -cm$; $0, m, a, bm$. So the criterion in observation 4 of Article 235 shows that F is composed from $(m, 0, -dm)$ and (a, bm, cmm). But when F is a negative form, it is transformed into the product of the simplest form of the same order $(-m, 0, dm)$ and the positive form $(-a, bm, -cmm)$ by the substitution

$1, 0, b, -cm;\ 0, -m, -a, bm$, and is therefore composed from them.

Second, if f is an improperly primitive form, we may suppose $\frac{1}{2}a$ coprime to $2dm$. For if this property does not yet hold for the form f, a form properly equivalent to f and having this property can be found. It follows easily that $(\frac{1}{2}a, bm, 2cmm)$ is a properly primitive form of the same determinant as F. We confirm just as easily that F is transformed into the product of the forms

$$(\pm 2m, \pm m, \pm\tfrac{1}{2}(m - dm)), \quad (\pm\tfrac{1}{2}a, bm, \pm 2cmm)$$

by the substitution

$$1, 0, \tfrac{1}{2}(1 \mp b), -cm; \quad 0, \pm 2m, \pm\tfrac{1}{2}a, (b \pm 1)m$$

where the lower signs are to be taken when F is a negative form and the upper signs in the remaining cases. The form is therefore composed from these two forms, the former being the simplest in the order O, the latter a properly primitive (positive) form.

251.

Problem. *Given two forms F, f of the same determinant D and belonging to the same order O, find a properly primitive form of determinant D whose composition with f produces F.*

Solution. Let φ be the simplest form of the order O; let $\mathfrak{F}$, $\mathfrak{f}$ be properly primitive forms of determinant D whose compositions with φ give F. f respectively; finally, let f' be a properly primitive form whose composition with $\mathfrak{f}$ gives $\mathfrak{F}$. Then the form F is composed from the three forms $\varphi, \mathfrak{f}, f'$, or from the two f, f'. *Q. E. I.*

Thus any class of a given order can be regarded as composed from any given class of the same order and some properly primitive class of the same determinant.

For a given determinant, the individual genera of the same order contain equally many classes.

252.

Theorem. *For a given determinant, the individual genera of the same order contain equally many classes.*

Proof. Let the genera G and H belong to the same order, let G consist of n classes $K, K', K'' \ldots K^{n-1}$, and let L be any class of the genus H. By the preceding article, find a properly primitive class M of the same determinant whose composition with K gives L, and denote the classes obtained by composing M with $K', K'' \ldots K^{n-1}$ by $L', L'' \ldots L^{n-1}$ respectively. Then the last observation of Article 249 shows that all the classes $L, L', L'' \ldots L^{n-1}$ are distinct, and by Article 248 they all belong to the same genus, *that is,* the genus H. Finally, we easily see that H cannot contain any other classes, since any class of the genus H can be regarded as composed from M and another class of the same determinant, which must always belong to the genus G. So H, like G, contains n distinct classes. *Q. E. D.*

Comparing the numbers of classes in the individual genera of different orders.

253.

The preceding theorem assumes that the order is the same and must not be extended to different orders. Thus, *for example,* for the determinant -171 there are 20 positive classes, which fall into four orders: the properly primitive order contains two genera, each comprising six classes; in the improperly primitive order two genera have four classes, two each; in the order derived from the properly primitive order of determinant -19 there is a single genus comprising three classes; finally, the order derived from the improperly primitive order of determinant -19 has a single genus consisting of one class. The negative classes behave in the same way. It is therefore worth investigating the general principle on which the connection between the numbers of classes in different orders depends. Suppose K, L are two classes of the same (positive) order O of determinant D, and M a properly primitive class of the same determinant whose composition with K gives L, such as can always be found by Article 251. In some cases M may be the *only* properly primitive class whose composition with K produces L; in others several distinct properly primitive classes may have this property. Suppose in general that there are r such properly primitive classes $M, M', M'' \dots M^{r-1}$, each of which, composed with K, gives the same class L, and denote their collection by W. Further, let L' be another class of the order O (different from L), and N' a properly primitive class of determinant D whose composition with L gives L', and denote the collection of classes $N'+M, N'+M', N'+M'' \dots N'+M^{r-1}$ (all properly primitive and distinct) by W'. It is then easy to see that K, composed with any class in W', produces L', so W and W' have no class in common. We also verify without difficulty that no properly primitive class outside the collection W', when composed with K, produces L'. Likewise, if L'' is another class of the order O, different from the classes L, L', there are r properly primitive forms, distinct both from one another and from the forms W, W', each of which, composed with K, produces L''. The same holds for all the remaining classes of the order O. Since every properly primitive (positive) class of determinant D, composed with K, produces a class of the order O, we easily conclude that if the total number of classes of the order O is n, the total number of properly primitive (positive) classes of the same determinant is rn.

We therefore have the general rule: if K, L denote any classes of the order O, and r the number of distinct properly primitive classes of the same determinant whose compositions with K each produce L, the total number of classes in the properly primitive (positive) order is r times as large as the number of classes of the order O.

Since the classes K, L in the order O can be chosen entirely at will, we may also take identical classes. It is useful to take the class. which contains the simplest form of this order. Taking this for K and L, then, reduces the matter to finding all the properly primitive classes whose compositions with K reproduce K itself. The following prepares the way for this.

254.

THEOREM. *If $F = (A, B, C)$ is the simplest form of the order O of determinant D, and $f = (a, b, c)$ a properly primitive form of the same determinant, this form f can represent the number AA if F is obtained by composing the forms f, F; and conversely, F is composed from itself and f if AA can be represented by f.*

Proof. I. If F is transformed into the product fF by the substitution p, p', p'', p'''; q, q', q'', q''', Article 235 gives

$$A(aq''q'' - 2bqq'' + cqq) = A^3, \quad \text{so}$$
$$AA = aq''q'' - 2bqq'' + cqq. \quad \textit{First part proved.}$$

II. *Assume* that AA can be represented by f, and denote the values of the indeterminates that give this representation by q''. $-q$, so that $AA = aq''q'' - 2bqq'' + cqq$, and set

$$\begin{aligned} q''a - q(b + B) &= Ap, \\ -qC &= Ap', \\ q''(b - B) - qc &= Ap'' \\ -q''C &= Ap''', \\ q''a - q(b - B) &= Aq', \\ q''(b + B) - qc &= Aq''' \end{aligned}$$

Having done this, we easily confirm that F is transformed into the product fF by the substitution p, p', p'', p'''; q, q', q'', q'''. and is therefore composed from f and F, provided all the numbers p, p' etc. are integers. Now, by the description of the simplest form, B is either 0 or $\frac{1}{2}A$, so $\frac{2B}{A}$ is an integer; the same description shows that $\frac{C}{A}$ is always an integer. Thus $q' - p$, p', $q''' - p''$, p''' are integers, and it only remains to prove that p and p'' are integers. But we have

$$pp + \frac{2pqB}{A} = a - \frac{qqC}{A}, \quad p''p'' + \frac{2p''q''B}{A} = c - \frac{q''q''C}{A}$$

so if $B = 0$, we have

$$pp = a - \frac{qqC}{A}, \quad p''p'' = c - \frac{q''q''C}{A}$$

and therefore p, p'' are integers; but if $B = \frac{1}{2}A$, we have

$$pp + pq = a - \frac{qqC}{A}, \quad p''p'' + p''q'' = c - \frac{q''q''C}{A}$$

from which it follows just as easily that p and p'' are integers in this case too. We conclude that F is composed from f and F. *Second part proved.*

255.

The problem is therefore reduced to finding all properly primitive classes of determinant D whose forms can represent AA. Clearly AA can be represented by any form whose leading coefficient is either AA or the square of a divisor of A. Conversely, if AA can be represented by a form f, assigning to its indeterminates the values αe, γe with greatest common divisor e, the form f is transformed by the substitution $\alpha, \beta, \gamma, \delta$ into a form whose leading coefficient is $\frac{AA}{ee}$. This form is properly equivalent to f if β, δ are chosen so that $\alpha\delta - \beta\gamma = 1$. Thus any class whose forms can represent AA contains forms whose leading coefficient is AA or the square of a divisor of A. The task is therefore to find all properly primitive classes of determinant D in which such forms occur. This is done as follows. Let a, a', a'' etc. be all the (positive) divisors of A; find all the values of the expression $\sqrt{D} \pmod{aa}$ lying between 0 and $aa - 1$ inclusive, denoting them by b, b', b'' etc., and set

$$bb - D = aac, \quad b'b' - D = aac', \quad b''b'' - D = aac'' \text{ etc.}$$

Denote the collection of forms (aa, b, c), (aa, b', c') etc. by V. It is easy to see that any class of determinant D containing a form with leading coefficient aa must also contain a form from V. Likewise find all forms of determinant D whose leading coefficient is $a'a'$ and whose middle coefficient lies between 0 and $a'a' - 1$ inclusive, and denote their collection by V'; similarly let V'' be the collection of such forms with leading coefficient $a''a''$, and so on. Remove from V, V', V'' etc. all forms that are not properly primitive, sort the remaining forms into classes, and if several belong to the same class, retain only one in each class. This gives all the required classes, and their number is to unity as the number of all properly primitive (positive) classes is to the number of classes in the order O.

Example. Let $D = -531$, and let O be the positive order derived from the improperly primitive order of determinant -59, whose simplest form is $(6, 3, 90)$, so $A = 6$. Here a, a', a'', a''' are $1, 2, 3, 6$; V contains the form $(1, 0, 531)$; V' the forms $(4, 1, 133)$, $(4, 3, 135)$; V'' the forms $(9, 0, 59)$, $(9, 3, 60)$, $(9, 6, 63)$; finally V''' the forms $(36, 3, 15)$, $(36, 9, 17)$, $(36, 15, 21)$, $(36, 21, 27)$, $(36, 27, 35)$, $(36, 33, 45)$. But six of these twelve forms must be removed: the second and third from V'', and the first, third, fourth and sixth from V''', all of which are derived forms. The six remaining forms are found to belong to distinct classes. In fact, the number of properly primitive (positive) classes of determinant -531 is 18, and the number of improperly primitive (positive) classes of determinant -59 (or the number of classes of determinant -531 derived from them) is 3, so the former is to the latter as 6 to 1.

256.

The following general observations will make this solution still clearer.

I. If the order O is derived from a properly primitive order, AA divides D; but if O is improperly primitive or derived from an improperly primitive order, A is even, D is divisible by $\frac{1}{4}AA$, and the quotient is $\equiv 1 \pmod 4$. Thus the square of any divisor of A divides either D itself or at least $4D$, and in the latter case the quotient is always $\equiv 1 \pmod 4$.

II. If aa divides D, all the values of the expression $\sqrt{D} \pmod{aa}$ that lie between 0 and $aa-1$ are $0, a, 2a \ldots aa-a$, so a is the number of forms in V; but only as many of them are properly primitive as there are numbers in

$$\frac{D}{aa}, \quad \frac{D}{aa}-1, \quad \frac{D}{aa}-4 \ldots \frac{D}{aa}-(a-1)^2$$

that have no common divisor with a. When $a=1$, V consists of a single form, $(1,0,-D)$, which is always properly primitive. When a is 2 or any power of 2, half of those a numbers are even and half odd, so V contains $\frac{1}{2}a$ properly primitive forms. When a is another prime number p or a power of a prime number p, three cases must be distinguished: all those a numbers are relatively prime to a, and so all the forms in V are properly primitive, if $\frac{D}{aa}$ is not divisible by p and is also a quadratic nonresidue modulo p; but if p divides $\frac{D}{aa}$, V contains $\frac{(p-1)a}{p}$ properly primitive forms; finally, if $\frac{D}{aa}$ is a quadratic residue modulo p not divisible by p, V contains $\frac{(p-2)a}{p}$ properly primitive forms. All this is proved without difficulty. In general, setting $a = 2^\nu p^\pi q^\chi r^\rho \ldots$, where p, q, r etc. denote distinct odd primes, the number of properly primitive forms in V is $NPQR \ldots$, where we must set

$$\begin{aligned}
&N = 1 \quad (\text{if } \nu = 0) \text{ or } N = 2^{\nu-1} \ (\text{if } \nu > 0)\\
&P = p^\pi \quad (\text{if } \tfrac{D}{aa} \text{ is a quadratic nonresidue modulo } p) \text{ or}\\
&P = (p-1)p^{\pi-1} \quad (\text{if } \tfrac{D}{aa} \text{ is divisible by } p) \text{ or}\\
&P = (p-2)p^{\pi-1} \quad (\text{if } \tfrac{D}{aa} \text{ is a quadratic residue modulo } p\\
&\qquad \text{and is not divisible by } p)
\end{aligned}$$

and Q, R etc. are to be defined from q, r etc. in the same way as P from p.

III. If aa does not divide D, $\frac{4D}{aa}$ is an integer and $\equiv 1 \pmod 4$, and the values of the expression $\sqrt{D} \pmod{aa}$ are $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a \ldots aa - \frac{1}{2}a$. Thus the number of forms in V is a, but only as many of them are properly primitive as there are numbers in

$$\frac{D}{aa}-\tfrac{1}{4}, \quad \frac{D}{aa}-\tfrac{9}{4}, \quad \frac{D}{aa}-\tfrac{25}{4} \quad \ldots \quad \frac{D}{aa}-(a-\tfrac{1}{2})^2$$

that are relatively prime to a. Whenever $\frac{4D}{aa} \equiv 1 \pmod 8$, all these numbers are even, so V contains no properly primitive form; but when $\frac{4D}{aa} \equiv 5 \pmod 8$. all those numbers are odd, so all forms in V are properly primitive if a is 2 or a power of 2. In general, in this case there are as many properly primitive forms in V as there are numbers in that list divisible by no odd prime divisor of a. This number is $NPQR \ldots$

if $a = 2^\nu p^\pi q^\chi r^\rho \ldots$, where we must set $N = 2^\nu$ and derive P, Q, R etc. from p, q, r etc. in the same way as in the preceding case.

IV. In this way, then, the numbers of properly primitive forms in V, V', V'' etc. can be determined. For the sum of all these numbers, the following general rule is found without much difficulty: if $A = 2^\nu \mathfrak{A}^\alpha \mathfrak{B}^\beta \mathfrak{C}^\gamma \ldots$, where $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. denote distinct odd primes, the total number of properly primitive forms in V, V', V'' etc. is $= \frac{An\mathfrak{abc}\ldots}{2\mathfrak{ABC}\ldots}$, where we must set

$$\begin{aligned}
&\mathfrak{n} = 1 \text{ (if } \tfrac{4D}{AA} \equiv 1, \text{ mod. } 8), \text{ or}\\
&\mathfrak{n} = 2 \text{ (if } \tfrac{D}{AA} \text{ is an integer), or}\\
&\mathfrak{n} = 3 \text{ (if } \tfrac{4D}{AA} \equiv 5, \text{ mod. } 8); \text{ further}\\
&\mathfrak{a} = \mathfrak{A} \text{ (if } \mathfrak{A} \text{ divides } \tfrac{4D}{AA}), \text{ or}\\
&\mathfrak{a} = \mathfrak{A} \pm 1 \text{ (if } \mathfrak{A} \text{ does not divide } \tfrac{4D}{AA},\\
&\qquad \text{taking the upper sign}\\
&\qquad \text{or the lower according as } \tfrac{4D}{AA} \text{ is a nonresidue}\\
&\qquad \text{or a quadratic residue modulo } \mathfrak{A})
\end{aligned}$$

and finally derive $\mathfrak{b}, \mathfrak{c}$ etc. from $\mathfrak{B}, \mathfrak{C}$ in the same way as $\mathfrak{a}$ from $\mathfrak{A}$. To give the proof in greater detail here. is ruled out by the need to be brief.

V. As for the number of classes supplied by the properly primitive forms in V, V', V'' etc., the following three cases must be distinguished.

First, when D is a negative number, each properly primitive form in V, V' etc. constitutes a separate class; that is, the number of classes sought is expressed by the formula given in the preceding observation, with two exceptions: when $\frac{4D}{AA}$ is either $= -4$ or $= -3$, or equivalently when D is either $= -AA$ or $= -\frac{3}{4}AA$. To prove this theorem, clearly we need only show that two distinct forms from V, V', V'' etc. cannot be properly equivalent. Suppose, then, that (hh, i, k), $(h'h', i', k')$ are two distinct properly primitive forms from V, V', V'' etc. belonging to the same class, and that the former is transformed into the latter by the proper substitution $\alpha, \beta, \gamma, \delta$. We then have the equations

$$\begin{aligned}
\alpha\delta - \beta\gamma &= 1,\\
hh\alpha\alpha + 2i\alpha\gamma + k\gamma\gamma &= h'h',\\
hh\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta &= i'
\end{aligned}$$

From these we easily conclude, *first*, that γ certainly is not $= 0$ (which would imply $\alpha = \pm 1$, $hh = h'h'$, $i' \equiv i$ (mod. hh), and thus that the proposed forms are identical, contrary to the hypothesis); *second*, that γ is divisible by the greatest common divisor of the numbers h, h'; (for, setting this divisor $= r$, it clearly also divides $2i, 2i'$ but is relatively prime to k; moreover, rr divides $hhk - h'h'k' = ii - i'i'$, from which we easily deduce that r also divides $i - i'$. But we have $\alpha i' - \beta h'h' = \alpha i + \gamma k$, so γk and therefore also γ are divisible by r); *third*, that $(\alpha hh + \gamma i)^2 - D\gamma\gamma = hhh'h'$. Setting $\alpha hh + \gamma i = rp$, $\gamma = rq$, then, p and q are integers, the latter not $= 0$, and $pp - Dqq = \frac{hhh'h'}{rr}$. But $\frac{hhh'h'}{rr}$ is the least number divisible by both hh and $h'h'$, and

therefore divides AA and so also $4D$. Thus $\frac{4Drr}{hhh'h'}$ is a (negative) integer; setting it $= -e$, we have $pp - Dqq = -\frac{4D}{e}$, or $4 = (\frac{2rp}{hh'})^2 + eqq$. In this equation the term $(\frac{2rp}{hh'})^2$, being a square less than 4, must be either 0 or 1. In the former case $eqq = 4$, and $D = -(\frac{hh'}{rq})^2$, from which it follows that $\frac{4D}{AA}$ is a square with a negative sign and therefore certainly not $\equiv 1 \pmod 4$, so O is neither improperly primitive nor derived from an improperly primitive order. Thus $\frac{D}{AA}$ is an integer, from which we easily deduce that e is divisible by 4, $qq = 1$, $D = -(\frac{hh'}{r})^2$, and that $\frac{AA}{D}$ too is an integer. We must therefore have $D = -AA$, or $\frac{D}{AA} = -1$, which is the first exception. In the latter case $eqq = 3$, so $e = 3$ and $4D = -3(\frac{hh'}{r})^2$; thus $3(\frac{hh'}{rA})^2$ is an integer which, since multiplication by the integer square $(\frac{rA}{hh'})^2$ gives 3, can only be 3. Hence $4D = -3AA$, or $D = -\frac{3}{4}AA$, which is the second exception. In all the remaining cases, therefore, all properly primitive forms in V, V', V'' etc. belong to distinct classes. — For the exceptional cases it is enough to state the results of an investigation that is not difficult but must be omitted here to keep things brief. In the former case the properly primitive forms in V, V', V'' etc. always belong to the same class in pairs, in the latter in threes, so the total number of classes sought is, in the former case, half the value of the expression given in the preceding observation, and in the latter one third of it.

Second, when D is a positive square, each properly primitive form in V, V', V'' etc. constitutes a separate class without exception. For suppose (hh, i, k), $(h'h', i', k')$ are two such distinct properly equivalent forms, and that the former is transformed into the latter by the proper substitution $\alpha, \beta, \gamma, \delta$. All the arguments used in the preceding case that do not assume D negative clearly hold here too. Thus, with p, q, r denoting the same things as there, $\frac{4Drr}{hhh'h'}$ is again an integer, but now positive rather than negative and also a square. Setting it $= gg$, we have $(\frac{2rp}{hh'})^2 - ggqq = 4$, *which is absurd,* since the difference of two squares cannot be 4 unless the smaller square is 0. The assumption therefore cannot hold.

For the *third* case, however, where D is a positive nonsquare, we do not yet have a general rule for comparing the number of properly primitive forms in V, V', V'' etc. with the number of distinct classes resulting from them. We can indeed say that the latter either equals the former or is a divisor of it. We have even discovered a special connection between the quotient of these numbers and the smallest values of t, u satisfying the equation $tt - Duu = AA$, but describing it here would take too long. Whether that quotient can be found in every case merely by inspecting the numbers D, A (as in the preceding cases), we cannot say with certainty. Here are some examples, whose number anyone can easily increase. For $D = 13$, $A = 2$, the number of properly primitive forms in V etc. is 3, all equivalent, so they constitute a single class; for $D = 37$, $A = 2$, there are again three properly primitive forms in V etc., belonging to three distinct classes; for $D = 588$, $A = 7$, there are eight properly primitive forms in V etc., constituting four classes; for $D = 867$, $A = 17$, V etc. contain 18 properly primitive forms, and just as many for $D = 1445$, $A = 17$, but for the former determinant they fall into two classes, and for the latter into six.

VI. Applying this general theory to the case. where O is an improperly primitive order, we conclude that the number of classes in this order is to the total number

of classes in the properly primitive order as 1 is to the number of distinct properly primitive classes constituted by the three forms $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$. Just one class results when $D \equiv 1 \pmod 8$, because in this case the second and third forms are improperly primitive; but when $D \equiv 5 \pmod 8$, all three forms are properly primitive and produce as many distinct classes if D is negative, except for the single case $D = -3$, in which they constitute one class. Finally, the case where D is positive (of the form $8n + 5$) is among those for which a general rule is still lacking. We can nevertheless say that in this case the three forms belong either to three distinct classes or to one, never to two. For it is easy to see that if the forms $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ belong respectively to the classes K, K', K'', then $K + K' = K'$, $K' + K' = K''$; thus, if K and K' are assumed identical, K' and K'' are identical too. Likewise, if K and K'' are assumed identical, K' and K'' are identical too; finally, since $K' + K'' = K$, the assumption that K' and K'' are identical implies that K and K'' coincide too. Thus either all three classes K, K', K'' are distinct or all three are identical. *For example,* below 600 there are 75 numbers of the form $8n + 5$, including 16 determinants for which the former case holds, so the number of classes in the properly primitive order is three times that in the improperly primitive order, namely $37, 101, 141, 189, 197, 269.$ $325, 333, 349, 373, 381, 389, 405, 485, 557, 573$; for the remaining 59 the latter case holds, so the number of classes is the same in both orders.

VII. There is hardly any need to observe that the preceding investigation not only allows us to compare the numbers of classes in different orders of the same determinant, but also applies to any different determinants whose ratio is that of squares. Namely, if O denotes any order of determinant dmm, and O' an order of determinant $dm'm'$, O can be compared with the properly primitive order of determinant dmm, and this with the order derived from the properly primitive order of determinant d, or, what comes to the same thing for the number of classes, with this order itself. The order O' can be compared with that same order in exactly the same way.

The number of ambiguous classes.

257.

Of all classes in a given order of a given determinant, the ambiguous classes in particular call for a fuller investigation, and determining their number will open the way to many other things. It is enough, however, to determine this number in the properly primitive order alone, since the remaining cases can easily be reduced to this one. We will do this by first showing how to find all properly primitive ambiguous forms (A, B, C) of the proposed determinant D in which either $B = 0$ or $B = \frac{1}{2}A$, and then how to find from their number the number of all properly primitive ambiguous classes of determinant D.

I. Clearly all properly primitive forms $(A, 0, C)$ of determinant D are found by taking for A each divisor of D (both positive and negative) for which $C = -\frac{D}{A}$ is relatively prime to A. Thus when $D = 1$, there are two such forms, $(1, 0, -1)$, $(-1, 0, 1)$; just as many when $D = -1$, namely $(1, 0, 1)$, $(-1, 0, -1)$; when D is a prime number or a power of a prime (with either a positive or a negative sign), there are four: $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. In general, when D is divisible by n distinct primes (among which 2 too must be counted here), there are altogether 2^{n+1} such forms. Namely, setting $D = \pm PQR\ldots$, where P, Q, R etc. denote distinct primes or powers of distinct primes, whose number is $= n$, the values of A are $1, P, Q, R$ etc. and products of any number of these numbers. By the theory of combinations the number of these values is 2^n, but it must be doubled, since each value must be given both a positive and. a negative sign.

II. Likewise, all properly primitive forms $(2B, B, C)$ of determinant D are obtained by taking for B all divisors of D (positive and negative) for which $C = \frac{1}{2}(B - \frac{D}{B})$ is an integer relatively prime to $2B$. Since C must be odd, and therefore $CC \equiv 1 \pmod 8$, it follows from $D = BB - 2BC = (B - C)^2 - CC$ that D is either $\equiv 3 \pmod 4$ when B is odd, or $\equiv 0 \pmod 8$ when B is even. Thus whenever D is congruent to one of the numbers $1, 2, 4, 5, 6$ modulo 8, there are no such forms. When $D \equiv 3 \pmod 4$, C is an odd integer whatever divisor of D is taken for B; but for C to have no common divisor with $2B$, B must be chosen so that $\frac{D}{B}$ is relatively prime to B. Thus for $D = -1$ there are two forms, $(2, 1, 1)$, $(-2. -1, -1)$, and in general it is easy to see that if the number of all primes dividing D is n, altogether 2^{n+1} forms result. — When D is divisible by 8, C is an integer if we take for B any even divisor of $\frac{1}{2}D$; the other condition, that $C = \frac{1}{2}B - \frac{D}{2B}$ be relatively prime to $2B$, is satisfied *first* by taking for B all divisors of D that are twice an odd number and for which $\frac{D}{B}$ has no common divisor with B. Their number (counting the different signs) is 2^{n+1} if D is assumed divisible by n distinct odd primes; *second*, by taking for B all divisors of $\frac{1}{2}D$ that are divisible by four and for which $\frac{D}{2B}$ is relatively prime to B. Their number too is 2^{n+1}, so in this case there are altogether 2^{n+2} such forms. Namely, setting $D = \pm 2^\mu PQR\ldots$, where μ denotes an exponent greater than 2 and P, Q, R distinct odd primes or powers of such primes whose number is n, we can take *both* for $\frac{1}{2}B$ *and* for $\frac{D}{2B}$ the values $1, P, Q, R$ etc. and products of any number of these numbers, with both positive and negative signs.

From all this we conclude that if D is assumed divisible by n distinct odd primes

(setting $n = 0$ when $D = \pm 1$ or ± 2 or a power of two), the number of all properly primitive forms (A, B, C) in which B is either 0 or $\frac{1}{2}A$ is 2^{n+1} when D is either $\equiv 1$ or $\equiv 5 \pmod 8$; 2^{n+2} when $D \equiv 2, 3, 4, 6$ or $7 \pmod 8$; and finally 2^{n+3} when $D \equiv 0 \pmod 8$. Comparing this with what we gave in Article 231 for the number of all possible characters of primitive forms of determinant D, we see that the former is in every case exactly twice the latter. Moreover, when D is negative, there are clearly as many positive as negative forms among those forms.

258.

All the forms found in the preceding article clearly belong to ambiguous classes, and conversely every properly primitive ambiguous class of determinant D must contain at least one of those forms. Such a class certainly contains ambiguous forms, and every properly primitive ambiguous form (a, b, c) of determinant D is equivalent to one of the forms of the preceding article, namely either

$$(a, 0, -\tfrac{D}{a}) \text{ or } (a, \tfrac{1}{2}a, \tfrac{1}{4}a - \tfrac{D}{a})$$

according as b is $\equiv 0$ or $\equiv \frac{1}{2}a \pmod{a}$. The problem is therefore reduced to finding how many distinct classes those forms constitute.

If the form $(a, 0, c)$ is among the forms of the preceding article, the form $(c, 0, a)$ occurs among them too and is always different from it, with the single exception $a = c = \pm 1$, and therefore $D = -1$, which we will set aside for a while. Since these forms clearly belong to the same class, it is enough to retain one, and we will discard the one whose leading coefficient is greater than the third; we also set aside the case $a = -c = \pm 1$, or $D = 1$. In this way we can reduce all the forms $(A, 0, C)$ to half their number, always retaining one of each pair; and in all those remaining we have $A < \sqrt{\pm D}$.

Likewise, if the form $(2b, b, c)$ occurs among the forms of the preceding article, so does

$$(4c - 2b,\ 2c - b,\ c) = \left(-\frac{2D}{b},\ -\frac{D}{b},\ c\right)$$

which is properly equivalent to it and different from it, with the single exception that we set aside, $c = b = \pm 1$, or $D = -1$. Of these two forms it is enough to retain the one whose leading coefficient is less than the other's (in this case they cannot be equal in magnitude but different in sign). Thus all the forms $(2B, B, C)$ too can be reduced to half their number, always discarding one of each pair; and in those remaining we have $B < \frac{D}{B}$, or $B < \sqrt{\pm D}$. In this way only half of all the forms of the preceding article remain. We will denote their collection by W, and need only show how many distinct classes arise from these forms. Moreover, when D is negative, there are clearly as many positive as negative forms in W.

I. When D is negative, the individual forms in W belong to distinct classes. For all the forms $(A, 0, C)$ are reduced; likewise all the forms $(2B, B, C)$ are reduced except those in which $C < 2B$. In such a form $2C < 2B + C$, so (since $B < \frac{D}{B}$, *that is,* $B < 2C - B$, and therefore $2B < 2C$, or $B < C$) we have $2C - 2B < C$ and $C - B < \frac{1}{2}C$, and hence $(C, C - B, C)$, which is clearly equivalent to it, is a reduced form. This gives as many reduced forms as there are forms in W, and since it is easy to see that neither identical nor opposite forms can occur among them (with the single exception $C - B = 0$, in which $B = C = \pm 1$, and therefore $D = -1$, which we have already set aside), they all belong to distinct classes. We conclude that the number of all properly primitive ambiguous classes of determinant D equals the number of forms in W, or half the number of forms in the preceding article. In the exceptional case $D = -1$ the same result holds by compensation: there are two classes, one containing the forms $(1, 0, 1)$, $(2, 1, 1)$, and the other $(-1, 0, -1)$, $(-2, -1, -1)$. In general, then,

for a negative determinant the number of all properly primitive ambiguous classes equals the number of all assignable characters of primitive forms of this determinant; but the number of positive properly primitive ambiguous classes is half as great.

II. When D is a positive square $= hh$, it is not difficult to prove that the individual forms in W belong to distinct classes. But in this case we can reach the solution still more briefly as follows. By Article 210 every properly primitive ambiguous class of determinant hh, and no other class, contains one reduced form $(a, h, 0)$, in which a is a value of the expression $\sqrt{1}$ (mod. $2h$) lying between 0 and $2h-1$ inclusive. Thus there are as many properly primitive ambiguous classes of determinant hh as that expression has values. From Article 105 it follows without difficulty that the number of these values is 2^n or 2^{n+1} or 2^{n+2}, according as h is odd, twice an odd number, or divisible by four; that is, according as $D \equiv 1$ or $\equiv 4$ or $\equiv 0$ (mod. 8), where n denotes the number of distinct odd prime divisors of h, or of D. Thus the number of properly primitive ambiguous classes is always half the total number of forms found in the preceding article, or equal to the number of forms in W, or of all possible characters.

III. When D is a positive nonsquare, derive from each form (A, B, C) in W another form (A, B', C') by taking $B' \equiv B$ (mod. A) between the bounds $\sqrt{D}$ and $\sqrt{D} \mp A$ (using the upper or lower sign according as A. is positive or negative), and $C' = \frac{B'B'-D}{A}$; denote their collection by W'. Clearly these forms are properly primitive ambiguous forms of determinant D, all distinct; moreover, they are all reduced. For when $A < \sqrt{D}$, B' is clearly $< \sqrt{D}$ and positive; also $B' > \sqrt{D} \mp A$, so $A > \sqrt{D} - B'$, and therefore A, taken positively, certainly lies between $\sqrt{D} + B'$ and $\sqrt{D} - B'$. But when $A > \sqrt{D}$, we cannot have $B = 0$ (since we discarded those forms), and must have $B = \frac{1}{2}A$. Thus B' equals $\frac{1}{2}A$ in magnitude and has a positive sign (for since $A < 2\sqrt{D}$, $\pm\frac{1}{2}A$ lies between the bounds assigned to B' and is congruent to B modulo A, so $B' = \pm\frac{1}{2}A$). Hence $B' < \sqrt{D}$, which gives $2B' < \sqrt{D} + B'$, or $A < \sqrt{D} + B'$; therefore $\pm A$ must lie between the bounds $\sqrt{D} + B'$ and $\sqrt{D} - B'$. Finally, W' contains all reduced properly primitive ambiguous forms of determinant D. For if (a, b, c) is such a form, either $b \equiv 0$ or $b \equiv \frac{1}{2}a$ (mod. a). In the former case we clearly cannot have $b < a$, and therefore not $a > \sqrt{D}$, so the form $\left(a, 0, -\frac{D}{a}\right)$ certainly belongs to W, and the corresponding (a, b, c) to W'; in the latter we certainly have $a < 2\sqrt{D}$, so $\left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a}\right)$ belongs to W, and the corresponding (a, b, c) to W'. Thus the number of forms in W equals the number of all reduced properly primitive ambiguous forms of determinant D. But since each ambiguous class contains *two* reduced ambiguous forms (Articles 187, 194), the number of all properly primitive ambiguous classes of determinant D is half the number of forms in W, or half the number of all assignable characters.

259.

The number of improperly primitive ambiguous classes of a given determinant D always equals the number of properly primitive ambiguous classes of the same determinant. Let K be the principal class, and K', K'' etc. the remaining properly primitive ambiguous classes of this determinant; let L be any improperly primitive ambiguous class of the same determinant, *for example,* the one containing the form $(2, 1, \frac{1}{2} - \frac{1}{2}D)$. Composing the class L with K gives the class L itself. Suppose composing the class L with K', K'' etc. gives the classes L', L'' etc. respectively. Clearly all belong to the same determinant D and are improperly primitive and ambiguous. The theorem will therefore be proved once we have shown that all the classes L, L', L'' etc. are distinct and that there are no other improperly primitive ambiguous classes of determinant D. For this we distinguish the following cases.

I. When the number of improperly primitive classes equals the number of properly primitive classes, each of the former arises by composing the class L with a definite properly primitive class, so all L, L', L'' etc. must be distinct. If $\mathfrak{L}$ denotes any improperly primitive ambiguous class of determinant D, there is a properly primitive class $\mathfrak{K}$ such that $\mathfrak{K} + L = \mathfrak{L}$. If the class $\mathfrak{K}$ has opposite class $\mathfrak{K}'$, we also have (since the classes L, $\mathfrak{L}$ are their own opposites) $\mathfrak{K}' + L = \mathfrak{L}$. Thus $\mathfrak{K}$ must be identical to $\mathfrak{K}'$ and therefore ambiguous; so $\mathfrak{K}$ occurs among the classes K, K', K'' etc., and $\mathfrak{L}$ among L, L', L'' etc.

II. When the number of improperly primitive classes is one third the number of properly primitive classes, let H be the class containing the form $\left(4, 1, \frac{1-D}{4}\right)$, and H' the one containing $\left(4, 3, \frac{9-D}{4}\right)$. Then H, H' are properly primitive and distinct both from one another and from the principal class K, and $H + H' = K$; $2H = H'$, $2H' = H$. If $\mathfrak{L}$ is any improperly primitive class of determinant D arising by composing the class L with the properly primitive class $\mathfrak{K}$, we also have $\mathfrak{L} = L + \mathfrak{K} + H$ and $\mathfrak{L} = L + \mathfrak{K} + H'$. Besides the three (properly primitive and distinct) classes $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$, no others composed with L produce $\mathfrak{L}$. Thus, if $\mathfrak{L}$ is ambiguous and $\mathfrak{K}'$ opposite to $\mathfrak{K}$, we also have $L + \mathfrak{K}' = \mathfrak{L}$, so $\mathfrak{K}'$ must be identical to one of those three classes. If $\mathfrak{K}' = \mathfrak{K}$, $\mathfrak{K}$ is ambiguous; if $\mathfrak{K}' = \mathfrak{K} + H$, we have $K = \mathfrak{K} + \mathfrak{K}' = 2\mathfrak{K} + H = 2(\mathfrak{K} + H')$, so $\mathfrak{K} + H'$ is ambiguous; likewise if $\mathfrak{K}' = \mathfrak{K} + H'$, $\mathfrak{K} + H$ is ambiguous. We conclude that $\mathfrak{L}$ must occur among the classes L, L', L'' etc. But it is easy to see that among the three classes $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ more than one cannot be ambiguous. For if both $\mathfrak{K}$ and $\mathfrak{K} + H$ were ambiguous, or identical to their respective opposites $\mathfrak{K}'$, $\mathfrak{K}' + H'$, we would have $\mathfrak{K} + H = \mathfrak{K} + H'$. The same conclusion follows from assuming $\mathfrak{K}$ and $\mathfrak{K} + H'$ ambiguous; finally, if $\mathfrak{K} + H$, $\mathfrak{K} + H'$ were ambiguous, or identical to their opposites $\mathfrak{K}' + H'$, $\mathfrak{K}' + H$, we would have $\mathfrak{K} + H + \mathfrak{K}' + H = \mathfrak{K}' + H' + \mathfrak{K} + H'$, giving $2H = 2H'$, or $H' = H$. Thus there is only one properly primitive ambiguous class whose composition with L produces $\mathfrak{L}$, so all L, L', L'' etc. are distinct.

The number of ambiguous classes in a *derived* order clearly equals the number of ambiguous classes in the primitive order from which it is derived, and so can always be determined from what precedes.

260.

PROBLEM. *A properly primitive class K of determinant D arises by doubling a properly primitive class k of the same determinant. Find all such classes whose doubling gives the class K.*

Solution. Let H be the principal class of determinant D, and H', H'', H''' etc. the remaining properly primitive ambiguous classes of the same determinant; denote the classes obtained by composing these with k, namely $k+H'$, $k+H''$, $k+H'''$, by k', k'', k''' etc. Then all the classes k, k', k'' etc. are properly primitive, of determinant D, and distinct; it is just as easy to see that doubling each gives the class K. If $\mathfrak{K}$ denotes any properly primitive class of determinant D whose doubling produces the class K, it must occur among the classes k, k', k'' etc. For set $\mathfrak{K} = k + \mathfrak{H}$, where $\mathfrak{H}$ is a properly primitive class of determinant D (Article 249). and then $2k + 2\mathfrak{H} = 2\mathfrak{K} = K = 2k$, from which we easily conclude that $2\mathfrak{H}$ coincides with the principal class, $\mathfrak{H}$ is ambiguous, that is, occurs among H, H', H'' etc., and $\mathfrak{K}$ among k, k', k'' etc. These classes therefore give the complete solution to the problem.

Moreover, when D is negative, clearly half of the classes k, k', k'' etc. are positive and half negative.

Thus every properly primitive class of determinant D that can arise by doubling any such class arises by doubling exactly as many such classes as there are properly primitive ambiguous classes of determinant D. Consequently, if the number of all properly primitive classes of determinant D is r, and the number of all properly primitive ambiguous classes of this determinant is n, the number of all properly primitive classes of the same determinant obtainable by doubling such a class is $\frac{r}{n}$. The same formula results if, for a negative determinant, the symbols r, n denote the numbers of *positive* classes: the former *all* properly primitive classes, the latter only the ambiguous ones. Thus, *for example,* for $D = -161$ the number of all positive properly primitive classes is 16, and the number of ambiguous classes 4, so the number of all classes obtainable by doubling some class must be 4. And indeed all classes in the principal genus are found to have this property: the principal class $(1, 0, 161)$ arises by doubling the four ambiguous classes; $(2, 1, 81)$ by doubling the classes $(9, 1, 18)$, $(9, -1, 18)$, $(11, 2, 15)$, $(11, -2, 15)$; $(9, 1, 18)$ by doubling the classes $(3, 1, 54)$, $(6, 1, 27)$, $(5, -2, 33)$, $(10, 3, 17)$; finally $(9, -1, 18)$ by doubling the classes $(3, -1, 54)$, $(6, -1, 27)$, $(5, 2, 33)$, $(10, -3, 17)$.

At least half of all assignable characters for a given determinant cannot correspond to properly primitive genera (positive for a negative determinant).

261.

THEOREM. *For a positive nonsquare determinant, at least half of all assignable characters cannot correspond to any properly primitive genera; for a negative determinant, to any positive properly primitive genera.*

Proof. Let m be the number of all properly primitive (positive) genera of determinant D, and k the number of classes in each genus, so that km is the number of all properly primitive (positive) classes; let n be the number of all distinct assignable characters for this determinant. Then by Article 258 the number of all properly primitive (positive) ambiguous classes is $\frac{1}{2}n$. Hence by the preceding article the number of all properly primitive classes obtainable by doubling such a class is $\frac{2km}{n}$. But by Article 247 all these classes belong to the principal genus, which contains k classes. Thus, if all classes of the principal genus can be obtained by doubling some class (as will be proved below to hold in every case), we have $\frac{2km}{n} = k$, or $m = \frac{1}{2}n$; but certainly we cannot have $\frac{2km}{n} > k$, and therefore not $m > \frac{1}{2}n$. Since, then, the number of all properly primitive (positive) genera is certainly no greater than half the number of all assignable characters, at least half of these characters cannot correspond to such genera. *This proves the theorem.* — It must be kept in mind, however, that this does not yet show that half of all assignable characters actually correspond to properly primitive (positive) genera. The truth of this very important proposition can only be brought out below from the deepest mysteries of numbers.

Since for a negative determinant there are always as many negative as positive genera, clearly no more than half of all assignable characters can belong to negative properly primitive genera. We will discuss this below, as well as improperly primitive genera. Finally, the theorem does not extend to positive square determinants: in this case it is easy to see that genera actually correspond to every assignable character.

A second proof of the fundamental theorem and the other theorems concerning the residues -1, $+2$, -2.

262.

Thus, when only two distinct characters can be assigned for a given nonsquare determinant D, only one corresponds to a properly primitive (positive) genus (which can only be the principal genus); the other belongs to no properly primitive (positive) form of that determinant. This happens for the determinants -1, 2, -2, -4. prime numbers of the form $4n + 1$ taken positively and those of the form $4n + 3$ taken negatively; finally, for all odd powers of primes of the form $4n + 1$ taken positively, and for powers of primes of the form $4n + 3$ taken positively or negatively according as their exponents are even or odd. From this principle we can draw a new method of proving not only the fundamental theorem but also the other theorems of the preceding section concerning the residues -1, $+2$, -2. It is entirely different from the methods used in the preceding section and seems no less elegant. We will pass

over the determinant -4 and those that are powers of primes, since they teach us nothing new.

Thus for the determinant -1 there is no positive form with character $3, 4$; for the determinant $+2$ there is no form at all with character 3 *and* $5, 8$; for the determinant -2 no positive form has character 5 *and* $7, 8$; for the determinant $+p$, if p is a prime of the form $4n + 1$, or for the determinant $-p$, if p is a prime of the form $4n + 3$, no properly primitive form (positive in the latter case) has character Np. We therefore prove the theorems of the preceding section as follows.

I. -1 is a nonresidue of every (positive) number of the form $4n + 3$. For if -1 were a residue of such a number A, setting $-1 = BB - AC$ would give (A, B, C) as a positive form of determinant -1 with character $3, 4$.

II. -1 is a residue of every prime p of the form $4n + 1$. For the character of the form $(-1, 0, p)$, like that of every properly primitive form of determinant p. is Rp, and therefore $-1Rp$.

III. Both $+2$ and -2 are residues of every prime p of the form $8n+1$. For either the forms $\left(8, 1, \frac{1-p}{8}\right)$, $\left(-8, 1, \frac{p-1}{8}\right)$ or the forms $\left(8, 3, \frac{9-p}{8}\right)$, $\left(-8, 3, \frac{p-9}{8}\right)$ are properly primitive (according as n is odd or even), so their character is Rp. Thus $+8Rp$ and $-8Rp$, which also gives $2Rp$, $-2Rp$.

IV. $+2$ is a nonresidue of every number of the form $8n + 3$ or $8n + 5$. For if it were a residue of such a number A, there would be a form (A, B, C) of determinant $+2$ with character 3 *and* $5, 8$.

V. Likewise -2 is a nonresidue of every number of the form $8n + 5$ or $8n + 7$; otherwise there would be a form (A, B, C) of determinant -2 with character 5 *and* $7, 8$.

VI. -2 is a residue of every prime p of the form $8n + 3$. This proposition can be proved in two ways. *First*, since by IV we have $+2Np$, and by I $-1Np$, we must have $-2Rp$. The *second* proof comes from considering the determinant $+2p$, for which four characters can be assigned, namely Rp, 1 *and* $3, 8$; Rp, 5 *and* $7, 8$; Np, 1 *and* $3, 8$; Np, 5 *and* $7, 8$. Thus at least two cannot correspond to any genera. Now the form $(1, 0, -2p)$ has the first character, and the form $(-1, 0, 2p)$ the fourth, so the second and third must be rejected. Since the character of the form $(p, 0, -2)$ relative to the number 8 is 1 *and* $3, 8$, its character relative to p can only be Rp, giving $-2Rp$.

VII. $+2$ is a residue of every prime p of the form $8n+7$, which can be proved in two ways. *First*, since I and V give $-1Np$, $-2Np$, we have $+2Rp$. *Second*, since either $\left(8, 1, \frac{1+p}{8}\right)$ or $\left(8, 3, \frac{9+p}{8}\right)$ is a properly primitive form of determinant $-p$ (according as n is even or odd), its character is Rp, and therefore $8Rp$ and $2Rp$.

VIII. Every prime p of the form $4n+1$ is a nonresidue of every odd number q that is a nonresidue of p. For if p were a residue of q, clearly there would be a properly primitive form of determinant p with character Np.

IX. Likewise, if any odd number q is a nonresidue of a prime p of the form $4n + 3$, $-p$ is a nonresidue of q; otherwise there would be a positive properly primitive form of determinant $-p$ with character Np.

X. Every prime p of the form $4n + 1$ is a residue of every other prime q that is a residue of p. If q too is of the form $4n + 1$, this follows at once from VIII; but if q is of the form $4n + 3$, $-q$ too is a residue of p (by II), and therefore pRq (by IX).

XI. If any prime q is a residue of another prime p of the form $4n + 3$, $-p$ is a residue of q. For if q is of the form $4n + 1$; VIII gives pRq, and therefore (by II) $-pRq$. But the case where q too is of the form $4n+3$ escapes this method, though it is easily settled by considering the determinant $+pq$. Of the four assignable characters for this determinant, Rp. Rq; Rp, Nq; Np, Rq; Np, Nq, two cannot correspond to any genera. Since the forms $(1, 0, -pq)$, $(-1, 0, pq)$ have respectively the first and fourth characters, the second and third cannot belong to any properly primitive form of determinant pq. Thus, since by hypothesis the character of the form $(q, 0, -p)$ relative to the number p is Rp, its character relative to q must be Rq, and therefore $-pRq$. *This proves the theorem.*

If in propositions VIII and IX q is taken to denote a prime, those propositions together with X and XI give the fundamental theorem of the preceding section.

A closer determination of the half of the characters to which no genera can correspond.

263.

Having established the fundamental theorem by a new proof, we will show how to distinguish, for any given nonsquare determinant, the half of the characters that cannot correspond to any properly primitive (positive) forms. We can do this more briefly since its basis is already contained in the investigation of Articles 147–150. Let ee be the greatest square dividing the proposed determinant D, and $D = D'ee$, so that D' contains no square factor. Further, let a, b, c etc. be all the odd prime divisors of D', so that D', apart from its sign, is either their product or twice that product. Let Ω denote the collection of individual characters Na, Nb, Nc etc. alone when $D' \equiv 1$ (mod. 4); with the character $3, 4$ adjoined when $D' \equiv 3$ and e is odd or twice an odd number; with $3, 8$ and $7, 8$ adjoined when $D' \equiv 3$ and e is divisible by four; with either the character 3 *and* $5, 8$ or the two $3, 8$ and $5, 8$ adjoined when $D' \equiv 2$ (mod. 8), according as e is odd or even; finally, with either the character 5 *and* $7, 8$ or the two $5, 8$ and $7, 8$ adjoined when $D' \equiv 6$ (mod. 8), according as e is odd or even. Then no complete character containing an odd number of the individual characters in Ω can correspond to properly primitive (positive) genera of determinant D. In all cases, individual characters expressing a relation to prime divisors of D that do not divide D' contribute nothing to the possibility or impossibility of genera. — From the theory of combinations it is very easy to see that this indeed excludes half of all assignable complete characters.

These rules are proved as follows. From the principles of the preceding section, or the theorems proved again in the preceding article, it follows without difficulty that if p is a prime (odd and positive) not dividing D and having one of the rejected characters, D' contains an odd number of factors that are nonresidues of p, so D', and therefore also D, is a nonresidue of p. It is also easy to see that a product of any number of odd numbers relatively prime to D, none of which has any rejected character, cannot have such a character either. Conversely, any positive odd number relatively prime to D that has one of the rejected characters must therefore contain a prime factor with the same property, so D is a nonresidue of that number. Thus, if

there were a properly primitive (positive) form of determinant D corresponding to a rejected character, D would be a nonresidue of every positive odd number relatively prime to it represented by such a form, which clearly cannot be reconciled with the theorem of Article 154.

For examples, compare the classifications in Articles 231, 232; anyone can increase their number at will.

264.

In this way, then, for any given nonsquare determinant all assignable characters are divided equally into two types P, Q, so that no character in Q can correspond to a properly primitive (positive) form, while for the remaining characters P, as far as we currently know, nothing prevents them from belonging to such forms. For these two types, note in particular the following proposition, which follows easily from their criterion: composing a character in P with a character in Q (by the rule of Article 246, just as if this too corresponded to a genus) gives a character in Q; but composing two characters in P. or two in Q gives a character in P. With this theorem, half of all assignable characters can also be excluded for negative and improperly primitive genera, as follows.

I. For a negative determinant D, the negative genera are completely opposite to the positive ones in this respect: no character in P belongs to a negative properly primitive genus, but all these genera have characters in Q. For when $D' \equiv 1 \pmod 4$, $-D'$ is a positive number of the form $4n+3$, so among a, b, c etc. there are an odd number of numbers of the form $4n+3$, each of which has -1 as a nonresidue. Thus in this case the complete character of the form $(-1, 0, D)$ contains an odd number of individual characters from Ω, and so belongs to Q. When $D' \equiv 3 \pmod 4$, the same reasoning shows that among a, b, c etc. there are either no numbers of the form $4n+3$, or two, or four, and so on. But since either $3, 4$ or $3, 8$ or $7, 8$ occurs in this case among the individual characters of the form $(-1, 0, D)$, its complete character also here · belongs to Q. The same conclusion follows just as easily in the remaining cases so that the negative form $(-1, 0, D)$ always has a character in Q. Since this form, composed with any other negative properly primitive form of the same determinant, produces such a positive form, clearly no negative properly primitive form can have a character in P.

II. For improperly primitive (positive) genera it is proved in the same way that the situation is either the same as for properly primitive genera or the opposite, according as $D \equiv 1$ or $\equiv 5 \pmod 8$. For in the former case we also have $D' \equiv 1 \pmod 8$, from which it follows easily that among the numbers a, b, c etc. there are either no numbers of the forms $8n+3$ and $8n+5$, or two, or four, and so on (for a product of any number of odd numbers, among which the numbers of the forms $8n+3$ and $8n+5$ together occur an odd number of times, is always either $\equiv 3$ or $\equiv 5 \pmod 8$, whereas the product of all a, b, c etc. must equal either D' or $-D'$). Thus the complete character of the form $(2, 1, \frac{1-D}{2})$ contains either no individual characters from Ω, or two, or four, and so on, and therefore belongs to P. Now every improperly primitive (positive) form of determinant D can be viewed as composed from $(2, 1, \frac{1-D}{2})$ and a properly primitive (positive) form of the same determinant, so clearly no improperly primitive (positive) form can have a character in Q in this case. In the other case. $D \equiv 5 \pmod 8$, everything is opposite: D', which is also $\equiv 5$, certainly contains an odd number of factors of the forms $8n+3$ and $8n+5$. Thus the character of the form $(2, 1, \frac{1-D}{2})$, and therefore also the character of every improperly primitive (positive) form of determinant D, belongs to Q, so no character in P can correspond to an improperly primitive positive genus.

III. Finally, for a negative determinant the negative improperly primitive genera

are again opposite to the positive improperly primitive genera: the former cannot have a character in P or in Q, according as $D \equiv 1$ or $\equiv 5 \pmod 8$, or according as $-D$ is of the form $8n+7$ or $8n+3$. This follows without difficulty from the fact that composing the form $(-1, 0, D)$, whose character is in Q, with negative improperly primitive forms of the same determinant produces positive improperly primitive forms. Thus, when characters Q are excluded from the latter, characters P must be excluded from the former, and conversely.

A special method of decomposing primes into two squares.

265.

The investigations of Articles 257, 258 into the number of ambiguous classes, on which everything above is built, give many other conclusions well worth attention, which must be omitted to keep this brief. But the following is so elegant that we cannot leave it out. For a positive determinant p that is a prime of the form $4n+1$, we showed that there is only one properly primitive ambiguous class. Thus all properly primitive ambiguous forms of such a determinant are properly equivalent. If, then, b is the positive integer immediately below $\sqrt{p}$, and $p - bb = a'$, the forms $(1, b, -a')$, $(-1, b, a')$ are properly equivalent; since both are clearly reduced, one occurs in the period of the other. Giving the former form index 0 in its period, the index of the latter must be odd (since the leading coefficients of these two forms have opposite signs); set it $= 2m+1$. Further, if the forms with indices $1, 2, 3$ etc. are respectively

$$(-a', b', a''), \quad (a'', b'', -a'''), \quad (-a''', b''', a'''') \text{ etc.}$$

then clearly the indices $2m$, $2m-1$, $2m-2$, $2m-3$ etc. correspond to the forms

$$(a', b, -1), \quad (-a'', b', a'), \quad (a''', b'', -a''), \quad (-a'''', b''', a''') \text{ etc.}$$

Thus, if the form of index m is (A, B, C), it is also $(-C, B, -A)$, so $C = -A$ and $p = BB + AA$. Consequently every prime of the form $4n+1$ can be decomposed into two squares (a proposition we derived above, in Article 182, from entirely different principles). Such a decomposition can be found by a very simple and entirely uniform method: develop the period of the reduced form whose determinant is that prime and whose leading coefficient is 1, up to a form whose outer coefficients are equal in magnitude and opposite in sign. Thus, *for example,* for $p = 233$ we have $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$, and $233 = 64 + 169$. Moreover, A must clearly be odd (since $(A, B, -A)$ must be properly primitive), and so B is even. — Since for a positive determinant p that is a prime of the form $4n+1$ the improperly primitive order too contains only one ambiguous class, clearly if g is the odd number immediately below $\sqrt{p}$, and $p - gg = 4h$, the reduced improperly primitive forms $(2, g, -2h)$, $(-2, g, 2h)$ are properly equivalent, and therefore one occurs in the period of the other. Reasoning just as above shows that the period of the form $(2, g, -2h)$ contains a form whose outer coefficients are equal in magnitude and opposite in sign, so this too gives a decomposition of the number p into two squares. The outer coefficients of this form are clearly even, and therefore its middle

coefficient odd. Since a prime can be decomposed into two squares in only one way, the form found by this second method is either $(B, \pm A, -B)$ or $(-B, \pm A, B)$. Thus in our example, for $p = 233$ we have $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$, and $233 = 169 + 64$ as above.

DIGRESSION CONTAINING A TREATMENT OF TERNARY FORMS.

266.

So far we have restricted our investigation to functions of the second degree involving *two* indeterminates, and there has been no need to give them a special name. But we can clearly regard this subject as a very special part of the most general investigation *of rational integral algebraic h o m o g e n e o u s functions of several indeterminates and various degrees*, and conveniently distinguish these functions by their degree as *forms of the second, third, fourth degree, etc.*, and by the number of indeterminates as *binary, ternary, quaternary forms*, etc. Thus the forms that we have so far called simply forms will be called *binary forms of the second degree*; functions such as

$$Axx + 2Bxy + Cyy + 2Dxz + 2Eyz + Fzz$$

where A, B, C, D, E, F denote given integers) will be called *ternary forms of the second degree*, and so on. This section is primarily devoted to binary forms of the second degree alone; but several truths concerning them, and very beautiful ones, still remain whose true source must be sought in the theory of ternary forms of the second degree. So we insert a short digression on that theory here, in which we will present, from its first elements, what is needed to complete the theory of binary forms. We hope that mathematicians will find this more welcome than if we either suppressed those truths or derived them by less natural methods. We must reserve a fuller investigation of this very important subject for another occasion, both because its richness would already take us far beyond the limits of this work, and because we hope that it will be enriched by further substantial advances in the future. Quaternary, quinary, etc. forms of the second degree, and all forms of higher degrees, are entirely excluded from our purpose here[*]. Let it be enough to draw mathematicians' attention to this vast field, in which they will find abundant material for exercising their powers and enriching higher arithmetic with outstanding advances.

267.

It will greatly help clarity to establish a fixed order among the three indeterminates entering a ternary form, just as for binary forms, so that the *first, second* and *third indeterminate* are distinguished from one another. In arranging the individual terms of a form, we will always follow this order: first comes the term involving the square of the first indeterminate, followed in turn by those involving the square of the second, the square of the third, twice the product of the second and third, twice the product of the first and third, and twice the product of the first and second. Finally, the given integers by which these squares and double products are multiplied will be called, in the same order, the *first, second, third, fourth, fifth, sixth coefficient.* Thus

$$axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

[*]For this reason, whenever we speak simply of binary or ternary forms from now on, forms *of the second degree* are always meant.

will be a ternary form in the proper order, whose first indeterminate is x, second x', third x'', first coefficient a, etc., fourth b, etc. But it will greatly shorten our notation if we do not always need to denote the indeterminates of a ternary form by special letters. So, when we disregard the indeterminates, we will also denote the same form by

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

Setting

$$\begin{array}{lll} bb - a'a'' = A, & b'b' - aa'' = A', & b''b'' - aa' = A'' \\ ab - b'b'' = B, & a'b' - bb'' = B', & a''b'' - bb' = B'' \end{array}$$

gives another form

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \dots F$$

which we will call the *adjoint of the form*

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \dots f$$

We then find, denoting for brevity the number

$$abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b'' \quad \text{by} \quad D$$

$$\begin{array}{lll} BB - A'A'' = aD, & B'B' - AA'' = a'D, & B''B'' - AA' = a''D \\ AB - B'B'' = bD, & A'B' - BB'' = b'D, & A''B'' - BB' = b''D \end{array}$$

This shows that the adjoint of the form F is the form

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}$$

The number D, on whose nature the properties of the ternary form f chiefly depend, will be called the *determinant* of this form. In this way the determinant of the form F becomes $= DD$, or equal to the square of the determinant of the form f, of which it is the adjoint.

Thus, *for example*, the ternary form $\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix}$ has the adjoint $\begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{pmatrix}$, and the determinant of each $= 1$.

Ternary forms of determinant 0 will be entirely excluded from the following investigation, since, as will be shown in the theory of ternary forms to be presented more fully on another occasion, they are ternary only *in appearance* and are in fact equivalent to binary forms.

268.

If a ternary form f of determinant D, whose indeterminates are x, x', x'' (the first $= x$, etc.), is transformed into a ternary form g of determinant E, whose indeterminates are y, y', y'', by a substitution of the form

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'' \\ x' &= \alpha' y + \beta' y' + \gamma' y'' \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \end{aligned}$$

where all nine coefficients α, β, etc. are assumed to be integers, then, for brevity, omitting the indeterminates, we will simply say that f passes into g by the substitution (S)

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

and that f *contains* g, or that g *is contained in* f. This assumption immediately gives six equations for the six coefficients in g, which we need not write down. An easy calculation then gives the following conclusions:

I. Denoting for brevity the number

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'' \quad \text{by } k$$

we find, after the necessary reductions, $E = kkD$. Thus D divides E, and the quotient is a square. So the number k plays a role in transformations of ternary forms similar to that of the number $\alpha\delta - \beta\gamma$ in Article 157 for transformations of binary forms: it is a square root of the quotient of the determinants. We might therefore conjecture that the difference in the sign of k also establishes here an essential distinction between proper and improper transformations and containments. But on looking more closely, it is clear. f also passes into g by the substitution

$$\begin{matrix} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma'' \end{matrix}$$

and in the value of k, replacing α by $-\alpha$, β by $-\beta$, etc. gives $-k$. So this substitution would be dissimilar to the substitution S, and every ternary form containing another in one way would also contain it in the other. Such a distinction, being of no use for ternary forms, will therefore be entirely ruled out here.

II. Denoting by F, G the adjoints of f, g, respectively, the coefficients in F are determined by the coefficients in f, and the coefficients in G by the values of the coefficients of the form g, known from the equations supplied by the substitution S. Expressing the coefficients of the form f by letters and comparing the values of the coefficients of the forms F, G, we readily confirm that F contains the form G and is transformed into it by the substitution (S')

$$\begin{matrix} \beta'\gamma'' - \beta''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\beta'' - \alpha''\beta' \\ \beta''\gamma - \beta\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\beta - \alpha\beta'' \\ \beta\gamma' - \beta'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\beta' - \alpha'\beta \end{matrix}$$

We omit the calculation itself, which presents no difficulties.

III. The form g is, by the substitution (S'')

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \beta''\gamma - \beta\gamma'', & \beta\gamma' - \beta'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\beta'' - \alpha''\beta', & \alpha''\beta - \alpha\beta'', & \alpha\beta' - \alpha'\beta \end{array}$$

clearly transformed into the same form into which f passes by

$$\begin{array}{lll} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{array}$$

that is, into the form obtained by multiplying each coefficient of the form f by kk. We will denote this form by f'.

IV. In exactly the same way it is proved that the form G, by the substitution (S''')

$$\begin{array}{lll} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{array}$$

passes into the form obtained from F by multiplying each coefficient by kk. We will denote this form by F'.

We will say that the substitution S''' arises *by transposing* the substitution S. Clearly, S then arises in turn by transposing the substitution S''', and S', S'' each by transposing the other. — The substitution S' can conveniently be called the *adjoint* of the substitution S, so the adjoint of the substitution S''' will be S''.

269.

If not only the form f contains g, but also the latter contains the former, the forms f, g will be called *equivalent*. In this case not only will D divide E, but E will also divide D, from which we easily conclude that $D = E$ must hold. Conversely, if a form f contains a form g of the same determinant, these two forms will be equivalent. For (using the same notation as in the preceding article and excluding the case where $D = 0$) we will have $k = \pm 1$, and so the form f'. into which g passes by the substitution S'', is identical to f, or f is contained in g. It is also clear that in this case the forms F, G, adjoints of f, g, will be equivalent to each other, and the latter will pass into the former by the substitution S'''. Finally, conversely, if the forms F, G are *assumed* equivalent, and the former passes into the latter by the substitution T, the forms f, g will also be equivalent: f will pass into g by the adjoint of the substitution T, and g into f by the transpose of the substitution T. For by these two substitutions, respectively, the adjoint of F passes into the adjoint of G, and the latter into the former. But these two forms are obtained from f, g by multiplying each coefficient by D, so we readily conclude that, by the same substitutions, f passes into g. and g into f, respectively.

270.

If a ternary form f contains a ternary form f', and the latter a form f'': then f will also contain f''. For it is very easy to see that if the following transformations hold:

f into f' by substitution	f' into f'' by 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 will be transformed by the substitution

$$\begin{array}{lll} \alpha\delta+\beta\delta'+\gamma\delta'', & \alpha\varepsilon+\beta\varepsilon'+\gamma\varepsilon'', & \alpha\zeta+\beta\zeta'+\gamma\zeta'' \\ \alpha'\delta+\beta'\delta'+\gamma'\delta'', & \alpha'\varepsilon+\beta'\varepsilon'+\gamma'\varepsilon'', & \alpha'\zeta+\beta'\zeta'+\gamma'\zeta'' \\ \alpha''\delta+\beta''\delta'+\gamma''\delta'', & \alpha''\varepsilon+\beta''\varepsilon'+\gamma''\varepsilon'', & \alpha''\zeta+\beta''\zeta'+\gamma''\zeta'' \end{array}$$

Thus, in the case where f is equivalent to f', and f' to f'', the form f will also be equivalent to the form f''. — It is also immediately clear how these theorems are to be applied to more forms.

271.

It is now clear that all ternary forms, just like binary forms, can be divided into *classes*, assigning equivalent forms to the same class and inequivalent forms to different classes. Forms with different determinants will therefore certainly belong to different classes, so there will be infinitely many classes of ternary forms. Ternary forms with the same determinant, however, make up sometimes fewer and sometimes more classes. But the outstanding property of these forms is that *all forms with the same given determinant always make up a finite number of classes.* Before developing this very important theorem more fully, we must describe the following essential distinction among ternary forms.

Some ternary forms are such that both positive and negative numbers can be represented by them without distinction, *for example* the form $xx + yy - zz$. They will therefore be called *indefinite forms.* By others, on the contrary, negative numbers cannot be represented, but only positive ones (apart from zero, obtained by setting each indeterminate $= 0$), as with $xx + yy + zz$, so they will be called *positive forms.* Finally, by others positive numbers cannot be represented, as with $-xx - yy - zz$, so they will be called *negative forms.* Positive and negative forms will be given the common name *definite forms.* Here are general criteria by which these properties of forms can be distinguished.

Multiplying the ternary form

$$f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

of determinant D by a, and denoting the coefficients of the adjoint of f, as in Article 267, by A, A', A'', B, B', B'', gives

$$(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = g$$

Multiplying again by A' gives

$$A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'x' = h$$

From this we immediately conclude that if both A' and aD are negative numbers, all values of h are negative. Clearly, then, the form f can represent only numbers whose sign is opposite to that of aA', *that is*, the same as that of a, or opposite to that of D. In this case, therefore, f will be a definite form, positive or negative according as a is positive or negative, or according as D is negative or positive.

If, however, either both aD, A' are positive, or one is positive and the other negative (neither $= 0$), it is easy to see that h can take both positive and negative values by a suitable choice of the quantities x, x', x''. In this case, then, f can take values with both the same sign as aA' and the opposite sign, and so it will be an indefinite form.

In the case where $A' = 0$, but not $a = 0$, we have

$$g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2Bx'')$$

Giving x' an arbitrary value (but not $= 0$), and taking x'' so that $\frac{A''x'}{2B} - x''$ has the same sign as Bx' (which is easily seen to be possible, since B cannot be $= 0$, as

this would give $BB - A'A'' = aD = 0$, and therefore also $D = 0$, a case we exclude), makes $x'(A''x' - 2Bx'')$ a positive quantity. It is then easy to see that x can be chosen so that g takes a negative value. Clearly these values can also be chosen so that, if desired, they are all integers. Finally, it is clear that whatever values are assigned to x', x'', x can be taken so large that g becomes positive. We conclude that in this case the form f is indefinite. Finally, if $a = 0$, we will have

$$f = a'x'x' + 2bx'x'' + a''x''x'' + 2x(b''x' + b'x'')$$

Taking x', x'' arbitrarily, but so that $b''x' + b'x''$ is not $= 0$ (which is clearly possible unless both b' and b'' are $= 0$; but then we would have $D = 0$), we readily see that x can be chosen so that f takes both positive and negative values. So in this case too f will be an indefinite form.

Just as here we have used the numbers aD, A' to judge the nature of the form f, we can also use aD and A'': f is a definite form if both aD and A'' are negative, and indefinite in every other case. In exactly the same way, considering the numbers $a'D$ and A, or $a'D$ and A'', or $a''D$ and A, or finally $a''D$ and A', can serve the same purpose.

From all this it follows that in a definite form the six numbers A, A', A'', aD, $a'D$, $a''D$ are negative. In a positive form, a, a', a'' will be positive and D negative; in a negative form, a, a', a'' will be negative and D positive. Thus all ternary forms with a given positive determinant fall into negative and indefinite forms, and all those with a negative determinant into positive and indefinite forms. Finally, there are no positive forms with a positive determinant, or negative forms with a negative determinant. — From the same considerations it is easy to see that the adjoint of a definite form is always definite, and indeed *negative*, while the adjoint of an indefinite form is indefinite.

Since all numbers representable by a given ternary form can clearly also be represented by every form equivalent to it, the ternary forms contained in the same class will either all be indefinite, all positive, or all negative. We may therefore extend these names of forms to entire classes as well.

272.

We will treat the theorem proposed in the preceding article, that all ternary forms of a given determinant fall into a *finite* number of classes, by a method similar to the one we used for binary forms. We will first show how any ternary form can be reduced to a simpler form, and then that for any given determinant there are only finitely many simplest forms (reached by such reductions). Suppose in general that a ternary form $f = \left(\begin{smallmatrix} a,\ a',\ a'' \\ b,\ b',\ b'' \end{smallmatrix}\right)$ of determinant D (different from zero) passes, by the substitution (S)

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

into an equivalent form $g = \left(\begin{smallmatrix} m,\ m',\ m'' \\ n,\ n',\ n'' \end{smallmatrix}\right)$. Our task will be to determine α, β, γ, etc. so that the form g becomes simpler than f. Let the adjoints of f, g be, respectively, $\left(\begin{smallmatrix} A,\ A',\ A'' \\ B,\ B',\ B'' \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} M,\ M',\ M'' \\ N,\ N',\ N'' \end{smallmatrix}\right)$. denoted by F, G. Then by Article 269, F will pass into G by the adjoint of the substitution S, and G into F by the substitution obtained by transposing S. The number

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma''$$

which must be either $= +1$ or $= -1$, will be denoted by k. With this understood, we observe:

I. If we set $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, we will have

$$\begin{aligned} m &= a\alpha\alpha + 2b''\alpha\alpha' + a'\alpha'\alpha', \\ m' &= a\beta\beta + 2b''\beta\beta' + a'\beta'\beta', \\ m'' &= a'' \\ n &= b\beta' + b'\beta, \\ n' &= b\alpha' + b'\alpha, \\ n'' &= a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta' \end{aligned}$$

Also, $\alpha\beta' - \beta\alpha'$ must be either $= +1$ or $= -1$. It is clear from this that the binary form (a, b'', a'), whose determinant is A'', is transformed by the substitution α, β, α', β' into the binary form (m, n'', m') of determinant M'', and is therefore equivalent to it, because $\alpha\beta' - \beta\alpha' = \pm 1$. Thus $M'' = A''$, which is also easily confirmed directly. So unless (a, b'', a') is already a simplest form in its class, we may choose α, β, α', β' so that (m, n'', m') is a simpler form. Indeed, the theory of equivalence of binary forms readily shows that this can be done so that m is no greater than $\sqrt{-\frac{4}{3}A''}$ if A'' is negative, or no greater than $\sqrt{A''}$ if A'' is positive, or $m = 0$ if $A'' = 0$. Thus in every case the (absolute) value of m can certainly be lowered below, or at least as far as, $\sqrt{\pm\frac{4}{3}A''}$. In this way the form f is reduced to another with a smaller first coefficient, if possible, and whose adjoint has the same third coefficient as the form F adjoint to f. This is the *first reduction*.

II. If, however, we set $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, we will have $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$. So the adjoint of the substitution S will be

$$\begin{array}{rrr} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta' \end{array}$$

by which F will pass into G. We will therefore have

$$\begin{aligned} m &= a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\beta'' + b''\beta' \\ m' &= a'\beta'\beta' + 2b\beta'\beta'' + a''\beta''\beta'' \\ m'' &= a'\gamma'\gamma' + 2b\gamma'\gamma'' + a''\gamma''\gamma'' \\ n &= a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'' \\ M' &= A'\gamma''\gamma'' - 2B\gamma'\gamma'' + A''\gamma'\gamma' \\ N &= -A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma' \\ M'' &= A'\beta''\beta'' - 2B\beta'\beta'' + A''\beta'\beta' \end{aligned}$$

It follows that the binary form (A'', B, A'), whose determinant is Da, passes by the substitution β', $-\gamma'$, $-\beta''$, γ'' into the form (M'', N, M') of determinant Dm, and so is equivalent to it (because $\beta'\gamma'' - \gamma'\beta'' = \pm 1$, or because $Da = Dm$). So unless (A'', B, A') is already a simplest form in its class, the coefficients β', γ', β'', γ'' can be chosen so that $(M''. N, M')$ is simpler. This can always be done so that M'', without regard to sign, is no greater than $\sqrt{\pm\frac{4}{3}Da}$. In this way the form f is reduced to another with the same first coefficient, but whose adjoint has, if possible, a smaller third coefficient than the form F adjoint to f. This is the *second reduction.*

III. Thus if f is a ternary form to which neither the first nor the second reduction is applicable, *that is*, which cannot be transformed into a simpler form by either: we must have both $aa <$ or $= \frac{4}{3}A''$, and $A''A'' <$ or $= \frac{4}{3}aD$, without regard to sign. Hence a^4 will be $<$ or $= \frac{16}{9}A''A''$, and so $a^4 <$ or $= \frac{64}{27}aD$, $a^3 <$ or $= \frac{64}{27}D$, and $a <$ or $= \frac{4}{3}\sqrt[3]{D}$; from this again $A''A'' <$ or $= \frac{16}{9}\sqrt[3]{D^4}$, and $A'' <$ or $= \frac{4}{3}\sqrt[3]{D^2}$. So as long as a or A'' still exceeds these bounds, one or the other of the preceding reductions must be applicable to the form f. — This conclusion must not be reversed, however, since it quite often happens that a ternary form whose first coefficient, and the third coefficient of its adjoint, are already below those bounds can nevertheless be made still simpler by one or the other reduction.

IV. If the first and second reductions are applied alternately to any given ternary form of determinant D, *that is*, the first or second to the form itself, the second or first to the resulting form, again the first or second to the next resulting form, etc., then clearly we must eventually reach a form to which neither can be applied any further. For the absolute magnitudes both of the first coefficients of the forms obtained in this way and of the third coefficients of their adjoints continually alternate between staying the same and decreasing. This process must eventually end somewhere, since

otherwise there would be two infinite sequences of continually decreasing numbers. We have now obtained a remarkable theorem: *Every ternary form of determinant D can be reduced to an equivalent form whose first coefficient is no greater than $\frac{4}{3}\sqrt[3]{D}$, and the third coefficient of its adjoint no greater than $\frac{4}{3}\sqrt[3]{D^2}$, without regard to sign, if the given form does not already have these properties.* — Instead of the first coefficient of the form f and the third of the adjoint of f, we could have treated in exactly the same way either the first coefficient of the form itself and the second of its adjoint; or the second of the form itself and the first or third of its adjoint; or the third of the form itself and the first or second of its adjoint. Each of these routes would equally have led us to our intended goal. But it is useful to keep consistently to one method, so that the operations involved can more easily be reduced to a fixed algorithm. Finally, we observe that for the two coefficients which we have shown how to lower below fixed bounds. still smaller bounds can be established if definite forms are separated from indefinite ones; this is not needed for our present purpose.

273.

Here are some examples to illustrate the preceding rules more fully.

Example 1. Let $f = \left(\begin{smallmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{smallmatrix}\right)$; then $F = \left(\begin{smallmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{smallmatrix}\right)$, $D = -1$. Since $(19, 1, 21)$ is a reduced binary form to which no other form with a first coefficient smaller than 19 is equivalent, the first reduction is not applicable here. But the theory of equivalence of binary forms shows that the binary form $(A'', B, A') = (-398, 257, -166)$ can be transformed into the simpler equivalent form $(-2, 1, -10)$, into which it passes by the substitution $2, 7, 3, 11$. So, setting $\beta' = 2$, $\gamma' = -7$, $\beta'' = -3$, $\gamma'' = 11$, we must apply to the form f the substitution $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11 \end{smallmatrix}\right\}$, by which it is found to pass into $\left(\begin{smallmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{smallmatrix}\right) \ldots f'$. The third coefficient of the adjoint of this form is -2, so in this respect f' must be regarded as simpler than f.

The first reduction can be applied to the form f'. For since the binary form $(19, -82, 354)$ is transformed into $(1, 0, 2)$ by the substitution $13, 4, 3, 1$: we must apply to the form f' the substitution $\left\{\begin{smallmatrix} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$, by which it passes into $\left(\begin{smallmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{smallmatrix}\right) \ldots f''$.

The second reduction can again be applied to the form f'', whose adjoint is $\left(\begin{smallmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{smallmatrix}\right)$. For $(-2, -95, -4513)$ passes by the substitution $47, 1, -1, 0$ into $(-1, 1, -2)$: so we must apply to f'' the substitution $\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0 \end{smallmatrix}\right\}$, by which it passes into $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right) \ldots f'''$. Its first coefficient cannot be decreased any further by the first reduction, nor can the third coefficient of its adjoint by the second.

Example 2. Let the given form be $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right) \ldots f$, whose adjoint is $\left(\begin{smallmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{smallmatrix}\right)$ and whose determinant = 2. Applying the second and first reductions alternately gives, in succession,

substitutions	take	into
$\left\{\begin{smallmatrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{smallmatrix}\right\}$	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'''	$\left(\begin{smallmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{smallmatrix}\right) = f''''$

The form f'''' cannot be reduced any further by the first or second reduction.

274.

When we have a ternary form whose first coefficient, and the third coefficient of its adjoint, have been lowered as far as possible by the preceding methods: the following method gives a further reduction.

Using the same notation as in Article 272, and setting $\alpha = 1$, $\alpha' = 0$, $\beta' = 1$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, *that is*, using the substitution

$$\begin{matrix} 1, & \beta, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1 \end{matrix}$$

we have

$$\begin{aligned} m &= a, \quad m' = a' + 2b''\beta + a\beta\beta, \\ m'' &= a'' + 2b\gamma' + 2b'\gamma + a\gamma\gamma + 2b''\gamma\gamma' + a'\gamma'\gamma' \\ n &= b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma, \\ n' &= b' + a\gamma + b''\gamma', \quad n'' = b'' + a\beta \end{aligned}$$

and also

$$M'' = A'', \quad N = B - A''\gamma', \quad N' = B' - N\beta - A''\gamma$$

Thus a substitution of this kind leaves unchanged the coefficients a, A'' which were decreased by the preceding reductions. Our task is therefore to obtain decreases in the remaining coefficients by a suitable choice of β, γ, γ'. For this purpose we first observe that if $A'' = 0$, we may assume that $a = 0$ as well. For if a is not $= 0$, the first reduction could still be applied once more, since every binary form of determinant 0 is equivalent to a form such as $(0, 0, h)$, or one whose first coefficient $= 0$ (see Article 215). In exactly the same way we may assume that $A'' = 0$ as well if $a = 0$, so that either neither of the numbers a, A'' is 0, or both are.

In the first case it is clear that β, γ, γ' can be chosen so that, without regard to sign, n'', N, N' are no greater, respectively, than $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$. Thus in the first example of the preceding article, the last form $\left(\begin{smallmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{smallmatrix}\right)$, whose adjoint is $\left(\begin{smallmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{smallmatrix}\right)$, passes by the substitution $\left\{\begin{smallmatrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$ into $\left(\begin{smallmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{smallmatrix}\right) \ldots f''''$, whose adjoint is $\left(\begin{smallmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$.

In the second case, where $a = A'' = 0$, and therefore also $b'' = 0$, we have

$$\begin{aligned} m &= 0, \quad m' = a', \quad m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'\gamma' \\ n &= b + a'\gamma' + b'\beta, \quad n' = b', \quad n'' = 0 \end{aligned}$$

So we will have

$$D = a'b'b' = m'n'n'$$

and it is easy to see that β and γ' can be chosen so that n equals the residue of b of smallest absolute value modulo the greatest common divisor of a', b'; that is, so that n is no greater than half this divisor without regard to sign, and hence $n = 0$ whenever a', b' are coprime. Having determined β, γ' in this way, we can choose the

value of γ so that m'' is no greater than b', without regard to sign. This would indeed be impossible if $b' = 0$, but then we would have $D = 0$, a case we have excluded. Thus for the last form in *Example* 2 of the preceding article we obtain $n = -2 - \beta + 2\gamma'$, so setting $\beta = -2$, $\gamma' = 0$ gives $n = 0$. Further, $m'' = 2 - 2\gamma$, and setting $\gamma = 1$ gives $m'' = 0$. We therefore have the substitution $\left\{\begin{smallmatrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{smallmatrix}\right\}$, by which that form passes into $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right) \ldots f''''''$.

275.

Suppose we have a sequence of equivalent ternary forms f, f', f'', f''', etc., and transformations of each of these forms into the next. From the transformations of the form f into f', and of the form f' into f'', Article 270 gives a transformation of the form f into f''. From this and the transformation of the form f'' into f''' follows a transformation of the form f into f''', etc. Clearly, in this way a transformation of the form f into any other in the sequence can be found. And since a transformation of the form f into any other equivalent form g gives a transformation of the form g into f (S'' from S, Articles 268, 269), we can in this way obtain a transformation of any form in the sequence f', f'', etc. into the first, f. — Thus for the forms in the first example of the preceding article we find the substitutions

$$\begin{array}{rrr|rrr|rrr} 13, & 4, & 0 & 13, & 188, & -4 & 13, & -20, & 16 \\ 6, & 2, & -7 & 6, & 87, & -2 & 6, & -9, & 7 \\ -9, & -3, & 11 & -9, & -130, & 3 & -9, & 14, & -11 \end{array}$$

by which f passes into f'', f''', f'''', respectively, and from the last substitution we obtain $\left\{\begin{smallmatrix} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3 \end{smallmatrix}\right\}$, by which f'''' passes into f. Similarly, for *Example* 2 of the preceding article, we obtain the substitutions

$$\begin{array}{rrr|rrr} 1, & -1, & 1 & 2, & -3, & -1 \\ -3, & 4, & -3 & 3, & 1, & 0 \\ 10, & -14, & 11 & 2, & 4, & 1 \end{array}$$

by which, respectively, the form $\left(\begin{smallmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{smallmatrix}\right)$ passes into $\left(\begin{smallmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{smallmatrix}\right)$, and the latter into the former.

276.

THEOREM. *The number of classes into which all ternary forms of a given determinant are divided is always finite.*

Proof. I. The number of all forms $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ of a given determinant D in which $a = 0$, $b'' = 0$, b is no greater than half the greatest common divisor of the numbers a', b'; and a'' no greater than b', is clearly finite. For since we must have $a'b'b' = D$, the only possible values of b' are $+1$, -1 and the roots, with positive and negative signs, of the squares dividing D (if there are any others besides 1). There are finitely many such values. For each value of b', however, the value of a' is determined, and the values of b, a'' are clearly limited to finitely many possibilities.

II. Similarly, there are finitely many forms $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ of determinant D in which a is not $= 0$ and is no greater than $\frac{4}{3}\sqrt[3]{\pm D}$; $b''b'' - aa' = A''$ is not $= 0$ and is no greater than $\frac{4}{3}\sqrt[3]{D^2}$; b'' is no greater than $\frac{1}{2}a$; and $ab - b'b'' = B$ and $a'b' - bb'' = B'$ are no greater than $\frac{1}{2}A''$. For the number of all combinations of values of a, b'', A'', B, B' will be finite. Once these are individually determined, the remaining coefficients of the form, a', b, b', a'', and the coefficients of its adjoint

$$bb - a'a'' = A, \quad b'b' - aa'' = A', \quad a''b'' - bb' = B''$$

will also be determined by the following equations:

$$\begin{aligned}
a' &= \frac{b''b'' - A''}{a}, \quad A' = \frac{BB - aD}{A''}, \\
A &= \frac{B'B' - a'D}{A''}, \quad B'' = \frac{BB' + b''D}{A''} \\
b &= \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, \\
b' &= \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''} \\
a'' &= \frac{b'b' - A'}{a} = \frac{bb - A}{a'} = \frac{bb' + B''}{b''}
\end{aligned}$$

Now all those forms are obtained by choosing, from all combinations of values of a, b'', A'', B, B', those for which a', a'', b, b' also take integer values, so their number is clearly finite.

III. All the forms in I and II therefore constitute finitely many classes. There may even be fewer classes than forms if some of the forms are equivalent to one another. Now by the preceding investigations every ternary form of determinant D must be equivalent to one of those forms, *that is*, belong to one of the classes which they constitute: these classes will therefore contain all forms of determinant D, *that is*, all ternary forms of determinant D will be divided into finitely many classes. *Q.E.D.*

277.

The rules for finding all the forms in I and II of the preceding article follow directly from their description, so a few examples will be enough. For $D = 1$, the choices of signs give these six forms I.

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$$

In forms II, a and A'' can have no values other than $+1$ and -1. For each of the four resulting combinations, b'', B and B' must be set $= 0$, giving four forms

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

Similarly, for $D = -1$ we have six forms I and four forms II,

$$\begin{pmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & -1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}; \quad \begin{pmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} -1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$$

For $D = 2$ we obtain six forms I

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$$

and eight forms II

$$\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

The number of classes arising from these forms in these three cases is, however, much smaller than the number of forms. For it is easily confirmed:

I. The form $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ passes into

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

by the respective substitutions

$$\begin{array}{ccc|ccc|ccc|ccc} 1, & 0, & 0 & 0, & 0, & 1 & 0, & 0, & 1 & 1, & 0, & -1 \\ 0, & 1, & 0 & 0, & 1, & -1 & 0, & 1, & 1 & 1, & 1, & -1 \\ 0, & 0, & -1 & \pm 1, & 1, & 0 & \pm 1, & -1, & -1 & 0, & -1, & 1 \end{array}$$

while the form $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ passes into $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ merely by permuting the indeterminates. Thus those ten ternary forms of determinant 1 reduce to these two $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$; instead of the first, if preferred, we can also take $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Since the former form is indefinite and the latter definite, it is clear that every indefinite ternary form of determinant 1 is equivalent to the form $xx + 2yz$, and every definite one to $-xx - yy - zz$.

II. In exactly the same way we find that every indefinite ternary form of determinant -1 is equivalent to the form $-xx+2yz$, and every definite one to $xx+yy+zz$.

III. For determinant 2, the second, sixth and seventh of the eight forms (II) can be discarded immediately, since they arise from the first merely by permuting the indeterminates. For the same reason we can also discard the fifth, which arises in this way from the third, and the eighth, which arises from the fourth. The three remaining forms, together with the six forms I, constitute three classes. For $\left(\begin{smallmatrix}0,&2,&0\\0,&1,&0\end{smallmatrix}\right)$ passes into $\left(\begin{smallmatrix}0,&2,&0\\0,&-1,&0\end{smallmatrix}\right)$ by the substitution $\left\{\begin{smallmatrix}1,&0,&0\\0,&1,&0\\0,&0,&-1\end{smallmatrix}\right\}$, and the form $\left(\begin{smallmatrix}1,&1,&-2\\0,&0,&0\end{smallmatrix}\right)$ into

$$\left(\begin{smallmatrix}0,&2,&1\\0,&1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}0,&2,&1\\0,&-1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}0,&2,&-1\\0,&1,&0\end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix}0,&2,&-1\\0,&-1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}1,&-1,&2\\0,&0,&0\end{smallmatrix}\right)$$

by the respective substitutions

$$\begin{array}{ccc|ccc|ccc|ccc|ccc}
1, & 0, & 1 & 1, & 0, & -1 & 1, & 0, & 0 & 1, & 0, & 0 & 1, & 0, & 0\\
1, & 2, & 0 & 1, & 2, & 0 & 1, & 2, & -1 & 1, & 2, & 1 & 0, & 1, & 2\\
1, & 1, & 0 & 1, & 1, & 0 & 1, & 1, & -1 & 1, & 1, & 1 & 0, & 1, & 1
\end{array}$$

Thus every ternary form of determinant 2 can be reduced to one of these three

$$\left(\begin{smallmatrix}0,&2,&0\\0,&-1,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}1,&1,&-2\\0,&0,&0\end{smallmatrix}\right),\quad \left(\begin{smallmatrix}-1,&-1,&-2\\0,&0,&0\end{smallmatrix}\right)$$

Instead of the first, if preferred, we can also take $\left(\begin{smallmatrix}2,&0,&0\\1,&0,&0\end{smallmatrix}\right)$. Clearly every definite ternary form must be equivalent to the third, $-xx-yy-2zz$, since the first two are indefinite. Every indefinite form is equivalent to the first or second: to the first, $2xx+2yz$, if its first, second and third coefficients are all even (since it is easy to see that any substitution takes such a form into a form of the same kind, so it cannot be equivalent to the second form); but to the second, $xx+yy-2zz$, if its first, second and third coefficients are not all even, but one, two or all are odd (for the same reason, the first form $2xx+2yz$ cannot be transformed into such a form by any substitution). So what happened in the examples of Articles 273, 274, namely that the definite form $\left(\begin{smallmatrix}19,&21,&50\\15,&28,&1\end{smallmatrix}\right)$ of determinant -1 reduced to $xx+yy+zz$, and the indefinite form $\left(\begin{smallmatrix}10,&26,&2\\7,&0,&4\end{smallmatrix}\right)$ of determinant 2 to $2xx-2yz$, or, which amounts to the same thing, to $2xx+2yz$, could have been predicted in advance from the preceding investigations.

278.

A ternary form with indeterminates x, x', x'' *represents* both numbers, by assigning specific values to x, x', x'', and binary forms, by substitutions of the kind

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

where m, n, m', etc. denote fixed numbers, and t, u the indeterminates of the represented form. A complete theory of ternary forms would therefore require solutions to the following problems: I. Find all representations of a given number by a given ternary form. II. Find all representations of a given binary form by a given ternary form. III. Decide whether two given ternary forms of the same determinant are equivalent, and if they are, find all transformations of one into the other. IV. Decide whether a given ternary form contains another given form of larger determinant, and if it does, find all transformations of the former into the latter. We will discuss these problems, which are much more difficult than the analogous problems for binary forms, more fully elsewhere. Here we restrict our investigation to showing how the first problem can be reduced to the second, and the second to the third. We will show how to solve the third in some very simple cases that shed particular light on the theory of binary forms. We exclude the fourth entirely here.

279.

Lemma. *Given any three integers a, a', a'' (not all $= 0$): find six others B, B', B'', C, C', C'' such that*

$$B'C'' - B''C' = a, \qquad B''C - BC'' = a', \qquad BC' - B'C = a''$$

Solution. Let α be the greatest common divisor of a, a', a''. and choose integers A, A', A'' so that

$$Aa + A'a' + A''a'' = \alpha$$

Next choose three integers $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ arbitrarily, with the sole condition that the three numbers $\mathfrak{C}'A'' - \mathfrak{C}''A'$, $\mathfrak{C}''A - \mathfrak{C}A''$, $\mathfrak{C}A' - \mathfrak{C}'A$, which we will denote, respectively, by b, b', b'', and their greatest common divisor by β, are not all $= 0$. Then set

$$a'b'' - a''b' = \alpha\beta C, \qquad a''b - ab'' = \alpha\beta C', \qquad ab' - a'b = \alpha\beta C''$$

Clearly C, C', C'' will be integers. Finally, choose integers $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ so that

$$\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta$$

put

$$\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = h$$

and set

$$B = \alpha\mathfrak{B} - hA, \qquad B' = \alpha\mathfrak{B}' - hA', \qquad B'' = \alpha\mathfrak{B}'' - hA''$$

These values of B, B', B'', C, C', C'' will satisfy the required equations.

For we find

$$aB + a'B' + a''B'' = 0$$
$$bA + b'A' + b''A'' = 0 \quad \text{so} \quad bB + b'B' + b''B'' = \alpha\beta$$

Now the values of C', C'' give

$$\begin{aligned}\alpha\beta(B'C'' - B''C') &= ab'B' - a'bB' - a''bB'' + ab''B'' \\ &= a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\beta a\end{aligned}$$

and hence $B'C'' - B''C' = a$; similarly we find $B''C - BC'' = a'$, $BC' - B'C = a''$. *Q.E.F.* — We must omit here the analysis by which this solution was found, as well as the method for finding all solutions from one.

280.

Suppose that the binary form

$$att + 2btu + cuu \ldots \varphi$$

whose determinant $= D$, is represented by the ternary form f, with indeterminates x, x', x'', by setting

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

and that f has the adjoint form F, with indeterminates X, X', X''. Then a calculation readily confirms (if we use separate letters for the coefficients of the forms f, F), or Article 268. II. directly shows, that the number D is represented by F on setting

$$X = m'n'' - m''n', \qquad X' = m''n - mn'', \qquad X'' = mn' - m'n$$

This representation of the number D can conveniently be called *adjoint* to the representation of the form φ by f. If the values of X, X', X'' have no common divisor, we will, for brevity, call this representation of D *proper*; otherwise, *improper*. We will give the same names to the representation of the form φ by f to which that representation of D is adjoint. Finding all proper representations of the number D by the form F now rests on the following points:

I. Every representation of D by F can be derived from some representation of some form of determinant D by the form f, *i.e.*, is adjoint to such a representation.

For let any representation of D by F be given by $X = L$, $X' = L'$, $X'' = L''$. By the lemma in the preceding article, choose m, m', m'', n, n', n'' so that

$$m'n'' - m''n' = L, \qquad m''n - mn'' = L', \qquad mn' - m'n = L''$$

and let f be transformed by the substitution

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

into the binary form $\varphi = att + 2btu + cuu$. It is then easy to see that D will be the determinant of the form φ, and that its representation by f will have the proposed representation of D by F as its adjoint.

Example. Let $f = xx + x'x' + x''x''$, so that $F = -XX - X'X' - X''X''$; let $D = -209$, with the representation by F given by $X = 1$, $X' = 8$, $X'' = 12$. This gives m, m', m'', n, n', n'' the values $-20, 1, 1, -12, 0, 1$, respectively, and gives $\varphi = 402tt + 482tu + 145uu$.

II. If φ, χ are properly equivalent binary forms, every representation of D by F that is adjoint to some representation of the form φ by f will also be adjoint to some representation of the form χ by f.

Let p, q be the indeterminates of the form χ; let φ be transformed into χ by the proper substitution $t = \alpha p + \beta q$, $u = \gamma p + \delta q$, and let some representation of the form φ by f be given by

$$x = mt + nu, \qquad x' = m't + n'u, \qquad x'' = m''t + n''u \ldots (R)$$

It is then easy to see that, if we set

$$\begin{array}{lll} \alpha m+\gamma n=g, & \alpha m'+\gamma n'=g', & \alpha m''+\gamma n''=g'' \\ \beta m+\delta n=h, & \beta m'+\delta n'=h', & \beta m''+\delta n''=h'' \end{array}$$

the form χ will be represented by f on setting

$$x=gp+hq, \qquad x'=g'p+h'q, \qquad x''=g''p+h''q \ldots (R')$$

and a calculation gives (since $\alpha\delta-\beta\gamma=1$)

$$g'h''-g''h'=m'n''-m''n', \quad g''h-gh''=m''n-mn'', \quad gh'-g'h=mn'-m'n$$

i.e., the representations R, R' have the same representation of D by F as their adjoint.

Thus, in the preceding example, the form φ is found to be equivalent to $\chi = 13pp-10pq+18qq$, into which it is transformed by the proper substitution $t=-3p+q$, $u=5p-2q$. This gives the representation of the form χ by f as $x=4q$, $x'=-3p+q$, $x''=2p-q$, from which we obtain the same representation of the number -209 that we started with.

III. Finally, suppose that two binary forms φ, χ of determinant D, with indeterminates t, u; p, q, can be represented by f, and that the same proper representation of D by F is adjoint to some representation of one and to some representation of the other. Then these forms must be properly equivalent. Suppose that φ is represented by f on setting

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

and χ on setting

$$x=gp+hq. \qquad x'=g'p+h'q, \qquad x''=g''p+h''q$$

and that

$$\begin{array}{c} m'n''-m''n'=g'h''-g''h'=L \\ m''n-mn''=g''h-gh''=L' \\ mn'-m'n=gh'-g'h=L'' \end{array}$$

Choose integers l, l', l'' so that $Ll+L'l'+L''l''=1$, and set

$$\begin{array}{lll} n'l''-n''l'=M, & n''l-nl''=M', & nl'-n'l=M'' \\ l'm''-l''m'=N, & l''m-lm''=N', & lm'-l'm=N'' \end{array}$$

Finally, set

$$\begin{array}{ll} gM+g'M'+g''M''=\alpha, & hM+h'M'+h''M''=\beta \\ gN+g'N'+g''N''=\gamma, & hN+h'N'+h''N''=\delta \end{array}$$

We readily obtain

$$\begin{array}{c} \alpha m+\gamma n=g-l(gL+g'L'+g''L'')=g \\ \beta m+\delta n=h-l(hL+h'L'+h''L'')=h \end{array}$$

and, in the same way,

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''$$

This shows. $mt + nu$, $m't + n'u$, $m''t + n''u$ are taken by the substitution

$$t = \alpha p + \beta q, \quad u = \gamma p + \delta q \ldots (S)$$

into $gp+hq$, $g'p+h'q$, $g''p+h''q$, respectively. So φ is clearly taken by the substitution S into the same form as f is on setting

$$x = gp + hq, \qquad x' = g'p + h'q, \qquad x'' = g''p + h''q$$

and therefore into the form χ, to which it is thus equivalent. Finally, making the required substitutions readily gives

$$\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1$$

so the substitution S is proper, and the forms φ, χ are properly equivalent.

These observations give the following rules for finding all proper representations of D by F: Work out all classes of binary forms of determinant D, and choose one form at will from each. Find all proper representations of each of these forms by f (discarding those that cannot be represented by f), and from each of these representations derive the representations of the number D by F. From I and II it is clear that this gives all possible proper representations, so the solution is complete; from III, that transformations of forms from different classes certainly produce different representations.

281.

Finding the *improper* representations of a given number D by the form F is easily reduced to the preceding case. For if D is divisible by no square (other than 1), clearly there are no such representations at all. Otherwise, if D is divisible by the squares $\lambda\lambda, \mu\mu, \nu\nu$ and so on, all improper representations of D by F are found by working out all proper representations of the numbers $\frac{D}{\lambda\lambda}$, $\frac{D}{\mu\mu}$, $\frac{D}{\nu\nu}$, and so on by the same form, and multiplying the values of the indeterminates by λ, μ, ν and so on, respectively.

In this way, finding all representations of a given number by a given ternary form *that is adjoint to some ternary form* depends on the second problem. The remaining cases reduce to this case, which at first may seem to have rather limited scope, as follows. Let D be the number to be represented by the form $\left(\begin{smallmatrix} g,g',g'' \\ h,h',h'' \end{smallmatrix}\right)$, with determinant Δ, whose adjoint form is $\left(\begin{smallmatrix} G,G',G'' \\ H,H',H'' \end{smallmatrix}\right) = f$. The form adjoint to this in turn will be $\left(\begin{smallmatrix} \Delta g,\Delta g',\Delta g'' \\ \Delta h,\Delta h',\Delta h'' \end{smallmatrix}\right) = F$, and clearly the representations of the number ΔD by F (whose determination depends on what precedes) are exactly identical with the representations of the number D by the proposed form. — Further, when all coefficients of the form f have a common divisor μ, all coefficients of the form F are clearly divisible by $\mu\mu$. So ΔD must also be divisible by $\mu\mu$ (otherwise there would

be no representations); and the representations of the number D by the proposed form coincide with the representations of the number $\frac{\Delta D}{\mu\mu}$ by the form obtained from F by dividing each coefficient by $\mu\mu$. This form is adjoint to the one obtained from f by dividing each coefficient by μ.

Finally, we note that this solution of the first problem does not apply in the single case where $D = 0$; for here not all binary forms of determinant D fall into a finite number of classes. We will solve this case below on other principles.

282.

Finding the representations of a given binary form whose determinant is not $= 0$[*)] by a given ternary form depends on the following observations:

I. From any proper representation of the binary form $(p, q, r) = \varphi$ of determinant D by the ternary form f of determinant Δ, we can derive integers B, B' such that

$$BB \equiv \Delta p, \qquad BB' \equiv -\Delta q, \qquad B'B' \equiv \Delta r \text{ (mod. } D)$$

i.e., a value of the expression $\sqrt{\Delta}(p, -q, r)(\text{mod. } D)$. Let a proper representation of the form φ by f be given by

$$x = \alpha t + \beta u, \qquad x' = \alpha' t + \beta' u, \qquad x'' = \alpha'' t + \beta'' u$$

(where x, x', x''; t, u denote the indeterminates of the forms f, φ). Choose integers $\gamma, \gamma', \gamma''$ so that

$$(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma''$$

$= k$ is either $= +1$ or $= -1$, and let f be transformed by the substitution

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

into the form $\left(\begin{smallmatrix} a,a',a'' \\ b,b',b'' \end{smallmatrix}\right) = g$, whose adjoint is $\left(\begin{smallmatrix} A,A',A'' \\ B,B',B'' \end{smallmatrix}\right) = G$. Then clearly $a = p$, $b'' = q$, $a' = r$, $A'' = D$, and Δ will be the determinant of the form g, so

$$BB = \Delta p + A'D, \qquad BB' = -\Delta q + B''D, \qquad B'B' = \Delta r + AD$$

Thus, *for example*, the form $19tt + 6tu + 41uu$ is represented by $xx + x'x' + x''x''$ on setting $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$. Then, setting $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$, we obtain $B = -171$, $B' = 27$, or the value $(-171, 27)$ of the expression $\sqrt{-1}(19, -3, 41)(\text{mod. } 770)$.

It follows that, if $\Delta(p, -q, r)$ is not a quadratic residue of D, φ cannot be properly represented by any ternary form of determinant Δ. So, in the case where Δ, D are relatively prime, Δ must be a characteristic number of the form φ.

II. Since $\gamma, \gamma', \gamma''$ can be chosen in infinitely many different ways, different values of B, B' will result. Let us see how they are related. Suppose that $\delta, \delta', \delta''$ too are such that

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$$

is either $= +1$ or $= -1$, and that the form f is transformed by the substitution

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

[*)] For brevity, we pass over this case here; it requires a somewhat different method.

into $\left(\begin{smallmatrix}\mathfrak{a},\mathfrak{a}',\mathfrak{a}''\\ \mathfrak{b},\mathfrak{b}',\mathfrak{b}''\end{smallmatrix}\right) = \mathfrak{g}$, whose adjoint is $\left(\begin{smallmatrix}\mathfrak{A},\mathfrak{A}',\mathfrak{A}''\\ \mathfrak{B},\mathfrak{B}',\mathfrak{B}''\end{smallmatrix}\right) = \mathfrak{G}$. Then $g, \mathfrak{g}$ will be equivalent, and so will G and $\mathfrak{G}$. Applying the rules given in Articles 269, 270[*)] shows that, if we set

$$(\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' = \zeta$$
$$(\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' = \eta$$

the form $\mathfrak{G}$ is transformed into G by the substitution

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k} \end{matrix}$$

This gives

$$B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}, \qquad B' = \zeta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}'$$

and so, since $\mathfrak{k}k = \pm 1$, either $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$, or $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). In the first case we call the values (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ equivalent; in the second, opposite. We will say that the representation of the form φ *belongs* to any value of the expression $\sqrt{\Delta}(p, -q, r)$(mod. D) that can be derived from it by the method in I. Thus all values to which the same representation belongs will be either equivalent or opposite.

III. Conversely, suppose that, as in I above, the representation of the form φ by f given by $x = \alpha t + \beta u$ and so on belongs to the value (B, B') derived from it with the help of the transformation

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

It will also belong to any other value $(\mathfrak{B}, \mathfrak{B}')$ that is equivalent or opposite to the first; *i.e.*, in place of $\gamma, \gamma', \gamma''$ we may choose other integers $\delta, \delta', \delta''$ for which the equation (Ω), namely

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1$$

holds, and which are such that the coefficients numbered 4 and 5 in the form adjoint to the one into which f is transformed by the substitution (S)

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

become $= \mathfrak{B}, \mathfrak{B}'$, respectively. For set

$$\pm B = \mathfrak{B} + \eta D, \qquad \pm B' = \mathfrak{B}' + \zeta D$$

[*)] From the transformation of the form f into g, derive the transformation of g into f; from this and the transformation of f into $\mathfrak{g}$, derive the transformation of g into $\mathfrak{g}$; finally, from this, by transposition, derive the transformation of $\mathfrak{G}$ into G.

(taking the upper or lower signs here and below according as the values $(B.\ B')$, $(\mathfrak{B}, \mathfrak{B}')$ are equivalent or opposite). Then ζ, η will be integers. Let g be transformed by the substitution

$$\begin{array}{lll} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{array}$$

into the form $\mathfrak{g}$. It is easy to see that its determinant is Δ, and that in its adjoint form the coefficients numbered 4 and 5 become $= \mathfrak{B}, \mathfrak{B}'$, respectively. But on setting

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta''$$

it is easy to see that f is transformed by the substitution (S) into $\mathfrak{g}$, and that the equation (Ω) is satisfied. *Q. E. D.*

283.

These principles give the following method for finding all proper representations of the binary form

$$\varphi = ptt + 2qtu + ruu$$

of determinant D by the ternary form f of determinant Δ.

I. Find all different (*i.e.*, nonequivalent) values of the expression $\sqrt{\Delta}(p, -q, r)$(mod. D). We solved this problem above (Article 233) for the case where φ is a primitive form and Δ is relatively prime to D. The remaining cases are very easily reduced to this one, but brevity prevents us from explaining this in detail here. We only note that, whenever Δ is relatively prime to D, the expression $\Delta(p, -q, r)$ cannot be a quadratic residue of D unless φ is a primitive form. For if we suppose

$$\Delta p = BB - DA', \qquad -\Delta q = BB' - DB'', \qquad \Delta r = B'B' - DA$$

we get

$$(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$$

Expanding and substituting $qq - pr$ for D then gives

$$(qq - pr)(B''B'' - AA') - \Delta(Ap + 2B''q + A'r) + \Delta\Delta = 0$$

From this we easily conclude that, if p, q, r had a common divisor, it would also divide $\Delta\Delta$; but then Δ could not be relatively prime to D. So p, q, r cannot have a common divisor; that is, φ will be a primitive form.

II. Let us denote the number of these values by m, and suppose that among them there are n values opposite to themselves (setting $n = 0$ when there are none). Then the remaining $m - n$ values clearly come in opposite pairs (since we suppose that all values have been found). Discard either value at will from each opposite pair, and in all $\frac{1}{2}(m + n)$ values will remain. Thus, *for example*, of the eight values of the expression $\sqrt{-1}(19, -3, 41)$ (mod. 770), namely $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$, $(-39, -237)$, $(-171, 27)$, $(-269, 83)$, $(-291, 127)$, the last four are to be discarded as opposite to the first four. Further, if (B, B') is a value opposite to itself, clearly $2B$, $2B'$, and therefore also $2\Delta p$, $2\Delta q$, $2\Delta r$, will be divisible by D. So, if Δ, D are relatively prime, $2p$, $2q$, $2r$ will also be divisible by D. Since, by I, in this case p, q, r cannot have a common divisor either, 2 too must be divisible by D. This is impossible unless D is either $= \pm 1$ or $= \pm 2$. So, for all values of D greater than 2, we will always have $n = 0$ if Δ is relatively prime to D.

III. Once this is done, every proper representation of the form φ by f must clearly belong to one of the remaining values, and to exactly one. So we must go through these values in turn and find the representations belonging to each. To find the representations belonging to a *given* value (B, B'), first determine the ternary form $g = \left(\begin{smallmatrix} a, a', a'' \\ b, b', b'' \end{smallmatrix}\right)$ whose determinant $= \Delta$ and in which $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$. The values of a'', b, b' are then found with the help of the equations in II of Article 276. These readily show that, in the case where Δ, D are relatively prime, $b, b'\, a''$ must be integers (since these three numbers give integers

when multiplied both by D and by Δ). Now, if either one of the coefficients b, b', b'' is fractional, or the forms f, g are not equivalent, there can be no representations of the form φ by f belonging to (B, B'). But if b, b', a'' are integers and the forms f, g are equivalent, every transformation of the former into the latter, such as

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

gives such a representation, namely

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

Clearly there can be no representation of this kind that cannot be derived from some transformation. In this way, the part of the second problem concerned with finding *proper* representations has now been reduced to the third problem.

IV. Further, different transformations of the form f into g always produce different representations, except in the single case where the value (B, B') is opposite to itself. In that case two transformations always give a single representation. For suppose that f is also transformed into g by the substitution

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

(which gives the same representation as the preceding transformation). Denoting by k, $\mathfrak{k}$, ζ, η the same numbers as in II of the preceding article, we will have

$$B = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$$

So, if k, $\mathfrak{k}$ are supposed to be both $= +1$ or both $= -1$, we will have (since we excluded the case $D = 0$) $\zeta = 0$, $\eta = 0$. This readily gives $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$. Thus the two transformations can differ only when one of the numbers k, $\mathfrak{k}$ is $+1$ and the other -1. Then $B \equiv -B$, $B' \equiv -B'$, (mod. D), or the value (B, B') is opposite to itself.

V. From the criteria for definite and indefinite forms given above (Article 271), it readily follows that, if Δ is positive, D negative, and φ a negative form, g is a negative definite form. But if Δ is positive, and either D is positive, or D is negative and φ a positive form, g is an indefinite form. Now f, g certainly cannot be equivalent unless they agree in this respect. So binary forms of positive determinant, as well as positive binary forms, clearly cannot be properly represented by a negative ternary form; nor can negative binary forms be properly represented by an indefinite ternary form of positive determinant. A ternary form of the former or latter kind represents only binary forms of the latter or former kind, respectively. In the same way, a definite ternary form of negative determinant (*i.e.*, a positive form) represents only positive binary forms, and an indefinite one only negative binary forms and forms of positive determinant.

284.

Since the *improper* representations of the binary form φ of determinant D by the ternary form f, whose adjoint is F, are those from which improper representations of the number D by the form F follow, φ clearly cannot be improperly represented by f unless D has square factors. Suppose that all squares dividing D (other than 1) are ee, $e'e'$, $e''e''$, and so on (there will be finitely many, since we suppose that $D = 0$ does not hold). Every improper representation of the form φ by f will give a representation of the number D by F in which the values of the indeterminates have one of the numbers e, e', e'', and so on as their greatest common divisor. In this respect, for brevity, we will say that each improper representation of the form φ *belongs* to the square divisor ee or $e'e'$ or $e''e''$, and so on. Now all representations of the form φ belonging to the same *given* square divisor ee (whose root e we take to be positive) are found by the following rules. Their synthetic proof, which we prefer here for brevity, will readily allow the analysis by which they were developed to be reconstructed.

First, find all binary forms of determinant $\frac{D}{ee}$ that are transformed into the form φ by a proper substitution of the form $T = \kappa t + \lambda u$, $U = \mu u$, where T, U denote the indeterminates of such a form; t, u those of the form φ; κ, μ positive integers (whose product is therefore $= e$); and λ a positive integer less than μ (or zero). These forms, with their corresponding transformations, are found as follows:

Set κ equal in turn to each positive divisor of e (including 1 and e), and put $\mu = \frac{e}{\kappa}$. For each pair of fixed values of κ, μ, give λ all integer values from 0 to $\mu - 1$. This will certainly give all transformations. Now the form that is transformed by any substitution $T = \kappa t + \lambda u$, $U = \mu u$ into φ is found by determining the form into which φ is transformed by $t = \frac{1}{\kappa}T - \frac{\lambda}{e}U$, $u = \frac{1}{\mu}U$. In this way we obtain the forms corresponding to each transformation; but of all these forms we must retain only those whose three coefficients are all integers[*)].

Second, let Φ be one of these forms, transformed into φ by the substitution $T = \kappa t + \lambda u$, $U = \mu u$. Find all *proper* representations of the form Φ by f (if there are any), and express them generally by

$$x = \mathfrak{A}T + \mathfrak{B}U, \quad x' = \mathfrak{A}'T + \mathfrak{B}'U, \quad x'' = \mathfrak{A}''T + \mathfrak{B}''U \quad \dots \quad (\mathfrak{R})$$

Finally, from each $(\mathfrak{R})$ derive the representation

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u \quad \dots \quad (\rho)$$

by the equations

$$\begin{array}{lll} \alpha = \kappa\mathfrak{A}, & \alpha' = \kappa\mathfrak{A}', & \alpha'' = \kappa\mathfrak{A}'' \quad \dots \quad (R) \\ \beta = \lambda\mathfrak{A} + \mu\mathfrak{B}, & \beta' = \lambda\mathfrak{A}' + \mu\mathfrak{B}', & \beta'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}'' \end{array}$$

Treat the other forms found by the first rule (if there are more) in exactly the same way as the form Φ, so that further representations are derived from each of their

[*)] If we could discuss this problem at greater length here, we could shorten the solution considerably. It is immediately clear that for κ we need take only those divisors of e whose square divides the first coefficient of the form φ. We reserve this problem, which also gives simpler solutions to the problems in Articles 213, 214, for another suitable occasion.

proper representations. I say that this gives all representations of the form φ belonging to the divisor ee, and each exactly once.

Proof. I. That the ternary form f is indeed transformed by any substitution (ρ) into φ is so obvious that it needs no further explanation. That each representation (ρ) is improper and belongs to the divisor ee follows because the numbers $\alpha'\beta''-\alpha''\beta'$, $\alpha''\beta-\alpha\beta''$, $\alpha\beta'-\alpha'\beta$ become $= e(\mathfrak{A}'\mathfrak{B}''-\mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B}-\mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}'-\mathfrak{A}'\mathfrak{B})$, respectively. Their greatest common divisor is therefore clearly e (since $(\mathfrak{R})$ is a proper representation).

II. We will show that, from any given representation (ρ) of the form φ, we can find a proper representation of a form of determinant $\frac{D}{ee}$ included among the forms found by the first rule. In other words, the given values of $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ determine integer values of κ, λ, μ satisfying the prescribed conditions, and values of $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ satisfying the equations (R), in exactly one way. First, the first three equations in (R) immediately show that we must take κ to be the positive greatest common divisor of α, α', α'' (for since $\mathfrak{A}'\mathfrak{B}''-\mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B}-\mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}'-\mathfrak{A}'\mathfrak{B}$ must have no common divisor, $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ cannot have one either). This also determines $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, as well as $\mu = \frac{e}{\kappa}$ (which is readily seen to be an integer). Suppose that three integers $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$ are chosen so that $\mathfrak{a}\mathfrak{A}+\mathfrak{a}'\mathfrak{A}'+\mathfrak{a}''\mathfrak{A}''=1$, and for brevity write k for $\mathfrak{a}\mathfrak{B}+\mathfrak{a}'\mathfrak{B}'+\mathfrak{a}''\mathfrak{B}''$. The last three equations in (R) then give $\mathfrak{a}\beta+\mathfrak{a}'\beta'+\mathfrak{a}''\beta''=\lambda+\mu k$. So there is clearly just one value of λ between the limits 0 and $\mu-1$. Since this also gives $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ fixed values, all that remains is to show that these are always integers. But we have

$$\begin{aligned}\mathfrak{B} = \frac{1}{\mu}(\beta-\lambda\mathfrak{A}) &= \frac{1}{\mu}(\beta(1-\mathfrak{a}\mathfrak{A})-\mathfrak{A}(\mathfrak{a}'\beta'+\mathfrak{a}''\beta''))+\mathfrak{A}k \\ &= \frac{1}{\mu}(\mathfrak{a}''(\mathfrak{A}''\beta-\mathfrak{A}\beta'')-\mathfrak{a}'(\mathfrak{A}\beta'-\mathfrak{A}'\beta))+\mathfrak{A}k \\ &= \frac{1}{e}(\mathfrak{a}''(\alpha''\beta-\alpha\beta'')-\mathfrak{a}'(\alpha\beta'-\alpha'\beta))+\mathfrak{A}k\end{aligned}$$

so it is clearly an integer. In the same way we readily confirm that $\mathfrak{B}'$, $\mathfrak{B}''$ also take integer values. — These arguments show that there can be no improper representation of the form φ by f belonging to the divisor ee which the method given either fails to produce or produces more than once.

If we now treat the remaining square divisors of D in the same way, finding the representations belonging to each, we will obtain all improper representations of the form φ by f.

Further, this solution readily shows that the theorem given for proper representations at the end of the preceding article extends to improper ones as well: in general, no positive binary form of negative determinant can be represented by a negative ternary form, and so on. For if φ is a binary form that cannot be properly represented by f because of that theorem, then none of the forms of determinants $\frac{D}{ee}$, $\frac{D}{e'e'}$, and so on that contain φ can be properly represented by f either. All these forms have determinants of the same sign as φ. Whenever these determinants are negative, they are all positive or all negative forms according as φ belongs to the former or the latter kind.

285.

We can say only a little here about the questions making up our third problem (to which the first two were reduced above): given two ternary forms of the same determinant, decide whether they are equivalent, and, if they are, find all transformations of one into the other. A complete solution, like the one we gave for the analogous problems for binary forms, faces still greater difficulties here. So we will restrict our investigation to certain special cases, for which this digression was chiefly intended.

I For determinant $+1$, we showed above that all ternary forms fall into two classes, one containing all indefinite forms, the other all definite (negative) forms. We immediately conclude that any two ternary forms of determinant 1 are equivalent if both are definite or both indefinite; but if one is definite and the other indefinite, they are not equivalent (the latter part clearly holds generally for forms of any determinant). — Likewise, any two forms of determinant -1 will certainly be equivalent if both are definite or both indefinite. — Two definite forms of determinant 2 will always be equivalent. Two indefinite ones will not be equivalent if the first three coefficients of one are all even, but those of the other are not all even; in the remaining cases (if both have their first three coefficients all even, or neither does) they will be equivalent. — We could give many more special propositions of this kind if we had worked out more examples above (Article 277).

II. In all these cases, if f, f' denote equivalent ternary forms, we can also find one transformation of either into the other. For, in all cases, we gave above a fairly small set of forms in each class of ternary forms, to one of which any form of the same class can be reduced by uniform methods; there we also showed how to reduce all of these to a single one. Let F be this form in the class containing f, f'. The rules given above allow us to find transformations of the forms f, f' into F, as well as of F into f, f'. From these, Article 270 gives transformations of the form f into f' and of f' into f.

III. It would therefore remain only to show how all possible transformations can be derived from one transformation of the ternary form f into another f'. This problem depends on a simpler one: finding all transformations of the ternary form f into itself. For if f is transformed into itself by several substitutions (τ), (τ'), (τ''), and so on, and by the substitution (t) into f', then combining the transformation (t) with (τ), (τ'), (τ''), and so on according to Article 270 clearly gives transformations that all take f into f'. Further, a calculation readily proves that every transformation of the form f into f' can be derived in this way by combining the given transformation (t) of the form f into f' with some (and indeed *just one*) transformation of the form f into itself. So combining the given transformation of the form f into f' with *all* transformations of f into itself gives *all* transformations of f into f', and each exactly once.

Here we restrict the search for all transformations of the form f into itself to the case where f is a definite form whose coefficients numbered $4, 5, 6$ are all $= 0$[*)]. So let $f = \left(\begin{smallmatrix} a, a', a'' \\ 0, 0, 0 \end{smallmatrix} \right)$, and let all substitutions that take f into itself be expressed generally by

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

so that the following equations must hold:

$$\begin{aligned} a\alpha\alpha + a'\alpha'\alpha' + a''\alpha''\alpha'' &= a \quad \ldots \quad (\Omega) \\ a\beta\beta + a'\beta'\beta' + a''\beta''\beta'' &= a' \\ a\gamma\gamma + a'\gamma'\gamma' + a''\gamma''\gamma'' &= a'' \\ a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' &= 0 \\ a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' &= 0 \\ a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' &= 0 \end{aligned}$$

We now have three cases to distinguish:

I. When a, a', a'' (which will have the same sign) are all unequal, suppose that $a < a'$, $a' < a''$ (if their order of magnitude is different, the same conclusions follow in exactly the same way). Then the first equation in (Ω) clearly requires $\alpha' = \alpha'' = 0$, and so $\alpha = \pm 1$. Equations $4, 5$ then give $\beta = 0$, $\gamma = 0$. Likewise, equation 2 gives $\beta'' = 0$, and so $\beta' = \pm 1$. From equation 6 we get $\gamma' = 0$, and from 3, $\gamma'' = \pm 1$, so (since the signs can be chosen independently) there are in all 8 different transformations.

II. When two of the numbers a, a', a'' are equal, *for example*, $a' = a''$, and the third is different, suppose

first that $a < a'$. Then, as in the preceding case, $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$. But equations $2, 3, 6$ readily give either $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$, or $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$.

But if, *second*, $a > a'$, the same conclusions follow in this way: equations $2, 3$ necessarily give $\beta = 0$, $\gamma = 0$, and either $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$, or $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$. Under either supposition, equations $4, 5$ give $\alpha' = 0$, $\alpha'' = 0$, and equation 1 gives $\alpha = \pm 1$. So in either case there are 16 different transformations. — The remaining two cases, where either $a = a''$ or $a = a'$, are handled in exactly the same way, if we interchange the symbols α, α', α'' with β, β', β'' in the first case, and with γ, γ', γ'' in the second, respectively.

III. When a, a', a'' are all equal, equations $1, 2, 3$ require that two of the three numbers α, α', α'', and likewise of β, β', β'', and also of γ, γ', γ'', be $= 0$, and the third $= \pm 1$. But equations $4, 5, 6$ readily show that only one of the three numbers α, β, γ can be $= \pm 1$, and likewise of α', β', γ', and of α'', β'', γ''.

[*)] The remaining cases where f is a definite form can be reduced to this one. But if f is an indefinite form, an entirely different method is needed, and there will be infinitely many transformations.

So there are only six combinations:

$$\left.\begin{array}{c|c|c|c|c|c|l} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array}\right| \quad \text{The other six coefficients } = 0$$

The choices of signs therefore give 48 transformations in all. — The same scheme includes the preceding cases as well: but of the first six columns we must take only the first when a, a', a'' are all unequal; the first and second when $a' = a''$; the first and third when $a = a'$; the first and sixth when $a = a''$.

It follows that, if the form $f = axx + a'x'x' + a''x''x''$ is transformed into an equivalent form f' by the substitution

$$x = \delta y + \varepsilon y' + \zeta y'', \quad x' = \delta' y + \varepsilon' y' + \zeta' y'', \quad x'' = \delta'' y + \varepsilon'' y' + \zeta'' y''$$

all transformations of the form f into f' are contained in the following scheme:

$$\left.\begin{array}{c|c|c|c|c|c|l} x & x & x' & x' & x'' & x'' & = \pm(\delta y + \varepsilon y' + \zeta y'') \\ x' & x'' & x & x'' & x & x' & = \pm(\delta' y + \varepsilon' y' + \zeta' y'') \\ x'' & x' & x'' & x & x' & x & = \pm(\delta'' y + \varepsilon'' y' + \zeta'' y'') \end{array}\right|$$

with the distinction that all of the first six columns must be used when $a = a' = a''$; columns 1 and 2 when a', a'' are equal and a different; 1 and 3 when $a = a'$; 1 and 6 when $a = a''$; finally, only the first column when a, a', a'' are all unequal. The number of transformations will be 48 in the first case, 16 in the second, third, and fourth, and 8 in the fifth.

* *
*

SOME APPLICATIONS TO THE THEORY OF BINARY FORMS.

Finding a form whose doubling gives a given binary form of the principal genus.

From this brief account of the first elements of the theory of ternary forms, we turn to some special applications. First place among them belongs to the following

286.

Problem. *Given a binary form $F = (A, B, C)$ of determinant D belonging to the principal genus, find a binary form f whose doubling gives it.*

Solution. I. Find a proper representation of the form opposite to F, namely $F' = ATT - 2BTU + CUU$, by the ternary form $xx - 2yz$, say

$$x = \alpha T + \beta U, \quad y = \alpha' T + \beta' U, \quad z = \alpha'' T + \beta'' U$$

The preceding theory of ternary forms readily shows that this is possible. For, by hypothesis, F is in the principal genus, so there is a value of the expression $\sqrt{(A, B, C)}(\mathrm{mod.}\, D)$. From it we can find a ternary form φ of determinant 1 containing $(A, -B, C)$ as a part. All its coefficients are readily seen to be integers. It is just as

easy to see that φ will be an indefinite form (since, by hypothesis, F certainly is not a negative form), so it must be equivalent to the form $xx - 2yz$. We can therefore give a transformation of the latter into the former, which provides a proper representation of the form F' by $xx - 2yz$. — We will then have

$$A = \alpha\alpha - 2\alpha'\alpha'', \quad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \quad C = \beta\beta - 2\beta'\beta''$$

Further, if we denote the numbers $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ by a, b, c, respectively, they will have no common divisor, and $D = bb - 2ac$.

II. With the help of the last observation in Article 235, it follows readily that F is transformed by the substitution $2\beta', \beta, \beta, \beta''$; $2\alpha', \alpha, \alpha, \alpha''$ into the product of the form $(2a, -b, c)$ with itself, and by the substitution $\beta', \beta, \beta, 2\beta''$; $\alpha', \alpha, \alpha, 2\alpha''$ into the product of the form $(a, -b, 2c)$ with itself. Now the greatest common divisor of the numbers $2a, 2b, 2c$ is 2. So, if c is odd, $2a, 2b, c$ will have no common divisor; that is, $(2a, -b, c)$ will be a properly primitive form. Likewise, if a is odd, $(a, -b, 2c)$ will be a properly primitive form. In the first case F arises by doubling the form $(2a, -b, c)$, in the second by doubling the form $(a, -b, 2c)$ (see conclusion 4, Article 235); and one of these cases certainly always occurs. For if both a, c were even, b would necessarily be odd. We readily confirm that $\beta''a + \beta b + \beta' c = 0$, $\alpha''a + \alpha b + \alpha' c = 0$, which would imply that βb, αb, and therefore also α and β, were even. But then A and C would be even, contrary to the hypothesis that F is a form of the principal genus and therefore of the properly primitive order. — Further, both a and c may be odd. In that case we immediately have two forms whose doubling gives F.

Example. Let the given form be $F = (5.2, 31)$, of determinant -151. A value of the expression $\sqrt{(5, 2, 31)}$ is found here to be $(55, 22)$, giving the ternary form $\varphi = \begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix}$. The rules of Article 272 give an equivalent form $\begin{pmatrix} 1, & 1. & -1 \\ 0, & 0, & 0 \end{pmatrix}$, which is transformed into φ by the substitution $\begin{Bmatrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{Bmatrix}$. Using the transformations given in Article 277, we then find that $\begin{pmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{pmatrix}$ is transformed into φ by the substitution $\begin{Bmatrix} 3. & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3 \end{Bmatrix}$. So $a = 11$, $b = -17$, $c = 20$. Since a is odd, F arises by doubling the form $(11, 17, 40)$, and is transformed into the product of this form with itself by the substitution $-1, -7, -7, -18;\ 2, 3, 3, 2$.

Genera actually correspond to all characters except those found impossible in Articles 263, 264.

287.

We add the following further remarks on the problem solved in the preceding article.

I. If the form F is transformed by the substitution p, p', p'', p'''; q, q', q'', q''' into the product of two forms (h, i, k), (h', i', k') (both, as we always suppose, understood in the proper sense), we have the following equations, which are readily derived from conclusion 3 of Article 235:

$$p''hn' - p'h'n - p(in' - i'n) = 0$$
$$(p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0$$
$$p'kn' - p''k'n - p'''(in' - i'n) = 0$$

and three others obtained by interchanging the numbers p, p', p'', p''' with q, q', q'', q'''. Here n, n' are the positive square roots of the quotients obtained by dividing the determinants of the forms (h, i, k), (h', i', k') by the determinant of the form F. So, if these forms are identical, or $n = n'$, $h = h'$, $i = i'$, $k = k'$, those equations become

$$(p'' - p')hn = 0, \quad (p'' - p')in = 0, \quad (p'' - p')kn = 0$$

This *necessarily* gives $p' = p''$, and in exactly the same way $q' = q''$. — So, giving the forms (h, i, k), (h', i', k') the *same* indeterminates t, u, and denoting the indeterminates of the form F by T, U, the substitution transforms F as follows:

$$T = ptt + 2p'tu + p'''uu, \quad U = qtt + 2q'tu + q'''uu \quad \text{into} \quad (htt + 2itu + kuu)^2$$

II. If the form F arises by doubling the form f, it also arises by doubling any other form in the same class as f; in other words, the class of the form F arises by doubling the class of the form f (see Article 238). Thus, in the example of the preceding article, $(5, 2, 31)$ also arises by doubling the form $(11, -5, 16)$, which is properly equivalent to $(11, 17, 40)$. From one class whose doubling gives the class of the form F, we find *all* such classes (if there are more) with the help of Problem 260. In our example there is no other positive class of this kind, since there is only one positive properly primitive ambiguous class of determinant -151 (namely the principal class). Composing the only negative ambiguous class $(-1, 0, -151)$ with the class $(11, -5, 16)$ gives the class $(-11, -5. -16)$, so this will be the only negative class whose doubling gives the class $(5, 2, 31)$.

III. The very solution of the problem in the preceding article has shown that every properly primitive (positive) class of binary forms belonging to the principal genus can arise by doubling some properly primitive class of the same determinant. So the theorem of Article 261, which assured us that *at least* half of all characters assignable to a given nonsquare determinant D cannot correspond to properly primitive (positive) genera, can now be extended: such genera actually correspond to *exactly* half of all these characters, and so none can correspond to the other half (see the proof

of that theorem). In Article 264 all these assignable characters were divided equally into two kinds P, Q. The latter Q were proved unable to correspond to properly primitive (positive) forms, while it remained uncertain whether genera always actually correspond to each of the remaining P. This doubt is now completely removed, and we are sure that in the whole collection of characters P there is none without a corresponding genus. — It also follows readily that, for a negative determinant, in the *negative* properly primitive order, where Article 264, I showed all P to be impossible and *only* Q possible, *all* Q are actually possible. For let K denote any character in Q, f any form in the negative properly primitive order of forms of determinant D, and K' its character, which will be in Q. Then the character composed from K, K' (according to Article 246) clearly belongs to P. So there are positive properly primitive forms of determinant D corresponding to it. Composing such a form with f clearly gives a negative properly primitive form of determinant D whose character is K. — Exactly the same argument proves that, in the improperly primitive order, the characters found by the rules of Article 264 II, III to be the *only* possible ones are *all* possible, whether they are P or Q. — Unless we are very much mistaken, these theorems rank among the most beautiful in the theory of binary forms, all the more so because, although they are extremely simple, they lie so deep that a rigorous proof cannot be given without the help of so many other investigations.

Theory of decomposing both numbers and binary forms into three squares.

We now turn to another application of the preceding digression: the decomposition of both numbers and binary forms into three squares. We begin with the following

288.

Problem. *Let M denote a positive number. Find the conditions under which there can be primitive negative binary forms of determinant $-M$ that are quadratic residues of M, that is, for which* 1 *is a characteristic number.*

Solution. Let Ω denote the collection of all particular characters given by the relations of the number 1 both to each (odd) prime divisor of M and to the number 8 or 4 when it divides M. These characters will clearly be Rp, Rp', Rp'', and so on, where p, p', p'', and so on denote those prime divisors; also $1, 4$ when 4 divides it, and $1, 8$ when 8 divides M. Further, let us use the letters P, Q in the same sense as in the preceding article, or in Article 264. We now distinguish the following cases.

I. When M is divisible by 4, Ω will be a complete character. Article 233 V shows that 1 can be a characteristic number only of forms whose character is Ω. But Ω is clearly the character of the principal form $(1, 0, M)$, so it belongs to P and therefore cannot belong to a properly primitive negative form. Since there are no improperly primitive forms for such a determinant, in this case there are no primitive negative forms at all that are residues of M.

II. When $M \equiv 3 \pmod 4$, exactly the same arguments hold, with the sole exception that in this case there is an *improperly* primitive negative order. In it the characters P will be possible or impossible according as $M \equiv 3$ or $\equiv 7 \pmod 8$; see Article 264, III. So, in the first case there will be a genus in this order whose character is Ω, and 1 will be a characteristic number of all forms in it. In the second case there can be no negative forms at all with this property.

III. When $M \equiv 1 \pmod 4$, Ω is not yet a complete character: the relation to the number 4 must be added. But Ω clearly must enter the character of a form whose characteristic number is 1; conversely, any form whose character is either $\Omega;\ 1, 4$ or $\Omega;\ 3, 4$ has characteristic number 1. Now $\Omega;\ 1, 4$ is clearly the character of the principal genus, which belongs to P, and so is impossible in the negative properly primitive order. For the same reason, $\Omega;\ 3, 4$ will belong to Q (Article 263), so a genus in the negative properly primitive order will correspond to it, all of whose forms will have characteristic number 1. There is no improperly primitive order in this case, or in the next.

IV. When $M \equiv 2 \pmod 4$, we must add to Ω the relation to 8 to make a complete character: either $1\ and\ 3, 8$ or $5\ and\ 7, 8$ when $M \equiv 2 \pmod 8$, and either $1\ and\ 7, 8$ or $3\ and\ 5, 8$ when $M \equiv 6 \pmod 8$. In the first case the character $\Omega;\ 1\ and\ 3, 8$ clearly belongs to P, and so $\Omega;\ 5\ and\ 7, 8$ to Q. Thus a negative properly primitive genus will correspond to it. In the second case, the same argument gives one genus in the negative properly primitive order whose forms have the prescribed property, namely the one whose character is $\Omega;\ 3\ and\ 5, 8$.

It follows that primitive negative forms of determinant $-M$ with characteristic number 1 exist when M is congruent to one of the numbers 1, 2, 3, 5, 6 modulo 8, and always in just one genus, which will be improper when $M \equiv 3$. There are no such forms at all when $M \equiv 0,\ 4$ or $7 \pmod 8$. Further, if $(-a, -b, -c)$ is a primitive negative form with characteristic number $+1$, clearly (a, b, c) is a primitive positive form with characteristic number -1. So, in the first five cases (when $M \equiv 1, 2, 3, 5, 6$), there is one primitive positive genus whose forms have characteristic number -1, and it is *improper* for $M \equiv 3$. In the remaining three cases (when $M \equiv 0, 4, 7$) there can be no such positive forms at all.

289.

From the general theory given in Article 282, we obtain the following results on proper representations of binary forms by the ternary form $xx + yy + zz = f$.

I. A binary form φ cannot be properly represented by f unless it is a primitive positive form and -1 (that is, the determinant of the form f) is its characteristic number. So, for a positive determinant, and also for a negative determinant $-M$ when M is either divisible by 4 or of the form $8n + 7$, there are no binary forms properly representable by f.

II. But if $\varphi = (p, q, r)$ is a primitive positive form of determinant $-M$, and -1 is a characteristic number of the form φ, and therefore also of its opposite $(p, -q, r)$, there will be proper representations of the form φ by f belonging to any given value of the expression $\sqrt{-}(p, -q, r)$. For all coefficients of the ternary form g of determinant -1 (Article 283) will necessarily be integers, and g will be a definite form, so it is certainly equivalent to f (Article 285, I).

III. By Article 283, III, the number of all representations belonging to the same value of the expression $\sqrt{-}(p, -q, r)$ is, in every case except $M = 1$ and $M = 2$, as large as the number of transformations of the form f into g, and so, by Article 285, $= 48$. The same article shows that, given one representation belonging to a given value, we derive the other 47 from it by permuting the values of x, y, z among themselves and reversing their signs in every possible way. So all 48 representations give *a single* decomposition of the form φ into three squares, if we consider only the squares themselves, without regard to their order or the signs of their roots.

IV. Let the number of all distinct odd primes dividing M be $= \mu$. It follows without difficulty from Article 233 that the number of all distinct values of the expression $\sqrt{-}(p, -q, r)(\text{mod. } M)$ will be $= 2^{\mu}$. By Article 283, we need consider only half of these (when $M > 2$). So the number of all proper representations of the form φ by f will be $= 48 \,.\, 2^{\mu-1} = 3 \,.\, 2^{\mu+3}$, while the number of distinct decompositions into three squares will be $= 2^{\mu-1}$.

Example. Let $\varphi = 19tt + 6tu + 41uu$, so $M = 770$. Here we must consider the following four values of the expression $\sqrt{-}(19, -3, 41)(\text{mod. } 770)$ (Article 283): $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$. To find the representations belonging to the value $(39, 237)$, we first obtain the ternary form $\left(\begin{smallmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{smallmatrix}\right) = g$. By the rules of Articles 272, 275, we find that f goes into it by the substitution $\left\{\begin{smallmatrix} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{smallmatrix}\right\}$, which gives the following representation of the form φ by f:

$$x = t - 6u, \quad y = -3t - 2u. \quad z = -3t - u$$

For brevity, we do not write out the other 47 representations belonging to the same value, which arise by permuting these values and reversing their signs. All 48 representations give the same decomposition of the form φ into the three squares

$$tt - 12tu + 36uu, \quad 9tt + 12tu + 4uu, \quad 9tt + 6tu + uu$$

In exactly the same way, the value $(171, -27)$ gives the decomposition into the squares $(3t + 5u)^2$, $(3t - 4u)^2$, tt; the value $(269, -83)$ gives $(t + 6u)^2 + (3t + u)^2 +$

$(3t-2u)^2$; and finally the value $(291,-127)$ gives $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$. Each of these decompositions is equivalent to 48 representations. — Besides these 192 representations, or four decompositions, there will be no others, since 770 is divisible by no square, so improper representations cannot exist.

290.

We will briefly discuss separately the forms of determinants -1 and -2, which were subject to certain exceptions. We first make the general observation that, if φ, φ' are any equivalent binary forms, and (Θ) is a given transformation of the former into the latter, combining any representation of the form φ by some ternary form f with the substitution (Θ) gives a representation of the form φ' by f. Further, proper representations of φ give proper representations of φ' in this way; distinct ones give distinct ones, and all of them give all of them. All this is very easily checked by calculation. So either of the forms φ, φ' can be represented by f in as many ways as the other.

I. First let $\varphi = tt+uu$, and let φ' be any other positive binary form of determinant -1, to which φ will therefore be equivalent. Let φ go into φ' by the substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. The form φ is represented by the ternary form $f = zz+yy+zz$ by setting $x = t$, $y = u$, $z = 0$. Permuting x, y, z gives *six* representations, and changing the signs of t, u gives four from each, making 24 distinct representations in all. A single decomposition into three squares is equivalent to these, and it is easy to see that there can be no other representations. It follows that the form φ', too, can be decomposed into three squares in only one way, namely $(\alpha t' + \beta u')^2$, $(\gamma t' + \delta u')^2$ and 0. This decomposition is equivalent to 24 representations.

II. Let $\varphi = tt + 2uu$, and let φ' be any other positive binary form of determinant -2, into which φ goes by the substitution $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. We then conclude, as in the preceding case, that φ, and therefore also φ', can be decomposed into three squares in only one way: φ into $tt + uu + uu$, and φ' into $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$. It is easy to see that such a decomposition is equivalent to 24 representations.

It follows that binary forms of determinants -1 and -2 agree completely with other binary forms as to the number of their representations by the ternary form $xx + yy + zz$. For in both cases $\mu = 0$, and the formula given in IV of the preceding article does indeed give 24 representations. The reason is that the two exceptions affecting these forms compensate for each other.

For brevity, we omit the application to the form $xx+yy+zz$ of the general theory of improper representations developed in Article 284.

291.

By Article 281, the problem of finding all proper representations of a given positive *number* M by the form $xx+yy+zz$ first reduces to finding the proper representations of the number $-M$ by the form $-xx-yy-zz = f$. By the rules of Article 280, these are obtained as follows.

I. Find all classes of binary forms of determinant $-M$ whose forms can be properly represented by $XX + YY + ZZ = F$ (the ternary form whose adjoint is f). When $M \equiv 0,\ 4$ or $7 \pmod 8$, Article 288 shows that there are no such classes, so M

cannot be decomposed into three squares having no common divisor*). But when $M \equiv 1,\ 2,\ 5$ or 6, there will be a positive properly primitive genus, and when $M \equiv 3$, an improperly primitive genus, containing all those classes. Let k denote the number of these classes.

II. Now choose k forms at will from these classes, one from each, and call them φ, φ', φ'', and so on. Find all proper representations of all of them by F. Their number will therefore be $3 \,.\, 2^{\mu+3}k = K$, where μ denotes the number of (odd) prime factors of M. Finally, from any such representation, as

$$X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u$$

derive the following representation of M by $xx + yy + zz$:

$$x = m'n'' - m''n', \quad y = m''n - mn'', \quad z = mn' - m'n$$

The collection of these K representations, which we denote by Ω, will necessarily contain all representations of M.

III. So we only need to ask whether *identical* representations can occur in Ω. Article 280, III already shows that representations in Ω derived from different forms, *for example* from φ and φ', must be distinct. So the only remaining question is whether distinct representations of the same form, *for example* φ, by F can give identical representations of the number M by $xx + yy + zz$. It is immediately clear that, if the representations of φ include

$$X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u \quad \ldots\ (r)$$

they also include

$$X = -mt - nu, \quad Y = -m't - n'u, \quad Z = -m''t - n''u \quad \ldots\ (r')$$

and that both give the same representation of M, which we denote by (R). So let us examine whether this same (R) can also follow from other representations of the form φ. From Article 280, III, on setting $\chi = \varphi$ there, we readily deduce that, if all proper transformations of the form φ into itself are given by

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

then all representations of the form φ from which R follows will be expressed by

$$\begin{aligned} x &= (\alpha m + \gamma n)t + (\beta m + \delta n)u \\ y &= (\alpha m' + \gamma n')t + (\beta m' + \delta n')u \\ z &= (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u \end{aligned}$$

But the theory of transformations of binary forms of negative determinant developed in Article 179 shows that, in every case except $M = 1$ and $M = 3$, there are only

*) This impossibility also follows from the fact that the sum of three odd squares is necessarily $\equiv 3 \pmod 8$; the sum of two odd squares and one even square is either $\equiv 2$ or $\equiv 6$; the sum of one odd square and two even squares is either $\equiv 1$ or $\equiv 5$; and finally the sum of three even squares is either $\equiv 0$ or $\equiv 4$. But in the last case the representation is clearly improper.

two proper transformations of the form φ into itself: $\alpha, \beta, \gamma, \delta = 1, 0, 0, 1$ and $= -1, 0, 0, -1$, respectively. (Since φ is a primitive form, what was denoted by m in Article 179 will be either 1 or 2, so, apart from the exceptional cases, (1) certainly applies there.) Thus (R) can arise only from r, r', so every proper representation of the number M occurs twice, and no more, in Ω. The number of all distinct proper representations of M will therefore be $\frac{1}{2}K = 3 \,.\, 2^{\mu+2}k$.

As for the exceptional cases, Article 179 gives the number of proper transformations of the form φ into itself as 4 for $M = 1$, and 6 for $M = 3$. And it is easily confirmed that the numbers of proper representations of the numbers 1, 3 are $\frac{1}{4}K$, $\frac{1}{6}K$, respectively. For each number can be decomposed into three squares in only one way: 1 into $1 + 0 + 0$, and 3 into $1 + 1 + 1$. The decomposition of 1 gives six distinct representations, and that of 3 gives eight. But K is $= 24$ for $M = 1$ (where $\mu = 0$, $k = 1$), and $= 48$ for $M = 3$ (where $\mu = 1$, $k = 1$).

Further, let h denote the number of classes in the principal genus, which by Article 252 equals the number of classes in any other properly primitive genus. We observe that $k = h$ for $M \equiv 1,\ 2,\ 5$ or 6 (mod. 8), but $k = \frac{1}{3}h$ for $M \equiv 3$ (mod. 8), with the single exception of $M = 3$, where $k = h = 1$. So, for numbers of the form $8n + 3$, the number of representations is *in general* $= 2^{\mu+2}h$, since for the number 3 the two exceptions compensate for each other.

292.

We distinguish decompositions of numbers into three squares (as we did above for binary forms) from representations by the form $xx+yy+zz$ by considering only the sizes of the squares in the former, but also their order and the signs of their roots in the latter. So we regard the representations $x = a$, $y = b$, $z = c$ and $x = a'$, $y = b'$, $z = c'$ as distinct unless $a = a'$, $b = b'$, $c = c'$ all hold. But we regard the decompositions into $aa + bb + cc$ and into $a'a' + b'b' + c'c'$ as one if these squares are equal to those without regard to order. It follows that

I. A decomposition of the number M into the squares $aa + bb + cc$ is equivalent to 48 representations if none is $= 0$ and all are unequal; but to 24 if *either* one is $= 0$ and the others unequal, *or* none is $= 0$ and two are equal. If, however, in a decomposition of a given number into three squares, two of them are $= 0$, *or* one is $= 0$ and the others equal, *or* all are equal, it will be equivalent to 6, *or* 12, *or* 8 representations, respectively. But these can occur only in the exceptional cases $M = 1, 2, 3$, respectively, since the representations must be proper. Excluding these, let the number of all decompositions of the number M into three squares (without a common divisor) be E, and suppose that among them there are e with one square 0 and e' with two equal squares. The former can also be regarded as decompositions into two squares, and the latter as decompositions into a square and twice a square. Then the number of all proper representations of the number M by $xx+yy+zz$ will be

$$= 24(e + e') + 48(E - e - e') = 48E - 24(e + e')$$

But from the theory of binary forms we readily deduce that e will be either $= 0$ or $= 2^{\mu-1}$, according as -1 is a quadratic nonresidue or residue of M, and also $e' = 0$ or $= 2^{\mu-1}$, according as -2 is a nonresidue or residue of M. Here μ denotes the number of (odd) prime factors of M (see Article 182; we omit a fuller account here). It follows readily that

$$\begin{aligned} E &= 2^{\mu-2}k, && \text{if both } -1 \text{ and } -2 \text{ are } N.R. \text{ of } M; \\ E &= 2^{\mu-2}(k+2), && \text{if both numbers are residues; finally} \\ E &= 2^{\mu-2}(k+1), && \text{if one is a residue and the other a nonresidue.} \end{aligned}$$

In the excluded cases $M = 1$ and $M = 2$, this formula would give $E = \frac{3}{4}$, whereas it should be $E = 1$. But for $M = 3$ it correctly gives $E = 1$, the exceptions compensating for each other.

So, if M is a prime, $\mu = 1$, and therefore $E = \frac{1}{2}(k + 2)$ when $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k + 1)$ when $M \equiv 3$ or $\equiv 5$. These special theorems were discovered by induction by the distinguished Le Gendre and given in his excellent paper, already cited several times, *Hist. de l'Ac. de Paris* 1785, p. 530 ff., though in a somewhat different form. This is mainly because he did not distinguish proper from improper equivalence, and so combined opposite classes.

II. To find all decompositions of the number M into three squares (without a common divisor), we do not need to find all proper representations of all the forms φ, φ', φ''. First, it is easy to confirm that all (48) representations of the form φ

belonging to the same value of the expression $\surd -(p,-q,r)$ (setting $\varphi = (p,q,r)$) give the same decomposition of the number M. So it is enough to have one of them, or, what comes to the same thing, only to write down all distinct decompositions*) of the form φ into three squares; and likewise for the others φ', φ'', and so on. Next, if φ belongs to a nonambiguous class, we may entirely omit the form chosen from the opposite class; in other words, it is enough to consider just one of two opposite classes. For the choice of a form from each class is completely arbitrary. Suppose that from the class opposite to the one containing φ we choose the form opposite to φ, and let it be $= \varphi'$. Then we readily see that, if the proper decompositions of the form φ are expressed generally by

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

all decompositions of the form φ' will be expressed by

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

and that these give the same decompositions of the number M as the former. Finally, if φ is a form in an ambiguous class, but is neither in the principal class nor equivalent to the form $(2,0,\frac{1}{2}M)$ or $(2,1,\frac{1}{2}(M+1))$ (according as M is even or odd), we may omit half the values of the expression $\surd -(p,-q,r)$. For brevity, however, we do not discuss this shortcut further here. — We can also use these same shortcuts when all proper representations of M by $xx+yy+zz$ are wanted, since these are very easily obtained from the decompositions.

As an example, we will find all decompositions of the number 770 into three squares. Here $\mu = 3$, $e = e' = 0$, and therefore $E = 2k$. Classifying the positive binary forms of determinant -770 gives the number of positive classes as $= 32$. We omit this classification for brevity, since anyone can easily construct it by the method of Article 231. All these classes are properly primitive and distributed among 8 genera, so that $k = 4$, and therefore $E = 8$. The genus whose characteristic number is -1 must clearly have the particular characters with respect to the numbers $5, 7, 11$ given by $R5$; $N7$; $N11$. From Article 263, we readily conclude that its character with respect to the number 8 must be 1 and 3, 8. Now in the genus with character 1 and 3, 8; $R5$; $N7$; $N11$ there are four classes, as whose representatives we choose the forms $(6,2,129)$, $(6,-2,129)$, $(19,3,41)$, $19,-3,41)$. But we discard the second and fourth classes, as they are opposite to the first and third. We have already given four decompositions of the form $(19,3,41)$ in Article 289. These give decompositions of the number 770 into $9+361+400$, $16+25+729$, $81+400+289$, $576+169+25$. In the same way we find four decompositions of the form $6tt+4tu+129uu$ into

$$(t-8u)^2 + (2t+u)^2 + (t+8u)^2,$$
$$(t-10u)^2 + (2t+5u)^2 + (t+2u)^2$$
$$(2t-5u)^2 + (t+10u)^2 + (t+2u)^2,$$
$$(2t+7u)^2 + (t-8u)^2 + (t-4u)^2$$

*) We must always understand *proper*, if we choose to transfer this term from representations to decompositions.

arising, respectively, from the following values of the expression $\surd -(6,-2,129)$: $(48,369)$, $(62,-149)$, $(92,-159)$, $(202,61)$. These give decompositions of the number 770 into $225+256+289$, $1+144+625$, $64+81+625$, $16+225+529$. Besides these eight decompositions there are no others.

What concerns decompositions of numbers into three squares having common divisors follows so easily from the general theory of Article 281 that there is no need to spend time on it.

Proof of Fermat's theorems that every integer can be decomposed into three triangular numbers or four squares.

293.

The preceding investigations also give a proof of the famous theorem that *every positive integer can be decomposed into three triangular numbers*, discovered long ago by Fermat, but for which a rigorous proof had been missing until now. Clearly any decomposition of the number M into triangular numbers

$$\tfrac{1}{2}x(x+1)+\tfrac{1}{2}y(y+1)+\tfrac{1}{2}z(z+1)$$

gives a decomposition of the number $8M+3$ into three odd squares

$$(2x+1)^2+(2y+1)^2+(2z+1)^2$$

and conversely. But by the preceding theory every positive integer $8M+3$ can be resolved into three squares, which must be odd (see the note to Article 291). The number of such resolutions depends both on the number of prime factors of $8M+3$ and on the number of classes into which the binary forms of determinant $-(8M+3)$ are distributed. There will be just as many decompositions of the number M into three triangular numbers. We assume, however, that $\frac{1}{2}x(x+1)$ is regarded as a triangular number for any integer value of x. If one preferred to exclude zero, the theorem would have to be changed to this: Every positive integer is either itself a triangular number or can be resolved into two or three triangular numbers. A similar change would be needed in the following theorem if one preferred to exclude zero from the squares.

The same principles prove another theorem of Fermat: *every positive integer can be decomposed into four squares.* Subtract any square (smaller than the number) from a number of the form $4n+2$, an even square from a number of the form $4n+1$, or an odd square from a number of the form $4n+3$. In all these cases the remainder can be resolved into three squares, and so the given number into four. Finally, a number of the form $4n$ can be expressed as $4^\mu N$, where N belongs to one of the preceding three forms. Resolving N into four squares also resolves $4^\mu N$. From a number of the form $8n+3$ we can also subtract a square whose root is divisible by four; from a number of the form $8n+7$, a square whose root is twice an odd number; and from a number of the form $8n+4$, an odd square. The remainder can then be resolved into three squares. This theorem had already been proved by the distinguished La Grange, *Nouv. Mém. de l'Ac. de Berlin* 1770, p. 123. His proof,

entirely different from ours, was explained more fully by the distinguished Euler in *Actis Ac. Petr. Vol.* II, p. 48. — Other theorems of Fermat, which form a kind of continuation of these, stating that every integer can be resolved into five pentagonal numbers, six hexagonal numbers, seven heptagonal numbers, *and so on*, still lack a proof and seem to require deeper principles.

Solution of the equation $axx + byy + czz = 0$.

294.

THEOREM. *Let a, b, c be pairwise coprime numbers, none of which is $= 0$ or divisible by a square. The equation*

$$axx + byy + czz = 0 \ldots (\Omega)$$

will have no integer solution (apart from $x = y = z = 0$, which we disregard) unless $-bc, -ac, -ab$ are quadratic residues of a, b, c, respectively, and these numbers do not all have the same sign. But when these four conditions hold, (Ω) will be solvable in integers.

Proof. If (Ω) is solvable in integers at all, it can also be solved by values of x, y, z having no common divisor. For any values satisfying the equation Ω still satisfy it when divided by their greatest common divisor. Now suppose $app + bqq + crr = 0$ and that p, q, r have no common divisor. They will then also be pairwise coprime. For if q, r had a common divisor μ, this would be coprime to p, but $\mu\mu$ would divide app, and therefore also a, contrary to the hypothesis. Likewise, p, r; p, q will be pairwise coprime. So $-app$ is represented by the binary form $byy + czz$, on assigning to y, z the coprime values q, r. Its determinant $-bc$ will therefore be a quadratic residue of app, and hence also of a (Article 154). In the same way, $-acRb, -abRc$. That (Ω) cannot have a solution if a, b, c all have the same sign is so obvious that it needs no explanation.

We will arrange the proof of the converse, which forms the second part of the theorem, as follows. *First*, we show how to find a ternary form equivalent to $\left(\begin{smallmatrix} a,b,c \\ 0,0,0 \end{smallmatrix}\right) \ldots f$ whose coefficients $2, 3, 4$ are divisible by abc. *Second*, from this we will derive a solution of the equation (Ω).

I. Find three integers A, B, C having no common divisor and such that A is coprime to b and c; B to a and c; C to a and b; while $aAA + bBB + cCC$ is divisible by abc. This is done as follows. Let $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ be values of the expressions $\sqrt{\ } - bc \pmod{a}$, $\sqrt{\ } - ac \pmod{b}$, $\sqrt{\ } - ab \pmod{c}$, respectively. They will necessarily be coprime to a, b, c, respectively. Choose three integers $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ completely at will, provided they are coprime to a, b, c, respectively (*for example*, all $= 1$), and determine A, B, C so that

$$\begin{aligned} A &\equiv \mathfrak{b}c \pmod{b} \quad \text{and} \quad \equiv \mathfrak{c}\mathfrak{C} \pmod{c} \\ B &\equiv \mathfrak{c}a \pmod{c} \quad \text{and} \quad \equiv \mathfrak{a}\mathfrak{A} \pmod{a} \\ C &\equiv \mathfrak{a}b \pmod{a} \quad \text{and} \quad \equiv \mathfrak{b}\mathfrak{B} \pmod{b} \end{aligned}$$

Then

$$\begin{aligned} aAA + bBB + cCC &\equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} + cbb) \\ &\equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} - \mathfrak{A}\mathfrak{A}b) \equiv 0 \pmod{a} \end{aligned}$$

so it will be divisible by a, and likewise by b, c, and therefore also by abc. Further, A is clearly necessarily coprime to b and c; B to a and c; C to a and b. But if these values of A, B, C have a (greatest) common divisor μ, this will clearly be coprime to a, b, c, and so to abc. Dividing those values by μ therefore gives new ones with no

common divisor, still making $aAA + bBB + cCC$ divisible by abc, and so satisfying all the conditions.

II. With A, B, C determined in this way, Aa, Bb, Cc will also have no common divisor. For if they had a common divisor μ, it would necessarily be coprime to a (since the latter is coprime to both Bb and Cc), and similarly to b and c. So μ would also have to divide A, B, C, contrary to the hypothesis. We can therefore find integers α, β, γ such that $\alpha Aa + \beta Bb + \gamma Cc = 1$. Find, further, six integers $\alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ such that

$$\beta'\gamma'' - \gamma'\beta'' = Aa, \quad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \quad \alpha'\beta'' - \beta'\alpha'' = Cc$$

Now let f go by the substitution

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

into $\left(\begin{smallmatrix} m,m',m'' \\ n,n',n'' \end{smallmatrix}\right) = g$ (which will be equivalent to f). I say that m', m'', n will be divisible by abc. For set

$$\begin{gathered} \beta''\gamma - \gamma''\beta = A', \quad \gamma''\alpha - \alpha''\gamma = B', \quad \alpha''\beta - \beta''\alpha = C' \\ \beta\gamma' - \gamma\beta' = A'', \quad \gamma\alpha' - \alpha\gamma' = B'', \quad \alpha\beta' - \beta\alpha' = C'' \end{gathered}$$

and we have

$$\begin{gathered} \alpha' = B''Cc - C''Bb, \quad \beta' = C''Aa - A''Cc, \quad \gamma' = A''Bb - B''Aa \\ \alpha'' = C'Bb - B'Cc, \quad \beta'' = A'Cc - C'Aa, \quad \gamma'' = B'Aa - A'Bb \end{gathered}$$

Substituting these values into the equations

$$\begin{aligned} m' &= a\alpha'\alpha' + b\beta'\beta' + c\gamma'\gamma' \\ m'' &= a\alpha''\alpha'' + b\beta''\beta'' + c\gamma''\gamma'' \\ n &= a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma'' \end{aligned}$$

gives, modulo a,

$$\begin{aligned} m' &\equiv bcA''A''(BBb + CCc) \equiv 0 \\ m'' &\equiv bcA'A'(BBb + CCc) \equiv 0 \\ n &\equiv bcA'A''(BBb + CCc) \equiv 0 \end{aligned}$$

that is, m', m'', n will be divisible by a. In the same way, these numbers are found to be divisible by b, c, and therefore also by abc, as claimed.

III. For convenience, write the determinant of the forms f, g as $-abc = d$, and set

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N''$$

Clearly f goes by the substitution (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

into the ternary form $\left(\begin{smallmatrix} Md,M'd,M''d \\ Nd,N'd,N''d \end{smallmatrix}\right) = g'$ of determinant d^3, which will therefore be contained under f. I now say that this form g' is necessarily equivalent to $\left(\begin{smallmatrix} d,0,0 \\ d,0,0 \end{smallmatrix}\right) = g''$. For $\left(\begin{smallmatrix} M,M',M'' \\ N,N',N'' \end{smallmatrix}\right) = g'''$ is clearly a ternary form of determinant 1. Further, since by the hypothesis a, b, c do not all have the same sign, f will be an indefinite form, from which it follows readily that g' and g''' must also be indefinite. So g''' will be equivalent to the form $\left(\begin{smallmatrix} 1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$ (Article 277), and we can find a transformation (S') of the former into the latter. But clearly (S') takes the form g' into g''. Thus g'', too, will be contained under f, and combining the substitutions $(S), (S')$ gives a transformation of the form f into g''. If this is

$$\begin{matrix} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{matrix}$$

we clearly have two solutions of the equation (Ω), namely $x = \delta', y = \varepsilon', z = \zeta'$ and $x = \delta'', y = \varepsilon'', z = \zeta''$. Neither set of values can all be $= 0$, since necessarily

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d. \quad \text{As required.}$$

Example. Let the given equation be $7xx - 15yy + 23zz = 0$, which is solvable because $345\,R\,7, -161\,R\,15, 105\,R\,23$. Here the values of $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ are $3, 7, 6$; setting $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$ gives $A = 98, B = -39, C = -8$. From this we obtain the substitution

$$\left\{\begin{matrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{matrix}\right\}$$

which takes f into $\left(\begin{smallmatrix} 1520,14490,-7245 \\ -2415,-1246,4735 \end{smallmatrix}\right) = g$. This gives

$$(S) = \left\{\begin{matrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{matrix}\right\}, \quad g''' = \left(\begin{smallmatrix} 3670800,6,-3 \\ -1,-1246,4735 \end{smallmatrix}\right).$$

The form g''' is found to go into $\left(\begin{smallmatrix} 1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$ by the substitution

$$\left\{\begin{matrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{matrix}\right\} \ldots (S')$$

Combining this with (S) gives $\left\{\begin{matrix} 9,11.12 \\ -1,9,-9 \\ -9,4,3 \end{matrix}\right\}$, which takes f into g''. So we have two solutions of the given equation, $x = 11, y = 9, z = 4$ and $x = 12, y = -9, z = 3$. The latter becomes simpler on dividing the values by the common divisor 3, giving $x = 4, y = -3, z = 1$.

295.

The latter part of the theorem in the preceding article can also be proved as follows. Find an integer h such that $ah \equiv \mathfrak{C} \pmod{c}$ (we use the symbols $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ in the same sense as in the preceding article), and set $ahh+b = ci$. It is then easy to see that i is an integer and that the number $-ab$ is the determinant of the binary form $(ac, ah, i) \ldots \varphi$. This form certainly will not be positive (since by the hypothesis a, b, c do not all have the same sign, ab and ac cannot both be positive). Further, it will have characteristic number -1, which we prove synthetically as follows. Determine integers e, e' such that

$$\begin{aligned} e &\equiv 0 \pmod{a} \text{ and } \equiv \mathfrak{B} \pmod{b}; \\ ce' &\equiv \mathfrak{A} \pmod{a} \text{ and } \equiv h\mathfrak{B} \pmod{b} \end{aligned}$$

Then (e, e') will be a value of the expression $\sqrt{-}(ac, ah, i) \pmod{-ab}$. For modulo a we have

$$\begin{aligned} ee \equiv 0 \equiv -ac, \quad ee' \equiv 0 \equiv -ah \\ cce'e' \equiv \mathfrak{A}\mathfrak{A} \equiv -bc \equiv -cci \quad \text{so } e'e' \equiv -i \end{aligned}$$

and modulo b we have

$$\begin{aligned} ee \equiv \mathfrak{B}\mathfrak{B} \equiv -ac, \quad cee' \equiv h\mathfrak{B}\mathfrak{B} \equiv -ach \quad \text{so } ee' \equiv -ah \\ cce'e' \equiv hh\mathfrak{B}\mathfrak{B} \equiv -achh \equiv -cci \quad \text{so } e'e' \equiv -i \end{aligned}$$

These same three congruences, which hold for both moduli a, b, will also hold modulo ab. From the theory of ternary forms we readily conclude that φ can be represented by the form $\left(\begin{smallmatrix} -1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$. So let

$$actt + 2ahtu + iuu = -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Multiplying by c gives

$$a(ct + hu)^2 + buu = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

It follows that, if t, u are assigned definite values making either $\gamma t + \delta u$ or $\varepsilon t + \zeta u$ become $= 0$, we have a solution of the equation Ω. It is therefore satisfied both by

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha\delta - \beta\gamma$$

and by

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha\zeta - \beta\varepsilon$$

Neither set of values can all become $= 0$. For if $\delta c - \gamma h = 0, \gamma = 0$, we would also have $\delta = 0$ and $\varphi = -(\alpha t + \beta u)^2$, giving $ab = 0$, contrary to the hypothesis; and likewise for the other set. — In our example we find the form φ to be $(161, -63, 24)$, the value of the expression $\sqrt{-}\varphi \pmod{105} = (7, -51)$, and the following representation of the form φ by $\left(\begin{smallmatrix} -1,0,0 \\ 1,0,0 \end{smallmatrix}\right)$:

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$$

This gives the solutions $x = 7, y = 11, z = -8$; $x = 20, y = 15, z = -5$, or, on dividing by 5 and disregarding the sign of z, $x = 4, y = 3, z = 1$.

Of these two methods for solving the equation Ω, the latter has the advantage of usually working with smaller numbers. But the former, which can also be shortened by various devices we pass over here, seems more elegant, especially because the numbers a, b, c are treated in exactly the same way and the calculation is unchanged by any permutation of them. This is different in the second method, where the calculation is usually most convenient if we take the smallest of the three given numbers for a and the largest for c, as we did in our example.

On the method by which the distinguished Le Gendre treated the fundamental theorem.

296.

The elegant theorem discussed in the preceding articles was first discovered by the distinguished Le Gendre, *Hist. de l'Ac. de Paris* 1784, p. 507, and supplied with a beautiful proof, entirely different from our two. At the same place this excellent geometer also tried to derive from it a proof of propositions agreeing with the fundamental theorem of the preceding section. We have already said above, in Article 151, that this proof seems to us unsuitable for that purpose. This is therefore the place to set out this proof, which is very elegant in itself, briefly and to give the reasons for our judgement. We begin with the following observation: *If the numbers a, b, c are all $\equiv 1 \pmod 4$, the equation $axx + byy + czz = 0 \ldots (\Omega)$ cannot be solvable.* For it is very easy to see that, in this case, the value of $axx + byy + czz$ must be either $\equiv 1$, $\equiv 2$ or $\equiv 3 \pmod 4$, unless x, y, z are all taken even. So, if Ω were solvable, it could only be by even values of x, y, z, *which is absurd*: any values satisfying the equation Ω still satisfy it when divided by their greatest common divisor, which must give at least one odd value. The different cases of the theorem to be proved now reduce to the following points.

I. Let p, q be primes of the form $4n + 3$ (positive and unequal). We cannot have $p\,R\,q, q\,R\,p$ simultaneously. For if this were possible, setting $1 = a, -p = b, -q = c$ would clearly satisfy all conditions for the solvability of the equation $axx + byy + czz = 0$ (Article 294). But by the preceding observation it has no solution, so the supposition cannot hold. Proposition 7 of Article 131 follows immediately.

II. If p is a prime of the form $4n + 1$ and q a prime of the form $4n + 3$, we cannot have $q\,R\,p, p\,N\,q$ simultaneously. Otherwise we would have $-p\,R\,q$, and the equation $xx + pyy - qzz = 0$ would be solvable, whereas by the preceding observation it has no solution. Cases 4 and 5 of Article 131 follow from this.

III. If p, q are primes of the form $4n+1$, we cannot have $p\,R\,q, q\,N\,p$ simultaneously. Take another prime r of the form $4n + 3$ that is a residue of q and of which p is a nonresidue. Then the cases just proved (II) give $q\,R\,r, r\,N\,p$. So, if $p\,R\,q, q\,N\,p$, we would have $qr\,R\,p, pr\,R\,q, pq\,N\,r$, and therefore $-pq\,R\,r$. Thus the equation $pxx + qyy - rzz = 0$ would be solvable, contrary to the preceding observation; so the supposition cannot hold. Cases 1 and 2 of Article 131 follow from this.

This case is handled more neatly as follows. Let r be a prime of the form $4n + 3$ of which p is a nonresidue. Then we also have $r\,N\,p$, and so (assuming $p\,R\,q, q\,N\,p$)

$qr\,R\,p$. Further, $-p\,R\,q, -p\,R\,r$, and therefore also $-p\,R\,qr$. So the equation $xx + pyy - qrzz = 0$ would be solvable, contrary to the preceding observation. From this, and so on.

IV. If p is a prime of the form $4n + 1$ and q a prime of the form $4n + 3$, we cannot have $p\,R\,q, q\,N\,p$ simultaneously. Take an auxiliary prime r of the form $4n+1$ that is a nonresidue of both p, q. Then (by II) $q\,N\,r$, and (by III) $p\,N\,r$; hence $pq\,R\,r$. So, if $p\,R\,q, q\,N\,p$, we would also have $pr\,N\,q, -pr\,R\,q, qr\,R\,p$, and the equation $pxx - qyy + rzz = 0$ would be solvable, *which is absurd*. — Cases 3 and 6 of Article 131 follow from this.

V. Let p, q be primes of the form $4n+3$. We cannot have $p\,N\,q, q\,N\,p$ simultaneously. For suppose this were possible, and take an auxiliary prime r of the form $4n+1$ that is a nonresidue of both p, q. We would have $qr\,R\,p, pr\,R\,q$; further (by II), $p\,N\,r, q\,N\,r$, giving $pq\,R\,r$ and $-pq\,R\,r$. Thus the equation $-pxx-qyy+rzz = 0$ would be possible, contrary to the preceding observation. Case 8 of Article 131 follows from this.

297.

Anyone looking more closely at the preceding proof will readily see that cases I and II have been settled without anything to object to. But the proofs of the other cases rely on the existence of auxiliary numbers. Unless that existence is proved, the method clearly loses all force. These assumptions may be so plausible that a less attentive reader might think they need no proof, and they certainly raise the theorem to be proved to the highest degree of *probability*; still, if geometric rigor is wanted, they must not be admitted without proof. As for the assumption in IV and V that there is a prime r of the form $4n+1$ that is a nonresidue of two other given primes p, q, Section IV readily shows that all numbers less than $4pq$ and coprime to it (there are $2(p-1)(q-1)$ of them) divide equally into four classes. One contains nonresidues of both p, q; the other three, residues of p and nonresidues of q, nonresidues of p and residues of q, and residues of both p, q. In each class, half the numbers are of the form $4n+1$ and half of the form $4n+3$. So among them there will be $\frac{1}{4}(p-1)(q-1)$ nonresidues of both p, q of the form $4n+1$. Call these $g.g', g''$, and so on, and let the remaining $\frac{7}{4}(p-1)(q-1)$ numbers be h, h', h'', and so on. Clearly all numbers contained in the forms $4pqt+g, 4pqt+g', 4pqt+g''$, and so on, (G) will also be nonresidues of p, q of the form $4n+1$. To establish the assumption, we therefore only need to prove that the forms (G) certainly contain *prime numbers*. This already seems very plausible in itself, since these forms, together with $4pqt+h, 4pqt+h'$, and so on, (H), contain all numbers coprime to $4pq$, and therefore also all prime numbers (except $2, p, q$). There seems to be no reason why the series of primes should not be equally distributed among those forms, so that an eighth belong to (G) and the rest to (H). Yet such reasoning clearly falls far short of geometric rigor. The distinguished Le Gendre himself admits that it seems quite difficult to prove the theorem that a form $kt+l$, with k, l given coprime numbers and t varying, certainly contains primes. He briefly points to a method that might lead there. But many preliminary investigations seem necessary to us before this route, at least, could lead to a rigorous proof. — — As for the other assumption (III, second method), that there is a prime r of the form $3n+3$ of which another given prime p of the form $4n+1$ is a nonresidue, the distinguished Le Gendre has added nothing at all. We proved above (Article 129) that primes of which p is a nonresidue certainly exist. But our method hardly seems suited to showing the existence of such primes *that are also of the form* $4n+3$, as is required here, though not in our first proof. We can, however, readily prove the truth of this assumption as follows. By Article 287 there is a positive genus of binary forms of determinant $-p$ with character $3, 4$; Np. Let (a, b, c) be such a form, with a odd, as we may assume. Then a will be of the form $4n+3$, and will either itself be prime or at least have a prime factor r of the form $4n+3$. But $-pRa$, and therefore also $-pRr$, giving pNr. Still, we must carefully note that the propositions of Articles 263, 287 rely on the fundamental theorem. So it would be circular reasoning to base any part of it on them. — — Finally, the assumption in III of the first method is much more unsupported still, so there is no need to add anything further about it here.

Let us add an observation on case V, which the preceding method does not adequately prove, but which is readily settled by the following argument. If we had

pNq, qNp simultaneously there, then $-pRq, -qRp$, from which we readily derive that -1 is a characteristic number of the form $(p, 0, q)$. So, by the theory of ternary forms, this form can be represented by $xx + yy + zz$. Let

$$ptt + quu = (\alpha t + \beta u)^2 + (\alpha' t + \beta' u)^2 + (\alpha'' t + \beta'' u)^2$$

or

$$\begin{aligned} \alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' &= p, \\ \beta\beta + \beta'\beta' + \beta''\beta'' &= q, \\ \alpha\beta + \alpha'\beta' + \alpha''\beta'' &= 0 \end{aligned}$$

Then equations 1 and 2 make all $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ odd. But clearly the third equation cannot then hold. — Case II can also be settled in much the same way.

298.

PROBLEM. *Let a, b, c be any numbers, none of them $= 0$. Find the conditions under which the equation*

$$axx + byy + czz = 0 \ldots (\omega).$$

Solution. Let $\alpha\alpha, \beta\beta, \gamma\gamma$ be the largest squares dividing bc, ac, ab, respectively, and set $\alpha a = \beta\gamma A,\ \beta b = \alpha\gamma B,\ \gamma c = \alpha\beta C$. Then A, B, C will be pairwise coprime integers. The equation (ω) will be solvable or unsolvable according as

$$AXX + BYY + CZZ = 0 \ldots (\Omega)$$

is solvable or unsolvable. This can be decided by Article 294.

Proof. Set $bc = \mathfrak{A}\alpha\alpha,\ ac = \mathfrak{B}\beta\beta,\ ab = \mathfrak{C}\gamma\gamma$. Then $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ are integers free of square factors, and $\mathfrak{A} = BC,\ \mathfrak{B} = AC,\ \mathfrak{C} = AB$. So $\mathfrak{A}\mathfrak{B}\mathfrak{C} = (ABC)^2$, and therefore $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ is necessarily an integer. Let the greatest common divisor of the numbers $\mathfrak{A}, A\mathfrak{A}$ be m, and let $\mathfrak{A} = gm,\ A\mathfrak{A} = hm$. Then g is coprime to h and, since $\mathfrak{A}$ is free of square factors, also to m. Now $hhm = gAA\mathfrak{A} = g\mathfrak{B}\mathfrak{C}$, so g divides hhm, which is clearly impossible unless $g = \pm 1$. Thus $\mathfrak{A} = \pm m,\ A = \pm h$, so it is an integer; similarly, B, C are integers. *This proves the first assertion.* — Since $\mathfrak{A} = BC$ has no square factors, B, C must be coprime. Similarly, A is coprime to C and to B. *This proves the second assertion.* — Finally, if (Ω) is satisfied by $X = P, Y = Q,\ Z = R$, then clearly (ω) is solved by $x = \alpha P, y = \beta Q, z = \gamma R$. Conversely, if the latter is satisfied by $x = p, y = q, z = r$, the former is satisfied by $X = \beta\gamma p,\ Y = \alpha\gamma q, Z = \alpha\beta r$. So either both are solvable or neither is. *This proves the third assertion.*

Representation of zero by arbitrary ternary forms.

299.

PROBLEM. *Given a ternary form*

$$f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$$

determine whether it can represent zero, with values of the indeterminates that are not all $= 0$.

Solution. I. When $a = 0$, the values of x', x'' can be chosen at will. The equation

$$a'x'x' + 2bx'x'' + a''x''x'' = -2x(b'x'' + b''x')$$

clearly gives x a definite rational value. Whenever this gives a fraction for x, we need only multiply the values of x, x', x'' by its denominator to obtain integers. The only values of x', x'' to exclude are those making $b'x'' + b''x' = 0$, unless they also make $a'x'x' + 2bx'x'' + a''x''x'' = 0$, in which case x can be chosen at will. It is also clear that all possible solutions can be obtained in this way. The case where b' is zero and $b'' = 0$ holds does not belong here: then x does not occur in f, so f is a binary form,

and whether it can represent zero must be decided from the theory of such forms applied to f.

II. When $a = 0$ does not hold, the equation $f = 0$ is equivalent to

$$(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = 0$$

where we set

$$b''b'' - aa' = A'',$$
$$ab - b'b'' = B,$$
$$b'b' - aa'' = A'$$

If here $A' = 0$ but not $B = 0$, then choosing $ax + b''x' + b'x''$ and x'' at will clearly determines x and x' rationally. If they are not integers, a suitable multiplier will at least make them integers. For the one value of x'', namely $x'' = 0$, the value of $ax + b''x' + b'x''$ is not arbitrary: it too must be set $= 0$. But then x' can be chosen at will and will give a rational value of x. — If, however, A'' is zero and $B = 0$ holds, and if A' is a square $= kk$, then $f = 0$ clearly reduces to the two linear equations

$$ax + b''x' + (b' + k)x'' = 0,$$
$$ax + b''x' + (b' - k)x'' = 0$$

of which *either* one *or* the other must hold. If instead, under the same assumption, A' is not a square, the solution of the proposed equation clearly depends on $x'' = 0$ and $ax + b''x' = 0$, which must hold *simultaneously*.

It hardly needs mentioning that the method in I also applies when a' is zero or $a'' = 0$ holds, and the method in II when $A' = 0$.

III. When neither a is zero nor $A'' = 0$ holds, the equation $f = 0$ is equivalent to

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''x'' = 0$$

where D denotes the determinant of the form f, or Da denotes the number $BB - A'A''$. When $D = 0$, the solution works much as at the end of the preceding case. If A'' is a square $= kk$, the proposed equation reduces to

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0,$$
$$kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$$

but if A'' is not a square, we must have

$$ax + b''x' + b'x'' = 0,$$
$$A''x' - Bx'' = 0$$

When, however, D is not $= 0$, we have reduced the problem to

$$A''tt - uu + Davv = 0$$

whose solvability can be decided by the preceding article. If its only solution is $t = 0,\ u = 0,\ v = 0$, then clearly the proposed equation also has no solution other

than $x = 0,\ x' = 0,\ x'' = 0$. But if it has another solution, any such integer values of t, u, v give, through the equations

$$\begin{aligned} ax + b''x' + b'x'' &= t, \\ A''x' - Bx'' &= u, \\ x'' &= v \end{aligned}$$

at least rational values of x, x', x''. If these involve fractions, a suitable multiplier will make them integers.

As soon as *one* integer solution of $f = 0$ has been found, the problem can be reduced to case I, and all solutions found as there, in the following way. Let $f = 0$ be satisfied by the values of x, x', x'' given by $\alpha, \alpha', \alpha''$, which we assume have no common factor. Choose integers $\beta, \beta', \beta'',\ \gamma, \gamma', \gamma''$ by Articles 40, 279 so that

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1$$

and let f change under the substitution

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y''. \\ x' &= \alpha' y + \beta' y' + \gamma' y'', \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \ldots (S) \end{aligned}$$

into

$$g = cyy + c'y'y' + c''y''y'' + 2dy'y'' + 2d'yy'' + 2d''yy'$$

Then clearly $c = 0$, and g is equivalent to f. So from all solutions of $g = 0$ we readily obtain, through S, all integer solutions of $f = 0$. Now I shows that all solutions of $g = 0$ are contained in the formulas

$$\begin{aligned} y &= -z(c'pp + 2dpq + c''qq), \\ y' &= 2z(d''pp + d'pq), \\ y'' &= 2z(d''pq + d'qq) \end{aligned}$$

where p, q are arbitrary integers and z is an arbitrary number, for which fractions are also allowed, provided y, y', y'' remain integers. Substituting these values of y, y', y'' in (S) gives all integer solutions of $f = 0$. — For example, if

$$f = xx + x'x' + x''x'' - 4x'x'' + 2xx'' + 8xx'$$

and one solution of $f = 0$ is $x = 1,\ x' = -2,\ x'' = 1$, then setting $\beta, \beta', \beta'',\ \gamma, \gamma', \gamma'' = 0, 1, 0, 0, 0, 1$ gives

$$g = y'y' + y''y'' - 4y'y'' + 12yy''$$

So all integer solutions of $g = 0$ are contained in the formula

$$\begin{aligned} y &= -z(pp - 4pq + qq), \\ y' &= 12zpq, \\ y'' &= 12zqq \end{aligned}$$

and therefore all solutions of $f = 0$ in

$$x = -z(pp - 4pq + qq)$$
$$x' = 2z(pp + 2pq + qq)$$
$$x'' = -z(pp - 4pq - 11qq)$$

General solution in rational numbers of indeterminate equations of the second degree in two unknowns.

300.

The problem of the preceding article directly gives the solution of the indeterminate equation

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

when only rational values are required. We have already solved it above, in Article 216 and the following articles, when integers are required. For all rational values of x, y can be written as $\frac{t}{v}, \frac{u}{v}$, with t, u, v integers. So solving that equation in rational numbers is clearly the same as solving

$$att + 2btu + cuu + 2dtv + 2euv + fvv = 0$$

in integers; this is the equation treated in the preceding article. Only solutions with $v = 0$ must be excluded. Such solutions cannot occur when $bb - ac$ is not a square. For example, all rational solutions of the equation

$$xx + 8xy + yy + 2x - 4y + 1 = 0$$

which was solved generally in integers in Article 221, are contained in the formula

$$x = \frac{pp - 4pq + qq}{pp - 4pq - 11qq},$$
$$y = -\frac{2pp + 4pq + 2qq}{pp - 4pq - 11qq}$$

where p, q are any integers. — We have dealt only briefly here with these two closely connected problems, and have left out many observations related to them, partly to avoid too long a discussion and partly because we have another solution of the problem in the preceding article, based on more general principles. Since explaining it requires a deeper investigation of ternary forms, we must reserve it for another occasion.

On the average number of genera.

301.

We return to binary forms, several of whose remarkable properties still need to be discussed. First we will add some observations on the number of genera and classes in the properly primitive order, positive for negative determinants. For brevity we restrict the investigation to this order.

The *number of genera* into which all properly primitive forms, positive for negative determinants, of a given positive or negative determinant $\pm D$ divide is always $1, 2, 4$ or a higher power of 2. Its exponent depends on the factors of D and can be found entirely in advance from the preceding investigations. Since primes are mixed with numbers of varying degrees of compositeness in the natural series of numbers, the number of genera for several successive determinants $\pm D, \pm(D+1), \pm(D+2)$, and so on, now increases and now decreases, and this irregular series seems to have no order. Yet if we add the numbers of genera corresponding to many successive determinants

$$\pm D, \quad \pm(D+1) \ \ldots \ \pm(D+m)$$

and divide the sum by the number of determinants, we obtain the *average number of genera*. This can be regarded as applying around the middle determinant $\pm(D+\frac{1}{2}m)$, and forms a very regular progression. We assume not only that m is large enough, but also that D is much larger, so that the ratio of the extreme determinants $D, D+m$ does not differ too much from equality. The regularity of this progression is to be understood as follows. If D' is much larger than D, the average number of genera around the determinant $\pm D'$ will be noticeably larger than around D. But if D, D' do not differ too much, the average numbers of genera around D and D' will also be nearly equal. Further, the average number of genera around the positive determinant $+D$ is always found nearly equal to the average around the negative one, and the more closely so the larger D is. For a small value the former is a little larger than the latter. The following examples, taken from a table classifying binary forms for more than 4000 determinants, will illustrate these observations. Among the hundred determinants from 801 to 900, there are 7 to which just one genus corresponds, and $32, 52, 8, 1$ to which $2, 4, 8$. 16 genera correspond, respectively. This gives 359 genera in all, so the average number = 3,59. The hundred negative determinants from -801 to 900 give 360 genera. All the following examples come from negative determinants. In the 16th hundred, from -1501 to -1600, the average number of genera is 3,89; in the 25th hundred it is 4,03; in the 51st it is 4,24; from the six hundred determinants $-9401 \ \ldots -10000$ we obtain 4,59. These examples show that the average number of genera grows much more slowly than the determinants themselves. But what is the law of this progression? — A rather difficult theoretical investigation, which would take too long to explain here, has shown that the average number of genera around the determinant $+D$ or $-D$ is very closely given by

$$\alpha \log D + \beta$$

where α, β are constants, namely

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

with π denoting half the circumference of a circle of radius 1, and

$$\beta = 2\alpha g + 3\alpha\alpha h - \frac{1}{6}\alpha \log 2 = 0{,}8830460462$$

where g is the sum of the series

$$1 - \log(1+1) + \frac{1}{2} - \log(1+\frac{1}{2}) + \frac{1}{3} - \log(1+\frac{1}{3}) + \text{etc.} = 0{,}5772156649$$

(see Euler, *Inst. Calc. Diff.*, p. 444), while h is the sum of the series

$$\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 + \text{etc.}$$

which has been found by approximation = 0,9375482543. This formula shows that the average number of genera increases in an arithmetic progression when the determinants increase in a geometric progression. The values of this formula for $D = 850\frac{1}{2}$, $1550\frac{1}{2}, 2450\frac{1}{2}, 5050\frac{1}{2}, 9700\frac{1}{2}$ are 3,617; 3,86; 4,046; 4,339; 4,604, differing little from the averages given above. The larger the middle determinant, and the more determinants used to calculate the average, the less it will differ from the value of the formula. This formula also lets us find very closely the total number of genera corresponding to successive determinants $\pm D, \pm(D+1) \ldots \pm (D+m)$, however far apart the extremes $D, D+m$ are, by calculating and adding the corresponding average numbers for each. This sum will be

$$= \alpha(\log D + \log(D+1) + \text{etc.} + \log(D+m)) + \beta(m+1)$$

or, with sufficient accuracy,

$$= \alpha((D+m)\log(D+m) - (D-1)\log(D-1)) + (\beta - \alpha)(m+1)$$

In this way the sum of the numbers of genera for the determinants -1 to -100 is found = 234,4, while it is actually 233; similarly, from -1 to -2000, = 7116,6, while it is 7112; from -9001 to -10000, where it is 4595, the formula gives 4594,9. Such agreement could hardly have been expected.

On the average number of classes.

302.

As regards the *number of classes*, always understood as properly primitive classes, positive for negative determinants, positive determinants behave quite differently from negative ones. So we will consider the two separately. They agree in this: for a given determinant, each genus contains equally many classes. Thus the total number of classes equals the product of the number of genera and the number of classes in each genus.

First, for negative determinants, the number of classes corresponding to several successive determinants $-D, -(D+1), -(D+2)$, and so on, forms just as irregular a progression as the number of genera. But the average number of classes, which will need no definition, grows very regularly, as the following examples show. The hundred determinants from -500 to -600 give 1729 classes, so the average number $= 17{,}29$. Similarly, in the 15th hundred the average number of classes is 28,26; from the two hundreds 24 and 25 we obtain 36,28; from the three 61, 62 and 63 we get 58,50; from the five $91 \ldots 95$, 71,56; finally, from the five $96 \ldots 100$, 73,54. These examples show that the average number of classes grows more slowly than the determinants, but much faster than the average number of genera. A little attention shows that it grows quite closely in proportion to the square roots of the middle determinants. Indeed, a theoretical investigation has shown us that the average number of classes around the determinant $-D$ is approximately expressed by

$$\gamma\sqrt{D} - \delta$$

where

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$$

with e denoting the sum of the series

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} \text{ etc.}$$

$$\delta = 0{,}2026423673 = \frac{2}{\pi\pi}$$

The averages calculated by this formula differ little from those taken above from the table of classifications. This formula also lets us find very closely the total number of all properly primitive classes, positive for negative determinants, corresponding to successive determinants $-D, -(D+1), -(D+2) \ldots -(D+m-1)$, however far apart the extremes may be, by adding the averages corresponding to those determinants according to the formula. This gives

$$= \gamma(\sqrt{D} + \sqrt{(D+1)} + \text{etc.} + \sqrt{(D+m-1)}) - \delta m$$

or, very nearly,

$$= \frac{2}{3}\gamma((D+m-\frac{1}{2})^{\frac{3}{2}} - (D-\frac{1}{2})^{\frac{3}{2}}) - \delta m$$

For example, for the hundred determinants $-1 \ldots -100$ this total is calculated from the formula $= 481{,}1$, while it is actually 477. The thousand determinants $-1 \ldots -1000$ give 15533 classes according to the table; the formula gives 15551,4. The second thousand gives 28595 classes according to the table, and the formula 28585,7; similarly, the third thousand actually gives 37092 classes, and the formula 37074,3; the tenth thousand gives 72549 by the table, and 72572 by the formula.

303.

The table of negative determinants, arranged by their different classifications, offers many other remarkable observations. For determinants of the form $-(8n+3)$, the number of classes, both in all the properly primitive genera together and in each separately, is always divisible by 3, with the sole exception of the determinant -3. The reason follows directly from Article 256, VI. For determinants whose forms make up a single genus, the number of classes is always odd. For such a determinant there is just one ambiguous class, the principal class; the remaining classes occur in opposite pairs, so their number must be even, and the total odd. This latter property also holds for positive determinants. — Further, the sequence of determinants corresponding to any given classification, that is, to given numbers of genera and classes, always seems to end. We illustrate this rather surprising observation with a few examples. The first number, in Roman numerals, gives the number of properly primitive genera, positive for negative determinants; the next gives the number of classes in each genus. Then follows the sequence of determinants with this classification, their negative sign being omitted for brevity.

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

Similarly, there are 20 determinants, the largest $= -1423$, with classification I. 9; 4, the largest $= -1303$, with classification I. 11; and so on. Classifications II. 3; II. 4; II. 5; IV. 2 correspond to no more than $48, 31, 44, 69$ determinants, respectively, the largest of these being $-652, -862, -1318, -1012$. The table from which we took these examples has been extended far beyond the largest determinants occurring here*), without any further determinants of these classifications appearing. So there seems no doubt that the sequences listed really have ended, and by analogy we may extend the same conclusion to any other classification. For example, since the entire tenth thousand of determinants offered none with fewer than 24 classes, it is highly likely that classifications I. 23; I. 21, and so on; II. 11; II. 10, and so on; IV. 5; IV. 4; IV. 3; VIII. 2 had already ended before -9000, or at least apply to very few determinants beyond -10000. But *rigorous* proofs of these observations seem very

*) As this is being printed, *continuously* as far as -3000, and also through the entire tenth thousand and several other scattered hundreds, together with very many individual determinants carefully chosen.

difficult. — It is no less remarkable that every determinant whose forms divide into 32 or more genera has at least two classes in each genus. Thus classifications XXXII. 1, LXIV. 1, and so on, do not occur at all; the smallest such determinant, -9240, has classification XXXII. 2. It seems quite probable that, as the number of genera grows, more and more classifications fail to occur. In this respect the 65 determinants given above, with classifications I. 1; II. 1; IV. 1; VIII. 1; XVI. 1, are very noteworthy. It is easy to see that they, and only they, have both these remarkable properties: all their classes of forms are ambiguous, and any forms contained in the same genus must be both properly and improperly equivalent. These same 65 numbers were already given by the distinguished Euler, from a slightly different viewpoint to be mentioned below and with a criterion easy to prove, in *Nouv. Mém. de l'Ac. de Berlin*, 1776, p. 338.

304.

The number of properly primitive classes formed by binary forms with a positive *square* determinant kk can be determined entirely in advance. It equals the number of numbers coprime to $2k$ and smaller than it. From this, arguments that are not difficult but must be omitted here show that the average number of classes for such determinants around kk is approximately expressed by $\frac{8k}{\pi\pi}$. — Positive nonsquare determinants, however, show quite remarkable behavior in this respect. For negative and square determinants, a small number of classes, for example classification I. 1 or I. 3 or II. 1, and so on, occurs only for small determinants and soon ceases altogether. By contrast, by far the greatest part of positive nonsquare determinants, at least those not very large, have classifications with just one class in each genus, so that I. 3; I. 5; II. 2; II. 3; IV. 2, and so on, are very rare. For example, among the 90 nonsquare determinants below 100, there are $11, 48, 27$ with classifications I. 1, II. 1, IV. 1, respectively. Only one, (37), has I. 3; two, (34 and 82), have II. 2; one, (79), has II. 3. Yet as the determinants grow, larger numbers of classes gradually become more frequent. Thus among the 96 nonsquare determinants from 101 to 200, two, $(101, 197)$, have I. 3; four, $(145, 146, 178, 194)$, have II. 2; three, $(141, 148, 189)$, have II. 3. Of the 197 determinants from 801 to 1000, three have I. 3; four II. 2; fourteen II. 3; two II. 5; two II. 6; fifteen IV. 2; six IV. 3; two IV. 4; four VIII. 2; the remaining 145 have one class in each genus. — It would be an interesting question, worthy of mathematicians' ingenuity, to investigate the law by which determinants with one class in each genus become steadily rarer. So far we can neither decide theoretically nor conjecture with enough confidence from observation whether they eventually cease altogether, which seems unlikely, or at least become *infinitely rare*, or whether their frequency comes ever closer to a fixed limit. The average number of classes grows only a little faster than the number of genera, and far more slowly than the square roots of the determinants. Between 800 and 1000 it is found $= 5, 01$. Let us add another observation that partly restores the analogy between positive and negative determinants. We have found that, for a positive determinant D, it is not so much the number of classes itself as this number multiplied by the logarithm of $t + u\sqrt{D}$, where t, u are the smallest numbers other than $1, 0$ satisfying $tt - Duu = 1$, that is analogous in several ways to the number of classes for a negative determinant.

These ways cannot be explained more fully here. The average value of that product is expressed just as accurately by a formula of the form $m\sqrt{D} - n$. But so far we have not been able to determine the values of the constants m, n theoretically. If any conclusion may be drawn from comparing a few hundreds of determinants, m seems to differ little from $2\frac{1}{3}$. — We reserve for another occasion a fuller discussion of the principles behind the preceding investigations into averages of quantities that do not follow an analytic law, but approach such a law asymptotically ever more closely. We now turn to another investigation, comparing different properly primitive classes of the same determinant, and bringing this long section to an end.

A special algorithm for properly primitive classes: regular and irregular determinants, and related matters.

305.

THEOREM. *Let K be the principal class of forms of a given determinant D, and C any other class in the principal genus of forms of the same determinant. Let $2C, 3C, 4C$, and so on, be the classes obtained by doubling, tripling, quadrupling, and so on, the class C, as in Article* 249. *If the progression $C, 2C, 3C$, and so on, is continued far enough, it eventually reaches a class identical with K. If mC is the first class identical with K, and the total number of classes in the principal genus $= n$, then either $m = n$ or m is a proper divisor of n.*

Proof. I. All the classes $K, C, 2C, 3C$, and so on, must belong to the principal genus by Article 247, so the first $n+1$ classes of this series, $K, C, 2C \ldots nC$, clearly cannot all be different. Thus either K is identical with one of the classes $C, 2C, 3C \ldots nC$, or at least two of these classes are identical with each other. Let $rC = sC$ and $r > s$. Then also

$$(r-1)C = (s-1)C, \quad (r-2)C = (s-2)C$$
$$\text{etc. and } (r+1-s)C = C$$

giving $(r-s)C = K$. *This proves the first assertion.*

II. This also gives at once either $m = n$ or $m < n$. It remains only to show that, in the latter case, m is a proper divisor of n. Since the classes

$$K, C, 2C \ldots (m-1)C, \text{ whose collection we denote by } \mathfrak{C}$$

do not yet exhaust the whole principal genus in this case, let C' be a class of this genus not contained in $\mathfrak{C}$. Consider the collection of classes obtained by composing C' with each class in $\mathfrak{C}$, namely

$$C', C'+C, C'+2C \ldots C'+(m-1)C, \text{ denoted by } \mathfrak{C}'$$

It is easy to see that all classes in $\mathfrak{C}'$ differ both from one another and from all those in $\mathfrak{C}$, and belong to the principal genus. If $\mathfrak{C}$ and $\mathfrak{C}'$ exhaust this genus, we therefore have $n = 2m$; if not, $2m < n$. In the latter case let C'' be a class of the principal genus contained in neither $\mathfrak{C}$ nor $\mathfrak{C}'$, and consider the collection of classes obtained by composing C'' with each class in $\mathfrak{C}$, that is,

$$C'', C''+C, C''+2C \ldots C''+(m-1)C, \text{ denoted by } \mathfrak{C}''$$

These clearly all differ from one another and from all those in $\mathfrak{C}$ and $\mathfrak{C}'$, and belong to the principal genus. So if $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ exhaust this genus, $n = 3m$; otherwise $n > 3m$. In that case another class C''', contained in the principal genus but in neither $\mathfrak{C}, \mathfrak{C}'$ nor $\mathfrak{C}''$, can be treated in the same way and shows that either $n = 4m$ or $n > 4m$, and so on. Since n and m are finite numbers, the principal genus must eventually be exhausted. Then n is a multiple of m, or m a proper divisor of n. *This proves the second assertion.*

Example. Let $D = -356$, $C = (5, 2, 72)$*). We find $2C = (20, 8, 21), 3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Here we therefore have $m = 6$, while n for this determinant is 12. Taking for C' the class $(8, 2, 45)$, the other five classes in $\mathfrak{C}'$ are $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

*) Classes are always expressed here by the simplest *forms* contained in them.

306.

The proof of the preceding theorem will be found entirely analogous to the proofs in Articles 45, 49. Indeed, the theory of multiplication of classes has a very close affinity in every respect with the subject treated in Section III. But the limits of this work do not let us pursue this theory as fully as it deserves. So we will add only a few observations here, also leaving out proofs that would require a longer preparation, and reserve a fuller investigation for another occasion.

I. If the series $K, C, 2C, 3C$, and so on, is continued beyond $(m-1)C$, the same classes appear again:

$$mC = K, \quad (m+1)C = C, \quad (m+2)C = 2C \text{ etc.}$$

More generally, regarding K as $0C$ for convenience, the classes $gC, g'C$ are identical or different according as g and g' are congruent or incongruent modulo m. Thus the class nC is always identical with the principal class K.

II. We will call the collection of classes $K, C, 2C \ldots (m-1)C$, denoted above by $\mathfrak{C}$, the *period* of the class C. This expression must not be confused with the *periods of reduced forms* of positive nonsquare determinant treated in Article 186 and the following articles. Clearly, composing any number of classes in the same period produces a class also contained in that period:

$$gC + g'C + g''C \text{ etc.} = (g + g' + g'' + \text{etc.})C$$

III. Since $C + (m-1)C = K$, the classes C and $(m-1)C$ are opposite; so are $2C$ and $(m-2)C$, $3C$ and $(m-3)C$, and so on. If m is even, the class $\frac{1}{2}mC$ is therefore opposite to itself and so *ambiguous*. Conversely, if $\mathfrak{C}$ contains another ambiguous class besides K, say gC, then $gC = (m-g)C$, giving $g = m - g = \frac{1}{2}m$. Thus, if m is even, there can be no ambiguous class other than K and $\frac{1}{2}mC$; if m is odd, none other than K can be contained in $\mathfrak{C}$.

IV. Suppose the period of a class hC contained in $\mathfrak{C}$ is

$$K, hC, 2hC, 3hC \ldots (m'-1)hC$$

Then $m'h$ is clearly the smallest multiple of h divisible by m. So if m and h are coprime, $m' = m$, and the two periods contain the same classes arranged in different orders. More generally, if μ denotes the greatest common divisor of m, h, then $m' = \frac{m}{\mu}$. Thus the number of classes in the period of any class from $\mathfrak{C}$ is either m or a proper divisor of m. More precisely, as many classes in $\mathfrak{C}$ have periods of m terms as there are numbers among $0, 1, 2 \ldots m-1$ coprime to m, that is, φm, using the notation of Article 39. In general, as many classes in $\mathfrak{C}$ have periods of $\frac{m}{\mu}$ terms as there are numbers among $0, 1, 2 \ldots m-1$ having μ as their greatest common divisor with m. Their number is readily seen to be $\varphi\frac{m}{\mu}$. So if $m = n$, that is, if $\mathfrak{C}$ contains the *whole* principal genus, this genus contains exactly φn classes whose periods include the whole genus, and φe classes whose periods have e terms, where e is any divisor of n. This conclusion holds in general whenever the principal genus contains a class whose period has n terms.

V. Under the same assumption, the system of classes of the principal genus is most conveniently arranged by adopting a class whose period has n terms as a kind of *base*, and placing the classes of the principal genus in the order in which they occur in that period. If we assign the *index* 0 to the principal class, 1 to the class chosen as base, and so on, then merely adding indices tells us which class results from composing any classes of the principal genus. Here is an example for the determinant -356, with the class $(9, 2, 40)$ chosen as base:

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. The analogy with Section III, together with examination of more than 200 negative determinants and far more positive nonsquare ones, may seem to make it highly probable that this assumption holds for *all* determinants. Yet that conclusion would be false, and extending the table of classifications would refute it. For brevity, let us call determinants for which the whole principal genus can be included in a single period *regular*, and the others, for which this is impossible, *irregular*. This subject seems to belong to the deepest mysteries of higher arithmetic and to leave room for extremely difficult investigations. We can illustrate it here only with a few observations, preceded by the following general one.

VII. If the principal genus contains classes C, C' whose periods consist of m, m' classes, and M is the smallest number divisible by m and m', then the same genus also contains classes whose periods have M terms. Resolve M into two coprime factors r, r', the former (r) dividing m and the latter (r') dividing m', as in Article 73. Then the class $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ has the required property. For suppose the period of C'' has g terms. Then

$$\begin{aligned} K = grC'' &= gmC + \frac{grm'}{r'}C' \\ &= K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C' \end{aligned}$$

so $\frac{grm'}{r'}$ must be divisible by m', or gr by r', and therefore also g by r'. In exactly the same way g is found divisible by r, and so also by $rr' = M$. But clearly $MC'' = K$, so M is also divisible by g. Thus necessarily $M = g$. It readily follows that the *largest* number of classes contained in any period for a given determinant is divisible by the number of classes in every other period of a class from the same principal genus. This also gives a method of finding a class whose period is as large as possible, and so, for a regular determinant, includes the whole principal genus. It is entirely analogous to the method of Articles 73, 74, though in practice various devices can shorten the work. The quotient of n by the number of classes in the largest period is 1 for regular determinants, but for irregular ones is always an integer greater than 1. For the latter it is particularly convenient for expressing the different kinds of irregularity, and may therefore be called the *irregularity exponent*.

VIII. So far there is no general rule for distinguishing regular from irregular determinants in advance, especially since the latter include both primes and composite numbers. A few particular observations must therefore suffice. If the principal genus contains more than two ambiguous classes, the determinant is certainly irregular and its irregularity exponent even. If that genus contains just one or two, the determinant is either regular or at least has an odd irregularity exponent. All negative determinants of the form $-(216k+27)$, except -27 alone, are irregular, with irregularity exponent divisible by 3. The same holds for negative determinants of the forms $-(1000k+75)$ and $-(1000k+675)$, except -75 alone, and for infinitely many others. If the irregularity exponent is a prime p, or is at least divisible by p, then n is divisible by pp. Thus if n has no square divisor, the determinant is certainly regular. Only for positive *square* determinants ee can we always tell in advance whether they are regular or irregular: regular when e is 1 or 2, an odd prime or a power of an odd prime, and irregular in all other cases. Among negative determinants, irregular ones grow steadily more frequent as the determinants grow. *For example*, in the whole first thousand there are thirteen irregular ones: omitting the negative sign, $576, 580, 820, 884, 900$, whose irregularity exponent is 2, and $243, 307, 339, 459, 675, 755, 891, 974$, whose irregularity exponent is 3. In the second thousand we have found 13 with exponent 2 and 15 with exponent 3; in the tenth thousand, 31 with exponent 2 and 32 with exponent 3. We cannot yet decide whether determinants with irregularity exponent greater than 3 occur below -10000. Beyond this limit any given exponent can occur. It is highly probable that, as the determinants grow, the frequency of irregular negative determinants relative to regular ones approaches a constant ratio ever more closely. Determining that ratio would be very worthy of mathematicians' ingenuity. — For positive nonsquare determinants, irregular ones are much rarer. Certainly infinitely many have an even irregularity exponent, *for example* 3026, for which it is 2. There also seems no doubt that ones with odd irregularity exponent exist, although we must admit that so far none has presented itself to us.

IX. For brevity we cannot discuss here the most convenient arrangement of the system of classes in the principal genus for an irregular determinant. We only observe that, since a single base does not suffice, two or even more classes must be chosen, from whose multiplication and composition all the classes can be produced. This gives *double or multiple indices*, serving much the same purpose as single indices for regular determinants. We will treat this more fully another time.

X. Finally, all the properties considered in this and the preceding article depend chiefly on the number n, which is analogous to $p-1$ in Section III. So this number deserves the closest attention, and it is most desirable to discover a general connection between it and its determinant. We think there is all the less reason to lose hope about this very important question, since we have already succeeded in expressing by an analytic formula the average value of the product of n and the number of genera, which can be determined in advance, at least for negative determinants, in Article 302.

307.

The investigations of the preceding articles cover only the classes of the principal genus. So they suffice both for positive determinants with just one genus altogether and for negative determinants with just one positive genus, if we choose not to consider the negative genus. It remains to add some observations on the other properly primitive genera as well.

I. If a genus G', different from the principal genus G of the same determinant, contains any ambiguous class, it contains as many as G. Let the ambiguous classes in G be $L,\ M, N$, and so on, including the principal class K, and those in G' be L', M', N', and so on. Denote the collection of the former by A, and of the latter by A'. Clearly all the classes $L + L',\ M + L',\ N + L'$, and so on, are ambiguous and different, and belong to G', so must be contained in A'. Thus the number of classes in A' certainly cannot be smaller than in A. Likewise the classes $L' + L'$, $M' + L',\ N' + L'$, and so on, are different and ambiguous, belong to G, and so are contained in A. Thus the number of classes in A cannot be smaller than in A'. The numbers of classes in A and A' must therefore be equal.

II. Since the total number of ambiguous classes equals the number of genera, by Articles 261, 287 III, if G contains just one ambiguous class, then clearly *every* genus must contain one ambiguous class. If G contains two, half of all genera contain two each and the others none. Finally, if G contains more, say a[*)], one a-th of all the genera contain a ambiguous classes each, and the others none.

III. In the case where G contains two ambiguous classes, let G, G', G'', and so on, be the genera containing two each, and H, H', H'', and so on, those containing none. Denote the former collection by $\mathfrak{G}$ and the latter by $\mathfrak{H}$. Composing two ambiguous classes always gives an ambiguous class, by Article 249. So composing two genera from $\mathfrak{G}$ clearly always gives a genus from $\mathfrak{G}$. It follows further that composing a genus from $\mathfrak{G}$ with one from $\mathfrak{H}$ gives a genus from $\mathfrak{H}$. For if, *for example*, $G' + H$ belonged not to $\mathfrak{H}$ but to $\mathfrak{G}$, then $G' + H + G'$ would also have to belong to $\mathfrak{G}$. *This is a contradiction*, since $G' + G' = G$, and therefore $G' + H + G' = H$. Finally, the genera $G + H,\ G' + H,\ G'' + H$, and so on, together with $H + H,\ H' + H,\ H'' + H$, and so on, are clearly all different, and so coincide with $\mathfrak{G}$ and $\mathfrak{H}$ taken together. But by what we have just proved the genera $G+H,\ G'+H,\ G''+H$, and so on, all belong to $\mathfrak{H}$, and therefore exhaust this collection. So the remaining genera $H + H,\ H' + H$, $H'' + H$, and so on, must all belong to $\mathfrak{G}$. *That is*, composing two genera from $\mathfrak{H}$ always gives a genus from $\mathfrak{G}$.

IV. If E is a class of a genus V different from the principal genus G, then clearly $2E, 4E, 6E$, and so on, all belong to G, while $3E, 5E, 7E$, and so on, belong to V. If the period of $2E$ has m terms, then in the series $E, 2E, 3E$, and so on, the class $2mE$, and no earlier one, is clearly identical with K. So the period of E has $2m$ terms. Thus the number of terms in the period of any class outside the principal genus is either $2n$ or a proper divisor of $2n$, where n is the number of classes in each genus.

V. Let C be a given class of the principal genus G, and E a class of a genus V whose doubling gives C, which always exists by Article 286. Let all the ambiguous

[*)] This can happen only for irregular determinants, and a will always be a power of two.

classes, properly primitive and of the same determinant, be K, K', K'', and so on. Then *all* classes whose doubling gives C are E $(= E + K)$, $E + K'$, $E + K''$, and so on. Denote their collection by $\mathfrak{Q}$. Their number equals the number of ambiguous classes, or the number of genera. Clearly, as many classes in $\mathfrak{Q}$ belong to the genus V as there are ambiguous classes in G. Denoting this number by a, we see that each genus contains either a classes from $\mathfrak{Q}$ or none. Thus, when $a = 1$, each genus contains one class from $\mathfrak{Q}$; when $a = 2$, half of all genera contain two classes each from $\mathfrak{Q}$, and the rest none. The former half either coincides entirely with $\mathfrak{G}$, in the same sense as in III above, and the latter with $\mathfrak{H}$, or the latter coincides with $\mathfrak{G}$ and the former with $\mathfrak{H}$. — When a is larger still, one a-th of all the genera always contain classes from $\mathfrak{Q}$, each containing a classes.

VI. Now suppose C is a class whose period has n terms. In the case where $a = 2$, and therefore n is even, it is easy to see that none of $\mathfrak{Q}$ can belong to G. For such a class would then be contained in the period of C. If it were $= rC$, or $2rC = C$, then $2r \equiv 1 \pmod{n}$, *which is a contradiction*. Since G belongs to $\mathfrak{G}$, all the classes $\mathfrak{Q}$ must therefore be distributed among the genera $\mathfrak{H}$. Now, for a regular determinant, G contains exactly φn classes whose periods have n terms. So in the case $a = 2$, each genus $\mathfrak{H}$ contains exactly $2\varphi n$ classes whose periods include $2n$ terms, and therefore both their own genus and the principal genus. When $a = 1$, each genus other than the principal one contains φn such classes.

VII. On these observations we base the following method of arranging the system of *all* properly primitive classes as conveniently as possible for any given regular determinant; irregular ones are set aside entirely. Choose any class E whose period contains $2n$ terms, and therefore both its own genus, say V, and the principal genus G. Arrange the classes of these two genera in their order in that period. This already finishes the task when there are no more than these two genera, or when it seems unnecessary to add the others, *for example* for a negative determinant with just two positive genera. If four or more genera are to be arranged, treat the others as follows. Let V' be one of the others and $V + V' = V''$. Then V' and V'' together contain two ambiguous classes, either one in each or two in one and none in the other. From these choose any one A. Composing A with each class in G and V clearly gives $2n$ different classes belonging to V' and V'', and therefore exhausting these genera. So these too can be arranged. — If genera remain beyond these four, let V''' be one of them, and $V'''', V''''', V'''''' $ the genera obtained by composing V''' with V, V' and V''. These four genera $V''' \ldots V''''''$ contain four ambiguous classes. Choosing one of them, A', and composing it with each class in G, V, V', V'' clearly produces all classes in $V''' \ldots V''''''$. — If more genera remain, continue in the same way until all are exhausted. Clearly, if the number of genera to be arranged is 2^μ, we need exactly $\mu - 1$ ambiguous classes. Any class in these genera can be produced either by multiplication of E, or by composing a class obtained from such multiplication with one or more ambiguous classes. Here are two examples illustrating these rules. We cannot add more here on the use of such an arrangement or the devices that can lighten the work.

I. Determinant -161.

Four positive genera; four classes in each.

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. Determinant -546.

Eight positive genera; three classes in each.

G

1 and $3, 8; R3; R7; R13$

$(1, 0, 546) = K$
$(22, -2, 25) = 2E$
$(22, 2, 25) = 4E$

V

5 and $7, 8; N3; N7; N13$

$(5, 2, 110) = E$
$(21, 0, 26) = 3E$
$(5, -2, 110) = 5E$

V'

1 and $3, 8; N3; R7; N13$

$(2, 0, 273) = A$
$(11, -2, 50) = A + 2E$
$(11, 2, 50) = A + 4E$

V''

5 and $7, 8; R3; N7; R13$

$(10, 2, 55) = A + E$
$(13, 0, 42) = A + 3E$
$(10, -2, 55) = A + 5E$

V'''

1 and $3, 8; N3; N7; R13$

$(3, 0, 182) = A'$
$(17, 7, 35) = A' + 2E$
$(17, -7, 35) = A' + 4E$

V''''

5 and $7, 8; R3; R7; N13$

$(15, -3, 37) = A' + E$
$(7, 0, 78) = A' + 3E$
$(15, 3, 37) = A' + 5E$

V''''''

1 and $3, 8; R3; N7; N13$

$(6, 0, 91) = A + A'$
$(19, 9, 33) = A + A' + 2E$
$(19, -9, 33) = A + A' + 4E$

V''''''

5 and $7, 8; N3; R7; R13$

$(23, 11, 29) = A + A' + E$
$(14, 0, 39) = A + A' + 3E$
$(23, -11, 29) = A + A' + 5E$

SECTION VI.

VARIOUS APPLICATIONS OF THE PRECEDING INVESTIGATIONS.

308.

We have already indicated in several places how rich higher arithmetic is in truths useful in other parts of mathematics as well. We thought it worthwhile to treat separately some applications that deserve a fuller account. Our aim is less to exhaust this subject, which could easily fill several volumes, than to illustrate it with a few examples. In this section we will first discuss the decomposition of fractions into simpler ones, then the conversion of common fractions into decimals. Next we will explain a new method of exclusion for solving indeterminate equations of the second degree, and finally give new, convenient methods for distinguishing primes from composite numbers and finding the factors of the latter. In the following section we will establish the general theory of a particular kind of functions, which extends very widely throughout analysis, insofar as it is very closely connected with higher arithmetic. In particular, we will seek to advance the theory of the division of the circle, of which only the first elements have so far become known.

Decomposition of fractions into simpler ones.

309.

PROBLEM. *Decompose a fraction $\frac{m}{n}$, whose denominator n is the product of two coprime numbers a, b, into two other fractions with denominators a, b.*

Solution. Let the required fractions be $\frac{x}{a}, \frac{y}{b}$. Then we must have $bx + ay = m$. Thus x is a root of the congruence $bx \equiv m \pmod{a}$, which can be found by Section II, while $y = \frac{m-bx}{a}$.

As we know, the congruence $bx \equiv m$ has infinitely many roots, all congruent modulo a, but just one that is positive and less than a. However, y may also turn out negative. We hardly need to point out that y can also be found from the congruence $ay \equiv m \pmod{b}$, and x from the equation $x = \frac{m-ay}{b}$. — *For example*, given the fraction $\frac{58}{77}$, the number 4 is the value of the expression $\frac{58}{11} \pmod 7$, so $\frac{58}{77}$ decomposes into $\frac{4}{7} + \frac{2}{11}$.

310.

Suppose a fraction $\frac{m}{n}$ is given whose denominator n is the product of any number of pairwise coprime factors a, b, c, d, and so on. By the preceding article it can first be decomposed into two fractions with denominators a and bcd, and so on; the second can again be decomposed into two with denominators b and cd, and so on; the latter again into two, and so on. Finally the given fraction takes the form

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \text{etc.}$$

Clearly we may take the numerators $\alpha, \beta, \gamma, \delta$, and so on, positive and less than their respective denominators, except the last. Once the others have been determined, the

last is no longer arbitrary, and may even be negative or greater than its denominator, since we do not assume $m < n$. It will then usually be useful to put it in the form $\frac{\varepsilon}{e} \mp k$, with ε positive and less than e, and k an integer. Finally, a, b, c, and so on, can clearly be chosen as primes or powers of primes.

Example. The fraction $\frac{391}{924}$, with denominator $= 4.3.7.11$, decomposes in this way into $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ into $\frac{2}{3} - \frac{38}{77}$; and $-\frac{38}{77}$ into $\frac{1}{7} - \frac{7}{11}$. Thus, writing $\frac{4}{11} - 1$ for $-\frac{7}{11}$, we get $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311.

A fraction $\frac{m}{n}$ can be put in the form $\frac{\alpha}{a} + \frac{\beta}{b} + \text{etc.} \mp k$ in *only one way*, with α, β, and so on, positive and less than a, b, and so on. For suppose

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{etc.} \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \text{etc.} \mp k'$$

with α', β', and so on, likewise positive and less than a, b, and so on. Then necessarily $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, and so on, and $k = k'$. Multiplying by $n = abc$, and so on, clearly gives $m \equiv \alpha bcd$ etc. $\equiv \alpha' bcd$ etc. (mod. a). Since bcd, and so on, is coprime to a, necessarily $\alpha \equiv \alpha'$, and hence $\alpha = \alpha'$. Likewise $\beta = \beta'$, and so on, from which $k = k'$ also follows at once. Now we are entirely free to choose which denominator's numerator to calculate first. So *all* the numerators can clearly be found in the same way as α in the preceding article: β from the congruence βacd etc. $\equiv m$ (mod. b), γ from γabd etc. $\equiv m$ (mod. c), and so on. The sum of all the fractions found in this way either equals the given fraction $\frac{m}{n}$, or differs from it by an integer $= k$. This also gives us a check on the calculation. Thus, in the example of the preceding article, the values of the expressions $\frac{391}{231}$ (mod. 4), $\frac{391}{308}$ (mod. 3), $\frac{391}{132}$ (mod. 7), $\frac{391}{84}$ (mod. 11) immediately give the numerators $1, 2, 1, 4$ corresponding to the denominators $4, 3, 7, 11$, and the sum of these fractions is found to exceed the given fraction by one.

Conversion of common fractions into decimals.

312.

DEFINITION. When a common fraction is converted into a decimal, we call the sequence of decimal digits*) (excluding the integer part, if there is one), whether finite or continuing indefinitely, the fraction's *mantissa*. We use this expression, otherwise customary only for logarithms, in a wider sense. Thus, *for example*, the mantissa of the fraction $\frac{1}{8}$ is 125, that of $\frac{35}{16}$ is 1875, and that of $\frac{2}{37}$ is 054054..., continuing indefinitely.

It follows at once from this definition that the fractions $\frac{l}{n}, \frac{m}{n}$, which have the same denominator, have the same or different mantissas according as their numerators l, m are congruent or incongruent modulo n. A finite mantissa does not change if any number of zeros are added on the right. The mantissa of the fraction $\frac{10m}{n}$ is obtained by removing the first digit from the mantissa of $\frac{m}{n}$. More generally, the mantissa of $\frac{10^\nu m}{n}$ is found by removing the first ν digits from that of $\frac{m}{n}$. The mantissa of $\frac{1}{n}$ begins at once with a significant digit, *that is*, one different from zero, if n is not > 10. But if $n > 10$, and the denominator is unequal to any power of 10 and has k digits, the first $k-1$ digits of the mantissa of $\frac{1}{n}$ are zeros, and only the next, the k-th, is significant. It follows easily that if $\frac{l}{n}, \frac{m}{n}$ have different mantissas, *that is*, if l, m are incongruent modulo n, these mantissas certainly cannot agree in their first k digits, but must differ at or before the k-th digit.

313.

PROBLEM. *Given the denominator of a fraction $\frac{m}{n}$ and the first k digits of its mantissa, find the numerator m, which we suppose less than n.*

Solution. Regard those k digits as an integer, multiply it by n, and divide the product by $.10^k$, or remove the last k digits. If the quotient is an integer, that is, if the digits removed are zeros, it is clearly the required numerator and the given mantissa is complete. Otherwise the required numerator is the next greater integer: the quotient increased by one after the following decimal digits have been discarded. The reason for this rule is so easily seen from the observations at the end of the preceding article that a fuller explanation is unnecessary.

Example. If the first two digits of the mantissa of a fraction with denominator 23 are known to be 69, we have the product $23.69 = 1587$. Removing its last two digits and adding one gives the required numerator $= 16$.

314.

We begin with fractions whose denominators are primes or powers of primes, and will later show how the others can be reduced to these. First we observe at once that the mantissa of a fraction $\frac{a}{p^\mu}$, whose numerator a we always suppose not divisible by the prime p, is finite and has μ digits if $p = 2$ or $= 5$. In the former case this mantissa, regarded as an integer, $= 5^\mu a$, and in the latter, $= 2^\mu a$. These facts are so obvious that they need no explanation.

*)For brevity we restrict the following investigation to the usual decimal system, since it can easily be extended to any other.

If p is any other prime, however, $10^r a$ is never divisible by p^μ, however large r is taken. Thus the mantissa of $F = \frac{a}{p^\mu}$ must continue indefinitely. Suppose 10^e is the lowest power of 10 congruent to unity modulo p^μ. Compare Section III, where we showed that e either equals $(p-1)p^{\mu-1}$ or is a proper divisor of it. It is easy to see that $10^e a$ is also the first number in the series $10a, 100a$, $1000a$, and so on, congruent to a modulo the same number. Now, by Article 312, the mantissas of the fractions $\frac{10a}{p^\mu}, \frac{100a}{p^\mu} \ldots \frac{10^e a}{p^\mu}$ arise by removing from the mantissa of F the first digit, the first two $\ldots e$ digits, respectively. So the same digits clearly repeat in this mantissa after the first e digits, and not sooner. We may call these first e digits, whose infinite repetition forms the mantissa, the *period* of this mantissa or of the fraction F. Clearly the length of the period, *that is*, the number of digits it contains $(= e)$, is entirely independent of the numerator a, and is determined by the denominator alone. Thus, *for example*, the period of $\frac{1}{11}$ is 09, and that of $\frac{3}{7}$ is 428571[*)].

315.

Once the period of a fraction is known, its mantissa can therefore be extended to any number of digits. Further, if $b \equiv 10^\lambda a \pmod{p^\mu}$, the period of $\frac{b}{p^\mu}$ clearly results from placing the first λ digits of the period of F, assuming $\lambda < e$, as we may, after the remaining $e - \lambda$ digits. Thus, with the period of F we also have the periods of all fractions whose numerators are congruent to $10a, 100a, 1000a$, and so on, modulo the denominator p^μ. Thus, *for example*, since $6 \equiv 3.10^2 \pmod{7}$, the period of $\frac{6}{7}$ is obtained at once from that of $\frac{3}{7}$ as 857142.

Whenever p^μ is the modulus and 10 is a primitive root, by Articles 57, 89, the period of $\frac{1}{p^\mu}$ immediately gives the period of any other fraction $\frac{m}{p^\mu}$ whose numerator m is not divisible by p. We remove as many digits from its left and restore them on its right as there are units in the index of m, with 10 taken as base. This makes clear why, in this case, 10 has always been taken as base in Table I; see Article 72.

[*)] The distinguished Robertson marks the beginning and end of the period by placing two dots above its first and last digits (*Theory of circulating fractions, Philos. Trans.* 1769 *p.* 207), which we do not think necessary here.

But when 10 is not a primitive root, the period of $\frac{1}{p^\mu}$ gives only the periods of fractions whose numerators are congruent to some power of 10 modulo p^μ. Let 10^e be the lowest power of 10 congruent to unity modulo p^μ, let $(p-1)p^{\mu-1} = ef$, and take as base a primitive root r for which the index of 10 is f, by Article 71. In this system the numerators of the fractions whose periods can be obtained from that of $\frac{1}{p^\mu}$ have indices $f, 2f, 3f \ldots ef - f$. Similarly, the period of $\frac{r}{p^\mu}$ gives the periods of fractions whose numerators $10r, 100r, 1000r$, and so on, correspond to the indices $f+1, 2f+1, 3f+1$, and so on. The period of the fraction with numerator rr, whose index is 2, gives the periods of fractions whose numerators have indices $f+2, 2f+2, 3f+2$, and so on. More generally, the period of the fraction with numerator r^i gives the periods of fractions whose numerators have indices $f+i, 2f+i, 3f+i$, and so on. It follows easily that, once we have the periods of the fractions with numerators $1, r, rr, r^3 \ldots r^{f-1}$, all the others can be deduced by transposition alone, using the following rule. Let the index of the numerator m of the given fraction $\frac{m}{p^\mu}$, in the system with base r, $= i$, which we suppose less than $(p-1)p^{\mu-1}$. By division by f, put $i = \alpha f + \beta$, with α, β positive integers, or also 0, and $\beta < f$. Then the period of $\frac{m}{p^\mu}$ is obtained from the period of the fraction with numerator r^β, and so 1 when $\beta = 0$, by placing its first α digits after the others. Thus we retain that very period when $\alpha = 0$. This sufficiently explains why, in constructing Table I, we followed the rule explained in Article 72.

316.

Following these principles, we have constructed a table of the necessary periods for all denominators of the form p^μ below 1000. We will publish it in full, or even extended further, when an occasion arises. Here Table III, carried only as far as 100, may suffice as a sample; it hardly needs explanation. For denominators for which 10 is a primitive root, it gives the periods of fractions with numerator 1, namely for $7, 17, 19, 23, 29, 47, 59, 61, 97$. For the others it gives f periods corresponding to the numerators $1, r, rr, \ldots r^{f-1}$, distinguished by the attached numbers $(0), (1), (2)$, and so on. The same primitive root has always been chosen as base r as in Table I. Thus the rules of the preceding article give the period of any fraction whose denominator is in this table, after the numerator's index has been calculated from Table I. For denominators so small, however, we can complete the task just as easily without Table I. By ordinary division we calculate as many initial digits of the required mantissa as Article 313 requires to distinguish it from all others with the same denominator, no more than 2 for Table III. We then examine all the periods corresponding to the given denominator until we reach those initial digits, which will undoubtedly mark the beginning of the period. But we must point out that these digits may also be separated: the first, or several of them, may form the end of a period, and the remaining digit or digits its beginning.

Example. We seek the period of $\frac{12}{19}$. Here, for the modulus 19, Table I gives $\text{ind. } 12 = 2\,\text{ind. } 2 + \text{ind. } 3 = 39 \equiv 3 \pmod{18}$, by Article 57. In this case there is just one period, corresponding to the numerator 1, so we must move its first three digits to the end. This gives the required period 631578947368421052. — The beginning of the period could have been found just as easily from its first two digits 63.

If we want the period of $\frac{45}{53}$, then, for the modulus 53, $\text{ind. } 45 = 2\,\text{ind. } 3 + \text{ind. } 5 = 49$. Here the number of periods is $4 = f$, and $49 = 12f + 1$, so, from the period marked (1), the first 12 digits must be placed after the last digit. The required period is therefore 8490566037735. In this case the initial digits 84 are separated in the table.

We further observe that Table III can also give the number corresponding to a given index for a given modulus, listed there under the heading of denominator, as we promised in Article 59. By the preceding results, we can clearly find the period of the fraction whose numerator, though unknown, corresponds to the given index. It is enough to take as many initial digits of this period as the denominator has digits. From them, Article 313 gives the numerator, or the required number corresponding to the given index.

317.

The preceding results give, without calculation, as many digits as we want of the mantissa of any fraction whose denominator is a prime or a power of a prime within the table's limits. But the investigations at the beginning of this section extend the table's range much further, to all fractions whose denominators are products of primes or powers of primes within those limits. For such a fraction can be decomposed into others whose denominators are these factors, and these can be converted into decimals to any number of digits; it remains only to add them. We hardly need to point out that the last digit of the resulting sum may be less than the correct

one. But the shortfall clearly cannot reach as many units as there are individual fractions being added. It is therefore useful to calculate these to a few more digits than we want the given fraction to be correct to. As an example, consider the fraction $\frac{6099380351}{1271808720} = F$*), whose denominator is the product of the numbers $16, 9, 5, 49, 13, 47, 59$. By the rules above we find $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$. These individual fractions are converted into decimals as follows:

$$\begin{array}{rcllr}
1 & = & 1 & & \\
\frac{11}{16} & = & 0,6875 & & \\
\frac{4}{5} & = & 0,8 & & \\
\frac{4}{9} & = & 0,4444444444 & 4444444444 & 44 \\
\frac{22}{49} & = & 0,4489795918 & 3673469387 & 75 \\
\frac{5}{13} & = & 0,3846153846 & 1538461538 & 46 \\
\frac{7}{47} & = & 0,1489361702 & 1276595744 & 68 \\
\frac{52}{59} & = & 0,8813559322 & 0338983050 & 84 \\
\hline
F & = & 4,7958315233 & 1271954166 & 17
\end{array}$$

The shortfall of this sum from the correct value is certainly less than five units in the last, twenty-second, digit, so the first twenty-one digits cannot be changed by it. Extending the calculation to more digits replaces the last two digits 17 by 1893936 ... . — Anyone will see, even without our pointing it out, that this method of converting common fractions into decimals is particularly suited to the case where many decimal digits are wanted. When a few suffice, ordinary division or logarithms can usually be used just as conveniently.

*) This fraction is one of those that approximate the square root of 23 as closely as possible; its excess is less than seven units in the twentieth decimal place.

318.

We have thus reduced the conversion of fractions whose denominators are composed of several distinct primes to the case where the denominator is a prime or a power of a prime. So we will add only a few observations about their mantissas. If the denominator contains neither the factor 2 nor 5, the mantissa here too consists of periods. For in this case as well the series $10, 100, 1000$ eventually reaches a term congruent to unity modulo the denominator. The exponent of this term, which can easily be determined by Article 92, also gives the length of the period, independently of the numerator, provided the latter is coprime to the denominator. — But if the denominator has the form $2^\alpha 5^\beta N$, where N is coprime to 10, and α and β are numbers at least one of which is not 0, the mantissa begins to consist of periods after the first α or β digits, according as α or β is greater. These periods agree in length with those of fractions with denominator N. This follows very easily from the decomposition of that fraction into two others with denominators $2^\alpha 5^\beta$ and N, the former of which terminates after the first α or β digits. — We could add many other observations on this subject, especially on devices for constructing a table like III as quickly as possible. For brevity we leave them out here all the more readily because much on this subject has already been given both by the distinguished Robertson in the work cited and by the distinguished Bernoulli (*Nouv. Mém. de l'Ac. de Berlin* 1771 *p.* 273).

Solving the congruence $xx \equiv A$ by the method of exclusion.

319.

We treated the *solvability* of the congruence $xx \equiv A \pmod{m}$, which is equivalent to the indeterminate equation $xx = A + my$, in Section IV (Article 146) in such a way that nothing further seems to be desired. As for finding the unknown itself, however, we have already observed above (Article 152) that indirect methods are far preferable to direct ones. If m is a prime number (to which case the others are easily reduced), we could use the table of indices I for this purpose, combined with III according to the observation in Article 316, as we showed more generally in Article 60; but this method would be restricted to the limits of the table. For these reasons, we hope that lovers of arithmetic will welcome the following general and convenient method.

First of all, we observe that it is enough to find only those values of x that are positive and no greater than $\frac{1}{2}m$, since every other value is congruent modulo m to one of these or its negative. For such a value of x, the value of y must lie between the bounds $-\frac{A}{m}$ and $\frac{1}{4}m - \frac{A}{m}$. The method that immediately suggests itself would therefore consist in taking each value of y within these bounds (denoting their collection by Ω), calculating the value of $A + my$, which we shall denote by V, and retaining only those for which V is a square. When m is a small number (*e.g.* below 40), this trial is so brief that there is hardly any need to shorten it; but when m is large, the work can be shortened as much as we please by the following *method of exclusion.*

320.

Let E be any integer coprime to m and greater than 2, and let all its distinct quadratic nonresidues (*i.e.* incongruent modulo E) be a, b, c, etc.; finally, let the roots of the congruences

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c \quad \text{etc. modulo } E$$

be α, β, γ, etc., which may all be taken positive and less than E. If, then, y is assigned a value congruent to one of these numbers α, β, γ, etc., modulo E, the resulting value of $V = A + my$ will be congruent to one of a, b, c, etc., and hence a nonresidue of E; it therefore cannot be a square. Thus, from Ω, all the numbers of the forms $Et + \alpha$, $Et + \beta, Et + \gamma$, etc., can at once be excluded as useless, and it will be enough to try the remaining numbers, whose collection we shall call Ω'. In this operation, the number E may be called an *exclusion number.*

Now, taking another suitable number E' as an exclusion number, we shall find in exactly the same way as many numbers α', β', γ', etc., as it has distinct quadratic nonresidues, to which y cannot be congruent modulo E'. We may therefore again remove from Ω' all the numbers of the forms $E't + \alpha', E't + \beta', E't + \gamma'$, etc. We can continue in this way, using further exclusion numbers, until the collection of numbers in Ω has been reduced so much that actually trying all those left seems no more difficult than making further exclusions.

Example. Given the equation $xx = 22 + 97y$, the bounds for the values of y will be $-\frac{22}{97}$ and $24\frac{1}{4} - \frac{22}{97}$, so that, since the value 0 is obviously useless, Ω will contain the

numbers $1, 2, 3 \ldots 24$. For $E = 3$ there is just one nonresidue, $a = 2$, giving $\alpha = 1$; hence we must exclude from Ω all numbers of the form $3t + 1$, and the number of those remaining, Ω', will be 16. Similarly, for $E = 4$ we have $a = 2, b = 3$, giving $\alpha = 0, \beta = 1$; hence the numbers of the forms $4t$ and $4t + 1$ must be rejected, leaving these eight: $2, 3, 6, 11, 14, 15, 18, 23$. Likewise, for $E = 5$, we find that the numbers of the forms $5t$ and $5t + 3$ must be rejected, leaving $2, 6, 11, 14$. The exclusion number 6 would remove numbers of the forms $6t + 1$ and $6t + 4$, but these, which coincide with the numbers of the form $3t + 1$, are already absent. The exclusion number 7 removes the numbers of the forms $7t + 2, 7t + 3, 7t + 5$, leaving $6, 11, 14$. Substituting these for y gives, respectively, $V = 604, 1089, 1380$, of which only the second value is a square; hence $x = \mp 33$.

321.

The operation with the exclusion number E removes, from the values of V corresponding to the values of y in Ω, all those that are quadratic nonresidues of E, while leaving the residues of the same number untouched. It is therefore easy to see that using the exclusion numbers E and $2E$ makes no difference if E is odd, since in this case E and $2E$ have the same residues and nonresidues. Hence, if the numbers $3, 4$, 5, etc., are used successively as exclusion numbers, the numbers $6, 10, 14$, etc., which are twice odd numbers, must be skipped as superfluous. It is also clear that the two operations with the exclusion numbers E, E' remove all those values of V that are nonresidues of both E, E' or of one of them, leaving those that are residues of both. Now, when E and E' have no common divisor, all the numbers removed are nonresidues of the product EE', and all those left are its residues. It is therefore evident that using the exclusion number EE' has exactly the same effect in this case as using both E, E', and is thus superfluous after these have been used. We may therefore also skip all exclusion numbers that can be resolved into two coprime factors, and it will be enough to use prime numbers that do not divide m, or powers of primes. Finally, it is clear that, after the exclusion number p^μ, a power of the prime p, has been used, the exclusion number p or p^ν, where $\nu < \mu$, becomes superfluous. For, since p^μ has left only its own residues among the values of V, certainly no nonresidues of p or of any lower power p^ν can remain. If, however, p or p^ν has already been used before p^μ, the latter can evidently remove only those values of V that are at once residues of p (or p^ν) and nonresidues of p^μ; hence it will be enough to take only nonresidues of p^μ of this kind for a, b, c, etc.

322.

The calculation of the numbers α, β, γ, etc., corresponding to any given exclusion number E is greatly shortened by the following observations. Let $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., be roots of the congruences $my \equiv a, my \equiv b, my \equiv c$, etc., (mod. E), and k a root of $my \equiv -A$; it will then be clear that $\alpha \equiv \mathfrak{A} + k, \beta \equiv \mathfrak{B} + k, \gamma \equiv \mathfrak{C} + k$, etc. Now, if we really had to obtain $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., by solving these congruences, this way of finding α, β, γ, etc., would certainly be no shorter than the one shown above; but this is by no means necessary. For, first, if E is a prime number and m a quadratic residue of E, it follows from Article 98 that $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., which are the values of the expressions $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}$, etc., (mod. E), are distinct nonresidues of E, and therefore coincide exactly

with α, β, γ, etc., apart from their order, which does not matter here. If, under the same assumption, m is a nonresidue of E, the numbers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., will coincide with all the quadratic residues except 0. If E is the square of an odd prime number, $= pp$, and p has already been used as an exclusion number, it is enough, by the preceding article, to take for a, b, c, etc., those nonresidues of pp that are residues of p, *i.e.* the numbers $p, 2p, 3p \ldots pp - p$ (namely, all numbers below pp except 0 that are divisible by p). It is then easy to see that $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., must give exactly the same numbers, only in a different order. Similarly, if, after the exclusion numbers p and pp have been used, we put $E = p^3$, it will be enough to take for a, b, c, etc., the products of the individual nonresidues of p by pp; then $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., will give either the same numbers or the products of pp by the individual residues of p except 0, according as m is a residue or a nonresidue of p. In general, taking for E any power of a prime number, say p^μ, after all lower powers have been used, we shall obtain for $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., the products of $p^{\mu-1}$ either by all numbers less than p, always excepting 0, when μ is even; or by all nonresidues of p less than p, when μ is odd and mRp; or by all residues, when mNp. — If $E = 4$, and hence $a = 2, b = 3$, we have for $\mathfrak{A}, \mathfrak{B}$ either 2 and 3 or 2 and 1, according as $m \equiv 1$ or $\equiv 3 \pmod 4$. If, after using the exclusion number 4, we put $E = 8$, we have $\alpha = 5$, giving $\mathfrak{A}$ the values $5, 7, 1, 3$, according as $m \equiv 1, 3, 5, 7 \pmod 8$. In general, however, if E is any higher power of two, say 2^μ, after the lower powers have been used, we must put $a = 2^{\mu-1}, b = 3.2^{\mu-2}$ when μ is even, giving $\mathfrak{A} = 2^{\mu-1}, \mathfrak{B} = 3.2^{\mu-2}$ or $= 2^{\mu-2}$, according as $m \equiv 1$ or $\equiv 3$; but when μ is odd, we must put $a = 5.2^{\mu-3}$, giving $\mathfrak{A}$ equal to the product of $2^{\mu-3}$ by $5, 7, 1$ or 3, according as $m \equiv 1, 3, 5$ or $7 \pmod 8$.

Those familiar with the subject will, moreover, readily devise an apparatus by which the useless values of y can be removed *mechanically* from Ω, once the numbers α, β, γ, etc., have been calculated for as many exclusion numbers as seem necessary; but we cannot discuss this here, any more than other devices for shortening the work.

Solving the indeterminate equation $mxx + nyy = A$ by exclusions.

323.

In Section V we showed how to find all representations of a given number A by the binary form $mxx+nyy$, or the solutions of the indeterminate equation $mxx+nyy = A$, by a general method whose brevity, too, seems to leave nothing to be desired if all the values of the expression $\sqrt{-mn}$ are already known modulo A itself and modulo that number divided by its square factors. Here, however, for the case where mn is positive, we shall explain a solution much more convenient than the direct one if those values must first be calculated for the latter. We shall assume that the numbers m, n and A are positive and pairwise coprime, since the other cases can easily be reduced to this one. It is also evident that it is enough to find positive values of x, y, since the others follow simply by changing the signs.

It is clear that x must be such that $\frac{A-mxx}{n}$, for which we shall write V, is positive, integral and a square. The first condition requires that x be no greater than $\sqrt{\frac{A}{m}}$; the second holds of itself when $n = 1$, and otherwise requires that the value of the expression $\frac{A}{m}$ (mod. n) be a quadratic residue of n. Denoting all the distinct values of the expression $\sqrt{\frac{A}{m}}$ (mod. n) by $\pm r, \pm r'$, etc., we must have x of one of the forms $nt + r, nt - r, nt + r'$, etc. The simplest procedure would therefore be to take all numbers of these forms below the bound $\sqrt{\frac{A}{m}}$ (denoting their collection by Ω), substitute them for x, and retain only those for which V becomes a square. In the next article we shall show how to shorten this trial as much as we please.

324.

The method of exclusion by which we shall do this consists, as in the preceding investigation, in taking several numbers at will, which here too we shall call *exclusion numbers*, finding the values of x for which the value of V is a quadratic nonresidue of these exclusion numbers, and removing such values of x from Ω. Reasoning entirely analogous to that given in Article 321 shows that we need use only exclusion numbers that are primes or powers of primes. For an exclusion number of the latter kind, we need remove from the values of V only those of its nonresidues that are residues of all lower powers of the same prime, provided the exclusions with these have already been made.

Let the exclusion number therefore be $E = p^\mu$, including the case $\mu = 1$, where p is a prime that does not divide m, and suppose[*)] that p^ν is the highest power of the same prime by which n is divisible. Let a, b, c, etc., be quadratic nonresidues of E: all of them when $\mu = 1$, and the necessary ones, namely those that are residues of the lower powers, when $\mu > 1$. Calculate the roots of the congruences $mz \equiv A - na$, $mz \equiv A - nb, mz \equiv A - nc$, etc., (mod. $Ep^\nu = p^{\mu+\nu}$), and let them be α, β, γ, etc. It is easy to see that, if a value of x gives $xx \equiv \alpha$ (mod. Ep^ν), the corresponding value of V will be $\equiv a$ (mod. E), and thus a nonresidue of E; and similarly for the other numbers β, γ, etc. Conversely, it is equally easy to see that, if a value of x produces $V \equiv a$ (mod. E), then for the same value we have $xx \equiv \alpha$ (mod. Ep^ν). Thus all

[*)] For brevity, we include together the two cases in which n is and is not divisible by p; in the latter we must put $\nu = 0$.

values of x for which xx is congruent to none of the numbers α, β, γ, etc., modulo Ep^ν produce values of V congruent to none of the numbers a, b, c, etc., modulo E. Now select from the numbers α, β, γ, etc., all the quadratic residues of Ep^ν, and call them g, g', g'', etc. Calculate the values of the expressions $\sqrt{g}, \sqrt{g'}.\sqrt{g''}$, etc., (mod. Ep^ν), and suppose that these give $\pm h, \pm h', \pm h''$, etc. Once this has been done, it is clear that all numbers of the forms $Ep^\nu t \pm h, Ep^\nu t \pm h', Ep^\nu t \pm h''$, etc., can safely be removed from Ω, and that no value of x remaining in Ω after this exclusion can correspond to a value of V of the forms $Eu + a, Eu + b, Eu + c$, etc. Moreover, it is evident that such values of V cannot arise from any value of x at all if none of the numbers α, β, γ, etc., are quadratic residues of Ep^ν; hence in this case the number E cannot be used as an exclusion number. — We may use as many exclusion numbers of this kind as we please, and thus reduce the collection of numbers in Ω as much as we please.

Let us now see whether primes dividing m, or powers of such primes, can also be used as exclusion numbers. Let B be the value of the expression $\frac{A}{n}$ (mod. m). It is clear that V is always congruent to B modulo m, whatever value is taken for x, and thus that a necessary condition for the proposed equation to be solvable is that B be a quadratic residue of m. Now let p denote any odd prime divisor of m, which by hypothesis divides neither n nor A, and hence does not divide B either. For any value of x, V will be a residue of p, and therefore of any power of p as well; hence p and its powers cannot serve as exclusion numbers. By exactly similar reasoning, when m is divisible by 8, a necessary condition for the proposed equation to be solvable is $B \equiv 1$ (mod. 8). Then V, for any value of x, will also be $\equiv 1$ (mod. 8), and powers of two are therefore unsuitable for exclusion. — But when m is divisible by 4 but not by 8, similar reasoning requires $B \equiv 1$ (mod. 4), and hence the value of the expression $\frac{A}{n}$ (mod. 8) is either 1 or 5; denote it by C. It is easy to see that, for an even value of x, we have $V \equiv C$, and for an odd value, $V \equiv C + 4$ (mod. 8). Thus even values must be rejected when $C = 5$, and odd values when $C = 1$. — Finally, when m is divisible by 2 but not by 4, let C, as before, be the value of the expression $\frac{A}{n}$ (mod. 8), which will be $1, 3, 5$ or 7; and let D be the value of $\frac{\frac{1}{2}m}{n}$ (mod. 4), which will be 1 or 3. Now the value of V is evidently always $\equiv C - 2Dxx$ (mod. 8), and hence, for even x, $\equiv C$, and for odd, $\equiv C - 2D$. It follows easily that all odd values of x must be rejected when $C = 1$; all even values when $C = 3$ and $D = 1$, or $C = 7$ and $D = 3$; and that all remaining values produce $V \equiv 1$ (mod. 8), a residue of any power of two. In the other cases, namely when $C = 5$, or $C = 3$ and $D = 3$, or $C = 7$ and $D = 1$, we have $V \equiv 3, 5$ or 7 (mod. 8), whether x is taken even or odd. Thus in these cases the proposed equation has no solution at all.

Moreover, just as we have shown here how to find the value of x by exclusions, we can, with the necessary changes, obtain the value of y. The method of exclusion can therefore always be applied to the proposed problem in two ways, unless $m = n = 1$, when they coincide. Of these, the one for which Ω contains fewer terms is generally preferable, and this can easily be estimated beforehand. — Finally, we hardly need to observe that, if after some exclusions *all* numbers have disappeared from Ω, this must be regarded as a certain indication that the proposed equation is impossible.

325.

Example. Let the equation $3xx + 455yy = 10857362$ be given. We shall solve it in two ways, *first* by finding the values of x, and then those of y. The bound for the former in this case is $\sqrt{3619120\frac{2}{3}}$, which lies between 1902 and 1903; the value of the expression $\frac{A}{3}$ (mod. 455) is 354, and the values of the expression $\sqrt{354}$ (mod. 455) are $\pm 82, \pm 152, \pm 173, \pm 212$. Hence Ω consists of the following 33 numbers: $82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902$. The number 3 cannot be used for exclusion in this case, because it divides m. For the exclusion number 4 we have $a = 2, b = 3$, giving $\alpha = 0, \beta = 3$; $g = 0$, and the values of the expression $\sqrt{g}$ (mod. 4) are 0 and 2. Thus all numbers of the forms $4t$ and $4t + 2$, *i.e.* all even numbers, must be removed from Ω; denote the sixteen remaining numbers by Ω'. For $E = 5$, which also divides n, the congruences $mz \equiv A - 2n$ and $mz \equiv A - 3n$ (mod. 25) have roots 9 and 24, both residues of 25, and the values of the expressions $\sqrt{9}$ and $\sqrt{24}$ (mod. 25) are ± 3, ± 7. Removing from Ω' all numbers of the forms $25t \pm 3$, $25t \pm 7$ leaves these ten (Ω''): $173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577$. For $E = 7$, the congruences $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) have roots $32, 39, 18$, all residues of 49, and the values of the expressions $\sqrt{32}, \sqrt{39}, \sqrt{18}$ (mod. 49) are $\pm 9, \pm 23, \pm 19$. Removing from Ω'' the numbers of the forms $49t \pm 9$, $49t \pm 19$, $49t \pm 23$ leaves these five (Ω'''): $537, 737, 1083, 1213, 1517$. For $E = 8$ we have $a = 5$, giving $\alpha = 5$, a nonresidue of 8; hence the exclusion number 8 cannot be used. The number 9 must be skipped for the same reason as 3. For $E = 11$, the numbers a, b, etc., are $2, 6, 7, 8, 10$; $\nu = 0$; hence α, β, etc., $= 8, 10, 5, 0, 1$, of which three are residues of 11, namely $0, 1, 5$. It follows that we must remove from Ω''' the numbers of the forms $11t$, $11t \pm 1$, $11t \pm 4$, leaving $537, 1083, 1213$. Trying these gives for V the respective values $21961, 16129, 14161$, of which only the second and third are squares. Thus the proposed equation admits two solutions with positive values of x, y, namely $x = 1083, y = 127$ and $x = 1213$, $y = 119$.

Second. If we wish to find the other unknown of the same equation by exclusions, put the equation in the form $455xx + 3yy = 10857362$, interchanging x and y so that all the notation of Articles 323, 324 may be retained. Here the bound for the values of x lies between 154 and 155; the value of the expression $\frac{A}{m}$ (mod. n) is 1, and the values of $\sqrt{1}$ (mod. 3) are $+1$ and -1. Hence Ω contains all numbers of the forms $3t + 1$ and $3t - 1$, *i.e.* all numbers not divisible by 3 up to and including 154, whose number is 103. Applying the rules given above, however, we find that for the exclusion numbers 3; 4; 9; 11; 17; 19; 23 we must reject the numbers of the forms $9t \pm 4$; $4t$, $4t \pm 2$, or all even numbers; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. Removing these leaves $119, 127$, the only two that give V a square value, yielding the same solutions as those obtained above.

326.

The preceding method is already so convenient in itself that it leaves hardly anything to be desired. Nevertheless, various devices can shorten it considerably, and we can touch on only a few of them here. We shall therefore restrict the investigation to the case where the exclusion number is an odd prime not dividing A, or a power of such a prime, especially since the other cases can either be reduced to this one or treated by an analogous method. Suppose, *first*, that the exclusion number $E = p$ is a prime dividing neither of the numbers m, n, and that the values of the expressions $\frac{A}{m}, -\frac{na}{m}, -\frac{nb}{m}, -\frac{nc}{m}$, etc., (mod. p) are respectively $k, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc. The numbers α, β, γ, etc., are then found from the congruences $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$, etc., (mod. p). But the numbers $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., can be obtained without calculating the congruences, by a device entirely similar to that used in Article 322. They will coincide either with all nonresidues or with all residues of p, except 0, according as the value of the expression $-\frac{m}{n}$ (mod. p), or, equivalently here, the number $-mn$, is a residue or a nonresidue of p. Thus, in *example* II of the preceding article, for $E = 17$ we have $k = 7$; $-mn = -1365 \equiv 12$ is a nonresidue of 17. Hence the numbers $\mathfrak{A}, \mathfrak{B}$, etc., will be $1, 2, 4, 8, 9, 13, 15, 16$, and the numbers α, β, etc., $8, 9, 11, 15, 16, 3, 5, 6$. Of these, the residues are $8, 9, 15, 16$, giving $\pm h, h'$, etc., the values $\pm 5, 3, 7, 4$. — Those who often have occasion to solve such problems will make their work much easier if, for several primes p, they calculate the values of h, h', etc., corresponding to the individual values of k $(1, 2, 3 \ldots p-1)$, under each of the two assumptions that $-mn$ is a residue or a nonresidue of p. We also observe that the number of values h, $-h, h'$, etc., is always $\frac{1}{2}(p-1)$ when both k and $-mn$ are residues or both are nonresidues of p; $\frac{1}{2}(p-3)$ when the former is $R.$ and the latter $NR.$; and $\frac{1}{2}(p+1)$ when the former is $NR.$ and the latter $R.$. But we must omit the proof of this theorem to avoid becoming too lengthy.

Second, the cases where E is a prime dividing n, or a power of an odd prime that does or does not divide n, can be treated still more conveniently. We shall include all these cases together and, retaining all the notation of Article 324, put $n = n'p^\nu$, so that n' is not divisible by p. The numbers a, b, c, etc., will be the products of $p^{\mu-1}$ either by all numbers less than p, except 0, or by all nonresidues of p below p, according as μ is even or odd; denote them generally by $up^{\mu-1}$. Let k be the value of the expression $\frac{A}{m}$ (mod. $p^{\mu+\nu}$). It will not be divisible by p, since the same property is assumed of A; further, it is clear that all of α, β, γ, etc., are congruent to k modulo p, and hence that p^μ excludes nothing from Ω if kNp. If, however, kRp, and hence also $kRp^{\mu+\nu}$, let r be a value of the expression $\sqrt{k}$ (mod. $p^{\mu+\nu}$), which will not be divisible by p, and e the value of $-\frac{n'}{2mr}$ (mod. p). Then $\alpha \equiv rr + 2erap^\nu$ (mod. $p^{\mu+\nu}$), from which it follows easily that α is a residue of $p^{\mu+\nu}$, and that the values of the expression $\sqrt{\alpha}$ (mod. $p^{\mu+\nu}$) are $\pm(r + eap^\nu)$; hence all of h, h', h'', etc., are expressed by $r + uep^{\mu+\nu-1}$. Finally, it follows without difficulty that the numbers h, h', h'', etc., arise by adding r to the products of $p^{\mu+\nu-1}$ either by all numbers below p, except 0, when μ is even; or by all nonresidues of p below this bound, when μ is odd and eRp, or, equivalently here, when $-2mrn'Rp$; or by all residues, except 0, when μ is odd and $-2mrn'Np$.

Moreover, once the numbers h, h', etc., have been found for each exclusion number we wish to use, the exclusion itself can also be performed by mechanical operations, which anyone familiar with these matters can readily devise for themselves if it seems worth the effort.

Finally, we must observe that any equation $axx+2bxy+cyy = M$ in which $bb-ac$ is negative, $= -D$, can easily be reduced to the form considered above. For, denoting the greatest common divisor of a, b by m, and putting

$$a = ma'. \quad b = mb', \quad \frac{D}{m} = a'c - mb'b' = n, \quad a'x + b'y = x'$$

the equation is evidently equivalent to $mx'x' + nyy = a'M$, which can be solved by the rules given above. Of its solutions, however, we must retain only those in which $x' - b'y$ is divisible by a', or from which x acquires integer values.

Another method for solving the congruence $xx \equiv A$ when A is negative.

327.

Just as the direct solution of the equation $axx + 2bxy + cyy = M$ given in Section V assumes the values of the expression $\sqrt{(bb - ac)}$ (mod. M) to be known, so, conversely, when $bb - ac$ is negative, the indirect solution explained above supplies a very convenient method for finding these values. Especially for a very large value of M, it is far preferable to the method of Article 322 and the following articles. We shall assume, however, that M is a prime number, or at least that its factors, if it is composite, are still unknown. For, if we knew that a prime p divides M, and that $M = p^\mu M'$, with M' no longer containing the factor p, it would be much more convenient to find the values of the expression $\sqrt{(bb - ac)}$ separately for the moduli p^μ and M', the former from the values modulo p, Article 101, and to deduce the values modulo M by combining these, Article 105.

We are therefore to find all the values of the expression $\sqrt{-D}$ (mod. M), assuming D and M positive, and M of a form of divisors of $xx+D$, Article 147 and the following articles; otherwise it would already be certain that no numbers could satisfy the proposed expression. Let the required values, which always occur in opposite pairs, be $\pm r, \pm r', \pm r''$, etc., and let $D + rr = Mh$, $D + r'r' = Mh'$, $D + r''r'' = Mh''$, etc. Further, denote the classes to which the forms (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''). $(M, -r'', h'')$, etc., belong respectively by $\mathfrak{C}, -\mathfrak{C}, \mathfrak{C}', -\mathfrak{C}', \mathfrak{C}'', -\mathfrak{C}''$, etc., and their collection by $\mathfrak{G}$. Generally speaking, these classes must be regarded as unknown. Nevertheless, it is clear, *first*, that all are positive and properly primitive; *second*, that all belong to the same genus, whose *character* can easily be determined from the nature of the number M, *i.e.* from its relations to the individual prime divisors of D, and also to 4 or 8 when these are necessary, Article 230. Since M is assumed to be of a form of divisors of $xx + D$, we can be certain beforehand that this character must correspond to a genus of positive, properly primitive forms of determinant $-D$, even if the expression $\sqrt{-D}$ (mod. M) should perhaps have no solutions. Thus, since this genus is known, all the classes it contains can be found; let them be C, C', C'', etc., and their collection G.

It is therefore clear that each class $\mathfrak{C}, -\mathfrak{C}$, etc., must be identical with some class in G. Several classes in $\mathfrak{G}$ may also be identical with one another, and hence with the same class in G; and when G contains just one class, all those in $\mathfrak{G}$ certainly coincide with it. Thus, if, from the classes C, C', C'', etc., we select the simplest forms f, f', f'', etc., one from each, a form from each class in $\mathfrak{G}$ will be found among them. Now, if $axx + 2bxy + cyy$ is a form contained in the class $\mathfrak{C}$, there will be two representations of M by it belonging to the value r; if one is $x = m, y = n$, the other is $x = -m, y = -n$. The sole exception is the case $D = 1$, in which there are four representations; see Article 180.

It follows that, if all representations of M by each of the forms f, f', f'', etc., are found by the indirect method given above, and the values of the expression $\sqrt{-D}$ (mod. M) to which the individual representations belong are then deduced, Article 154 and the following articles, *all* values of this expression will be obtained, each twice, or, if $D = 1$, four times. *Q. E. F.* If there are forms among f, f', etc., by which M cannot be represented, this indicates that they belong to no class in $\mathfrak{G}$, and they must therefore be disregarded. If, however, M cannot be represented by any of these forms, $-D$ must be a quadratic nonresidue of M. — The following observations should also be kept in mind in these operations.

I. The representations of M by the forms f, f', etc., used here are understood to be those in which the values of the indeterminates are coprime. If others occur in which these values have a common divisor μ, which can happen only when $\mu\mu$ divides M and will certainly happen when $-D \,\mathrm{R}\, \frac{M}{\mu\mu}$, they must be entirely disregarded for the present purpose, though they may be useful in another respect.

II. Other things being equal, the work is evidently easier the smaller the number of classes f, f', f'', etc., and therefore shortest when D is one of the 65 numbers given in Article 303, for which each genus contains only one class.

III. Since two such representations $x = m, y = n$ and $x = -m, y = -n$ always belong to the same value, it is clear that it is enough to consider only representations in which y is positive. Distinct representations *of this kind* therefore always correspond to distinct values of the expression $\sqrt{-D}$ (mod. M), so that the number of all distinct values equals the number of all resulting representations of this kind, always excepting $D = 1$, when the former number is half the latter.

IV. Since knowing either of the two opposite values $+r, -r$ immediately gives the other, the operations can be shortened somewhat further. If the value r is obtained from a representation of M by a form contained in the class C, *i.e.* if $\mathfrak{C} = C$, the opposite value $-r$ will evidently arise from a representation by a form in the class opposite to C, which differs from the class C unless the latter is ambiguous. Hence, when not all classes in G are ambiguous, only half the remaining classes need be considered: one from each opposite pair. The other can be disregarded, since, without calculation, we can already foresee that its values will be opposite to those supplied by the first. When C is ambiguous, however, both values r and $-r$ arise from it together. Namely, if the ambiguous form selected from C is $axx + 2bxy + cyy$, and the value r came from the representation $x = m, y = n$, the value $-r$ will come from $x = -m - \frac{2bn}{a}$, $y = n$.

V. In the case $D = 1$, there is just one class altogether, from which we may suppose that the form $xx+yy$ has been selected. If the value r comes from the representation $x = m, y = n$, the same value comes from $x = -m, y = -n$; $x = n, y = -m$; $x = -n$, $y = m$, and the opposite value $-r$ from $x = m, y = -n; x = -m, y = n$; $x = n$, $y = m$; $x = -n, y = -m$. Thus one of these eight representations, which constitute a single decomposition, is enough, provided we associate the opposite value with the one obtained.

VI. By Article 155, the value of the expression $\sqrt{-D}$ (mod. M) to which the representation $M = amm + 2bmn + cnn$ belongs is $\mu(mb+nc) - \nu(ma+nb)$, or any number congruent to it modulo M, with μ, ν chosen so that $\mu m + \nu n = 1$. Denoting such a value by v, we have

$$\begin{aligned} mv &\equiv \mu m(mb+nc) - \nu(M - mnb - nnc) \\ &\equiv (\mu m + \nu n)(mb+nc) \equiv mb+nc \text{ (mod. } M) \end{aligned}$$

Thus v is a value of the expression $\frac{mb+nc}{m}$ (mod. M); similarly, we find that v is a value of the expression $-\frac{ma+nb}{n}$ (mod. M). These formulas are often preferable to the one from which they were deduced.

328.

Examples. I. We seek all values of the expression $\sqrt{-1365}$ (mod. $5428681 = M$). The number M is here $\equiv 1, 1, 1, 6, 11$ (mod. $4, 3, 5, 7, 13$), and is therefore of a form of divisors of $xx+1$, $xx+3$, $xx-5$, and of a form of non-divisors of $xx+7$, $xx-13$, and hence of a form of divisors of $xx + 1365$. The character of the genus in which the classes $\mathfrak{G}$ are found will be $1, 4$; $R3$; $R5$; $N7$; $N13$. This genus contains just one class, from which we choose the form $6xx + 6xy + 229yy$. To find all representations of M by it, we put $2x+y = x'$, giving $3x'x' + 455yy = 2M$. This equation admits four solutions in which y is positive, namely $y = 127$, $x' = \pm 1083$, $y = 119$, $x' = \pm 1213$. These give four solutions of the equation $6xx + 6xy + 229yy = M$ in which y is positive:

x	478	−605	547	−666
y	127	127	119	119

The first solution gives for v the value of the expression $\frac{30517}{478}$, or $-\frac{3249}{127}$ (mod. M), from which we find 2350978; the second produces the opposite value −2350978; the third gives 2600262, and the fourth its opposite −2600262.

II. If the values of the expression $\sqrt{-286}$ (mod. $4272943 = M$) are sought, the character of the genus containing the classes $\mathfrak{G}$ is found to be 1 and $7, 8$; $R11$; $R13$. It is therefore the principal genus, containing three classes represented by the forms $(1, 0, 286)$, $(14, 6, 23)$, $(14, -6, 23)$. The third may be disregarded, since it is opposite to the second. The form $xx + 286yy$ gives two representations of M in which y is positive, namely $y = 103$, $x = \pm 1113$, yielding the values 1493445, −1493445 of the proposed expression. But by the form $(14, 6, 23)$, M is found not to be representable, so there are no values other than the two found.

III. Given the expression $\sqrt{-70}$ (mod. 997331), the classes $\mathfrak{G}$ must lie in the genus whose character is 3 and $5, 8$; $R5$; $N7$. There is just one class in this genus, represented by the form $(5, 0, 14)$. But calculation shows that 997331 cannot be represented by the form $(5, 0, 14)$; hence -70 must be a quadratic nonresidue of that number.

Two methods for distinguishing composite numbers from primes and finding the factors of the former.

329.

It is so well known that the problem of distinguishing primes from composite numbers and resolving the latter into their prime factors is among the most important and useful problems in all arithmetic, and has occupied the diligence and ingenuity of mathematicians both ancient and modern, that a lengthy discussion would be superfluous. Nevertheless, we must admit that all methods proposed so far are either restricted to very special cases or so laborious and lengthy that they exhaust even a practiced calculator's patience for numbers that do not exceed the limits of the tables constructed by deserving men, that is, numbers for which elaborate methods are unnecessary; for larger numbers they can generally hardly be used at all. Those tables, which are in everyone's hands and which we may hope will gradually be extended further, certainly suffice in most ordinary cases. Yet an experienced calculator quite often has occasion to gain great advantages from factoring large numbers, advantages that amply repay a moderate expenditure of time. Moreover, the dignity of the science seems to require that every means of solving so elegant and celebrated a problem be carefully developed. For these reasons we do not doubt that the following two methods, whose effectiveness and brevity we can confirm from long experience, will be welcome to lovers of arithmetic. It is, moreover, inherent in the nature of the problem that *every* method becomes progressively longer as the numbers to which it is applied grow larger. With the following methods, however, the difficulties increase very slowly, and numbers of seven, eight or even more digits have always been treated successfully, especially by the second method, with all the speed that can reasonably be expected for such large numbers, which by all methods known hitherto would require work intolerable even to an indefatigable calculator.

Before using the following methods, it is always very useful to try dividing the proposed number by some of the smallest primes, say $2, 3, 5, 7$, etc., up to 19 or further. This is not only to avoid regretting the discovery, by subtle and elaborate methods, of a divisor that could have been found much more easily by division alone[*)], but also because, when none of these divisions succeeds, the second method makes very profitable use of the *remainders* from them. Thus, for example, if 314159265 is to be resolved into its factors, division by 3 succeeds twice, followed by divisions by 5 and 7, giving $314159265 = 9.5.7.997331$. It is therefore enough to examine more closely the number 997331, which is found not divisible by $11, 13, 17, 19$. Similarly, given 43429448, we shall remove the factor 8 and apply the more elaborate methods to the quotient 5428681.

[*)] All the more so because, generally speaking, scarcely one number in six is found not divisible by any of $2, 3, 5 \ldots 19$.

330.

The FIRST METHOD rests on the theorem that *any positive or negative number that is a quadratic residue of another number M is also a residue of every divisor of M.* It is well known that, if M is divisible by no prime below $\sqrt{M}$, then M is certainly prime. If, however, all primes below this bound dividing M are p, q, etc., then M either consists of these *alone*, or their powers, or can contain only *one* other prime factor greater than $\sqrt{M}$, which is found by dividing M by p, q, etc., as often as possible. Denote the collection of all primes below $\sqrt{M}$, excluding those by which division has already been tried unsuccessfully, by Ω. It is evident that it is enough to find all prime divisors of M contained in Ω. Now, if we know from any source that a number r, not a square, is a quadratic residue of M, no prime for which r is $NR.$ can be a divisor of M. We may therefore remove from Ω all such primes, which will generally make up about half of the whole. If another number that is not a square, r', is also known to be a residue of M, we may again exclude from the primes remaining in Ω after the first exclusion those for which r' is $NR.$. These will again make up about half of them, provided the residues r and r' are independent, *i.e.* unless one is necessarily, of itself, a residue of all numbers of which the other is a residue, as would happen if rr' were a square. If still other residues of M are known, r'', r''', etc., all independent of the others[*)], similar exclusions can be made with each. These reduce the collection of numbers in Ω very rapidly, so that soon either all are removed, in which case M is certainly prime, or so few remain, evidently including all prime divisors of M, if it has any, that division by them can be tried without difficulty. For a number not much above a million, six or seven exclusions will generally be more than enough; for a number of eight or nine digits, nine or ten. Two points now remain to be discussed: *first*, how to find sufficiently many suitable residues of M, and *then*, how to perform the exclusion itself most conveniently. But we shall reverse the order of these questions, especially because the second will show which residues are most suitable for this purpose.

[*)] If the product of any number of r, r', r'', etc., is a square, each of them, for example r, will be a residue of every prime, dividing none of these numbers, that is a residue of the remaining numbers r', r'', etc. Thus, for any number of residues to be regarded as independent, no product of two, three, etc., may be a square.

331.

In Section IV we explained in detail how to distinguish the primes of which a given number r (which we may assume is divisible by no square) is a residue from those of which it is a nonresidue, or the divisors of the expression $xx - r$ from its non-divisors: all the former are contained in certain formulas of the kind $rz + a,\ rz + b$, etc., or of the kind $4rz + a,\ 4rz + b$, etc., and the latter in other similar formulas. Whenever r is a very small number, these formulas allow the exclusions to be made very conveniently; for example, we must exclude all numbers of the form $4z+3$ when $r = -1$; all numbers of the forms $8z + 3$ and $8z + 5$ when $z = 2$, etc. But we cannot always find such residues of the proposed number M, and applying the formulas for a large value of r is not convenient enough. It is therefore an enormous advantage, and remarkably eases the work of exclusion, to have a *table* already constructed for a sufficiently large collection of numbers (r), both positive and negative, divisible by no square, distinguishing the primes of which each of these (r) is a residue from those of which it is a nonresidue. Such a table can be arranged like the sample appended to this work and already described above; but to be sufficiently useful for the present purpose, the primes placed in the margin (the moduli) must be continued much further, say at least to 1000 or 10000. It is also much more convenient to include composite and negative numbers among the headings, although, as Section IV shows, this is not absolutely necessary. Such a table will be most convenient to use if its individual vertical columns are cut out and glued onto strips or rods (like Napier's), so that those needed in any given case, namely those corresponding to the numbers r, r', r'', etc., residues of the proposed number to be factored, can be examined separately. When they are placed *properly* beside the first column of the table (which gives the moduli), that is, so that the positions on the individual rods corresponding to the same prime in the first column are aligned with it, or lie on the same horizontal line, we can clearly recognize at a glance the primes that, after the exclusions with the residues r, r', r'', remain in Ω: they are precisely those numbers in the first column that have a stroke beside them on *all* the adjacent rods, and we must reject all those with a blank space beside them on *any* rod. An example will make this sufficiently clear. If it is known from some source that the numbers $-6, +13, -14, +17, +37, -53$ are residues of 997331, we must put together the first column (which in this case must extend to 997, the prime immediately below $\sqrt{997331}$) and the strips headed

by the numbers $-6, +13$, etc. Here is part of the resulting arrangement:

	-6	$+13$	-14	$+17$	$+37$	-53
3	–	–	–		–	–
5	–		–			
7	–		–		–	
11	–				–	
13		–	–	–		–
17		–		–		–
19			–	–		–
23		–	–			–
			etc.			
113		–	–			–
127	–	–	–	–	–	–
131	–	–	–			
			etc.			

Just as a glance shows here that, among the primes *included in this part of the arrangement*, only 127 remains after the exclusions with the residues $-6, 13$, etc., in Ω, so the complete arrangement extended to 997 shows that *absolutely* no other prime remains in Ω; on trying the division, we find that 997331 is indeed divisible by 127. In this way, therefore, that number has been resolved into the prime factors 127×7853[*)].

This account also makes it sufficiently clear that residues which are not too large, or can at least be resolved into prime factors which are not too large, are particularly useful: the direct use of the auxiliary table does not extend beyond the numbers among its headings, and its indirect use covers only those that can be resolved into factors contained in the table.

332.

We will give three different methods of finding residues of a given number M. Before explaining them, we make two observations that allow simpler residues to be derived from less suitable ones. *First*, if a number akk divisible by the square kk (which is assumed coprime to M) is a residue of M, then a is also a residue; for this reason, residues divisible by large squares are just as useful as small ones, and we will assume that the square factors of all residues supplied by the following methods have been removed at once. *Second*, if two or more numbers are residues, their product is also a residue. Combining this observation with the preceding one very often allows us to derive a very simple residue from several that are not all simple enough, provided they contain many common factors. For this reason, residues composed of many factors which are not too large are also very suitable, and it will be useful to

[*)]The author would gladly publish the fairly extensive apparatus of the table described here, which he had constructed for his own use, if the small number of people to whom it can be useful were sufficient to cover the costs of such an undertaking. If, meanwhile, any lover of arithmetic, having thoroughly understood the principles, wishes to construct such a table for himself by his own efforts, the author will take great pleasure in sharing with him by letter all the aids and devices.

resolve them all into their factors at once. The force of these observations will be better understood through examples and frequent use than through rules.

I. The simplest method, and the most convenient for those who have already gained some skill through frequent practice, consists in decomposing M, or more generally any multiple of M, in any way into two parts $kM = a + b$ (whether both are positive or one positive and the other negative). Their product with its sign changed will be a residue of M; for $-ab \equiv aa \equiv bb \pmod{M}$, and hence $-ab \,R\, M$. The numbers a, b should be chosen so that their product is divisible by a large square and the quotient is either small or at least resolvable into factors which are not too large; this can always be done without difficulty. We particularly recommend taking for a a square, or twice a square, or three times a square, etc., differing from the number M by a number which is either small or resolvable into convenient factors. For example, we find

$$\begin{aligned} 997331 &= 999^2 - 2.5.67 \\ &= 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2 \\ &= 3.575^2 + 11.31.4^2 = 3.577^2 - 7.13.4^2 \\ &= 3.578^2 - 7.19.37 = 11.299^2 + 2.3.5.29.4^2 \\ &= 11.301^2 + 5.12^2 \end{aligned}$$

etc. This gives the following residues: $2.5.67$, -5.11, $-2.3.17$, $-3.11.31$, $3.7.13$, $3.7.19.37$, $-2.3.5.11.29$; the last decomposition supplies the residue -5.11, which we already have. Instead of the residues $-3.11.31$, $-2.3.5.11.29$, we can take $3.5.31$, $2.3.29$, obtained by combining them with -5.11.

II. The second and third methods follow from the fact that, if two binary forms (A, B, C), (A', B', C') of the same determinant M, or $-M$, or more generally $\pm kM$, belong to the same genus, the numbers AA', AC', $A'C$ are residues of kM. This is readily seen from the fact that any characteristic number of one form, say m, is also a characteristic number of the other, and hence mA, mC, mA', mC' are all residues of kM. Thus, if (a, b, a') is a reduced form of positive determinant M, or more generally kM, and (a', b', a''), (a'', b'', a'''), etc., are forms in its period, and hence equivalent to it and all the more certainly contained in the same genus, the numbers aa', aa'', aa''', etc., will all be residues of M. A large number of forms in such a period can be calculated very easily with the algorithm of Article 187; the simplest residues usually result from setting $a = 1$; those containing factors which are too large should be rejected. Here are the beginnings of the periods of the forms $(1, 998, -1327)$ and $(1, 1412, -918)$, whose determinants are 997331, 1994662:

$(1, \ 998, \ -1327)$	$(1, \ 1412, \ -918)$
$(-1327, \ 329, \ 670)$	$(-918, \ 1342, \ 211)$
$(670, \ 341, \ -1315)$	$(211, \ 1401, \ -151)$
$(-1315, \ 974, \ 37)$	$(-151, \ 1317, \ 1723)$
$(37, \ 987, \ -626)$	$(1723, \ 406, \ -1062)$
$(-626, \ 891, \ 325)$	$(-1062, \ 656, \ 1473)$
$(325, \ 734, \ -1411)$	$(1473, \ 817, \ -901)$
$(-1411, \ 677, \ 382)$	$(-901, \ 985, \ 1137)$
$(382, \ 851, \ -715)$	etc.

Thus the number 997331 has all the numbers $-1327, 670$, etc., as residues; omitting those containing factors which are too large, we have the following: $2.5.67$, 37, 13, -17.83, $-5.11.13$, $-2.3.17$, -2.59, -17.53. The residue $2.5.67$, as well as -5.11, which results from combining the third with the fifth, had already been found above.

III. If C is any class of forms of negative determinant $-M$, or more generally $-kM$, different from the principal class, and its period is $2C$, $3C$, etc. (Article 307), the classes $2C$, $4C$, etc., will belong to the principal genus, and $3C$, $5C$, etc., to the same genus as C. Thus, if (a, b, c) is a (simplest) form in C, and (a', b', c') a form in some class of that period, say nC, either a' or aa' will be a residue of M, according as n is even or odd (in the former case clearly also c', and in the latter ac', ca' and cc'). The period, that is, the simplest forms in its classes, can be worked out with remarkable ease when a is very small, especially in the case $= 3$, which can always be achieved when $kM \equiv 2 \pmod 3$. Here is the beginning of the period of the class containing the form $(3, 1, 332444)$:

C	$(3, \ 1, \ 332444)$	$6C$	$(729. \ -209, \ 1428)$
$2C$	$(9, \ -2, \ 110815)$	$7C$	$(476, \ 209, \ 2187)$
$3C$	$(27, \ 7, \ 36940)$	$8C$	$(1027, \ 342, \ 1085)$
$4C$	$(81, \ 34, \ 12327)$	$9C$	$(932, \ -437, \ 1275)$
$5C$	$(243, \ 34, \ 4109)$	$10C$	$(425, \ 12, \ 2347)$

This gives the residues (rejecting the useless ones) 3.476, 1027, 1085, 425, or (removing square factors) $3.7.17$, 13.79, $5.7.31$, 17. By combining these suitably with

the eight residues found in II, we easily obtain the following twelve: -2.3, 13, -2.7, 17, 37, -53, -5.11, 79, -83, -2.59, $-2.5.31$, $2.5.67$; the first six are the same as those we used in Article 331. We could have added the residues 19 and -29 if we had also wished to use those found in I; the others obtained there already depend on those developed here.

333.

The SECOND METHOD of factoring a given number M comes from considering the values of an expression such as $\sqrt{-D}$ (mod. M), and rests on the following observations.

I. When M is a prime or a power of a prime (the prime being odd and not dividing D), $-D$ will be a residue or a nonresidue of M according as M is contained in a form of divisors or in a form of non-divisors of $xx + D$; in the former case the expression $\sqrt{-D}$ (mod. M) will have only two distinct values, which will be opposite.

II. But when M is composite, say $= pp'p''$, etc., where p, p', p'', etc., denote primes (distinct, odd, and not dividing D) or powers of such primes, $-D$ will be a residue of M only when it is a residue of each of p, p', p'', etc., that is, when all these numbers are contained in forms of divisors of $xx + D$. If we denote the values of the expression $\sqrt{-D}$ modulo p, p', p'', etc., respectively, by $\pm r$, $\pm r'$, $\pm r''$, etc., all the values of the same expression modulo M arise by finding the numbers which, modulo p, are $\equiv r$ or $\equiv -r$, modulo p', either $\equiv r'$ or $\equiv -r'$, etc. Their number will therefore be $= 2^\mu$, where μ counts the numbers p, p', p'', etc. Thus, if these values are $R, -R, R', -R'$, R'', etc., we automatically have $R \equiv R$ modulo all of p, p', p'', etc., but modulo none of them $R \equiv -R$. Hence the greatest common divisor of M and $R - R$ will be M, and 1 will be the greatest common divisor of M and $R + R$. But two values which are neither identical nor opposite, such as R and R', must be congruent modulo one or more of the numbers p, p', p'', etc., but not modulo all of them, and modulo the rest $R \equiv -R'$; hence the product of the former will be the greatest common divisor of M and $R - R'$, and the product of the latter the greatest common divisor of M and $R + R'$. It follows easily that, if we calculate all the greatest common divisors of M and the differences between the individual values of the expression $\sqrt{-D}$ (mod. M) and any given value, their collection contains the numbers $1, p, p', p''$, etc., and all products of two, three, etc., of these numbers. *In this way, therefore, from the values of that expression we can obtain the numbers p, p', p'', etc.*

Moreover, the method of Article 327 reduces each of these values to the values of expressions of the form $\frac{m}{n}$ (mod. M), where the denominator n is coprime to M; for the present purpose it is not even necessary to calculate these expressions themselves. For the greatest common divisor of M and the difference between R and R', which agree with $\frac{m}{n}, \frac{m'}{n'}$, is clearly also the greatest common divisor of M and $nn'(R - R')$. Equivalently, it is the greatest common divisor of M and $mn' - m'n$, to which $nn'(R - R')$ is congruent modulo M.

334.

The preceding observations can be applied to our problem in two ways. The first not only decides whether the proposed number M is prime or composite, but in the latter case also supplies the factors themselves; the second has the advantage of usually allowing a quicker calculation, but sometimes fails to produce the factors themselves of composite numbers, which it likewise distinguishes completely from primes, unless it is repeated several times.

I. Find a negative number $-D$ which is a quadratic residue of M; for this purpose the methods given in Article 332 under I and II can be used. In itself, the choice of residue is arbitrary, and here, unlike the preceding method, we do not need D to be a small number; but the calculation will be shorter, the smaller the number of classes of binary forms in each properly primitive genus of determinant $-D$. Hence residues among the 65 numbers of Article 303, if any present themselves, will be particularly suitable. Thus for $M = 997331$, of all the negative residues obtained above, -102 would be the most suitable. Find all the distinct values of the expression $\sqrt{-D}$ (mod. M); if only two result (opposite ones), M will certainly be either a prime or a power of a prime; if there are more, say 2^μ, M will be composed of μ distinct primes, or powers of primes, and these factors can be obtained by the method of the preceding article. Whether these factors are primes or powers of primes will be very easy to recognize in itself; furthermore, the very procedure by which the values of the expression $\sqrt{-D}$ are found automatically indicates all primes some power of which divides M. Namely, if M is divisible by the square of a prime π, that calculation will certainly also have produced one or more representations of M, $M = amm + 2bmn + cnn$, in which the greatest common divisor of the numbers m, n is π (indeed, because in this case $-D$ is also a residue of $\frac{M}{\pi\pi}$). But when no representation has appeared in which m and n have a common divisor, this is a sure indication that M is divisible by no square, and hence all of p, p', p'', etc., are primes.

Example. By the method given above we find four values of the expression $\sqrt{-408}$ (mod. 997331) agreeing with the values of $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$; the greatest common divisors of 997331 with $3.1664 - 113.2824$ and $3.1664 + 113.2824$, or with 314120 and 324104, will be 7853 and 127, whence $997331 = 127.7853$, as above.

II. Take any negative number $-D$ such that M is contained in a form of divisors of $xx + D$. In itself, the choice of such a number is arbitrary, but for convenience we should particularly seek to make the number of classes in the genera of determinant $-D$ as small as possible. Finding such a number presents no difficulty if we proceed by trial; for usually, among a considerable collection of numbers tried, M is contained in a form of divisors for about as many as in a form of non-divisors. It will therefore be most useful to begin the trial with the 65 numbers of Article 303 (starting with the largest), and if it should happen that none is suitable (which, generally speaking, occurs only once in 16384 cases), to proceed to others for which each genus contains two classes. — Then find the values of the expression $\sqrt{-D}$ (mod. M), and if any are found, deduce the factors of M from them in exactly the same way as above; but if no values appear, so that $-D$ is a nonresidue of M, then M certainly cannot be either a prime or a power of a prime. If, in this case, the factors themselves are wanted, we must either repeat the same operation, choosing other values for D, or turn to another method.

Thus, for example, on making the trial, we find that 997331 is contained in a form of non-divisors of $xx + 1848$, $xx + 1365$, $xx + 1320$, but in a form of divisors of $xx + 840$; the values of the expression $\sqrt{-840}$ (mod. 997331) give the expressions $\pm\frac{1272}{163}, \pm\frac{3288}{125}$, from which the same factors are deduced as before. — Anyone wanting further examples may consult Article 328: the first shows that $5428681 = 307.17683$; the second, that 4272943 is a prime; the third, that 997331 is certainly composed of several primes.

* *
*

The limits of this work have allowed us to pursue here only the main points of the two methods of finding factors; we reserve a fuller investigation, together with further auxiliary tables and other aids, for another occasion.

SEVENTH SECTION

ON

THE EQUATIONS DEFINING DIVISIONS OF THE CIRCLE.

335.

Among the most brilliant advances added to mathematics by the work of recent mathematicians, the theory of functions depending on the circle undoubtedly holds a particularly distinguished place. The greatest mathematicians of recent times have devoted their industry and insight so persistently to this remarkable kind of quantity, to which we are so often led in investigations of the most varied kinds, and whose help no part of mathematics can do without, and have built from it so vast a subject, that one could hardly have expected any part of this theory, much less an elementary part lying, as it were, at its very threshold, still to admit substantial advances. I am speaking of the theory of trigonometric functions corresponding to arcs commensurable with the circumference, or the theory of regular polygons; this section will show how little of it has so far been developed. Readers might wonder why such an investigation is undertaken in this work in particular, devoted chiefly to a subject which at first sight seems entirely different; but the treatment itself will make sufficiently clear how closely this subject is connected with higher arithmetic.

The principles of the theory we are about to present also extend much further than we carry them here. They can be applied not only to circular functions, but with equal success to many other transcendental functions, for example those depending on the integral $\int \frac{dx}{\sqrt{(1-x^4)}}$, and also to various kinds of congruences. But since we are preparing an extensive separate work on those transcendental functions, and congruences will be treated in detail in the continuation of the arithmetical investigations, we have thought it appropriate to consider only circular functions here. Indeed, even these, which we could treat in the fullest generality, we will reduce to the simplest case by the means to be explained in the following articles, both for brevity and to make the entirely new principles of this theory easier to understand.

The investigation is reduced to the simplest case, in which the number of parts into which the circle is to be divided is a prime.

336.

Denote the circumference of the circle, or four right angles, by P, and suppose m, n are integers, and n the product of pairwise coprime factors a, b, c, etc. By Article 310 the angle $A = \frac{mP}{n}$ can be put in the form $A = (\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\text{etc.})P$, and its trigonometric functions can be derived by known methods from the functions belonging to the parts $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, etc. Thus, since we can take primes or powers of primes for a, b, c, etc., it clearly suffices to consider division of the circle into a number of parts equal to a prime or a power of a prime, and the polygon with n sides will follow immediately from the polygons with a, b, c, etc., sides. Here, however, we will restrict the investigation

to the case in which the circle is to be divided into a number of parts which is an (odd) prime, chiefly for the following reason. It is known that the circular functions corresponding to the angle $\frac{mP}{pp}$ can be derived from the functions belonging to $\frac{mP}{p}$ by solving an equation of degree p, and likewise from these, by an equation of the same degree, the functions belonging to $\frac{mP}{p^3}$, etc.; thus, if the polygon with p sides is already given, determining the polygon with p^λ sides necessarily requires solving $\lambda - 1$ equations of degree p. Although the following theory can also be extended to this case, this route will still lead to just as many equations of degree p, which, if p is a prime, cannot in any way be reduced to lower degrees. For example, it will be shown below that the polygon with 17 sides can be constructed geometrically; but in determining the polygon with 289 sides there is no way to avoid an equation of degree 17.

Equations for the trigonometric functions of arcs which are one or more parts of the whole circumference; reduction of trigonometric functions to the roots of the equation $x^n - 1 = 0$.

337.

It is well known that the trigonometric functions of all the angles $\frac{kP}{n}$, where k ranges over all the numbers $0, 1, 2 \ldots n-1$, can be expressed by roots of equations of degree n: namely, the *sines* by the roots of (I)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n.n-3}{1.2}x^{n-4} - \frac{1}{64}\frac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx = 0$$

the *cosines* by the roots of (II)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n.n-3}{1.2}x^{n-4} - \frac{1}{64}\frac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0$$

and finally the *tangents* by the roots of (III)

$$x^n - \frac{n.n-1}{1.2}x^{n-2} + \frac{n.n-1.n-2.n-3}{1.2.3.4}x^{n-4} - \text{etc.} \pm nx = 0$$

These equations (which hold generally for every odd value of n, and II also for even values) can easily be reduced, on setting $n = 2m + 1$, to degree m: I and III by dividing the left side by x and substituting y for xx. Equation II clearly has the root $x = 1$ $(= \cos 0)$, and the remaining roots are always equal in pairs $(\cos\frac{P}{n} = \cos\frac{(n-1)P}{n},\ \cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc.); thus its left side is divisible by $x - 1$,

and the quotient will be a square. Taking its square root reduces equation II to

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{m-2.m-3}{1.2}x^{m-4} + \frac{1}{32}\frac{m-3.m-4}{1.2}x^{m-5} - \text{etc.} = 0$$

whose roots will be the cosines of the angles $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{mP}{n}$. Further reductions of these equations, at least for the case in which n is a prime, have not so far been available.

None of these equations, however, is as easy to handle or as suitable for our purpose as $x^n - 1 = 0$, whose roots are known to be very closely connected with theirs. Namely, writing i for the imaginary quantity $\sqrt{-1}$ for brevity, the roots of the equation $x^n - 1 = 0$ are given by

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r,$$

where k is to take all the values $0, 1, 2 \ldots n-1$. Thus, since $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, the roots of equation I are given by $\frac{1}{2i}(r - \frac{1}{r})$, or by $i\frac{1-rr}{2r}$; the roots of equation II by $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+rr}{2r}$; and finally the roots of equation III by $\frac{i(1-rr)}{1+rr}$. For this reason we will base the investigation on considering the equation $x^n - 1 = 0$, assuming n to be an odd prime. To avoid having to interrupt the order of the investigations, we give the following lemma first.

338.

Problem. *Given the equation*

$$(W) \ldots z^m + Az^{m-1} + \text{etc.} = 0,$$

find an equation (W') *whose roots are the* λ*-th powers of the roots of the equation* (W)*, where* λ *denotes a given positive integer exponent. Solution.* Denote the roots of the equation W by a, b, c, etc.; the roots of the equation W' must be $a^\lambda, b^\lambda, c^\lambda$, etc. By Newton's well-known theorem, the coefficients of the equation W allow us to find the sums of any powers of the roots a, b, c, etc. Thus find the sums

$$a^\lambda + b^\lambda + c^\lambda + \text{etc.}, \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} \text{ etc. etc.}$$
$$\text{up to} \quad a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{etc.}$$

from which, proceeding in reverse by the same theorem, we can deduce the coefficients of the equation W'. *Q. E. F.* — At the same time this shows that, if all the coefficients in W are rational, all those in W' will also be rational. It can indeed be proved by another route that, if the former are all integers, the latter will also all be integers; but we will not dwell here on this theorem, which is not so necessary for our purpose.

339.

The equation $x^n - 1 = 0$ (under the assumption, always to be understood from now on, that n is an odd prime) has a single real root, $x = 1$; the remaining $n - 1$ roots satisfy the equation

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$$

and are all imaginary. We will denote their collection by Ω, and the function

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 \quad \text{by} \quad X$$

respectively. Thus, if r is any root in Ω, we have $1 = r^n = r^{2n}$, etc., and generally $r^{en} = 1$ for every integer value of e, positive or negative; hence, if λ, μ are integers congruent modulo n, we clearly have $r^\lambda = r^\mu$. But if λ, μ are incongruent modulo n, r^λ and r^μ will be unequal; for in this case an integer ν can be chosen so that $(\lambda - \mu)\nu \equiv 1 \pmod{n}$, whence $r^{(\lambda-\mu)\nu} = r$, and therefore $r^{\lambda-\mu}$ is certainly not $= 1$. It is also clear that every power of r is a root of the equation $x^n - 1 = 0$; thus, since the quantities $1\ (= r^0), r, rr \ldots r^{n-1}$ are all distinct, they give all the roots of the equation $x^n - 1 = 0$, and hence the collection $r, rr, r^3 \ldots r^{n-1}$ coincides with Ω. More generally, it follows easily that Ω coincides with the collection $r^e, r^{2e}, r^{3e} \ldots r^{(n-1)e}$ if e is any integer not divisible by n, positive or negative. We therefore have

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$$

whence

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1,$$
$$\text{and} \quad 1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

We will call two roots such as r and $\frac{1}{r}\ (= r^{n-1})$, or generally r^e and r^{-e}, *reciprocal*; clearly the product of the two simple factors $x - r$ and $x - \frac{1}{r}$ is real, $= xx - 2x\cos\omega + 1$, where the angle ω is equal either to the angle $\frac{P}{n}$ or to one of its multiples.

340.

Thus, if one root in Ω is denoted by r, all the roots of the equation $x^n - 1 = 0$ are expressed by powers of r, and a product formed in any way from several roots of this equation can be represented by r^λ, where λ is either 0, or positive and $< n$. Now let $\varphi(t, u, v \ldots)$ denote a rational integral algebraic function of the indeterminates t, u, v, etc., expressible as a sum of terms of the form $ht^\alpha u^\beta v^\gamma \ldots$. It is clear that, if we substitute for t, u, v, etc., some of the roots of the equation $x^n - 1 = 0$, say $t = a$, $u = b, v = c$, etc., $\varphi(a, b, c \ldots)$ can be put in the form

$$A + A'r + A''rr + A'''r^3 + \ldots + A^\nu r^{n-1}$$

where the coefficients A, A', etc. (some of which may be absent and hence $= 0$) are fixed quantities; moreover, all these coefficients will be integers if all the fixed coefficients in $\varphi(t, u, v \ldots)$, that is, all the h, are integers. If we then replace $t, u, v \ldots$ by $aa, bb, cc \ldots$, respectively, any term such as $ht^\alpha u^\beta v^\gamma \ldots$, which previously reduced to r^σ, will now become $r^{2\sigma}$. It follows easily that

$$\varphi(aa, bb, cc \ldots) = A + A'rr + A''r^4 + A'''r^6 + \ldots + A^\nu r^{2n-2}$$

Similarly, for any integer value of λ, we have in general

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

This proposition is of the greatest importance and forms the foundation of the following investigations. — This also gives

$$\varphi(1, 1, 1 \ldots) = \varphi(a^n, b^n, c^n \ldots) = A + A' + A'' + \ldots + A^\nu$$

and

$$\varphi(a, b, c \ldots) + \varphi(aa, bb, cc \ldots) + \varphi(a^3, b^3, c^3 \ldots) + \ldots + \varphi(a^n, b^n, c^n \ldots) = nA$$

Thus this sum is always an integer divisible by n whenever all the fixed coefficients in $\varphi(t, u, v \ldots)$ are integers.

Theory of the roots of the equation $x^n - 1 = 0$ (where n is assumed prime). Omitting the root 1, the remaining roots (Ω) are contained in the equation $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$. The function X cannot be resolved into factors of lower degree whose coefficients are all rational.

341.

THEOREM. *If the function X is divisible by the function of lower degree*

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L$$

the coefficients $A, B \ldots L$ cannot all be integers.

Proof. Let $X = PQ$, and let $\mathfrak{P}$ be the collection of roots of the equation $P = 0$, and $\mathfrak{Q}$ the collection of roots of the equation $Q = 0$, so that Ω consists of $\mathfrak{P}$ and $\mathfrak{Q}$ taken together. Further, let $\mathfrak{R}$ be the collection of roots reciprocal to those in $\mathfrak{P}$, and $\mathfrak{S}$ the collection of roots reciprocal to those in $\mathfrak{Q}$. Let the roots contained in $\mathfrak{R}$ be the roots of the equation $R = 0$ (which is easily seen to be $x^\lambda + \frac{K}{L}x^{\lambda-1} + \text{etc.} + \frac{A}{L}x + \frac{1}{L} = 0$), and those contained in $\mathfrak{S}$ the roots of the equation $S = 0$. Clearly the roots $\mathfrak{R}$ and $\mathfrak{S}$ taken together also form the collection Ω, and $RS = X$. We now distinguish four cases.

I. When $\mathfrak{P}$ coincides with $\mathfrak{R}$, and hence $P = R$. In this case the roots in $\mathfrak{P}$ clearly come in reciprocal pairs, so P is a product of $\frac{1}{2}\lambda$ quadratic factors of the form $xx - 2x\cos\omega + 1$; since such a factor is $= (x - \cos\omega)^2 + \sin\omega^2$, it is easily seen that P necessarily takes a positive real value for every real value of x. Let the equations whose roots are respectively the squares, cubes, fourth powers ... and powers of order $n-1$ of the roots in $\mathfrak{P}$ be $P' = 0$, $P'' = 0, P''' = 0, \ldots P^\nu = 0$, and let the values of the functions $P, P', P'' \ldots P^\nu$ obtained by setting $x = 1$ be respectively $p, p', p'' \ldots p^\nu$. Then, by what was said above, p will be a positive quantity, and for exactly the same reason p', p'', etc., will also be positive. Now p is the value of the function $(1-t)(1-u)(1-v)$, etc., obtained by substituting for t, u, v, etc., the roots in $\mathfrak{P}$; p' is the value of the same function when we substitute for t, u, v, etc., the squares of those roots, etc.; moreover, the value for $t = 1, u = 1, v = 1$, etc., is clearly $= 0$. Thus the sum $p + p' + p'' \ldots + p^\nu$ will be an integer divisible by n. It is also easily seen that the product $PP'P'' \ldots$ is $= X^\lambda$, and hence $pp'p'' \ldots = n^\lambda$. Now, if all the coefficients in P were rational, all those in P', P'', etc., would also be rational by Article 338; by Article 42, however, all these coefficients would necessarily be integers. Thus p, p', p'', etc., would all be integers; since their product is n^λ, and their number satisfies $n - 1 > \lambda$, some of them (at least $n - 1 - \lambda$) must necessarily be $= 1$, and the rest equal to n or to a power of n. Thus, if g of them are $= 1$, the sum $p + p' + \text{etc.}$ will clearly be $\equiv g \pmod{n}$, and hence certainly not divisible by n. The assumption therefore cannot hold.

II. When $\mathfrak{P}$ and $\mathfrak{R}$ do not coincide but contain some common roots, let $\mathfrak{T}$ be their collection, and $T = 0$ the equation whose roots they are. Then T will be the greatest common divisor of the functions P, R (as is known from the theory of equations). The roots in $\mathfrak{T}$ clearly come in reciprocal pairs; hence, by what has been proved above, the coefficients in T cannot all be rational. But they certainly would be if all those

in P, and hence also all those in R, were rational, as follows directly from the nature of the operation of finding the greatest common divisor. The assumption is therefore absurd.

III. When $\mathfrak{Q}$ and $\mathfrak{S}$ either coincide or at least contain common roots, in exactly the same way the coefficients in Q cannot all be rational; but they would be rational if all those in P were rational. This is therefore impossible.

IV. But if neither the pair $\mathfrak{P}$ and $\mathfrak{R}$ nor the pair $\mathfrak{Q}$ and $\mathfrak{S}$ has any common root, all the roots $\mathfrak{P}$ must be found in $\mathfrak{S}$, and all those in $\mathfrak{Q}$ in $\mathfrak{R}$, whence $P = S$ and $Q = R$. Therefore $X = PQ$ will be the product of P and R, that is,

$$\begin{aligned} &\text{of} \quad x^\lambda + Ax^{\lambda-1} \ldots + Kx + L \\ &\text{and} \quad x^\lambda + \frac{K}{L}x^{\lambda-1} \ldots + \frac{A}{L}x + \frac{1}{L} \end{aligned}$$

whence, setting $x = 1$, we obtain

$$nL = (1 + A \ldots + K + L)^2$$

Now, if all the coefficients in P were rational, and hence also integers by Article 42, L, which must divide the last coefficient in X, namely unity, would necessarily be $= \pm 1$, whence $\pm n$ would be a square. Since this contradicts the hypothesis, the assumption cannot hold.

This theorem therefore shows that, however X is resolved into factors, at least some of their coefficients will be irrational, and hence cannot be determined except by an equation of higher degree.

The aim of the following investigations is explained.

342.

The aim of the following investigations, which it will be useful to explain briefly, is to resolve X STEP BY STEP into more and more factors, determining their coefficients by equations of the lowest possible degree, until we reach linear factors, or the roots Ω themselves. Namely, we will show that, if the number $n - 1$ is resolved in any way into integer factors α, β, γ, etc. (each of which may be taken prime), X can be resolved into α factors of degree $\frac{n-1}{\alpha}$, whose coefficients are determined by an equation of degree α; each of these factors in turn into β others of degree $\frac{n-1}{\alpha\beta}$, with the help of an equation of degree β, etc. Thus, if ν denotes the number of factors α, β, γ, etc., finding the roots Ω reduces to solving ν equations of degrees α, β, γ, etc. *For example*, for $n = 17$, where $n - 1 = 2.2.2.2$, four quadratic equations must be solved; for $n = 73$, three quadratic and two cubic equations.

In what follows we will very often have to consider powers of the root r whose exponents are themselves powers, and such expressions are troublesome to set in type. To make printing easier, we will henceforth use the following abbreviation. For r, rr, r^3, etc., we will write $[1], [2], [3]$, etc., and generally for r^λ, where λ denotes any integer, $[\lambda]$. Such expressions are therefore not yet fully determined, but become so as soon as, for r or $[1]$, a specific root in Ω is chosen. Thus, in general $[\lambda], [\mu]$

will be equal or unequal according as λ, μ are congruent or incongruent modulo n; furthermore $[0] = 1$; $[\lambda].[\mu] = [\lambda+\mu]$; $[\lambda]^\nu = [\lambda\nu]$; the sum $[0]+[\lambda]+[2\lambda]\ldots+[(n-1)\lambda]$ is either 0 or n, according as λ is not divisible or is divisible by n.

All the roots Ω are distributed into certain classes (periods).

343.

If, for the modulus n, g is a number of the kind we called a primitive root in Section III, the $n-1$ numbers $1, g, gg \ldots g^{n-2}$ will be congruent to $1, 2, 3 \ldots n-1$ modulo n, although in a different order: each number of one sequence has a congruent number in the other. It follows at once that the roots $[1], [g], [gg] \ldots [g^{n-2}]$ coincide with Ω; in exactly the same way, more generally,

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

coincide, where λ denotes any integer not divisible by n. Further, since $g^{n-1} \equiv 1 \pmod{n}$, it is readily seen that the two roots $[\lambda g^\mu], [\lambda g^\nu]$ are identical or different according as μ, ν are congruent or incongruent modulo $n-1$. Thus, if G is another primitive root, the roots $[1], [g] \ldots [g^{n-2}]$ will also agree with $[1], [G] \ldots [G^{n-2}]$ if order is disregarded. But it is also easily proved that, if e is a divisor of $n-1$, and we set $n-1 = ef$, $g^e = h$, $G^e = H$, the f numbers $1, h, hh \ldots h^{f-1}$ will be congruent to $1, H, H^2 \ldots H^{f-1}$ modulo n (without regard to order). For suppose $G \equiv g^\omega \pmod{n}$, and let μ be any positive number $< f$, and ν the least residue of $\mu\omega \pmod{f}$. Then $\nu e \equiv \mu\omega e \pmod{n-1}$, hence $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$, or $H^\mu \equiv h^\nu$; that is, each number of the latter sequence $1, H, H^2$, etc., has a congruent number in the sequence $1, h, hh \ldots$, and likewise conversely. — It is therefore clear that the f roots $[1], [h], [hh] \ldots [h^{f-1}]$ are identical with $[1], [H], [H^2] \ldots [H^{f-1}]$; more generally, it is readily seen in the same way that

$$[\lambda], [\lambda h], [\lambda hh] \ldots [\lambda h^{f-1}]$$
$$\text{with} \quad [\lambda], [\lambda H], [\lambda H^2] \ldots [\lambda H^{f-1}]$$

agree. We will denote the *sum* of such f roots $[\lambda] + [\lambda h] + \text{etc.} + [\lambda h^{f-1}]$, which, since it does not change when another primitive root is taken for g, must be regarded as independent of g, by $(f; \lambda)$; the *collection* of the same roots we will call the *period* (f, λ), without regard to the order of the roots[*]. — In writing such a period, it will be useful to reduce each of its roots to the simplest expression, namely to substitute for the numbers $\lambda, \lambda h, \lambda hh$, etc., the least residues modulo n; the terms of the period may also be arranged by their size, if desired.

For example, for $n = 19$, where 2 is a primitive root, the period $(6, 1)$ consists of the roots $[1], [8], [64], [512], [4096], [32768]$, or $[1], [7], [8], [11], [12], [18]$. Similarly the period $(6, 2)$ consists of $[2], [3], [5], [14], [16], [17]$. The period $(6, 3)$ is found to be identical with the preceding one. The period $(6, 4)$ contains $[4], [6], [9], [10], [13], [15]$.

[*] In what follows, we may also call the sum the numerical value of the period, or simply the period where there is no risk of ambiguity.

Various theorems on the periods of the roots Ω.

344.

The following observations about these periods immediately present themselves:

I. Since $\lambda h^f \equiv \lambda,\ \lambda h^{f+1} \equiv \lambda h$, etc., (mod. n), clearly the same roots that constitute (f, λ) also constitute $(f, \lambda h), (f, \lambda hh)$, etc.; thus, in general, if $[\lambda']$ denotes any root in (f, λ), this period will be completely identical with (f, λ'). Hence, if two periods consisting of equally many roots (which we will call *similar*) have any common root, they are clearly identical. Thus it is impossible for two roots to occur together in one period, while only one of them occurs in another similar period. It is also clear that, if two roots $[\lambda], [\lambda']$ belong to the same period of f terms, the value of the expression $\frac{\lambda'}{\lambda}$ (mod. n) is congruent to some power of h, or we may put $\lambda' \equiv \lambda g^{\nu e}$ (mod. n).

II. If $f = n-1,\ e = 1$, the period $(f, 1)$ clearly coincides with Ω; in the other cases Ω will be composed of e periods $(f, 1), (f, g), (f, gg) \ldots (f, g^{e-1})$. These periods are therefore all distinct, and clearly any other similar period (f, λ) coincides with one of them, provided $[\lambda]$ belongs to Ω, that is, if λ is not divisible by n. But the period $(f, 0)$, or (f, kn), clearly consists of f units. It is just as easily seen that, if λ is any number not divisible by n, the collection of e periods $(f, \lambda), (f, \lambda g), (f, \lambda gg) \ldots (f, \lambda g^{e-1})$ also coincides with Ω. — Thus, *for example*, for $n = 19,\ f = 6$, Ω consists of the three periods $(6, 1), (6, 2), (6, 4)$, to one of which any other similar period, except $(6, 0)$, reduces.

III. If $n - 1$ is the product of three positive numbers a, b, c, clearly any period of bc terms is composed of b periods of c terms: namely, (bc, λ) of $(c, \lambda), (c, \lambda g^a), (c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$, and these will therefore be said to be contained in the former. Thus, for $n = 19$, the period $(6, 1)$ consists of the three periods $(2, 1), (2, 8), (2, 7)$; the first contains the roots r, r^{18}, the second r^8, r^{11}, and the third r^7, r^{12}.

345.

THEOREM. *Let $(f,\lambda),(f,\mu)$ be two similar periods, identical or distinct, and let (f,λ) consist of the roots $[\lambda],[\lambda'],[\lambda'']$, etc. Then the product of (f,λ) and (f,μ) will be a sum of f similar periods, namely*

$$= (f,\lambda+\mu)+(f,\lambda'+\mu)+(f,\lambda''+\mu)+\text{etc.} = W$$

Proof. As above, let $n-1=ef$; let g be a primitive root modulo n, and $h=g^e$, whence, by what precedes, $(f,\lambda)=(f,\lambda h)=(f,\lambda hh)$, etc. The required product will therefore be

$$= [\mu].(f,\lambda)+[\mu h].(f,\lambda h)+[\mu hh].(f,\lambda hh)+\text{etc.}$$

and hence

$$\begin{array}{llll} =[\lambda+\mu] & +[\lambda h+\mu] & \ldots+[\lambda h^{f-1}+\mu] & \\ +[\lambda h+\mu h] & +[\lambda hh+\mu h] & \ldots+[\lambda h^{f}+\mu h] & \\ +[\lambda hh+\mu hh] & +[\lambda h^3+\mu hh] & \ldots+[\lambda h^{f+1}+\mu hh] & \text{etc.} \end{array}$$

This expression contains altogether ff roots. If each vertical column is now summed separately, we clearly obtain

$$(f,\lambda+\mu)+(f,\lambda h+\mu)+\ldots+(f,\lambda h^{f-1}+\mu)$$

This expression is readily seen to agree with W, since, by hypothesis, the numbers $\lambda,\lambda',\lambda''$, etc., must be congruent to $\lambda,\lambda h,\lambda hh\ldots\lambda h^{f-1}$ modulo n (the order is immaterial here), and therefore so must also

$$\begin{array}{c} \lambda+\mu,\ \lambda'+\mu,\ \lambda''+\mu \quad \text{etc.} \quad \text{to} \\ \lambda+\mu,\ \lambda h+\mu,\ \lambda hh+\mu\ldots\lambda h^{f-1}+\mu. \end{array} \quad \textit{Q. E. D.}$$

We add the following corollaries to this theorem:

I. If k denotes any integer, the product of $(f,k\lambda)$ and $(f,k\mu)$ will be

$$= (f,k(\lambda+\mu))+(f,k(\lambda'+\mu))+(f,k(\lambda''+\mu))+\text{etc.}$$

II. Since each part of which W consists agrees either with the sum $(f,0)$, which is $=f$, or with one of $(f,1)$, (f,g), $(f,gg)\ldots(f,g^{e-1})$, W can be reduced to the following form

$$W = af+b(f,1)+b'(f,g)+b''(f,gg) \\ +\ldots+b^{\varepsilon}(f,g^{e-1})$$

where the coefficients a,b,b', etc., will be positive integers (or some of them may also be $=0$). It is further clear that the product of $(f,k\lambda)$ and $(f,k\mu)$ then becomes

$$= af+b(f,k)+b'(f,kg)+\ldots+b^{\varepsilon}(f,kg^{e-1})$$

Thus, *for example*, for $n=19$, the product of the sum (6.1) with itself, or the square of this sum, becomes $=(6,2)+(6,8)+(6,9)+(6.12)+(6,13)+(6,19)=6+2(6,1)+(6,2)+2(6,4)$.

III. Since the product of each part of W and a similar period (f,ν) can be reduced to an analogous form, it is clear that the product of three periods $(f,\lambda).(f,\mu).(f,\nu)$ can also be represented by $cf + d(f,1) \ldots + d^{\varepsilon}(f,g^{e-1})$, and that the coefficients c, d, etc., will be integers and positive (or $= 0$); moreover, for any integer value of k,

$$(f,k\lambda).(f,k\mu).(f,k\nu) = cf + d(f,k) + d'(f,kg) + \text{etc.}$$

In the same way this theorem extends to products of any number of similar periods, and it makes no difference whether these periods are all distinct, or partly or all identical.

IV. It follows that, if in any rational integral algebraic function $F = \varphi(t,u,v\ldots)$ the indeterminates t, u, v, etc., are replaced respectively by similar periods $(f,\lambda), (f,\mu), (f,\nu)$, etc., its value can be reduced to the form

$$A + B(f,1) + B'(f,g) + B''(f,gg) + \ldots + B^{\varepsilon}(f,g^{e-1})$$

and the coefficients A, B, B', etc., will all be integers if all the fixed coefficients in F are integers. If we then replace t, u, v, etc., respectively by $(f,k\lambda), (f,k\mu), (f,k\nu)$, etc., the value of F reduces to $A + B(f,k) + B'(f,kg) + \text{etc.}$

346.

THEOREM. *Assuming that λ is a number not divisible by n, and writing p for (f,λ) for brevity, any other similar period (f,μ), where μ is also assumed not divisible by n, can be reduced to the following form*

$$\alpha + \beta p + \gamma pp + \ldots + \theta p^{e-1}$$

so that the coefficients α, β, etc., are fixed rational quantities.

Proof. For brevity, denote the periods $(f,\lambda g), (f,\lambda gg), (f,\lambda g^3)$, etc., up to $(f,\lambda g^{e-1})$, whose number is $e-1$, and with one of which (f,μ) must agree, by p', p'', p''', etc. We then immediately have the equation

$$0 = 1 + p + p' + p'' + p''' + \text{etc.} \quad . \ . \ . \ . \ . \quad \text{(I)}$$

Expanding the values of the powers of p up to the power with exponent $e-1$, according to the rules of the preceding article, gives $e-2$ further equations of the following kind.

$$0 = pp + A + ap + a'p' + a''p'' + a'''p''' + \text{etc.} \quad . \ . \quad \text{(II)}$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc.} \quad . \ . \quad \text{(III)}$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{etc.} \quad . \ . \quad \text{(IV)} \quad \text{etc.}$$

Here all the coefficients A, a, a', etc., B, b, b', etc., etc., will be integers and, as should be carefully noted and follows directly from the preceding article, completely independent of λ; *that is*, the same equations will continue to hold whatever other value is assigned to λ. This observation clearly extends to equation I as well, provided λ is taken not divisible by n. — Let us assume $(f,\mu) = p'$; for it is readily seen that, if (f,μ) agrees with another of the periods p'', p''', etc., arguments entirely analogous to those that follow can be used. Since the number of equations I, II, III, etc., is

$e-1$, the quantities p'', p''', etc., whose number is $= e-2$, can be eliminated from them by known methods, giving an equation of the following kind (Z), free of those quantities,

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}pp + \text{etc.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

This can be done so that all the coefficients $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{N}$ are integers and certainly not all $= 0$. Now, if $\mathfrak{N} = 0$ does not hold, it is immediately clear that p' is thereby determined in the way stated in the theorem. It therefore remains to show that $\mathfrak{N} = 0$ cannot occur.

Assuming $\mathfrak{N} = 0$, equation Z becomes $\mathfrak{M}p^{e-1} + \text{etc.} + \mathfrak{B}p + \mathfrak{A} = 0$; since its degree certainly does not exceed $e-1$, no more than $e-1$ distinct values of p can satisfy it. But since the equations from which Z was derived are independent of λ, it is clear that Z also does not depend on λ, or holds whatever integer not divisible by n is taken for λ. Thus equation Z will be satisfied whichever of the e sums $(f,1), (f,g), (f,gg) \ldots (f,g^{e-1})$ is set equal to p. It follows directly that these sums cannot all be unequal, but at least two must be equal to one another. Let one of two such equal sums contain the roots $[\zeta], [\zeta'], [\zeta'']$, etc., and the other $[\eta], [\eta'], [\eta'']$, etc.; assume (as we may) that all the numbers ζ, ζ', ζ'', etc., η, η', η'', etc., are positive and $< n$; clearly they will also all be distinct, and none $= 0$. Denote the function

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \text{etc.} - x^{\eta} - x^{\eta'} - x^{\eta''} - \text{etc.}$$

whose highest term does not exceed x^{n-1} by Y. Clearly $Y = 0$ when $x = [1]$ is set; hence Y contains the factor $x - [1]$, which it will have in *common* with the function denoted above by X. But this is easily shown to be absurd. For if Y had any common factor with X, the *greatest* common divisor of the functions X, Y (which certainly cannot reach degree $n-1$, as is already clear from the fact that Y is divisible by x) would have all its coefficients rational, as follows directly from the nature of the operations for finding the greatest common divisor of two such functions whose coefficients are all rational. But in Article 341 we showed that X cannot contain a factor of degree less than $n-1$ whose coefficients are all rational. Therefore the assumption $\mathfrak{N} = 0$ cannot hold.

Example. For $n = 19$, $f = 6$, $pp = 6+2p+p'+2p''$; from this and $0 = 1+p+p'+p''$ we deduce $p' = 4 - pp$, $p'' = -5 - p + pp$. Thus

$$\begin{aligned}
(6,2) &= 4 - (6,1)^2, \quad & (6,4) &= -5 - (6,1) + (6,1)^2 \\
(6,4) &= 4 - (6,2)^2, \quad & (6.1) &= -5 - (6,2) + (6,2)^2 \\
(6,1) &= 4 - (6,4)^2, \quad & (6,2) &= -5 - (6,4) + (6,4)^2
\end{aligned}$$

347.

THEOREM. *If $F = \varphi(t, u.v \ldots)$ is a symmetric*[*)] *algebraic rational integral function of f indeterminates t, u, v, etc., and, on substituting for these the f roots contained in the period (f, λ), the value of F is reduced by the rules of Article 340 to the form*

$$A + A'[1] + A''[2] + \text{etc.} = W$$

then the roots in this expression that belong to any one and the same period of f terms will have equal coefficients.

Proof. Let $[p], [q]$ be two roots belonging to one and the same period, and assume p, q positive and less than n, so that we must show that $[p]$ and $[q]$ have the same coefficient in W. Let $q \equiv pg^{\nu e} \pmod{n}$; further, let the roots contained in (f, λ) be $[\lambda], [\lambda'], [\lambda'']$, etc., where we assume the numbers $\lambda, \lambda', \lambda''$, etc., positive and less than n; finally, let the least positive residues of the numbers $\lambda g^{\nu e}, \lambda' g^{\nu e}, \lambda'' g^{\nu e}$, etc., modulo n, be μ, μ', μ'', etc. These will clearly be identical with the numbers $\lambda, \lambda', \lambda''$, etc., although in a different order. Now Article 340 shows that

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}] \ldots) = (\text{I})$$

reduces to

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{etc.}$$

$$\text{or to} \quad A + A'[\theta] + A''[\theta'] + \text{etc.} = (W')$$

where θ, θ', etc., denote the least residues of the numbers $g^{\nu e}, 2g^{\nu e}$, etc., modulo n. It is therefore clear that $[q]$ has the same coefficient in (W') as $[p]$ has in (W). But it is readily seen that expanding the expression (I) gives the same result as expanding $\varphi([\mu], [\mu'].[\mu'']$ etc.), since $\mu \equiv \lambda g^{\nu e}, \mu' \equiv \lambda' g^{\nu e}$, etc., $\pmod{n}$; the latter expression in turn gives the same result as $\varphi([\lambda], [\lambda'], [\lambda'']$ etc.), since the numbers μ, μ', μ'', etc., differ from $\lambda, \lambda', \lambda''$, etc., only in their order, which makes no difference in a symmetric function. It follows that W' will be completely identical with W; hence the root $[q]$ will have the same coefficient in W as $[p]$. *Q. E. D.*

It is therefore clear that W can be reduced to the form

$$A + a(f, 1) + a'(f, g) + a''(f, gg) \ldots + a^{\varepsilon}(f, g^{e-1})$$

where the coefficients $A, a \ldots a^{\varepsilon}$ are fixed quantities, which will also be integers if all the rational coefficients in F are integers. — Thus, *for example*, if $n = 19$, $f = 6$, $\lambda = 1$, and the function φ denotes the sum of the pairwise products of the indeterminates, its value reduces to $3 + (6, 1) + (6, 4)$.

It is further easily seen that, if we then substitute for t, u, v, etc., the roots from another period $(f, k\lambda)$, the value of F becomes

$$A + a(f, k) + a'(f, kg) + a''(f, kgg) + \text{etc.}$$

[*)] Functions are called symmetric, as is known, when all the indeterminates occur in them in the same way, or, more clearly, when they do not change however the indeterminates are permuted among themselves; such functions are *for instance* the sum of all of them, the product of all of them, the sum of their pairwise products, etc.

348.

In any equation

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \ldots = 0$$

the coefficients α, β, γ, etc., are symmetric functions of the roots, namely α the sum of all of them, β the sum of their pairwise products, γ the sum of their products taken three at a time, etc. Thus, in the equation whose roots are the roots contained in the period (f, λ), the first coefficient will be $= (f, \lambda)$, while each of the others can be reduced to a form such as

$$A + a(f, 1) + a'(f, g) \ldots + a^{\varepsilon}(f, g^{e-1})$$

where all of A, a, a', etc., will be integers. It is also clear that the equation whose roots are those contained in any other period $(f, k\lambda)$ is derived from it by replacing, in each coefficient, $(f, 1)$ by (f, k); similarly, replacing (f, g) by (f, kg) and, in general, (f, p) by (f, kp). In this way we can therefore specify e equations $z = 0, z' = 0, z'' = 0$, etc., whose roots are the roots contained in $(f, 1)$, in (f, g), (f, gg), etc., as soon as the e sums $(f, 1), (f, g), (f, gg)$, etc., are known, or rather as soon as any *one* of them has been found, since, by Article 346, all the others can be deduced rationally from one. At the same time, this resolves the function X into e factors of degree f: for the product of the functions z, z', z'', etc., will clearly be $= X$.

Example. For $n = 19$, the sum of all the roots in the period $(6, 1)$ is $= (6, 1) = \alpha$; the sum of their pairwise products is $= 3 + (6, 1) + (6, 4) = \beta$; similarly, the sum of the products taken three at a time is found to be $= 2 + 2(6, 1) + (6, 2) = \gamma$; the sum of the products taken four at a time $= 3 + (6, 1) + (6, 4) = \delta$; the sum of the products taken five at a time $= (6, 1) = \varepsilon$; the product of all of them $= 1$. Thus the equation

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x x - \varepsilon x + 1 = 0$$

includes all the roots contained in $(6, 1)$. If, in the coefficients α, β, γ, etc., we replace $(6, 1), (6, 2), (6, 4)$ respectively by $(6, 2), (6, 4), (6, 1)$, we obtain the equation $z' = 0$, which includes the roots in $(6, 2)$; if the same interchange is applied here again, we obtain the equation $z'' = 0$, including the roots in $(6, 4)$, and the product $zz'z''$ will be $= X$.

349.

It is usually more convenient, especially when f is a large number, to deduce the coefficients β, γ, etc., from the sums of the powers of the roots by Newton's theorem. For it is immediately clear that the sum of the squares of the roots contained in (f, λ) is $= (f, 2\lambda)$, the sum of their cubes $= (f, 3\lambda)$, etc. Thus, writing $(f, \lambda), (f, 2\lambda)$, $(f, 3\lambda)$, etc., as q, q', q'', etc., for brevity, we have

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'' \quad \text{etc.}$$

Here the products of two periods must immediately be converted into sums of periods by Article 345. Thus, in our example, writing $(6,1), (6,2), (6,4)$ respectively as p, p', p'', we obtain $q, q', q'', q''', q'''', q''''$ respectively $= p, p', p', p'', p', p''$; hence

$$\begin{aligned} \alpha &= p, \quad 2\beta = pp - p' = 6 + 2p + 2p'' \\ 3\gamma &= (3 + p + p'')p - pp' + p' = 6 + 6p + 3p' \\ 4\delta &= (2 + 2p + p')p - (3 + p + p'')p' \\ &\qquad + pp' - p'' = 12 + 4p + 4p'' \quad \text{etc.} \end{aligned}$$

It suffices, however, to calculate only half the coefficients in this way. For it is not difficult to prove that the last ones, in reverse order, are either equal to the first ones, namely the last $= 1$, the next to last $= \alpha$, the one before that $= \beta$, etc., or can be deduced from them respectively by replacing $(f, 1), (f, g)$, etc., by $(f, -1), (f, -g)$, etc., or $(f, n-1)$, $(f, n-g)$, etc. The first case occurs when f is even, the second when f is odd; the last coefficient, however, is always $= 1$. This rests on the theorem of Article 79; but, for brevity, we do not dwell on this subject.

350.

THEOREM. *Let $n - 1$ be the product of three positive integers α, β, γ; let the period $(\beta\gamma, \lambda)$, which has $\beta\gamma$ terms, consist of β smaller periods of γ terms, namely $(\gamma, \lambda).(\gamma, \lambda'), (\gamma, \lambda'')$, etc. Suppose that, in a function of β indeterminates of the same kind as in Article 347, namely $F = \varphi(t, u, v \ldots)$, the indeterminates t, u, v, etc., are replaced respectively by the sums $(\gamma, \lambda), (\gamma, \lambda'), (\gamma, \lambda'')$, etc., and its value is reduced by the rules of Article 345, IV, to*

$$\begin{aligned} A + a(\gamma, 1) + a'(\gamma, g) \ldots + a^{\zeta}(\gamma, g^{\alpha\beta-\alpha}) \\ \ldots + a^{\theta}(\gamma, g^{\alpha\beta-1}) = W \end{aligned}$$

Then I say that, if F is a symmetric function, the periods in W that are contained in the same period of $\beta\gamma$ terms, that is, generally such periods as (γ, g^{μ}) and $(\gamma, g^{\alpha\nu+\mu})$, where ν denotes any integer, will have the same coefficients.

Proof. Since the period $(\beta\gamma, \lambda g^{\alpha})$ is identical with $(\beta\gamma, \lambda)$, the smaller periods $(\gamma, \lambda g^{\alpha}), (\gamma, \lambda' g^{\alpha}), (\gamma, \lambda'' g^{\alpha})$, etc., of which the former clearly consists, must agree with those of which the latter consists, although in a different order. Thus, if we suppose that, on substituting these respectively for t, u, v, etc., F becomes W', W'

will coincide with W. But by Article 347 we have

$$\begin{aligned} W' &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \\ &\qquad \ldots + a^{\zeta}(\gamma, g^{\alpha\beta}) \ldots + a^{\theta}(\gamma, g^{\alpha\beta+\alpha-1}) \\ &= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \\ &\qquad \ldots + a^{\zeta}(\gamma, 1) \ldots + a^{\theta}(\gamma, g^{\alpha-1}) \end{aligned}$$

Therefore, since this expression must agree with W, the first, second, third, etc., coefficients in W (starting with a) must agree, respectively, with those in positions $\alpha+1, \alpha+2, \alpha+3$, etc. It follows readily that, in general, the coefficients of the periods $(\gamma, g^{\mu}), (\gamma, g^{\alpha+\mu}), (\gamma, g^{2\alpha+\mu}) \ldots (\gamma, g^{\nu\alpha+\mu})$, which occupy positions $\mu + 1, \alpha + \mu + 1$, $2\alpha + \mu + 1 \ldots \nu\alpha + \mu + 1$, must agree with one another. *Q. E. D.*

It is therefore clear that W can be reduced to the form

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1})$$

where all the coefficients A, a, etc., will be integers if all the fixed coefficients in F are integers. It is further easily seen that, if we then substitute for the indeterminates in F the β periods of γ terms contained in another period of $\beta\gamma$ terms, namely $(\beta\gamma, \lambda k)$, which are clearly $(\gamma, \lambda k), (\gamma, \lambda' k), (\gamma, \lambda'' k)$, etc., the resulting value will be $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \ldots + a^{\varepsilon}(\beta\gamma, g^{\alpha-1}k)$.

It is also clear that the theorem extends to the case where $\alpha = 1$, or $\beta\gamma = n - 1$: here *all* the coefficients in W will be equal, so that W reduces to the form $A + a(\beta\gamma, 1)$.

351.

Keeping all the notation of the preceding article, it is clear that each coefficient of the equation whose roots are the β sums $(\gamma,\lambda),(\gamma,\lambda'),(\gamma,\lambda'')$, etc., can be reduced to a form such as

$$A+a(\beta\gamma,1)+a'(\beta\gamma,g)\ldots+a^{\varepsilon}(\beta\gamma,g^{\alpha-1})$$

and that the numbers A,a, etc., are all integers. The equation whose roots are the β periods of γ terms contained in another period $(\beta\gamma,k\lambda)$ is derived from it by replacing every period $(\beta\gamma,\mu)$ throughout the coefficients by $(\beta\gamma,k\mu)$. Thus, if $\alpha=1$, all the β periods of γ terms will be determined by an equation of degree β, each of whose coefficients reduces to the form $A+a(\beta\gamma,1)$, *and is therefore a known quantity*, since $(\beta\gamma,1)=(n-1,1)=-1$. If, however, $\alpha>1$, the coefficients of the equation whose roots are all the periods of γ terms contained in any given period of $\beta\gamma$ terms will be known quantities as soon as the numerical values of all the α periods of $\beta\gamma$ terms are known. — The coefficients of these equations can often be calculated more conveniently, especially when β is not very small, by first finding the sums of powers of the roots and then deducing the coefficients from them by Newton's theorem, just as above in Article 349.

Example I. For $n=19$, we seek the equation whose roots are the sums $(6,1),(6,2),(6,4)$. Denoting these roots respectively by p,p',p'', and the required equation by

$$x^3-Axx+Bx-C=0$$

we obtain

$$A=p+p'+p'',\quad B=pp'+pp''+p'p'',\quad C=pp'p''$$

Hence

$$A=(18,1)=-1$$

Further, we have

$$pp'=p+2p'+3p'',\quad pp''=2p+3p'+p'',$$
$$p'p''=3p+p'+2p''$$

whence

$$B=6(p+p'+p'')=6(18,1)=-6$$

Finally,

$$C=(p+2p'+3p'')p''=3(6,0)+11(p+p'+p'')$$
$$=18-11=7$$

so the required equation is

$$x^3+xx-6x-7=0$$

Using the other method, we have

$$p+p'+p''=-1$$

$$pp = 6 + 2p + p' + 2p'', \quad p'p' = 6 + 2p' + p'' + 2p,$$
$$p''p'' = 6 + 2p'' + p + 2p'$$

whence

$$pp + p'p' + p''p'' = 18 + 5(p + p' + p'') = 13$$

and similarly

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2$$

From these, Newton's theorem gives the same equation as before.

II. For $n = 19$, we seek the equation whose roots are the sums $(2,1), (2,7), (2,8)$. Denoting these respectively by q, q', q'', we find

$$q + q' + q'' = (6,1),$$
$$qq' + qq'' + q'q'' = (6,1) + (6,4), \quad qq'q'' = 2 + (6,2)$$

Thus, keeping the notation of the preceding example, the required equation will be

$$x^3 - pxx + (p + p'')x - 2 - p' = 0$$

The equation whose roots are the sums $(2,2), (2,3), (2,5)$, contained in $(6,2)$, is deduced from the preceding one by replacing p, p', p'' respectively by p', p'', p. Applying the same substitution again gives the equation whose roots are the sums $(2,4), (2,6)$. $(2,9)$ contained in $(6,4)$.

The solution of the equation $X = 0$ is built on the preceding investigations.

352.

The preceding theorems, together with their attached corollaries, contain the main points of the whole theory, and the method for finding the values of the roots Ω can now be given briefly.

First choose a number g that is a primitive root modulo n, and find the least residues of the powers of g up to g^{n-2} modulo n. Resolve $n-1$ into factors, and into prime factors if we wish to reduce the problem to equations of the lowest possible degree. Let these, in an entirely arbitrary order, be $\alpha, \beta, \gamma \ldots \zeta$, and put

$$\frac{n-1}{\alpha} = \beta\gamma \ldots \zeta = a, \qquad \frac{n-1}{\alpha\beta} = \gamma \ldots \zeta = b, \quad \text{etc.}$$

Distribute all the roots Ω into α periods of a terms; each of these in turn into β periods of b terms; each of these again into γ periods, etc. By the preceding article, find the equation of degree α, (A), whose roots are those α sums of a terms; their values will therefore become known by solving this equation.

But a difficulty arises here, since it seems uncertain to which root of the equation (A) each sum is to be set equal, namely which root should be denoted by $(a,1)$, which by (a,g), etc. This can be resolved as follows. We may use $(a,1)$ to denote any root of equation (A); for each of its roots is a sum of a roots from Ω, and it is entirely arbitrary which root from Ω is denoted by [1]. We may therefore clearly assume that

one of the roots of which any given root of equation (A) consists is expressed by [1], so that this root of equation (A) becomes $(a, 1)$. The root [1], however, is not yet fully determined by this: it remains entirely arbitrary or undetermined which of the roots constituting $(a, 1)$ we wish to take for [1]. But as soon as $(a, 1)$ is determined, all the other sums of a terms can also be deduced rationally from it (Article 346). This also shows that only a single root need be found by solving the equation. — The following, less direct method can also be used for this purpose. Take a definite root for [1], *that is*, put $[1] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, choosing the integer k at will, provided it is not divisible by n. Then [2], [3], etc., will also indicate definite roots, and therefore the sums $(a, 1)$, (a, g), etc., will denote definite quantities. Once these have been calculated with a light hand from sine tables, namely with enough accuracy to decide which are greater and which smaller, no doubt can remain about the notation by which the individual roots of equation (A) are to be distinguished.

When all the α sums of a terms have been found in this way, find, by the preceding article, the equation (B) of degree β, whose roots are the β sums of b terms contained in $(a, 1)$; all the coefficients of this equation will be known quantities. Since it is still arbitrary which of the $a = \beta b$ roots contained in $(a, 1)$ is denoted by [1], any given root of equation (B) can be expressed by $(b, 1)$, for we may clearly assume that one of the b roots composing it is denoted by [1]. Thus find any one root of equation (B) by solving it, set it $= (b, 1)$, and from it derive, by Article 346, all the other sums of b terms. This also gives us a check on the calculation, since those sums of b terms that belong to the same periods of a terms must always yield known sums. — In some cases it may be just as convenient to find $\alpha - 1$ other equations of degree β, whose roots are respectively the individual β sums of b terms contained in the remaining periods of a terms, $(a, g), (a, gg)$, etc., and to find *all* the roots both of these equations and of equation B by solving them. We must then decide, as above with the help of a sine table, to which periods of b terms the individual roots obtained in this way are to be set equal. Various other devices can also be used to make this decision, which cannot be fully explained here; one, however, for the case $\beta = 2$, is particularly useful and can be explained more briefly by examples than by rules, and will be found in the following examples.

After the values of all the $\alpha\beta$ sums of b terms have been found in this way, equations of degree γ can in exactly the same way determine from them all the $\alpha\beta\gamma$ sums of c terms. Namely, we must find *either one* equation of degree γ, whose roots are the γ sums of c terms contained in $(b, 1)$, by Article 350; obtain any one root by solving it, set it $= (c, 1)$, and finally deduce from it, by Article 346, all the other similar sums; *or* we must develop in the same way a total of $\alpha\beta$ equations of degree γ, whose roots are respectively the γ sums of c terms contained in the individual periods of b terms, extract the values of all the roots of all these equations by solving them, and finally determine their order as above with the help of a sine table, or, for $\gamma = 2$, by the device to be shown below in the examples.

Continuing in this way, we will clearly at last obtain all the $\frac{n-1}{\zeta}$ sums of ζ terms. Thus, if we develop by Article 348 the equation of degree ζ whose roots are the ζ roots from Ω contained in $(\zeta, 1)$, all its coefficients will be known quantities. If any one of its roots is obtained by solving it, we may set it $= [1]$, and all the other roots

Ω will be obtained from its powers. If preferred, all the roots of that equation can also be found by solving it, and, in addition, by solving $\frac{n-1}{\zeta} - 1$ other equations of degree ζ, which respectively give all the ζ roots contained in each of the remaining periods of ζ terms, all the other roots Ω can be found.

It is also clear that, as soon as the first equation (A) is solved, or as soon as the values of all the α sums of a terms are known, Article 348 immediately gives the resolution of the function X into α factors of degree a. Further, after solving equation (B), or after finding the values of all the $\alpha\beta$ sums of b terms, each of those factors is again resolved into β, or X into $\alpha\beta$ factors of degree b, etc.

353.

First example, for $n = 19$. Since here $n - 1 = 3.3.2$, finding the roots Ω is to be reduced to solving two cubic equations and one quadratic equation. This example will be easier to understand because most of the necessary operations are already contained in the preceding articles. Taking the number 2 for the primitive root g gives the following least residues of its powers (the exponents of the powers are written above the residues in the first row):

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

From this, Articles 344 and 345 easily give the following distribution of all the roots Ω into three periods of six terms, and of each of these into three periods of two terms:

$$\Omega = (18,1)\left\{\begin{array}{ll} (6,1)\left\{\begin{array}{ll} (2,1)\ldots & [1],[18] \\ 2,8)\ldots & [8],[11] \\ (2,7)\ldots & [7],[12] \end{array}\right. \\ (6,2)\left\{\begin{array}{ll} (2,2)\ldots & [2],[17] \\ (2,16)\ldots & [3],[16] \\ (2,14)\ldots & [5],[14] \end{array}\right. \\ (6,4)\left\{\begin{array}{ll} (2,4)\ldots & [4],[15] \\ (2,13)\ldots & [6],[13] \\ (2,9)\ldots & [9],[10] \end{array}\right. \end{array}\right.$$

The equation (A), whose roots are the sums $(6,1),(6,2),(6,4)$, is found to be $x^3 + xx - 6x - 7 = 0$, one of whose roots is found to be $-1{,}2218761623$. Denoting this by $(6,1)$, we obtain

$$(6,2) = 4 - (6,1)^2 = 2{,}5070186441$$
$$(6,4) = -5 - (6,1) + (6,1)^2 = -2.2851424818$$

Thus X will be resolved into three factors of degree 6 if these values are substituted in Article 348.

The equation (B), whose roots are the sums $(2,1),(2.7),(2,8)$, is found to be

$$x^3 - (6,1)xx + ((6,1) + (6,4))x - 2 - (6,2) = 0$$

or

$$x^3 + 1{,}2218761623xx - 3{,}5070186441x - 4{,}5070186441 = 0$$

One of its roots is found to be $-1{,}3545631433$, which we will denote by $(2,1)$. The method of Article 346 gives the following equations, in which, for brevity, q is written for $(2,1)$:

$$(2,2) = qq - 2, \quad (2,3) = q^3 - 3q,$$
$$(2,4) = q^4 - 4qq + 2, \quad (2,5) = q^5 - 5q^3 + 5q$$
$$(2,6) = q^6 - 6q^4 + 9qq - 2,$$
$$(2,7) = q^7 - 7q^5 + 14q^3 - 7q$$
$$(2,8) = q^8 - 8q^6 + 20q^4 - 16qq + 2,$$
$$(2,9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q$$

In the present case these equations can be developed more conveniently by the following considerations than by the rules of Article 346. If we suppose

$$[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$$

we have

$$\begin{aligned}[18] &= \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} \\ &= \cos\frac{kP}{19} - i\sin\frac{kP}{19},\end{aligned}$$

and therefore $(2,1) = 2\cos\frac{kP}{19}$, and also, in general,

$$[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19},$$

and therefore $(2,\lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$ Thus, if $\frac{1}{2}q = \cos\omega$, we will have $(2,2) = 2\cos 2\omega, (2,3) = 2\cos 3\omega$, etc. The known equations for the cosines of multiple angles then give the same formulas as above. — These formulas now give the following numerical values:

$(2,2) = -0{,}1651586909$	$(2,6) = 0{,}4909709743$
$(2,3) = 1{,}5782810188$	$(2,7) = -1{,}7589475024$
$(2,4) = -1{,}9727226068$	$(2,8) = 1{,}8916344834$
$(2,5) = 1{,}0938963162$	$(2,9) = -0{,}8033908493$

The values of $(2,7), (2,8)$ can also be found from equation (B), whose two remaining roots they are. The doubt as to which of these roots is $(2,7)$ and which is $(2,8)$ will be removed either by an approximate calculation using the preceding formulas or by sine tables. Even a cursory consultation of these shows that $(2,1) = 2\cos\omega$ when we put $\omega = \frac{7}{19}P$, whence we must have

$$(2,7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P,$$

and $(2,8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$ Similarly, the sums $(2,2), (2,3), (2,5)$ can also be found by means of the equation

$$x^3 - (6,2)xx + ((6,1) + (6,2))x - 2 - (6,4) = 0$$

whose roots they are; the uncertainty about which roots are to be set equal to the respective sums will be removed in exactly the same way as before. Likewise, the sums $(2,4), (2,6), (2,9)$ can also be found by the equation

$$x^3 - (6,4)xx + ((6,2) + (6,4))x - 2 - (6,1) = 0$$

Finally, [1] and [18] are the roots of the equation $xx - (2,1)x + 1 = 0$, one of which is $= \frac{1}{2}(2,1) + i\sqrt{(1 - \frac{1}{4}(2,1)^2)} = \frac{1}{2}(2,1) + i\sqrt{(\frac{1}{2} - \frac{1}{4}(2,2))}$, the other $= \frac{1}{2}(2,1) - i\sqrt{(\frac{1}{2} - \frac{1}{4}(2,2))}$, giving the numerical values $= -0{,}6772815716 \pm 0{,}7357239107i$. The

sixteen remaining roots can be deduced either by developing the powers of either of these roots or by solving eight other similar equations. In the latter method, we must decide, either by sine tables or by the device to be explained in the next example, for which root the imaginary part is to take the positive sign and for which the negative sign. The following values were found in this way, with the upper sign understood to correspond to the first root and the lower to the second:

$$\begin{aligned}
&[1] \text{ and } [18] = -0{,}6772815716 \pm 0{,}7357239107i \\
&[2] \text{ and } [17] = -0{,}0825793455 \mp 0{,}9965844930i \\
&[3] \text{ and } [16] = 0{,}7891405094 \pm 0{,}6142127127i \\
&[4] \text{ and } [15] = -0{,}9863613034 \pm 0{,}1645945903i \\
&[5] \text{ and } [14] = 0{,}5469481581 \mp 0{,}8371664783i \\
&[6] \text{ and } [13] = 0{,}2454854871 \pm 0{,}9694002659i \\
&[7] \text{ and } [12] = -0{,}8794737512 \mp 0{,}4759473930i \\
&[8] \text{ and } [11] = 0{,}9458172417 \mp 0{,}3246994692i \\
&[9] \text{ and } [10] = -0.4016954247 \pm 0{,}9157733267i
\end{aligned}$$

354.

Second example, for $n = 17$. Here we have $n - 1 = 2.2.2.2$, so the calculation of the roots Ω is to be reduced to four quadratic equations. Here we will take the number 3 for the primitive root; its powers give the following least residues modulo 17:

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

This gives the following distributions of the collection Ω into two periods of eight terms, four of four terms, and eight of two terms:

$$\Omega = (16,1)\begin{cases}(8,1)\begin{cases}(4,1)\begin{cases}(2,1)\ldots & [1],[16]\\(2,13)\ldots & [4],[13]\end{cases}\\(4,9)\begin{cases}(2,9)\ldots & [8],[9]\\(2,15)\ldots & [2],[15]\end{cases}\end{cases}\\(8,3)\begin{cases}(4,3)\begin{cases}(2,3)\ldots & [3],[14]\\(2,5)\ldots & [5],[12]\end{cases}\\(4.10)\begin{cases}(2,10)\ldots & [7],[10]\\(2,11)\ldots & [6],[11]\end{cases}\end{cases}\end{cases}$$

By the rules of Article 351, the equation (A), whose roots are the sums $(8,1), (8,3)$, is found to be $xx+x-4=0$. Its roots are calculated to be $-\frac{1}{2}+\frac{1}{2}\sqrt{17} = 1{,}5615528128$ and $-\frac{1}{2}-\frac{1}{2}\sqrt{17} = -2{,}5615528128$. We will set the first $= (8,1)$, so the second must necessarily be set $= (8,3)$.

Further, the equation whose roots are the sums $(4,1)$ and $(4,9)$ is found to be $(B) : xx-(8,1)x-1=0$. Its roots are $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{(4+(8,1)^2)} = \frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{(12+3(8,1)+4(8,3))}$. We will set the root in which the radical quantity takes the positive sign, and whose numerical value is 2,0494811777, $= (4,1)$; the other root, in which the radical quantity is taken negatively and whose value is $-0{,}4879283649$, must then be denoted by $(4,9)$. The remaining sums of four terms, namely $(4,3)$ and $(4,10)$,

can be found in two ways. *First*, by the method of Article 346, which gives the following formulas, in which, for brevity, we write for $(4,1)$ the letter p:

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0{,}3441507314$$
$$(4,10) = \frac{3}{2} + 2p - pp - \frac{1}{2}p^3 = -2{,}9057035442$$

The same method also gives the formula $(4,9) = -1-6p+pp+p^3$, which yields the same value as we gave before. *Second*, the sums $(4,3)$, $(4,10)$ can also be determined by solving the equation whose roots they are. This equation is $xx - (8,3)x - 1 = 0$, whence its roots are $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{(4+(8,3)^2)}$, or $\frac{1}{2}(8,3)+\frac{1}{2}\sqrt{(12+4(8,1)+3(8,3))}$ and $\frac{1}{2}(8,3) - \frac{1}{2}\sqrt{(12+4(8,1)+3(8,3))}$. The doubt as to *which* root should be denoted by $(4,3)$ and which by $(4,10)$ will be removed by the following device, which we mentioned in Article 352. Develop the product of $(4,1)-(4,9)$ and $(4,3)-(4,10)$; the result will be found to be $2(8,1)-2(8,3)$ [*)] Now the value of this expression is clearly positive, namely $= +2\sqrt{17}$, and the first factor of the product, $(4,1)-(4,9)$, is also positive, namely $= +\sqrt{(12+3(8,1)+4(8,3))}$. Thus the other factor, $(4,3)-(4,10)$, must necessarily also be positive, and therefore $(4,3)$ must be set equal to the *first* root, in which the radical is preceded by the positive sign, and $(4,10)$ to the second. This gives the same numerical values as above.

Having found all the sums of four terms, we proceed to the sums of two terms. The equation (C), whose roots are $(2,1),(2,13)$, contained in $(4,1)$, is found to be $xx - (4,1)x + (4,3) = 0$. Its roots are $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(-4(4,3)+(4,1)^2)}$ or $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(4+(4,9)-2(4,3))}$. We set the one in which the radical quantity is taken positively, and whose value is found to be $= 1{,}8649444588$, $= (2,1)$; thus $(2,13)$ will be equal to the other, whose value is $= 0{,}1845367189$. If we wish to find the remaining sums of two terms by the method of Article 346, for $(2,2),(2,3),(2,4),(2,5),(2,6),(2,7),(2,8)$ we can use the same formulas that we gave in the preceding example for quantities bearing the same notation, namely $(2,2)$, (or $(2,15)$), $= (2,1)^2 - 2$, etc. If, however, we prefer to calculate them in pairs by solving a quadratic equation, for $(2,9),(2,15)$ we find the equation $xx - (4,9)x + (4,10) = 0$, whose roots are $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{(4+(4,1)-2(4,10))}$. How the choice of sign is to be determined here will be decided in the same way as above. Namely, developing the product of $(2,1)-(2,13)$ and $(2,9)-(2,15)$ gives $-(4,1)+(4,9)-(4,3)+(4,10)$. Since this is clearly negative, whereas the factor $(2,1)-(2,13)$ is positive, $(2,9)-(2,15)$ must necessarily be negative. Thus, in the expression given above, the upper, positive sign must be taken for $(2,15)$ and the lower, negative sign for $(2,9)$. From this we calculate $(2,9) = -1{,}9659461994$, $(2,15) = 1{,}4780178344$. — Likewise, since developing the product of $(2,1)-(2,13)$ and $(2,3)-(2,5)$ gives $(4,9)-(4,10)$, hence a positive quantity, we conclude that the factor $(2,3)-(2,5)$ is positive. A calculation similar

[*)] The true nature of this device consists in the fact that it could be foreseen a priori that the developed product would contain no sums of four terms, but could be expressed through sums of eight terms alone. Those familiar with the subject will very easily see the reason for this, which must be passed over here for brevity.

to the preceding one then gives

$$\begin{aligned}(2,3) &= \tfrac{1}{2}(4,3) + \tfrac{1}{2}\sqrt{(4+(4,10)-2(4,9))}\\ &= 0{,}8914767116\\ (2,5) &= \tfrac{1}{2}(4,3) - \tfrac{1}{2}\sqrt{(4+(4,10)-2(4,9))}\\ &= -0{,}5473259801\end{aligned}$$

Finally, entirely similar operations give

$$\begin{aligned}(2,10) &= \tfrac{1}{2}(4,10) - \tfrac{1}{2}\sqrt{(4+(4,3)-2(4,1))}\\ &= -1{,}7004342715\\ (2,11) &= \tfrac{1}{2}(4,10) + \tfrac{1}{2}\sqrt{(4+(4,3)-2(4,1))}\\ &= -1{,}2052692728\end{aligned}$$

It remains to descend to the roots Ω themselves. The equation (D), whose roots are [1] and [16], is $xx-(2,1)x+1=0$, whence the roots $\frac{1}{2}(2,1)\pm\frac{1}{2}\sqrt{((2,1)^2-4)}$, or rather $\frac{1}{2}(2,1)\pm i\sqrt{(4-(2,1)^2)}$, or $\frac{1}{2}(2,1)\pm\frac{1}{2}i\sqrt{(2-(2,15))}$. We take the upper sign for [1], the lower for [16]. The fourteen remaining roots will be obtained either through the powers of [1] or by solving seven quadratic equations, each of which gives a pair of roots; the uncertainty about the signs of the radical quantities can be removed by the same device as before. Thus [4] and [13] are the roots of the equation $xx-(2,13)x+1=0$, and therefore $\frac{1}{2}(2,13)\pm\frac{1}{2}i\sqrt{(2-(2,9))}$. Developing the product of $[1]-[16]$ and $[4]-[13]$, however, gives $(2,5)-(2,3)$, hence a negative real quantity. Since $[1]-[16]$ is $+i\sqrt{(2-(2,15))}$, that is, the product of the imaginary quantity i and a *positive* real quantity, $[4]-[13]$ must also be the product of i and a *positive* real quantity, because $ii=-1$. We conclude that the upper sign must be taken for [4] and the lower for [13]. Similarly, for the roots [8] and [9] we find $\frac{1}{2}(2,9)\pm\frac{1}{2}i\sqrt{(2-(2,1))}$. Since the product of $[1]-[16]$ and $[8]-[9]$ is $(2,9)-(2,10)$, hence negative, the upper sign must be taken for [8] and the lower for [9]. Calculating the remaining roots in the same way, we obtain the following numerical values, where the upper signs are understood to correspond to the first roots and the lower to the second:

$$\begin{aligned}[1],\ [16] \quad &\ldots \quad 0{,}9324722294 \pm 0{,}3612416662i\\ [2],\ [15] \quad &\ldots \quad 0{,}7390089172 \pm 0{,}6736956436i\\ [3],\ [14] \quad &\ldots \quad 0{,}4457383558 \pm 0{,}8951632914i\\ [4],\ [13] \quad &\ldots \quad 0{,}0922683595 \pm 0{,}9957341763i\\ [5],\ [12] \quad &\ldots \quad -0{,}2736629901 \pm 0{,}9618256432i\\ [6],\ [11] \quad &\ldots \quad -0{,}6026346364 \pm 0{,}7980172273i\\ [7],\ [10] \quad &\ldots \quad -0{,}8502171357 \pm 0{,}5264321629i\\ [8],\ [9] \quad &\ldots \quad -0{,}9829730997 \pm 0{,}1837495178i\end{aligned}$$

* *
*

What has been given above could indeed suffice for solving the equation $x^n - 1 = 0$, and therefore also for finding the trigonometric functions corresponding to arcs commensurable with the circumference. Yet, because of the importance of the subject, we cannot bring this investigation to an end without first adding here a few items from the wealth both of observations that shed light on it and of propositions related to it or dependent on it. We will chiefly choose those that can be completed without an extensive apparatus of other investigations, and we wish them to be regarded only as *samples* of this very extensive theory, which is to be treated at length in the future.

Further investigations on the periods of the roots.
Sums with an even number of terms are real quantities.

355.

Since n is always assumed to be odd, 2 is among the factors of $n-1$, and the collection Ω is formed from $\frac{1}{2}(n-1)$ periods of two terms. A period such as $(2,\lambda)$ will consist of the roots $[\lambda]$ and $[\lambda g^{\frac{1}{2}(n-1)}]$, where, as above, g denotes any primitive root modulo n. But we have $g^{\frac{1}{2}(n-1)} \equiv -1 \pmod{n}$, and therefore $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (see Article 62), whence $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$. Thus, if we suppose $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, and therefore $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, the sum is $(2,\lambda) = 2\cos\frac{kP}{n}$. From this we draw here only the conclusion that the value of any sum of two terms is a real quantity. Since any period whose number of terms is even $= 2a$ can be divided into a periods of two terms each, it is clear, more generally, that the value of any sum with an even number of terms is always a real quantity. Thus, if in Article 352 the factor two is reserved for the last place among the factors α, β, γ, etc., all operations, until sums of two terms are reached, will be carried out with real quantities. Imaginary quantities will be introduced only when you pass from these sums to the roots themselves.

On the equation that determines the distribution of the roots Ω into two periods.

356.

The auxiliary equations that determine, for each value of n, the sums constituting the collection Ω deserve the closest attention: they are connected in a remarkable way with the deepest properties of the number n. Here, however, we will restrict our investigation to the following two cases. *First*, we will discuss the quadratic equation whose roots are the sums of $\frac{1}{2}(n-1)$ terms; *second*, for the case where $n-1$ contains the factor 3, the cubic equation whose roots are the sums of $\frac{1}{3}(n-1)$ terms.

Writing, for brevity, m for $\frac{1}{2}(n-1)$, and denoting by g any primitive root modulo n, the collection Ω will consist of two periods $(m,1)$ and (m,g). The first will contain the roots $[1],[gg],[g^4]\ldots[g^{n-3}]$, the second $[g],[g^3],[g^5]\ldots[g^{n-2}]$. Suppose the least positive residues of the numbers $gg, g^4 \ldots g^{n-3}$ modulo n are, in any order, R, R', R'', etc., and likewise those of $g, g^3, g^5 \ldots g^{n-2}$ are N, N', N'', etc. Then the roots constituting $(m,1)$ will coincide with $[1],[R],[R'],[R'']$, etc., and the roots of the period (m,g) with $[N],[N'],[N'']$, etc. It is now clear that all the numbers $1, R, R', R''$, etc., are *quadratic residues* of the number n. Since they are all distinct and smaller than n, and their number is $= \frac{1}{2}(n-1)$, hence equal to the number of all the positive residues of n below n, these residues will coincide exactly with those numbers. It follows at once that all the numbers N, N', N'', etc., which are distinct both from one another and from $1, R, R'$, etc., and together with these exhaust all the numbers $1, 2, 3 \ldots n-1$, must coincide with all the positive *quadratic nonresidues* of n below n. If we now suppose that the equation whose roots are the sums $(m,1)$, (m,g) is

$$xx - Ax + B = 0$$

then

$$A = (m,1) + (m,g) = -1, \quad B = (m,1) \times (m,g)$$

By Article 345, the product of $(m,1)$ and (m,g) is

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{etc.} = W$$

and can therefore be reduced to a form such as $\alpha(m,0) + \beta(m,1) + \gamma(m,g)$. To determine the coefficients α, β, γ, we observe, *first*, that $\alpha + \beta + \gamma = m$ (since the number of sums in W is $= m$); *second*, that $\beta = \gamma$ (this follows from Article 350, since the product $(m,1) \times (m,g)$ is a symmetric function of the sums $(m,1), (m,g)$, of which the larger sum $(n-1,1)$ is composed); *third*, since all the numbers $N+1$, $N'+1, N''+1$, etc., lie strictly between the limits 2 and $n+1$, it is clear that either no sum in W reduces to $(m,0)$, and therefore $\alpha = 0$, when among the numbers N, N', N'', etc., $n-1$ does not occur; or one does, namely (m,n), and hence $\alpha = 1$, when $n-1$ is found among the numbers N, N', N'', etc. We conclude that in the first case $\alpha = 0,\ \beta = \gamma = \frac{1}{2}m$, in the second $\alpha = 1,\ \beta = \gamma = \frac{1}{2}(m-1)$. At the same time it follows, since the numbers β and γ must necessarily be integers, that the first case occurs, that is, $n-1$ (or, equivalently, -1) is not found among the nonresidues of n, when m is even, or equivalently n is of the form $4k+1$; the second case occurs, that is, $n-1$ or -1 is found among the nonresidues of n, whenever m is odd, or equivalently n is of the form $4k+3$[*)]. Thus the required product, since $(m,0) = m$, $(m,1) + (m,g) = -1$, is in the first case $= -\frac{1}{2}m$, in the second $= \frac{1}{2}(m+1)$. The required equation is therefore, in the former case, $xx + x - \frac{1}{4}(n-1) = 0$, whose roots are $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$; in the latter, $xx + x + \frac{1}{4}(n+1) = 0$, whose roots are $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$.

Thus, whichever root from Ω is taken for [1], the difference between the sums $\Sigma[\mathfrak{R}]$ and $\Sigma[\mathfrak{N}]$, where for $\mathfrak{R}$ we substitute all the positive quadratic residues and for $\mathfrak{N}$ all the positive quadratic nonresidues of n below n, will be $= \pm\sqrt{n}$ for $n \equiv 1$, and $= \pm i\sqrt{n}$ for $n \equiv 3 \pmod 4$. It also follows easily that, if k denotes any integer not divisible by n, we have

$$\Sigma \cos \frac{k\mathfrak{R}P}{n} - \Sigma \cos \frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{and}$$
$$\Sigma \sin \frac{k\mathfrak{R}P}{n} - \Sigma \sin \frac{k\mathfrak{N}P}{n} = 0$$

for $n \equiv 1 \pmod 4$; on the other hand, for $n \equiv 3 \pmod 4$ the former difference is $= 0$, the latter $= \pm\sqrt{n}$. These theorems are especially worth remembering for their elegance. We also observe that the upper signs always hold when for k we take unity or, more generally, a quadratic residue of n, and the lower signs when for k we take a nonresidue; also that these theorems can be extended to any composite values of n with their elegance preserved, or rather increased. But we must refrain from discussing these matters here, since they require a deeper investigation, and reserve their consideration for another occasion

[*)] In this way we have obtained a new proof of the theorem that -1 is a residue of all prime numbers of the form $4k+1$, and a nonresidue of all those of the form $4k+3$, which was already proved above (Articles 108, 109 and 262) in several different ways. If we prefer to assume this theorem, there is no need, in distinguishing the two different cases, to take account of the condition that β, γ are already integers in themselves.

Proof of the theorem mentioned in Section IV.

357.

Let the equation of degree m, whose roots are the m roots contained in the period $(m, 1)$, be

$$x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$$

or $z = 0$. Then $a = (m, 1)$, and each of the remaining coefficients b, etc., is contained in a form such as $\mathfrak{A}+\mathfrak{B}(m, 1)+\mathfrak{C}(m, g)$, with $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ integers (Article 348). Denoting by z' the function into which z passes when $(m, 1)$ is everywhere replaced by (m, g), and (m, g) by (m, gg), or equivalently $(m, 1)$, the roots of the equation $z' = 0$ will be the roots contained in (m, g), and the product is

$$zz' = \frac{x^n - 1}{x - 1} = X$$

Thus z can be reduced to a form such as $R+S(m, 1)+T(m, g)$, where R, S, T will be polynomials in x, all of whose coefficients will also be integers. This gives

$$z' = R + S(m, g) + T(m, 1)$$

From this, writing for brevity p and q for $(m, 1)$ and (m, g), respectively, we obtain

$$\begin{aligned} 2z &= 2R + (S + T)(p + q) - (T - S)(p - q) \\ &= 2R - S - T - (T - S)(p - q) \end{aligned}$$

and similarly

$$2z' = 2R - S - T + (T - S)(p - q)$$

Thus, putting

$$2R - S - T = Y, \quad T - S = Z$$

we have $4X = YY - (p - q)^2 ZZ$, and therefore, since $(p - q)^2 = \pm n$,

$$4X = YY \mp nZZ$$

The upper sign holds when n is of the form $4k + 1$, the lower when n is of the form $4k + 3$. This is the theorem whose proof we promised above (Article 124). It will easily be seen that the two highest terms of the function Y are always $2x^m + x^{m-1}$, and the highest term of the function Z is x^{m-1}. The remaining coefficients, which will clearly all be integers, vary with the different nature of the number n and cannot be given by a general analytic formula.

Example. For $n = 17$, the rules of Article 348 give the equation whose roots are the eight roots contained in $(8, 1)$ as

$$\begin{aligned} x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 \\ - (4p + 3q)x^3 + (4 + p + 2q)xx - px + 1 = 0 \end{aligned}$$

whence

$$R = x^8 + 4x^6 + 6x^4 + 4xx + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$$

and hence

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5xx + x + 2$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + xx + x$$

Here are a few more examples:

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	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5xx - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + xx + x$

On the equation for the distribution of the roots Ω into three periods.

358.

We proceed to consider the cubic equations that, when n is of the form $3k + 1$, determine the three sums of $\frac{1}{3}(n-1)$ terms constituting the collection Ω. Let g be any primitive root modulo n, and put $\frac{1}{3}(n-1) = m$; the value thus defined will be an even integer. Then the three sums constituting Ω will be $(m,1),(m,g),(m,gg)$, for which we will write p, p', p'', respectively. Clearly, the first contains the roots $[1],[g^3],[g^6]\ldots[g^{n-4}]$, the second $[g],[g^4]\ldots[g^{n-3}]$, and the third $[gg],[g^5]\ldots[g^{n-2}]$. Supposing the required equation to be

$$x^3 - Axx + Bx - C = 0$$

we have

$$A = p + p' + p'', \quad B = pp' + p'p'' + pp'', \quad C = pp'p''$$

whence we immediately obtain $A = -1$. Let the least positive residues of the numbers g^3, $g^6 \ldots g^{n-4}$ modulo n be, in any order, $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., and let $\mathfrak{K}$ be their collection with the number 1 added. Similarly, let $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$, etc., be the least residues of the numbers $g, g^4, g^7 \ldots g^{n-3}$, and $\mathfrak{K}'$ their collection; finally, let $\mathfrak{A}'', \mathfrak{B}'', \mathfrak{C}''$, etc., be the least residues of $gg, g^5, g^8 \ldots g^{n-2}$, and $\mathfrak{K}''$ their collection. Thus all the numbers in $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ will be distinct and will coincide with $1, 2, 3 \ldots n-1$. Above all, we must observe here that the number $n-1$ necessarily occurs in $\mathfrak{K}$, since it is easily seen to

be the residue of $g^{\frac{3m}{2}}$. It also follows easily that two numbers such as $h, n-h$ always occur in the *same* one of the three collections $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$. For if one is the residue of the power g^{λ}, the other will be the residue of the power $g^{\lambda+\frac{3m}{2}}$, or of $g^{\lambda-\frac{3m}{2}}$ if $\lambda > \frac{3m}{2}$. Let $(\mathfrak{K}\mathfrak{K})$ denote the count of numbers in the sequence $1, 2, 3 \ldots n-1$ that, together with the numbers immediately following them, greater by one, are contained in $\mathfrak{K}$. Similarly, let $(\mathfrak{K}\mathfrak{K}')$ be the count of numbers in the same sequence that are themselves contained in $\mathfrak{K}$, while their immediate successors are contained in $\mathfrak{K}'$. The meaning of the symbols $(\mathfrak{K}\mathfrak{K}''), (\mathfrak{K}'\mathfrak{K}), (\mathfrak{K}'\mathfrak{K}'), (\mathfrak{K}'\mathfrak{K}''), (\mathfrak{K}''\mathfrak{K}), (\mathfrak{K}''\mathfrak{K}'), (\mathfrak{K}''\mathfrak{K}'')$ will then also be clear at once. I now claim, *first*, that $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$. Suppose h, h', h'', etc., are all the numbers of the sequence $1, 2, 3 \ldots n-1$ that are themselves in $\mathfrak{K}$, while the next greater numbers $h+1, h'+1, h''+1$, etc., are in $\mathfrak{K}'$, and whose number is therefore $= (\mathfrak{K}\mathfrak{K}')$. It is clear that all the numbers $n-h-1$, $n-h'-1, n-h''-1$, etc., are contained in $\mathfrak{K}'$, while the next greater numbers $n-h, n-h'$, etc., are in $\mathfrak{K}$. Since there are altogether $(\mathfrak{K}'\mathfrak{K})$ such numbers, we certainly cannot have $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$. In the same way it is proved that we cannot have $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$, so these numbers must necessarily be equal. Exactly the same reasoning proves $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. Second, since every number of $\mathfrak{K}$, except the largest, $n-1$, must have an immediate successor contained either in $\mathfrak{K}$, in $\mathfrak{K}'$, or in $\mathfrak{K}''$, the sum $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ will equal the count of all the numbers in $\mathfrak{K}$ diminished by one, namely $= m-1$. For a similar reason we will have

$$(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'')$$
$$= (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m$$

With these preparations, we expand, by the rules of Article 345, the product pp' into $(m, \mathfrak{A}'+1) + (m, \mathfrak{B}'+1) + (m, \mathfrak{C}'+1) + \text{etc.}$. This expression is easily seen to reduce to $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$. Since, by Article 345 I, the product $p'p''$ arises from it by replacing $(m,1), (m,g), (m,gg)$ respectively by $(m,g), (m,gg), (mg^3)$, that is, p, p', p'' respectively by p', p'', p, we obtain $p'p'' = (\mathfrak{K}'\mathfrak{K})p' + (\mathfrak{K}'\mathfrak{K}')p'' + (\mathfrak{K}'\mathfrak{K}'')p$, and in exactly the same way $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$. From this it follows immediately, *first*, that

$$B = m(p + p' + p'') = -m$$

second, since, in the same way as pp' was expanded before, pp'' also reduces to $(\mathfrak{K}''\mathfrak{K})p + (\mathfrak{K}''\mathfrak{K}')p' + (\mathfrak{K}''\mathfrak{K}'')p''$, and this expression must be identical with the preceding one, we necessarily have $(\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}'\mathfrak{K}')$ and $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K})$. Hence, putting

$$(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}') = a,$$
$$(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') = b,$$
$$(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') = c$$

we obtain $m-1 = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K}) + b + c$ and $a+b+c = m$, whence $(\mathfrak{K}\mathfrak{K}) = a-1$. Thus those nine unknown quantities have been reduced to three, a, b, c, or rather, because of the equation $a+b+c = m$, to two. Finally, it is clear that the square pp expands into $(m, 1+1) + (m, \mathfrak{A}+1) + (m, \mathfrak{B}+1) + (m, \mathfrak{C}+1) + \text{etc.}$. Among the parts of this expression there will be (m, n), which reduces to $(m, 0)$, or to m; the remaining parts are easily seen to reduce to $(\mathfrak{K}\mathfrak{K})p + (\mathfrak{K}\mathfrak{K}')p' + (\mathfrak{K}\mathfrak{K}'')p''$, whence we will have $pp = m + (a-1)p + bp' + cp''$.

In this way the preceding investigations have given us these four reductions.

$$\begin{aligned} pp &= m + (a-1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'' \end{aligned}$$

Between the three unknowns a, b, c there is the condition

$$a + b + c = m \quad \ldots\ldots\ldots\ldots \text{ (I)}$$

and it is also certain that they are integers. We deduce

$$\begin{aligned} C = p \times p'p'' &= app + bpp' + cpp'' \\ &= am + (aa + bb + cc - a)p \\ &\quad + (ab + bc + ac)p' + (ab + bc + ac)p'' \end{aligned}$$

But since $pp'p''$ is a symmetric function of the sums p, p', p'', the coefficients multiplying these in the preceding expression must necessarily be equal (Article 350). This gives the new equation

$$aa + bb + cc - a = ab + bc + ac \quad \ldots \text{ (II)}$$

and hence $C = am + (ab + bc + ac)(p + p' + p'')$, or, because of I and $p + p' + p'' = -1$,

$$C = aa - bc \quad \ldots\ldots \text{ (III)}$$

Now, although C here depends on three unknowns between which we have only two equations, these equations, together with the condition that a, b, c are integers, suffice to determine C completely. To show this, we write equation II as

$$\begin{aligned} 12a + 12b + 12c + 4 = {} & 36aa + 36bb + 36cc \\ & - 36ab - 36ac - 36bc \\ & - 24a + 12b + 12c + 4 \end{aligned}$$

By I, the left side is $= 12m + 4 = 4n$; the right side reduces to

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2$$

or, writing k for $2a - b - c$, to $(3k - 2)^2 + 27(b - c)^2$. It is thus clear that the number $4n$ (that is, in general, four times any prime of the form $3m + 1$) can be represented by the form $xx + 27yy$. This can indeed be deduced without difficulty from the general theory of binary forms, yet it is quite remarkable that such a decomposition is connected with the values of a, b, c. But the number $4n$ can always be decomposed in only one way into a square and 27 times a square, which we prove as follows[*]. If we suppose

$$4n = tt + 27uu = t't' + 27u'u'$$

[*] This proposition could be proved more directly from the principles of Section V.

we obtain, *first*,

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16nn$$

second,

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16nn$$

third,

$$(tu' + t'u)(tu' - t'u) = 4n(u'u' - uu)$$

From the third equation it follows that n, since it is a prime number, divides one of the numbers $tu' + t'u, tu' - t'u$; from the first and second it is clear that each of these numbers is smaller than n. Thus the one divisible by n must necessarily be $= 0$, and therefore also $u'u' - uu = 0$, whence $u'u' = uu$ and $t't' = tt$: the two decompositions do not differ. Thus, if we suppose the decomposition of $4n$ into a square and 27 times a square to be known (it can be found either by the direct method of Section V or by the indirect method given in Articles 323 and 324), namely if $4n = MM + 27NN$, the squares $(3k-2)^2, (b-c)^2$ will be determined, and we will now have obtained two equations in place of equation II. But it is easily seen that not only the square $(3k-2)^2$ but also the root $3k-2$ itself is fully determined. Since it must necessarily be either $= +M$ or $= -M$, the ambiguity is removed by the requirement that k be an integer. We therefore set $3k - 2 = +M$ or $= -M$, according as M is of the form $3z+1$ or $3z+2$[†]. Now, since $k = 2a - b - c = 3a - m$, we have $a = \frac{1}{3}(m+k)$, $b + c = m - a = \frac{1}{3}(2m - k)$, whence

$$\begin{aligned} C = aa - bc &= aa - \tfrac{1}{4}(b+c)^2 + \tfrac{1}{4}(b-c)^2 \\ &= \tfrac{1}{9}(m+k)^2 - \tfrac{1}{36}(2m-k)^2 + \tfrac{1}{4}NN \\ &= \tfrac{1}{12}kk + \tfrac{1}{3}km + \tfrac{1}{4}NN \end{aligned}$$

and so all the coefficients of the required equation have been found. *Q.E.F.* — This formula becomes still simpler if for NN we substitute its value from the equation $(3k-2)^2 + 27NN = 4n = 12m + 4$, which gives, after calculation,

$$C = \tfrac{1}{9}(m + k + 3km) = \tfrac{1}{9}(m + kn)$$

The same value can also be reduced to $(3k-2)NN + k^3 - 2kk + k - km + m$. Though less suitable for use, this expression immediately shows that C certainly is an integer, as it should be.

Example. For $n = 19$, we have $4n = 49 + 27$, whence $3k - 2 = +7, k = 3$, $C = \frac{1}{9}(6 + 57) = 7$, and the required equation is $x^3 + xx - 6x - 7 = 0$, as above (Article 351). — Similarly, for $n = 7, 13, 31, 37, 43, 61, 67$ the value of k is found to be, respectively, $1, -1, 2, -3, -2, 1, -1$, whence $C = 1, -1, 8, -11, -8, 9, -5$.

[†] Clearly, M cannot be of the form $3z$, since otherwise $4n$ would be divisible by 3. — We need not consider here the ambiguity as to whether $b - c$ should be set $= N$ or $= -N$. Nor can it, by the nature of the matter, be removed in any way, since it depends on the choice of the primitive root g: for some primitive roots the difference $b - c$ is positive, for others negative.

Although the problem solved in this article is rather intricate, we did not wish to suppress it, both because of the elegance of its solution and because it gave occasion to use various devices that can also be applied with great benefit to other questions[*)].

[*)]Corollary. Let ε be a root of the equation $x^3 - 1 = 0$, and you will have $(p + \varepsilon p' + \varepsilon\varepsilon p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$. Put $\frac{M}{\sqrt{4n}} = \cos\varphi, \quad \frac{N\sqrt{27}}{\sqrt{4n}} = \sin\varphi$; then

$$p = -\tfrac{1}{3} + \tfrac{2}{3}\cos\tfrac{1}{3}\varphi\sqrt{n};$$
$$M \equiv +1 \pmod 3; \quad 1 \equiv M(1.2.3\ldots m)^3 \pmod n$$

Putting $3x + 1 = y$, the equation becomes $y^3 - 3ny - Mn = 0$.

Reducing the equations used to find the roots Ω to pure power equations.

359.

The preceding investigations concerned the *finding* of auxiliary equations; we will now explain a particularly remarkable property concerning their *solution*. As is well known, all the efforts of the greatest geometers to find the general solution of equations beyond the fourth degree, or (to define more precisely what I am seeking) THE REDUCTION OF MIXED EQUATIONS TO PURE POWER EQUATIONS, have so far always been fruitless, and scarcely any doubt remains that this problem proposes something impossible rather than something beyond the powers of present-day analysis. (Compare our remarks on this subject in *Demonstr. nova etc. art. 9.*) Nevertheless, it is certain that there are countless mixed equations of every degree that admit such a reduction to pure power equations, and we hope that geometers will welcome our showing that our auxiliary equations always belong to this class. But because of the great extent of this investigation, we give here only the principal points needed to show the possibility, and defer to another time the fuller treatment that this subject so richly deserves. We must first make some general observations about the roots of the equation $x^e - 1 = 0$, including the case where e is composite.

I. These roots are represented (as is known from elementary books) by $\cos\frac{kP}{e} + i\sin\frac{kP}{e}$, where k is to take the e numbers $0, 1, 2, 3 \ldots e-1$, or any others congruent to these modulo e. One root, for $k = 0$, or generally for k divisible by e, becomes $= 1$; every other value of k corresponds to a root different from 1.

II. Since $(\cos\frac{kP}{e} + i\sin\frac{kP}{e})^\lambda = \cos\frac{\lambda kP}{e} + i\sin\frac{\lambda kP}{e}$, it is clear that if R is a root corresponding to a value of k coprime to e, in the progression R, RR, R^3, etc., the term in position e is indeed $= 1$, but all the preceding terms differ from 1. It follows at once that all e quantities $1, R, RR, R^3 \ldots R^{e-1}$ are unequal, and since they evidently all satisfy the equation $x^e - 1 = 0$, they represent all its roots.

III. Finally, under the same assumption, we have

$$1 + R^\lambda + R^{2\lambda} \ldots + R^{\lambda(e-1)} = 0$$

for every integer value of λ not divisible by e; for the sum is $= \frac{1-R^{\lambda e}}{1-R^\lambda}$, and the numerator of this fraction becomes $= 0$, whereas its denominator does not become $= 0$. When, however, λ is divisible by e, that sum evidently becomes $= e$.

360.

Let, as throughout the preceding discussion, n be a prime, g a primitive root modulo n, and $n-1$ the product of three positive integers α, β, γ. For brevity we will immediately set up the investigation so that it also includes the cases where α is one or $\gamma = 1$; when $\gamma = 1$, the sums $(\gamma, 1), (\gamma, g)$, etc., must be replaced by the roots $[1], [g]$, etc. We therefore suppose that from all the α known sums of $\beta\gamma$ terms $(\beta\gamma, 1), (\beta\gamma, g), (\beta\gamma, gg) \ldots (\beta\gamma, g^{\alpha-1})$ we are to derive the sums of γ terms. We previously reduced this task to a mixed equation of degree β; we will now show how to accomplish it by a pure power equation of the same degree. For brevity, we will write, for the sums

$$(\gamma, 1), (\gamma, g^\alpha), (\gamma, g^{2\alpha}) \ldots (\gamma, g^{\alpha\beta-\alpha})$$

contained in $(\beta\gamma, 1)$, $a, b, c \ldots m$ respectively; for the sums

$$(\gamma, g), (\gamma, g^{\alpha+1}) \ldots (\gamma, g^{\alpha\beta-\alpha+1})$$

contained in $(\beta\gamma, g)$, $a', b' \ldots m'$ respectively; for the sums

$$(\gamma, gg), (\gamma, g^{\alpha+2}) \ldots (\gamma, g^{\alpha\beta-\alpha+2})$$

we write $a'', b'' \ldots m''$ respectively; and so on as far as those contained in $(\beta\gamma, g^{\alpha-1})$.

I. Now let R denote an unspecified root of the equation $x^\beta - 1 = 0$, and suppose that expanding the power with exponent β of the function

$$t = a + Rb + RRc \ldots + R^{\beta-1}m$$

according to the rules of Article 345 gives

$$\begin{aligned} &N + Aa + Bb + Cc \ldots + Mm \\ &+ A'a' + B'b' + C'c' \ldots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ &+ \text{etc.} = T \end{aligned}$$

where all the coefficients N, A, B, A', etc., will be polynomials in R. Suppose also that the powers with exponent β of two other functions

$$\begin{aligned} u &= R^\beta a + Rb + RRc \ldots + R^{\beta-1}m, \\ u' &= b + Rc + RRd \ldots + R^{\beta-2}m + R^{\beta-1}a \end{aligned}$$

expand into U and U' respectively. It is easy to see from Article 350 that, since u' arises from t by interchanging the sums $a, b, c \ldots m$ with $b, c, d \ldots a$ respectively, we will have

$$\begin{aligned} U' &= N + Ab + Bc + Cd \ldots + Ma \\ &+ A'b' + B'c' + C'd' \ldots + M'a' \\ &+ A''b'' + B''c'' + C''d'' \ldots + M''a'' \\ &+ \text{etc.} \end{aligned}$$

Further, since $u = Ru'$, we clearly have $U = R^\beta U'$, so that, because $R^\beta = 1$, the corresponding coefficients in U and U' are equal. Finally, since t and u differ only in that a is multiplied by unity in t and in u by R^β, it is easy to see that all corresponding coefficients (that is, those multiplying the same sums) in T and U are equal, and therefore so are all corresponding coefficients in T and U'. Hence we finally conclude that $A = B = C$, etc., $= M$; $A' = B' = C'$, etc., $A'' = B'' = C''$, etc., etc. Thus T reduces to a form such as

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, gg) \text{ etc.}$$

where each coefficient N, A, A', etc., may be reduced to a form such as

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{etc.}$$

in which p, p', p'', etc., are given integers.

II. If for R we take a definite root of the equation $x^\beta - 1 = 0$ (whose solution we suppose already known), and specifically a root of which no power lower than the one with exponent β equals unity, then T too will be a definite quantity, from which t may be derived by the pure power equation $t^\beta - T = 0$. But since this equation has β roots, namely $t, Rt, RRt \dots R^{\beta-1}t$, it may seem doubtful which root we ought to adopt. That the choice is entirely arbitrary will, however, become clear as follows. We must remember that, after all the sums of $\beta\gamma$ terms have been determined, the root [1] is determined only to the extent that some one of the $\beta\gamma$ roots contained in $(\beta\gamma, 1)$ must be denoted by this symbol; and therefore it is entirely arbitrary which of the β sums making up $(\beta\gamma, 1)$ we choose to denote by a. Now suppose that, with some definite sum denoted by a, we obtain $t = \mathfrak{T}$. It is easy to see that if we subsequently wish the sum just denoted by b to be denoted by a, those previously denoted by c, $d \dots a, b$ now become $b, c \dots m, a$, and the value of t now becomes $= \frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\beta-1}$. Similarly, if we choose to denote by a the sum originally denoted by c, the value of t will become $\mathfrak{T}R^{\beta-2}$, and so on: t can be regarded as equal to any of the quantities $\mathfrak{T}, \mathfrak{T}R^{\beta-1}, \mathfrak{T}R^{\beta-2}$, etc., that is to any root of the equation $x^\beta - T = 0$, according as we suppose one or another of the sums contained in $(\beta\gamma, 1)$ to be denoted by $(\gamma, 1)$. *Q. E. D.*

III. After the quantity t has been determined in this way, we must find $\beta - 1$ others that arise from t when, in its expression, R is successively replaced by RR, $R^3, R^4 \dots R^\beta$, namely

$$t' = a + RRb + R^4c \dots + R^{2\beta-2}m,$$
$$t'' = a + R^3b + R^6c \dots + R^{3\beta-3}m \text{ etc.}$$

The last is already known, since it evidently becomes $= a + b + c \dots + m = (\beta\gamma, 1)$; the others may be obtained as follows. If, according to the rules of Article 345 and in the same way as t^β earlier in I, we expand the product $t^{\beta-2}t'$, it will be proved by a method entirely analogous to the preceding one that the result can be reduced to a form such as

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, gg) \text{ etc.} = T'$$

in which $\mathfrak{N}, \mathfrak{A}, \mathfrak{A}'$, etc., are polynomials in R, so that T' is a known quantity, from which we will obtain $t' = \frac{T'tt}{T}$. In exactly the same way, if we suppose that expanding the product $t^{\beta-3}t''$ gives T'', this expression will have a similar form, and from its known value we will therefore derive t'' by the equation $t'' = \frac{T''t^3}{T}$; similarly, t''' will be found by an equation such as $t''' = \frac{T''''t^4}{T}$, in which T''' is a known quantity, and so on.

This method would not be applicable if $t = 0$ could occur, whence we would also have to have $T = T' = T''$, etc., $= 0$; but this can be proved impossible, although we must omit the proof here because of its length. — There are also special devices for converting the fractions $\frac{T'}{T}, \frac{T''}{T}$, etc., into *polynomials* in R, as well as shorter methods, in the case $\alpha = 1$, of obtaining the values of t', t'', etc. We must pass over all these here without discussion.

IV. Finally, as soon as t, t', t'', etc., have been found, observation III of the preceding article immediately gives $t + t' + t'' + \text{etc.} = \beta a$, so that the value of a will be known, from which the values of all the remaining sums of γ terms may be derived by Article 346. — The values of b, c, d, etc., can also be obtained from the following equations, whose reason will be readily apparent to any attentive reader:

$$\beta b = R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{etc.}$$
$$\beta c = R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{etc.}$$
$$\beta d = R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \text{etc. etc.}$$

Of the many observations relating to the preceding investigation, we touch on only one here. As regards the solution of the pure power equation $x^\beta - T = 0$, it is clear that T in most cases has an imaginary value $P + iQ$, so that this solution will, as is known, depend partly on dividing an angle (whose tangent $= \frac{Q}{P}$) and partly on dividing a ratio (unity to $\sqrt{(PP + QQ)}$) into β parts. It is very remarkable here (though we do not pursue this in greater detail) that the value of $\sqrt[\beta]{(PP + QQ)}$ can always be expressed *rationally* in terms of quantities already known, so that, apart from extracting a square root, *only* the division of an angle is required for the solution, e.g. for $\beta = 3$ only the trisection of an angle.

Finally, since nothing prevents our setting $\alpha = 1, \gamma = 1$ and therefore $\beta = n - 1$, it is evident that solving the equation $x^n - 1 = 0$ can at once be reduced to solving the pure power equation of degree $n - 1$, namely $x^{n-1} - T = 0$, where T will be determined by the roots of the equation $x^{n-1} - 1 = 0$. From this, with the help of the observation just made, it follows that dividing the whole circle into n parts requires 1° dividing the whole circle into $n - 1$ parts, 2° dividing another arc, which can be constructed after that division has been made, into $n - 1$ parts, 3° extracting a single square root; and it can indeed be shown that this is always $\sqrt{n}$.

Application of the preceding investigations to trigonometric functions. A method of identifying the angles corresponding to the individual roots Ω.

361.

It remains for us to examine more closely the connection between the roots Ω and the trigonometric functions of the angles $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$. The method we have given for finding the roots Ω still leaves uncertain (unless sine tables have been consulted during the work in the way described above, which would, however, be less direct) *which* roots correspond to *each* of these angles, that is which root is $= \cos\frac{P}{n} + i\sin\frac{P}{n}$, which is $= \cos\frac{2P}{n} + i\sin\frac{2P}{n}$, etc. This uncertainty is easily removed by considering that the cosines of the angles $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{2n}$ steadily decrease (provided their signs are also taken into account), while their sines are all positive; the angles $\frac{(n-1)P}{n}, \frac{(n-2)P}{n}, \frac{(n-3)P}{n} \ldots \frac{(n+1)P}{2n}$, on the other hand, have respectively the same cosines as those angles, but negative sines whose absolute magnitudes equal the sines of those angles. Thus the two roots among Ω with the greatest real parts (equal to one another) will correspond to the angles $\frac{P}{n}, \frac{(n-1)P}{n}$: to the former, the root in which the imaginary quantity i is multiplied by a positive quantity; to the latter, the root in which i is multiplied by a negative quantity. Of the $n-3$ remaining roots, those with the greatest real parts will again correspond to the angles $\frac{2P}{n}, \frac{(n-2)P}{n}$, and so on. — Once the root corresponding to the angle $\frac{P}{n}$ has been identified, those corresponding to the remaining angles can also be distinguished by the fact that, if the former is supposed to be $= [\lambda]$, the angles $\frac{2P}{n}, \frac{3P}{n}, \frac{4P}{n}$, etc., evidently correspond to the roots $[2\lambda], [3\lambda], [4\lambda]$, etc. Thus in the example of Article 353 one sees at once that the angle $\frac{1}{19}P$ can correspond to no root other than [11], and the angle $\frac{18}{19}P$ to the root [8]; similarly, the angles $\frac{2}{19}P, \frac{17}{19}P, \frac{3}{19}P, \frac{16}{19}P$, etc., correspond to the roots [3], [16], [14], [5], etc. In the example of Article 354, the angle $\frac{1}{17}P$ evidently corresponds to the root [1], the angle $\frac{2}{17}P$ to [2], etc. In this way, therefore, the cosines and sines of the angles $\frac{P}{n}, \frac{2P}{n}$, etc., will be fully determined.

Tangents, cotangents, secants and cosecants are derived from sines and cosines without division.

362.

As for the remaining trigonometric functions of these angles, they could easily be derived from the corresponding cosines and sines by the usual methods: namely, the secants and tangents by dividing unity and the sines by the cosines, and the cosecants and cotangents by dividing unity and the cosines by the sines. But the same result is usually obtained more conveniently with the help of the following formulas, without divisions, by additions alone. Let ω be any of the angles $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$, and let $\cos\omega + i\sin\omega = R$, so that R will be one of the roots Ω, and

$$\cos\omega = \tfrac{1}{2}(R + \tfrac{1}{R}) = \frac{1+RR}{2R},$$
$$\sin\omega = \tfrac{1}{2i}(R - \tfrac{1}{R}) = \frac{i(1-RR)}{2R}$$

Hence

$$\sec\omega = \frac{2R}{1+RR}. \quad \operatorname{tang}\omega = \frac{i(1-RR)}{1+RR},$$
$$\operatorname{cosec}\omega = \frac{2Ri}{RR-1}, \quad \operatorname{cotang}\omega = \frac{i(RR+1)}{RR-1}$$

We will now show how to transform the numerators of these four fractions so that they become divisible by their denominators.

I. Since $R = R^{n+1} = R^{2n+1}$, we have $2R = R + R^{2n+1}$, an expression evidently divisible by $1 + RR$, since n is odd. Hence

$$\sec\omega = R - R^3 + R^5 - R^7 \ldots + R^{2n-1}$$

and therefore (since $\sin\omega = -\sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega$, etc., evidently imply $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega$$

or finally (since $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$, etc.),

$$= 2(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega) \pm \cos n\omega$$

the upper or lower sign applying according as n has the form $4k+1$ or $4k+3$. This formula can evidently also be written as

$$\sec\omega = \pm(1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega)$$

II. Similarly, substituting $1 - R^{2n+2}$ for $1 - RR$ gives

$$\operatorname{tang}\omega = i(1 - RR + R^4 - R^6 \ldots - R^{2n})$$

or (since $1 - R^{2n} = 0$, $RR - R^{2n-2} = 2i\sin 2\omega$, $R^4 - R^{2n-4} = 2i\sin 4\omega$, etc.),

$$\operatorname{tang}\omega = 2(\sin 2\omega - \sin 4\omega + \sin 6\omega \ldots \mp \sin(n-1)\omega)$$

III. Since we have $1 + RR + R^4 \ldots + R^{2n-2} = 0$, it follows that

$$n = n - 1 - RR - R^4 \ldots R^{2n-2}$$
$$= (1-1) + (1-RR) + (1-R^4) \ldots + (1-R^{2n-2})$$

and each part of this sum is divisible by $1 - RR$. Hence

$$\begin{aligned}\frac{n}{1-RR} &= 1 + (1 + RR) + (1 + RR + R^4) \ldots \\ &\quad + (1 + RR + R^4 \ldots + R^{2n-4}) \\ &= (n-1) + (n-2)RR + (n-3)R^4 \ldots + R^{2n-4}\end{aligned}$$

so that, multiplying by 2, subtracting

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

and again multiplying by R, we obtain

$$\begin{aligned}\frac{2nR}{1-RR} &= (n-1)R + (n-3)R^3 + (n-5)R^5 \ldots \\ &\quad - (n-3)R^{2n-3} - (n-1)R^{2n-1}\end{aligned}$$

from which we immediately deduce

$$\begin{aligned}\operatorname{cosec}\omega &= \frac{1}{n}\big((n-1)\sin\omega + (n-3)\sin 3\omega \ldots \\ &\qquad - (n-1)\sin(2n-1)\omega\big) \\ &= \frac{2}{n}\big((n-1)\sin\omega + (n-3)\sin 3\omega \\ &\qquad + \text{etc.} + 2\sin(n-2)\omega\big)\end{aligned}$$

This formula can also be written as

$$\operatorname{cosec}\omega = -\frac{2}{n}(2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega)$$

IV. Multiplying the value of $\frac{n}{1-RR}$ given above by $1 + RR$ and subtracting

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

gives

$$\frac{n(1+RR)}{1-RR} = (n-2)RR + (n-4)R^4 + (n-6)R^6 \ldots - (n-2)R^{2n-2}$$

from which it immediately follows that

$$\begin{aligned}\operatorname{cotang}\omega &= \frac{1}{n}\big((n-2)\sin 2\omega + (n-4)\sin 4\omega \\ &\qquad + (n-6)\sin 6\omega \ldots - (n-2)\sin(n-2)\omega \\ &= \frac{2}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega \ldots \\ &\qquad + 3\sin(n-3)\omega + \sin(n-1)\omega)\end{aligned}$$

This formula may also be written in the following way:

$$\operatorname{cotang}\omega = -\frac{2}{n}(\sin\omega + 3\sin 3\omega \ldots + (n-2)\sin(n-2)\omega)$$

A method of successively reducing the degree of equations for trigonometric functions.

363.

Just as, on the assumption $n-1=ef$, the function X can be resolved into e factors of degree f as soon as the values of all the e sums of f terms are known (Article 348), so too, if we suppose $Z=0$ to be an equation of degree $n-1$ whose roots are the sines or any other trigonometric functions of the angles $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$, the function Z can then be resolved into e factors of degree f. The principal points of this procedure are as follows.

Let Ω consist of the e periods of f terms $(f,1)=P, P'.P''$, etc.; let the period P consist of the roots $[1],[a],[b],[c]$, etc.; P' of $[a'],[b'],[c']$, etc.; P'' of $[a''],[b''],[c'']$, etc., etc. Let the root $[1]$ correspond to the angle ω, and therefore the roots $[a],[b]$, etc., to the angles $a\omega, b\omega$, etc., the roots $[a'],[b']$, etc., to the angles $a'\omega, b'\omega$, etc., and the roots $[a'']$, $[b'']$, etc., to the angles $a''\omega, b''\omega$, etc., etc. It is easy to see that all these angles taken together agree with the angles $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$ as regards their trigonometric functions.*) If, therefore, the function in question is denoted by the symbol φ placed before the angle, and we set the product of the e factors

$$x-\varphi\omega, \quad x-\varphi a\omega, \quad x-\varphi b\omega \quad \text{etc.}$$

$=Y$, the product of $x-\varphi a'\omega, x-\varphi b'\omega$, etc., $=Y'$, and the product of $x-\varphi a''\omega$, $x-\varphi b''\omega$, etc., $=Y''$, and so on, we necessarily have the product $YY'Y''\ldots=Z$. It now remains to show that all the coefficients in the functions Y, Y', Y'', etc., can be reduced to a form such as

$$A+B(f,1)+C(f,g)+D(f,gg)\ldots+L(f,g^{e-1})$$

Once this is done, they must evidently all be regarded as known as soon as the values of all the sums of f terms are known. We will accomplish this as follows.

Just as $\cos\omega=\frac{1}{2}[1]+\frac{1}{2}[1]^{n-1}$, $\sin\omega=-\frac{1}{2}i[1]+\frac{1}{2}i[1]^{n-1}$, so too, by the preceding article, the remaining trigonometric functions of the angle ω can be reduced to a form such as $\mathfrak{A}+\mathfrak{B}[1]+\mathfrak{C}[1]^2+\mathfrak{D}[1]^3+$ etc.. It is readily seen that the function of the angle $k\omega$ then becomes $=\mathfrak{A}+\mathfrak{B}[k]+\mathfrak{C}[k]^2+\mathfrak{D}[k]^3+$ etc., where k denotes any integer. Now each coefficient in Y is a symmetric polynomial in $\varphi\omega, \varphi a\omega, \varphi b\omega$, etc. It is therefore clear that substituting the values of these quantities makes each coefficient a symmetric polynomial in $[1],[a],[b]$, etc.; hence, by Article 347, they reduce to the form $A+B(f,1)+C(f,g)+$ etc.. By exactly the same reasoning, all the coefficients in Y', Y'', etc., can also be reduced to a similar form. *Q. E. D.*

*)Two angles agree in this respect if their difference equals either the whole circumference or some multiple of it. We could call such angles *congruent modulo the circumference*, if we wished to understand congruence in a somewhat broader sense.

364.

We add some further observations on the problem of the preceding article.

I. Since each coefficient in Y' is a function of the roots contained in the period P' (which we may set $= (f, a')$) identical to the function of the roots in P given by the corresponding coefficient in Y, it is evident from Article 347 that Y' can be derived from Y by substituting everywhere in Y, for $(f,1),(f,g),(f,gg)$, etc., respectively, $(f,a'),(f,a'g),(f,a'gg)$, etc. Similarly, Y'' is derived from Y by substituting everywhere in Y, for $(f,1),(f,g),(f,gg)$, etc., respectively, $(f,a''),(f,a''g),(f,a''gg)$, etc., etc. Thus, as soon as the function Y has been expanded, the remaining functions Y', Y'', etc., follow from it without difficulty.

II. If we suppose

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{etc.}$$

the coefficients α, β, etc., will respectively be the sum of the roots of the equation $Y = 0$ that is the quantities $\varphi\omega, \varphi a\omega, \varphi b\omega$, etc., the sum of their products in pairs, and so on. But these coefficients will usually be obtained much more conveniently by a method similar to that given in Article 349: calculating the sum of the roots $\varphi\omega, \varphi a\omega$, $\varphi b\omega$, etc., the sum of their squares, cubes, etc., and deriving those coefficients from these by Newton's theorem. — Whenever φ denotes the tangent, secant, cotangent or cosecant, there are further shortcuts, which we pass over here without discussion.

III. The case where f is even deserves special consideration; each period P, P', P'', etc., is then composed of $\frac{1}{2}f$ periods of two terms. Let P consist of $(2,1),(2,\mathfrak{a}),(2,\mathfrak{b})$, $(2,\mathfrak{c})$, etc. The numbers $1, \mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, etc., and $n-1, n-\mathfrak{a}.n-\mathfrak{b}, n-\mathfrak{c}$, etc., taken together will then agree with $1, a, b, c$, etc., or at least (which here amounts to the same thing) be congruent to them modulo n. But we have $\varphi(n-1)\omega = \pm\varphi\omega,\ \varphi(n-\mathfrak{a})\omega = \pm\varphi\mathfrak{a}\omega$, etc., the upper signs applying whenever φ denotes the cosine or secant, and the lower signs when φ denotes the sine, tangent, cotangent or cosecant. It follows that in the first two cases the factors making up Y always occur in equal pairs, so that Y is a square, and specifically $Y = yy$ if y is set equal to the product of

$$x - \varphi\omega,\ x - \varphi\mathfrak{a}\omega,\ x - \varphi\mathfrak{b}\omega \text{ etc.}$$

Similarly, in the same cases the remaining functions Y', Y'', etc., will be squares. Specifically, if we suppose that P' consists of $(2,\mathfrak{a}'),(2,\mathfrak{b}'),(2,\mathfrak{c}')$, etc., P'' of $(2,\mathfrak{a}'')$, $(2,\mathfrak{b}''),(2,\mathfrak{c}'')$, etc., etc., and that the product of $x-\varphi\mathfrak{a}'\omega, x-\varphi\mathfrak{b}'\omega, x-\varphi\mathfrak{c}'\omega$, etc., is $= y'$, the product of $x-\varphi\mathfrak{a}''\omega, x-\varphi\mathfrak{b}''\omega$, etc., $= y''$, and so on, we will have $Y' = y'y'$, $Y'' = y''y''$, etc. The function Z will also be a square (compare Article 337 above), and its square root will equal the product of y, y', y'', etc. Further, it is easy to see that y', y'', etc., are derived from y in the same way as we said above in I that Y', Y'', etc., follow from Y; and that each coefficient in y too can be reduced to the form

$$A + B(f,1) + C(f,g) + \text{etc.}$$

since the sums of the individual powers of the roots of the equation $y = 0$ are evidently halves of the powers of the roots of the equation $Y = 0$, and hence reducible to such a form. In the last four cases, however, Y will be the product of the factors

$$xx - (\varphi\omega)^2,\ xx - (\varphi\mathfrak{a}\omega)^2,\ xx - (\varphi\mathfrak{b}\omega)^2 \text{ etc.}$$

and therefore of the form

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{etc.}$$

It is clear that the coefficients λ, μ, etc., can be derived from the sums of the squares, fourth powers, etc., of the roots $\varphi\omega, \varphi\mathfrak{a}\omega, \varphi\mathfrak{b}\omega$, etc.; and the functions Y', Y'', etc., will behave similarly.

Example I. Let $n = 17, f = 8$ and let φ denote the cosine. We then have

$$\begin{aligned} Z = \big(&x^8 + \tfrac{1}{2}x^7 - \tfrac{7}{4}x^6 - \tfrac{3}{4}x^5 + \tfrac{15}{16}x^4 \\ &+ \tfrac{5}{16}x^3 - \tfrac{5}{32}xx - \tfrac{1}{32}x + \tfrac{1}{256}\big)^2 \end{aligned}$$

and must therefore resolve $\sqrt{Z}$ into two factors of degree four, y, y'. The period $P = (8,1)$ consists of $(2,1), (2,9), (2,13), (2,15)$, so that y will be the product of the factors

$$x - \varphi\omega,\ x - \varphi 9\omega,\ x - \varphi 13\omega,\ x - \varphi 15\omega$$

Substituting $\frac{1}{2}[k] + \frac{1}{2}[n-k]$ for $\varphi k\omega$ gives

$$\begin{gathered} \varphi\omega + \varphi 9\omega + \varphi 13\omega + \varphi 15\omega = \tfrac{1}{2}(8,1), \\ (\varphi\omega)^2 + (\varphi 9\omega)^2 + (\varphi 13\omega)^2 + (\varphi 15\omega)^2 = 2 + \tfrac{1}{4}(8,1) \end{gathered}$$

Similarly, the sum of the cubes is $= \frac{3}{8}(8,1) + \frac{1}{8}(8,3)$, and the sum of the fourth powers $= 1\frac{1}{2} + \frac{5}{16}(8,1)$. Determining the coefficients in y from these by Newton's theorem gives

$$\begin{aligned} y = x^4 &- \tfrac{1}{2}(8,1)x^3 + \tfrac{1}{4}((8,1) + 2(8,3))xx \\ &- \tfrac{1}{8}((8,1) + 3(8,3))x + \tfrac{1}{16}((8,1) + (8,3)) \end{aligned}$$

Now y' is derived from y by interchanging $(8,1)$ and $(8,3)$; substituting for $(8,1)$, $(8,3)$ the values $-\frac{1}{2} + \frac{1}{2}\sqrt{17}, -\frac{1}{2} - \frac{1}{2}\sqrt{17}$ therefore gives

$$\begin{aligned} y = x^4 &+ (\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} + \tfrac{1}{8}\sqrt{17})xx \\ &+ (\tfrac{1}{4} + \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16} \end{aligned}$$

$$\begin{aligned} y' = x^4 &+ (\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} - \tfrac{1}{8}\sqrt{17})xx \\ &+ (\tfrac{1}{4} - \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16} \end{aligned}$$

Similarly, $\sqrt{Z}$ can be resolved into four factors of degree two, of which the first will be $(x - \varphi\omega)(x - \varphi 13\omega)$, the second $(x - \varphi 9\omega)(x - \varphi 15\omega)$, the third $(x - \varphi 3\omega)(x - \varphi 5\omega)$, and the fourth $(x - \varphi 10\omega)(x - \varphi 11\omega)$. All the coefficients in these factors can be expressed in terms of the four sums $(4,1), (4,9), (4,3), (4,10)$. Evidently, the product of the first factor and the second will be y, and the product of the third and fourth y'.

Example II. If, everything else remaining unchanged, φ is supposed to denote the sine, so that

$$\begin{aligned} Z = x^{16} &- \tfrac{17}{4}x^{14} + \tfrac{119}{16}x^{12} - \tfrac{221}{32}x^{10} \\ &+ \tfrac{935}{256}x^8 - \tfrac{561}{512}x^6 + \tfrac{357}{2048}x^4 - \tfrac{51}{4096}xx + \tfrac{17}{65536} \end{aligned}$$

must be resolved into two factors of degree 8, y, y', then y will be the product of four quadratic factors

$$xx - (\varphi\omega)^2,\ xx - (\varphi 9\omega)^2,\ xx - (\varphi 13\omega)^2,\ xx - (\varphi 15\omega)^2$$

Now, since $\varphi k\omega = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$, we have

$$\begin{aligned} (\varphi k\omega)^2 &= -\tfrac{1}{4}[2k] + \tfrac{1}{2}[n] - \tfrac{1}{4}[2n-2k] \\ &= \tfrac{1}{2} - \tfrac{1}{4}[2k] - \tfrac{1}{4}[2n-2k] \end{aligned}$$

From this we derive the sum of the squares of the roots $\varphi\omega, \varphi 9\omega, \varphi 13\omega.\varphi 15\omega$, namely $2 - \frac{1}{4}(8,1)$, the sum of their fourth powers $= \frac{3}{2} - \frac{3}{16}(8,1)$, the sum of their sixth powers $= \frac{5}{4} - \frac{9}{64}(8,1) - \frac{1}{64}(8,3)$, and the sum of their eighth powers $\frac{35}{32} - \frac{27}{256}(8,1) - \frac{1}{32}(8,3)$. Hence

$$\begin{aligned} y = x^8 &- (2 - \tfrac{1}{4}(8,1))x^6 \\ &+ (\tfrac{3}{2} - \tfrac{5}{16}(8,1) + \tfrac{1}{8}(8,3))x^4 \\ &- (\tfrac{1}{2} - \tfrac{9}{64}(8,1) + \tfrac{5}{64}(8,3))xx \\ &+ \tfrac{1}{16} - \tfrac{5}{256}(8,1) + \tfrac{3}{256}(8,3) \end{aligned}$$

We derive y' from y by interchanging $(8,1), (8,3)$, so that substituting the values of these sums gives

$$\begin{aligned} y = x^8 &- (\tfrac{17}{8} - \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} - \tfrac{7}{32}\sqrt{17})x^4 \\ &- (\tfrac{17}{32} - \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} - \tfrac{1}{64}\sqrt{17} \end{aligned}$$

$$\begin{aligned} y' = x^8 &- (\tfrac{17}{8} + \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} + \tfrac{7}{32}\sqrt{17})x^4 \\ &- (\tfrac{17}{32} + \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} + \tfrac{1}{64}\sqrt{17} \end{aligned}$$

Similarly, Z can be resolved into four factors whose coefficients can be expressed in terms of sums of four terms; the product of two of them will be y, and the product of the remaining two y'.

Divisions of the circle that can be carried out by quadratic equations or by geometric constructions.

365.

Through the preceding investigations we have therefore reduced the division of the circle into n parts, when n is prime, to the solution of as many equations as there are factors into which the number $n-1$ can be resolved; the degrees of these equations are determined by the sizes of the factors. Thus, whenever $n-1$ is a power of the number 2, as happens for n at the values 3, 5, 17, 257, 65537, etc., the division of the circle reduces to quadratic equations alone, and the trigonometric functions of the angles $\frac{P}{n}$, $\frac{2P}{n}$, etc., can be expressed by square roots of greater or lesser complexity (according to the size of n). In these cases, therefore, the division of the circle into n parts, or the drawing of a regular polygon of n sides, can evidently be accomplished by geometric constructions. Thus, e.g. for $n = 17$, Articles 354 and 361 readily give the following expression for the cosine of the angle $\frac{1}{17}P$:

$$\begin{aligned} &-\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34 - 2\sqrt{17})} \\ &\quad + \tfrac{1}{8}\sqrt{(17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17})} \\ &\qquad - 2\sqrt{(34 + 2\sqrt{17})} \end{aligned}$$

The cosines of multiples of this angle have a similar form, but the sines have one more radical sign. It is indeed greatly to be wondered at that, although the geometric divisibility of the circle into three and five parts was already known in Euclid's time, nothing was added to these discoveries over an interval of 2000 years, and all geometers pronounced it certain that, apart from these divisions and those that follow from them of themselves, namely divisions into $15, 3.2^\mu, 5.2^\mu, 15.2^\mu$ and also into 2^μ parts, no others could be accomplished by geometric constructions. — Further, it is easy to prove that if the prime n is $= 2^m + 1$, the exponent m too can contain no prime factors other than the number 2, and must therefore be either $= 1$, or $= 2$, or equal to a higher power of the number 2. For if m were divisible by any odd number ζ (greater than unity), and $m = \zeta\eta$, then $2^m + 1$ would be divisible by $2^\eta + 1$, and therefore necessarily composite. Thus all values of n for which we arrive at quadratic equations alone are contained in the form $2^{2^\nu} + 1$; the five numbers 3, 5, 17, 257, 65537 arise by setting $\nu = 0, 1, 2, 3, 4$, or $m = 1, 2, 4, 8, 16$. The division of the circle can by no means be carried out geometrically for *all* numbers contained in that form, but only for those that are prime. Fermat, misled by induction, had indeed asserted that all numbers contained in that form must be prime; but the distinguished Euler was the first to notice that this rule is already false for $\nu = 5$, or $m = 32$, since the number $2^{32} + 1 = 4294967297$ contains the factor 641.

Whenever, however, $n-1$ contains prime factors other than 2, we always arrive at higher equations: namely, at one or more cubic equations when 3 occurs once or more among the prime factors of $n-1$, at equations of the fifth degree when $n-1$ is divisible by 5, and so on; AND WE CAN PROVE WITH COMPLETE RIGOR THAT THESE HIGHER EQUATIONS CAN IN NO WAY BE AVOIDED OR REDUCED TO LOWER ONES, although the limits of this work do not allow us to give this proof here. We

nevertheless thought it necessary to mention this, so that no one should hope to achieve by geometric constructions still other divisions beyond those suggested by our theory, e.g. divisions into 7, 11, 13, 19, etc., parts, and waste time in vain.

366.

If the circle is to be divided into a^α parts, where a denotes a prime, this can evidently be accomplished geometrically when $a = 2$, but for no other value of a, provided $\alpha > 1$. For then, besides the equations required for division into a parts, it is necessary to solve $\alpha - 1$ further equations of degree a; these too can in no way be avoided or reduced in degree. Thus the degrees of the necessary equations can be known in general from the prime factors of the number $(a-1)a^{\alpha-1}$ (that is, also in the case $\alpha = 1$).

Finally, if the circle is to be divided into $N = a^\alpha b^\beta c^\gamma \ldots$ parts, where a, b, c, etc., denote unequal primes, it suffices to have carried out the divisions into $a^\alpha, b^\beta, c^\gamma$, etc., parts (Article 336). To know the degrees of the equations needed for this purpose, we must therefore consider the prime factors of the numbers

$$(a-1)a^{\alpha-1}, \quad (b-1)b^{\beta-1}, \quad (c-1)c^{\gamma-1} \text{ etc.}$$

or, what here amounts to the same thing, of their product. Observe that this product expresses the number of numbers coprime to N and smaller than it (Article 38). The division can therefore be accomplished geometrically only when this number is a power of two; when, however, it contains prime factors other than 2, say p, p', etc., equations of degree p, p', etc., can in no way be avoided. From this we conclude in general that, for the circle to be divisible geometrically into N parts, N must be *either* 2 or a higher power of 2, *or* a prime of the form $2^m + 1$, *or* a product of several such primes, *or* the product of one or more such primes with 2 or a higher power of 2. More briefly, it is required that N contain neither an odd prime factor that is not of the form $2^m + 1$, nor any prime factor of the form $2^m + 1$ more than once. The following values of N occur below 300, 38 in all: $2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272$.

ADDITIONS.

On Article 28. The indeterminate equation $ax = by \pm 1$ was first solved not by the distinguished Euler (as stated there), but already by Bachet de Meziriac, a geometer of the 17th century and the celebrated editor and commentator of Diophantus, for whom the distinguished La Grange claimed this honor (*Add. à l'Algèbre d'Euler p.* 525, where the nature of the method is also indicated). Bachet gave his discovery in the second edition of his book *Problèmes plaisans et délectables qui se font par les nombres*, 1624; it does not yet appear in the first edition (Lyon 1612), which alone I have been able to see, although it is already announced there.

On Articles 151, 296, 297. The distinguished Le Gendre set out his proof again in his excellent work *Essai d'une théorie des nombres*, p. 214 ff., but without any essential change; this method therefore remains subject to all the objections raised in Article 297. The theorem (on which one assumption rests) that primes occur in every arithmetic progression $l, l + k, l + 2k$, etc., if k and l have no common divisor, has indeed been considered at greater length in this work, p. 12 ff.; but the requirements of geometric rigor still seem not to have been met. Yet even when this theorem has been fully proved, the other assumption will remain (that there are primes of the form $4n + 3$ for which a given prime of the form $4n + 1$, taken positively, is a quadratic nonresidue), and I do not know whether this can be proved *rigorously* unless the fundamental theorem itself is already *assumed*. Further, it should be observed that the distinguished Le Gendre did not make this latter assumption tacitly, but himself also acknowledged it, p. 221.

On Articles 288—293. On the same subject, presented here as a special application of the theory of ternary forms, and apparently so fully treated in rigor and generality that nothing further could be desired, the distinguished Le Gendre undertook a much more extensive investigation in Part III of his work, pp. 321—400.*) He used principles and methods entirely different from ours, but on this path became involved in several difficulties that prevented him from supporting the principal theorems by a rigorous proof. He himself candidly indicated these difficulties; but, unless we are mistaken, these may perhaps be removed more easily than the difficulty that here too the theorem just mentioned (In every arithmetic progression, etc.) is assumed, p. 371, end of the note.

On Article 306 VIII. In the third thousand of negative determinants, 37 irregular ones have been found, of which 18 have index of irregularity 2, and the remaining 19 have index 3.

*) Even without our warning, readers will take care not to confuse our ternary forms with what the distinguished Le Gendre called *forme trinaire d'un nombre*. By this expression he meant the decomposition of a number into three squares.

On the same article X. The question posed here has recently been completely solved. We will present this investigation, which casts remarkable light on several parts of both higher arithmetic and analysis, in the continuation of this work as soon as possible. It has also shown that the coefficient m in Article 304 is $= \gamma\pi =$ 2,3458847616, where γ denotes the same quantity as in Article 302, and π, as there, the semicircumference of a circle whose radius is 1.

TABLES.

TABLE I. (Articles 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

TABLE II. (Article 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	—	—	—			—						—			—	—	—		—			—	—		—	—

TABLE III. (Article 316).

3	(0)..3; (1)..6
7	(0)..142857
9	(0)..1; (1)..2; (2)..4; (3)..8; (4)..7; (5)..5
11	(0)..09; (1)..18; (2)..36; (3)..72; (4)..45
13	(0)..076923; (1)..461538
17	(0)..0588235294 117647
19	(0)..0526315789 47368421
23	(0)..0434782608 6956521739 13
27	(0)..037; (1)..074; (2)..148; (3)..296; (4)..592; (5)..185
29	(0)..0344827586 2068965517 24137931
31	(0)..0322580645 16129; (1)..5483870967 74193
37	(0)..027; (1)..135; (2)..675; (3)..378; (4)..891; (5)..459 (6)..297; (7)..486; (8)..432; (9)..162; (10)..810; (11)..054
41	(0)..02439; (1)..14634; (2)..87804; (3)..26829; (4)..60975; (5)..65853; (6)..95121; (7)..70731
43	(0)..0232558139 5348837209 3; (1)..6511627906 9767441860 4
47	(0)..0212765957 4468085106 3829787234 0425531914 893617
49	(0)..0204081632 6530612244 8979591836 7346938775 51
53	(0)..0188679245 283; (1)..4905660377 358; (2)..7547169811 320; (3)..6226415094 339
59	(0)..0169491525 4237288135 5932203389 8305084745 7627118644 06779661
61	(0)..0163934426 2295081967 2131147540 9836065573 7704918032 7868852459
67	(0)..0149253731 3432835820 8955223880 597; (1)..1791044776 1194029850 7462686567 164
71	(0)..0140845070 4225352112 6760563380 28169; (1)..8732394366 1971830985 9154929577 46478
73	(0)..01369863; (1)..06849315; (2)..34246575; (3)..71232876; (4)..56164383 (5)..80821917; (6)..04109589; (7)..20547945; (8)..02739726
79	(0)..0126582278 481; (1)..3670886075 949; (2)..6455696202 531 (3)..7215189873 417; (4)..9240506329 113; (5)..7974683544 303
81	(0)..012345679; (1)..135802469; (2)..493827160; (3)..432098765; (4)..753086419; (5)..283950617
83	(0)..0120481927 7108433734 9397590361 4457831325 3 (1)..6024096385 5421686746 9879518072 2891566265 0
89	(0)..0112359550 5617977528 0898876404 4943820224 7191 (1)..3370786516 8539325842 6966292134 8314606741 5730
97	(0)..0103092783 5051546391 7525773195 8762886597 9381443298 9690721649 4845360824 7422680412 3711340206 185567

CONTENTS.

DEDICATION ..... p. 3.

PREFACE ..... p. 5.

SECTION I. Congruence of numbers in general ..... p. 9.

Congruent numbers, moduli, residues and nonresidues, Article 1 f.
Least residues, 4.
Elementary propositions on congruent numbers, 5.
Some applications, 12.

SECTION II. Congruences of the first degree ..... p. 14.

Preliminary theorems on prime numbers, factors, etc., Article 13.
Solution of congruences of the first degree, 26.
Finding a number congruent to given residues for given moduli, 32.
Linear congruences involving several unknowns, 37.
Various theorems, 38.

SECTION III. Residues of powers ..... p. 38.

The residues of the terms of a geometric progression beginning with unity form a periodic sequence, Article 45.
Prime moduli are considered first.
Setting the modulus $= p$, the number of terms in the period divides $p - 1$, Article 49.
Fermat's theorem, 50.
How many numbers correspond to periods whose number of terms is a given divisor of $p - 1$, Article 52.
Primitive roots, bases, indices, 57.
The algorithm of indices, 58.
The roots of the congruence $x^n \equiv A$, Article 60.
The relation between indices in different systems, 69.
Bases suited to particular uses, 72.
A method of finding primitive roots, 73.
Various theorems on periods and primitive roots, 75.
(Wilson's theorem, 76).
Moduli that are powers of prime numbers, Article 82.
Moduli that are powers of two, 90.
Moduli composed of several primes, 92.

SECTION IV. Congruences of the second degree ..... p. 73.

Quadratic residues and nonresidues, Article 94.
Whenever the modulus is prime, the number of residues smaller than it equals the number of nonresidues, 96.

Whether a composite number is a residue or a nonresidue of a given prime depends on the nature of its factors, 98.
Composite moduli, 100.
A general criterion for whether a given number is a residue or a nonresidue of a given prime, 106.
Investigations of primes for which given numbers are residues or nonresidues, 107.
The residue -1, Article 108.
The residues $+2$ and -2, Article 112.
The residues $+3$ and -3, Article 117.
The residues $+5$ and -5, Article 121.
On ± 7, Article 124.
Preparation for the general investigation, 125.
A general (*fundamental*) theorem is established by induction, and conclusions are deduced from it, 130.
A rigorous proof of this theorem, 135.
An analogous method of proving the theorem of Article 114, 145.
Solution of the general problem, 146.
Linear forms containing all primes for which any given number is either a residue or a nonresidue, 147.
The work of others on these investigations, 151.
Congruences of the second degree that are not pure, 152.

Section V. Forms and indeterminate equations of the second degree . . . . . p. 120.

The aim of the investigation; definition and notation of forms, Article 153.
Representation of numbers; the determinant, 154.
Values of the expression $\sqrt{(bb-ac)}$ (mod. M) to which the representation of the number M by the form (a,b,c) belongs, 155.
A form containing another, or contained in another; proper and improper transformations, 157.
Proper and improper equivalence, 158.
Opposite forms, 159, adjacent forms, 160.
Common divisors of the coefficients of forms, 161.
The relation among all similar transformations of a given form into a given form, 162.
Ambiguous forms, 163.
A theorem on the case where a form is contained in another both properly and improperly, 164.
General results on representations of numbers by forms and their relation to transformations, 166.
Forms of negative determinant, 171.
Special applications to decomposing numbers into two squares, into a square and twice a square, and into a square and three times a square, 182.
Forms of positive nonsquare determinant, 183.
Forms of square determinant, Article 206.
Forms contained in others to which they are nevertheless not equivalent, 213.

Forms of determinant 0, Article 215.
The general solution in integers of all indeterminate equations of the second degree involving two unknowns, 216.
Historical notes, 222.

Further investigations of forms.

Distribution of forms of a given determinant into classes, Article 223; of classes into orders, 226.
Division of orders into genera, 228.
Composition of forms, 234.
Composition of orders, 245, genera, 246, classes, 249.
For a given determinant, each genus of the same order contains equally many classes, 252.
Comparison of the numbers of classes contained in the individual genera of different orders, 253.
The number of ambiguous classes, 257.
At least half of all characters that can be assigned for a given determinant cannot have corresponding properly primitive genera (positive for negative determinants), 261.
A second proof of the fundamental theorem and the other theorems concerning the residues $-1, +2, -2$, 262.
A closer determination of the half of the characters to which genera cannot correspond, 263.
A special method of decomposing primes into two squares, 265.

A digression containing a treatment of ternary forms, Article 266 ff.

Some applications to the theory of binary forms.
Finding a form whose duplication produces a given binary form of the principal genus, 286.
Genera do in fact correspond to all characters except those found impossible in Articles 262, 263, 287 III.
The theory of decomposing both numbers and binary forms into three squares, 288.
Proof of Fermat's theorems that every integer can be decomposed into three triangular numbers or four squares, 293.
Solution of the equation $axx + byy + czz = 0$, Article 294.
The method by which the distinguished Le Gendre treated the fundamental theorem, 296.
Representation of zero by arbitrary ternary forms, 299.
The general solution in rational quantities of indeterminate equations of the second degree involving two unknowns, 300.
The average number of genera. 301; of classes, 302.
A special algorithm of properly primitive classes; regular and irregular determinants, etc., 305.

SECTION VI. Various applications of the preceding investigations ..... p. 380.

Decomposition of fractions into simpler ones, Article 309.

Conversion of common fractions into decimals, 312.

Solution of the congruence $xx \equiv A$ by the method of exclusion, 319.

Solution of the indeterminate equation $mxx + nyy = A$ by exclusions, 323.

Another method of solving the congruence $xx \equiv A$ for the case where A is negative, Article 327.

Two methods of distinguishing composite numbers from primes and finding the factors of the former, 329.

SECTION VII. Equations defining divisions of the circle ..... p. 412.

The investigation is reduced to the simplest case, where the number of parts into which the circle is to be divided is prime, Article 336.

Equations for trigonometric functions of arcs that are one part or several parts of the whole circumference; reduction of trigonometric functions to roots of the equation $x^n - 1 = 0$, Article 337.

Theory of the roots of this equation (where n is assumed to be prime).

Omitting the root 1, the remaining roots (Ω) are contained in the equation $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$.

The function X cannot be resolved into factors of lower degree in which all coefficients are rational, 341.

The aim of the following investigations is stated, 342.

All roots Ω are distributed into certain classes (periods), 343.

Various theorems on these periods, 344 ff.

The solution of the equation $X = 0$ is built on these investigations, Article 352.

Examples for $n = 19$, where the task is reduced to two cubic equations and one quadratic, and for $n = 17$, where it is reduced to four quadratics, Articles 353. 354.

Further investigations of this subject.

Sums with an even number of terms are real quantities, 355.

The equation defining the distribution of the roots Ω into two periods, 356.

Proof of the theorem mentioned in Section IV, 357.

The equation for distributing the roots Ω into three periods, 358.

Reduction to pure equations of the equations by which the roots Ω are found, 359.

Application of the preceding investigations to trigonometric functions.

A method of identifying the angles to which the individual roots Ω correspond, 361.

Tangents, cotangents, secants and cosecants are derived from sines and cosines without division, 362.

A method of successively lowering the degrees of equations for trigonometric functions, 363.

Divisions of the circle that can be carried out by quadratic equations or by geometric constructions, 365.

Additions ..... p. 465.

Tables ..... p. 467.

Printed at Goslar by E. W. G. Kircher.

APPENDIX.

MANUSCRIPT NOTES BY GAUSS.

On Article 40. *With a third number C added, let λ' be the greatest common divisor of the numbers λ, C, and determine numbers k, γ such that $k\lambda + \gamma C = \lambda'$, whence $k\alpha A + k\beta B + \gamma C = \lambda'$. It is clear that λ' is a common divisor of the numbers $A, B.C$, and indeed the greatest; for if there were a greater one $= \theta$, then*

$$k\alpha.\frac{A}{\theta} + k\beta.\frac{B}{\theta} + \gamma.\frac{C}{\theta} = \frac{\lambda'}{\theta} \quad \textit{integer, Q. E. A.}$$

Thus what was proposed has been accomplished, on setting $k\alpha = a$, $k\beta = b$, $\gamma = c$, $\lambda' = \mu$.

On Article 114. *The proof can be presented more elegantly as follows: $(a^{3n} - a^n)^2 = 2 + (a^{4n} + 1)(a^{2n} - 2)$, $(a^{3n} + a^n)^2 = -2 + (a^{4n} + 1)(a^{2n} + 2)$, and hence $\sqrt{2} \equiv \pm(a^{3n} - a^n)$, $\sqrt{-2} \equiv \pm(a^{3n} + a^n)$ (mod. $8n + 1$)*

In Article 256 VI the 16 positive determinants of the form $8n + 5$ for which the number of properly primitive classes is three times as large as that of improperly primitive classes, '37, .. 573', are supplemented by: *677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997, so that among 125 there are 31.*

On the words of Article 301: By this method the sum of the numbers of genera for determinants $-$: up to -100 is found $= 234, 4$, whereas it is actually 233. — — *From -1 to -3000, table 11166, formula 11167,9.*

On Article 336. *If all numbers of the form $2^{2^m} + 1$ were prime, a sufficiently approximate expression for the number of the numbers in question (N) smaller than a given number M would be $\frac{1}{2}\left(\frac{\log M}{\log 2}\right)^2$.*

On the theorem in Article 42 on the divisors of a polynomial with integer coefficients — — *1797 July 22.*

On the words of Article 130: After we have rigorously proved that every prime of the form $4n+1$, taken both positively and negatively, is a nonresidue of some smaller prime, — — *We discovered this proof in 1796, on April 8.*

On Article 131. *The fundamental theorem was discovered by induction in March 1795. The first proof, given in this section, was found in April 1796.*

On the words of Article 133: Let us undertake the investigation (of the fundamental theorem) still more generally. Consider any two odd coprime numbers, with any signs, P and Q. — — *1796 April 29.*

On the words of Article 145: Moreover, the theorems concerning the residues $+2$ and -2 would then have had to be assumed; but since our proof has been completed without these theorems, we obtain from it a new method of proving them. — — *1797 February 4.*

On the heading of Section V: Forms and indeterminate equations of the second degree. — — *From June 22, 1796 onward.*

On the words of Article 234: .. we pass to another subject of the greatest importance, hitherto untouched by anyone, the composition of forms. — — *These investigations were begun in the autumn of 1798.*

On the words of Article 262: From this principle we can derive a new method of proving not only the fundamental theorem, but also the other theorems of the preceding section concerning the residues $-1, +2, -2$, — — *The principles of this method first presented themselves in 1796, on July 27, but were developed and brought into their present form in the spring of 1800.*

On the words of Article 266: .. but since several truths concerning them, and very beautiful ones, still remain, whose proper source must be sought in the theory of ternary forms of the second degree, we insert here a short digression on this theory, — — *February 14, 1799.*

On the words of Article 272: namely, by showing first how any ternary form can be reduced to a simpler form, and then that the number of the simplest forms (reached by such reductions) is finite for any given determinant. — — *1800 February 13.*

On the words of Article 287 III: In an entirely similar way it is proved that in the improperly primitive order all the characters found to be the only possible ones by the rules of Article 264 II, III are possible, whether they are P or Q. — These theorems, etc. — — *They were first supplied with proofs in April 1798.*

On the words of Article 302: The average number of classes, however (which will need no definition), grows very regularly, — — *The first idea at the beginning of 1799.*

On the words of Article 306 X: Finally, we observe that, since all the properties considered in this and the preceding article depend chiefly on the number n, which is something similar to $p - 1$ in Section III, this number deserves the closest attention; it would therefore be most desirable to discover a general relation between it and the determinant to which it belongs. — — *It has turned out as we wished—and so completely that nothing further remains to be desired. November 30—December 3, 1800.*

On Article 365. *We discovered that the circle can be divided geometrically into 17 parts in 1796, on March 30.*

CLOSING NOTE ON THE NEW EDITION.

This first volume of GAUSS's works is a reprint of the seven sections of the Disquis. Arithm. published in octavo in 1801. The eighth section, referred to at several places and probably originally intended by GAUSS for publication with the others, is among his manuscripts. Since he did not finish preparing it in the same way as the first seven sections, it will accompany the posthumous arithmetical papers in this edition.

Textual changes have been made in the Disqu. Ar. only at the following places:

In Article 125 the two insertions (if > 5) and (> 17; but $-13N3$, $-17N5$) have been added.

In Article 126. *Proof.* 'in the series (I), a terms are divisible by p, b terms by p^2, c terms by p^3, etc.' has been substituted for 'in the series (I), a terms are divisible by p but not by p^2, b terms by p^2 but not by p^3, c terms by p^3 but not by p^4, etc.'

In Article 128 III the passage 'For if $+b$ or $-b \equiv r \pmod{p}$, then $bb \equiv rr \pmod{2p}$, and hence the term $\frac{1}{2}(a - bb)$ is divisible by p.' was still followed, in the edition of 1801, by 'and much more so $2(a - bb)$.'; these latter words have been omitted.

In Article 129, $2\sqrt{a+1}$ has everywhere been substituted for $2\sqrt{a}$, and accordingly 9 for 4 as the number below which a certainly does not fall.

In Article 139 the end of the investigation of case (4) read 'It is easy to see that from this equation we can deduce $a'pRh$, $\pm ahpRa'$, $\pm aa'hRp$; these agree with what we found in (2). In the remaining cases the proof is the same.' This has been changed in accordance with the note that GAUSS added to Article 2 of the paper *Theorematis arithmetici demonstratio nova*: 'It will not be out of place to indicate and correct here a slight error that, through I know not what negligence, slipped into the exposition of that proof. On page (108), from line (14) onward, the following reasoning is to be substituted: It is easy to see that from this equation we can deduce $a'pRh \ldots (\alpha)$; $\pm ahRa' \ldots (\delta)$; $\pm ahRp \ldots (\gamma)$. From (α), which agrees with (α) in (2), it follows, just as there, that either hRp, hRa' hold together, or hNp, hNa'. But in the former case (δ) would give aRa', contrary to the hypothesis; hence hNp, and therefore by (γ) also aNp.

In Article 171, in accordance with a manuscript note, 'in which A is neither greater than $\sqrt{\frac{4}{3}D}$, C, nor less than $2B$' has been substituted for 'in which A is not $> \sqrt{\frac{4}{3}D}$, B not $> \frac{1}{2}A$, C not $< A$'.

In Article 174. *Second method.* 'Since a will not be $> \sqrt{\frac{4}{3}D}$, all forms obtained in this way will evidently be reduced.' has been substituted for 'Any forms obtained in this way in which $a > \sqrt{\frac{4}{3}D}$ must be rejected; all the rest will evidently be reduced.'

In Article 256 VI the earlier edition includes, among the positive determinants of the form $8n + 5$ for which the number of classes in the properly primitive order is three times as large as that in the improperly primitive order, also the determinant 397; but it has equally many classes of both kinds.

In Article 302, in accordance with a manuscript note, the number of classes for the second thousand of negative determinants is given as 28595, rather than 28603 as in the earlier edition.

In Article 303 the numbers of determinants for the classifications II. 4; II. 5; IV. 2 are given, from the tables found among the posthumous papers, as 31, 44, 69, rather than 32, 42, 68 as in the earlier edition.

In Article 325, '$23t,\ 23t \pm 1,\ 23t \pm 5,\ 23t \pm 7,\ 23t \pm 9,\ 23t \pm 10$. When these have been deleted, 119, 127 are found to remain, and these two alone give V a square value' has been substituted for '$23t,\ 23t \pm 5,\ 23t \pm 7, 23t \pm 9,\ 23t \pm 10$. When these have been deleted, 119, 127, 137 are found to remain, of which the first two alone give V a square value.'

In Article 360 IV the words 'whereas for most other cubic equations whose roots are all real, trisection of both an angle and a ratio cannot be avoided.', which followed 'for example, for $\beta = 3$ only trisection of an angle', and whose incorrectness Gauss noted in his own copy, have been omitted.

The notes on pages 80, 102, 133, 211, 263, 265, 449 are taken from the posthumous manuscripts.

To make the work easier to survey, the outward form of the new edition has been changed in several respects from the printing of 1801. This was thought all the more justified because Gauss, by his own account, also considered saving space in other respects. Many formulas that were contained in the line of text have been set out separately. The summaries, which preceded the work as a collection, have also been placed before the individual divisions, rather than only before the sections as in the first edition; the more general ones have been used as page headings.

GÖTTINGEN,
PRINTED AT THE DIETERICH UNIVERSITY PRESS
W. FR. KAESTNER.

Carl Friedrich Gauss

Arithmetical Papers

English translation

Volume II: arithmetical papers, reviews and manuscript studies

AI-translated into English using OpenAI GPT-6.1 Sol.

This selection contains the historical title matter and first five complete papers of Volume II: A New Proof of an Arithmetical Theorem (Articles 1–7); Summation of Certain Special Series (Articles 1–36); New Proofs and Extensions of the Fundamental Theorem in the Theory of Quadratic Residues, with its introduction, fifth proof (Articles 1–3), sixth proof (Articles 1–6) and new algorithm (Articles 1–6); and both papers on the Theory of Biquadratic Residues (Articles 1–23 and 24–76). Five self-reviews from 1808–1831 and seven reviews of other writings from 1809–1831 follow. The latter concern irrational radicals, the factor tables of Chernac and Burckhardt, Erchinger's construction of the regular seventeen-sided polygon, and Seeber's positive ternary quadratic forms.

The manuscript studies include Solution of a Pure Congruence, Analysis of Residues, Chapter VI, first part (Articles 237–252); General Investigations of Congruences, Chapter VIII (Articles 330–375 as printed, including the unfinished ending of Article 375), with R. Dedekind's historical remarks; and Further Development of the Investigations of Pure Equations, complete as printed (Articles 1–19), with Dedekind's remarks. The fragment Proof of Some Theorems Concerning the Periods of Classes of Binary Quadratic Forms follows, with both theorems, the unfinished ending of the second proof, and Stern's historical remark.

The texts marked [I.] and [II.] of On the Connection between the Number of Classes into Which Binary Quadratic Forms Are Distributed and Their Determinant, First Paper, follow in full as printed, each with its title and Articles 1–8. The text marked [II.] was presented in 1837. Fragments III–X follow, with their historical editorial notes. Historical remarks on [I.]–[X.] follow. Geometrical Aspect of Ternary Forms follows with its two diagrams, crystallographic tables and Schering's historical remarks.

Originally German title matter, reviews, the manuscript division title, Fragments III–IV and VIII–X, the geometric notes and the historical remarks are rendered in modern German in the German reader. Their historical originals are supplied separately. The posthumous On the Theory of Biquadratic Residues, text [I.], is included in full as printed, Articles 1–19, with all five diagrams. Text [II.], Preparations for the General Theory of Biquadratic Residues, follows in full as printed, with both preparatory sections and Articles 1–12. Text [III.], Theory of Biquadratic Residues, follows in full as printed, with its title and Articles 1–14, including the joint heading 7–8. Text [IV.] follows in full as printed, Articles 1–5; its second method ends after the fourth step. Text [V.] follows in full as printed, Articles 1–17, with its editable lattice diagram. Text [VI.] follows in full as printed, Articles 1–6. Schering's complete historical remarks on texts [I.]–[VI.] follow. The originally German prose of these texts is rendered in modern German in the German reader; the historical originals are supplied separately. On the Theory of Complex Numbers follows in full as printed: six fragments [I.]–[VI.] on the decomposition of cubes, the nearest integer, measures of numbers, units and congruences, followed by Schering's historical remarks. The originally German passages are rendered in modern German in the German reader, and their historical originals are supplied separately. The complete historical table of the quadratic character of the primes from 2 to 997 as residues with respect to the primes from 3 to 503 as divisors follows. The complete historical table for converting common fractions with denominators from the first thousand into decimal fractions follows. The complete historical table of the frequency of prime numbers follows, including its matrices and closing observations. The complete letter from Gauss to Enke of 24 December 1849 follows, including its tables and discussion of prime-number frequency. The German reader renders the originally German letter in modern German; its historical original is supplied separately. The complete historical table of the number of classes of binary quadratic forms follows, with its negative and positive determinants and all printed summaries. Its historical values and abbreviations are retained. The German title is rendered in modern German in the German reader; the historical source is supplied separately.

The complete historical Table for Circle Division follows, with all nine factor tables and their printed index lists. Its originally German title and headings are rendered in modern German in the German reader; the historical source is supplied separately. A New Quadrature of the Circle follows with its four complete printed calculations and the arc table, including its historical blanks. On Calculating Common Logarithms follows in full as printed, with its tables and bracketed historical editorial account. Its German original is supplied separately; the German reader gives a modern German rendering. The First Ten Thousand Squares, Indices of Primes in the Higher Number Domain, and the Auxiliary Table for Solving the Indeterminate Equation by the Method of Exclusion follow in full as printed. The original German texts are supplied separately; the German reader gives modern German renderings. The Eighth Section, A Fuller Consideration of Certain Investigations Concerning Circle Division, follows through its whole printed ending in Article 373, including the interruption in Article 371. Both letters from Gauss to Dirichlet, dated 13 September 1826 and 30 May 1828, follow in full with their numerical tables. Their German originals are supplied separately; the German reader gives modern German renderings. Other volumes of Gauss's works lie outside this reader. Complete Volume I accompanies it in the collected reader.

Historical source: Carl Friedrich Gauss, Werke, Volume II, second printing, Göttingen, 1876.

AI-translated into English using OpenAI GPT-6.1 Sol.

Schering's complete historical closing remarks, the historical contents and the Göttingen imprint follow. Originally German passages are rendered in modern German in the German reader; their historical originals are supplied separately.

Translation sources and terminology

Historical text: Carl Friedrich Gauss, *Werke*, Volume II, second printing, Göttingen, 1876. Historical editorial contributions retain their own authorship and signatures. Originally German passages are rendered in modern German in the German reader; their historical originals are supplied separately.
These English and German editions are AI-translated using OpenAI GPT-6.1 Sol, with AI-produced typesetting. The following named human translations and writings are scholarly references for the terminology and usage specified below. Gauss's original-language text remains the mathematical source.

H. Maser.

German translator and editor, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Corresponding arithmetical passages and German mathematical terminology.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead and Adam Miller Hiltebeitel.

Translators of Gauss's *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX edition. Related English geometrical terminology and usage.
`https://www.gutenberg.org/ebooks/36856`

Paul Taylor; Bernard Leak.

Taylor's English translation of Gauss's second proof of the fundamental theorem of algebra, with corrections by Leak, 1983. Related English algebraic terminology.
The consulted online edition identifies the translation as December 1983, its LaTeX version as August 2003, and the underlying source as last modified on 8 June 2007. Its acknowledgements credit Mark Wainwright for returning Taylor's notes and Nikita Danilov for typo corrections.
`https://www.paultaylor.eu/misc/gauss.html`

Ulrich Görtz.

Algebra, WS 2021/22, 3.1.1–3.1.3 and opening of 3.1.4; *Lineare Algebra II*, SS 2021, 18.4. Contemporary German arithmetic and algebraic usage.
`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. Related contemporary German terminology for quadratic forms.
`https://arxiv.org/abs/1510.06214v3`

Ian O. Angell and Moreton Moore.

Projections of cubic crystals, IUCr, Table 2. English crystallographic nomenclature.
IUCr: Projections of cubic crystals, Table 2

Th. Hahn, H. Klapper, U. Müller and M. I. Aroyo.

Point groups and crystal classes, *International Tables for Crystallography A*, 2016, chapter 3.2. Crystal-form names.
https://doi.org/10.1107/97809553602060000930

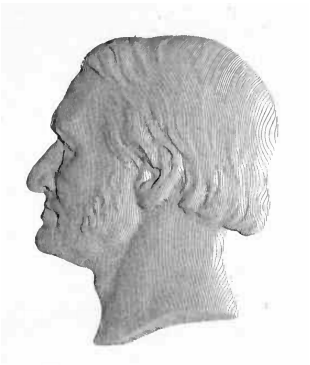
CARL FRIEDRICH GAUSS COLLECTED WORKS

VOLUME II.

CARL FRIEDRICH GAUSS

COLLECTED WORKS

SECOND VOLUME.



SECOND PRINTING

PUBLISHED
BY THE
ROYAL SOCIETY OF SCIENCES
AT
GÖTTINGEN
1876.

A NEW PROOF

OF AN ARITHMETICAL THEOREM

BY

CARL FRIEDRICH GAUSS

PRESENTED TO THE ROYAL SOCIETY OF SCIENCES JANUARY 15, 1808.

Commentationes societatis regiae scientiarum Gottingensis. Vol. XVI.
Gottingae MDCCCVIII.

A NEW PROOF

OF AN ARITHMETICAL THEOREM.

1.

Questions in higher arithmetic very often present a singular phenomenon, which occurs much more rarely in analysis and contributes greatly to their charm. In analytic investigations we usually cannot reach new truths unless we have first thoroughly mastered the principles on which they rest and which must, as it were, open the way to them. In arithmetic, by contrast, most elegant new truths very frequently spring forth through induction and a kind of unexpected good fortune; their proofs lie so deeply hidden and are wrapped in such darkness that they elude every attempt and deny access to the keenest investigations. Moreover, so great and so wonderful is the connection among arithmetical truths that at first sight seem utterly different, that quite often, while we are seeking something quite different, we at last most happily reach the proof so greatly desired and previously sought in vain through long reflection, by a path far different from the one expected. Usually, however, truths of this kind are of such a nature that they can be approached by several very different paths, and the paths that first present themselves are not always the shortest. It must therefore certainly be highly valued if, after such a truth has long been investigated in vain, and has then indeed been proved, but by rather obscure detours, we finally succeed in discovering the simplest and genuine path.

2.

Among the questions discussed in the preceding article, a distinguished place is held by the theorem containing almost the whole theory of quadratic residues, which in the *Arithmetical Investigations* (Section IV) is distinguished by the name of the *fundamental theorem*. The illustrious LEGENDRE must undoubtedly be regarded as the *first* discoverer of this most elegant theorem, after the great geometers EULER and LAGRANGE had, long before, already discovered several of its special cases by induction. I do not pause here to enumerate these men's attempts at a proof; those who wish may consult the work just mentioned. Let me add only, in confirmation of what was said in the preceding article, what concerns my own attempts. I came upon the theorem itself independently in the year 1795, when I was entirely ignorant of everything that had already been worked out in higher arithmetic and wholly cut off from access to the literature. But for an entire year it tormented me and eluded my most strenuous efforts, until at last I obtained the proof given in the fourth section of that work. Afterwards three others, resting on wholly

different principles, presented themselves to me; I gave one in the fifth section, and the others, not inferior to it in elegance, I shall make public on another occasion. But all these proofs, although they seem to leave nothing to be desired in rigour, are derived from principles that are too different in kind, perhaps excepting the first, which nevertheless proceeds by more laborious reasoning and is burdened by rather lengthy operations. I therefore do not hesitate to declare that a *genuine* proof has so far been lacking. Let the experts now judge whether the one that I recently succeeded in discovering, and that the following pages present, deserves to be honoured with this name.

3.

THEOREM. *Let p be a positive prime number; k any integer not divisible by p; use the following definitions:*

A *collection of the numbers* $1,\ 2,\ 3\ \ldots.\ \frac{1}{2}(p-1)$
B *collection of these* $\frac{1}{2}(p+1),\ \frac{1}{2}(p+3),\ \frac{1}{2}(p+5)\ \ldots.\ p-1$

Take the products of k by the individual numbers in A, and their least positive residues modulo p, which are evidently all distinct and belong partly to A, partly to B. Now if altogether B contains μ of the residues, k will be either a quadratic residue or a quadratic nonresidue of p, according as μ is even or odd.

Proof. Let the residues belonging to A be $a,\ a'\ a''\ \ldots.$, and the remaining ones, belonging to B, be $b, b', b'' \ldots.$. It is clear that the complements of the latter, $p-b, p-b', p-b'' \ldots.$, are all distinct from the numbers $a,\ a',\ a''\ \ldots.$, but together with these fill out the collection A. Thus we have

$$1\,.\,2\,.\,3\ \ldots.\ \tfrac{1}{2}(p-1) = aa'a''\ \ldots.\ (p-b)(p-b')(p-b'')\ \ldots.$$

But the latter product evidently becomes

$$\equiv (-1)^{\mu} aa'a''\ \ldots.\ bb'b''\ \ldots.\ \equiv (-1)^{\mu} k\,.\,2k\,.\,3k\ \ldots.\ \tfrac{1}{2}(p-1)k$$
$$\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}\,1\,.\,2\,.\,3\ \ldots.\ \tfrac{1}{2}(p-1) (\mathrm{mod}.p)$$

Hence we have

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

or $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, according as μ is even or odd; our theorem follows immediately.

4.

We can greatly shorten the following reasoning by introducing some suitable notation. Thus the symbol (k, p) will denote for us the number of products among

$$k,\ 2k,\ 3k\ \ldots.\ \tfrac{1}{2}(p-1)k,$$

whose least positive residues modulo p exceed half of it. Further, when x is any noninteger quantity, we shall use the symbol $[x]$ to denote the integer immediately smaller than x itself, so that $x - [x]$ is always a positive quantity lying between the limits 0 and 1. The following relations are now obtained with little trouble:

I. $[x] + [-x] = -1$.

II. $[x] + h = [x + h]$, whenever h is an integer.

III. $[x] + [h - x] = h - 1$.

IV. If $x - [x]$ is a fraction smaller than $\frac{1}{2}$, then $[2x] - 2[x] = 0$; but if $x - [x]$ is greater than $\frac{1}{2}$, then $[2x] - 2[x] = 1$.

V. Thus, when the least positive residue of the integer h modulo p lies below $\frac{1}{2}p$, we have $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 0$; but when that residue lies above $\frac{1}{2}p$, we have $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 1$.

VI. It follows at once that $(k, p) =$

$$\left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \left[\frac{6k}{p}\right] \ldots. + \left[\frac{(p-1)k}{p}\right]$$
$$- 2\left[\frac{k}{p}\right] - 2\left[\frac{2k}{p}\right] - 2\left[\frac{3k}{p}\right] \ldots. - 2\left[\frac{\frac{1}{2}(p-1)k}{p}\right].$$

VII. From VI and I we obtain without difficulty

$$(k, p) + (-k, p) = \tfrac{1}{2}(p-1)$$

It follows that $-k$ has either the same or the opposite relation to p (insofar as it is a quadratic residue or nonresidue of it) as $+k$, according as p is of the form $4n + 1$ or of the form $4n + 3$. In the former case -1 is evidently a residue, in the latter a nonresidue, of p.

VIII. We shall transform the formula given in VI as follows. By III we have

$$\left[\frac{(p-1)k}{p}\right] = k - 1 - \left[\frac{k}{p}\right],$$
$$\left[\frac{(p-3)k}{p}\right] = k - 1 - \left[\frac{3k}{p}\right],$$
$$\left[\frac{(p-5)k}{p}\right] = k - 1 - \left[\frac{5k}{p}\right] \ldots.$$

Applying these substitutions to the last $\frac{p\mp 1}{4}$ terms of the upper series in that expression, we have

first, whenever p is of the form $4n+1$

$$(k,p) = \tfrac{1}{4}(k-1)(p-1)$$
$$- 2\left\{\left[\frac{k}{p}\right] + \left[\frac{3k}{p}\right] + \left[\frac{5k}{p}\right] \ldots. + \left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\}$$
$$- \left\{\left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] \ldots. + \left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

second, whenever p is of the form $4n+3$

$$(k,p) = \tfrac{1}{4}(k-1)(p+1)$$
$$- 2\left\{\left[\frac{k}{p}\right] + \left[\frac{3k}{p}\right] + \left[\frac{5k}{p}\right] \ldots. + \left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$
$$- \left\{\left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] \ldots. + \left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

IX. For the special case $k = +2$, the formulas just given yield $(2,p) = \frac{1}{4}(p\mp 1)$, taking the upper or lower sign according as p is of the form $4n+1$ or $4n+3$. Thus $(2,p)$ is even, and hence $2Rp$, whenever p is of the form $8n+1$ or $8n+7$; on the other hand, $(2,p)$ is odd and $2Np$, whenever p is of the form $8n+3$ or $8n+5$.

5.

THEOREM. *Let x be a positive noninteger quantity, among whose multiples x, $2x$, $3x \ldots$. up to nx none is an integer; put $[nx] = h$, from which it is easily concluded that among the multiples of the reciprocal quantity $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x} \ldots\ldots$ up to $\frac{h}{x}$ an integer is likewise not found. Then I say that we have*

$$\left.\begin{array}{l} [x] + [2x] + [3x] \,..\, + [nx] \\ + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \left[\frac{3}{x}\right] \ldots. + \left[\frac{h}{x}\right] \end{array}\right\} = nh.$$

Proof. In the series $[x] + [2x] + [3x] \ldots. + [nx]$, which we shall put $= \Omega$, the first terms up to and including the term in position $\left[\frac{1}{x}\right]$ are evidently all $= 0$; the following ones up to the term in position $\left[\frac{2}{x}\right]$ are all $= 1$; the following ones up to the term in position $\left[\frac{3}{x}\right]$ are all $= 2$, and so on. Hence we have

$$\left.\begin{array}{l} \Omega = 0 \times \left[\frac{1}{x}\right] \\ \quad + 1 \times \left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} \\ \quad + 2 \times \left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\} \\ \quad + 3 \times \left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} \\ \qquad \text{etc.} \\ \quad + (h-1) \left\{\left[\frac{h}{x}\right] - \left[\frac{h-1}{x}\right]\right\} \\ \quad + h \left\{n - \left[\frac{h}{x}\right]\right\} \end{array}\right\} = hn - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] \ldots. - \left[\frac{h}{x}\right]$$

Q. E. D.

6.

THEOREM. *If k, p denote any positive odd numbers relatively prime to each other, we have*

$$\left.\begin{aligned}&\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\&+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots.+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{aligned}\right\}=\tfrac{1}{4}(k-1)(p-1).$$

Proof. Supposing, as we may, that $k<p$, we have $\frac{\frac{1}{2}(p-1)k}{p}$ less than $\frac{1}{2}k$, but greater than $\frac{1}{2}(k-1)$, and therefore $\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=\frac{1}{2}(k-1)$. Thus the present theorem evidently follows immediately from the preceding one by putting there $\frac{k}{p}=x$, $\frac{1}{2}(p-1)=n$, and hence $\frac{1}{2}(k-1)=h$.

Moreover, it can be proved in a similar manner that, if k is an *even* number relatively prime to p, we have

$$\left.\begin{aligned}&\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots.+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\&+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots.+\left[\frac{\frac{1}{2}kp}{k}\right]\end{aligned}\right\}=\tfrac{1}{4}k(p-1)$$

But we do not dwell on this proposition, which is not needed for our purpose.

7.

The fundamental theorem now follows immediately by combining the preceding theorem with proposition VIII of Article 4. Namely, if k, p denote any unequal positive prime numbers, and we put

$$(k,p) + \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] \ldots . + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] = L$$

$$(p,k) + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] \ldots . + \left[\frac{\frac{1}{2}(k-1)p}{k}\right] = M$$

it is clear from VIII of Article 4 that L and M are always even numbers. But by the theorem of Article 6 we have

$$L + M = (k,p) + (p,k) + \tfrac{1}{4}(k-1)(p-1)$$

Thus whenever $\frac{1}{4}(k-1)(p-1)$ is even, which happens if either both k, p or at least one of them is of the form $4n+1$, (k,p) and (p,k) must necessarily be either both even or both odd. But whenever $\frac{1}{4}(k-1)(p-1)$ is odd, which happens if both k, p are of the form $4n+3$, one of the numbers (k,p), (p,k) must necessarily be even and the other odd. Thus in the former case the relation of k to p and the relation of p to k (insofar as one is a residue or nonresidue of the other) are identical, and in the latter case opposite.

Q. E. D.

SUMMATION

OF CERTAIN

SPECIAL SERIES

BY

CARL FRIEDRICH GAUSS

PRESENTED TO THE SOCIETY AUGUST XXIV, MDCCCVIII.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. I.
Gottingae MDCCCXI.

SUMMATION

OF CERTAIN SPECIAL SERIES.

1.

Among the more notable truths to which the theory of circle division has opened the way, the summation proposed in Disquiss. Arithmet., Article 356, holds a distinguished place. This is due both to its particular elegance and remarkable fruitfulness, which another investigation will later give us occasion to discuss more fully, and to the unusual difficulties that beset its rigorous and complete proof. These difficulties should have been all the less expected because they concern a certain restriction of the theorem more than the theorem itself: once this restriction is disregarded, a proof is immediately available and follows very easily from the theory developed in that work. The theorem was given there in the following form. Suppose that n is a prime number. Represent all the quadratic residues of n between 1 and $n-1$ inclusive by a, and all the nonresidues between the same limits by b; finally, let ω be the arc $\frac{360^0}{n}$, and k any fixed integer not divisible by n. Then we have

I. for a value of n of the form $4m+1$,

$$\begin{aligned}
\Sigma \cos ak\omega &= -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n} \\
\Sigma \cos bk\omega &= -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ and hence} \\
\Sigma \cos ak\omega - \Sigma \cos bk\omega &= \pm\sqrt{n} \\
\Sigma \sin ak\omega &= 0 \\
\Sigma \sin bk\omega &= 0
\end{aligned}$$

II. for a value of n of the form $4m+3$,

$$\begin{aligned}
\Sigma \cos ak\omega &= -\tfrac{1}{2} \\
\Sigma \cos bk\omega &= -\tfrac{1}{2} \\
\Sigma \sin ak\omega &= \pm\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin bk\omega &= \mp\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin ak\omega - \Sigma \sin bk\omega &= \pm\sqrt{n}
\end{aligned}$$

These summations were proved with full rigor in the place cited, and the only difficulty that remains here is to determine the *sign* to be placed before the radical. It can indeed be shown without difficulty that this sign depends on the number k to the following extent: the *same* sign must hold for all values of k that are quadratic residues of n, and the opposite sign for all values of k

that are quadratic nonresidues of n. Thus the whole question turns on the value $k = 1$: as soon as the sign for this value is known, the signs for all the other values of k are immediately available as well. Yet this very question, which at first seems to be among the easier ones, presents us with unforeseen difficulties, and the method that had guided us this far without impediment utterly refuses any further help.

2.

Before proceeding further, it will be useful to work out some examples of our summation numerically; we should, however, first make a few general observations.

I. In the case where n is a prime number of the form $4m + 1$, let all the quadratic residues of n between 1 and $\frac{1}{2}(n-1)$ inclusive be represented by a', and all the nonresidues between the same limits by b'. All the $n - a'$ are known to be among the a, and all the $n - b'$ among the b. Since all the a', b', $n-a'$, $n-b'$ together evidently make up the entire collection of numbers 1, 2, 3 .... $n-1$, all the a' together with all the $n - a'$ comprise all the a; likewise all the b' together with all the $n - b'$ comprise all the b. Hence

$$\begin{aligned}
\Sigma \cos ak\omega &= \Sigma \cos a'k\omega + \Sigma \cos(n-a')k\omega \\
\Sigma \cos bk\omega &= \Sigma \cos b'k\omega + \Sigma \cos(n-b')k\omega \\
\Sigma \sin ak\omega &= \Sigma \sin a'k\omega + \Sigma \sin(n-a')k\omega \\
\Sigma \sin bk\omega &= \Sigma \sin b'k\omega + \Sigma \sin(n-b')k\omega
\end{aligned}$$

Now, since $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, $\sin(n-b')k\omega = -\sin b'k\omega$, it follows at once that

$$\begin{aligned}
\Sigma \sin ak\omega &= \Sigma \sin a'k\omega - \Sigma \sin a'k\omega = 0 \\
\Sigma \sin bk\omega &= \Sigma \sin b'k\omega - \Sigma \sin b'k\omega = 0
\end{aligned}$$

The summation of the cosines takes the form

$$\begin{aligned}
\Sigma \cos ak\omega &= 2\Sigma \cos a'k\omega \\
\Sigma \cos bk\omega &= 2\Sigma \cos b'k\omega
\end{aligned}$$

so that we must have

$$\begin{aligned}
1 + 4\Sigma \cos a'k\omega &= \pm\sqrt{n} \\
1 + 4\Sigma \cos b'k\omega &= \mp\sqrt{n} \\
2\Sigma \cos a'k\omega - 2\Sigma \cos b'k\omega &= \pm\sqrt{n}
\end{aligned}$$

II. In the case where n is of the form $4m + 3$, the complement of any residue a to n is a nonresidue, and the complement of any b is a residue. Thus all the $n - a$ coincide with all the b, and all the $n - b$ with all the a. This gives

$$\Sigma \cos ak\omega = \Sigma \cos(n - b)k\omega = \Sigma \cos bk\omega$$

Since all the a and b together make up all the numbers 1, 2, $3 \ldots . n - 1$, and hence $\Sigma \cos ak\omega + \Sigma \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \text{etc.} + \cos(n - 1)k\omega = -1$, the summations

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$

follow immediately. Likewise,

$$\Sigma \sin ak\omega = \Sigma \sin(n - b)k\omega = -\Sigma \sin bk\omega$$

which shows how the two summations

$$2\Sigma \sin ak\omega = \pm\sqrt{n}$$
$$2\Sigma \sin bk\omega = \mp\sqrt{n}$$

depend on one another.

3.

Here are the numerical calculations for several examples:

I. For $n = 5$ there is one value of a', namely $a' = 1$, and one value of b', namely $b' = 2$. We have

$$\cos\omega = +0{,}3090169944 \qquad \cos 2\omega = -0{,}8090169944$$

and hence $1 + 4\cos\omega = +\sqrt{5}$, $\quad 1 + 4\cos 2\omega = -\sqrt{5}$.

II. For $n = 13$ there are three values of a', namely 1, 3, 4, and as many values of b', namely 2, 5, 6. We calculate

$\cos\omega$	$= +0{,}8854560257$	$\cos 2\omega$	$= +0{,}5680647467$
$\cos 3\omega$	$= +0{,}1205366803$	$\cos 5\omega$	$= -0{,}7485107482$
$\cos 4\omega$	$= -0{,}3546048870$	$\cos 6\omega$	$= -0{,}9709418174$
Sum	$= +0{,}6513878190$	Sum	$= -1{,}1513878189$

Hence $1 + 4\Sigma \cos a'\omega = +\sqrt{13}$, $\quad 1 + 4\Sigma \cos b'\omega = -\sqrt{13}$.

III. For $n = 17$ we have four values of a', namely 1, 2, 4, 8, and as many values of b', namely 3, 5, 6, 7. The cosines are therefore calculated as follows:

$$\begin{array}{rcl|rcl} \cos\omega &=& +0{,}9324722294 & \cos 3\omega &=& +0{,}4457383558 \\ \cos 2\omega &=& +0{,}7390089172 & \cos 5\omega &=& -0{,}2736629901 \\ \cos 4\omega &=& +0{,}0922683595 & \cos 6\omega &=& -0{,}6026346364 \\ \cos 8\omega &=& -0{,}9829730997 & \cos 7\omega &=& -0{,}8502171357 \\ \hline \text{Sum} &=& +0{,}7807764064 & \text{Sum} &=& -1{,}2807764065 \end{array}$$

Hence $1 + 4\Sigma \cos a'\omega = +\sqrt{17}$, $\quad 1 + 4\Sigma \cos b'\omega = -\sqrt{17}$.

IV. For $n = 3$ there is just one value of a, namely $a = 1$, to which corresponds

$$\sin\omega = +0{,}8660254038$$

Hence $2\sin\omega = +\sqrt{3}$.

V. For $n = 7$ there are three values of a, namely 1, 2, 4. These give the sines

$$\begin{array}{rcl} \sin\omega &=& +0{,}7818314825 \\ \sin 2\omega &=& +0{,}9749279122 \\ \sin 4\omega &=& -0{,}4338837391 \\ \hline \text{Sum} &=& +1{,}3228756556, \end{array}$$ and hence $2\Sigma \sin a\omega = +\sqrt{7}$.

VI. For $n = 11$ the values of a are 1, 3, 4, 5, 9, to which correspond the sines

$$\begin{array}{rcl} \sin\omega &=& +0{,}5406408175 \\ \sin 3\omega &=& +0{,}9898214419 \\ \sin 4\omega &=& +0{,}7557495744 \\ \sin 5\omega &=& +0{,}2817325568 \\ \sin 9\omega &=& -0{,}9096319954 \\ \hline \text{Sum} &=& +1{,}6583123952, \end{array}$$ and hence $2\Sigma \sin a\omega = +\sqrt{11}$.

VII. For $n = 19$ the values of a are 1, 4, 5, 6, 7, 9, 11, 16, 17, to which correspond the sines

$$\begin{aligned}
\sin\omega &= +0{,}3246994692\\
\sin 4\omega &= +0{,}9694002659\\
\sin 5\omega &= +0{,}9965844930\\
\sin 6\omega &= +0{,}9157733267\\
\sin 7\omega &= +0{,}7357239107\\
\sin 9\omega &= +0{,}1645945903\\
\sin 11\omega &= -0{,}4759473930\\
\sin 16\omega &= -0{,}8371664783\\
\sin 17\omega &= -0{,}6142127127\\
\text{Sum} &= +2{,}1794494718,
\end{aligned}$$

and hence $2\Sigma \sin a\omega = +\sqrt{19}$.

4.

In all these examples the radical takes the positive sign. This is also easily confirmed for the larger values $n = 23$, $n = 29$, etc., and already makes it highly probable that the same holds in general. But a proof of this phenomenon cannot be drawn from the principles set out in the place cited, and it must with full justification be regarded as a matter for deeper investigation. The purpose of this paper is therefore to present a rigorous proof of this most elegant theorem, attempted in vain in various ways over several years and finally achieved through unusual and quite subtle considerations. At the same time we shall bring the theorem to a far greater degree of generality, preserving, or rather increasing, its elegance. Finally, as a crowning addition, we shall show the remarkable and very close connection between this summation and another arithmetical theorem of the greatest importance. We hope that these investigations will themselves be welcome to geometers, and that the methods by which we have accomplished all this, and which may also be useful on other occasions, will be considered worthy of their attention.

5.

Our proof comes from considering a special kind of series whose terms depend on expressions such as

$$\frac{(1-x^m)\,(1-x^{m-1})\,(1-x^{m-2})\ldots.(1-x^{m-\mu+1})}{(1-x)\,(1-xx)\,(1-x^3)\ldots..(1-x^\mu)}$$

For brevity we shall denote such a fraction by (m, μ), and first make a few general observations about functions of this kind.

I. Whenever m is a positive integer less than μ, the function (m, μ) evidently vanishes, since the numerator contains the factor $1 - x^0$. For $m = \mu$, the factors in the numerator are identical, in reverse order, to those in the denominator, so that $(\mu, \mu) = 1$. Finally, for the case where m is a positive integer greater than μ, we have the formulas

$$(\mu+1,\mu) = \frac{1-x^{\mu+1}}{1-x} = (\mu+1,1)$$
$$(\mu+2,\mu) = \frac{(1-x^{\mu+2})\,(1-x^{\mu+1})}{(1-x)\qquad(1-xx)} = (\mu+2,2)$$
$$(\mu+3,\mu) = \frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)\qquad(1-xx)\qquad(1-x^3)} = (\mu+3,3) \text{ etc.}$$

or, in general,

$$(m,\mu) = (m, m-\mu)$$

II. Further, it is easily confirmed that in general

$$(m,\mu+1) = (m-1,\mu+1) + x^{m-\mu-1}(m-1,\mu)$$

and since we likewise have

$$(m-1,\mu+1) = (m-2,\mu+1) + x^{m-\mu-2}(m-2,\mu)$$
$$(m-2,\mu+1) = (m-3,\mu+1) + x^{m-\mu-3}(m-3,\mu)$$
$$(m-3,\mu+1) = (m-4,\mu+1) + x^{m-\mu-4}(m-4,\mu), \text{ etc.}$$

and can continue this series as far as

$$\begin{aligned}(\mu+2,\mu+1) &= (\mu+1,\mu+1) + x(\mu+1,\mu)\\ &= (\mu,\mu) + x(\mu+1,\mu)\end{aligned}$$

provided that m is a positive integer greater than $\mu+1$, we obtain

$$\begin{aligned}(m,\mu+1) = (\mu,\mu) &+ x(\mu+1,\mu) + xx(\mu+2,\mu)\\ &+ x^3(\mu+3,\mu) + \text{etc.}\\ &+ x^{m-\mu-1}(m-1,\mu)\end{aligned}$$

This shows that if, for some fixed value of μ, every function (m, μ) is a polynomial whenever m is a positive integer, then every function $(m, \mu + 1)$ must also be a polynomial. Since that supposition holds for $\mu = 1$, it therefore also holds for $\mu = 2$, and hence for $\mu = 3$, etc. That is, in general, for any positive integral value of m, (m, μ) is a polynomial, or equivalently the product

$$(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \dots (1 - x^{m-\mu+1})$$

is divisible by

$$(1 - x)(1 - x^2)(1 - x^3) \dots (1 - x^\mu)$$

6.

We shall now consider two series, both of which can lead to our goal. The first series is

$$1 - \frac{1-x^m}{1-x} + \frac{(1-x^m)\,(1-x^{m-1})}{(1-x)\,(1-xx)} - \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)\quad(1-xx)\quad(1-x^3)} + \text{etc.}$$

or

$$1 - (m,1) + (m,2) - (m,3) + (m,4) - \text{etc.}$$

which for brevity we shall denote by $f(x,m)$. First, it is immediately evident that whenever m is a positive integer this series *terminates* after its term in position $m+1$ (with $= \pm 1$), and that in this case its sum must therefore be a finite polynomial in x. Further, Article 5, II, shows that in general, for any value of m,

$$\begin{aligned} 1 &= 1 \\ -(m,1) &= -(m-1,1) - x^{m-1} \\ +(m,2) &= +(m-1,2) + x^{m-2}(m-1,1) \\ -(m,3) &= -(m-1,3) - x^{m-3}(m-1,2), \text{ etc.} \end{aligned}$$

and hence

$$\begin{aligned} f(x,m) = 1 - x^{m-1} &- (1-x^{m-2})(m-1,1) \\ &+ (1-x^{m-3})(m-1,2) \\ &- (1-x^{m-4})(m-1,3) + \text{etc.} \end{aligned}$$

But evidently

$$\begin{aligned} (1-x^{m-2})(m-1,1) &= (1-x^{m-1})(m-2,1) \\ (1-x^{m-3})(m-1,2) &= (1-x^{m-1})(m-2,2) \\ (1-x^{m-4})(m-1,3) &= (1-x^{m-1})(m-2,3), \text{ etc.} \end{aligned}$$

from which we deduce the equation

$$f(x,m) = (1-x^{m-1})f(x,m-2) \;\ldots\ldots\ldots\; [1]$$

7.

Since for $m = 0$ we have $f(x, m) = 1$, the formula just found gives

$$f(x,2) = 1 - x$$
$$f(x,4) = (1-x)(1-x^3)$$
$$f(x,6) = (1-x)(1-x^3)(1-x^5)$$
$$f(x,8) = (1-x)(1-x^3)(1-x^5)(1-x^7), \text{ etc.}$$

or, in general, for any even value of m,

$$f(x,m) = (1-x)(1-x^3)(1-x^5)\ldots.(1-x^{m-1}) \ldots [2].$$

On the other hand, since for $m = 1$ we have $f(x, m) = 0$, we also have

$$f(x,3) = 0$$
$$f(x,5) = 0$$
$$f(x,7) = 0 \text{ etc.}$$

or, in general, for any odd value of m,

$$f(x,m) = 0$$

The latter summation could, moreover, already have been derived from the fact that in the series

$$1 - (m,1) + (m,2) - (m,3) + \text{etc.} + (m,m-1) - (m,m)$$

the last term cancels the first, the next to last cancels the second, etc.

8.

For our purpose the case where m is a positive odd integer is sufficient. But the unusual nature of the matter makes it worthwhile to add a few remarks about the cases where m is fractional or negative. Our series then evidently no longer terminates, but continues to infinity; it is also easily seen that it becomes divergent whenever x is given a value less than 1, so that its summation must be restricted to values of x greater than 1.

By formula [1] of Article 6 we have

$$f(x,-2) = \frac{1}{1-\frac{1}{x}}$$

$$f(x,-4) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}}$$

$$f(x,-6) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}} \cdot \frac{1}{1-\frac{1}{x^5}}, \text{ etc.}$$

so that the value of the function $f(x,m)$ can also be given in finite terms for a negative even integral value of m. For the remaining values of m, however, we shall convert the function $f(x,m)$ into an *infinite product* as follows.

As m tends to a negative *infinite* value, the function $f(x,m)$ becomes

$$1 + \frac{1}{x-1} + \frac{1}{x-1} \cdot \frac{1}{xx-1} + \frac{1}{x-1} \cdot \frac{1}{xx-1} \cdot \frac{1}{x^3-1} + \text{etc.}$$

This series is therefore equal to the infinite product

$$\frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}} \cdot \frac{1}{1-\frac{1}{x^5}} \cdot \frac{1}{1-\frac{1}{x^7}} \text{ etc. to infinity.}$$

Further, since in general

$$f(x,m) = f(x,m-2\lambda) \,.\, (1-x^{m-1})(1-x^{m-3}) \\ (1-x^{m-5}) \,..\, (1-x^{m-2\lambda+1})$$

we have

$$f(x,m) = f(x,-\infty) \,.\, (1-x^{m-1})(1-x^{m-3})(1-x^{m-5}) \\ \text{etc. to infinity.} \\ = \frac{1-x^{m-1}}{1-x^{-1}} \cdot \frac{1-x^{m-3}}{1-x^{-3}} \cdot \frac{1-x^{m-5}}{1-x^{-5}} \cdot \frac{1-x^{m-7}}{1-x^{-7}} \\ \text{etc. to infinity.}$$

whose factors evidently converge ever more closely to unity as they continue.

The case $m = -1$ deserves particular attention. Here

$$f(x,-1) = 1 + x^{-1} + x^{-3} + x^{-6} + x^{-10} + \text{etc.}$$

This series is therefore equal to the infinite product

$$\frac{1-x^{-2}}{1-x^{-1}} \cdot \frac{1-x^{-4}}{1-x^{-3}} \cdot \frac{1-x^{-6}}{1-x^{-5}} \text{ etc.}$$

or, writing x for x^{-1}, we obtain

$$1+x+x^3+x^6+\text{etc.} = \frac{1-xx}{1-x} \cdot \frac{1-x^4}{1-x^3} \cdot \frac{1-x^6}{1-x^5} \cdot \frac{1-x^8}{1-x^7} \text{ etc.}$$

This equality between two rather intricate expressions, to which we shall return on another occasion, is certainly very remarkable.

9.

Secondly, we shall consider the series

$$1+x^{\frac{1}{2}}\frac{1-x^m}{1-x}+x\frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)} + x^{\frac{3}{2}}\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)}+\text{etc.}$$

or

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+xx(m,4)+\text{etc.}$$

which we shall denote by $F(x,m)$. We restrict this investigation to the case where m is a positive integer, so that this series too always ends at its term in position $m+1$ (with $= x^{\frac{1}{2}m}(m,m)$). Since

$$(m,m)=1, \quad (m,m-1)=(m,1), \quad (m,m-2)=(m,2), \text{ etc.}$$

the series can also be written as follows:

$$F(x,m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m,1) + x^{\frac{1}{2}(m-2)}(m,2) + x^{\frac{1}{2}(m-3)}(m,3)+\text{etc.}$$

This gives

$$\begin{aligned}(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = 1 &+ x^{\frac{1}{2}}(m,1)+x(m,2)\\ &+ x^{\frac{3}{2}}(m,3)+\text{etc.}\\ &+ x^{\frac{1}{2}}\,.\,x^m + x\,.\,x^{m-1}(m,1)\\ &+ x^{\frac{3}{2}}\,.\,x^{m-2}(m,2)+\text{etc.}\end{aligned}$$

Since we have (Article 5, II)

$$\begin{aligned}(m,1)+x^m &= (m+1,1)\\ (m,2)+x^{m-1}(m,1) &= (m+1,2)\\ (m,3)+x^{m-2}(m,2) &= (m+1,3),\ \text{etc.}\end{aligned}$$

we obtain

$$(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = F(x,m+1)\ \ldots\ldots\ [3]$$

But $F(x,0)=1$, so that

$$\begin{aligned}F(x,1) &= 1+x^{\frac{1}{2}}\\ F(x,2) &= (1+x^{\frac{1}{2}})(1+x)\\ F(x,3) &= (1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}}),\ \text{etc.}\end{aligned}$$

or, in general,

$$\begin{aligned}F(x,m) = (1+x^{\frac{1}{2}})&(1+x)(1+x^{\frac{3}{2}})\\ &\ldots.(1+x^{\frac{1}{2}m})\ \ldots.\quad [4]\end{aligned}$$

10.

With these preliminary investigations in place, let us now come closer to our aim. For a prime value of n, the squares 1, 4, $9\ldots.(\frac{1}{2}(n-1))^2$ are all incongruent to one another modulo n; their least residues for this modulus must therefore be identical to the numbers a, and hence

$$\begin{aligned}\Sigma\cos ak\omega &= \cos k\omega+\cos 4k\omega+\cos 9k\omega\\ &\quad+\text{etc.}+\cos(\tfrac{1}{2}(n-1))^2k\omega\\ \Sigma\sin ak\omega &= \sin k\omega+\sin 4k\omega+\sin 9k\omega\\ &\quad+\text{etc.}+\sin(\tfrac{1}{2}(n-1))^2k\omega\end{aligned}$$

Likewise, since the same squares 1, 4, $9\ldots.(\frac{1}{2}(n-1))^2$, in reverse order, are congruent to $(\frac{1}{2}(n+1))^2$, $(\frac{1}{2}(n+3))^2$, $(\frac{1}{2}(n+5))^2\ldots.(n-1)^2$, we also have

$$\begin{aligned}\Sigma\cos ak\omega &= \cos(\tfrac{1}{2}(n+1))^2k\omega\\ &\quad+\cos(\tfrac{1}{2}(n+3))^2k\omega+\text{etc.}+\cos(n-1)^2k\omega\\ \Sigma\sin ak\omega &= \sin(\tfrac{1}{2}(n+1))^2k\omega\\ &\quad+\sin(\tfrac{1}{2}(n+3))^2k\omega+\text{etc.}+\sin(n-1)^2k\omega\end{aligned}$$

Thus, putting

$$\begin{aligned} T &= 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega \\ &\quad + \text{etc.} + \cos(n-1)^2 k\omega \\ U &= \quad \sin k\omega + \sin 4k\omega + \sin 9k\omega \\ &\quad + \text{etc.} + \sin(n-1)^2 k\omega \end{aligned}$$

we obtain

$$\begin{aligned} 1 + 2\Sigma \cos ak\omega &= T \\ 2\Sigma \sin ak\omega &= U \end{aligned}$$

This shows that the summations proposed in Article 1 depend on summing the series T and U. We shall therefore leave the former aside and direct our investigation to these, carrying it out generally enough to include both prime values of n and any composite values. We shall, however, suppose that the number k is relatively prime to n: the case where k and n have a common divisor can be reduced to this one without difficulty.

11.

Let us denote the imaginary quantity $\sqrt{-1}$ by i and put

$$\cos k\omega + i \sin k\omega = r$$

Then $r^n = 1$, or r is a root of the equation $r^n - 1 = 0$. It is easy to see that all the numbers k, $2k$, $3k \ldots . (n-1)k$ are not divisible by n and are incongruent to one another modulo n. Thus the powers of r

$$1,\ r,\ rr,\ r^3 \ldots . r^{n-1}$$

are all unequal, while each also satisfies the equation $x^n - 1 = 0$. For this reason these powers represent *all* the roots of the equation $x^n - 1 = 0$.

These conclusions would not hold if k had a common divisor with n. For if ν were such a common divisor, $k \,.\, \dfrac{n}{\nu}$ would be divisible by n, and hence a power lower than r^n, namely $r^{\frac{n}{\nu}}$, would equal unity. In this case, therefore, the powers of r represent at most $\dfrac{n}{\nu}$ roots of the equation $x^n - 1 = 0$, and indeed give that many distinct roots if ν is the *greatest* common divisor of the numbers k, n. In our case, where k and n are supposed relatively prime, r can conveniently be called a *proper root* of the equation $x^n - 1 = 0$. In the other case, where k and n have a (greatest) common divisor ν, r would be called an *improper root* of that equation. Then, however, the same r would evidently be a proper root of the equation $x^{\frac{n}{\nu}} - 1 = 0$. The simplest improper root is unity, and when n is a prime number there are no other improper roots at all.

12.

Now, if we put

$$W = 1 + r + r^4 + r^9 + \text{etc.} + \text{etc.} + r^{(n-1)^2}$$

we evidently have $W = T + iU$, so that T is the real part of W, and U is obtained from the imaginary part of W by removing the factor i. The whole question is therefore reduced to finding the sum W. For this purpose we can use either the series considered in Article 6 or the one we showed how to sum in Article 9; the former, however, is less suitable when n is even. Nevertheless, we hope that readers will welcome our treating the case where n is odd by two methods.

First, then, suppose that n is an odd number, that r denotes any proper root of the equation $x^n - 1 = 0$, and that in the function $f(x, m)$ we put $x = r$ and $m = n - 1$. We evidently obtain

$$\begin{aligned}
\frac{1 - x^m}{1 - x} &= \frac{1 - r^{-1}}{1 - r} = -r^{-1} \\
\frac{1 - x^{m-1}}{1 - xx} &= \frac{1 - r^{-2}}{1 - rr} = -r^{-2} \\
\frac{1 - x^{m-2}}{1 - x^3} &= \frac{1 - r^{-3}}{1 - r^3} = -r^{-3}, \text{ etc.}
\end{aligned}$$

as far as

$$\frac{1 - x}{1 - x^m} = \frac{1 - r^{-m}}{1 - r^m} = -r^{-m}$$

(It is worth pointing out that these equations hold only insofar as r is supposed to be a proper root: if r were an improper root, the numerator and denominator of some of these fractions would vanish together, and the fractions would therefore become indeterminate).

From this we deduce the following equation

$$\begin{aligned}
f(r, n-1) &= 1 + r^{-1} + r^{-3} + r^{-6} + \text{etc.} + r^{-\frac{1}{2}(n-1)n} \\
&= (1 - r)(1 - r^3)(1 - r^5) \ldots . (1 - r^{n-2})
\end{aligned}$$

The same equation still holds if we replace r by r^λ, where λ denotes any integer relatively prime to n: for then r^λ too is a proper root of the equation $x^n - 1 = 0$. Let us therefore replace r by r^{n-2}, or equivalently r^{-2}. We obtain

$$\begin{aligned}
&1 + r^2 + r^6 + r^{12} + \text{etc.} + r^{(n-1)n} \\
&\quad = (1 - r^{-2})(1 - r^{-6})(1 - r^{-10}) \ldots (1 - r^{-2(n-2)})
\end{aligned}$$

Let us multiply both sides of this equation by

$$r \,.\, r^3 \,.\, r^5 \,.\,.\,.\,. \, r^{(n-2)} = r^{\frac{1}{4}(n-1)^2}$$

and, since

$$\begin{aligned}
r^{2+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-3)^2}, \\
r^{(n-1)n+\frac{1}{4}n-1)^2} &= r^{\frac{1}{4}(n+1)^2} \\
r^{6+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-5)^2}, \\
r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+3)^2} \\
r^{12+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-7)^2}, \\
r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+5)^2}, \text{ etc.}
\end{aligned}$$

the following equation results:

$$\begin{aligned}
&r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \text{etc.} + r + 1 \\
&+ r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} \\
&\qquad + \text{etc.} + r^{\frac{1}{4}(2n-2)^2} \\
&\qquad = (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \,.\,.\,.\,. \, (r^{n-2} - r^{-n+2})
\end{aligned}$$

or, arranging the terms on the left side differently,

$$\begin{aligned}
&1 + r + r^4 + \text{etc.} + r^{(n-1)^2} \\
&\qquad = (r - r^{-1})(r^3 - r^{-3}) \,.\,.\, (r^{n-2} - r^{-n+2}) \quad .. \quad [5]
\end{aligned}$$

13.

The factors on the right side of equation [5] can also be written as follows:

$$r - r^{-1} = -(r^{n-1} - r^{-n+1})$$
$$r^3 - r^{-3} = -(r^{n-3} - r^{-n+3})$$
$$r^5 - r^{-5} = -(r^{n-5} - r^{-n+5}), \text{ etc.}$$

up to

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2})$$

The equation then takes this form:

$$W = (-1)^{\frac{1}{2}(n-1)}(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \\ \ldots . (r^{n-1} - r^{-n+1})$$

Multiplying this equation by [5] in its original form gives

$$W^2 = (-1)^{\frac{1}{2}(n-1)}(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \\ \ldots . (r^{n-1} - r^{-n+1})$$

where $(-1)^{\frac{1}{2}(n-1)}$ is either $= +1$ or $= -1$, according as n is of the form $4\mu + 1$ or of the form $4\mu + 3$. Hence

$$W^2 = \pm r^{\frac{1}{2}n(n-1)}(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \\ \ldots . (1 - r^{-2(n-1)})$$

But it is easy to see that r^{-2}, r^{-4}, $r^{-6} \ldots . r^{-2n+2}$ give all the roots of the equation $x^n - 1 = 0$ except the root $x = 1$. The following identity must therefore hold for an indeterminate:

$$(x - r^{-2})(x - r^{-4})(x - r^{-6}) \ldots . (x - r^{-2n+2}) \\ = x^{n-1} + x^{n-2} + x^{n-3} + \text{etc.} + x + 1$$

Thus, putting $x = 1$, we obtain

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \ldots . (1 - r^{-2n+2}) = n$$

and since evidently $r^{\frac{1}{2}n(n-1)} = 1$, our equation becomes

$$W^2 = \pm n \ldots . \ldots . \ldots . [6]$$

Thus, in the case where n is of the form $4\mu + 1$, we have

$$W = \pm\sqrt{n}, \quad \text{and hence} \quad T = \pm\sqrt{n}, \quad U = 0$$

In the other case, where n is of the form $4\mu + 3$, we instead have

$$W = \pm i\sqrt{n}, \quad \text{and so} \quad T = 0, \quad U = \pm\sqrt{n}$$

14.

The method of the preceding article gives only the absolute value of the sums T, U, and leaves it uncertain whether T in the first case and U in the second should be set $= +\sqrt{n}$ or $= -\sqrt{n}$. But, at least for the case where $k = 1$, this can be decided from equation [5] as follows. Since, for $k = 1$,

$$\begin{aligned} r - r^{-1} &= 2i \sin \omega \\ r^3 - r^{-3} &= 2i \sin 3\omega \\ r^5 - r^{-5} &= 2i \sin 5\omega \text{ etc.} \end{aligned}$$

that equation becomes

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega$$

Now, in the case where n is of the form $4\mu+1$, the sequence of odd numbers

$$1,\ 3,\ 5,\ 7 \ldots . \tfrac{1}{2}(n-3), \quad \tfrac{1}{2}(n+1) \ldots . (n-2)$$

contains $\frac{1}{4}(n-1)$ numbers smaller than $\frac{1}{2}n$, to which positive sines evidently correspond. The remaining $\frac{1}{4}(n-1)$, on the other hand, are greater than $\frac{1}{2}n$, and negative sines correspond to them. The product of all the sines must therefore equal a positive quantity multiplied by $(-1)^{\frac{1}{4}(n-1)}$. Thus W will equal a positive real quantity multiplied by i^{n-1}, or by 1, since $i^4 = 1$ and $n-1$ is divisible by 4: that is, W will be real and positive. Hence we must have

$$W = +\sqrt{n}, \quad T = +\sqrt{n}$$

In the other case, where n is of the form $4\mu + 3$, in the sequence of odd numbers

$$1,\ 3,\ 5,\ 7 \ldots . \tfrac{1}{2}(n-1), \quad \tfrac{1}{2}(n+3) \ldots . (n-2)$$

the first $\frac{1}{4}(n+1)$ will be smaller than $\frac{1}{2}n$, but the remaining $\frac{1}{4}(n-3)$ will be greater. Thus, among the sines of the arcs ω, 3ω, $5\omega \ldots . (n-2)\omega$, there will be $\frac{1}{4}(n-3)$ negative ones, and so W will be the product of $i^{\frac{1}{2}(n-1)}$, a positive real quantity and $(-1)^{\frac{1}{4}(n-3)}$. The third factor is $= i^{\frac{1}{2}(n-3)}$, which, multiplied by the first, gives $i^{n-2} = i$, since $i^{n-3} = 1$. We must therefore have

$$W = +i\sqrt{n}, \quad \text{and} \quad U = +\sqrt{n}$$

15.

We shall now show how the same conclusions can be derived from the series considered in Article 9. In equation [4], replace $x^{\frac{1}{2}}$ by $-y^{-1}$; we then obtain

$$1 - y^{-1}\frac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\frac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} - y^{-3}\frac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+4})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \text{etc.}$$

up to the term in position $m+1$

$$= (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4}) \ldots (1 \pm y^{-m}) \ldots . \text{ [7]}$$

If we take for y a proper root of the equation $y^n - 1 = 0$, say r, and at the same time put $m = n-1$, we obtain

$$\frac{1-y^{-2m}}{1-y^{-2}} = \frac{1-r^2}{1-r^{-2}} = -r^2$$
$$\frac{1-y^{-2m+2}}{1-y^{-4}} = \frac{1-r^4}{1-r^{-4}} = -r^4$$
$$\frac{1-y^{-2m+4}}{1-y^{-6}} = \frac{1-r^6}{1-r^{-6}} = -r^6$$

up to

$$\frac{1-y^{-2}}{1-y^{-2m}} = \frac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2}$$

Here we should note that none of the denominators $1-r^{-2}$, $1-r^{-4}$, etc. becomes $= 0$. Equation [7] therefore takes this form:

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = (1-r^{-1})(1+r^{-2})(1-r^{-3}) \ldots . (1+r^{-n+1})$$

Multiplying, on the right side of this equation, the first term by the last, the second by the next to last, etc., we obtain

$$(1-r^{-1})(1+r^{-n+1}) = r - r^{-1}$$
$$(1+r^{-2})(1-r^{-n+2}) = r^{n-2} - r^{-n+2}$$
$$(1-r^{-3})(1+r^{-n+3}) = r^3 - r^{-3}$$
$$(1+r^{-4})(1-r^{-n+4}) = r^{n-4} - r^{-n+4} \text{ etc.}$$

It is easy to see that these partial products combine to form the product

$$(r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \\ \ldots . (r^{n-4} - r^{-n+4})(r^{n-2} - r^{-n+2})$$

which will therefore be

$$= 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = W$$

This equation is identical with equation [5], derived in Article 12 from the first series; the remaining arguments are then established in the same way as in Articles 13 and 14.

16.

We turn to the other case, where n is an even number. First let n be of the form $4\mu + 2$, or twice an odd number. It is clear that the numbers $\frac{1}{4}nn$, $(\frac{1}{2}n + 1)^2 - 1$, $(\frac{1}{2}n + 2)^2 - 4$, etc., or in general $(\frac{1}{2}n + \lambda)^2 - \lambda\lambda$, give odd quotients when divided by $\frac{1}{2}n$, and are therefore congruent, modulo n, to $\frac{1}{2}n$. It follows that, if r is a proper root of the equation $x^n - 1 = 0$, and hence $r^{\frac{1}{2}n} = -1$, we have

$$\begin{aligned} r^{(\frac{1}{2}n)^2} &= -1 \\ r^{(\frac{1}{2}n+1)^2} &= -r \\ r^{(\frac{1}{2}n+2)^2} &= -r^4 \\ r^{(\frac{1}{2}n+2)^2} &= -r^9 \text{ etc.} \end{aligned}$$

Thus, in the series

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ cancels the first, the next cancels the second, etc., so that

$$W = 0, \quad T = 0, \quad U = 0$$

17.

The case remains where n is of the form 4μ, or divisible by four. Here, in general, $(\frac{1}{2}n+\lambda)^2 - \lambda\lambda$ is divisible by n, and therefore

$$r^{(\frac{1}{2}n+\lambda)^2} = r^{\lambda\lambda}$$

Thus, in the series

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ equals the first, the next equals the second, etc., so that

$$W = 2(1 + r + r^4 + r^9 + \text{etc.} + r^{(\frac{1}{2}n-1)^2})$$

Now suppose that in equation [7] of Article 15 we put $m = \frac{1}{2}n - 1$, and take for y a proper root of the equation $y^n - 1 = 0$, say r. Then, just as in Article 15, the equation takes the following form:

$$\begin{aligned} &1 + r + r^4 + \text{etc.} + r^{(\frac{1}{2}n-1)^2} \\ &\quad = (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots . (1 - r^{-\frac{1}{2}n+1}) \end{aligned}$$

or

$$\begin{aligned} W = 2(1 - r^{-1})(1 + r^{-2})(1 - r^{-3})(1 + r^{-4}) \\ \ldots (1 - r^{-\frac{1}{2}n+1}) \quad .. \quad [8] \end{aligned}$$

Further, since $r^{\frac{1}{2}n} = -1$, and therefore

$$\begin{aligned} 1 + r^{-2} &= -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2}) \\ 1 + r^{-4} &= -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4}) \\ 1 + r^{-6} &= -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6}) \text{ etc.} \end{aligned}$$

and the product of the factors $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-4}$, $-r^{\frac{1}{2}n-6}$, etc., up to $-r^2$ is $= (-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}$, the preceding equation can also be written as

$$\begin{aligned} W = 2(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}(1 - r^{-1})(1 - r^{-2}) \\ (1 - r^{-3})(1 - r^{-4}) \ldots . (1 - r^{-\frac{1}{2}n+1}) \end{aligned}$$

Since we have

$$1 - r^{-1} = -r^{-1}(1 - r^{-n+1})$$
$$1 - r^{-2} = -r^{-2}(1 - r^{-n+2})$$
$$1 - r^{-3} = -r^{-3}(1 - r^{-n+3}) \text{ etc.}$$

we obtain

$$(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots (1 - r^{-\frac{1}{2}n+1})$$
$$= (-1)^{\frac{1}{2}n-1} r^{-\frac{1}{8}nn+\frac{1}{4}n}(1 - r^{-\frac{1}{2}n-1})$$
$$(1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1})$$

and hence

$$W = 2(-1)^{\frac{3}{4}n-2} r^{-\frac{1}{16}nn}(1 - r^{-\frac{1}{2}n-1})$$
$$(1 - r^{-\frac{1}{2}n-2})(1 - r^{-\frac{1}{2}n-3}) \dots . (1 - r^{-n+1})$$

Multiplying this value of W by the one found earlier, and introducing the factor $1 - r^{-\frac{1}{2}n}$ on both sides, gives

$$(1 - r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3} r^{-\frac{1}{4}n}(1 - r^{-1}.)$$
$$(1 - r^{-2})(1 - r^{-3}) \dots . (1 - r^{-n+1})$$

But we have

$$1 - r^{-\frac{1}{2}n} = 2$$
$$(-1)^{n-3} = -1$$
$$r^{-\frac{1}{4}n} = -r^{\frac{1}{4}n}$$

$$(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots . (1 - r^{-n+1}) = n$$

From this we finally conclude

$$W^2 = 2r^{\frac{1}{4}n} n \text{ . . . . . [9]}$$

Now it is easy to see that $r^{\frac{1}{4}n}$ is either $= +i$ or $= -i$, according as k is of the form $4\mu + 1$ or of the form $4\mu + 3$. And since

$$2i = (1 + i)^2, \quad -2i = (1 - i)^2$$

in the case where k is of the form $4\mu + 1$, we have

$$W = \pm(1 + i)\sqrt{n}, \quad \text{and so} \quad T = U = \pm\sqrt{n}$$

but in the other case, where k is of the form $4\mu + 3$,

$$W = \pm(1-i)\sqrt{n}, \quad \text{and so} \quad T = -U = \pm\sqrt{n}$$

18.

The method of the preceding article supplied the absolute values of the functions T, U, and specified the conditions under which they must be given equal or opposite signs; but it does not yet determine the signs themselves. For the case where $k = 1$, we shall supply what is missing as follows.

Let us put $\rho = \cos\frac{1}{2}\omega + i\sin\frac{1}{2}\omega$, so that $r = \rho\rho$. Since $\rho^n = -1$, it is clear that equation [8] can be written as

$$W = 2(1+\rho^{n-2})(1+\rho^{-4})(1+\rho^{n-6})(1+\rho^{-8})$$
$$\ldots(1+\rho^{-n+4})(1+\rho^2)$$

or, with the factors arranged in a different order,

$$W = 2(1+\rho^2)(1+\rho^{-4})(1+\rho^6)(1+\rho^{-8})$$
$$\ldots(1+\rho^{-n+4})(1+\rho^{n-2})$$

Now we have

$$1+\rho^2 = 2\rho\cos\frac{1}{2}\omega$$
$$1+\rho^{-4} = 2\rho^{-2}\cos\omega$$
$$1+\rho^{-6} = 2\rho^3\cos\frac{3}{2}\omega$$
$$1+\rho^{-8} = 2\rho^{-4}\cos 2\omega, \text{ etc.}$$

up to

$$1+\rho^{-n+4} = 2\rho^{-\frac{1}{2}n+2}, \cos(\frac{1}{4}n-1)\omega$$
$$1+\rho^{n-2} = 2\rho^{\frac{1}{2}n-1}\cos(\frac{1}{4}n-\frac{1}{2})\omega$$

Thus we have

$$W = 2^{\frac{1}{2}n}\rho^{\frac{1}{4}n}\cos\frac{1}{2}\omega\cos\omega\,\frac{3}{2}\omega$$
$$\ldots.\cos(\frac{1}{4}n-\frac{1}{2})\omega$$

The cosines entering this product are evidently all positive, while the factor $\rho^{\frac{1}{4}n}$ is $= \cos 45^0 + i \sin 45^0 = (1+i)\sqrt{\frac{1}{2}}$. From this we conclude that W is the product of $1+i$ and a positive real quantity, so that necessarily

$$W = (1+i)\sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}$$

19.

It will be worthwhile to collect all the summations developed so far into a single overview here. In general, we have

$T =$	$U =$	for n of the form
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

and, when we set $k = 1$, the radical must be given the positive sign. What we observed by induction in Article 3 for prime values of n has therefore now been proved with full rigor. Nothing remains except to show how to determine the signs in every case, for any values of k. But before we can tackle this task in full generality, we must first consider more closely the cases where n is a prime number or a power of a prime number.

20.

First let n be an odd prime number. From what we set out in Article 10, it is clear that $W = 1 + 2\Sigma r^a = 1 + 2\Sigma R^{ak}$ if we put $R = \cos\omega + i\sin\omega$, with a, as there, denoting indefinitely all the quadratic residues of n lying between 1 and $n-1$. If we likewise use b to denote indefinitely all the quadratic nonresidues between the same limits, we readily see that all the numbers ak are congruent modulo n either to all the a or to all the b (without regard to order), according as k is a residue or a nonresidue. Thus, in the first case, we have

$$W = 1 + 2\Sigma R^a = 1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2}$$

and hence $W = +\sqrt{n}$ if n is of the form $4\mu+1$, and $W = +i\sqrt{n}$ if n is of the form $4\mu+3$.

In the other case, where k is a nonresidue of n, we have

$$W = 1 + 2\Sigma R^b$$

Since all the a, b evidently make up the complete collection of numbers 1, 2, 3 …, and therefore

$$\Sigma R^a + \Sigma R^b = R + R^2 + R^3 + \text{etc.} + R^{n-1} = -1$$

we obtain

$$W = -1 - 2\Sigma R^a = -(1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2})$$

and hence $W = -\sqrt{n}$ if n is of the form $4\mu + 1$, and $W = -i\sqrt{n}$ if n is of the form $4\mu + 3$.

From this we conclude:

first, if n is of the form $4\mu + 1$ and k is a quadratic residue of n,

$$T = +\sqrt{n}, \quad U = 0$$

second, if n is of the form $4\mu + 1$ and k is a nonresidue of n,

$$T = -\sqrt{n}, \quad U = 0$$

third, if n is of the form $4\mu + 3$ and k is a residue of n,

$$T = 0, \quad U = +\sqrt{n}$$

fourth, if n is of the form $4\mu + 3$ and k is a nonresidue of n,

$$T = 0, \quad U = -\sqrt{n}$$

21.

Second, let n be the square or a higher power of an odd prime number p, and put $n = p^{2\varkappa}q$, with q either $= 1$ or $= p$. Here we should first note that, if λ is any integer not divisible by $p^{\varkappa}$, we have

$$\begin{aligned} & r^{\lambda\lambda} + r^{(\lambda+p^{\varkappa}q)^2} + r^{(\lambda+2p^{\varkappa}q)^2} + r^{(\lambda+3p^{\varkappa}q)^2} \\ & \quad + \text{etc.} + r^{(\lambda+n-p^{\varkappa}q)^3} \\ & = r^{\lambda\lambda}\{1 + r^{2\lambda p^{\varkappa}q} + r^{4\lambda p^{\varkappa}q} \\ & \quad + r^{6\lambda p^{\varkappa}q} + \text{etc.} + r^{2\lambda(n-p^{\varkappa}q)}\} \\ & = \frac{r^{\lambda\lambda}(1 - r^{2\lambda n})}{1 - r^{2\lambda p^{\varkappa}q}} = 0 \end{aligned}$$

It is then easy to see that

$$W = 1 + r^{p^{2\varkappa}} + r^{4p^{2\varkappa}} + r^{9p^{2\varkappa}} + \text{etc.} + r^{(n-p^{\varkappa})^2}$$

For the remaining terms of the series

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

can be divided into $(p^\varkappa - 1)q$ partial series, each with $p^\varkappa$ terms, whose sums vanish under the transformation just given.

It follows that in the case where $q = 1$, or where n is a power of a prime number with an even exponent, we have

$$W = p^\varkappa = +\sqrt{n}, \text{ and so } T = +\sqrt{n}, \quad U = 0$$

In the other case, where $q = p$, or where n is a power of a prime number with an odd exponent, we shall put $r^{p^{2\varkappa}} = \rho$. Then ρ is a proper root of the equation $x^p - 1 = 0$, namely $\rho = \cos \frac{k}{p} 360^0 + i \sin \frac{k}{p} 360^0$, and we obtain

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p^{\varkappa+1}-1)^2} \\ &= p^\varkappa (1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p-1)^2}) \end{aligned}$$

But the sum of the series $1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p-1)^2}$ is determined by the preceding article. It follows directly that

$$\begin{aligned} W &= \pm\sqrt{n} = T, \quad \text{if } p \text{ is of the form } 4\mu + 1 \\ W &= \pm i\sqrt{n} = iU, \quad \text{if } p \text{ is of the form } 4\mu + 3 \end{aligned}$$

with the positive or negative sign, according as k is a residue or a nonresidue of p.

22.

What we set out in Articles 20 and 21 also readily gives the following proposition, which will be of considerable use to us below. Put

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

with h denoting any integer not divisible by p. Then, in the case where $n = p$, or where n is a power of p with an odd exponent, we have

$$\begin{aligned} W' &= W, \text{ if } h \text{ is a quadratic residue of } p \\ W' &= -W, \text{ if } h \text{ is a quadratic nonresidue of } p \end{aligned}$$

For W' evidently arises from W if, for k, we substitute kh. In the first case, k and kh are alike, and in the second they are unlike, with respect to being residues or nonresidues of p.

But in the case where n is a power of p with an even exponent, we evidently have $W' = +\sqrt{n}$, and therefore always $W' = W$.

23.

In Articles 20, 21 and 22 we considered odd prime numbers and powers of such numbers. The case therefore remains where n is a power of two.

For $n = 2$, we evidently have $W = 1 + r = 0$.

For $n = 4$, we obtain $W = 1 + r + r^4 + r^9 = 2 + 2r$. Thus $W = 2 + 2i$ whenever k is of the form $4\mu + 1$, and $W = 2 - 2i$ whenever k is of the form $4\mu + 3$.

For $n = 8$, we have $W = 1+r+r^4+r^9+r^{16}+r^{25}+r^{36}+r^{49} = 2+4r+2r^4 = 4r$. Hence

$$\begin{aligned} W &= (1+i)\sqrt{8}, \quad \text{whenever } k \text{ is of the form } 8\mu+1 \\ W &= (-1+i)\sqrt{8}, \quad \text{whenever } k \text{ is of the form } 8\mu+3 \\ W &= (-1-i)\sqrt{8}, \quad \text{whenever } k \text{ is of the form } 8\mu+5 \\ W &= (1-i)\sqrt{8}, \quad \text{whenever } k \text{ is of the form } 8\mu+7 \end{aligned}$$

If n is a higher power of two, put $n = 2^{2\varkappa}q$, with q either $= 1$ or $= 2$, and $\varkappa$ greater than 1. Here we must first observe that, if λ is any integer not divisible by $2^{\varkappa-1}$, we have

$$\begin{aligned} & r^{\lambda\lambda} + r^{(\lambda+2^{\varkappa}q)^2} + r^{(\lambda+2.2^{\varkappa}q)^2} + r^{(\lambda+3.2^{\varkappa}q)^2} \\ & \quad + \text{etc.} + r^{(\lambda+n-2^{\varkappa}q)^2} \\ & = r^{\lambda\lambda}\{1 + r^{2^{\varkappa+1}\lambda q} + r^{2.2^{\varkappa+1}\lambda q} \\ & \quad + r^{3.2^{\varkappa+1}\lambda q} + \text{etc.} + r^{(2n-2^{\varkappa+1}q)\lambda}\} \\ & = \frac{r^{\lambda\lambda}(1 - r^{2\lambda n})}{1 - r^{2^{\varkappa+1}\lambda q}} = 0 \end{aligned}$$

It is then easy to see that

$$W = 1 + r^{2^{2\varkappa-2}} + r^{4.2^{2\varkappa-2}} + r^{9.2^{2\varkappa-2}} + \text{etc.} + r^{(n-2^{\varkappa-1})^2}$$

Put $r^{2^{2\varkappa-2}} = \rho$. Then ρ is a root of the equation $x^{4q} - 1 = 0$, namely $\rho = \cos\frac{k}{4q}360^0 + i\sin\frac{k}{4q}360^0$; we then obtain

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(2^{\varkappa+1}q-1)^2} \\ &= 2^{\varkappa-1}(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}) \end{aligned}$$

But the sum of the series $1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}$ is determined by what we explained for the cases $n = 4$, $n = 8$. From this we conclude

that in the case where $q = 1$, or where n is a power of the number 4, we have

$$W = (1+i)2^{\varkappa} = (1+i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 4\mu+1$$
$$W = (1-i)2^{\varkappa} = (1-i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 4\mu+3$$

these are exactly the formulas given for $n = 4$;

but in the case where $q = 2$, or where n is a power of two with an odd exponent greater than 3, we have

$$W = (1+i)2^{\varkappa}\sqrt{2} = (1+i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 8\mu+1$$
$$W = (-1+i)2^{\varkappa}\sqrt{2} = (-1+i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 8\mu+3$$
$$W = (-1-i)2^{\varkappa}\sqrt{2} = (-1-i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 8\mu+5$$
$$W = (1-i)2^{\varkappa}\sqrt{2} = (1-i)\sqrt{n}, \quad \text{if } k \text{ is of the form } 8\mu+7$$

these too agree exactly with those we gave for $n = 8$.

24.

Here too it will be worthwhile to determine the ratio of the sum of the series

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

to W, where h denotes any odd integer. Since W' arises from W by changing k into kh, the value of W' depends on the form of the number kh in the same way as W depends on the form of k. Put $\frac{W'}{W} = l$. It is clear that

I. in the case where $n = 4$, or it is a higher power of two with an even exponent, we have

$$l = 1, \quad \text{if } h \text{ is of the form } 4\mu+1$$
$$l = -i, \quad \text{if } h \text{ is of the form } 4\mu+3, \text{ and } k \text{ is of the form } 4\mu+1$$
$$l = +i, \quad \text{if } h \text{ is of the form } 4\mu+3, \text{ and } k \text{ is of the same form.}$$

II. in the case where $n = 8$, or it is a higher power of two with an odd exponent, we have

$l = 1$, if h is of the form $8\mu + 1$,
$l = -1$, if h is of the form $8\mu + 5$,
$l = +i$, if either h is of the form $8\mu + 3$, and k is of the form $4\mu + 1$,
or h is of the form $8\mu + 7$, and k is of the form $4\mu + 3$,
$l = -i$, if either h is of the form $8\mu + 3$, and k is of the form $4\mu + 3$,
or h is of the form $8\mu + 7$, and k is of the form $4\mu + 1$.

The preceding articles have completely determined the sum W for the cases where n is a prime number or a power of a prime number. It therefore remains to complete the cases where n is composed of several prime numbers; the following theorem will prepare the way for us:

25.

THEOREM. *Let n be the product of two coprime positive integers a, b, and put*

$$P = 1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b-1)^2 aa}$$
$$Q = 1 + r^{bb} + r^{4bb} + r^{9bb} + \text{etc.} + r^{(a-1)^2 bb}$$

Then I claim that $W = PQ$.

Proof. Let α denote indefinitely the numbers $0, 1, 2, 3 \ldots . a - 1$, β the numbers $0, 1, 2, 3 \ldots . b - 1$, and ν the numbers $0, 1, 2, 3 \ldots . n - 1$. Then evidently

$$P = \Sigma r^{aa\beta\beta}, \quad Q = \Sigma r^{bb\alpha\alpha}, \quad W = \Sigma r^{\nu\nu}$$

Thus $PQ = \Sigma r^{aa\beta\beta + bb\alpha\alpha}$, on substituting all the values of α and β, combined with one another in every way. Further, since $2ab\alpha\beta = 2\alpha\beta n$, we have $PQ = \Sigma r^{(a\beta + b\alpha)^2}$. But it is easy to see that the individual values of $a\beta + b\alpha$ are different from one another and equal to some value of ν. Hence $PQ = \Sigma r^{\nu\nu} = W$.

It should also be noted that r^{aa} is a proper root of the equation $x^b - 1 = 0$, and r^{bb} a proper root of the equation $x^a - 1 = 0$.

26.

Now let n be the product of three pairwise coprime numbers a, b, c. It is clear that, on putting $bc = b'$, a and b' will also be coprime; hence W is the product of the two factors

$$1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b'-1)^2 aa}$$
$$1 + r^{b'b'} + r^{4b'b'} + r^{9b'b'} + \text{etc.} + r^{(a-1)^2 b'b'}$$

But since r^{aa} is a proper root of the equation $x^{bc} - 1 = 0$, the first factor itself will be the product of

$$1 + \rho^{bb} + \rho^{4bb} + \rho^{9bb} + \text{etc.} + \rho^{(c-1)^2 bb}$$
$$1 + \rho^{cc} + \rho^{4cc} + \rho^{9cc} + \text{etc.} + \rho^{(b-1)^2 cc}$$

if we put $r^{aa} = \rho$. It is therefore clear that W is the product of the three factors

$$1 + r^{bbcc} + r^{4bbcc} + r^{9bbcc} + \text{etc.} + r^{(a-1)^2 bbcc}$$
$$1 + r^{aacc} + r^{4aacc} + r^{9aacc} + \text{etc.} + r^{(b-1)^2 aacc}$$
$$1 + r^{aabb} + r^{4aabb} + r^{9aabb} + \text{etc.} + r^{(c-1)^2 aabb}$$

where r^{bbcc}, r^{aacc}, r^{aabb} are respectively proper roots of the equations $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$.

27.

It is easy to conclude in general that, if n is the product of any number of pairwise coprime factors a, b, c, etc., W is the product of the same number of factors, namely

$$1 + r^{\frac{nn}{aa}} + r^{\frac{4nn}{aa}} + r^{\frac{9nn}{aa}} + \text{etc.} + r^{\frac{(a-1)^2 nn}{aa}}$$
$$1 + r^{\frac{nn}{bb}} + r^{\frac{4nn}{bb}} + r^{\frac{9nn}{bb}} + \text{etc.} + r^{\frac{(b-1)^2 nn}{bb}}$$
$$1 + r^{\frac{nn}{cc}} + r^{\frac{4nn}{cc}} + r^{\frac{9nn}{cc}} + \text{etc.} + r^{\frac{(c-1)^2 nn}{cc}}, \text{ etc.}$$

where $r^{\frac{nn}{aa}}$, $r^{\frac{nn}{bb}}$, $r^{\frac{nn}{cc}}$, etc. are proper roots of the equations $x^a - 1 = 0$, $x^b - 1 = 0$. $x^c - 1 = 0$, etc.

28.

These principles now make the transition to a complete determination of W for any value of n immediately clear. Specifically, resolve n into factors a, b, c, etc., that are either distinct prime numbers or powers of distinct prime numbers, and put $r^{\frac{nn}{aa}} = A$, $r^{\frac{nn}{bb}} = B$, $r^{\frac{nn}{cc}} = C$, etc. Then A, B, C, etc. will be proper roots of the equations $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$, etc., and W the product of the factors

$$1 + A + A^4 + A^9 + \text{etc.} + A^{(a-1)^2}$$
$$1 + B + B^4 + B^9 + \text{etc.} + B^{(b-1)^2}$$
$$1 + C + C^4 + C^9 + \text{etc.} + C^{(c-1)^2}$$

Each of these factors can be determined from what we showed in Articles $20, 21, 23$, so the value of the product will also become known. It will be useful to collect the rules for determining these factors in a single overview here. Since the root A is $= \frac{kn}{a} . \frac{360^0}{a}$, the sum $1 + A + A^4 + A^9 + \text{etc.} + A^{(a-1)^2}$, which we shall denote by L, will be determined by the number $\frac{kn}{a}$ in the same way as W is determined by k in our general investigation. Twelve cases must now be distinguished.

I. If a is a prime number of the form $4\mu + 1$, say $= p$, or a power of such a prime number with an odd exponent, and $\frac{kn}{a}$ is a quadratic residue of p, then $L = +\sqrt{a}$.

II. If the other conditions remain unchanged and $\frac{kn}{a}$ is a quadratic nonresidue of p, then $L = -\sqrt{a}$.

III. If a is a prime number of the form $4\mu + 3$, say $= p$, or a power of such a prime number with an odd exponent, and $\frac{kn}{a}$ is a quadratic residue of p, then $L = +i\sqrt{a}$.

IV. If, with the other conditions as in III, $\frac{kn}{a}$ is a quadratic nonresidue of p, then $L = -i\sqrt{a}$.

V. If a is the square, or a higher power with an even exponent, of an (odd) prime number, then $L = +\sqrt{a}$.

VI. If $a = 2$, then $L = 0$.

VII. If $a = 4$, or it is a higher power of two with an even exponent, and $\frac{kn}{a}$ is of the form $4\mu + 1$, then $L = (1 + i)\sqrt{a}$.

VIII. If, with the other conditions as in VII, $\frac{kn}{a}$ is of the form $4\mu + 3$, then $L = (1 - i)\sqrt{a}$.

IX. If $a = 8$, or it is a higher power of two with an odd exponent, and $\frac{kn}{a}$ is of the form $8\mu + 1$, then $L = (1 + i)\sqrt{a}$.

X. If, with the other conditions as in IX, $\frac{kn}{a}$ is of the form $8\mu + 3$, then $L = (-1 + i)\sqrt{a}$.

XI. If the other conditions remain unchanged and $\frac{kn}{a}$ is of the form $8\mu + 5$, then $L = (-1 - i)\sqrt{a}$.

XII. If the other conditions remain unchanged and $\frac{kn}{a}$ is of the form $8\mu+7$, then $L = (1-i)\sqrt{a}$.

29.

For example, let $n = 2520 = 8 \,.\, 9 \,.\, 5 \,.\, 7$ and $k = 13$. Here we obtain

for $a = 8$, by case XII, $L = (1-i)\sqrt{8}$
for the factor 9, by case V, the corresponding sum is $= \sqrt{9}$
for the factor 5, by case II, the corresponding sum is $= -\sqrt{5}$
for the factor 7, by case III, the corresponding sum is $= +i\sqrt{7}$.

Thus $W = (1-i) \,.\, (-i) \,.\, \sqrt{2520} = (-1-i)\sqrt{2520}$.
For the same value of n, let $k = 1$; then the corresponding sums are

for the factor 8 the sum $(-1+i)\sqrt{8}$
for the factor 9 the sum $\sqrt{9}$
for the factor 5 the sum $\sqrt{5}$
for the factor 7 the sum $-i\sqrt{7}$

This gives the product $W = (1+i)\sqrt{2520}$.

30.

Another method for determining the sum W in general follows from what we set out in Articles 22. 24. Put $\cos\omega + i\sin\omega = \rho$, and

$$\rho^{\frac{nn}{aa}} = \alpha, \quad \rho^{\frac{nn}{bb}} = \beta, \quad \rho^{\frac{nn}{cc}} = \gamma \text{ etc.}$$

so that $r = \rho^k$, $A = \alpha^k$, $B = \beta^k$, $C = \gamma^k$ etc. Then

$$1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(n-1)^2}$$

is the product of the factors

$$1 + \alpha + \alpha^4 + \alpha^9 + \text{etc.} + \alpha^{(a-1)^2}$$
$$1 + \beta + \beta^4 + \beta^9 + \text{etc.} + \beta^{(b-1)^2}$$
$$1 + \gamma + \gamma^4 + \gamma^9 + \text{etc.} + \gamma^{(c-1)^2}, \text{ etc.}$$

and therefore W is the product of the factors

$$w = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(n-1)^2}$$

$$\mathfrak{A} = \frac{1 + A + A^4 + A^9 + \text{etc.} + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \text{etc.} + \alpha^{(a-1)^2}}$$

$$\mathfrak{B} = \frac{1 + B + B^4 + B^9 + \text{etc.} + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \text{etc.} + \beta^{(b-1)^2}}$$

$$\mathfrak{C} = \frac{1 + C + C^4 + C^9 + \text{etc.} + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \text{etc.} + \gamma^{(c-1)^2}}$$

The first factor w has already been determined by the investigations given above (Article 19); the remaining factors $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. follow from the formulas of Articles 22. 24, which we collect here again to have everything together[*]. Twelve cases must be distinguished here, namely

I. If a is an (odd) prime number $= p$, or a power of such a number with an odd exponent, and k is a quadratic residue of p, the corresponding factor is $\mathfrak{A} = +1$.

II. If the other conditions remain unchanged and k is a quadratic non-residue of p, then $\mathfrak{A} = -1$.

III. If a is the square of an odd prime number, or a higher power of it with an even exponent, then $\mathfrak{A} = +1$.

IV. If a is $= 4$, or a higher power of two with an even exponent, and k is of the form $4\mu + 1$, then $\mathfrak{A} = +1$.

V. If, with the other conditions as in IV, k is of the form $4\mu + 3$ and $\frac{n}{a}$ of the form $4\mu + 1$, then $\mathfrak{A} = -i$.

VI. If, with the other conditions as in IV, k is of the form $4\mu + 3$ and $\frac{n}{a}$ of the form $4\mu + 3$, then $\mathfrak{A} = +i$.

VII. If a is $= 8$, or a higher power of two with an odd exponent, and k is of the form $8\mu + 1$, then $\mathfrak{A} = +1$.

VIII. If, with the other conditions as in VII, k is of the form $8\mu + 5$, then $\mathfrak{A} = -1$.

IX. If, with the other conditions as in VII, k is of the form $8\mu + 3$ and $\frac{n}{a}$ of the form $4\mu + 1$, then $\mathfrak{A} = +i$.

X. If, with the other conditions as in VII, k is of the form $8\mu + 3$ and $\frac{n}{a}$ of the form $4\mu + 3$, then $\mathfrak{A} = -i$.

XI. If, with the other conditions as in VII, k is of the form $8\mu + 7$ and $\frac{n}{a}$ of the form $4\mu + 1$, then $\mathfrak{A} = -i$.

XII. If, with the other conditions as in VII, k is of the form $8\mu + 7$ and $\frac{n}{a}$ of the form $4\mu + 3$, then $\mathfrak{A} = +i$.

[*] Clearly, what were k and h there are here $\frac{n}{a}$ and k for the second factor, $\frac{n}{b}$ and k for the third factor, etc.

We omit the case where $a = 2$; here $\mathfrak{A}$ would indeed be $= \frac{0}{0}$, or indeterminate, but then we always have $W = 0$.

The remaining factors $\mathfrak{B}, \mathfrak{C}$ etc. depend on b, c etc. in the same way as $\mathfrak{A}$ depends on a, insofar as these enter into their determination.

31.

By this second method, the first example of Article 29 runs as follows:

The factor w is $= (1+i)\sqrt{2520}$
For $a = 8$ the corresponding factor $\mathfrak{A}$ is, by case VIII, $= -1$
For the second factor of n, 9, the corresponding factor is $+1$ (by case III.)
For the factor 5 the corresponding factor is -1 (by case II.)
For the factor 7 the corresponding factor is -1 (by case II.)

This gives the product $W = (-1-i)\sqrt{2520}$, as in Article 29.

32.

Since the value of W can be determined by *two* methods, one of which rests on the relations of the numbers $\frac{nk}{a}$, $\frac{nk}{b}$, $\frac{nk}{c}$ etc. to the numbers a, b, c etc., while the other depends on the relations of k to the numbers a, b, c etc., there must be a conditional connection among all these relations, so that any one can be determined from the others. Suppose that all the numbers a, b, c etc. are odd prime numbers, and take $k = 1$. Divide the factors a, b, c etc. into two classes: one contains those of the form $4\mu + 1$, denoted by p, p', p'' etc.; the other consists of those of the form $4\mu+3$, denoted by q, q', q'' etc. We shall denote the number of the latter by m. With this done, we first observe that n is of the form $4\mu + 1$ if m is even (this also includes the case where there are no factors at all in the second class, or $m = 0$), whereas n is of the form $4\mu+3$ if m is odd. Now the determination of W by the first method is carried out as follows. Let the numbers $P, P'\ P''$ etc., Q, Q', Q'' etc. depend on the relations of the numbers $\frac{n}{p}$, $\frac{n}{p'}$, $\frac{n}{p''}$ etc., $\frac{n}{q}$, $\frac{n}{q'}$, $\frac{n}{q''}$ etc. to the numbers p, p', p'' etc., q, q', q'' etc., respectively, in such a way that we put

$$P = +1, \text{ if } \frac{n}{p} \text{ is a quadratic residue of } p$$
$$P = -1, \text{ if } \frac{n}{p} \text{ is a quadratic nonresidue of } p$$

and similarly for the others. Then W will be the product of the factors $P\sqrt{p}$, $P'\sqrt{p'}$, $P''\sqrt{p''}$ etc. $iQ\sqrt{q}$, $iQ'\sqrt{q'}$, $iQ''\sqrt{q''}$ etc., and therefore

$$W = PP'P'' \ldots QQ'Q'' \ldots i^m\sqrt{n}$$

By the second method, or rather directly from the rules of Article 19, we have

$$W = +\sqrt{n}, \text{ if } n \text{ is of the form } 4\mu + 1,$$
$$\text{or equivalently, if } m \text{ is even}$$
$$W = +i\sqrt{n}, \text{ if } n \text{ is of the form } 4\mu + 3,$$
$$\text{or if } m \text{ is odd.}$$

Both cases can be combined in the following formula:

$$W = i^{mm}\sqrt{n}$$

It therefore follows that

$$PP'P'' \ldots QQ'Q'' \ldots = i^{mm-m}$$

But i^{mm-m} is $= 1$ whenever m is of the form 4μ or $4\mu + 1$, and $= -1$ whenever m is of the form $4\mu+2$ or $4\mu+3$. From this we deduce the following most elegant

THEOREM. *Let a, b, c etc. denote distinct positive odd prime numbers, and put their product $= n$. Let m of them be of the form $4\mu + 3$, and the rest of the form $4\mu + 1$. The number of those among a, b, c etc. for which $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$ etc., respectively, are nonresidues will be even whenever m is of the form 4μ or $4\mu + 1$, but odd whenever m is of the form $4\mu + 2$ or $4\mu + 3$.*

Thus, for example, putting $a = 3$, $b = 5$, $c = 7$, $d = 11$, we have three numbers of the form $4\mu + 3$, namely 3, 7 and 11; and $5 \,.\, 7 \,.\, 11\, R3$; $3 \,.\, 7 \,.\, 11\, R5$; $3 \,.\, 5 \,.\, 11\, R7$; $3 \,.\, 5 \,.\, 7\, N11$, so that only $\frac{n}{d}$ is a nonresidue of d.

33.

The celebrated *fundamental theorem* about quadratic residues is nothing other than a special case of the theorem just developed. Specifically, by limiting the number of the numbers a, b, c etc. to *two*, it is clear that, if just one of them, or neither, is of the form $4\mu + 3$, we must have either both aRb, bRa, or both aNb, bNa; but if both are of the form $4\mu + 3$, one must be a nonresidue of the other, and the latter a residue of the former. Here, then, is a *fourth* proof of this most important theorem, whose first and second proofs we gave in the Disquisitiones Arithmeticae, and the third recently in a separate paper (*Commentt. T. XVI*); we shall later set out two others, again resting on entirely different principles. It is certainly most remarkable that this most beautiful theorem, which at first so stubbornly eluded every attempt, could later be reached by so many paths, worlds apart from one another.

34.

The remaining theorems, which form a kind of supplement to the fundamental theorem, namely those by which we distinguish the prime numbers for which $-1, +2$ and -2 are residues or nonresidues, can also be derived from the same principles. We shall begin with the residue $+2$.

Putting $n = 8a$, with a a prime number, and $k = 1$, the method of Article 28 makes W the product of two factors. One of them will be $+\sqrt{a}$, or $+i\sqrt{a}$, if 8, or equivalently 2, is a quadratic residue of a; but $-\sqrt{a}$ or $-i\sqrt{a}$ if 2 is a nonresidue of a. The second factor is

$$\begin{aligned}
&(1+i)\sqrt{8}, \quad \text{if } a \text{ is of the form } 8\mu+1\\
&(-1+i)\sqrt{8}, \quad \text{if } a \text{ is of the form } 8\mu+3\\
&(-1-i)\sqrt{8}, \quad \text{if } a \text{ is of the form } 8\mu+5\\
&(1-i)\sqrt{8}, \quad \text{if } a \text{ is of the form } 8\mu+7
\end{aligned}$$

But by Article 18 we always have $W = (1+i)\sqrt{n}$; dividing this value by the four values of the second factor shows that the first factor must be

$$\begin{aligned}
&+\sqrt{a}, \quad \text{if } a \text{ is of the form } 8\mu+1\\
&-i\sqrt{a}, \quad \text{if } a \text{ is of the form } 8\mu+3\\
&-\sqrt{a}, \quad \text{if } a \text{ is of the form } 8\mu+5\\
&+i\sqrt{a}, \quad \text{if } a \text{ is of the form } 8\mu+7
\end{aligned}$$

It follows immediately that 2 must be a residue of a in the first and fourth cases, but a nonresidue in the second and third.

35.

The prime numbers for which -1 is a residue or a nonresidue are easily distinguished with the aid of the following theorem, which is also quite remarkable in itself.

THEOREM. *The product of the two factors*

$$W' = 1 + r^{-1} + r^{-4} + \text{etc.} + r^{-(n-1)^2}$$
$$W = 1 + r + r^4 + \text{etc.} + r^{(n-1)^2}$$

is $= n$ *if* n *is odd; or* $= 0$ *if* n *is twice an odd number; or* $= 2n$ *if* n *is divisible by four.*

Proof. Since we evidently have

$$\begin{aligned} W &= r + r^4 + r^9 + \text{etc.} + r^{nn} \\ &= r^4 + r^9 + \text{etc.} + r^{(n+1)^2} \\ &= r^9 + \text{etc.} + r^{(n+2)^2} \quad \text{etc.} \end{aligned}$$

the product WW' can also be written as follows:

$$\begin{aligned} & 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} \\ & + r^{-1}(r + r^4 + r^9 + r^{16} + \text{etc.} + r^{nn}) \\ & + r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \text{etc.} + r^{(n+1)^2}) \\ & + r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \text{etc.} + r^{(n+2)^2}) \\ & \text{etc.} \\ & + r^{-(n-1)^2}(r^{(n-1)^2} + r^{nn} + r^{(n+1)^2} \\ & \qquad + r^{(n+2)^2} + \text{etc.} + r^{(2n-2)^2}) \end{aligned}$$

Summing this expression vertically gives

$$\begin{aligned} & n \\ & + r(1 + rr + r^4 + r^6 + \text{etc.} + r^{2n-2}) \\ & + r^4(1 + r^4 + r^8 + r^{12} + \text{etc.} + r^{4n-4}) \\ & + r^9(1 + r^6 + r^{12} + r^{18} + \text{etc.} + r^{6n-6}) \\ & + \text{etc.} \\ & + r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} \\ & \qquad + r^{6n-6} + \text{etc.} + r^{2(n-1)^2}) \end{aligned}$$

Now, if n is odd, each part of this expression, except the first, n, will be $= 0$; for the second is evidently $\frac{r(1-r^{2n})}{1-rr}$, the third $\frac{r^4(1-r^{4n})}{1-r^4}$ etc. Whenever n is even, however, we must also except the part

$$r^{\frac{1}{4}nn}(1 + r^n + r^{2n} + r^{3n} + \text{etc.} + r^{nn-n})$$

which is $= nr^{\frac{1}{4}nn}$. In the first case, therefore, $WW' = n$, but in the second $= n + nr^{\frac{1}{4}nn}$; now $r^{\frac{1}{4}nn}$ is $= +1$ if n is divisible by four, and then we obtain $WW' = 2n$; on the other hand, $r^{\frac{1}{4}nn} = -1$ if n is twice an odd number, in which case $WW' = 0$. Q. E. D.

36.

Article 22 establishes that, if n is an odd prime number, $\frac{W'}{W}$ is $= +1$ or $= -1$ according as -1 is a residue or a nonresidue of n. Hence in the first case we must have $W^2 = +n$, and in the second $W^2 = -n$; by Article 13 we therefore conclude that the first case can occur only when n is of the form $4\mu + 1$, and the second when n is of the form $4\mu + 3$.

Finally, combining the conditions found for the residues $+2$ and -1 immediately shows that -2 is a residue of every prime number of the form $8\mu + 1$ or $8\mu + 3$, and a nonresidue of every prime number of the form $8\mu + 5$ or $8\mu + 7$.

NEW PROOFS AND EXTENSIONS OF THE FUNDAMENTAL THEOREM IN THE THEORY OF QUADRATIC RESIDUES

BY

CARL FRIEDRICH GAUSS

PRESENTED TO THE ROYAL SOCIETY OF SCIENCES ON FEBRUARY 10, 1817.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. IV.
Gottingae MDCCCXVIII.

NEW PROOFS AND EXTENSIONS OF THE FUNDAMENTAL THEOREM IN THE THEORY OF QUADRATIC RESIDUES.

The fundamental theorem about quadratic residues, which ranks among the most beautiful truths of higher arithmetic, was readily discovered by induction, but proved with far greater difficulty. It often happens in this field that the proofs of the simplest truths, which seem to offer themselves to the investigator through induction of their own accord, lie deeply hidden and can finally be brought to light only after many unsuccessful attempts, perhaps by a path very different from the one along which they were sought. Then it often happens that, once one path has been found, *several* others gradually open up, leading to the same goal: some more briefly and directly, others as if by a roundabout way, starting from very different principles between which and the question at hand one would scarcely have suspected any connection. This remarkable connection among more hidden truths not only gives these investigations a particular charm; it also deserves careful study and unravelling, since it often yields new resources or advances for the science itself.

Although the arithmetical theorem considered here might therefore seem, through the earlier efforts that supplied four entirely different proofs[*)], to have been fully dealt with, I nevertheless return to the same subject and add two further proofs, which will certainly shed new light on it. The first is related to the third in a certain respect, since it starts from the same lemma; it then follows a different path, however, so that it can rightly be regarded as a new proof, which in elegance will seem, if not superior to that third proof, at least by no means inferior. The sixth proof rests on an entirely different and subtler principle, and gives a new example of the remarkable connection between arithmetical truths that at first sight seem very far apart. These two proofs are accompanied by a very simple new algorithm for deciding whether a given integer is a quadratic residue or a nonresidue of a given prime number.

[*)] Two are given in the fourth and fifth sections of the *Disquisitiones Arithmeticae*; the third in a separate paper (*Commentt. Soc. Gotting. Vol. XVI*), and the fourth in the paper *Summatio quarundam serierum singularium* (*Commentt. Recentiores, Vol. I*).

There was another reason that led me to publish now, in particular, the new proofs promised nine years ago. When I began in 1805 to investigate the theory of cubic and biquadratic residues, a far more difficult subject, I experienced much the same course of events as before in the theory of quadratic residues. The theorems that completely settle these questions, and display a remarkable analogy with the theorems about quadratic residues, were immediately discovered by induction as soon as they were sought along a suitable path; but all attempts to obtain proofs complete in every respect remained unsuccessful for a long time. This was precisely what prompted me to strive so eagerly to add more and more proofs to those already known for quadratic residues, sustained by the hope that, among many different methods, one or another might help to illuminate the related subject. This hope was by no means in vain, and tireless work was finally followed by good results. Soon it will be possible to bring the fruits of my nights of work before the public; but before I undertake this arduous task, I have resolved to return once more to the theory of quadratic residues, complete everything that still remains to be done in it, and thus, as it were, take leave of this part of higher arithmetic.

FIFTH PROOF OF THE FUNDAMENTAL THEOREM IN THE THEORY OF QUADRATIC RESIDUES.

1.

We have already stated in the introduction that the fifth and third proofs start from the same lemma. For convenience, we have thought it appropriate to repeat it here in notation adapted to the present investigation.

LEMMA. *Let m be a prime number (positive and odd), and M an integer not divisible by m. Take the least positive residues of the numbers*

$$M,\ 2M,\ 3M,\ 4M\ \ldots\ldots\ \tfrac{1}{2}(m-1)M$$

modulo m. Some will be less than $\frac{1}{2}m$, and others greater; let the number of the latter be $= n$. Then M is a quadratic residue or a nonresidue of m, according as n is even or odd.

PROOF. Let those of these residues which are less than $\frac{1}{2}m$ be a, b, c, d etc., and the remaining ones, greater than $\frac{1}{2}m$, be a', b', c', d' etc. The complements of the latter to m, namely $m-a'$, $m-b'$, $m-c'$, $m-d'$ etc., are evidently all less than $\frac{1}{2}m$ and distinct both from one another and from the residues a, b, c, d etc. Thus, taken together with these, they are precisely all the numbers $1,\ 2,\ 3,\ 4\ldots.\frac{1}{2}(m-1)$, though in a different order. Putting the product

$$1\,.\,2\,.\,3\,.\,4\ldots..\tfrac{1}{2}(m-1) = P$$

we therefore have

$$P = abcd\ldots. \times (m-a')(m-b')(m-c')(m-d')\ldots.$$

and hence

$$(-1)^n P = abcd\ldots. \times (a'-m)(b'-m)(c'-m)(d'-m)\ldots.$$

Furthermore, modulo m, we have

$$\begin{aligned} PM^{\frac{1}{2}(m-1)} &\equiv abcd\,..\times a'b'c'd'\,..\\ &\equiv abcd\,..\times (a'-m)(b'-m)(c'-m)(d'-m)\,.. \end{aligned}$$

and hence

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n$$

It follows that $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, taking the upper or lower sign according as n is even or odd. With the aid of the theorem proved in Article 106 of the *Disquisitiones Arithmeticae*, the lemma follows immediately.

2.

THEOREM. *Let m, M be positive odd integers coprime to one another, and let n be the number of those among the least positive residues of the numbers*

$$M,\ 2M,\ 3M \ldots\ldots \tfrac{1}{2}(m-1)M$$

modulo m which are greater than $\frac{1}{2}m$. Likewise, let N be the number of those among the least positive residues of the numbers

$$m,\ 2m,\ 3m \ldots\ldots \tfrac{1}{2}(M-1)m$$

modulo M which are greater than $\frac{1}{2}M$. Then the three numbers n, N, $\frac{1}{4}(m-1)(M-1)$ are either all even, or one is even and the other two odd.

PROOF. Let us denote

by f the collection of numbers $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(m-1)$.
by f' the collection of numbers $m-1,\ m-2,\ m-3 \ldots\ldots \frac{1}{2}(m+1)$
by F the collection of numbers $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(M-1)$
by F' the collection of numbers $M-1,\ M-2,\ M-3 \ldots\ldots \frac{1}{2}(M+1)$

Thus n indicates how many numbers Mf have their least positive residues modulo m in the collection f'. Likewise, N indicates how many numbers mF have their least positive residues modulo M in the collection F'. Finally, let

φ denote the collection of numbers $1,\ 2,\ 3 \ldots\ldots \frac{1}{2}(mM-1)$
φ' denote the collection of numbers $mM-1,\ mM-2,\ mM-3 \ldots\ldots \frac{1}{2}(mM+1)$

Every integer not divisible by m must be congruent modulo m either to a residue from f or to one from f'. Likewise, every integer not divisible by M is congruent modulo M either to a residue from F or to one from F'. Thus all the numbers in φ, among which evidently none is divisible by both m and M, can be divided into eight classes as follows.

I. The first class contains the numbers congruent modulo m to a number from f, and modulo M to a number from F. We shall denote their number by α.

II. The numbers congruent modulo m, M, respectively, to numbers from f, F'; we put their number $= \beta$.

III. The numbers congruent modulo m, M, respectively, to numbers from f', F; we put their number $= \gamma$.

IV. The numbers congruent modulo m, M, respectively, to numbers from f', F'; let their number be $= \delta$.

V. The numbers divisible by m, but congruent modulo M to residues from F.

VI. The numbers divisible by m, but congruent modulo M to residues from F'.

VII. The numbers divisible by M, but congruent modulo m to residues from f.

VIII. The numbers divisible by M, but congruent modulo m to residues from f'.

Evidently classes V and VI together contain all the numbers mF. The number contained in VI is $= N$, so the number contained in V is $\frac{1}{2}(M-1)-N$. Likewise, classes VII and VIII together contain all the numbers Mf; class VIII contains n numbers, and class VII contains $\frac{1}{2}(m-1)-n$.

In just the same way, all the numbers in φ' are divided into eight classes IX . . XVI. If we keep the same order in doing this, it is easy to see that the numbers in the classes

IX, X, XI, XII, XIII, XIV, XV, XVI

are, respectively, the complements to mM of the numbers in the classes

IV, III, II, I, VI, V, VIII, VII

so that class IX contains δ numbers, class X contains γ, and so on. It is now clear that, if all the numbers of the first class are combined with all those of the ninth, we obtain all the numbers below mM which are congruent modulo m to a number from f, and modulo M to a number from F. It is easy to see that their number equals the number of all combinations of each individual f with each individual F. We therefore have

$$\alpha + \delta = \tfrac{1}{4}(m-1)(M-1)$$

and by a similar argument we also have

$$\beta + \gamma = \tfrac{1}{4}(m-1)(M-1)$$

Combining all the numbers of classes II, IV and VI evidently gives all the numbers below $\frac{1}{2}mM$ which are congruent to a residue from F' modulo M. These same numbers can also be written as follows:

$$F',\ M+F',\ 2M+F',\ 3M+F' \ldots .\ \tfrac{1}{2}(m-3)M+F'$$

Their total number is therefore $= \frac{1}{4}(m-1)(M-1)$, or we have

$$\beta + \delta + N = \tfrac{1}{4}(m-1)(M-1)$$

Likewise, combining all of classes III, IV and VIII gives

$$\gamma + \delta + n = \tfrac{1}{4}(m-1)(M-1)$$

These four equations give the following:

$$\begin{aligned} 2\alpha &= \tfrac{1}{4}(m-1)(M-1) + n + N \\ 2\beta &= \tfrac{1}{4}(m-1)(M-1) + n - N \\ 2\gamma &= \tfrac{1}{4}(m-1)(M-1) - n + N \\ 2\delta &= \tfrac{1}{4}(m-1)(M-1) - n - N \end{aligned}$$

each of which establishes the theorem.

3.

If we now suppose that m and M are prime numbers, the fundamental theorem follows immediately by combining the preceding theorem with the lemma of Article 1. For it is clear that

I. whenever the numbers m, M both have the form $4k+1$, or just one of them does, the number $\frac{1}{4}(m-1)(M-1)$ is even. Thus n and N are either both even or both odd, and consequently either each of m and M is a quadratic residue of the other, or each is a quadratic nonresidue of the other.

II. Whenever both numbers m, M are of the form $4k+3$, however, $\frac{1}{4}(m-1)(M-1)$ is odd. Hence one of the numbers n, N is even and the other odd, and consequently one of the numbers m, M is a quadratic residue of the other, and the other a quadratic nonresidue of the first. Q. E. D.

SIXTH PROOF OF THE FUNDAMENTAL THEOREM IN THE THEORY OF QUADRATIC RESIDUES.

1.

THEOREM. *Let p denote a prime number (positive and odd), n a positive integer not divisible by p, and x an indeterminate quantity. Then the function*

$$1 + x^n + x^{2n} + x^{3n} + \text{etc.} + x^{np-n}$$

is divisible by

$$1 + x + xx + x^3 + \text{etc.} + x^{p-1}$$

PROOF. Take a positive integer g such that $gn \equiv 1 \pmod{p}$, and put $gn = 1 + hp$. Then we have

$$\begin{aligned}\frac{1 + x^n + x^{2n} + x^{3n} + \text{etc.}\, x^{np-n}}{1 + x + xx + x^3 + \text{etc.}\, x^{p-1}} &= \frac{(1 - x^{np})(1 - x)}{(1 - x^n)(1 - x^p)} \\ &= \frac{(1 - x^{np})(1 - x^{gn} - x + x^{hp+1})}{(1 - x^n)(1 - x^p)} \\ &= \frac{1 - x^{np}}{1 - x^p} \cdot \frac{1 - x^{gn}}{1 - x^n} - \frac{x(1 - x^{np})}{1 - x^n} \cdot \frac{1 - x^{hp}}{1 - x^p}\end{aligned}$$

which is evidently a polynomial. Q. E. D.

Thus every polynomial in x divisible by $\frac{1-x^{np}}{1-x^n}$ is also divisible by $\frac{1-x^p}{1-x}$.

2.

Let α denote a positive primitive root modulo p; that is, let α be a positive integer such that the least positive residues of the powers $1, \alpha, \alpha\alpha, \alpha^3 \ldots\ldots \alpha^{p-2}$ modulo p are precisely the numbers $1, 2, 3, 4 \ldots\ldots p-1$, without regard to order. Further, denoting by fx the function

$$x + x^\alpha + x^{\alpha\alpha} + x^{\alpha^3} + \text{etc.} + x^{\alpha^{p-2}} + 1$$

it is clear that $fx - 1 - x - xx - x^3 - \text{etc.} - x^{p-1}$ is divisible by $1 - x^p$, and therefore all the more by $\frac{1-x^p}{1-x} = 1 + x + xx + x^3 + \text{etc.} + x^{p-1}$. This last function therefore also divides fx itself. Since x represents an indeterminate quantity, it follows that $f(x^n)$ is also divisible by $\frac{1-x^{np}}{1-x^n}$, and hence, by the preceding article, by $\frac{1-x^p}{1-x}$, whenever n is an integer not divisible by p. If, on the other hand, n is an integer divisible by p, the individual terms of the function $f(x^n)$, each decreased by one, are divisible by $1 - x^p$. In this case, therefore, $f(x^n) - p$ is also divisible by $1 - x^p$, and hence by $\frac{1-x^p}{1-x}$.

3.

THEOREM. *Putting*

$$x - x^{\alpha} + x^{\alpha\alpha} - x^{\alpha^3} + x^{\alpha^4} - \text{etc.} - x^{\alpha^{p-2}} = \xi$$

then $\xi\xi \mp p$ *is divisible by* $\frac{1-x^p}{1-x}$, *taking the upper sign whenever* p *is of the form* $4k+1$, *and the lower whenever* p *is of the form* $4k+3$.

PROOF. It is easy to see that, of the following $p-1$ functions

$$\begin{aligned}
&+ x\xi - xx + x^{\alpha+1} - x^{\alpha\alpha+1} \\
&\qquad + \text{etc.} + x^{\alpha^{p-2}+1} \\
&- x^{\alpha}\xi - x^{2\alpha} + x^{\alpha\alpha+\alpha} - x^{\alpha^3+\alpha} \\
&\qquad + \text{etc.} + x^{\alpha^{p-1}+\alpha} \\
&+ x^{\alpha\alpha}\xi - x^{2\alpha\alpha} + x^{\alpha^3+\alpha\alpha} - x^{\alpha^4+\alpha\alpha} \\
&\qquad + \text{etc.} + x^{\alpha^p+\alpha\alpha} \\
&- x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} \\
&\qquad + \text{etc.} + x^{\alpha^{p+1}+\alpha^3}
\end{aligned}$$

etc., as far as

$$-x^{\alpha^{p-2}}\xi - x^{2\alpha^{p-2}} + x^{\alpha^{p-1}+\alpha^{p-2}} - x^{\alpha^p+\alpha^{p-2}} + \text{etc.} + x^{\alpha^{2p-4}+\alpha^{p-2}}$$

the first is $= 0$, while each of the others is divisible by $1 - x^p$. Their sum is therefore also divisible by $1 - x^p$, and is found to be

$$\begin{aligned}
&= \xi\xi - (f(xx) - 1) + (f(x^{\alpha+1}) - 1) - (f(x^{\alpha\alpha+1}) - 1) \\
&\qquad + (f(x^{\alpha^3+1}) - 1) - \text{etc.} \\
&\qquad + (f(x^{\alpha^{p-2}+1}) - 1) \\
&= \xi\xi - f(xx) + f(x^{\alpha+1}) - f(x^{\alpha\alpha+1}) \\
&\qquad + f(x^{\alpha^3+1}) - \text{etc.} + f(x^{\alpha^{p-2}+1}) = \Omega
\end{aligned}$$

Thus this expression Ω is also divisible by $\frac{1-x^p}{1-x}$. Now, among the exponents $2,\ \alpha+1,\ \alpha\alpha+1,\ \alpha^3+1 \ldots\ldots \alpha^{p-2}+1$, only one is divisible by p, namely $\alpha^{\frac{1}{2}(p-1)}+1$. Hence, by the preceding article, the following individual parts of the expression Ω

$$f(xx), \quad f(x^{\alpha+1}), \quad f(x^{\alpha\alpha+1}), \quad (fx^{\alpha^3+1}) \quad \text{etc.}$$

with the sole exception of the term $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$, are divisible by $\frac{1-x^p}{1-x}$. Those parts may therefore be removed, leaving the following function still divisible by $\frac{1-x^p}{1-x}$:

$$\xi\xi \mp f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$$

Here the upper or lower sign applies according as p is of the form $4k+1$ or of the form $4k+3$. Since, moreover, $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})-p$ is divisible by $\frac{1-x^p}{1-x}$, $\xi\xi \mp p$ is also divisible by $\frac{1-x^p}{1-x}$. Q. E. D.

To prevent any ambiguity from the double sign, we shall use ε to denote the number $+1$ or -1, according as p is of the form $4k+1$ or $4k+3$. Thus $\frac{(1-x)(\xi\xi-\varepsilon p)}{1-x^p}$ is a polynomial in x, which we shall denote by Z.

4.

Let q be a positive odd number, so that $\frac{1}{2}(q-1)$ is an integer. Then $(\xi\xi)^{\frac{1}{2}(q-1)} - (\varepsilon p)^{\frac{1}{2}(q-1)}$ is divisible by $\xi\xi - \varepsilon p$, and hence also by $\frac{1-x^p}{1-x}$. Let us put $\varepsilon^{\frac{1}{2}(q-1)} = \delta$, and

$$\xi^{q-1} - \delta p^{\frac{1}{2}(q-1)} = \frac{1-x^p}{1-x} \cdot Y$$

Then Y is a polynomial in x, and $\delta = .+1$ whenever one of the numbers p, q, or indeed both, is of the form $4k+1$. On the other hand, $\delta = -1$ whenever both p, q are of the form $4k+3$.

5.

Let us now suppose that q too is a prime number, different from p. It is clear from the theorem proved in Article 51 of the *Disquisitiones Arithmeticae* that

$$. \quad \xi^q - (x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}})$$

is divisible by q, or is of the form qX, where X is a polynomial in x whose numerical coefficients are also integers (as is also to be understood of the other polynomials Z, Y, W occurring here). For the modulus p and primitive root α, let us denote the index of the number q by μ; that is, let $q \equiv \alpha^\mu \pmod{p}$. The numbers $q,\ q\alpha,\ q\alpha\alpha,\ q\alpha^3 \ldots\ldots q\alpha^{p-2}$ are therefore congruent modulo p, respectively, to the numbers $\alpha^\mu,\ \alpha^{\mu+1},\ \alpha^{\mu+2} \ldots\ldots \alpha^{p-2},\ 1,\ \alpha,\ \alpha\alpha \ldots\ldots \alpha^{\mu-1}$, so that

$$\begin{array}{l}
x^q - x^{\alpha^\mu} \\
x^{q\alpha} - x^{\alpha^{1+1}} \\
x^{q\alpha\alpha} - x^{\alpha^{\mu+2}} \\
x^{q\alpha^3} - x^{\alpha^{\mu+3}} \\
\quad . \\
\quad . \\
\quad . \\
\quad . \\
x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}} \\
x^{q\alpha^{p-\mu-1}} - x \\
x^{q\alpha^{p-\mu}} - x^\alpha \\
x^{q\alpha^{p-\mu+1}} - x^{\alpha\alpha} \\
\quad . \\
\quad . \\
\quad . \\
\quad . \\
x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}}
\end{array}$$

are divisible by $1 - x^p$. Taking these quantities alternately with positive and negative signs and adding them shows that $1 - x^p$ divides the function

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}} \mp \xi$$

with the upper or lower sign applying according as μ is even or odd; that is, according as q is a quadratic residue or a nonresidue of p. We shall therefore put

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}} - \gamma\xi = (1 - x^p)W$$

taking $\gamma = +1$ or $\gamma = -1$, according as q is a quadratic residue or a nonresidue of p. It is clear that W is a polynomial.

6.

With these preparations, we combine the preceding equations to obtain

$$\begin{aligned} q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) & \\ & + \frac{1 - x^p}{1 - x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ & + Y\xi\xi - W\xi(1 - x)) \end{aligned}$$

Let us suppose that dividing the function ξX by

$$x^{p-1} + x^{p-2} + x^{p-3} + \text{etc.} + x + 1$$

yields the quotient U with remainder T, or that we have

$$\xi X = \frac{1 - x^p}{1 - x} \cdot U + T$$

where U, T are polynomials whose numerical coefficients are also integers, and T is certainly of lower degree than the divisor. We therefore have

$$\begin{aligned} qT - \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) & \\ & = \frac{1 - x^p}{1 - x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) \\ & \quad + Y\xi\xi - W\xi(1 - x) - qU) \end{aligned}$$

This equation evidently cannot hold unless the left side and the right side each vanish separately. Thus $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ is divisible by q, as is $\delta p^{\frac{1}{2}(q-1)} - \gamma$; and therefore, since $\delta\delta = 1$, the number $p^{\frac{1}{2}(q-1)} - \gamma\delta$ is also divisible by q.

Now, if β denotes unity taken positively or negatively, according as p is a quadratic residue or a quadratic nonresidue of the number q, then $p^{\frac{1}{2}(q-1)} - \beta$ is divisible by q, and hence so is $\beta - \gamma\delta$. This cannot happen unless $\beta = \gamma\delta$. The fundamental theorem follows immediately. Namely,

I. Whenever the numbers p, q both have the form $4k + 1$, or just one of them does, so that $\delta = +1$, we have $\beta = \gamma$. Consequently either q is a quadratic residue of p and at the same time p a quadratic residue of q; or q is a nonresidue of p and at the same time p a nonresidue of q.

II. Whenever both p, q are of the form $4k + 3$, so that $\delta = -1$, we have $\beta = -\gamma$. Consequently either q is a quadratic residue of p and at the same time p a nonresidue of q; or q is a nonresidue of p and at the same time p a residue of q.

Q. E. D.

A new algorithm for deciding whether a given positive integer is a quadratic residue or a nonresidue of a given positive prime number.

1.

Before presenting a new solution to this problem, we shall briefly recall the solution given in the *Disquisitiones Arithmeticae*. It can be carried out quite readily with the help of the fundamental theorem and the following known theorems:

I. The relation of the number a to the number b (whether the former is a quadratic residue or a nonresidue of the latter) is the same as that of the number c to b, if $a \equiv c \pmod{b}$.

II. If a is the product of the factors $\alpha, \beta, \gamma, \delta$ etc., and b is prime, the relation of a to b depends on the relations of these factors to b as follows: a is a quadratic residue of b or a nonresidue according as an even or an odd number of those factors are nonresidues of b. Thus a factor that is a square can be disregarded entirely in this examination; if a factor is an integer raised to an odd power, that integer itself can take its place.

III. The number 2 is a quadratic residue of every prime of the form $8m+1$ or $8m+7$, and a nonresidue of every prime of the form $8m+3$ or $8m+5$.

Suppose, then, that a number a is given whose relation to a prime b is sought. If a is greater than b, first replace it by its least positive residue modulo b. Once this residue has been resolved into prime factors, theorem II reduces the question to finding the relation of each factor to b. The relation of the factor 2 (if it occurs once, three times, five times, etc.) is known from theorem III; by the fundamental theorem, the relation of each remaining factor depends on the relation of b itself to that factor. Thus, in place of the single relation of the given number to the prime b, we must now investigate several relations of the number b to other odd primes smaller than b. These problems are reduced in the same way to smaller moduli, and these successive reductions must evidently come to an end.

2.

To illustrate this solution, suppose that the relation of the number 103 to 379 is sought. Since 103 is already less than 379 and is itself prime, the fundamental theorem applies immediately: it tells us that the required relation is opposite to that of the number 379 to 103. This in turn is the same as the relation of the number 70 to 103, which itself depends on the relations of 2, 5, 7 to 103. The first of these is known from theorem III. By the fundamental theorem, the second depends on the relation of the number 103 to 5, which by theorem I is the same as that of 3 to 5; this in turn depends, by the fundamental theorem, on the relation of 5 to 3, which by theorem I is the same as that of 2 to 3, known from theorem III. Likewise, by the

fundamental theorem, the relation of 7 to 103 depends on that of 103 to 7, which by theorem I is the same as that of 5 to 7; this in turn depends, by the fundamental theorem, on the relation of 7 to 5, which by theorem I is the same as that of 2 to 5, known from theorem III. If we now wish to turn this analysis into a synthesis, the decision is reduced to fourteen steps. We give them all here, so that the greater elegance of the new solution may stand out more clearly.

1. The number 2 is a quadratic residue of the number 103 (theorem III).
2. The number 2 is a quadratic nonresidue of the number 3 (theorem III).
3. The number 5 is a quadratic nonresidue of the number 3 (from I and 2).
4. The number 3 is a quadratic nonresidue of the number 5 (the fundamental theorem and 3).
5. The number 103 is a quadratic nonresidue of the number 5 (I and 4).
6. The number 5 is a quadratic nonresidue of the number 103 (the fundamental theorem and 5).
7. The number 2 is a quadratic nonresidue of the number 5 (theorem III).
8. The number 7 is a quadratic nonresidue of the number 5 (I and 7).
9. The number 5 is a quadratic nonresidue of the number 7 (the fundamental theorem and 8).
10. The number 103 is a quadratic nonresidue of the number 7 (I and 9).
11. The number 7 is a quadratic residue of the number 103 (the fundamental theorem and 10).
12. The number 70 is a quadratic nonresidue of the number 103 (II, 1, 6, 11).
13. The number 379 is a quadratic nonresidue of the number 103 (I and 12).
14. The number 103 is a quadratic residue of the number 379 (the fundamental theorem and 13).

For brevity, in what follows we shall use the notation introduced in *Comment. Gotting. Vol. XVI.* By $[x]$ we shall mean the quantity x itself when x is an integer, and the greatest integer below x when x is not an integer. Thus $x - [x]$ is always nonnegative and less than unity.

3.

Problem. *Let a, b be positive integers coprime to one another, and put $[\frac{1}{2}a] = a'$. Find the sum*

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \left[\frac{3b}{a}\right] + \left[\frac{4b}{a}\right] + \text{etc.} + \left[\frac{a'b}{a}\right]$$

SOLUTION. For brevity, let us denote such a sum by $\varphi(a, b)$, so that we also have

$$\varphi(b, a) = \left[\frac{a}{b}\right] + \left[\frac{2a}{b}\right] + \left[\frac{3a}{b}\right] + \text{etc.} + \left[\frac{b'a}{b}\right]$$

if we put $[\frac{1}{2}b] = b'$. In the third proof of the fundamental theorem it was shown that, when a and b are odd,

$$\varphi(a, b) + \varphi(b, a) = a'b'$$

By following the same method, the truth of this proposition extends easily to the case in which one of the numbers $a,\ b$ is odd, as we already indicated there. Divide a by b, as in the method for finding the greatest common divisor of two integers, and let β be the quotient and c the remainder; then divide b by c, and so on, obtaining the equations

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \varepsilon e + f \text{ etc.} \end{aligned}$$

In this way the continually decreasing sequence of numbers b, c, d, e, f etc. will eventually reach unity, since by hypothesis a and b are coprime. The last equation is therefore

$$k = \lambda l + 1$$

Since evidently

$$\begin{aligned} \left[\frac{a}{b}\right] &= \left[\beta + \frac{c}{b}\right] = \beta + \left[\frac{c}{b}\right] \\ \left[\frac{2a}{b}\right] &= \left[2\beta + \frac{2c}{b}\right] = 2\beta + \left[\frac{2c}{b}\right] \\ \left[\frac{3a}{b}\right] &= \left[3\beta + \frac{3c}{b}\right] = 3\beta + \left[\frac{3c}{b}\right] \end{aligned}$$

etc.. we have

$$\varphi(b, a) = \varphi(b, c) + \tfrac{1}{2}\beta(b'b' + b')$$

and consequently

$$\varphi(a, b) = a'b' - \tfrac{1}{2}\beta(b'b' + b') - \varphi(b, c)$$

By similar reasoning, on putting $[\frac{1}{2}c] = c'$, $[\frac{1}{2}d] = d'$ $[\frac{1}{2}e] = e'$ etc., we obtain

$$\begin{aligned}\varphi(b,c) &= b'c' - \tfrac{1}{2}\gamma(c'c' + c') - \varphi(c,d)\\ \varphi(c,d) &= c'd' - \tfrac{1}{2}\delta(d'd' + d') - \varphi(d,e).\\ \varphi(d,e) &= d'e' - \tfrac{1}{2}\varepsilon(e'e' + e') - \varphi(e,f)\end{aligned}$$

etc., as far as

$$\varphi(k,l) = k'l' - \tfrac{1}{2}\lambda(l'l' + l') - \varphi(l,1)$$

Since evidently $\varphi(l,1) = 0$, we obtain from this the formula

$$\begin{aligned}\varphi(a,b) = {} & a'b' - b'c' + c'd' - d'e' + \text{etc.} \pm k'l'\\ & - \tfrac{1}{2}\beta(b'b' + b') + \tfrac{1}{2}\gamma(c'c' + c') - \tfrac{1}{2}\delta(d'd' + d')\\ & + \tfrac{1}{2}\varepsilon(e'e' + e') - \text{etc.} \mp \tfrac{1}{2}\lambda(l'l' + l')\end{aligned}$$

4.

It now follows easily from the third proof that the relation of the number b to a, whenever a is prime, can be read directly from the value of the sum $\varphi(a, 2b)$. According as this sum is even or odd, b is a quadratic residue of a or a nonresidue. The sum $\varphi(a,b)$ itself can also be used for the same purpose, provided that we distinguish the case in which b is odd from that in which it is even. Namely,

I. When b is odd, b is a quadratic residue or a nonresidue of a according as $\varphi(a,b)$ is even or odd.

II. When b is even, the same rule holds if, in addition, a is of the form $8n+1$ or $8n+7$; but if, for an even value of b, the modulus a is of the form $8n+3$ or $8n+5$, the opposite rule must be applied: b is a quadratic residue of a if $\varphi(a,b)$ is odd, and a nonresidue if $\varphi(a,b)$ is even.

All this follows very easily from Article 4 of the third proof.

5.

Example. To find the relation of the number 103 to the prime 379, we have, for calculating the sum $\varphi(379, 103)$,

$$\begin{array}{r|r|l} a = 379 & a' = 189 & \\ b = 103 & b' = 51 & \beta = 3 \\ c = 70 & c' = 35 & \gamma = 1 \\ d = 33 & d' = 16 & \delta = 2 \\ e = 4 & e' = 2 & \varepsilon = 8 \end{array}$$

and hence

$$\begin{aligned} \varphi(379, 103) &= 9639 - 1785 + 560 - 32 - 3978 + 630 - 272 + 24 \\ &= 4786 \end{aligned}$$

so 103 is a quadratic residue of the number 379. If we prefer to use the sum $(379, 206)$ for the same purpose, we have the following scheme:

$$\begin{array}{r|r|l} 379 & 189 & \\ 206 & 103 & 1 \\ 173 & 86 & 1 \\ 33 & 16 & 5 \\ 8 & 4 & 4 \end{array}$$

from which we obtain

$$\begin{aligned} \varphi(379, 206) &= 19467 - 8858 + 1376 - 64 - 5356 + 3741 - 680 + 40 \\ &= 9666 \end{aligned}$$

Thus 103 is a quadratic residue of the number 379.

6.

To determine the relation of the number b to a, it is not necessary to calculate the individual terms of the sum $\varphi(a, b)$; it is enough to know how many of them are odd. Our rule can therefore also be stated as follows:

As above, take $a = \beta b + c,\ b = \gamma c + d,\ c = \delta d + e$ etc., until the sequence of numbers $a,\ b,\ c,\ d,\ e$ etc. reaches unity. Put $[\frac{1}{2}a] = a',\ [\frac{1}{2}b] = b',\ [\frac{1}{2}c] = c'$ etc., and let μ count the odd numbers in the sequence a', b', c' etc. that are immediately followed by an odd number. Further, let ν count the odd numbers in the sequence β, γ, δ etc. whose corresponding numbers in the sequence b', c', d' etc., respectively, have the form $4n + 1$ or $4n + 2$. Then b is a quadratic residue or a nonresidue of a according as $\mu + \nu$ is even or odd, with the sole exception that, when b is even and a is of the form $8n + 3$ or $8n + 5$, the opposite rule holds.

In our example the sequence a', b', c', d', e' has two instances in which an odd entry is immediately followed by an odd entry, so $\mu = 2$; the sequence $\beta', \gamma', \delta', \varepsilon'$ does contain two odd numbers, but their corresponding numbers in the sequence b', c', d', e' have the form $4n+3$, so $\nu = 0$. Thus $\mu+\nu$ is even, and consequently 103 is a quadratic residue of the number 379.

THEORY

OF BIQUADRATIC RESIDUES

FIRST PAPER

BY

CARL FRIEDRICH GAUSS

PRESENTED TO THE ROYAL SOCIETY ON APRIL 5, 1825.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VI.
Göttingen MDCCCXXVIII.

THEORY OF BIQUADRATIC RESIDUES.

FIRST PAPER.

1.

The theory of quadratic residues reduces to a few fundamental theorems that rank among the most beautiful jewels of higher arithmetic. As is well known, these were first easily discovered through inductive observation and then proved in many different ways, leaving nothing further to be desired.

The theory of cubic and biquadratic residues, however, requires much deeper investigation. When we began to explore it in 1805, besides the results that lie, as it were, at the threshold, some special theorems presented themselves, remarkable both for their simplicity and for the difficulty of their proofs. But we soon found that the principles of arithmetic used up to then were wholly insufficient to establish the general theory. Rather, the theory necessarily requires the field of higher arithmetic to be enlarged, as it were, infinitely many times over. What this means will become entirely clear as these investigations continue. As soon as we entered this new field, inductive observation immediately opened a path to knowledge of the simplest theorems encompassing the entire theory. Their proofs, however, lay so deeply hidden that only after many unsuccessful attempts could they finally be brought to light.

Now that we are preparing to publish these studies, we shall begin with the theory of biquadratic residues. In this first paper we shall present the investigations that could already be completed on this side of the enlarged field of arithmetic. They pave the way to that field, as it were, and also contribute some new developments to the theory of the division of the circle.

2.

We introduced the notion of a biquadratic residue in Article 115 of the *Disquisitiones Arithmeticae*: an integer a, positive or negative, is called a biquadratic residue of the integer p if a can be congruent to a fourth power modulo p, and a biquadratic nonresidue if no such congruence exists. Throughout the following investigations, unless we expressly state otherwise, we shall assume that the modulus p is an odd positive prime and that a is not divisible by p, since all the remaining cases can very easily be reduced to this one.

3.

Clearly, every biquadratic residue of p is also a quadratic residue of the same number, and hence every quadratic nonresidue is also a biquadratic nonresidue. The converse also holds whenever p is a prime of the form $4n+3$.

For if, in this case, a is a quadratic residue of p, let us put $a \equiv bb \pmod{p}$. Here b is either a quadratic residue of p or a nonresidue. In the first case, let us put $b \equiv cc$, giving $a \equiv c^4$; that is, a is a biquadratic residue of p. In the second case, $-b$ is a quadratic residue of p (since -1 is a nonresidue of every prime of the form $4n + 3$). Putting $-b \equiv cc$ again gives $a \equiv c^4$, and a is a biquadratic residue of p. It is also easy to see that in this case the congruence $x^4 \equiv a \pmod{p}$ has no solutions besides $x \equiv c$ and $x \equiv -c$. Since these evident propositions exhaust the entire theory of biquadratic residues for prime moduli of the form $4n+3$, we shall exclude these moduli altogether from our investigation, restricting it to prime moduli of the form $4n + 1$.

4.

Thus, when p is a prime of the form $4n+1$, the converse of the proposition in the preceding article does not hold: there can be quadratic residues that are not also biquadratic residues. This happens whenever a quadratic residue is congruent to the square of a quadratic nonresidue. For put $a \equiv bb$, with b a quadratic nonresidue of p. If the congruence $x^4 \equiv a$ could be satisfied by a value $x \equiv c$, we would have $c^4 \equiv bb$, so that the product $(cc-b)(cc+b)$ would be divisible by p. Then p would have to divide either the factor $cc - b$ or the other factor $cc + b$; that is, either $+b$ or $-b$ would be a quadratic residue of p, and therefore both would be (since -1 is a quadratic residue), contrary to the hypothesis.

All integers not divisible by p could therefore be divided into three classes: the first would contain the biquadratic residues, the second the biquadratic nonresidues that are also quadratic residues, and the third the quadratic nonresidues. Clearly it suffices to classify only the numbers $1, 2, 3 \ldots . p - 1$. Half would belong to the third class, while the other half would be divided between the first and second classes.

5.

It will be better, however, to establish four classes as follows.

Let A be the collection of all biquadratic residues of p between 1 and $p-1$, inclusive, and let e be any chosen quadratic nonresidue of p. Further, let B be the collection of the least positive residues of the products eA modulo p, and let C, D respectively be the collections of the least positive residues of the products eeA, e^3A modulo p. It is then easy to see that the individual numbers in B are distinct, as are those in C and those in D; zero cannot occur among any of these numbers. Also, all numbers in A and C are quadratic residues of p, while all those in B and D are quadratic nonresidues. Thus neither of the collections A, C can have a number in common with B or D. But neither can A have a number in common with C, nor B with D. For suppose

I. that some number in A, say a, also occurs in C, where it arises from the congruent product eea', with a' a number in A. Put $a \equiv \alpha^4$, $a' \equiv \alpha'^4$, and choose an integer Θ such that $\Theta\alpha' \equiv 1$. We then have $ee\alpha'^4 \equiv \alpha^4$, and multiplying by Θ^4 gives

$$ee \equiv \alpha^4\Theta^4$$

That is, ee is a biquadratic residue, and hence e a quadratic residue, contrary to the hypothesis.

II. Similarly, suppose that a number belongs to both collections B, D, arising from the products ea, e^3a', with a, a' numbers in A. The congruence $ea \equiv e^3a'$ would imply $a \equiv eea'$. We would thus have a number arising from the product eea' that belonged to both C and A, which we have just proved impossible.

It is also easy to prove that *all* quadratic residues of p between 1 and $p-1$, inclusive, must occur either in A or in C, and all quadratic nonresidues of p between those limits must occur either in B or in D. For

I. Every such quadratic residue that is also a biquadratic residue belongs to A by hypothesis.

II. Write a quadratic residue h (less than p) that is also a biquadratic nonresidue as $\equiv gg$, where g is a quadratic nonresidue. Choose an integer γ such that $e\gamma \equiv g$. Then γ is a quadratic residue of p, which we write as $\equiv kk$. Hence

$$h \equiv gg \equiv ee\gamma\gamma \equiv eek^4$$

Since the least residue of k^4 belongs to A, the number h, which arises by multiplying it by ee, must belong to C.

III. Let h denote a quadratic nonresidue of p between 1 and $p-1$. Find an integer g between the same limits such that $eg \equiv h$. Then g is a quadratic

residue and so belongs to either A or C. In the first case, h evidently belongs to B, and in the second to D.

All this shows that the numbers $1, 2, 3 \ldots . p-1$ are distributed among the four lists A, B, C, D so that each occurs in one of them; each list must therefore contain $\frac{1}{4}(p-1)$ numbers. In this classification, the numbers belonging to A and C are intrinsic to those classes. The distinction between B and D, however, is arbitrary insofar as it depends on the choice of e, which itself always belongs to B. Thus, if a number from D is chosen instead, the classes B, D are interchanged.

6.

Since -1 is a quadratic residue of p, let us put $-1 \equiv ff \pmod{p}$. The four roots of the congruence $x^4 \equiv 1$ are then $1, f, -1, -f$. Thus if a is a biquadratic residue of p, say $\equiv \alpha^4$, the four roots of the congruence $x^4 \equiv a$ are $\alpha, f\alpha, -\alpha, -f\alpha$, which are easily seen to be pairwise incongruent. Hence, if we collect the least positive residues of the fourth powers $1, 16, 81, 256 \ldots . (p-1)^4$, they are always equal in groups of four, giving $\frac{1}{4}(p-1)$ distinct biquadratic residues that form the collection A. If we collect the least residues of the fourth powers only as far as $(\frac{1}{2}p - \frac{1}{2})^4$, each occurs twice.

7.

The product of two biquadratic residues is clearly a biquadratic residue: multiplying two numbers from class A always gives a product whose least positive residue belongs to the same class. Similarly, the product of a number from B and one from D, or of a number from C and one from C, has its least residue in A.

In B lie the residues of the products $A.B$ and $C.D$; in C those of $A.C$, $B.B$ and $D.D$; and finally in D those of $A.D$ and $B.C$.

The proofs are so evident that it suffices to indicate one. Let, for example, c and d be numbers from C and D, and put $c \equiv eea$, $d \equiv e^3a'$, with a, a' numbers from A. Then e^4aa' is a biquadratic residue, so its least residue belongs to A. For the product we have $cd \equiv e.e^4aa'$, so its least residue belongs to B.

We can now also easily decide which class contains a product of several factors. Assign to the classes A, B, C, D the characters $0, 1, 2, 3$, respectively. The character of a product is then either the sum of the characters of its individual factors or the least residue of that sum modulo 4.

8.

It seemed worthwhile to develop these elementary propositions without using the theory of power residues. With its help, everything can be proved much more easily still.

Let g be a primitive root for the modulus p: a number such that in the sequence of powers $g, gg, g^3 \ldots$., none before g^{p-1} is congruent to unity modulo p. Then the least positive residues of the numbers $1, g, gg, g^3 \ldots . g^{p-2}$ agree, apart from their order, with $1, 2, 3 \ldots . . p-1$, and are distributed among four classes as follows:

to	least residues of the numbers
A	$1,\ g^4, g^8, g^{12} \ldots . . g^{p-5}$
B	$g,\ g^5, g^9, g^{13} \ldots . . g^{p-4}$
C	$gg, g^6, g^{10}, g^{14} \ldots . . g^{p-3}$
D	$g^3, g^7, g^{11}, g^{15} \ldots . . g^{p-2}$

All the preceding propositions follow directly from this.

Just as the numbers $1, 2, 3 \ldots . p-1$ have here been divided among four classes, whose collections we denote by A, B, C, D, we may assign *any* integer not divisible by p to one of these classes according to its least residue modulo p.

9.

We denote by f the least residue of the power $g^{\frac{1}{4}(p-1)}$ modulo p. Since $ff \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ (*Disquis. Arithm.*, Article 62), the symbol f clearly has the same meaning here as in Article 6. Thus the power $g^{\frac{1}{4}\lambda(p-1)}$, with λ a positive integer, is congruent modulo p to $1, f, -1, -f$, according as λ has the form $4m, 4m+1, 4m+2, 4m+3$, respectively, or according as the least residue of g^λ belongs to A, B, C, D, respectively. This gives us a very simple criterion for deciding which class contains a given number h not divisible by p: h belongs to A, B, C or D according as the power $h^{\frac{1}{4}(p-1)}$ is congruent modulo p to $1, f, -1$ or $-f$.

As a corollary, -1 always belongs to class A when p has the form $8n+1$, and to class C when p has the form $8n+5$. A proof of this theorem independent of the theory of power residues can easily be obtained from what we established in Article 115, III of the *Disquisitiones Arithmeticae*.

10.

Since *all* primitive roots for the modulus p arise as residues of the powers g^λ, on taking for λ all numbers coprime to $p-1$, it is easy to see that these roots are equally divided between B and D, with the base g always in B. If we replace g as base by another primitive root from B, the classification remains the same; if we use a primitive root from D as base, the classes B and D are interchanged.

If the classification is based on the criterion in the preceding article, the distinction between B and D depends on which root of the congruence $xx \equiv -1 \pmod{p}$ we choose as the characteristic number f.

11.

To make it easier to illustrate by examples the subtler investigations that we are about to undertake, we give here the construction of the classes for all moduli below 100. For each modulus we have chosen the least primitive root.

$$p = 5$$

$$g = 2,\ f = 2$$

A	1
B	2
C	4
D	3

$$p = 13$$

$$g = 2,\ f = 8$$

A	$1, 3, 9$
B	$2, 5, 6$
C	$4, 10, 12$
D	$7, 8, 11$

$$p = 17$$

$$g = 3,\ f = 13$$

A	$1, 4, 13, 16$
B	$3, 5, 12, 14$
C	$2, 8, 9, 15$
D	$6, 7, 10, 11$

$$p = 29$$

$$g = 2,\ f = 12$$

A	$1, 7, 16, 20, 23, 24, 25$
B	$2, 3, 11, 14, 17, 19, 21$
C	$4, 5, 6, 9, 13, 22, 28$
D	$8, 10, 12, 15, 18, 26, 27$

$$p = 37$$

$$g = 2,\ f = 31$$

A	$1, 7, 9, 10, 12, 16, 26, 33, 34$
B	$2, 14, 15, 18, 20, 24, 29, 31, 32$
C	$3, 4, 11, 21, 25, 27, 28, 30, 36$
D	$5, 6, 8, 13, 17, 19, 22, 23, 35$

$$p = 41$$

$$g = 6,\ \ f = 32$$

A	$1, 4, 10, 16, 18, 23, 25, 31, 37, 40$
B	$6, 14, 15, 17, 19, 22, 24, 26, 27, 35$
C	$2, 5, 8, 9, 20, 21, 32, 33, 36, 39$
D	$3, 7, 11, 12, 13, 28, 29, 30, 34, 38$

$$p = 53$$

$$g = 2,\ \ f = 30$$

A	$1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49$
B	$2, 3, 19, 20, 26, 30, 31, 32, 35, 39, 41, 45, 48$
C	$4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43, 52$
D	$5, 8, 12, 14, 18, 21, 22, 23, 27, 33, 34, 50, 51$

$$p = 61$$

$$g = 2,\ \ f = 11$$

A	$1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58$
B	$2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55$
C	$3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60$
D	$6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59$

$$p = 73$$

$$g = 5,\ \ f = 27$$

A	$1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72$
B	$5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68$
C	$3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70$
D	$11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62$

$$p = 89$$

$$g = 3,\ \ f = 34$$

A	$1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44.\ 45,$
	$50, 57, 64, 67, 73, 78, 81, 85, 87, 88$
B	$3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46,$
	$48, 56, 61, 65, 66, 75, 77, 82, 83, 86$
C	$5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47,$
	$49, 53, 55, 68, 69, 71, 72, 79, 80, 84$
D	$13, 15.\ 19, 26, 27, 29.\ 30, 31, 35, 37, 38.\ 51,$
	$52, 54, 58, 59, 60, 62, 63, 70, 74, 76$

$$p = 97$$

$$g = 5,\ \ f = 22$$

A	$1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47,$
	$50, 54, 61, 62, 64, 73, 75, 81, 88, 91, 93, 96$
B	$5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45,$
	$52, 56, 67, 68, 74, 76, 77, 78, 80, 83, 84, 92$
C	$2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48,$
	$49, 53, 65.\ 66, 70, 72, 79, 85, 86, 89, 94, 95$
D	$7, 10, 15, 26, 28, 34, 37, 38, 39.\ 40, 42, 46,$
	$51, 55, 57, 58, 59, 60, 63, 69, 71, 82, 87, 90$

12.

Since 2 is a quadratic residue of every prime of the form $8n + 1$, but a nonresidue of every prime of the form $8n + 5$, for prime moduli of the first form 2 belongs to class A or C, and for moduli of the second form to B or D. The distinction between B and D is not intrinsic, depending only on the choice of f, so we shall set moduli of the form $8n + 5$ aside for a while. An *inductive investigation* of moduli of the form $8n + 1$ gives 2 in A for $p = 73, 89, 113, 233, 257, 281, 337, 353$, etc.; in contrast, 2 belongs to C for $p = 17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457$, etc.

Since, moreover, for a prime modulus of the form $8n+1$, -1 is a biquadratic residue, -2 clearly always belongs to the same class as $+2$.

13.

When we compare the examples in the preceding article, at least at first sight no simple criterion seems to offer itself for distinguishing the first moduli from the second. Nevertheless, there are *two* such criteria, remarkable for their elegance and simplicity. The following considerations will prepare the way to one of them.

The modulus p, being a prime of the form $8n+1$, can be expressed in the form $aa+2bb$ in exactly one way (*Disquiss. Arithm.*, Article 182, II). We assume that the roots a, b are taken positive. Clearly a is odd and b even; let us put $b = 2^\lambda c$, with c odd. We now observe:

I. Since $p \equiv aa \pmod{c}$, p is a quadratic residue of c, and hence also of each prime factor into which c is resolved. Conversely, by the fundamental theorem, each of these prime factors is a quadratic residue of p, and so their product c is also a quadratic residue of p. Since this also holds for 2, b is clearly a quadratic residue of p, and hence both bb and $-bb$ are biquadratic residues.

II. Thus $-2bb$ must belong to the same class as 2. Since $aa \equiv -2bb$, 2 clearly belongs to class A or C according as a is a quadratic residue of p or a quadratic nonresidue.

III. Now suppose that a has been resolved into prime factors. Denote those of the form $8m+1$ or $8m+7$ by $\alpha, \alpha', \alpha''$, etc., and those of the form $8m+3$ or $8m+5$ by β, β', β'', etc.; let the number of the latter be $= \mu$. Since $p \equiv 2bb \pmod{a}$, p is a quadratic residue of those prime factors of a of which 2 is a quadratic residue, that is, of $\alpha, \alpha', \alpha''$, etc.; it is a quadratic nonresidue of those factors of which 2 is a quadratic nonresidue, that is, of β, β', β'', etc. Conversely, by the fundamental theorem, each of $\alpha, \alpha', \alpha''$, etc., is a quadratic residue of p, while each of β, β', β'', etc., is a quadratic nonresidue. We therefore conclude that their product a is a quadratic residue of p or a nonresidue according as μ is even or odd.

IV. It is easy to verify that the product of all $\alpha, \alpha', \alpha''$, etc., has the form $8m+1$ or $8m+7$, and that the same holds for the product of all β, β', β'', etc., when their number is even. In this case the product a must therefore also have the form $8m+1$ or $8m+7$. In contrast, the product of all β, β', β'', etc., when their number is odd, has the form $8m+3$ or $8m+5$, and the same therefore holds for the product a in this case.

From all this we obtain the elegant theorem:

Whenever a has the form $8m+1$ or $8m+7$, 2 belongs to A; whenever a has the form $8m+3$ or $8m+5$, 2 belongs to C.

The examples listed in the preceding article confirm this. The first moduli decompose as follows: $73 = 1 + 2 \,.\, 36$, $89 = 81 + 2 \,.\, 4$, $113 = 81 + 2 \,.\, 16$, $233 = 225 + 2 \,.\, 4$, $257 = 225 + 2 \,.\, 16$, $281 = 81 + 2 \,.\, 100$, $337 = 49 + 2 \,.\, 144$, $353 = 225 + 2 \,.\, 64$; the second as follows: $17 = 9 + 2 \,.\, 4$, $41 = 9 + 2 \,.\, 16$, $97 = 25 + 2 \,.\, 36$, $137 = 9 + 2 \,.\, 64$, $193 = 121 + 2 \,.\, 36$, $241 = 169 + 2 \,.\, 36$, $313 = 25 + 2 \,.\, 144$, $401 = 9 + 2 \,.\, 196$, $409 = 121 + 2 \,.\, 144$, $433 = 361 + 2 \,.\, 36$, $449 = 441 + 2 \,.\, 4$, $457 = 169 + 2 \,.\, 144$.

14.

The decomposition of p into a square and twice a square has revealed such a remarkable connection with the classification of 2 that it seems worthwhile to ask whether a decomposition into two squares, which p is also known to admit, might give a similar result. Here are the decompositions of the numbers p for which 2 belongs to class

A	C
$9 + 64$	$1 + 16$
$25 + 64$	$25 + 16$
$49 + 64$	$81 + 16$
$169 + 64$	$121 + 16$
$1 + 256$	$49 + 144$
$25 + 256$	$225 + 16$
$81 + 256$	$169 + 144$
$289 + 64$	$1 + 400$
	$9 + 400$
	$289 + 144$
	$49 + 400$
	$441 + 16$

First we observe that, of the two squares into which p decomposes, one must be odd, which we put $= aa$, and the other even, which we put $= bb$. Since aa has the form $8n+1$, values of b that are twice an odd number clearly correspond to values of p of the form $8n + 5$, which are excluded from our inductive investigation here, since they would have 2 in class B or D. For values of p of the form $8n + 1$, however, b must be divisible by four. If we may trust the inductive evidence presented by this table, 2 belongs to class A for every modulus for which b has the form $8n$, and to class C for every modulus for which b has the form $8n + 4$. This theorem, however, requires much deeper investigation than the one obtained in the preceding article. Its proof must be preceded by several preliminary investigations concerning the order in which the numbers in A, B, C, D follow one another.

15.

Let us denote the number of numbers in A immediately followed by a number in A, B, C, D, respectively, by $(00), (01), (02), (03)$; likewise the number of numbers in B followed by a number in A, B, C, D, respectively, by $(10), (11), (12), (13)$. Similarly, let C contain respectively $(20), (21), (22), (23)$ numbers, and D contain $(30), (31), (32), (33)$ numbers, followed by a number in A, B, C, D. We propose to determine these sixteen counts a priori. To help readers compare the general reasoning with examples, it seemed useful to give here the numerical values of the entries in the scheme (S)

$$\begin{array}{llll} (00), & (01), & (02), & (03) \\ (10), & (11), & (12), & (13) \\ (20). & (21), & (22), & (23) \\ (30), & (31), & (32), & (33) \end{array}$$

for each modulus whose classification we gave in Article 11.

$p = 5$	$p = 13$	$p = 17$	$p = 29$
0, 1, 0. 0	0, 1, 2, 0	0, 2, 1, 0	2. 3, 0. 2
0, 0, 0, 1	1, 1, 0, 1	2, 0, 1, 1	1, 1, 2, 3
0, 0, 0, 0	0, 1, 0, 1	1, 1, 1, 1	2, 1, 2. 1
0, 0, 1, 0	1, 0, 1, 1	0, 1, 1, 2	1, 2, 3, 1

$p = 37$	$p = 41$	$p = 53$	$p = 61$
2, 1, 2, 4	0, 4, 3, 2	2, 3, 6, 2	4, 3, 2, 6
2, 2, 4, 1	4, 2, 2, 2	4, 4, 2, 3	3, 3, 6, 3
2, 2, 2, 2	3, 2, 3, 2	2, 4, 2, 4	4, 3, 4, 3
2, 4, 1, 2	2, 2, 2, 4	4, 2, 3, 4	3, 6, 3, 3

$p = 73$	$p = 89$	$p = 97$
5, 6, 4, 2	3, 8, 6, 4	2, 6, 7, 8
6, 2, 5, 5	8, 4, 5, 5	6, 8, 5, 5
4, 5, 4, 5	6, 5, 6, 5	7, 5, 7, 5
2, 5, 5, 6	4, 5, 5, 8	8, 5, 5, 6

Since moduli of the forms $8n + 1$ and $8n + 5$ behave differently, we must treat them separately. We begin with the first.

16.

The symbol (00) indicates how many different ways the equation $\alpha + 1 = \alpha'$ can be satisfied, with α, α' denoting arbitrary numbers in A. For a modulus of the form $8n + 1$, as understood here, α' and $p - \alpha'$ belong to the same

collection. We may therefore say more elegantly that (00) expresses the number of different ways of satisfying the equation $1 + \alpha + \alpha' = p$. Clearly the congruence $1 + \alpha + \alpha' \equiv 0 \pmod{p}$ can also take the place of this equation.

Likewise,

(01) indicates the number of solutions of the congruence $1+\alpha+\beta \equiv 0 \pmod{p}$
(02) the number of solutions of the congruence $1 + \alpha + \gamma \equiv 0$
(03) the number of solutions of the congruence $1 + \alpha + \delta \equiv 0$
(11) the number of solutions of the congruence $1 + \beta + \beta' \equiv 0$, etc.

where β and β' denote arbitrary numbers in B, γ numbers in C, and δ numbers in D. We immediately obtain the following six equations:

$$(01) = (10), \quad (02) = (20), \quad (03) = (30),$$
$$(12) = (21), \quad (13) = (31), \quad (23) = (32)$$

From any given solution of the congruence $1 + \alpha + \beta \equiv 0$ we obtain a solution of $1 + \delta + \delta' \equiv 0$ by taking for δ the number between $1 \ldots . p - 1$ that satisfies $\beta\delta \equiv 1$ (which clearly belongs to D), and for δ' the least positive residue of the product $\alpha\delta$ (which likewise belongs to D). The reverse passage from a given solution of $1 + \delta + \delta' \equiv 0$ to a solution of $1 + \alpha + \beta \equiv 0$ is equally clear: choose β so that $\beta\delta \equiv 1$, and at the same time put $\alpha \equiv \beta\delta'$. Thus the two congruences have the same number of solutions, or $(01) = (33)$.

Similarly, from the congruence $1 + \alpha + \gamma \equiv 0$ we derive $\gamma' + \gamma'' + 1 \equiv 0$ by choosing γ' in C so that $\gamma\gamma' \equiv 1$, and γ'' in the same collection congruent to the product $\alpha\gamma'$. It follows easily that these two congruences admit the same number of solutions, or $(02) = (22)$.

Likewise, from $1 + \alpha + \delta \equiv 0$ we derive $\beta + \beta' + 1 \equiv 0$ by choosing β, β' so that $\beta\delta \equiv 1$, $\beta\alpha \equiv \beta'$, giving $(03) = (11)$.

Finally, from $1 + \beta + \gamma \equiv 0$ we similarly derive both $\delta + 1 + \beta' \equiv 0$ and $\gamma' + \delta' + 1 \equiv 0$, and conclude that $(12) = (13) = (23)$.

We have thus obtained eleven equations among our sixteen unknowns, reducing them to five. The scheme S can therefore be written as

$$\begin{array}{cccc} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i \end{array}$$

Three further equations of condition can easily be added. Every number in A, except the last, $p - 1$, must be followed by a number in one of the collections A, B, C or D. Thus

$$(00) + (01) + (02) + (03) = 2n - 1$$

and likewise

$$(10)+(11)+(12)+(13)=2n$$
$$(20)+(21)+(22)+(23)=2n$$
$$(30)+(31)+(32)+(33)=2n$$

In the notation just introduced, the first three equations give

$$h+i+k+l=2n-1$$
$$i+l+2m=2n$$
$$k+m=n$$

The fourth is identical to the second. These equations allow us to eliminate three unknowns, so that all sixteen have now been reduced to two.

17.

To determine them completely, it will be useful to investigate the number of solutions of the congruence

$$1+\alpha+\beta+\gamma\equiv 0 \pmod{p}$$

where α,β,γ denote arbitrary numbers in A,B,C. Clearly $\alpha=p-1$ is inadmissible, since $\beta+\gamma\equiv 0$ cannot hold. Substituting the remaining values for α in turn gives h,i,k,l values of $1+\alpha$ belonging to A,B,C,D, respectively. For each *given* value of $1+\alpha$ belonging to A, say $1+\alpha=\alpha^0$, the congruence $\alpha^0+\beta+\gamma\equiv 0$ admits as many solutions as $1+\beta'+\gamma'\equiv 0$ (put $\beta\equiv\alpha^0\beta'$, $\gamma\equiv\alpha^0\gamma'$), that is, $(12)=m$ solutions. Likewise, for each given value of $1+\alpha$ belonging to B, say $1+\alpha=\beta^0$, the congruence $\beta^0+\beta+\gamma\equiv 0$ has as many solutions as $1+\alpha'+\beta'\equiv 0$ (put $\beta\equiv\beta^0\alpha'$, $\gamma\equiv\beta^0\beta'$), that is, $(01)=i$ solutions. Similarly, for each given value of $1+\alpha$ belonging to C, say $1+\alpha=\gamma^0$, the congruence $\gamma^0+\beta+\gamma\equiv 0$ can be solved in as many different ways as $1+\delta+\alpha'\equiv 0$ (put $\beta\equiv\gamma^0\delta$, $\gamma\equiv\gamma^0\alpha'$), so the number of solutions is $(03)=l$. Finally, for each given value of $1+\alpha$ belonging to D, say $1+\alpha=\delta^0$, the congruence $\delta^0+\beta+\gamma\equiv 0$ has as many solutions as $1+\gamma'+\delta'\equiv 0$ (put $\beta\equiv\delta^0\gamma'$, $\gamma\equiv\delta^0\delta'$), that is, $(23)=m$ solutions. Adding all these counts, the congruence $1+\alpha+\beta+\gamma\equiv 0$ clearly admits

$$hm+ii+kl+lm$$

different solutions.

In exactly the same way we find that, on substituting for β the numbers in B in turn, the sum $1+\beta$ takes respectively $(10),(11),(12),(13)$, or i,l,m,m, values belonging to A,B,C,D. For each *given* value of $1+\beta$ belonging to these collections, the congruence $1+\beta+\alpha+\gamma\equiv 0$ admits respectively

$(02), (31), (20), (13)$, or k, m, k, m, different solutions. The total number of solutions is therefore

$$= ik + lm + km + mm$$

We obtain the same value by basing the calculation on the values of the sum $1 + \gamma$.

18.

These two expressions for the same count give the equation

$$0 = hm + ii + kl - ik - km - mm$$

and hence, eliminating h by means of $h = 2m - k - 1$,

$$0 = (k - m)^2 + ii + kl - ik - kk - m$$

The last two equations of Article 16 give $k = \frac{1}{2}(l + i)$. Substituting this value turns $ii + kl - ik - kk$ into $\frac{1}{4}(l - i)^2$, so the preceding equation, multiplied by 4, becomes

$$0 = 4(k - m)^2 + (l - i)^2 - 4m$$

Since $4m = 2(k + m) - 2(k - m) = 2n - 2(k - m)$, it follows that

$$2n = 4(k - m)^2 + 2(k - m) + (l - i)^2$$

or

$$8n + 1 = (4(k - m) + 1)^2 + 4(l - i)^2$$

Thus, putting

$$4(k - m) + 1 = a, \quad 2l - 2i = b$$

we have

$$p = aa + bb$$

It is known that p can be decomposed into two squares in exactly one way, with the odd square taken as aa and the even square as bb, so aa, bb are completely determined numbers. But a itself is also completely determined: the square root must be taken positive or negative according as the positive root has the form $4M+1$ or $4M+3$. We shall shortly discuss how to determine the sign of b.

Combining these new equations with the last three equations of Article 16 completely determines the five numbers h, i, k, l, m in terms of a, b and n, as follows:

$$\begin{aligned} 8h &= 4n - 3a - 5 \\ 8i &= 4n + a - 2b - 1 \\ 8k &= 4n + a - 1 \\ 8l &= 4n + a + 2b - 1 \\ 8m &= 4n - a + 1 \end{aligned}$$

If, in place of n, we prefer to use the modulus p, the scheme S, with every entry multiplied by 16 to avoid fractions, is

$p-6a-11$	$p+2a-4b-3$	$p+2a-3$	$p+2a+4b-3$
$p+2a-4b-3$	$p+2a+4b-3$	$p-2a+1$	$p-2a+1$
$p+2a-3$	$p-2a+1$	$p+2a-3$	$p-2a+1$
$p+2a+4b-3$	$p-2a+1$	$p-2a+1$	$p+2a-4b-3$

19.

It remains to show how to choose the sign of b. In Article 10 we pointed out that the distinction between B and D, which is not intrinsic, depends on the choice of f, for which either root of $xx \equiv -1$ must be taken, and that the two collections are interchanged when one root is replaced by the other. Inspection of the scheme just given shows that a similar interchange accompanies a change in the sign of b. We can therefore foresee that there must be a connection between the sign of b and f. To find it, we first observe that, if μ denotes a nonnegative integer and z takes all the values $1, 2, 3 \ldots . p-1$, then modulo p we have either $\Sigma z^\mu \equiv 0$ or $\Sigma z^\mu \equiv -1$, according as μ is not divisible by $p-1$ or is divisible by it. The latter part of the theorem follows from the fact that for a value of μ divisible by $p-1$, $z^\mu \equiv 1$. We prove the former part as follows. Let g denote a primitive root. All the values of z coincide with the least residues of all g^y when y takes all the values $0, 1, 2, 3 \ldots . p-2$, and hence $\Sigma z^\mu \equiv \Sigma g^{\mu . y}$. Now

$$\Sigma g^{\mu y} = \frac{g^{\mu(p-1)} - 1}{g^\mu - 1}, \quad \text{and hence}$$
$$(g^\mu - 1)\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0$$

For a value of μ not divisible by $p-1$, g^μ cannot be congruent to 1, or equivalently $g^\mu - 1$ cannot be divisible by p. Hence $\Sigma z^\mu \equiv 0$. Q. E. D.

Now expand the power $(z^4+1)^{\frac{1}{4}(p-1)}$ by the binomial theorem. The preceding lemma gives

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \text{ (mod. } p)$$

The least residues of all z^4 give all the numbers in A, each occurring four times. Among the least residues of z^4+1 we therefore have

$$\begin{array}{ll} 4(00) & \text{to } A \\ 4(01) & \text{to } B \\ 4(02) & \text{to } C \\ 4(03) & \text{to } D \end{array}$$

belonging to those classes, and four are $= 0$ (namely, when $z^4 \equiv p-1$). Using the criteria for the collections A, B, C, D, we obtain

$$\begin{aligned} \Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv\ & 4(00) + 4f(01) \\ & - 4(02) - 4f(03) \end{aligned}$$

and hence

$$-2 \equiv 4(00) + 4f(01) - 4(02) - 4f(03)$$

or, substituting for $(00), (01)$, etc., the values found in the preceding article,

$$-2 \equiv -2a - 2 - 2bf$$

We therefore conclude that we must always have $a + bf \equiv 0$, or, multiplying by f,

$$b \equiv af$$

This congruence determines the sign of b when f has already been chosen, or determines f when the sign of b is prescribed in some other way.

20.

Having completely solved our problem for moduli of the form $8n+1$, we turn to the other case, where p has the form $8n+5$. We can treat it more briefly, since all the arguments differ little from the preceding ones.

Since, for such a modulus, -1 belongs to class C, the numbers in the collections A, B, C, D have their complements to the sum p in the classes C, D, A, B, respectively. It follows readily that

symbol	denotes the number of solutions of the congruence
(00)	$1+\alpha+\gamma \equiv 0$
(01)	$1+\alpha+\delta \equiv 0$
(02)	$1+\alpha+\alpha' \equiv 0$
(03)	$1+\alpha+\beta \equiv 0$
(10)	$1+\beta+\gamma \equiv 0$
(11)	$1+\beta+\delta \equiv 0$
(12)	$1+\beta+\alpha \equiv 0$
(13)	$1+\beta+\beta' \equiv 0$
(20)	$1+\gamma+\gamma' \equiv 0$
(21)	$1+\gamma+\delta \equiv 0$
(22)	$1+\gamma+\alpha \equiv 0$
(23)	$1+\gamma+\beta \equiv 0$
(30)	$1+\delta+\gamma \equiv 0$
(31)	$1+\delta+\delta' \equiv 0$
(32)	$1+\delta+\alpha \equiv 0$
(33)	$1+\delta+\beta \equiv 0$

from which we immediately obtain six equations:

$$(00)=(22), \quad (01)=(32), \quad (03)=(12),$$
$$(10)=(23), \quad (11)=(33), \quad (21)=(30)$$

Multiplying the congruence $1+\alpha+\gamma \equiv 0$ by a number γ' from the collection C, chosen so that $\gamma\gamma' \equiv 1$, and taking for γ'' the least residue of the product $\alpha\gamma'$, which must evidently also belong to the collection C, gives $\gamma'+\gamma''+1 \equiv 0$, from which we conclude that $(00)=(20)$.

In exactly the same way we obtain the equations $(01)=(13)$, $(03)=(31)$, $(10)=(11)=(21)$.

With these eleven equations we can reduce our sixteen unknowns to five and write the scheme S as follows:

$$\begin{array}{cccc} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m \end{array}$$

We also have the equations

$$\begin{aligned}(00)+(01)+(02)+(03)&=2n+1\\(10)+(11)+(12)+(13)&=2n+1\\(20)+(21)+(22)+(23)&=2n\\(30)+(31)+(32)+(33)&=2n+1\end{aligned}$$

or, using the notation just introduced, these three (I):

$$\begin{aligned}h+i+k+l&=2n+1\\2m+i+l&=2n+1\\h+m&=n\end{aligned}$$

With their help we can therefore now reduce our unknowns to two.

We shall derive the remaining equations by considering the number of solutions of the congruence $1+\alpha+\beta+\gamma\equiv 0$ (here too, α,β,γ denote unspecified numbers from the collections A,B,C, respectively). Consider *first* that $1+\alpha$ gives h,i,k,l numbers belonging to A,B,C,D, respectively, and that for each given value of α in these four cases there are m,l,i,m solutions, respectively. The total number of solutions will be

$$=hm+il+ik+lm$$

Second, since $1+\beta$ gives m,m,l,i numbers belonging to A,B,C,D, and for each *given* value of β in these four cases there are h,m,h,m solutions, the total number of solutions will be

$$=hm+mm+hl+im$$

From this we derive the equation

$$0=mm+hl+im-il-ik-lm$$

which, using the equation $k=2m-h$ obtained from (I), becomes

$$0=mm+hl+hi-il-im-lm$$

Now from equations I we also have $l+i=1+2h$, and hence

$$\begin{aligned}2i&=1+2h+(i-l)\\2l&=1+2h-(i-l)\end{aligned}$$

Substituting these values into the preceding equation gives

$$0=4mm-4m-1-8hm+4hh+(i-l)^2$$

If, finally, we replace $4m$ here with $2(h+m)-2(h-m)$, or, by the last equation in I, with $2n-2(h-m)$, we obtain

$$0 = 4(h-m)^2 - 2n + 2(h-m) - 1 + (i-l)^2$$

and hence

$$8n + 5 = (4(h-m)+1)^2 + 4(i-l)^2$$

Thus, putting

$$4(h-m)+1 = a, \quad 2i-2l = b$$

gives

$$p = aa + bb$$

Since here too p can be split in only one way into two squares, one even and the other odd, aa and bb will be completely determined numbers: evidently aa must be set equal to the odd square and bb to the even one. Moreover, the *sign* of a must be chosen so that $a \equiv 1 \pmod 4$, and the sign of b so that $b \equiv af \pmod p$, as is readily proved by arguments entirely similar to those used in the preceding article.

With these preliminaries, the five numbers h, i, k, l, m are determined in terms of a, b and n as follows:

$$\begin{aligned} 8h &= 4n + a - 1 \\ 8i &= 4n + a + 2b + 3 \\ 8k &= 4n - 3a + 3 \\ 8l &= 4n + a - 2b + 3 \\ 8m &= 4n - a + 1 \end{aligned}$$

Or, if we prefer expressions in terms of p, the terms of the scheme S, multiplied by 16, will be as follows:

$p+2a-7$	$p+2a+4b+1$	$p-2a+1$	$p+2a-4b+1$
$p-2a-3$	$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$
$p+2a-7$	$p-2a-3$	$p+2a-7$	$p-2a-3$
$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$	$p-2a-3$

21.

Having solved our problem, we return to the main investigation, now undertaking the complete determination of the collection to which the number 2 belongs.

I. Whenever p has the form $8n+1$, we already know that the number 2 lies either in the collection A or in the collection C. In the former case we readily see that the numbers $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ also belong to A, and in the latter to C. Now consider that, if α and $\alpha+1$ are consecutive numbers in the collection A, then $p-\alpha-1$, $p-\alpha$ are also such numbers; or, equivalently, numbers in the collection A that are followed by a number in the same collection are always paired (α and $p-1-\alpha$). Their number, (00), will therefore always be even, unless one is paired with itself, that is, unless $\frac{1}{2}(p-1)$ belongs to A, in which case their number will be odd. From this we conclude that (00) is odd whenever 2 belongs to the collection A, and even whenever 2 belongs to C. But we have

$$16(00) = aa + bb - 6a - 11$$

or, putting $a = 4q+1$, $b = 4r$ (see Article 14),

$$(00) = qq - q + rr - 1$$

Since $qq-q$ is evidently always even, (00) will be odd or even according as r is even or odd. Thus 2 will belong to A or to C according as b has the form $8m$ or the form $8m+4$. This is precisely the theorem found by inductive investigation in Article 14.

II. We can treat the other case, where p has the form $8n+5$, just as completely. Here the number 2 belongs either to B or to D. We readily see that in the former case $\frac{1}{2}(p-1)$ belongs to B and $\frac{1}{2}(p+1)$ to D, whereas in the latter $\frac{1}{2}(p-1)$ belongs to D and $\frac{1}{2}(p+1)$ to B. Now consider that, if β is a number from B followed by a number from D, then $p-\beta-1$ will also be a number from B and $p-\beta$ from D; that is, numbers with this property always occur in pairs. Their number, (13), will therefore be even, except when one of them is paired with itself, that is, when $\frac{1}{2}(p-1)$ belongs to B and $\frac{1}{2}(p+1)$ to D; in this case (13) will be odd. From this we conclude that (13) is even whenever 2 belongs to D, and odd whenever 2 belongs to B. But we have

$$16(13) = aa + bb + 2a + 4b + 1$$

or, putting $a = 4q+1$, $b = 4r+2$,

$$(13) = qq + q + rr + 2r + 1$$

Thus (13) will be odd whenever r is even; conversely, (13) will be even whenever r is odd. From this we conclude that 2 belongs to B whenever b has the form $8m+2$, and to D whenever b has the form $8m+6$.

The result of these investigations can be stated as follows:

The number 2 *belongs to the collection* A, B, C *or* D *according as the number* $\frac{1}{2}b$ *has the form* $4m$, $4m+1$, $4m+2$ *or* $4m+3$.

22.

In the *Disquisitiones Arithmeticae* we explained the general theory of circle division and of the solution of the equation $x^p - 1 = 0$. Among other things, we showed that, if μ is a divisor of the number $p-1$, the function $\frac{x^p-1}{x-1}$ can be split into μ factors of degree $\frac{p-1}{\mu}$ with the help of an auxiliary equation of degree μ. Besides the general theory of this factorization, we separately considered the special cases where $\mu = 2$ or $\mu = 3$ in Articles 356–358 of that work, and showed how to give the auxiliary equation a priori, that is, without working out the scheme of least residues of the powers of a primitive root for the modulus p. Even without our pointing it out, attentive readers will readily see the very close connection between the next case of that theory, namely $\mu = 4$, and the investigations developed here in Articles 15–20, with whose help that case too can be treated completely without difficulty. But we reserve this treatment for another occasion, and accordingly have preferred to carry out the investigation in this paper in a purely arithmetical form, without bringing in the theory of the equation $x^p - 1 = 0$ at all. Instead, as a finishing touch, we shall add some further new, purely arithmetical theorems very closely connected with the subject treated so far.

23.

If the power $(x^4+1)^{\frac{1}{2}(p-1)}$ is expanded by the binomial theorem, there will be three terms in which the exponent of x is divisible by $p-1$, namely

$$x^{2(p-1)}, \quad Px^{p-1} \quad \text{and } 1$$

where P denotes the middle coefficient

$$\frac{\frac{1}{2}(p-1) \,.\, \frac{1}{2}(p-3) \,.\, \frac{1}{2}(p-5) \,.\, \ldots \,.\, \frac{1}{4}(p+3)}{1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, \frac{1}{4}(p-1)}$$

Thus, substituting for x the numbers $1, 2, 3 \ldots p-1$ in turn, we obtain by the lemma in Article 19

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2 - P$$

But, considering what we explained in Article 19, and also that the numbers in the collections A, B, C, D, raised to the power with exponent $\frac{1}{2}(p-1)$, are congruent modulo p to the numbers $+1, -1, +1, -1$, respectively, we readily see that

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv 4(00) - 4(01) + 4(02) - 4(03)$$

and hence, by the schemes given at the ends of Articles 18, 20,

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2a - 2$$

Comparing these two values gives a particularly elegant theorem: we have

$$P \equiv 2a \pmod{p}$$

Denoting the four products

$$\begin{array}{l} 1 \,.\, 2 \,.\, 3 \,.\, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \,.\, \frac{1}{4}(p-1) \\ \frac{1}{4}(p+3) \,.\, \frac{1}{4}(p+7) \,.\, \frac{1}{4}(p+11) \,.\, \ldots\ldots \,.\, \frac{1}{2}(p-1) \\ \frac{1}{2}(p+1) \,.\, \frac{1}{2}(p+3) \,.\, \frac{1}{2}(p+5) \,.\, \ldots\ldots \,.\, \frac{3}{4}(p-1) \\ \frac{1}{4}(3p+1) \,.\, \frac{1}{4}(3p+5) \,.\, \frac{1}{4}(3p+9) \,.\, \ldots\ldots \,.\, (p-1) \end{array}$$

by q, r, s, t, respectively, we can write the preceding theorem as

$$2a \equiv \frac{r}{q} \pmod{p}$$

Since each factor of q has its complement to p in t, we have $q \equiv t \pmod{p}$ whenever the number of factors is even, that is, whenever p has the form $8m+1$, and $q \equiv -t$ whenever the number of factors is odd, or p has the form $8m+5$. Likewise, in the former case $r \equiv s$, and in the latter $r \equiv -s$. In both cases $qr \equiv st$, and since we know that $qrst \equiv -1$, we have $qqrr \equiv -1$, and hence $qr \equiv \pm f \pmod{p}$. Combining this congruence with the theorem just found gives $rr \equiv \pm 2af$, and thus, by Articles 19, 20,

$$2b \equiv \pm rr \pmod{p}^{*)}$$

It is very remarkable that the splitting of the number p into two squares can be found by entirely direct operations: the root of the odd square will be the least absolute residue of $\frac{r}{2q}$, and the root of the even square the least absolute residue of $\frac{1}{2}rr$ modulo p. The expression $\frac{r}{2q}$, whose value for $p = 5$ is $= 1$, can also be written as follows for larger values of p:

$$\frac{6 \,.\, 10 \,.\, 14 \,.\, 18 \,.\, \ldots \,.\, (p-3)}{2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, \ldots \,.\, \frac{1}{4}(p-1)}$$

But since we also know the sign with which this formula gives the root of the odd square, namely the sign that always makes it of the form $4m+1$, it deserves particular attention that a similar general criterion for the sign of the root of the even square has not yet been found. If anyone finds such a criterion and communicates it to us, we shall be very grateful. Meanwhile, it seemed appropriate to include here the values of the numbers a, b, f obtained, for values of p below 200, from the least residues of the expressions $\frac{r}{2q}$, $\frac{1}{2}rr$, qr.

*) and $\{(a \mp b)q\}^2 \equiv a \equiv \left(\frac{r-qrr}{2}\right)^2$

p	a	b	f
5	+1	+2	2
13	−3	−2	5
17	+1	−4	13
29	+5	+2	12
37	+1	−6	31
41	+5	+4	9
53	−7	−2	23
61	+5	−6	11
73	−3	−8	27
89	+5	−8	34
97	+9	+4	22
101	+1	−10	91
109	−3	+10	33
113	−7	+8	15
137	−11	+4	37
149	−7	−10	44
157	−11	−6	129
173	+13	+2	80
181	+9	+10	162
193	−7	+12	81
197	+1	−14	183

THEORY

OF BIQUADRATIC RESIDUES

SECOND PAPER

BY

CARL FRIEDRICH GAUSS

PRESENTED TO THE ROYAL SOCIETY ON APRIL 15, 1831.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VII.
Göttingen MDCCCXXXII.

THEORY OF BIQUADRATIC RESIDUES.

SECOND PAPER.

24.

In the first paper we completely dealt with everything required for the biquadratic classification of the number $+2$. Namely, we think of all numbers not divisible by the modulus p (assumed to be a prime number of the form $4n+1$) as distributed among four collections A, B, C, D, according as each, raised to the power with exponent $\frac{1}{4}(p-1)$, becomes congruent modulo p to $+1$, $+f$, -1, $-f$, with f denoting either root of the congruence $ff \equiv -1 \pmod{p}$. We found that the decision as to which collection the number $+2$ belongs to depends on splitting the number p into two squares: if we put $p = aa + bb$, with aa denoting the odd square and bb the even one, and further assume that the *signs* of a, b are chosen so that $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$, then the number $+2$ must belong to the collection A, B, C, D according as $\frac{1}{2}b$ has the form $4n$, $4n+1$, $4n+2$, $4n+3$, respectively.

A rule for classifying the number -2 also follows immediately. Since -1 belongs to class A when $\frac{1}{2}b$ is even, and to class C when it is odd, the theorem in Article 7 shows that the number -2 belongs to class A, B, C, D according as $\frac{1}{2}b$ has the form $4n$, $4n+3$, $4n+2$, $4n+1$, respectively.

These theorems can also be expressed as follows:

Belongs	$+2$	-2
to the collection	if b, modulo 8, is congruent to	
A	0	0
B	$2a$	$6a$
C	$4a$	$4a$
D	$6a$	$2a$

We readily see that, stated in this way, the theorems no longer depend on the condition $a \equiv 1 \pmod{4}$, but still hold if $a \equiv 3 \pmod{4}$, provided that the other condition, $af \equiv b \pmod{p}$, is maintained.

It is equally easy to see that the content of these theorems can be elegantly condensed into a single formula, namely:

if a and b are taken positive, we always have

$$b^{\frac{1}{2}ab} \equiv a^{\frac{1}{2}ab}\, 2^{\frac{1}{4}(p-1)} \pmod{p}$$

25.

Let us now see how far inductive investigation points towards the classification of the number 3. The table in Article 11, continued further (always taking the least primitive root), shows that +3 belongs

to the collection

A for			B for			C for			D for		
p	a	b	p	a	b	p	a	b	p	a	b
13	−3	+2	17	+1	−4	37	+1	−6	5	+1	+2
109	−3	+10	29	+5	+2	61	+5	−6	41	+5	−4
181	+9	+10	53	−7	+2	73	−3	−8	149	−7	+10
193	−7	−12	89	+5	−8	97	+9	+4	173	+13	+2
229	−15	+2	101	+1	+10	157	−11	−6			
277	+9	+14	113	−7	−8	241	−15	−4			
			137	−11	−4						
			197	+1	−14						
			233	+13	+8						
			257	+1	−16						
			269	+13	+10						
			281	+5	+16						
			293	+17	+2						

At least at first sight, we see no simple connection between the values of the numbers a, b to which the same collection corresponds. But, considering that a similar decision in the theory of quadratic residues is made by a simpler rule for the number −3 than for the number +3, we may hope for equally favourable success in the theory of biquadratic residues. We find that −3 belongs to the collection

A for			B for			C for			D for		
p	a	b	p	a	b	p	a	b	p	a	b
37	+1	−6	5	+1	+2	13	−3	+2	29	+5	+2
61	+5	−6	17	+1	−4	73	−3	−8	41	+5	−4
157	−11	−6	89	+5	−8	97	+9	+4	53	−7	+2
193	−7	−12	113	−7	−8	109	−3	+10	101	+1	+10
			137	−11	−4	181	+9	+10	197	+1	−14
			149	−7	+10	229	−15	+2	269	+13	+10
			173	+13	+2	241	−15	−4	293	+17	+2
			233	+13	+8	277	+9	+14			
			257	+1	−16						
			281	+5	+16						

where the law suggested by inductive investigation presents itself at once. Namely, -3 belongs to the collection

A, whenever b is divisible by 3, equivalently $b \equiv 0 \pmod 3$
B, whenever $a + b$ is divisible by 3, equivalently $b \equiv 2a \pmod 3$
C, whenever a is divisible by 3, equivalently $a \equiv 0 \pmod 3$
D, whenever $a - b$ is divisible by 3, equivalently $b \equiv a \pmod 3$

26.

We find that the number $+5$ is to be assigned to the collection

A for $p =$	101, 109, 149, 181, 269
B for $p =$	13, 17, 73, 97, 157, 193, 197, 233, 277, 293
C for $p =$	29, 41, 61, 89, 229, 241, 281
D for $p =$	37, 53, 113, 137, 173, 257

Considering the values of the numbers a, b corresponding to each p, we find the law here as readily as for the classification of the number -3. Namely, we arrive at the collection

A, whenever $b \equiv 0 \pmod 5$
B, whenever $b \equiv a$
C, whenever $a \equiv 0$
D, whenever $b \equiv 4a$

These rules evidently cover all cases, since for $b \equiv 2a$ or $b \equiv 3a \pmod 5$ we would have $aa + bb \equiv 0$, Q. E. A., since by hypothesis p is a prime number different from 5.

27.

Likewise, inductive investigation applied to the numbers -7, -11, $+13$, $+17$, -19, -23 and carried far enough points to the following rules:

For the number -7

A	$a \equiv 0$, or $b \equiv 0 \pmod 7$
B	$b \equiv 4a$, or $b \equiv 5a$
C	$b \equiv a$, or $b \equiv 6a$
D	$b \equiv 2a$, or $b \equiv 3a$

For the number -11.

A	$b \equiv 0,\ 5a,$ or $6a \pmod{11}$
B	$b \equiv a,\ 3a$ or $4a$
C	$a \equiv 0,$ or $b \equiv 2a$ or $9a$
D	$b \equiv 7a,\ 8a$ or $10a$

For the number +13.

A	$b \equiv 0,\ 4a,\ 9a \pmod{13}$
B	$b \equiv 6a,\ 11a,\ 12a$
C	$a \equiv 0;\ b \equiv 3a,\ 10a$
D	$b \equiv a,\ 2a,\ 7a$

For the number +17.

A	$a \equiv 0;\ b \equiv 0,\ a,\ 16a \pmod{17}$
B	$b \equiv 2a,\ 6a,\ 8a,\ 14a$
C	$b \equiv 5a,\ 7a,\ 10a,\ 12a$
D	$b \equiv 3a,\ 9a,\ 11a,\ 15a$

For the number −19.

A	$b \equiv 0,\ 2a,\ 5a,\ 14a,\ 17a \pmod{19}$
B	$b \equiv 3a,\ 7a,\ 11a,\ 13a,\ 18a$
C	$a \equiv 0;\ b \equiv 4a,\ 9a,\ 10a,\ 15a$
D	$b \equiv a,\ 6a,\ 8a,\ 12a,\ 16a$

For the number −23.

A	$a \equiv 0;\ b \equiv 0,\ 7a,\ 10a,\ 13a,\ 16a \pmod{23}$
B	$b \equiv 2a,\ 3a,\ 4a,\ 11a,\ 15a,\ 17a$
C	$b \equiv a,\ 5a,\ 9a,\ 14a,\ 18a,\ 22a$
D	$b \equiv 6a,\ 8a,\ 12a,\ 19a,\ 20a,\ 21a$

28.

The special theorems obtained in this way by inductive investigation are found to be confirmed as far as that investigation is continued, and reveal a particularly beautiful form of the criteria. But when they are compared with one another to draw general conclusions, the following observations immediately present themselves.

The criteria for deciding which collection the prime number $\pm q$ belongs to (taking the upper or lower sign according as q has the form $4n+1$ or $4n+3$) depend on the forms of the numbers a, b compared with one another with respect to the modulus q. Namely,

I. Whenever $a \equiv 0 \pmod{q}$, $\pm q$ belongs to a definite collection, which is A for $q = 7,\ 17,\ 23$, and C for $q = 3,\ 11,\ 13,\ 19$. This suggests the conjecture that the former case holds generally whenever q has the form $8n \pm 1$, and the latter whenever q has the form $8n \pm 3$. Moreover, the collections B and D can already be excluded without inductive investigation when the value of a is divisible by q, in which case $p \equiv bb \pmod{q}$, that is, p is a quadratic residue of q; hence, by the fundamental theorem, $\pm q$ must be a quadratic residue of p.

II. When a is not divisible by q, the criterion depends on the value of the expression $\frac{b}{a} \pmod{q}$. This expression does admit q different values, namely $0,\ 1,\ 2,\ 3 \ldots . q - 1$; but whenever q has the form $4n + 1$, the two values of the expression $\sqrt{-1} \pmod{q}$ must be excluded. They evidently cannot be values of the expression $\frac{b}{a} \pmod{q}$, since $p = aa + bb$ is always assumed to be a prime number different from q. The number of admissible values of the expression $\frac{b}{a} \pmod{q}$ is therefore $= q - 2$ for $q \equiv 1 \pmod{4}$, while it remains $= q$ for $q \equiv 3 \pmod{4}$.

These values are now distributed among four classes: some, to be denoted without further specification by α, correspond to the collection A; others, denoted by β, to the collection B; others, γ, to the collection C; and finally the rest, δ, to the collection D. Thus $\pm q$ is to be assigned to the collection A, B, C, D according as $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, $b \equiv \delta a \pmod{q}$.

But the *law* of this distribution seems more deeply hidden, although some general features are readily noticed. The number of values in three of the classes is found to be the same, namely $= \frac{1}{4}(q - 1)$ or $\frac{1}{4}(q + 1)$, while in one (specifically, the one corresponding to the collection with the criterion $a \equiv 0$) it is smaller by one. Thus the total number of different criteria for each collection is the same, namely $= \frac{1}{4}(q - 1)$ or $\frac{1}{4}(q + 1)$. We further observe that 0 is always found in the first class (among the α), and that the complements of the numbers $\alpha, \beta, \gamma, \delta$ to q, namely $q - \alpha$, $q - \beta$, $q - \gamma$, $q - \delta$, are found in the first, fourth, third and second classes, respectively. Finally, we see that the values of the expressions $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta} \pmod{q}$ belong to the first, fourth, third and second classes whenever the criterion $a \equiv 0$ corresponds to the collection A, but to the third, second, first and fourth classes, respectively, whenever the criterion $a \equiv 0$ refers to the collection C. But this is about the limit of what can be reached by inductive investigation, unless we rather boldly presume to anticipate what will later be drawn from the genuine sources.

29.

Before going further, we should note that the criteria for prime numbers (taken positively when they have the form $4n + 1$, negatively when they have the form $4n + 3$) suffice to decide the question for all other numbers, provided that the theorem of Article 7 and the criteria for -1 and ± 2 are also used.

Thus, for example, if criteria for the number $+3$ are wanted, the criteria given in Article 25, which concern -3, will also hold for $+3$ whenever $\frac{1}{2}b$ is even. The collections A, B, C, D must instead be exchanged with the collections C, D, A, B whenever $\frac{1}{2}b$ is odd, giving the following rules:

$+3$ belongs

to the collection	if
A	$b \equiv 0 \pmod{12}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 2 \pmod 4$
B	$b \equiv 8a$ or $10a \pmod{12}$
C	$b \equiv 6a \pmod{12}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 4$
D	$b \equiv 2a$ or $4a \pmod{12}$

Likewise, the criteria for ± 6 are obtained by combining the criteria for ∓ 2 and -3; namely,

$+6$ belongs

to the collection	if
A	$b \equiv 0,\quad 2a, 22a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 4a \pmod 8$
B	$b \equiv 4a,\quad 6a,\quad 8a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 2a \pmod 8$
C	$b \equiv 10a, 12a, 14a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 8$
D	$b \equiv 16a, 18a, 20a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 6a \pmod 8$

while -6 belongs

to the collection	if
A	$b \equiv 0,\quad 10a, 14a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 4a \pmod 8$
B	$b \equiv 4a,\quad 8a, 18a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 6a \pmod 8$
C	$b \equiv 2a, 12a, 22a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 0 \pmod 8$
D	$b \equiv 6a, 16a, 20a \pmod{24}$; or simultaneously $a \equiv 0 \pmod 3,\ b \equiv 2a \pmod 8$

In the same way, the criteria for the number $+21$ will be assembled from the criteria for -3 and -7; the criteria for -105 from those for -1, -3, $+5$, -7, etc.

30.

Inductive investigation thus opens up a very rich harvest of particular theorems related to the theorem for the number 2. But a common bond is lacking, rigorous proofs are lacking, since the method by which we completed the treatment of the number 2 in the first paper admits no further application. There are indeed various methods by which proofs could be obtained for particular cases, especially those concerning the distribution of quadratic residues between the collections A, C. We do not dwell on them, however, since a general theory embracing *all* cases must be our aim. Having begun to devote our thoughts to this matter in 1805, we soon became convinced that the true source of the general theory must be sought in an extension of the domain of arithmetic, as we already indicated in Article 1.

While higher arithmetic, in the questions treated so far, deals only with real integers, the theorems on biquadratic residues shine in their full simplicity and genuine beauty only when the domain of arithmetic is extended to *imaginary* quantities. Its objects are then, without restriction, numbers of the form $a + bi$, where i denotes, as usual, the imaginary quantity $\sqrt{-1}$, and a, b range without restriction over all real integers between $-\infty$ and $+\infty$. We shall call such numbers *complex integers*, treating real numbers as a species contained within the complex numbers rather than as opposed to them. The present paper will set out both the elementary theory of complex numbers and the first beginnings of the theory of biquadratic residues, which we shall undertake to complete in every respect in a subsequent continuation*).

*)We should at least mention here in passing that the domain thus defined is particularly suited to the theory of biquadratic residues. The theory of cubic residues must similarly be built on the consideration of numbers of the form $a + bh$, where h is an imaginary root of the equation $h^3 - 1 = 0$, say $h = -\frac{1}{2} + \sqrt{\frac{3}{4}} \,.\, i$; and likewise the theory of residues of higher powers will require the introduction of other imaginary quantities.

31.

First we introduce some names that will help us to be brief and clear. The domain of complex numbers $a + bi$ contains

I. real numbers, where $b = 0$, and among these, according to the nature of a,

1) zero,

2) positive numbers,

3) negative numbers;

II. imaginary numbers, where b is unequal to zero. Here we distinguish in turn

1) imaginary numbers without a real part, that is, where $a = 0$;

2) imaginary numbers with a real part, where b is nonzero and $a = 0$ also does not hold.

The former may, if desired, be called pure imaginary numbers, and the latter mixed imaginary numbers.

In this theory we use four units, $+1$, -1, $+i$, $-i$, which will be called simply positive, negative, positive imaginary and negative imaginary.

We shall call the three products of any complex number by -1, $+i$, $-i$ its *companions* or *numbers associated with it*. Thus, except for zero (which is associated with itself), four *distinct* numbers are always associated.

By contrast, we call the number obtained from a complex number by exchanging i with $-i$ its *conjugate*. Among imaginary numbers, therefore, two *distinct* numbers are always conjugate, while real numbers are their own conjugates, if we choose to extend the name to them.

We call the product of a complex number and its conjugate the *norm* of each. The square of a real number is therefore to be taken as its norm.

In general we have eight related numbers, namely,

$$\begin{array}{r|r} a+bi & a-bi \\ -b+ai & -b-ai \\ -a-bi & -a+bi \\ b-ai & b+ai \end{array}$$

in which we see two groups of four associated numbers and four pairs of conjugates; their common norm is $aa + bb$. But the eight numbers reduce to four distinct ones whenever either $a = \pm b$, or $a, b = 0$ for one of the two numbers.

The following results follow immediately from these definitions:

The conjugate of the product of two complex numbers is the product of their conjugates.

The same holds for a product of more factors, and also for quotients.

The norm of the product of two complex numbers is equal to the product of their norms.

This theorem also extends to products of any number of factors and to quotients.

The norm of any complex number (except zero, an exception that from now on we shall generally leave understood) is a *positive* number.

Moreover, nothing prevents us from extending our definitions to fractional or even irrational values of a, b; but $a + bi$ will be called a complex integer only when *each* of a, b is an integer, and rational only when *each* of a, b is rational.

32.

The rules for arithmetic operations on complex numbers are well known: introducing the norm reduces division to multiplication, since

$$\frac{a+bi}{c+di} = (a+bi)\,.\,\frac{c-di}{cc+dd} = \frac{ac+bd}{cc+dd} + \frac{bc-ad}{cc+dd}\,.\,i$$

The square root is extracted with the help of the formula

$$\sqrt{(a+bi)} = \pm\left(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} + i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}}\right)$$

if b is positive, or of the formula

$$\sqrt{(a+bi)} = \pm\left(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} - i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}}\right)$$

if b is negative. There is no need to dwell here on how transforming the complex quantity $a + bi$ into $r(\cos\varphi + i\sin\varphi)$ makes calculations easier.

33.

We call a complex integer that can be resolved into two factors different from the units[*)] a composite complex number; a number that admits no such factorization will be called a complex prime. It follows immediately that every real composite number is also a composite complex number. But a real prime may be a composite complex number, and this holds for the number 2 and all positive real primes of the form $4n+1$ (except the number 1), since they are known to be decomposable into two positive squares. For example, $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$, $13 = (3+2i)(3-2i)$, $17 = (1+4i)(1-4i)$, etc.

On the other hand, positive real primes of the form $4n+3$ are always complex primes. For if such a number q were $= (a+bi)(\alpha+\beta i)$, we should also have $q = (a-bi)(\alpha-\beta i)$, and therefore $qq = (aa+bb)(\alpha\alpha+\beta\beta)$. But qq can be resolved into positive factors greater than unity in only one way, namely into $q \times q$, so we should have to have $q = aa+bb = \alpha\alpha+\beta\beta$, Q. E. A.; for the sum of two squares cannot have the form $4n+3$.

Negative real numbers evidently retain the same names as positive ones, and the same holds for pure imaginary numbers.

It therefore remains to show how to distinguish composites from primes among mixed imaginary numbers. This is done by the following

THEOREM. *Every mixed imaginary integer $a+bi$ is a complex prime or a composite number according as its norm is a real prime or a composite number.*

Proof. I. Since the norm of a composite complex number is always composite, a complex number whose norm is a real prime must evidently be a complex prime. Q. E. P.

II. If, however, the norm $aa+bb$ is composite, let p be a positive real prime dividing it. We must now distinguish two cases.

1) If p has the form $4n+3$, we know that $aa+bb$ cannot be divisible by p unless p divides both a, b, so that $a+bi$ will be composite.

[*)] Or, equivalently, factors whose norms are greater than unity.

2) If p does not have the form $4n+3$, it can certainly be decomposed into two squares. We therefore put $p = \alpha\alpha + \beta\beta$. Since

$$(a\alpha + b\beta)(a\alpha - b\beta) = aa(\alpha\alpha + \beta\beta) - \beta\beta(aa + bb)$$

and this is therefore divisible by p, p must divide one of the factors $a\alpha + b\beta$, $a\alpha - b\beta$. Moreover, since

$$(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 = (a\alpha - b\beta)^2 + (b\alpha + a\beta)^2 = (aa + bb)(\alpha\alpha + \beta\beta)$$

and this is therefore divisible by pp, in the first case $b\alpha - a\beta$, and in the second $b\alpha + a\beta$, must also be divisible by p. Thus in the first case

$$\frac{a+bi}{\alpha+\beta i} = \frac{a\alpha + b\beta}{p} + \frac{b\alpha - a\beta}{p} \,.\, i$$

will be a complex integer, while in the second

$$\frac{a+bi}{\alpha-\beta i} = \frac{a\alpha - b\beta}{p} + \frac{b\alpha + a\beta}{p} \,.\, i$$

will be an integer. Since the given number is therefore divisible by $\alpha + \beta i$ or by $\alpha - \beta i$, and the norm of the quotient $= \frac{aa+bb}{p}$ differs from unity by hypothesis, $a + bi$ is evidently a composite complex number in either case. Q. E. S.

34.

The following four kinds therefore exhaust the entire range of complex primes:

1) the four units, $1, +i, -1, -i$, which, however, we shall usually leave understood to be excluded when discussing prime numbers;

2) the number $1 + i$ with its three associates $-1 + i$, $-1 - i$, $1 - i$;

3) the positive real primes of the form $4n + 3$ with their three associates each;

4) the complex numbers whose norms are real primes of the form $4n + 1$ greater than unity. To each given norm of this kind there always correspond eight complex primes and no more, since such a norm can be decomposed into two squares in only one way.

35.

Just as real integers are divided into even and odd, and the former in turn into those divisible by four and those that are twice an odd number, an equally essential distinction presents itself among complex numbers. They are either

not divisible by $1+i$, namely numbers $a+bi$ in which one of the numbers a, b is odd and the other even;

or divisible by $1+i$ but not by 2, whenever both a, b are odd;

or divisible by 2, whenever both a, b are even.

The numbers of the first class may suitably be called *odd complex numbers*, those of the second *half-even*, and those of the third *even*.

A product of several complex factors will always be odd when all the factors are odd; half-even when one factor is half-even and the others odd; and even when the factors include at least two half-even ones or at least one even one.

The norm of any odd complex number has the form $4n+1$; the norm of a half-even number has the form $8n+2$; finally, the norm of an even number is the product of a number of the form $4n+1$ and the number 4 or a higher power of two.

36.

Since the relation between four associated complex numbers is analogous to that between two opposite real numbers (that is, numbers equal in absolute value and bearing opposite signs), and the positive one of these is usually and rightly regarded as primary, the question arises whether a similar distinction can be established among four associated complex numbers, and whether it should be considered useful. To decide this, we must consider that the principle of distinction must be such that the product of two numbers regarded as primary among their respective associates always becomes primary among its own associates. But we soon become convinced that no such principle exists at all unless the distinction is restricted to integers; indeed, a *useful* distinction must be limited to odd numbers. For these, however, the proposed aim can be reached in two ways. Namely,

I. The product of two numbers $a+bi, a'+b'i$ such that a, a' have the form $4n+1$ and b, b' are even will have the same property: the real part will be $\equiv 1 \pmod 4$, and the imaginary part even. And it is easy to see that among four associated odd numbers only one has that form.

II. If a number $a+bi$ is such that $a-1$ and b are either both divisible by four or both twice an odd number, its product with a complex number of the same form will have the same form; and it is easy to see that only one of four associated odd numbers has this form.

Of these two principles, which are almost equally suitable, we shall adopt the latter: among four associated odd complex numbers we shall regard as primary the one congruent to the positive unit modulo $2+2i$. This will let us state several notable theorems more concisely. For example, the complex primes $-1+2i$, $-1-2i$, $+3+2i$, $+3-2i$, $+1+4i$, $+1-4i$, etc., are primary, as are the real numbers -3, -7, -11, -19, etc., which must evidently always be taken with a negative sign. The conjugate of an odd primary complex number will also be primary.

For half-even and even numbers in general, a similar distinction would be too arbitrary and of little use. Of the associated primes $1+i$, $1-i$, $-1+i$, $-1-i$, we can indeed choose one as primary in preference to the others, but we shall not extend such a distinction to composites.

37.

If some factors of a composite complex number are themselves composite, and these in turn are resolved into their factors, we evidently arrive eventually at prime factors; that is, every composite number can be resolved into prime factors. If any of these are not primary, replace each by the product of its primary associate and $i, -1$ or $-i$. In this way, every composite complex number M can evidently be reduced to the form

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \dots .$$

where A, B, C, etc., are distinct primary complex primes, and $\mu = 0, 1, 2$ or 3. Concerning this factorization, we have the theorem that it can be carried out in only one way. On a passing consideration this theorem might seem evident in itself, but it certainly needs a proof. The following paves the way to that proof.

THEOREM. *The product $M = A^{\alpha} B^{\beta} C^{\gamma} \dots$, where A, B, C, etc., denote distinct primary complex primes, cannot be divisible by any primary complex prime that does not occur among A, B, C, etc.*

Proof. Let P be a primary complex prime not contained among A, B, C, etc., and let p, a, b, c, etc., be the norms of the numbers P, A, B, C, etc. It follows readily that the norm of M will be $= a^{\alpha} b^{\beta} c^{\gamma}$, etc.; hence, if M were divisible by P, this number would have to be divisible by p. Since the individual norms are either real primes (from the sequence $2, 5, 13, 17$, etc.) or squares of real primes (from the sequence $9, 49, 121$, etc.), this evidently cannot happen unless p is identical with one of the norms a, b, c, etc. We therefore suppose $p = a$. But since P, A are distinct primary complex primes by hypothesis, it is easy to see that these conditions cannot hold together unless P, A are conjugate imaginary complex numbers, and consequently $p = a$ is an odd real prime (not the square of a prime). We therefore suppose $A = k+li$, $P = k-li$.

Hence, extending the notion and notation of congruence to complex integers, we have $A \equiv 2k \pmod{P}$, from which it follows readily that

$$M \equiv 2^\alpha k^\alpha B^\beta C^\gamma \dots . \pmod{P}$$

Therefore, if M is assumed divisible by P, then

$$2^\alpha k^\alpha B^\beta C^\gamma \dots .$$

will also be divisible by P, and consequently the norm of this number, which is

$$= 2^{2\alpha} k^{2\alpha} b^\beta c^\gamma \dots .$$

will be divisible by p. But since 2 and k are certainly not divisible by p, it follows that p must be identical with one of the numbers b, c, etc.; let, for example, $p = b$. From this, however, we conclude that either $B = k+li$ or $B = k-li$, that is, either $B = A$ or $B = P$, both contrary to the hypothesis.

The other theorem, that factorization into primes can be carried out in only one way, follows very easily from this theorem, by reasoning entirely analogous to that which we used for real numbers in the *Disquisitiones Arithmeticae* (Article 16). It would therefore be superfluous to dwell on it here.

38.

We now turn to the congruence of numbers with respect to complex moduli. At the outset of this investigation, however, we should indicate how the domain of complex quantities can be made visible to intuition.

Every real quantity can be expressed by a segment of a line infinite in both directions, taken from an arbitrary starting point and measured against an arbitrary segment adopted as the unit. It can thus be represented by the other endpoint, with points on one side of the starting point representing positive quantities and those on the other negative quantities. In the same way, any complex quantity can be represented by a point in an infinite plane in which a fixed line corresponds to the real quantities: the complex quantity $x+iy$ by the point with abscissa $= x$ and ordinate, taken positively on one side of the line of abscissas and negatively on the other, $= y$. In this way we may say that any complex quantity measures the difference between the position of the point to which it corresponds and that of the starting point. The positive unit denotes an arbitrary fixed displacement in an arbitrary fixed direction; the negative unit an equally large displacement in the opposite direction; and the imaginary units equally large displacements in the two perpendicular lateral directions.

This sheds considerable light on the metaphysics of the quantities we call imaginary. If the starting point is denoted by (0), and two complex quantities m, m' correspond to points M, M', whose positions relative to (0) they

express, the difference $m-m'$ is nothing other than the position of M relative to M'. On the other hand, if the product mm' represents the position of N relative to (0), it is easy to see that this position is determined by the position of M relative to (0) in the same way as the position of M' is determined by the position of the point corresponding to the positive unit. Thus we may aptly say that the positions of the points corresponding to the complex quantities mm' $m, m', 1$ form a *proportion*. But we reserve a fuller treatment of this matter for another occasion. The difficulties in which the theory of imaginary quantities is thought to be entangled have largely arisen from unsuitable names (some have even used the discordant name of impossible quantities). Had we started from the concepts offered by two-dimensional manifolds, as seen in their greatest purity in our intuitions of space, and called positive quantities direct, negative quantities inverse and imaginary quantities lateral, simplicity would have taken the place of complications, and clarity the place of darkness.

39.

What was set out in the preceding article concerns continuous complex quantities. In arithmetic, which deals only with integers, the representation of complex numbers will be a system of equally spaced points arranged on equally spaced lines so as to divide the infinite plane into infinitely many equal squares. All numbers divisible by a given complex number $a+bi=m$ will likewise form infinitely many squares with sides $=\sqrt{(aa+bb)}$, or areas $=aa+bb$. The latter squares will be inclined to the former whenever neither of the numbers a, b is $=0$. Each number not divisible by the modulus m will correspond to a point either inside such a square or on a side shared by two squares; the latter case, however, cannot occur unless a, b have a common divisor. It is also clear that numbers congruent modulo m occupy corresponding positions in their squares. Hence, if we collect all the numbers lying inside a specified square, together with all those that may lie on two of its non-opposite sides, and finally add a number divisible by m, we readily obtain a complete system of incongruent residues modulo m: every integer must be congruent to one of them, and to only one. Nor would it be difficult to show that the number of these residues equals the norm of the modulus, namely $=aa+bb$. But it seems advisable to prove this very important theorem in another, purely arithmetical way.

40.

THEOREM. *For a given complex modulus $m=a+bi$, whose norm is $aa+bb=p$ and for which a, b are relatively prime, every complex integer will be congruent to a residue in the sequence $0, 1, 2, 3 \ldots p-1$, and to no more than one.*

Proof. I. Let α, β be integers such that $\alpha a + \beta b = 1$. Then

$$i = \alpha b - \beta a + m(\beta + \alpha i)$$

Thus, for a given complex integer $A + Bi$, we have

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha B i)$$

Denote by h the least positive residue of $A + (\alpha b - \beta a)B$ modulo p, and put

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki)$$

Then

$$A + Bi = h + m(\beta B + ak + (\alpha B - bk)i)$$

or

$$A + Bi \equiv h(\text{mod. } m). \qquad \text{Q. E. P.}$$

II. Whenever two real numbers h, h' are congruent to the same complex number modulo m, they are also congruent to each other. We therefore put $h - h' = m(c + di)$, giving

$$(h - h')(a - bi) = p(c + di)$$

and hence

$$(h - h')a = pc, \quad (h - h')b = -pd$$

and also, since $a\alpha + b\beta = 1$,

$$h - h' = p(c\alpha - d\beta), \text{ i. e. } h \equiv h'(\text{mod. } p)$$

Thus h and h', if distinct, cannot both belong to the collection of numbers $0, 1, 2, 3 \ldots . p - 1$. Q. E. S.

41.

THEOREM. *For a complex modulus $m = .a+bi$, whose norm is $aa+bb = p$ and for which a, b are not relatively prime but have greatest common divisor λ (which we suppose taken positively), every complex number is congruent to a residue $x + yi$ such that x is one of the numbers $0, 1, 2, 3 \ldots . \frac{p}{\lambda} - 1$ and y one of the numbers $0, 1, 2, 3 \ldots . \lambda - 1$, and to exactly one of all the p residues of this form.*

Proof. I. Taking integers α, β such that $\alpha a + \beta b = \lambda$, we have $\lambda i = \alpha b - \beta a + m(\beta + \alpha i)$. Now let $A + Bi$ be a given complex number, y the least positive residue of B modulo λ, and x the least positive residue of $A + (\alpha b - \beta a) . \frac{B-y}{\lambda}$ modulo $\frac{p}{\lambda}$, and put

$$A + (\alpha b - \beta a) . \frac{B-y}{\lambda} = x + \frac{p}{\lambda} . k$$

Then

$$\begin{aligned} A + Bi - (x + yi) &= \frac{p}{\lambda} . k + (B - y)i - (\alpha b - \beta a)\frac{B-y}{\lambda} \\ &= \frac{p}{\lambda} . k + \frac{B-y}{\lambda} . m(\beta + \alpha i) \\ &= \left(\frac{a}{\lambda} - \frac{b}{\lambda} . i\right) km + \frac{B-y}{\lambda}(\beta + \alpha i)m \end{aligned}$$

which is divisible by m; equivalently, $A + Bi \equiv x + yi (\text{mod. } m)$ Q. E. P.

II. Suppose that, modulo m, two numbers $x + yi, x' + y'i$ are congruent to the same complex number, and therefore also to each other modulo m. All the more, they are congruent modulo λ, so $y \equiv y' (\text{mod.} \lambda)$. If both y, y' are therefore assumed to belong to the numbers $0, 1, 2, 3 \ldots . \lambda - 1$, we must have $y = y'$. We then also have $x \equiv x' (\text{mod. } m)$: $x - x'$ is divisible by m, and consequently the integer $\frac{x-x'}{\lambda}$ is divisible by $\frac{a}{\lambda} + \frac{b}{\lambda} . i$, or

$$\frac{x - x'}{\lambda} \equiv 0 \left(\text{mod.} \frac{a}{\lambda} + \frac{b}{\lambda} . i\right)$$

But since $\frac{a}{\lambda}, \frac{b}{\lambda}$ are relatively prime, the second part of the theorem in the preceding article shows that $\frac{x-x'}{\lambda}$ is also divisible by the norm of $\frac{a}{\lambda} + \frac{b}{\lambda} . i$, that is, by the number $\frac{p}{\lambda\lambda}$, and consequently $x - x'$ by $\frac{p}{\lambda}$. Thus, if both x, x' are also assumed to belong to the collection of numbers $0, 1, 2, 3 \ldots . \frac{p}{\lambda} - 1$, we must have $x = x'$, or the residues $x + yi, x' + y'i$ are identical. Q. E. S.

It is also evident that this includes the case where the modulus is real, namely $b = 0$ and consequently $\lambda = \pm a$, as well as the case where it is purely imaginary, namely $a = 0$ and consequently $\lambda = \pm b$. In either case we have $\frac{p}{\lambda} = \lambda$.

42.

Thus, assigning complex numbers congruent to one another modulo a given modulus to the same class, and incongruent numbers to different classes, we obtain altogether p classes exhausting the whole range of integers, where p denotes the norm of the modulus. A collection of that many numbers, one taken from each class, gives a complete system of incongruent residues, such as we specified in Articles 40, 41. In that system, the choice of residues representing their classes was based on the principle of adopting in each class a residue $x + yi$ for which y has its least value and, among all those with that same least value of y, the one for which x has its least value, excluding negative values for both x and y. But other purposes will call for other principles. In particular, we should note the method of choosing residues that give the simplest quotients when divided by the modulus. If $\alpha + \beta i, \alpha' + \beta' i, \alpha'' + \beta'' i$, etc., are quotients obtained by dividing congruent numbers by the modulus, the differences among $\alpha, \alpha', \alpha''$, etc., are evidently integers, as are the differences among β, β', β'', etc. It is clear that there is always one residue for which α and β lie between the bounds 0 and 1, the former included and the latter excluded. We simply call such a residue a least residue. If preferred, the bounds $-\frac{1}{2}$ and $+\frac{1}{2}$ may be adopted instead, one included and the other excluded; we shall call a residue satisfying this restriction *absolutely least*.

Concerning · these least residues, the following problems arise.

43.

The least residue of a given complex number $A+Bi$ modulo $a+bi$, of norm $= p$, is found as follows. If $x+yi$ is the required least residue, $(x+yi)(a-bi)$ will be the least residue of the product $(A+Bi)(a-bi)$ modulo $(a+bi)(a-bi)$, that is, modulo p. Put

$$aA + bB = Fp + f, \quad aB - bA = Gp + g$$

so that f, g are the least residues of $aA + bB, aB - bA$ modulo p. Then

$$x + yi = \frac{f + gi}{a - bi}$$

or

$$x = \frac{af - bg}{p} = A - aF + bG$$
$$y = \frac{ag + bf}{p} = B - aG - bF$$

Evidently, the least residues f, g must be taken either between the bounds 0 and $p - 1$ or between $-\frac{1}{2}p$ and $+\frac{1}{2}p$, according as the complex number's simply least or absolutely least residue is required.

44.

A complete system of least residues for a given modulus can be constructed in several ways. The first method begins by determining the bounds within which the real terms must lie, and then, for each value within those bounds, assigning bounds to the imaginary parts. The general criterion for a least residue $x+yi$ modulo $a+bi$ is that both $ax+by = \xi$ and $ay-bx = \eta$ lie between the bounds 0 and $aa+bb$ when simply least residues are considered, or between $-\frac{1}{2}(aa+bb)$ and $+\frac{1}{2}(aa+bb)$ when absolutely least residues are required, one bound being excluded. Special rules would require distinguishing the cases arising from the different signs of the numbers a, b. Since developing that distinction presents no difficulty, we refrain from dwelling on it here; it will suffice to show the nature of the method by a single example.

For the modulus $5+2i$, the simply least residues $x+yi$ must be such that both $5x+2y = \xi$ and $5y-2x = \eta$ equal one of the numbers $0, 1, 2, 3 \ldots . 28$. The equation $29x = 5\xi - 2\eta$ shows that positive values of x cannot exceed $\frac{5.28}{29}$, and negative values, disregarding their sign, cannot exceed $\frac{2.28}{29}$. All admissible values of x are therefore $-1, 0, 1, 2, 3, 4$. For $x = -1$, $2y$ must equal one of the numbers $5, 6, 7 \ldots . 33$, and $5y$ one of the numbers $-2, -1, 0, 1 \ldots . 26$; hence the least value of y is $+3$ and the greatest $+5$. Treating the remaining values of x in the same way gives the following table of all the least residues:

x	y
-1	$3, 4, 5$
0	$0, 1, 2, 3, 4, 5$
$+1$	$1, 2, 3 \,.\, 4, 5 \,.\, 6$
$+2$	$1, 2, 3, 4, 5, 6$
$+3$	$2, 3, 4 \,.\, 5, 6$
$+4$	$2, 3, 4$

Similarly, for absolutely least residues, ξ and η must equal one of the numbers $-14, -13, -12 \ldots . + 14$. Hence $29x$ cannot lie outside the bounds $-7 \,.\, 14$ and $+7 \,.\, 14$, so x must equal one of the numbers $-3, -2, -1, 0, 1, 2, 3$. For $x = -3$, $2y = \xi - 5x = \xi + 15$ will equal one of the numbers $1, 2, 3 \ldots . 29$, while $5y = \eta + 2x = \eta - 6$ will equal one of the numbers $-20, -19, -18 \ldots . + 8$; this gives for y the single value $+1$. Treating the remaining values of x in the same way, we have the table of all the absolutely least residues:

x	y
-3	$+1$
-2	$-2, -1, 0, +1, +2$
-1	$-3, -2, -1, 0, +1, +2$
0	$-2, -1, 0, +1, +2$
$+1$	$-2, -1, 0, +1, +2, +3$
$+2$	$-2, -1, 0, +1, +2$
$+3$	-1

45.

In applying the second method, it will be useful to distinguish two cases.

In the first case, where a and b have no common divisor, put $a\alpha + \beta b = 1$, and let k be the least positive residue of $\beta a - \alpha b$ modulo p. The identities

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b),$$
$$b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b)$$

then show that $ak \equiv -b, bk \equiv a (\text{mod. } p)$. Thus, putting as above $ax + by = \xi$, $ay - bx = \eta$, we have $\eta \equiv k\xi$, $\xi \equiv -k\eta (\text{mod. } p)$. All the numbers $\xi + \eta i$ to which simply least residues $x + yi$ correspond are therefore obtained by taking either for ξ, successively, the values $0, 1, 2, 3 \ldots . p - 1$, and for η the least positive residues of the products $k\xi$ modulo p, or, in another order, for η those values and for ξ the least residues of the products $-k\eta$. From each $\xi + \eta i$ the corresponding $x + yi$ is then found by the formula

$$x + yi = \frac{\xi + \eta i}{a - bi} = \frac{a\xi - b\eta}{p} + \frac{a\eta + b\xi}{p} \,.\, i$$

It is also clear that η, as ξ increases by one, either increases by k or decreases by $p - k$, and consequently $x + yi$ undergoes

$$\text{either the change } \frac{a - kb}{p} + \frac{ak + b}{p} \,.\, i$$
$$\text{or this one } \frac{a - kb}{p} + b + \left(\frac{ak + b}{p} - a \right) i$$

This observation serves to make the construction easier.

Finally, if absolutely least residues $x + yi$ are required, these instructions evidently change only in that ξ must successively be given values between the bounds $-\frac{1}{2}p$ and $+\frac{1}{2}p$, while for η we must take the absolutely least residues of the products $k\xi$. Here is a table of least residues for the modulus $5 + 2i$, arranged in this way:

Simply least residues.

$\xi + \eta i$	$x + yi$	$\xi + \eta i$	$x + yi$	$\xi + \eta i$	$x + yi$
0	0	$10 + 25i$	$+5i$	$20 + 21i$	$+2 + 5i$
$1 + 17i$	$-1 + 3i$	$11 + 13i$	$+1 + 3i$	$21 + 9i$	$+3 + 3i$
$2 + 5i$	$+i$	$12 + i$	$+2 + i$	$22 + 26i$	$+2 + 6i$
$3 + 22i$	$+1 + 4i$	$13 + 18i$	$+1 + 4i$	$23 + 14i$	$+3 + 4i$
$4 + 10i$	$+2i$	$14 + 6i$	$+2 + 2i$	$24 + 2i$	$+4 + 2i$
$5 + 27i$	$-1 + 5i$	$15 + 23i$	$+1 + 5i$	$25 + 19i$	$+3 + 5i$
$6 + 15i$	$+3i$	$16 + 11i$	$+2 + 3i$	$26 + 7i$	$+4 + 3i$
$7 + 3i$	$+1 + i$	$17 + 28i$	$+1 + 6i$	$27 + 24i$	$+3 + 6i$
$8 + 20i$	$+4i$	$18 + 16i$	$+2 + 4i$	$28 + 12i$	$+4 + 4i$
$9 + 8i$	$+1 + 2i$	$19 + 4i$	$+3 + 2i$		

Absolutely least residues.

$\xi + \eta i$	$x + yi$	$\xi + \eta i$	$x + yi$	$\xi + \eta i$	$x + yi$
$-14 - 6i$	$-2 - 2i$	$-4 - 10i$	$-2i$	$+5 - 2i$	$+1$
$-13 + 11i$	$-3 + i$	$-3 + 7i$	$-1 + i$	$+6 - 14i$	$+2 - 2i$
$-12 - i$	$-2 - i$	$-2 - 5i$	$-i$	$+7 + 3i$	$+1 + i$
$-11 - 13i$	$-1 - 3i$	$-1 + 12i$	$-1 + 2i$	$+8 - 9i$	$+2 - i$
$-10 + 4i$	-2	0	0	$+9 + 8i$	$+1 + 2i$
$-9 - 8i$	$-1 - 2i$	$+1 - 12i$	$+1 - 2i$	$+10 - 4i$	$+2$
$-8 + 9i$	$-2 + i$	$+2 + 5i$	$+i$	$+11 + 13i$	$+1 + 3i$
$-7 - 3i$	$-1 - i$	$+3 - 7i$	$+1 - i$	$+12 + i$	$+2 + i$
$-6 + 14i$	$-2 + 2i$	$+4 + 10i$	$+2i$	$+13 - 11i$	$+3 - i$
$-5 + 2i$	-1			$+14 + 6i$	$+2 + 2i$

The second case, where a, b are not relatively prime, can easily be reduced to the preceding one. Let λ be the greatest common divisor of a, b, and let $a = \lambda a'$, $b = \lambda b'$. Let F denote any least residue modulo λ, with the modulus regarded as a complex number: that is, let it represent any number $x + yi$ such that x, y lie either between the bounds 0 and λ or between $-\frac{1}{2}\lambda$ and $+\frac{1}{2}\lambda$, according as simply least or absolutely least residues are considered. Further, let F' denote any least residue modulo $a' + b'i$. Then $(a' + b'i)F + F'$ will represent any least residue modulo $a + bi$, and a complete system of these residues results when all values of F are combined with all values of F'.

46.

Two complex numbers are called relatively prime if they have no common divisors other than the units. Whenever such common divisors do exist, those whose norm is greatest are called greatest common divisors.

If the factorization of two given numbers into prime factors is available, the greatest common divisor is determined in exactly the same way as for real numbers (*Disquiss. Ar.* Article 18). This also shows that every common divisor of two given numbers must divide their greatest common divisor found in this way. Since it is already evident that its three associates are also common divisors, there will always be four numbers, and no more, that are to be called greatest common divisors; their norm will be a multiple of the norm of any other common divisor.

If the factorization of two given numbers into simple factors is not available, the greatest common divisor is found by an algorithm similar to that for real numbers. Let m, m' be the two given numbers, and form by repeated division the sequence m'', m''', etc., so that m'' is the absolutely least residue of m modulo m', then m''' the absolutely least residue of m' modulo m'', and so on. Denoting the norms of m, m', m'', m''', etc., respectively by p, p', p'', p''', etc., $\frac{p''}{p'}$ will be the norm of the quotient $\frac{m''}{m'}$ and thus, by the definition of an absolutely least residue, certainly no greater than $\frac{1}{2}$; the same holds for $\frac{p'''}{p''}$, etc. The positive real integers p', p'', p''', etc., will therefore form a steadily decreasing sequence, so that a term 0 must eventually be reached. Equivalently, in the sequence m, m', m'', m''', etc., we shall eventually reach a term that divides the preceding term without a remainder. Let this be $m^{(n+1)}$, and put

$$\begin{aligned} m &= km' + m'' \\ m' &= k'm'' + m''' \\ m'' &= k''m''' + m'''' \end{aligned}$$

and so on, as far as

$$m^{(n)} = k^{(n)} m^{(n+1)}$$

Going through these equations in reverse order shows that $m^{(n+1)}$ divides each preceding term $m^{(n)} \ldots . m'', m', m$; going through the same equations in forward order makes it clear that every common divisor of m, m' also divides each subsequent term. The first conclusion shows that $m^{(n+1)}$ is a common divisor of m, m'; the second, that this divisor is greatest.

Whenever the last residue $m^{(n+1)}$ equals one of the four units $1, -1, i, -i$, this will show that m and m' are relatively prime.

47.

If the equations of the preceding article, omitting the last, are combined so as to eliminate $m'', m''', m'''' \dots . m^{(n)}$, an equation of the following form results:

$$m^{(n+1)} = hm + h'm'$$

where h, h' are integers; more specifically, if we use the notation introduced in *Disquiss. Ar.* Article 27,

$$\begin{aligned} h &= \pm[k', k'', k''' \dots . k^{(n-1)}] \\ &= \pm[k^{(n-1)}, k^{(n-2)} \dots . k'', k'] \\ h' &= \mp[k, k', k'', k''' \dots . k^{(n-1)}] \\ &= \mp[k^{(n-1)}, k^{(n-2)} \dots . k'', k', k] \end{aligned}$$

the upper or lower signs applying according as n is even or odd. We state this theorem as follows:

A greatest common divisor of two complex numbers m, m' can be put in the form $hm + h'm'$, with h, h' integers.

This evidently holds for the greatest common divisor to which the algorithm of the preceding article led, and also for its three associates. For these, the coefficients h, h' must be replaced either by $hi, h'i$, by $-h, -h'$ or by $-hi, -h'i$.

Thus, whenever the numbers m, m' are relatively prime, the following equation can be satisfied:

$$1 = hm + h'm'$$

For example, let the given numbers be $31 + 6i = m$, $11 - 20i = m'$. Here we find

$$\begin{aligned} k &= i, & m'' &= +11 - 5i \\ k' &= +1 - i, & m''' &= +5 - 4i \\ k'' &= +2, & m'''' &= +1 + 3i \\ k''' &= -1 - 2i, & m''''' &= +i \\ k'''' &= +3 - i \end{aligned}$$

and hence

$$\begin{aligned} [k', k'', k'''] &= -6 - 5i \\ [k, k', k'', k'''] &= +4 - 10i \end{aligned}$$

and therefore

$$m''''' = i = (6 + 5i)m + (4 - 10i)m'$$

as well as

$$1 = (5 - 6i)m + (-10 - 4i)m'$$

which is confirmed by carrying out the calculation.

48.

The foregoing has prepared everything required for the theory of congruences of the first degree in the arithmetic of complex numbers. But since this theory does not differ essentially from the one that applies to the arithmetic of real numbers and has been set out at length in the *Disquisitiones Arithmeticae*, it will suffice to set down the main points here.

I. The congruence $mt \equiv 1 \pmod{m'}$ is equivalent to the indeterminate equation $mt + m'u = 1$. If this equation is satisfied by the values $t = h, u = h'$, the general solution of the congruence is expressed by $t \equiv h \pmod{m'}$. The condition for solvability is that the modulus m' and the coefficient m have no common divisor.

II. The solution of the congruence $ax + b \equiv c \pmod{M}$, in the case where a, M are relatively prime, depends on the solution of

$$at \equiv 1 \pmod{M}$$

If $t = h$ satisfies this congruence, the general solution of the former is contained in the formula

$$x \equiv (c - b)h \pmod{M}$$

III, The congruence $ax + b \equiv c(\text{mod. } M)$, in the case where a, M have a common divisor λ, is equivalent to

$$\frac{a}{\lambda} \,.\, x \equiv \frac{c-b}{\lambda} \quad \left(\text{mod.} \frac{M}{\lambda}\right)$$

Thus, when λ is taken to be the greatest common divisor of a, M, the solution of the given congruence is reduced to the preceding case. It is clear that the necessary and sufficient condition for solvability is that λ also divide the difference $c - b$.

49.

So far we have touched only on elementary matters, which nevertheless could not be omitted for the sake of the connection. In deeper investigations, the arithmetic of complex numbers resembles the arithmetic of real numbers in that more elegant and simpler theorems result when we admit only moduli that are prime numbers. Indeed, extending them to composite moduli usually involves more length than difficulty, and more work than ingenuity. The following discussion will therefore deal chiefly with prime moduli.

50.

Let X denote a function of the indeterminate x of the following form:

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

where n is a positive real integer, A, B, C, etc., real or imaginary integers, and m a complex integer. Here too we shall call any integer a *root* of the congruence $X \equiv 0 \pmod{m}$ if, when substituted for x, it gives X a value divisible by the modulus m. We shall not regard solutions given by roots congruent modulo the modulus as different.

Whenever the modulus is a prime number, here too such a congruence of degree n cannot have more than n different solutions. Let α denote any fixed integer (complex). X can be put by division by $x - \alpha$, with the indeterminate left free, in the form $X = (x - \alpha)X' + h$, where h is a fixed integer and X' a function of degree $n - 1$ with integer coefficients. Whenever α is a root of the congruence $X \equiv 0 \pmod{m}$, h is evidently divisible by m; equivalently, with the indeterminate left free, we have $X \equiv (x - \alpha)X' \pmod{m}$.

Similarly, if β denotes a fixed integer and X' is put in the form $(x - \beta)X'' + h'$, X'' will be a function of degree $n - 2$ with integer coefficients. If β is supposed to be a root of the congruence $X \equiv 0$, it must also satisfy $(\beta - \alpha)X' \equiv 0$, and also $X' \equiv 0$ if the roots α, β are incongruent. We conclude that h' must also be divisible by m; equivalently, with the indeterminate left free, $X \equiv (x - \alpha)(x - \beta)X'' \pmod{m}$.

In the same way, on adding a third root γ, incongruent to the preceding ones, we shall have, with the indeterminate left free, $X \equiv (x-\alpha)(x-\beta)(x-\gamma)X'''$, where X''' is a function of degree $n-3$ with integer coefficients. We may continue in the same way. It is also clear that the coefficient of the highest term in each function is $= A$, which we may suppose not divisible by m, since otherwise the congruence $X \equiv 0$ would essentially have to be assigned a lower degree. Thus, whenever there are n incongruent roots, say $\alpha, \beta, \gamma \ldots . \nu$, we have, with the indeterminate left free,

$$X \equiv A(x-\alpha)(x-\beta)(x-\gamma)\ldots.(x-\nu) \pmod{m}$$

Consequently, substituting a new value incongruent to each of $\alpha, \beta, \gamma \ldots . \nu$ would certainly give X a value not divisible by m, from which the theorem follows at once.

This proof essentially agrees with the one we gave in *Disq. Ar.* Article 43, every step of which applies to complex numbers just as it does to real numbers.

51.

Most of what was given in the third section of the *Disquisitiones Arithmeticae* concerning residues of powers also holds in the arithmetic of complex numbers, with slight changes; indeed, the proofs of the theorems could generally be retained. So that nothing is missing, however, we shall present the principal theorems supported by concise proofs. Throughout, the modulus is to be understood to be a prime number.

THEOREM. *If k denotes an integer not divisible by the modulus m, of norm $= p$, then $k^{p-1} \equiv 1 \pmod{m}$.*

Proof. Let a, b, c, etc., form a complete system of incongruent residues modulo m, but with the residue divisible by m omitted, so that the number of these numbers, whose collection we denote by C, is $= p-1$. Further, let C' be the collection of products ka, kb, kc, etc. By hypothesis, none of these products is divisible by m, so each has a congruent residue in the collection C: we may thus have $ak \equiv a', bk \equiv b', ck \equiv c'$, etc., (mod. m), where the numbers a', b', c', etc., themselves occur in the collection C. Denote the collection of a', b', c', etc., by C''. Let P, P', P'' be the products of the individual numbers in the collections C, C', C'', respectively; that is,

$$\begin{aligned} P &= abc\ldots. \\ P' &= k^{p-1}abc\ldots. = k^{p-1}P \\ P'' &= a'b'c'\ldots. \end{aligned}$$

Since the numbers in C'' are congruent, in succession, to the numbers in C', we have $P'' \equiv P'$, or $P'' \equiv k^{p-1}P$. But any two numbers in C'' are readily seen to be incongruent, and therefore all are distinct. The numbers in C'' must consequently coincide exactly with those in C, with only their order changed, giving $P'' = P$. Thus $(k^{p-1} - 1)P$ is divisible by m. Since m is a prime number dividing none of the individual factors of P, $k^{p-1} - 1$ must necessarily be divisible by m. Q. E. D.

52.

THEOREM. *If k, as in the preceding article, denotes an integer not divisible by the modulus m, and t the least exponent (apart from 0) for which $k^t \equiv 1 \pmod{m}$, then t divides every other exponent u for which $k^u \equiv 1 \pmod{m}$.*

Proof. If t did not divide u, let gt be the multiple of u next greater than u, so that $gt - u$ is a positive integer less than t. From $k^t \equiv 1, k^u \equiv 1$ it follows that $0 \equiv k^{gt} - k^u \equiv k^u(k^{gt-u} - 1)$, and hence $k^{gt-u} \equiv 1$: there is a power of k with an exponent less than t that is congruent to unity, contrary to the hypothesis.

It follows as a corollary that t certainly divides $p - 1$.

Here too we shall call numbers k for which $t = p - 1$ *primitive roots* for. the modulus m. We shall now show that such numbers really exist.

53.

Factor the number $p - 1$ into its prime factors, so that

$$p - 1 = a^\alpha b^\beta c^\gamma \ldots .$$

where a, b, c, etc., denote distinct positive real prime numbers. Let A, B, C, etc., be integers (complex) not divisible by m, and respectively *not* satisfying the congruences

$$x^{\frac{p-1}{a}} \equiv 1, \quad x^{\frac{p-1}{b}} \equiv 1, \quad x^{\frac{p-1}{c}} \equiv 1 \quad \text{etc.}$$

modulo m. The existence of such numbers is clear from the theorem of Article 50. Finally, let h be congruent modulo m to the product

$$A^{\frac{p-1}{a^\alpha}} B^{\frac{p-1}{b^\beta}} C^{\frac{p-1}{c^\gamma}} \ldots .$$

Then I say that h will be a primitive root.

Proof. Denoting by t the exponent of the lowest power h^t congruent to unity, if h were not a primitive root, t would be a proper divisor of $p - 1$; that is, $\frac{p-1}{t}$ would be an integer greater than unity. This integer evidently has its real prime factors among a, b, c, etc. Let us therefore suppose, as we may, that $\frac{p-1}{t}$ is divisible by a, and put $p - 1 = atu$. Since $h^t \equiv 1$, we then also have $h^{tu} \equiv 1$, or

$$A^{\frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} C^{\frac{p-1}{c^\gamma} \cdot \frac{p-1}{a}} \ldots . \equiv 1$$

But $\frac{p-1}{ab^\beta}$ is evidently an integer, so

$$B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} = (B^{p-1})^{\frac{p-1}{ab^\beta}} \equiv 1$$

and similarly $C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \equiv 1$, and so on; consequently we must have $A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$ Now determine a positive integer λ such that

$$\lambda b^\beta c^\gamma \ldots . \equiv 1 \pmod{a}$$

This can be done, since the prime number a does not divide $b^\beta c^\gamma \ldots .$; put $\lambda b^\beta c^\gamma \ldots . = 1 + a\mu$. Evidently $A^{\lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$; or, since $\lambda \,.\, \frac{p-1}{a^\alpha} \,.\, \frac{p-1}{a} = (1+a\mu)\frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}$, we have $A^{(p-1)\mu} \,.\, A^{\frac{p-1}{a}} \equiv 1$. Hence, since $A^{(p-1)\mu} \equiv 1$ holds of itself, we also have $A^{\frac{p-1}{a}} \equiv 1$, contrary to the hypothesis. The supposition that t is a proper divisor of $p-1$ therefore cannot stand, and h must necessarily be a primitive root.

54.

Let h be a primitive root for the modulus m, of norm $= p$. The terms of the progression

$$1, h, hh, h^3 \ldots . h^{p-2}$$

will be incongruent to one another. It follows easily that every integer not divisible by the modulus must be congruent to one of them: this sequence gives a complete system of incongruent residues with zero excluded. The exponent of the power to which a given number is congruent may be called its *index*, while h is regarded as the *base*. Here are some examples, in which we have placed the absolutely least residue beside each index.

First example.

$$m = 5 + 4i, \quad p = 41, \quad h = 1 + 2i$$

Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue
0	$+1$	8	-4	16	$-2+2i$	24	$+2i$	32	$+1+i$
1	$+1+2i$	9	$-3+i$	17	$-1+2i$	25	$-3i$	33	$+1+3i$
2	$+1-i$	10	$-i$	18	$+4i$	26	$+2+2i$	34	$+2$
3	$+3+i$	11	$+2-i$	19	$+1+3i$	27	$+2+i$	35	-3
4	$-2i$	12	$-1-i$	20	-1	28	$+4$	36	$+2-2i$
5	$+3i$	13	$+1-3i$	21	$-1-2i$	29	$+3-i$	37	$+1-2i$
6	$-2-2i$	14	-2	22	$-1+i$	30	$+i$	38	$-4i$
7	$-2-i$	15	$+3$	23	$-3-i$	31	$-2+i$	39	$-1-3i$

Second example.

$$m = 7, \quad p = 49, \quad h = 1 + 2i$$

Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue
0	$+1$	10	$-1-i$	20	$+2i$	30	$+2-2i$	40	$+3$
1	$+1+2i$	11	$+1-3i$	21	$+3+2i$	31	$-1+2i$	41	$+3-i$
2	$-3-3i$	12	$-i$	22	$-1+i$	32	$+2$	42	$-2-2i$
3	$+3-2i$	13	$+2-i$	23	$-3-i$	33	$+2-3i$	43	$+2+i$
4	$-3i$	14	$-3+3i$	24	-1	34	$+1+i$	44	$-2i$
5	$-1-3i$	15	$-2-3i$	25	$-1-2i$	35	$-1+3i$	45	$-3-2i$
6	$-2+2i$	16	-3	26	$+3+3i$	36	$+i$	46	$+1-i$
7	$+1-2i$	17	$-3+i$	27	$-3+2i$	37	$-2+i$	47	$+3+i$
8	-2	18	$+2+2i$	28	$+3i$	38	$+3-3i$		
9	$-2+3i$	19	$-2-i$	29	$+1+3i$	39	$+2+3i$		

55.

We add some observations about primitive roots and the calculation of indices, omitting their proofs because they are easy.

I. In a given system, indices congruent modulo $p-1$ correspond to residues congruent modulo m, and conversely.

II. Residues corresponding to indices relatively prime to $p-1$ are themselves primitive roots, and conversely.

III. Suppose that, with a primitive root h taken as the base, the index of another primitive root h' is t, and, conversely, t' is the index of h when h' is taken as the base. Then $tt' \equiv 1 \pmod{p-1}$. Under the same assumptions, if the indices of some other number in these two systems are respectively u, u', then $tu' \equiv u, t'u \equiv u' \pmod{p-1}$.

IV. Excluding the numbers $1, 1+i$ and their three associates each, as being too trivial, from the moduli we consider leaves the prime numbers that we placed third and fourth in Article 34. The norms of the latter are real prime numbers of the form $4n+1$; those of the former, however, are squares of odd real prime numbers. Thus, in either case, $p-1$ is divisible by 4.

V. Denote the index of -1 by u. Then $2u \equiv 0 \pmod{p-1}$, so either $u \equiv 0$ or $u \equiv \frac{1}{2}(p-1)$. But since the index 0 corresponds to the residue $+1$, the index of -1 must be $\frac{1}{2}(p-1)$.

VI. Similarly, denoting by u the index of i, we have $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$, and therefore either $u \equiv \frac{1}{4}(p-1)$ or $u \equiv \frac{3}{4}(p-1)$. Here, however, the ambiguity depends on the choice of primitive root. Specifically, if, with the primitive root h taken as the base, the index of i is $\frac{1}{4}(p-1)$, the index becomes $\frac{3}{4}(p-1)$ when h^μ is taken as the base, where μ denotes a positive integer of the form $4n+3$ relatively prime to $p-1$, for example the number $p-2$ itself; and conversely. Thus one half of the primitive roots gives i the index $\frac{1}{4}(p-1)$, and the other half the index $\frac{3}{4}(p-1)$. Evidently, for the former bases $-i$ has the index $\frac{3}{4}(p-1)$, and for the latter the index $\frac{1}{4}(p-1)$.

VII. Whenever the modulus is a positive real prime number of the form $4n+3$, say $= q$, so that $p = qq$, the indices of all real numbers are divisible by $q+1$. For, if t denotes the index of the real number k, then, because $k^{q-1} \equiv \pmod{q}$, we have $(q-1)t \equiv 0 \pmod{qq-1}$, and consequently $\frac{t}{q+1}$ is an integer. Similarly, the indices of purely imaginary numbers such as ki are divisible by $\frac{1}{2}(q+1)$. Thus primitive roots for such moduli must evidently be sought only among mixed numbers.

VIII. For a modulus m that is a mixed complex prime number, however, whose norm p is consequently a real prime number of the form $4n+1$, any primitive roots may also be chosen among real numbers, among which a complete system of incongruent residues can indeed be exhibited (Article 40). Every real number that is a primitive root for the complex modulus m is evidently also, in the arithmetic of real numbers, a primitive root for the modulus p, and conversely.

56.

Although the theory of quadratic residues and nonresidues in the arithmetic of complex numbers is contained within the theory of biquadratic residues itself, we shall present its principal theorems separately here before turning to the latter. For brevity, however, we shall discuss only the principal case, where the modulus is an odd complex prime number.

Let m be such a modulus, and p its norm. Evidently, any integer not divisible by m, a condition always to be understood here, can or cannot be congruent to a square modulo m, according as its index, with some primitive root taken as the base, is even or odd. In the former case that integer is called a quadratic residue of m, and in the latter a nonresidue. It follows that, among $p-1$ numbers forming a complete system of incongruent residues not divisible by m, one half belongs to the quadratic residues and the other half to the quadratic nonresidues. Any other number outside this system must be assigned the same character in this respect as the number in the system congruent to it.

It also follows that the product of two quadratic residues, as well as the product of two nonresidues, is a quadratic residue, whereas the product of a quadratic residue and a nonresidue is a nonresidue. In general, a product of any number of factors is a quadratic residue or a nonresidue according as the number of nonresidues among its factors is even or odd.

The following general criterion for distinguishing quadratic residues from nonresidues presents itself at once:

A number k not divisible by the modulus is a quadratic residue or a nonresidue of it according as $k^{\frac{1}{2}(p-1)} \equiv 1$ or $k^{\frac{1}{2}(p-1)} \equiv -1 \pmod{m}$.

This theorem follows at once from the fact that, with any primitive root taken as the base, the index of the power $k^{\frac{1}{2}(p-1)}$ becomes either $\equiv 0$ or $\equiv \frac{1}{2}(p-1)$, according as the index of k is even or odd.

57.

For a given modulus, it is easy to divide a complete system of incongruent residues into two classes, quadratic residues and nonresidues. This also assigns all the remaining numbers to their respective classes. But a much deeper investigation is needed to find criteria distinguishing the moduli for which a given number is a quadratic residue from those for which it is a nonresidue.

As for the real units $+1$ and -1, these are actual squares in the arithmetic of complex numbers, and therefore quadratic residues for *every* modulus. It follows just as easily from the criterion in the preceding article that i, and likewise $-i$, is a quadratic residue of every modulus whose norm p has the form $8n+1$, but a nonresidue of every modulus whose norm has the form $8n+5$. Since it evidently makes no difference whether m or one of its associates

$im, -m, -im$ is taken as the modulus, we may suppose that the modulus is the primary one among its associates (Article 36, II). Thus, putting the modulus $= a + bi$, we may suppose a odd and b even. We then always have $aa \equiv 1 \pmod 8$, while bb is either $\equiv 0$ or $\equiv 4 \pmod 8$, according as b is divisible by four or twice an odd number. Thus $+i$ and $-i$ are evidently quadratic residues of the modulus in the former case and nonresidues in the latter.

58.

Since the character of a composite number, whether it is a quadratic residue or a nonresidue, depends on the characters of its factors, it evidently suffices to restrict the development of criteria distinguishing the moduli for which a given number k is a quadratic residue from those for which it is a nonresidue to values of k that are prime numbers and, moreover, primary among their associates. In this investigation, *examining examples* immediately supplies very elegant theorems.

Let us begin with $1 + i$, which is found to be a quadratic residue of the moduli

$$-1 + 2i,\ +3 - 2i,\ -5 - 2i,\ -1 - 6i,\ +5 + 4i,\ +5 - 4i,$$
$$-7,\ +7 + 2i,\ -5 + 6i, \quad \text{etc.}$$

but a quadratic nonresidue of the following:

$$-1 - 2i,\ -3,\ +3 + 2i,\ +1 + 4i,\ +1 - 4i,\ -5 + 2i,$$
$$-1 + 6i,\ +7 - 2i,\ -5 - 6i,\ -3 + 8i,\ -3 - 8i,$$
$$+5 + 8i,\ +5 - 8i,\ +9 + 4i,\ +9 - 4i \quad \text{etc.}$$

Examining this list carefully, in which we have always entered the primary one of each four associated moduli, we readily notice that all the moduli $a+bi$ in the first class satisfy $a+b \equiv +1 \pmod 8$, while those in the second satisfy $a + b \equiv -3 \pmod 8$. If, in place of the primary modulus m, we take its associate $-m$, this criterion must evidently change so that $a + b \equiv -1$ for moduli in the first class, and $\equiv +3 \pmod 8$ for those in the second. Thus, provided our examination of examples has not misled us, in general, if $a + bi$ denotes a prime number in which a is odd. b even, $1+i$ is a quadratic residue or a quadratic nonresidue of it according as $a + b \equiv \pm 1$ or $\equiv \pm 3 \pmod 8$.

The same rule holds for $-1-i$ as for $1+i$. On the other hand, considering $1 - i$ as the product of $-i$ and $1 + i$, $1 - i$ evidently has the same character as must be assigned to $1 + i$ whenever b is divisible by four, but the opposite character whenever b is twice an odd number. It follows easily that $1 - i$ is a quadratic residue of the prime number $a + bi$ whenever $a - b \equiv \pm 1$, but a nonresidue whenever $a - b \equiv \pm 3 \pmod 8$, always supposing a odd and b even.

This second proposition can also be deduced from the first with the help of a more general theorem, which we state as follows:

In the theory of quadratic residues, the character of $\alpha+\beta i$ with respect to the modulus $a+bi$ is the same as that of $\alpha-\beta i$ with respect to the modulus $a-bi$.

The proof of this theorem follows from the fact that both moduli have the same norm p, and that whenever $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ is divisible by $a+bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ is also divisible by $a-bi$, while whenever $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ is divisible by $a+bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ must also be divisible by $a-bi$.

59.

Let us proceed to odd prime numbers.

We find that $-1+2i$ is a quadratic residue of the moduli $+3+2i$, $+1-4i$, $-5+2i$, $-5-2i$, $-1-6i$, $+7-2i$, $-3+8i$, $+5+8i$, $+5-8i$, $+9+4i$, etc.,

but a nonresidue of the moduli $-1-2i$, -3, $+3-2i$, $+1+4i$, $-1+6i$, $+5+4i$, $+5-4i$, -7, $+7+2i$, $-5+6i$, $-5-6i$, $-3-8i$, $+9-4i$, etc.

Reducing the moduli of the first class to their absolutely least residues modulo $-1+2i$, we find only $+1$ and -1, namely $+3+2i\equiv-1$, $+1-4i\equiv-1$, $-5+2i\equiv+1$, $-5-2i\equiv-1$, etc.

On the other hand, all moduli of the second class are found to be congruent modulo $-1+2i$ either to $+i$ or to $-i$.

But $+1,-1$ are themselves quadratic residues of the modulus $-1+2i$, while $+i$ and $-i$ are its nonresidues. Thus, as far as the examination of examples can be trusted, the following theorem emerges: $-1+2i$ is a quadratic residue or a quadratic nonresidue of the prime number $a+bi$ according as the latter is a quadratic residue or a quadratic nonresidue of $-1+2i$, provided that $a+bi$ is the primary one of its four associates, or rather, that a is odd and b even.

Analogous theorems concerning $+1-2i$, $-1-2i$, $+1+2i$ follow directly from this theorem.

60.

Examining examples similarly for -3 or $+3$, we find that each is a quadratic residue of the moduli $+3+2i$, $+3-2i$, $-1+6i$, $-1-6i$, -7, $-5+6i$, $-5-6i$, $-3+8i$, $-3-8i$, $+9+4i$, $+9-4i$, etc.,

but a nonresidue of $-1+2i$, $-1-2i$, $+1+4i$, $+1-4i$, $-5+2i$, $-5-2i$, $+5+4i$, $+5-4i$, $+7+2i$, $+7-2i$, $+5+8i$, $+5-8i$, etc.

The former are congruent modulo 3 to one of the four numbers $+1,-1,+i,-i$, the latter to one of $+1+i,+1-i,-1+i,-1-i$. The former are precisely the quadratic residues of 3, and the latter its nonresidues.

Thus this examination of examples shows that the prime number $a+bi$, supposing a odd and b even, has the same relation to -3, and also to $+3$,

as the latter has to it, in respect of whether one is a quadratic residue or a nonresidue of the other.

Extending a similar examination to other prime numbers, we find this most elegant law of reciprocity confirmed everywhere, and are led to the following fundamental theorem about quadratic residues in the arithmetic of complex numbers:

If $a + bi, A + Bi$ denote prime numbers such that a, A are odd and b, B even, either each is a quadratic residue of the other, or each is a nonresidue of the other.

Yet despite the theorem's great simplicity, its proof is beset by great difficulties. We shall not dwell on these here, however, since the theorem itself is only a special case of a more general theorem that, as it were, exhausts the substance of the theory of biquadratic residues. Let us now turn to that theory.

61.

We extend to the arithmetic of complex numbers what was said in Article 2 of the preceding paper about the notion of a biquadratic residue and nonresidue. Here, as there, we restrict the investigation to moduli that are prime numbers. It will also usually be tacitly understood that the modulus is chosen to be primary among its associates, that is, $\equiv 1$ modulo $2+2i$, and that the numbers whose character, as biquadratic residues or nonresidues, is under consideration are not divisible by the modulus.

For a given modulus, therefore, the numbers not divisible by it could be divided into three classes: the first containing biquadratic residues; the second, those biquadratic nonresidues that are quadratic residues; and the third, quadratic nonresidues.

But here too it is better to establish two classes in place of the third, so that there are four in all.

With any primitive root taken as the base, biquadratic residues will have indices divisible by 4, or of the form $4n$; those nonresidues that are quadratic residues will have indices of the form $4n+2$; finally, the indices of quadratic nonresidues will be partly of the form $4n+1$, partly of the form $4n+3$. Four classes do arise in this way, but the distinction between the latter two would not be absolute: it would depend on the choice of the primitive root taken as the base. For it is easy to see that one half of the primitive roots gives a given quadratic nonresidue an index of the form $4n+1$, and the other half an index of the form $4n+3$. To remove this ambiguity, we shall always suppose that a primitive root is chosen for which the index $\frac{1}{4}(p-1)$ belongs to the number $+i$ (compare Article 55, VI). This gives a classification that we can state more concisely, independently of primitive roots, as follows.

Let the *first* class contain those numbers k for which $k^{\frac{1}{4}(p-1)} \equiv 1$; these numbers are biquadratic residues of the modulus.

Let the *second* class contain those for which $k^{\frac{1}{4}(p-1)} \equiv i$.

The *third*, those for which $k^{\frac{1}{4}(p-1)} \equiv -1$.

Finally, the *fourth*, those for which $k^{\frac{1}{4}(p-1)} \equiv -i$.

The third class will contain those biquadratic nonresidues that are quadratic residues; quadratic nonresidues will be distributed between the second and fourth classes.

We shall assign to the numbers in these classes the *biquadratic characters* $0, 1, 2, 3$, respectively. If we define the character λ of a number k modulo m as the exponent of that power of i to which $k^{\frac{1}{4}(p-1)}$ is congruent, then evidently characters congruent modulo 4 must be regarded as equivalent. For the time being, this notion is restricted to moduli that are prime numbers: in a continuation of these investigations we shall show how it can also be applied to composite moduli.

62.

To make an extensive examination of examples concerning the characters of numbers easier, we append a compact table here. With its help, the character of any given number with respect to a modulus whose norm does not exceed 157 is obtained with little work, provided that the following observations are taken into account.

Since the character of a composite number is equal to, or congruent modulo 4 to, the sum of the characters of its individual factors, it suffices if we can assign the characters of prime numbers for a given modulus. Further, since the characters of the units $-1, i, -i$ are evidently congruent to the numbers $\frac{1}{2}(p-1), \frac{1}{4}(p-1), \frac{3}{4}(p-1)$ modulo 4, it will also suffice to give the characters of numbers that are primary among their associates. Finally, since moduli congruent modulo m have the same character, it suffices to enter in the table the characters of numbers contained in a system of absolutely least residues. In addition, reasoning similar to that in Article 58 shows that, if for the modulus $a+bi$ the character of $A+Bi$ is λ, while for the modulus $a-bi$ λ' is the character of $A-Bi$, then we always have $\lambda \equiv -\lambda' \pmod 4$, or, equivalently, $\lambda+\lambda'$ is divisible by 4. It therefore suffices to enter in the table moduli in which b is either 0 or positive.

Thus, for example, if the character of $11-6i$ with respect to the modulus $-5-6i$ is sought, we substitute the numbers $11+6i, -5+6i$ for them. We then determine (Article 43) the absolutely least residue of $11+6i$ modulo $-5+6i$, which is $-1-4i = -1\times(1+4i)$. Since for the modulus $-5+6i$ the character of -1 is 30, while the character of $1+4i$, from the table, is 2, we obtain 32, or 0, as the character of $11+6i$ for the modulus $-5+6i$; and, by the last observation, this is also the character of $11-6i$ for the modulus $-5-6i$. Likewise, if the character of $-5+6i$ with respect to the modulus $11+6i$ is sought, its absolutely least residue $1-5i$ is factored into $-i\ 1+i,\ 3-2i$, to which the characters $117, 0, 1$ correspond. Hence the character sought will be 118, or 2; the same character must also be assigned to $-5-6i$ with respect to the modulus $11-6i$.

Modulus.	Character.	Numbers.
-3	3	$1+i$
$+3+2i$	3	$1+i$
$+1+4i$	1	$-1+2i$
	3	$1+i$
$-5+2i$	0	$-1-2i$
	1	$1+i$
	2	$-1+2i$
$-1+6i$	0	-3
	1	$1+i,\ -1+2i$

Modulus.	Character.	Numbers.
$-1+6i$	2	$-1-2i$
$+5+4i$	0	$1+i$
	1	-3
	3	$-1+2i,\ -1-2i$
-7	0	-3
	1	$-1+2i,\ 3-2i$
	2	$1+i$
	3	$-1-2i,\ 3+2i$
$+7+2i$	0	$1+i,\ 3+2i,\ 3-2i,\ 1-4i$
	1	-3
	2	$-1-2i,\ 1+4i$
	3	$-1+2i$
$-5+6i$	0	$1+i,\ -3,\ 3+2i,\ 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\ -1-2i$
$-3+8i$	0	$-1+2i,\ 3-2i,\ 1-4i$
	1	$1+i,\ 3+2i$
	2	-3
	3	$-1-2i,\ 1+4i,\ -5+2i$
$+5+8i$	0	$-1-2i$
	1	$-5-2i,\ -1+6i$
	2	$-1+2i,\ 3-2i$
	3	$1+i,\ -3,\ 3+2i,\ 1+4i,\ 1-4i$
$+9+4i$	0	$-1+2i,\ 3+2i$
	1	$1+i,\ -1-2i,\ 3-2i$
	2	$-3,\ 1+4i$
	3	$1-4i,\ -5+2i$
$-1+10i$	0	$1+i,\ -1+2i,\ -1-2i,\ 3+2i$
	1	-3
	2	$3-2i,\ -5+2i,\ 5-4i$
	3	$1+4i,\ 1-4i$

Modulus.	Character.	Numbers.
$+3+10i$	1	$1+i,\ -1-2i,\ 1-4i$
	2	$-3,\ 3+2i,\ 1+4i,\ -5-2i$
	3	$-1+2i,\ 3-2i$
$-7+8i$	0	$1+i,\ -7$
	1	$3+2i,\ 3-2i,\ 1-4i,\ -5-2i$
	2	$-1-2i,\ 1+4i,\ -5+2i,\ -1-6i$
	3	$-1+2i,\ -3,\ -1+6i$
-11	0	-3
	1	$1+i,\ 3-2i,\ 1+4i,\ -5+2i,\ 5+4i$
	2	$-1+2i,\ -1-2i$
	3	$3+2i,\ 1-4i,\ -5-2i,\ 5-4i$
$-11+4i$	0	$1+i,\ -1+2i,\ 3+2i,\ 5+4i$
	1	$-1-2i,\ -1+6i$
	2	$-5+2i$
	3	$-3,\ 3-2i,\ 1+4i,\ 1-4i,\ -5-2i$
$+7+10i$	0	$1+4i,\ 1-4i,\ -1+6i,\ -1-6i$
	1	$-1+2i,\ 3+2i,\ -5+2i$
	2	$1+i,\ 3-2i$
	3	$-1-2i,\ -3,\ -5-2i$
$+11+6i$	0	$1+i,\ -1+2i,\ -3,\ 1+4i,\ 1-4i,\ -7$
	1	$-1-2i,\ 3+2i,\ 3-2i$
	2	$-5-2i,\ -1+6i,\ 5-4i$
	3	$-5+2i,\ 5+4i,\ 7-2i.$

63.

We shall now seek, by examining examples, common criteria for the moduli for which a given prime number has the same character. We always suppose the moduli to be primary among their associates, that is, numbers $a+bi$ for which either $a \equiv 1, b \equiv 0$ or $a \equiv 3, b \equiv 2 \pmod 4$.

For the number $1+i$, with which we begin, the rule suggested by the examples is more easily grasped if we separate moduli of the first kind, for which $a \equiv 1, b \equiv 0$, from moduli of the second kind, for which $a \equiv 3, b \equiv 2$. With the help of the table in the preceding article, we find the following correspondences:

Character	Moduli of the first kind.
0	$5+4i,\ -7+8i,\ -7-8i,\ -11+4i$
1	$1-4i,\ -3+8i,\ -3-8i,\ 9+4i,\ -11$
2	$5-4i,\ -7,\ -11-4i$
3	$-3,\ 1+4i,\ 5+8i,\ 5-8i,\ 9-4i$

If we consider these seventeen examples carefully, in all of them we find the character $\equiv \frac{1}{4}(a-b-1) \pmod 4$.

Likewise, the correspondences are

Character	Moduli of the second kind.
0	$3-2i,\ -1-6i,\ 7+2i,\ -5+6i,\ -1+10i,\ 11+6i$
1	$-5+2i,\ -1+6i,\ 7-2i,\ -1-10i,\ 3+10i$
2	$-1+2i,\ -5-2i,\ 3-10i,\ 7+10i$
3	$-1-2i,\ 3+2i,\ -5-6i,\ 7-10i,\ 11-6i$

In all these twenty examples, with a little attention, the character is found to be $\equiv \frac{1}{4}(a-b-5) \pmod 4$.

These two rules can easily be combined into one valid for both kinds of moduli, if we consider that $\frac{1}{4}bb$ is $\equiv 0$ for moduli of the first kind and $\equiv 1 \pmod 4$ for those of the second. Thus the character of $1+i$ with respect to any prime modulus that is primary among its associates is $\equiv \frac{1}{4}(a-b-1-bb) \pmod 4$.

We should note in passing that, since $(b+1)^2$ always has the form $8n+1$, or, equivalently, $\frac{1}{4}(2b+bb)$ is even, this character is always even or odd according as $\frac{1}{4}(a+b-1)$ is even or odd. This agrees with the rule for the quadratic character stated in Article 58.

Since $\frac{1}{4}(a-b-1), \frac{1}{4}(a-b+3)$ are integers, one even and the other odd, their product will be even, or, equivalently, $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod 4$. Hence the following expression can also be used in place of the one given for the biquadratic character:

$$\frac{1}{4}(a-b-1-bb) - \frac{1}{8}(a-b-1)(a-b+3) = \frac{1}{8}(-aa+2ab-3bb+1)$$

This form also has the advantage that it is not restricted to primary moduli, but supposes only that a is odd and b even. For under this supposition either $a+bi$ or $-a-bi$ will evidently be primary among its associates, and the value of that formula is the same for either modulus.

64.

Starting from the last rule obtained in the preceding article, we find

Number	Character $\equiv$
$-1+i$	$\frac{1}{8}(aa+2ab-bb-1)$
$-1-i$	$\frac{1}{8}(-aa+2ab+bb+1)$
$+1-i$	$\frac{1}{8}(aa+2ab+3bb-1)$

This follows at once from the fact that the character of i is $\frac{1}{4}(aa+bb-1)$, while that of -1 is $\frac{1}{2}(aa+bb-1) \equiv \frac{1}{2}bb$, since $aa-1$ always has the form $8n$. These four rules, although so far obtained by examining examples, are evidently connected in such a way that, as soon as the proof of one has been completed, the other three will have been proved at the same time. It is scarcely necessary to point out that these rules too suppose only that a is odd and b even.

If we are willing to use formulas restricted to primary moduli, we can use the following form:

Number	Character $\equiv$
$-1+i$	$\frac{1}{4}(-a-b+1-bb)$
$-1-i$	$\frac{1}{4}(a-b-1+bb)$
$+1-i$	$\frac{1}{4}(-a-b+1+bb)$

The simplest formulas result if, as we did at the beginning of our examination of examples, we distinguish moduli of the first and second kinds. The characters are

Number	For moduli of the first kind	For moduli of the second kind
$-1+i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b-3)$
$-1-i$	$\frac{1}{4}(a-b-1)$	$\frac{1}{4}(a-b+3)$
$+1-i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b+5)$

65.

For the number $-1+2i$, to which we now proceed, we shall likewise use the same distinction between those moduli $a+bi$ for which $a \equiv 1, b \equiv 0$ and those for which $a \equiv 3, b \equiv 2$. The table in Article 62 shows that, with respect to that number, the following correspondences hold:

Character	Moduli of the first kind
0	$-3+8i,\ +5-8i,\ +9+4i,\ -11+4i$
1	$+1+4i,\ +5-4i,\ -7,\ -3-8i$
2	$+1-4i,\ +5+8i,\ -7-8i,\ -11$
3	$-3,\ +5+4i,\ +9-4i,\ -7+8i,\ -11-4i$

Reducing each of these moduli to its absolutely least residue modulo $-1+2i$, we observe that all those to which character 0 corresponds are $\equiv 1$; those to which character 1 corresponds are $\equiv i$; those whose character is 2 become $\equiv -1$; finally, all those whose character is 3 become $\equiv -i$. But the characters of $1, i, -1, -i$ for the modulus $-1+2i$ are themselves $0, 1, 2, 3$, respectively. Thus, in all these 17 examples, the character of $-1+2i$ with respect to a modulus $a+bi$ of the first kind is identical with the character of that number with respect to the modulus $-1+2i$.

Likewise, with the help of the table, we find the correspondences

Character	Moduli of the second kind
0	$+3+2i,\ -5-2i,\ -1+10i,\ -1-10i,\ +11+6i$
1	$+3-2i,\ -1+6i,\ -5-6i,\ +7+10i,\ +7-10i$
2	$-5+2i,\ -1-6i,\ +7-2i$
3	$-1-2i,\ +7+2i,\ -5+6i,\ +3+10i,\ +3-10i,\ +11-6i$

Reducing these moduli to their least residues modulo $-1+2i$, all those to which the characters $0, 1, 2, 3$ respectively correspond are found congruent to $-1, -i, +1, +i$. But when, conversely, $-1+2i$ is taken as the modulus, these very numbers have the characters $2, 3, 0, 1$, respectively. Consequently, in all these 19 examples, the character of $-1+2i$ with respect to a modulus of the second kind differs by two units from the character of that number with respect to $-1+2i$ taken as the modulus.

Moreover, it is readily seen that entirely similar results will hold for $-1-2i$.

66.

For the number -3, we omit the distinction between moduli of the first and second kinds, since the result shows that it is superfluous here. Thus the correspondences are

Character	Moduli
0	$-1+6i,\ -1-6i,\ -7,\ -5+6i,$ $-5-6i,\ -11,\ 11+6i,\ 11-6i$
1	$-1-2i,\ 1-4i,\ -5+2i,\ 5+4i,\ 7+2i,$ $5-8i,\ -1+10i,\ -7-8i,\ -11-4i,\ 7-10i$
2	$3+2i,\ 3-2i,\ -3+8i,\ -3-8i,$ $9+4i,\ 3+10i,\ 3-10i$
3	$-1+2i,\ 1+4i,\ -5-2i,\ 5-4i,\ 7-2i,$ $5+8i,\ -1-10i,\ -7+8i,\ -11+4i,\ 7+10i$

Reducing these moduli to their least residues modulo 3, we see that those to which character 0 corresponds are partly $\equiv 1$, partly $\equiv -1$; those whose character is 1 become either $\equiv 1 - i$ or $\equiv -1 + i$; those whose character is 2 become either $\equiv i$ or $\equiv -i$; finally, those to which character 3 belongs are either $\equiv 1 + i$ or $\equiv -1 - i$. From this examination of examples we therefore conclude that the character of -3 for a modulus that is a prime number primary among its associates is identical with the character of that very number when 3, or equivalently -3, is considered as the modulus.

67.

Examining examples similarly for other prime numbers, we find that $3 \pm 2i, -1 \pm 6i, 7 \pm 2i, -5 \pm 6i$, etc., give theorems similar to the one reached in Article 65 for $-1+2i$, whereas $1 \pm 4i, 5 \pm 4i, -3 \pm 8i, 5 \pm 8i, 9 \pm 4i$, etc., behave in the same way as -3. The examination of examples thus leads to a most elegant theorem,. which, by analogy with the theory of quadratic residues in the arithmetic of real numbers, may be called the FUNDAMENTAL THEOREM of the theory of biquadratic residues, namely:

Let $a + bi, a' + b'i$ denote distinct prime numbers, primary among their respective associates, that is, congruent to unity modulo $2+2i$. The biquadratic character of $a+bi$ with respect to the modulus $a'+b'i$ will be identical with the character of $a' + b'i$ with respect to the modulus $a + bi$, if either both numbers $a + bi, a' + b'i$, or at least one of them, belong to the first kind, that is, are congruent to unity modulo 4. On the other hand, those characters will differ from one another by two units if neither number $a + bi, a' + b'i$ belongs to the first kind, that is, if each is congruent modulo 4 to $3 + 2i$.

Yet despite the great simplicity of this theorem, its proof must be counted among the most deeply hidden mysteries of higher arithmetic. At least as matters now stand, it can be unravelled only through the most subtle investigations, which would go far beyond the limits of the present paper. We therefore reserve the publication of this proof, as well as the development of the connection between this theorem and those that we had begun to establish by examining examples at the beginning of this paper, for a third paper. Nevertheless, by way of conclusion, we shall give here what is required to prove the theorems proposed in Articles 63. 64.

68.

We begin with prime numbers $a + bi$ for which $b = 0$ (the third species in Article 34). Here, for the number to be primary among its associates, a must therefore be a negative real prime number of the form $-(4n + 3)$, for which we shall write $-q$, such as $-3, -7, -11, -19$, etc. Denoting by λ the character of $1 + i$, with that number taken as the modulus, we must have

$$i^{\lambda} \equiv (1+i)^{\frac{1}{4}(qq-1)} \equiv 2^{\frac{1}{8}(qq-1)} \,.\, i^{\frac{1}{8}(qq-1)} \pmod{q}$$

But it is known that 2 is a quadratic residue or a quadratic nonresidue of q according as q has the form $8n+7$ or the form $8n+3$. From this we conclude that, in general,

$$2^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{4}(q+1)} \equiv i^{\frac{1}{2}(q+1)} \pmod{q}$$

and consequently, raising to the power with exponent $\frac{1}{4}(q+1)$,

$$2^{\frac{1}{8}(qq-1)} \equiv i^{\frac{1}{8}(q+1)^2} \pmod{q}$$

The preceding equation therefore takes the form

$$i^{\lambda} \equiv i^{\frac{1}{8}(q+1)^2 + \frac{1}{8}(qq-1)} \equiv i^{\frac{1}{4}(qq+q)} \pmod{q}$$

whence it follows that

$$\lambda \equiv \frac{1}{4}(qq+q) \equiv \frac{1}{4}(q+1)^2 - \frac{1}{4}(q+1) \pmod{4}$$

or, since $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$, $\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(a-1) \pmod{4}$. This is precisely the theorem of Article 63 for the case $b = 0$.

69.

Moduli $a+bi$ for which $b=0$ does not hold (numbers of the fourth species in Art. 34) are much harder to deal with, however, and several investigations must come first. We shall denote the norm $aa+bb$, which will be a real prime of the form $4n+1$, by p.

Let S denote the collection of all simply least residues for the modulus $a+bi=m$, with zero excluded, so that the count of the numbers contained in S is $=p-1$. Let $x+yi$ denote any number of this system, and put $ax+by=\xi, ay-bx=\eta$. Then ξ,η will be integers lying between the bounds 0 and p, *excluding the bounds*. For in the present case, where a,b are relatively prime, the formulas of Art. 45, namely $\eta\equiv k\xi, \xi\equiv -k\eta \pmod p$, show that neither of the numbers ξ,η can be $=0$ unless the other vanishes at the same time, so that $x=0, y=0$, a combination we have already excluded. Thus the criterion for a number $x+yi$ to be contained in S is that the four numbers $\xi,\eta,p-\xi,p-\eta$ be positive.

We further observe that $\xi=\eta$ cannot hold for any such number. For it would follow that $p(x+y)=a(\xi+\eta)+b(\xi-\eta)=2a\xi$, which is absurd, since none of the factors $2,a,\xi$ is divisible by p. Similarly, the equation $p(x-y+a+b)=2a\xi+(a+b)(p-\xi-\eta)$ shows that $\xi+\eta=p$ cannot hold. Since the numbers $\xi-\eta, p-\xi-\eta$ must therefore be either positive or negative, we obtain from this a subdivision of the system S into four collections C, C', C'', C''', assigning the numbers as follows:

Into collection	Numbers for which
C	$\xi-\eta$ positive, $p-\xi-\eta$ positive
C'	$\xi-\eta$ positive, $p-\xi-\eta$ negative
C''	$\xi-\eta$ negative, $p-\xi-\eta$ negative
C'''	$\xi-\eta$ negative, $p-\xi-\eta$ positive

The criterion for a number of the collection C is thus, strictly speaking, sixfold: the six numbers $\xi,\eta,p-\xi,p-\eta,\xi-\eta,p-\xi-\eta$ must be positive. But conditions $2,5$ and 6 evidently already imply the others. The same applies to the collections C', C'', C''', so that the complete criteria are threefold, namely:

For collection	The following numbers must be positive
C	$\eta,\quad \xi-\eta,\quad p-\xi-\eta$
C'	$p-\xi,\quad \xi-\eta,\quad \xi+\eta-p$
C''	$p-\eta,\quad \eta-\xi,\quad \xi+\eta-p$
C'''	$\xi,\quad \eta-\xi,\quad p-\xi-\eta$

Even without our pointing it out, anyone will readily understand that, in the geometric representation of complex numbers (see Art. 39), the numbers of the system S lie inside the square whose sides join the points representing the numbers $0, a+bi, (1+i)(a+bi), i(a+bi)$, and that the subdivision of the system S corresponds to the division of the square by its diagonals. Here, however, we have preferred to use purely arithmetical reasoning, leaving illustration by a geometric representation to the experienced reader for the sake of brevity.

70.

If four complex numbers $r = x + yi, r' = x' + y'i, r'' = x'' + y''i, r''' = x''' + y'''i$ are related in such a way that $r' = m+ir, r'' = m+ir' = (1+i)m-r, r''' = m + ir'' = im - ir$, and the first, r, is supposed to belong to the collection C, then the others r', r'', r''' will belong respectively to the collections C', C'', C'''. For, putting $\xi = ax + by, \eta = ay - bx, \xi' = ax' + by', \eta' = ay' - bx', \xi'' = ax'' + by'', \eta'' = ay'' - bx'', \xi''' = ax''' + by''', \eta''' = ay''' - bx'''$, we find

$$\begin{aligned} \eta = p - \xi' = p - \eta'' = \xi''' \\ \xi - \eta = \xi' + \eta' - p = \eta'' - \xi'' = p - \xi''' - \eta''' \\ p - \xi - \eta = \xi' - \eta' = \xi'' + \eta'' - p = \eta''' - \xi''' \end{aligned}$$

from which the truth of the theorem follows at once by the criteria. Since $r = m + ir'''$ holds again, it is easy to see that, if r is supposed to belong to C', the numbers r', r'', r''' belong respectively to C'', C''', C; if it belongs to C'', they belong to C''', C, C'; and finally, if it belongs to C''', they belong to C, C', C''.

At the same time, we conclude that the individual collections C, C', C'', C''' contain equally many numbers, namely $\frac{1}{4}(p-1)$.

37.

THEOREM. *Let k denote an integer not divisible by m. If each number of the collection C is multiplied by k, and the simply least residues of the products modulo m are distributed among the collections C, C', C'', C''', with the counts of the residues belonging to these individual collections denoted respectively by c, c', c'', c''', then the character of the number k with respect to the modulus m will be $\equiv c' + 2c'' + 3c'''$ (mod 4).*

Proof. Let those c least residues belonging to C be $\alpha, \beta, \gamma, \delta$, etc.; next, let the c' residues belonging to C' be $m+i\alpha', m+i\beta', m+i\gamma', m+i\delta'$, etc.; further, let the c'' residues belonging to C'' be $(1+i)m-\alpha'', (1+i)m-\beta'', (1+i)m-\gamma'', (1+i)m-\delta''$, etc.; and finally, let the c''' residues belonging to C''' be $im-i\alpha''', im-i\beta''', im-i\gamma''', im-i\delta'''$, etc. Now consider four products, namely:

1) the product of all $\frac{1}{4}(p-1)$ numbers constituting the collection C:

2) the product of the products obtained by multiplying each of these numbers by k;

3) the product of the least residues of these products, namely of the numbers $\alpha, \beta, \gamma, \delta$, etc., $m+i\alpha', m+i\beta'$, etc., etc.

4) the product of all $c+c'+c''+c'''$ numbers $\alpha, \beta, \gamma, \delta$, etc., $\alpha', \beta', \gamma', \delta'$, etc., $\alpha'', \beta'', \gamma'', \delta''$, etc.

Denoting these four products in order by P, P', P'', P''', we evidently have

$$P' = k^{\frac{1}{4}(p-1)}P, \quad P' \equiv P'', \quad P'' \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

and therefore

$$Pk^{\frac{1}{4}(p-1)} \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

It is easy to see, however, that the numbers $\alpha', \beta', \gamma', \delta'$, etc., $\alpha'', \beta'', \gamma'', \delta''$, etc., $\alpha''', \beta''', \gamma''', \delta'''$, etc., all belong to the collection C, and are distinct both from one another and from the numbers $\alpha, \beta, \gamma, \delta$, etc., just as the latter themselves are distinct from one another. All these numbers taken together, disregarding their order, must therefore be exactly the same as all the numbers constituting the collection C. Hence we conclude that $P = P'''$, and consequently

$$Pk^{\frac{1}{4}(p-1)} \equiv Pi^{c'+2c''+3c'''} \pmod{m}$$

Finally, since none of the individual factors of the product P is divisible by m, we conclude that

$$k^{\frac{1}{4}(p-1)} \equiv i^{c'+2c''+3c'''} \pmod{m}$$

so that $c'+2c''+3c'''$ will be the character of the number k with respect to the modulus m. Q. E. D.

72.

To apply the general theorem of the preceding article to the number $1+i$, we must subdivide the collection C again into two smaller collections G and G'. We shall assign to the collection G those numbers $x+yi$ for which $ax+by=\xi$ is less than $\frac{1}{2}p$, and to the other collection G' those for which ξ is greater than $\frac{1}{2}p$. We shall denote the counts of the numbers contained in the collections G, G' respectively by g, g', so that $g+g'=\frac{1}{4}(p-1)$.

The complete criterion for numbers belonging to G is therefore that the three numbers $\eta, \xi-\eta, p-2\xi$ be positive. For the third condition for the collection C, requiring $p-\xi-\eta$ to be positive, is already implicitly contained in these conditions, since $p-\xi-\eta=(\xi-\eta)+(p-2\xi)$. Similarly, the complete criterion for numbers belonging to G' consists in positive values of the three numbers $\eta, p-\xi-\eta, 2\xi-p$.

It follows easily that the product of any number of the collection G by the number $1+i$ belongs to the collection C'''. For, putting

$$(x+yi)(1+i)=x'+y'i, \quad \text{and} \quad ax'+by'=\xi', \ ay'-bx'=\eta', \ \text{we find}$$
$$\xi'=\xi-\eta, \quad \eta'-\xi'=2\eta, \quad p-\xi'-\eta'=p-2\xi$$

that is, the criterion for the number $x+yi$ to belong to the collection G is identical with the criterion for the number $x'+y'i$ to belong to the collection C'''.

In precisely the same way, it is shown that the product of any number of the collection G' by $1+i$ belongs to the collection C''.

Thus, if in the preceding article we give k the value $1+i$, we have $c=0, c'=0, c''=g', c'''=g$, and the character of the number $1+i$ becomes $3g+2g'=\frac{1}{2}(p-1)+g$. Since the characters of the numbers $i, -1$ are $\frac{1}{4}(p-1), \frac{1}{2}(p-1)$, the characters of the numbers $-1+i, -1-i, 1-i$ will respectively be $\frac{3}{4}(p-1)+g, g, \frac{1}{4}(p-1)+g$. The whole matter now turns, therefore, on determining the number g.

73.

What we have set out in Arts. 69—72 is, strictly speaking, independent of the assumption that m is a primary number. From now on, however, we shall at least suppose that a is odd and b even, and further that a, b and $a-b$ are positive numbers. First of all, we must establish the bounds on the values of x in the collection G.

Putting $ay - bx = \eta, (a+b)x - (a-b)y = \zeta, p - 2ax - 2by = \theta$, the criterion for numbers $x+yi$ to belong to the collection G consists in the three conditions that η, ζ, θ be positive numbers. Since $px = (a-b)\eta + a\zeta, p(a - 2x) = a\theta + 2b\eta$, it is evident that x and $2a - x$ must be positive numbers, or that x must equal one of the numbers $1, 2, 3 \ldots \frac{1}{2}(a-1)$. Further, since $(a-b)\theta = 2b\zeta + p(a-b-2x)$, it is clear that, as long as x is less than $\frac{1}{2}(a-b)$, the second condition (requiring ζ to be positive) already implies the third (that θ must be positive). Conversely, whenever x is greater than $\frac{1}{2}(a-b)$, the second condition is already contained in the third. Thus, for the values x takes in $1, 2, 3 \ldots \frac{1}{2}(a-b-1)$, we need only ensure that η and ζ are positive, or that y is greater than $\frac{bx}{a}$ and less than $\frac{(a+b)x}{a-b}$. For such a given value of x, the total count of numbers $x+yi$ is therefore

$$\left[\frac{(a+b)x}{a-b}\right] - \left[\frac{bx}{a}\right]$$

if we use the brackets in the same sense in which we have already used them repeatedly elsewhere (compare *Theorematis arithm. dem. nova*, Art. 4, and *Theorematis fund. in doctr. de residuis quadr.* etc., *Algorithm. nov.*, Art. 3). For the values x takes in $\frac{1}{2}(a-b+1), \frac{1}{2}(a-b+3) \ldots . \frac{1}{2}(a-1)$, on the other hand, it suffices to give η and θ positive values, or to make y greater than $\frac{bx}{a}$ and less than $\frac{p-2ax}{2b}$, or $\frac{1}{2}b + \frac{aa-2ax}{2b}$. Thus, for such a given value of x, the total count of numbers $x+yi$ is

$$\left[\frac{1}{2}b + \frac{aa-2ax}{2b}\right] - \left[\frac{bx}{a}\right]$$

Hence we conclude that the count of numbers in the collection G is

$$g = \Sigma\left[\frac{(a+b)x}{a-b}\right] + \Sigma\left[\frac{1}{2}b + \frac{aa-2ax}{2b}\right] - \Sigma\left[\frac{bx}{a}\right]$$

where the first sum extends over all integer values of x from 1 to $\frac{1}{2}(a-b-1)$, the second from $\frac{1}{2}(a-b+1)$ to $\frac{1}{2}(a-1)$, and the third from 1 to $\frac{1}{2}(a-1)$.

If we use the symbol φ in the same sense as in the place cited (*Theorematis fund.* etc., *Algor. nov.*, Art. 3), namely so that

$$\varphi(t,u) = \left[\frac{u}{t}\right] + \left[\frac{2u}{t}\right] + \left[\frac{3u}{t}\right] \ldots . + \left[\frac{t'u}{t}\right]$$

where t, u denote any positive numbers and t' the number $[\frac{1}{2}t]$, then the first term becomes $= \varphi(a-b, a+b)$, and the third $= -\varphi(a,b)$; the second, however, becomes

$$= \frac{1}{4}bb + \Sigma\left[\frac{aa-2ax}{2b}\right]$$

But, writing the terms in reverse order, we have

$$\begin{aligned}\Sigma\left[\frac{aa-2ax}{2b}\right] &= \left[\frac{a}{2b}\right] + \left[\frac{3a}{2b}\right] + \left[\frac{5a}{5b}\right] + \ldots . + \left[\frac{(b-1)a}{2b}\right] \\ &= \varphi(2b,a) - \varphi(b,a)\end{aligned}$$

Our formula therefore takes the following form:

$$g = \varphi(a-b, a+b) + \varphi(2b,a) - \varphi(a,b) - \varphi(b,a) + \frac{1}{4}bb$$

Let us first consider the term $\varphi(a-b, a+b)$, which immediately changes into $\varphi(a-b, 2b) + 1 + 2 + 3 +$ etc. $+ \frac{1}{2}(a-b-1)$, or into

$$\varphi(a-b, 2b) + \frac{1}{8}((a-b)^2 - 1)$$

Next, since the general theorem gives $\varphi(t,u) + \varphi(u,t) = [\frac{1}{2}t] \,.\, [\frac{1}{2}u]$ when t, u are relatively prime positive integers, we have

$$\varphi(a-b, 2b) = \frac{1}{2}b(a-b-1) - \varphi(2b, a-b)$$

and consequently

$$\varphi(a-b, a+b) = \frac{1}{8}(aa + 2ab - 3bb - 4b - 1) - \varphi(2b, a-b)$$

Let us arrange the parts of $\varphi(2b, a-b)$ as follows:

$$\begin{aligned}&\left[\frac{a-b}{2b}\right] + \left[\frac{3(a-b)}{2b}\right] + \left[\frac{5(a-b)}{2b}\right] + \text{ etc. } + \left[\frac{(b-1)(a-b)}{2b}\right] \\ &+ \left[\frac{a-b}{b}\right] + \left[\frac{2(a-b)}{b}\right] + \left[\frac{3(a-b)}{b}\right] + \text{ etc. } + \left[\frac{\frac{1}{2}b(a-b)}{b}\right]\end{aligned}$$

The second series evidently becomes

$$= \varphi(b, a-b) = \varphi(b,a) - 1 - 2 - 3 - \text{ etc. } - \frac{1}{2}b$$
$$= \varphi(b,a) - \frac{1}{8}(bb + 2b)$$

We write the first series, with the order of its terms reversed, as follows:

$$\left[\frac{1}{2}(a+1-b) - \frac{a}{2b}\right] + \left[\frac{1}{2}(a+3-b) - \frac{3a}{2b}\right]$$
$$+ \left[\frac{1}{2}(a+5-b) - \frac{5a}{2b}\right] + \text{etc.} + \left[\frac{1}{2}(a-1) - \frac{(b-1)a}{2b}\right]$$

This expression. Since, with t denoting an integer and u a fraction, we generally have $[t-u] = t - 1 - [u]$, it changes into the following:

$$\frac{1}{8}b(2a-4-b) - \left[\frac{a}{2b}\right] - \left[\frac{3a}{2b}\right] - \left[\frac{5a}{2b}\right] - \text{ etc. } - \left[\frac{(b-1)a}{2b}\right]$$
$$= \frac{1}{8}b(2a-4-b) - \varphi(2b,a) + \varphi(b,a)$$

Hence

$$\varphi(2b, a-b) = 2\varphi(b,a) - \varphi(2b,a) + \frac{1}{4}b(a-3-b)$$

and therefore

$$\varphi(a-b, a+b) = \varphi(2b,a) - 2\varphi(b,a) + \frac{1}{8}(aa - bb + 2b - 1)$$

Substituting this value in the formula for g given above, and also substituting $\varphi(a,b) + \varphi(b,a) = \frac{1}{4}b(a-1)$, we obtain

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \frac{1}{8}(aa - 2ab + bb + 4b - 1)$$

74.

Precisely similar reasoning deals with the case where a, b remain positive but $a-b$ is negative, or $b-a$ positive. The equations $p(a-2x) = 2b\eta + a\theta$, $p(b-a+2x) = 2b\zeta + (b-a)\theta$ show that $\frac{1}{2}a - x$ and $x + \frac{1}{2}(b-a)$ must be positive, and hence that x must equal one of the numbers $-\frac{1}{2}(b-a-1), -\frac{1}{2}(b-a-3), -\frac{1}{2}(b-a-5) \ldots + \frac{1}{2}(a-1)$. Further, the equation $px + (b-a)\eta = a\zeta$ shows that, for negative values of x, the condition requiring η to be positive is already contained in the condition requiring ζ to be positive, whereas the reverse holds whenever x is given a positive value. Thus the values of y, for a fixed negative value of x, must lie between $\frac{(a+b)x}{a-b}$ and $\frac{p-2ax}{2b}$, whereas for a positive value of x they must lie between $\frac{bx}{a}$ and $\frac{p-2ax}{2b}$. For $x = 0$, these bounds are evidently 0 and $\frac{p-2ax}{2b}$, with the value $y = 0$ itself excluded. Hence

$$g = -\Sigma \left[\frac{(a+b)x}{a-b}\right] + \Sigma \left[\frac{1}{2}b + \frac{aa-2ax}{2b}\right] - \Sigma \left[\frac{bx}{a}\right]$$

where the first sum extends over all negative values of. x from -1 to $-\frac{1}{2}(b-a-1)$; the second over all values of x from $-\frac{1}{2}(b-a-1)$ to $\frac{1}{2}(a-1)$; and the third over all positive values of x from $+1$ to $\frac{1}{2}(a-1)$. In this way the first sum gives $-\varphi(b-a, b+a)$, the second, as in the preceding article, $\frac{1}{4}bb + \varphi(2b, a) - \varphi(b, a)$, and finally the third $-\varphi(a, b)$; thus we have

$$g = -\varphi(b-a, b+a) + \varphi(2b, a) - \varphi(b, a) - \varphi(a, b) + \frac{1}{4}bb$$

Now, in the same way as in the preceding article, we obtain

$$\begin{aligned}\varphi(b-a, b+a) &= \varphi(b-a, 2b) - \frac{1}{8}((b-a)^2 - 1) \\ &= \frac{1}{8}(3bb - 2ab - aa - 4b + 1) - \varphi(2b, b-a)\end{aligned}$$

as well as

$$\varphi(2b, b-a) = \varphi(2b, a) - 2\varphi(b, a) + \frac{1}{4}b(b-1-a)$$

and consequently

$$\varphi(b-a, b+a) = 2\varphi(b, a) - \varphi(2b, a) + \frac{1}{8}(bb - aa - 2b + 1)$$

and finally

$$g = 2\varphi(2b, a) - 2\varphi(b, a) + \frac{1}{8}(aa - 2ab + bb + 4b - 1)$$

It is therefore proved that the same formula for g holds whether $a-b$ is positive or negative, provided that a, b are positive.

75.

To obtain a further reduction, we put

$$L = \left[\frac{a}{2b}\right] + \left[\frac{2a}{2b}\right] + \left[\frac{3a}{2b}\right] + \text{etc.} + \left[\frac{\frac{1}{2}ba}{2b}\right]$$

$$M = \left[\frac{(\frac{1}{2}b+1)a}{2b}\right] + \left[\frac{(\frac{1}{2}b+2)a}{2b}\right] + \left[\frac{(\frac{1}{2}b+3)a}{2b}\right] + \text{etc.} + \left[\frac{ba}{2b}\right]$$

$$N = \left[\frac{a+b}{2b}\right] + \left[\frac{2a+b}{2b}\right] + \left[\frac{3a+b}{2b}\right] + \text{etc.} + \left[\frac{\frac{1}{2}ba+b}{2b}\right]$$

It is easy to see that $[u]+[u+\frac{1}{2}] = [2u]$ holds in general, whatever real quantity u denotes. Thus $L + N = \varphi(b, a)$, and since evidently $L + M = \varphi(2b, a)$, we have

$$\varphi(2b, a) - \varphi(b, a) = M - N$$

Further, it is evident that the sum of the first term of the series N and the next-to-last term of the series M, namely $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right]$, is $= \frac{1}{2}(a-1)$, and that the same sum is formed by the second term of the series N and the third-to-last term of the series M, and so on. Since the last term of the series M is also $= \frac{1}{2}(a-1)$, while the last term of the series N is $= \left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$, with the upper or lower sign applying according as a is of the form $4n+1$ or $4n-1$, we have

$$M + N = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1)$$

and therefore

$$\varphi(2b, a) - \varphi(b, a) = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1) - 2N$$

Thus the formula for g found in Arts. 73 and 74 becomes

$$g = \frac{1}{8}((a+b)^2 - 1) + 2n - 4N$$

putting $a \mp 1 = 4n$, where n will be an integer. Since this gives $1 = 16nn - 8an + aa$, this formula can also be written as follows:

$$g = \frac{1}{8}(-aa + 2ab + bb + 1) + 4(\frac{1}{2}(a+1)n - nn - N)$$

Since g is the character of the number $-1-i$ for the modulus $a+bi$, this character is therefore $\equiv \frac{1}{8}(-aa + 2ab + bb + 1) \pmod 4$. This is precisely the theorem found above (Art. 64) by examining examples, and the theorems concerning the characters of the numbers $1+i$, $1-i$, $-1+i$ follow from it at once. Thus these four theorems have now been rigorously proved for the case where a and b are positive.

76.

If a remains positive and b is negative, put $b = -b'$, so that b' is positive. It is now proved that, for the modulus $a + b'i$, the character of the number $-1 - i$ is $\equiv \frac{1}{8}(-aa + 2ab' + b'b' + 1) \pmod 4$. Hence the character of the number $-1 + i$ for the modulus $a - b'i$, by the theorem stated in Art. 62, is $\equiv \frac{1}{8}(aa - 2ab' - b'b' - 1)$, that is, the character of the number $-1 + i$ for the modulus $a + bi$ becomes $\equiv \frac{1}{8}(aa + 2ab - bb - 1)$. This is precisely the theorem stated in Art. 64, from which the other three concerning the characters of the numbers $1 + i$, $1 - i$, $-1 - i$ follow at once. Thus these theorems are also proved for the case where b is negative, that is, for all cases where a is positive.

Finally, if a is negative, put $a = -a'$, $b = -b'$. By what has already been proved, the character of the number $1 + i$ with respect to the modulus $a' + b'i$ is $\equiv \frac{1}{8}(-a'a' + 2a'b' - 3b'b' + 1) \pmod 4$, and it makes no difference whether we take the number $a' + b'i$ or its opposite $-a' - b'i$ as the modulus. Thus the character of the number $1 + i$ with respect to the modulus $a + bi$ is evidently $\equiv \frac{1}{8}(-aa + 2ab - 3bb + 1)$, and the same applies to the characters of the numbers $1 - i$, $-1 + i$, $-1 - i$.

We therefore conclude that the proof of the theorems concerning the characters of the numbers $1 + i$, $1 - i$, $-1 + i$, $-1 - i$ (Arts. 63. 64) is no longer subject to any restriction.

REVIEWS

OF HIS OWN

WRITINGS.

Göttingische gelehrte Anzeigen. 1808 May 12.

A paper submitted by Professor Gauss to the Royal Society of Sciences on January 15 of this year,

Theorematis arithmetici demonstratio nova,

an account of whose contents we still owe here, concerns the famous fundamental theorem in the theory of quadratic residues, which plays so important a role both throughout *higher arithmetic* and in the neighbouring parts of analysis. As is well known, an integer a is called a *quadratic residue* of the integer b if there are numbers of the form $xx - a$ divisible by b, while in the opposite case a is called a *quadratic nonresidue* of b. The number a may be positive or negative, whereas b is always regarded as positive. Higher arithmetic teaches that all prime numbers b for which a given number a is a quadratic residue are included in certain linear forms, while other linear forms contain all the primes of which a is a nonresidue. Thus, for example, -1 is a quadratic residue of all primes of the form $4n + 1$ and a quadratic nonresidue of all primes of the form $4n + 3$; further, $+2$ is a quadratic residue of all primes of the forms $8n + 1$, $8n + 7$, but a quadratic nonresidue of all primes of the forms $8n + 3$, $8n + 5$. There are infinitely many similar special theorems, but all can be derived by combining the two just mentioned with the following general theorem: Two distinct positive (odd) primes, p, q, always bear the *same* relation to each other (that is, one is a quadratic residue or nonresidue of the other according as the other is a residue or nonresidue of the first) if either both have the form $4n + 1$, or at least one does. Their mutual relation is opposite, however (that is, one is a nonresidue of the other if the latter is a residue of the former, and conversely), whenever *both* have the form $4n + 3$. This is the fundamental theorem mentioned above, which can be expressed in more than one form. The form chosen here is the one in which it is newly proved in Professor Gauss's paper.

The most beautiful theorems of higher arithmetic, especially those discussed here, have the peculiarity that they are easily discovered by examining examples, whereas their proofs lie extremely well hidden and can be found only through very deep investigations. This is precisely what gives higher arithmetic the magical appeal that has made it the favourite field of the foremost mathematicians, quite apart from its inexhaustible wealth, in which it so far surpasses every other part of pure mathematics. The two special theorems mentioned above were already known to Fermat, who claimed also to possess their proofs. Whether he was mistaken in this we cannot decide, since he never published anything about them; but we can certainly regard

it as possible, since there are several examples of self-deception among other great mathematicians, notably EULER, LEGENDRE, and also FERMAT himself. EULER gave the first proof of the first of these theorems. But this great mathematician did not succeed in proving the other, despite his devoted efforts over many years; it was left to LAGRANGE to fill that gap. Both mathematicians also proved various other special theorems, but a greater number, which they found by examining examples, always eluded their attempts at proof. It is, however, a remarkable twist of chance that neither mathematician discovered in this way the general fundamental theorem, which admits of so simple a statement. It was first presented, though in a somewhat different form, by LEGENDRE in the *Histoire de l'Académie des Sciences de Paris* 1785. Both there and later in his *Essai d'une théorie des nombres*, this excellent analyst sought to base the proof on very ingenious investigations, which nevertheless failed to reach the desired goal; and, unless we are mistaken, that goal could not have been reached by this route either.

The author of the paper to which this review is devoted entered the field of higher arithmetic at a time when all earlier work by other mathematicians in this subject was entirely unknown to him. It is chiefly to this circumstance that we must attribute his having followed a wholly distinctive course throughout. He found that fundamental theorem very early by examining examples, but only a whole year later, after many difficulties and unsuccessful attempts, did he succeed in finding the first completely rigorous proof, developed in the fourth section of his *Disquisitiones Arithmeticae*. This proof, however, rests on very laborious and lengthy arguments. He subsequently found three other proofs, which are free of that inconvenience but instead require other very deep investigations, wholly different in content. One of these proofs is also given in the cited work, Art. 262; the other two will be made known in due course. The wish therefore remained that it might be possible to discover a shorter proof, independent of investigations of an unrelated kind. The author thus hopes that friends of higher arithmetic will take pleasure in a fifth proof, presented in the present paper in fewer than five pages, which seems to leave nothing to be desired in any respect. Given the concentrated brevity of this proof, we can admittedly give only an imperfect idea of its course here. Anything more would be all the more unnecessary, since Volume XVI of the *Commentationes*, in which it has already been printed, will appear shortly.

The proof rests on the following new theorem: Let p denote a (positive odd) prime and k any integer not divisible by p. Suppose further that, among the remainders obtained by dividing the $\frac{1}{2}(p-1)$ products k, $2k$, $3k \ldots . \frac{1}{2}(p-1)k$ by p, there are in all μ remainders greater than $\frac{1}{2}p$ (and hence $\frac{1}{2}(p-1)-\mu$ less than $\frac{1}{2}p$). Then k will be a quadratic residue of p if μ is even, but a quadratic nonresidue if μ is odd. The number μ, which depends only on k and p, may be represented by the symbol (k, p). A sequence of deductions that cannot be abridged now shows that, if k and p are two relatively prime odd numbers, $(k, p) + (p, k) + \frac{1}{4}(k-1)(p-1)$ is always an *even* number. It follows that, whenever k and p both have the form $4n+3$, one of the numbers (k, p), (p, k) must be even and the other odd; in all other cases, that is, whenever both numbers k and p, or at least one of them, have the form $4n+1$, either $.(k, p)$, (p, k) must both be even or both must be odd. Combined with the theorem above, this immediately gives the truth of the fundamental theorem.—The same route by which these results are obtained also gives, in the paper, a new proof of the two special theorems mentioned above. It is easy to show that $(-1, p) = \frac{1}{2}(p-1)$, hence even or odd according as p has the form $4n+1$ or $4n+3$; similarly, $(2, p) = \frac{1}{4}(p-1)$ if p has the form $4n+1$, and $(2, p) = \frac{1}{4}(p+1)$ if p has the form $4n+3$. Thus $(2, p)$ is even whenever p has the form $8n+1$ or $8n+7$, but odd whenever p has the form $8n+3$ or $8n+5$.

Göttingische Gelehrte Anzeigen. 1808 September 19.

A lecture submitted by Professor Gauss to the Royal Society of Sciences,

Summatio quarumdam serierum singularium,

aims to develop more fully and in greater generality a remarkable investigation concerning the division of the circle, whose foundation had already been laid in the *Disquisitionibus Arithmeticis*, to provide it with complete proofs, and to show its unexpected connection with other important truths. Let n denote a prime, k any integer not divisible by n, and ω the arc $\frac{1}{n}360^\circ$. Among the numbers $1, 2, 3, 4, \ldots . n-1$, let the distinct quadratic residues of n be represented by a, a', a'', and so on, while the numbers remaining after these have been excluded, or the quadratic nonresidues of n, are represented by b, b', b'', and so on. It is proved in the cited work, Art. 356, that, when n has the form $4n+1$,

$$\left.\begin{array}{l}\cos ak\omega + \cos a'k\omega + \cos a''k\omega + \text{etc.} \\ -\cos bk\omega - \cos b'k\omega - \cos b''k\omega - \text{etc.}\end{array}\right\} = \pm\sqrt{n}.$$

and

$$\left.\begin{array}{l}\sin ak\omega + \sin a'k\omega + \sin a''k\omega + \text{etc.} \\ -\sin bk\omega - \sin b'k\omega - \sin b''k\omega - \text{etc.}\end{array}\right\} = 0$$

whereas, when n has the form $4m+3$, the sum of the first series becomes $= 0$ and that of the second $= \pm\sqrt{n}$. The sign to be placed before the radical depends on the value of the number k, or rather on its relation to n, and is easily determined for *all* values of k at a given value of n once it is determined for *one*. For it can be shown that *the same* sign applies to all values of k that are quadratic residues of n, and the opposite sign to all those that are quadratic nonresidues of n. Since the investigation had already been carried this far in the cited work, and only the determination of the sign for any one value of k remained, one would have thought that, with the main matter settled, this further determination could easily be supplied. This seemed all the more likely because examining examples immediately gives an extremely simple result: for $k = 1$, or for all values that are quadratic residues of n, the radical in the formulas above must always be taken *positively*. Yet in seeking a proof of this observation we encounter wholly unexpected difficulties, and the procedure that led so satisfactorily to the absolute value of those series proves entirely inadequate when the complete determination of the signs is required. The *metaphysical* reason for this phenomenon (to use the expression customary among French mathematicians) must be sought in the

fact that, in dividing the circle, analysis makes no distinction between the arcs $\omega, 2\omega, 3\omega \ldots (n-1)\omega$, but treats them all alike. As this gives the investigation a new interest, Professor GAUSS found in it, as it were, an invitation to leave nothing untried in overcoming the difficulty. Only after many and varied unsuccessful attempts did he succeed, by a route remarkable in itself. He starts from the summation of certain series whose terms have the following form:

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)\ (1-xx)\ (1-x^3)\ldots.(1-x^\mu)}$$

If, for brevity, we denote such a function by (m, μ), which, as the paper shows, is always a *polynomial* in x, then the series

$$1-(m,1)+(m,2)-(m,3)+\text{etc.}$$

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+\text{etc.}$$

terminate after the term in position $m+1$, provided that m denotes a positive integer. For even values of m the sum of the first series becomes

$$=(1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1})$$

and $=0$ for odd values of m, whereas the sum of the second series always becomes

$$=(1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}})\ldots(1+x^{\frac{1}{2}m})$$

For fractional and negative values of m, too, the summation of these series leads to interesting results, though they are not needed for the present purpose. We content ourselves with giving just one of them here. The infinite series

$$1+x+x^3+x^6+x^{10}+\text{etc.}$$

whose exponents are the triangular numbers is the product of the factors

$$\frac{1-xx}{1-x}\times\frac{1-x^4}{1-x^3}\times\frac{1-x^6}{1-x^5}\times\frac{1-x^8}{1-x^7}\ \text{etc.}$$

or, if preferred, of

$$(1+x)^2(1+xx)^2(1+x^3)^2(1+x^4)^2\ \text{etc.}$$

multiplied by

$$(1-x)(1-xx)1-x^3)(1-x^4)\ \text{etc.}$$

An account of how these summations are applied to the main subject would take us too far here. We may refer readers to the paper itself all the more

readily since it will soon appear in print. The summations quoted above are only a special application of the summation of the following series:

$$1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega + \text{etc.} + \cos(n-1)^2 k\omega = T$$

$$\sin k\omega + \sin 4k\omega + \sin 9k\omega + \text{etc.} + \sin(n-1)^2 k\omega = U$$

which the paper gives for all values of k, and without the restriction that n be prime. It is shown that

$$T = \pm\sqrt{n}, \quad T = \pm\sqrt{n}, \quad T = 0, \quad T = 0$$

and

$$U = \pm\sqrt{n}, \quad U = 0, \quad U = 0, \quad U = \pm\sqrt{n}$$

according as n has the forms $4m, 4m+1, 4m+2, 4m+3$, respectively. Here again the sign of the radical depends on k. Its determination requires many individual cases to be distinguished, and is developed and proved by two different routes in such a way that nothing will remain to be desired. Comparing these two routes also leads to the following very remarkable theorem: Let n be the product of any number of distinct odd primes a, b, c, d, and so on, of which altogether μ have the form $4m+3$. Suppose further that among those factors there are altogether ν for each of which the product of the others (respectively $\frac{n}{a}, \frac{n}{b}, \frac{n}{c}, \frac{n}{d}$, and so on) is a quadratic nonresidue. Then ν will be even whenever μ has the form $4m$ or $4m+1$, but odd whenever μ has the form $4m+2$ or $4m+3$. The known fundamental theorem concerning quadratic residues is only a special case of this theorem; conversely, the theorem just stated is easily derived from that fundamental theorem. Thus these investigations also provide a fourth proof of this important theorem, which the author first proved by two entirely different routes in the *Disquisitionibus Arithmeticis*, and recently by a third, equally different route in a separate paper.

Göttingische gelehrte Anzeigen. 1817 March 10.

On 10 February Court Councillor Gauss submitted a lecture to the Royal Society, entitled:

Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae.

A distinctive feature of higher arithmetic is that so many of its most beautiful theorems can be discovered with the greatest ease by examining examples, while their proofs are far from readily apparent. Often they are found only after many unsuccessful attempts, through deeply probing investigations and fortunate combinations. This remarkable phenomenon arises from the often wonderful interconnection between the different branches of this part of mathematics. For the same reason, theorems for which a proof was initially sought in vain for years can often later be proved in several entirely different ways. Once a new theorem has been discovered through examples, finding *some* proof must of course be the first requirement; but after this has succeeded, in higher arithmetic we must not always regard the investigation as finished and the search for other proofs as a needless luxury. For one thing, we do not usually find the most beautiful and simplest proofs first; for another, insight into the wonderful interconnection of the truth of higher arithmetic is precisely one of the chief attractions of this study, and not infrequently leads in turn to the discovery of new truths. For these reasons, finding new proofs of truths already known must here often be considered at least as important as discovering the truth itself. These reflections are familiar to those who know higher arithmetic: much of Euler's contribution to it is known to consist in finding proofs of theorems which Fermat had already discovered, apparently through examples.

The theory of quadratic residues provides a clear illustration of these remarks. It rests chiefly on the so-called fundamental theorem, which states that the mutual relations of two (odd positive) primes to one another (insofar as one is a quadratic residue or nonresidue of the other) are the same whenever one or both primes have the form $4k + 1$, but opposite whenever both primes have the form $4k + 3$. For readers less familiar with higher arithmetic, we recall that an integer is called a quadratic residue of another if adding a multiple of the latter to the former can give a square; it is called a nonresidue if this is impossible. We do not intend to repeat the whole history of this beautiful theorem, so easily discovered through examples. We merely observe that the author of the present paper, after investigations initially pursued in vain for quite some time, has already given, one after another, four

entirely different proofs. Two are contained in the *Disquisitionibus Arithmeticis*; the third is the subject of a separate paper in the sixteenth volume of the Commentationes; and the fourth is interwoven with the paper *summatio quarumdam serierum singularium* in the first volume of the *Commentationes recentiores*. For these two papers readers may consult our reviews of 1808, May 12 and September 19, which also give fuller historical references. That the author did not stop at these four proofs, although each leaves nothing to be desired as regards rigour, needs no justification among the friends of higher arithmetic. Still, he would probably not have worked so eagerly to add further proofs if a particular circumstance had not prompted him to do so, and this must be mentioned here. In the year 1805 he began to study the theories of cubic and biquadratic residues, which are much richer and more interesting still than the theory of quadratic residues. These investigations revealed the same phenomena as the latter theory, only, as it were, on a larger scale. As soon as the right path was taken, examining examples immediately yielded a number of extremely simple theorems which exhaust those theories, bear a surprising resemblance to the theorems for quadratic residues, and in particular also provide a counterpart to the fundamental theorem. But the difficulty of finding entirely satisfactory proofs of these theorems proved greater still, and only after many attempts, continued over a considerable number of years, did the author finally reach his goal. The close analogy between the theorems for quadratic and higher residues suggested that there must also be analogous proofs for the two. Yet the methods of proof first found for quadratic residues could not be applied to the higher residues at all; this was precisely what led him to keep seeking further new proofs for the former. The author therefore wishes the present paper, which opens up some further resources for the theory of quadratic residues, to be regarded as a precursor to the theory of cubic and biquadratic residues. He intends to publish that theory in the future; its subjects are among the most difficult in higher arithmetic.

The present paper consists of three independent parts. It contains the fifth and sixth proofs of the fundamental theorem, and a new method, connected with the third proof, · for deciding whether a given integer is a quadratic residue or nonresidue of a given prime. Of the first four proofs, the third was unquestionably the one that combined the greatest simplicity with independence from investigations of a different kind; LEGENDRE therefore also included it in the new edition of his *Essai d'une théorie des nombres*. The *fifth* proof seems at least to equal the third in both respects. The two proofs are related insofar as they start from the same theorem, but in their subsequent development they are completely different from one another.

The theorem is as follows. Let m be a (positive odd) prime and M an integer not divisible by m. If, among the remainders obtained by dividing the products

$$M,\ 2M,\ 3M,\ 4M \ldots\ldots \tfrac{1}{2}(m-1)M$$

by m, the number of those greater than $\frac{1}{2}m$ is denoted by n, then M is a quadratic residue or nonresidue of m according as n is even or odd. To obtain a proof of the fundamental theorem, it is now assumed that M, too, is an odd positive prime, and that N has the same meaning with respect to M and m as n has with respect to m and M. Thus whether N is even or odd determines whether m is a quadratic residue or nonresidue of M. By a very short chain of arguments the author shows that the number of all positive integers which are less than $\frac{1}{2}mM$ and at the same time on division by m leave a remainder less than $\frac{1}{2}m$, and on division by M a remainder less than $\frac{1}{2}M$,

$$= \tfrac{1}{8}(m-1)(M-1) + \tfrac{1}{2}n + \tfrac{1}{2}N$$

and consequently that

$$\tfrac{1}{4}(m-1)(M-1) + n + N$$

is always an even number. Thus, whenever at least one of the numbers m, M has the form $4k+1$, so that $\frac{1}{4}(m-1)(M-1)$ is even, $n+N$ will also be even; hence n and N are either both even or both odd. If, on the other hand, both m and M have the form $4k+3$, then $n+N$ must be odd, so one of the numbers n, N is even and the other odd. Together with the theorem above, this gives the fundamental theorem at once.

The *sixth* proof is as short and elegant as the fifth, but rests on somewhat more intricate combinations. The limited space of these pages allows us only to touch on its main point, omitting the details. Let the following symbols denote:

p, q two (distinct positive odd) primes,

α a so-called *primitive root* for the modulus p, that is, an integer not divisible by p (here taken positive), such that no power lower than α^{p-1} is congruent to one modulo p

x an indeterminate quantity

ξ the function

$$x - x^{\alpha} + x^{\zeta} - x^{\eta} + x^{\theta} - \text{etc.} - x^{\lambda}$$

where, for convenience in printing, $\zeta, \eta, \theta \ldots \lambda$ stand for the numbers $\alpha\alpha, \alpha^3, \alpha^4 \ldots \alpha^{p-2}$;

ε one, taken positively if p has the form $4k+1$, negatively if p has the form $4k+3$;

δ one, taken positively if at least one of the numbers p, q has the form $4k+1$, negatively if both have the form $4k+3$;

γ one, taken positively if q is a quadratic residue of p, negatively if q is a quadratic nonresidue of p;

β one, taken positively if p is a quadratic residue of q, negatively if p is a quadratic nonresidue of q.

With these preparations it follows readily from Article 51 of the *Disquisitiones Arithmeticae* that the function

$$\xi^q - x^q + x^{q\alpha} - x^{q\zeta} + x^{q\eta} - x^{q\theta} + \text{etc.} + x^{q\lambda}$$

has, when expanded, coefficients all divisible by q. Hence, if this function is set $= qX$, then X is a *polynomial* whose coefficients, too, are integers. By arguments which it would take too much space to discuss here, the paper proves that dividing the function $qX\xi$ by $x^{p-1}+x^{p-2}+x^{p-3}+x^{p-4}+\text{etc.}+x+1$ leaves the remainder

$$\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$$

and therefore that dividing the function $X\xi$ by the same divisor leaves the remainder

$$\frac{\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)}{q}$$

This quantity must therefore be an integer. Since $\delta\delta = 1$, it follows readily that

$$p^{\frac{1}{2}(q-1)} - \gamma\delta$$

must be divisible by q. A known theorem also gives that $p^{\frac{1}{2}(q-1)} - \beta$ is divisible by q, so necessarily $\beta = \gamma\delta$, from which the fundamental theorem again follows at once.

The fundamental theorem, together with some known theorems, can indeed provide a fairly short way of deciding whether a given positive integer is a quadratic residue or nonresidue of a given prime, as the paper shows in detail. But further reflection on the third proof of the fundamental theorem led the author to a much more flexible solution. This forms the paper's third part; here we give only its final rule, omitting the reasoning behind it for brevity. To decide whether the positive integer b, not divisible by the prime a, is a quadratic residue or nonresidue of that prime, form, in just the same way as when finding the greatest common divisor of a and b, the equations

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \varepsilon e + f \text{ etc.} \end{aligned}$$

until the sequence of numbers a, b, c, d, e, f and so on reaches .the unit. Let. the numbers $\frac{1}{2}a, \frac{1}{2}b, \frac{1}{2}c, \frac{1}{2}d$ and so on, with their fractional part $\frac{1}{2}$ discarded whenever any of the numbers a, b, c, d and so on is odd, be denoted by a', b', c', d' and so on. Let μ be the number of occurrences of two odd numbers immediately following one another in the sequence a', b', c', d' and so on. Finally, let ν be the number of odd numbers in the sequence $\beta, \gamma, \delta, \varepsilon$ and so on to which, in the sequence b', c', d', e' and so on, a number of the form $4k + 1$ or $4k + 2$ respectively corresponds. Then b is a quadratic residue or nonresidue of a according as $\mu + \nu$ is even or odd, except in the single case where b is even and a has the form $8k + 3$ or $8k + 5$. In that case the rule is reversed: an even $\mu + \nu$ indicates that b is a quadratic nonresidue of a, while an odd $\mu + \nu$ indicates that b is a quadratic residue of a.

.Göttingische gelehrta Anzeigen. 1825 April 11.

On 5 April Court Councillor Gauss presented a lecture to the Royal Society, entitled:

Theoria Residuorum Biquadraticorum, Commentatio prima.

The theory of quadratic residues is known to form one of the most interesting parts of higher arithmetic. After repeated investigations it can now be regarded as complete and closed. Accounts of its history can be found in these pages for 1808 May 12 and September 19, and 1817 March 10. The last of these also gave some preliminary information about the investigations which the author of the present paper had been pursuing since the year 1805 into the related theory of cubic and biquadratic residues, equally fruitful and interesting but far more difficult. Although he already possessed the essential elements of this theory at that time, other work has so far prevented him from publishing anything about it. Only now has he been able to begin writing up part of these investigations. He has begun with the theory of biquadratic residues, which is more closely related to the theory of quadratic residues than is that of cubic residues. The present paper, however, is by no means intended to exhaust this exceptionally rich subject. The development of the *general* theory, which requires a quite distinctive extension of the domain of higher arithmetic, is reserved for a future continuation. This first paper contains those investigations which could be set out completely without such an extension. Only some of the results can be selected for this review.

An integer a is called a biquadratic residue of the integer p if there are numbers of the form $x^4 - a$ divisible by p; a biquadratic nonresidue if no numbers of that form can be divisible by p. Clearly all biquadratic residues of p are also quadratic residues of the same number, and hence all quadratic nonresidues are also biquadratic nonresidues. But not all quadratic residues are also biquadratic residues. It suffices to restrict the investigations to the case where p is a prime of the form $4n + 1$ and a is not divisible by p, since all other cases can easily be reduced to this one.

The investigations of this subject divide into two parts, according as p or a is regarded as given. The first is much less difficult than the second and, compared with it, is to be regarded as entirely elementary. The paper contains a complete account of everything essential to be said about it.

From the second part, by contrast, only a few special cases are treated here. These could be dealt with without too much preparation and can serve as preliminaries to the general theory to be given in the future. They are the cases where $a = -1$ and $a = \pm 2$ are set.

The first presents no difficulty at all: the *Disquisitiones Arithmeticae* had already shown that -1 is a biquadratic residue of p whenever p has the form $8n+1$, but only a quadratic residue and a biquadratic nonresidue of p when p has the form $8n+5$. The case $a = \pm 2$ is quite different. It has long been known that $+2$ and -2 are quadratic, and therefore also biquadratic, nonresidues of p when p has the form $8n+5$, and at least quadratic residues when p has the form $8n+1$. It is also known that for this form of p, $+2$ and -2 are either both biquadratic residues or both biquadratic nonresidues: but deciding which of these two cases occurs is an investigation of a much higher order. The paper develops two different criteria for this purpose.

The first criterion is connected with the decomposition of the number p into one square plus twice another, which, as is known (since, as already remarked, p is assumed to be prime), is always possible and possible in only one way. If we set $p = gg + 2hh$, then ± 2 is a biquadratic residue of p when g has the form $8n+1$ or $8n+7$, but a biquadratic nonresidue when g has the form $8n+3$ or $8n+5$.

The second criterion is connected with the decomposition of the number p into two squares, which is also known to be always possible and possible in only one way. If we set $p = ee + ff$ and suppose that ee denotes the odd square and ff the even square, then the assumed form $p = 8n+1$ already implies that $\frac{1}{2}f$, too, is even. Thus f has either the form $8m$ or the form $8m+4$: in the first case ± 2 is a biquadratic residue, in the other a biquadratic nonresidue of p.

We only touch here on an observation for which higher arithmetic so often provides an occasion: it is not so much the beauty and simplicity of the theorems themselves as the difficulty of proving them that makes them especially remarkable. Once there is reason to suspect a connection between the behaviour of the number ± 2 and the two decompositions of the number p just described, it is extremely easy to discover that connection by examining examples. But even for the first criterion its proof is not quite easy; for the second it lies much deeper, closely bound up with other subtle auxiliary investigations, which in turn lead to a remarkable extension of the theory of circle division. It is chiefly this wonderful interconnection of truths. that, as has often been observed, gives higher arithmetic such a distinctive appeal. Naturally these proofs themselves cannot be excerpted here; readers must consult the paper itself. But a couple of other new arithmetical theorems, also closely connected with the proof of the second criterion, deserve to be singled out here because of their simplicity.

Let p be a prime of the form $4k+1$, and put this number $= ee + ff$ so that ee denotes the odd square and ff the even square. If we further set

$$1 \,.\, 2 \,.\, 3 \ldots\ldots \; k = q$$

$$(k+1)(k+2)(k+3) \ldots\ldots 2k = r$$

then $\pm e$ is always the least remainder obtained by dividing $\frac{r}{2q}$ by p, and $\pm f$ the least remainder obtained by dividing $\frac{1}{2}rr$ by p (where the least remainder is always understood to be taken between the bounds $-\frac{1}{2}p$ and $+\frac{1}{2}p$). The number $\frac{r}{2q}$, whose value for $p = 5$ is 1, can for larger values of p also be put in the following form:

$$\frac{6 \,.\, 10 \,.\, 14 \,.\, 18 \ldots\ldots (p-3)}{2 \,.\, 3 \,.\, 4 \,.\, 5 \ldots\ldots k}$$

It is very remarkable that the decomposition of the number p into two squares can thus be obtained quite directly. But an accompanying circumstance is almost more remarkable still. This procedure always gives the root of the odd square, e, with a positive sign if e, taken positively, has the form $4m+1$, and with a negative sign if e, taken positively, has the form $4m+3$. By contrast, no general rule whatever has yet been found for the sign with which the root of the even square, f, emerges from this operation, either a priori or by examining examples. At the end of the paper the author therefore recommends this subject to the friends of higher arithmetic for further investigation, convinced that success would also open up a fruitful source of new extensions of this beautiful part of mathematics.

Göttingische gelehrte Anzeigen. 1831, April 23.

A paper presented to the Royal Society on April 15 by Court Councillor Gauss:

Theoria residuorum biquadraticorum, commentatio secunda,

continues the paper already printed in the sixth volume of the *Commentationes novae*, which was also reviewed in these pages at the time, in 1825, on April 11. Even this continuation, although more than twice as long as the first paper, does not yet exhaust this exceptionally rich subject, and completion of the whole will remain reserved for a future third paper.

Although the basic concepts of these theories and the contents of the first paper may be assumed known to everyone who has made higher arithmetic a subject of study, we nevertheless wish to recall those concepts briefly here for the convenience of readers interested in this part of mathematics who do not have the first paper immediately to hand. With respect to any integer p, another integer k is called a biquadratic residue if there are numbers of the form $x^4 - k$ that are divisible by p; in the opposite case it is called a biquadratic nonresidue of p. It is sufficient here to restrict attention to the case where p is a prime of the form $4n + 1$, and k is not divisible by that prime, since all other cases are either clear in themselves or can be reduced to this one.

For such a *given* value of p, all numbers not divisible by p fall into *four* classes. One contains the biquadratic residues, a second contains those biquadratic nonresidues that are quadratic residues of p, and the biquadratic nonresidues that are also quadratic nonresidues are divided between the remaining two. The principle of this division is that either $k^n - 1$, or $k^n + 1$, or $k^n - f$, or $k^n + f$ will always be divisible by p, where f denotes an integer that makes $ff + 1$ divisible by p. Anyone familiar with the elementary terminology will see how these verbal definitions can be expressed in it.

The theory of this classification is completed in the first paper, both for the immediately evident case $k = -1$ and for the cases $k = \pm 2$, which require subtle auxiliary investigations. The beginning of the present paper now proceeds to larger values of k. At first, however, only values that are themselves primes need be considered, and the outcome shows that the results take their simplest form when the values are taken positively or negatively according as their absolute values have the form $4m + 1$ or $4m + 3$. Examining examples immediately yields a rich harvest of new theorems with great ease; we give only a few of them here. The numbering of the classes as $1, 2, 3, 4$ refers to the cases where k^n is congruent to $1, f, -1, -f$, respectively. At the same

time, the value always chosen for f is the one that makes $a + bf$ divisible by p, where $aa + bb$ represents the decomposition of p into an odd and an even square. Thus examining examples shows that -3 always belongs to class $1, 2, 3, 4$ according as $b, a + b, a, a - b$, respectively, is divisible by 3; that $+5$ belongs to these classes in order according as $b, a - b, a, a + b$, respectively, is divisible by 5; and that -7 falls into class 1 when a or b; into class 2 when $a - 2b$ or $a - 3b$; into class 3 when $a - b$ or $a + b$; and into class 4 when $a + 2b$ or $a + 3b$ is divisible by 7, divisibility being the condition in each of these cases. Similar theorems result for $-11, +13, +17, -19, -23$, and so on. Yet, easy as it is to discover all such particular theorems by examining examples, it seems difficult to find a general law for these forms by that route, even though some common features soon become apparent; and finding proofs of these theorems is much more difficult still. The methods used for $+2$ and -2 in the first paper no longer apply here. Although other methods might also settle what concerns the first and third classes, they prove inadequate for establishing *complete* proofs.

One therefore soon recognizes that this rich region of higher arithmetic can be entered only by entirely new routes. In the first paper, the author had already indicated that a particular extension of the whole field of higher arithmetic was essential for this purpose, without then explaining more closely what it consisted in. The present paper is intended to bring this subject to light.

This consists in nothing other than the following: to give the theory of biquadratic residues its true foundation, the field of higher arithmetic, which had otherwise been extended only to the real integers, must also be extended to the imaginary ones, and these must be granted entirely equal rights of citizenship with the former. Once this is understood, that theory appears in an entirely new light, and its results acquire a most surprising simplicity.

Before the theory of biquadratic residues itself can be developed in this extended domain of numbers, however, the preceding parts of higher arithmetic, which have so far been treated only in relation to real numbers, must share in this extension. We can mention only a few of these preliminary investigations here. The author calls a quantity $a + bi$, where a and b denote real quantities and i is written for $\sqrt{-1}$ for brevity, a complex integer when a and b are both integers. Complex quantities thus do not stand opposed to real ones: they include them as the special case where $b = 0$. For convenient use, several concepts relating to complex quantities needed particular names, but we shall try to avoid those names in this review.

Just as the arithmetic of real numbers speaks of only two units, the positive and the negative, so in the arithmetic of complex numbers we have four units, $+1$, -1, $+i$, $-i$. A complex integer is called *composite* if it is the product of two integer factors that are not units; a complex number that does not

admit *such* a factorization is called a complex prime. For example, the real number 3 is prime even when considered as a complex number, whereas 5 is composite as a complex number $= (1 + 2i)(1 - 2i)$. Just as in the higher arithmetic of real numbers, primes play a principal role in this extended field of the science.

If a complex integer $a + bi$ is taken as modulus, one can give $aa + bb$ pairwise incongruent complex numbers, and no more, to one of which any given complex integer must be congruent; these can be called a complete system of incongruent residues. The so-called least and absolutely least residues in the arithmetic of real numbers have their exact counterparts here as well. For example, for the modulus $1+2i$, the complete system of absolutely least residues consists of 0, 1, i, -1 and $-i$. Almost all the investigations in the first four sections of the *Disquisitiones Arithmeticae* also have their place, with some modifications, in the extended arithmetic. The celebrated theorem of FERMAT, for example, takes the following form here: if $a + bi$ is a complex prime, and k a complex number not divisible by it, then always $k^{aa+bb-1} \equiv 1$ for the modulus $a + bi$. Especially remarkable, however, is that the Fundamental Theorem for quadratic residues has its exact counterpart in the arithmetic of complex numbers, in an even simpler form: if $a + bi$, $A + Bi$ are complex primes, with a and A odd, b and B even, then the first is a quadratic residue of the second if the second is a quadratic residue of the first, whereas the first is a quadratic nonresidue of the second if the second is a quadratic nonresidue of the first.

After these preliminary investigations, the paper turns to the theory of biquadratic residues itself. In place of the mere distinction between biquadratic residues and nonresidues, it first establishes a division of the numbers not divisible by the modulus into four classes. If the modulus is a complex prime $a + bi$, with a always assumed odd and b even, and p written for $aa + bb$ for brevity, and if k is a complex number not divisible by $a + bi$, then $k^{\frac{1}{4}(p-1)}$ will always be congruent to one of $+1, +i, -1, -i$. This establishes a division of all numbers not divisible by $a + bi$ into four classes, to which the biquadratic characters $0, 1, 2, 3$ are assigned in order. Clearly, character 0 refers to the biquadratic residues, the others to the biquadratic nonresidues, with character 2 also corresponding to quadratic $\cdot$ residues, and characters 1 and 3 to quadratic nonresidues.

It is easy to see that the main task is to determine this character only for values of k that are themselves complex primes, and here examining examples immediately leads to exceedingly simple results.

If first $k = 1 + i$, the character of this number is always found to be $\equiv \frac{1}{8}(-aa + 2ab - 3bb + 1) (\text{mod. } 4)$, and similar expressions are found for the cases $k = 1 - i$, $k = -1 + i$, $k = -1 - i$.

If, on the other hand, $k = \alpha + \beta i$ is a prime with α odd and β even, examining examples very easily yields a law of reciprocity entirely analogous to the Fundamental Theorem for quadratic residues. It can be expressed most simply as follows:

If both $\alpha + \beta - 1$ and $a + b - 1$ are divisible by 4 (all other cases can easily be reduced to this one), and the character of $\alpha + \beta i$ with respect to the modulus $a + bi$ is denoted by λ, whereas the character of $a + bi$ with respect to the modulus $\alpha + \beta i$ is denoted by l, then $\lambda = l$ if one of β, b (or both) is divisible by 4. whereas $\lambda = l \pm 2$ if neither of β, b is divisible by 4.

These theorems contain essentially everything of substance in the theory of biquadratic residues. Yet, easy as it was to discover them by examining examples, it is difficult to give rigorous proofs of them, especially of the second, the Fundamental Theorem of biquadratic residues. Because of the great length the present paper has already reached, the author was compelled to leave the presentation of the proof of the latter theorem, which he has possessed for 20 years, for a future third paper. The present paper does, however, give the complete proof of the former theorem concerning $1 + i$ (on which the other theorems for $1 - i$, $-1 + i$, $-1 - i$ depend), and this can already give some idea of the subject's complexity.

We still have a few general remarks to add. Moving the theory of biquadratic residues into the domain of complex numbers might seem objectionable and unnatural to someone less familiar with the nature of imaginary quantities and caught up in false ideas about them. It might suggest that the investigation is thereby left, as it were, hanging in the air, becomes unstable, and moves entirely beyond intuitive understanding. Nothing could be less well founded than such an opinion. On the contrary, the arithmetic of complex numbers admits the clearest visual representation. Although the author has followed a purely arithmetical treatment in this presentation, he has also given the necessary indications for this visual representation, which makes understanding more vivid and is therefore highly to be recommended. these will suffice for readers who think for themselves. Just as absolute integers are represented by a row of equally spaced points on a straight line, in which the starting point represents 0, the next point 1, and so on; and just as representing negative numbers then requires only an unbounded extension of this row on the opposite side of the starting point: so representing complex integers requires only the addition that this row be regarded as lying in a fixed unbounded plane, and that an unlimited number of similar rows be taken parallel to it on both sides, at equal distances from one another. In place of a row of points, we then have a system of points that can be arranged as rows of rows in two ways, and that serves to divide the whole plane into equal squares. The point nearest 0 in the first adjacent row on one side of the row representing the real numbers then corresponds to i, just as the point

nearest 0 in the first adjacent row on the other side corresponds to $-i$, and so on. With this representation, the execution of arithmetical operations on complex quantities, congruence, the formation of a complete system of incongruent numbers for a given modulus, and so on, admit a visual representation that leaves nothing to be desired.

On the other hand, this places the true metaphysics of imaginary quantities in a new, bright light.

Our general arithmetic, whose scope far surpasses the geometry of the ancients, is entirely a creation of modern times. Starting originally from the concept of absolute integers, it has extended its domain step by step: fractions were added to integers, irrational numbers to rational numbers, negative numbers to positive numbers, imaginary numbers to real numbers. Yet each advance was initially made with timid, hesitant steps. The first algebraists still called the negative roots of equations false roots, and they are indeed such when the problem to which they relate is presented in a form where the nature of the quantity sought admits no opposite. But just as there is no hesitation about including fractions in *general* arithmetic, although there are so many countable things for which a fraction has no meaning, so negative numbers could not be denied equal rights with positive ones in that arithmetic because countless things admit no opposite: the reality of negative numbers is sufficiently justified, since they find an adequate substrate in countless other cases. All this has, of course, long been understood. But imaginary quantities, set against real ones—formerly. and here and there even now, though inappropriately, called *impossible*—are still more tolerated than naturalized as citizens. They thus appear more like a play of signs empty of content in itself, to which any conceivable substrate is unconditionally denied, without anyone wishing to spurn the rich tribute this play of signs ultimately contributes to the treasury of relations among real quantities.

For many years the author has viewed this highly important part of mathematics from a different standpoint, from which imaginary quantities can be given an object just as well as negative ones. Until now, however, there has been no occasion to state it explicitly in public, although attentive readers will readily find traces of it in the paper on equations published in 1799 and in the prize essay on the transformation of surfaces. The present paper briefly indicates its main features, which are as follows.

Positive and negative numbers can have an application only where what is counted has an opposite that, conceived as combined with it, is equivalent to cancellation. Strictly considered, this condition holds only where what is counted consists of relations between pairs of objects, rather than substances (objects conceivable in themselves). It is postulated that these objects are arranged in a row in a definite way, for example $A, B, C, D \ldots$, and that the relation of A to B can be regarded as equal to the relation of B to C, and so

on. Here the concept of opposition requires nothing more than *interchanging* the members of the relation, so that if the relation (or transition) from A to B counts as $+1$, the relation from B to A must be represented by -1. Thus, insofar as such a row is unbounded on both sides, every real integer represents the relation of a member chosen arbitrarily as starting point to a definite member of the row.

But if the objects are of a kind that cannot be arranged in a single row, even an unbounded one, and can only be arranged in rows of rows, or, equivalently, form a manifold of two dimensions; and if the relations of one row to another, or the transitions from one to another, behave similarly to the earlier transitions from one member of a row to another member of the same row, then measuring the transition from one member of the system to another clearly requires, besides the former units $+1$ and -1, two further units $+i$ and $-i$, likewise opposite to one another. But it must also be postulated that the unit i always denotes the transition from a given member of a row to a *definite* member of the immediately adjacent row. In this way the system can therefore be arranged as rows of rows in two ways.

The mathematician abstracts entirely from the nature of the objects and the content of their relations; the sole concern is to count the relations and compare them with one another. In this respect, just as the relations denoted by $+1$ and -1, considered in themselves, are taken to be of the same kind, the mathematician is entitled to extend this to all four elements $+1$, -1, $+i$ and $-i$.

These relations can be brought within intuition only by a representation in space. The simplest case is where there is no reason to arrange the symbols of the objects in any way other than a square pattern: an unbounded plane is divided into squares by two systems of parallel lines crossing at right angles, and the intersections are chosen as the symbols. Each such point A has four neighbours. If the relation of A to one neighbouring point is denoted by $+1$, the relation to be denoted by -1 is thereby determined, whereas either of the other two may be chosen for $+i$, or the point corresponding to $+i$ may be taken at will to the *right* or to the *left*. Once forward and backward *in* the plane, and above and below with respect to its two sides, have been fixed (at will), this distinction between right and left is entirely determined *in itself*, although we can communicate our intuition of this distinction to others *only* by pointing to actually existing material things[*)]. Even after we have decided the latter point, however, we see that it depended on our arbitrary choice which of the two rows crossing at a point we wished to regard as the

[*)] KANT has already made both observations, but one cannot understand how this perceptive philosopher could believe he found in the first a proof of his opinion that space is *only* the form of our outer intuition, since the second so clearly proves the opposite, and that space must have a real meaning independent of our mode of intuition.

principal row, and which direction in it as corresponding to positive numbers. We also see that if we wish to take the relation previously treated as $+i$ for $+1$, we must necessarily take the relation previously denoted by -1 for $+i$. In mathematical language, this says that $+i$ is a mean proportional between $+1$ and -1, or corresponds to the sign $\sqrt{-1}$: we deliberately do not say *the* mean proportional, for $-i$ clearly has an equal claim. The possibility of giving $\sqrt{-1}$ an intuitive meaning is thus fully justified here, and nothing more is required to admit this quantity into the domain of the objects of arithmetic.

We believed that this brief presentation of the main points of a new theory of so-called imaginary quantities would serve readers interested in mathematics. If this subject has hitherto been viewed from a mistaken standpoint and mysterious obscurity has been found in it, this is largely attributable to the unsuitable names. Had $+1$, -1, $\sqrt{-1}$ been called direct, inverse and lateral units, for example, instead of positive, negative and imaginary (or even impossible) units, such obscurity could scarcely have been spoken of. The author has reserved a fuller treatment of the subject, which is really touched on only incidentally in the present paper, for the future. The question why relations among things that form a manifold of more than two dimensions cannot yield further kinds of quantities admissible in general arithmetic will then also receive its answer.

REVIEWS

OF OTHER AUTHORS'

WRITINGS.

Göttingische gelehrte Anzeigen. 1809, March 11.

Recherches sur l'irréductibilité Arithmétique et Géométrique des nombres et de leurs puissances. 1808. (No place of publication. 25 pages in large quarto.)

A work whose aim is to represent irrational radical quantities in the form of rational quantities. We must content ourselves with having drawn the attention of readers interested in mathematics to this little work, since the limits of these pages do not allow us to give a fuller account and examination here of the author's distinctive standpoint and treatment of radical quantities, which departs entirely from the usual one.

Göttingische Gelehrte Anzeigen. 1812, March 23.

Cribrum Arithmeticum, sive tabula continens numeros primos a compositis segregatos, occurrentes in serie numerorum ab unitate progredientium usque ad decies centena milia et ultra haec ad viginti millia (1020000). *Numeris compositis, per* 2, 3, 5 *non dividuis, adscripti sunt divisores simplices, non minimi tantum, sed omnino omnes. Confecit* Ladislaus Chernac, *Pannonius, A. L. M. Philos. et Medic. Doctor, in almo lyceo Daventriensi philosophiae professor. Daventriae* 1811. (At the author's expense, printed by J. H. Lange. XXII and 1022 pages, large quarto.)

The full title of this important and highly meritorious work already sufficiently indicates its contents: it is a table of all the prime factors of all numbers not divisible by 2, 3 and 5, from 1 to 1020000, calculated through several years of work as careful as it was laborious, and printed neatly and, as far as we have found by occasional checks, very correctly. Anyone who frequently carries out calculations with larger numbers can readily judge the value of such a gift to arithmetic. The author deserves double thanks: both for the exceedingly laborious work itself, by which he has placed his name beside the unforgettable names of Rhaeticus, Pitiscus, Brigg, Vlacq, Wolfram, Taylor and others, and for the certainly very considerable expense incurred in printing it, for which a publisher would otherwise scarcely have been found. Such tables have often been calculated before, though mostly on a smaller scale, but have either remained entirely in manuscript or have not been completely printed. As is well known, Lambert formerly did all he could to encourage the continuation of Pell's often reprinted table, which extends to 100000. According to a report by Bernoulli in Lambert's correspondence,

Oberreit had extended it to 500000, and a copy had come into Schulze's hands. Anton Felkel, as reported in the Monatl. Correspondenz, volume 2, page 223, had completed it in manuscript up to two million and intended later to provide it up to 2460000; but what had already been printed in Vienna at public expense was used for cartridges in the Turkish war because no buyers could be found! Thus many years of meritorious work were lost to the public: all the more, therefore, we considered it our duty to announce the publication of the present work here. The first million is now available for everyone's use; anyone with the opportunity and enthusiasm for this subject may therefore direct their efforts to what follows.

Göttingische gelehrte Anzeigen. 1814, November 3.

Tables des diviseurs pour tous les nombres du deuxième million, ou plus exactement depuis 1020000 *à* 2028000, *avec les nombres premiers qui s'y trouvent. Par* J. Ch. Burckhardt, *membre de l'institut impérial, du bureau des longitudes de France, et de plusieurs autres sociétés savantes. Paris*, 1814. *Mme Ve Courcier.* (VIII. and 112 pages in folio.)

Sooner than we would have dared to hope when reviewing Chernac's factor table covering the first million, we can already report the completion and publication of a similar table for the second million. Through this laborious work the distinguished author, whose name itself guarantees the greatest care and accuracy, has placed all those interested in arithmetic deeply in his debt. Chernac's table for the first million gives all the prime factors; Burckhardt's for the second, however, gives only the least divisor in each case. The complete factorization of a number in the second million therefore requires division by the least divisor and looking up the quotient in Chernac's table. But this small effort is of no significance compared with the great advantage of having the table occupy so much less space, while the prospect remains of seeing it extended in time to ten million. The author made it possible to fit the table into this small volume partly by restricting it to the least divisor and partly by printing it as economically as possible. If a stands for any of the eighty numbers below 300 that are not divisible by 2, 3 and 5, then every number not divisible by 2, 3 and 5 is included in the form $300n + a$. All eighty numbers for which n has the same value are found in a single vertical column, and each page contains thirty such columns. Thus each page includes, out of nine thousand numbers proceeding in their natural order, all those not divisible by 2, 3 or 5.

The method by which Mr. BURCKHARDT constructed his table deserves special mention here. He had a grid engraved on copper, in which 81 horizontal and 78 vertical lines formed a rectangle divided into 80×77, that is, 6160 small squares, and had the necessary number of impressions made from it. At the side, the eighty values of a could also be engraved immediately; the values of $300n$, in continuous order, were written with a pen above the 77 vertical columns. Thus each sheet represents all the numbers not divisible by 2, 3 and 5 found among each set of 23100 numbers proceeding in their natural order, and 44 sheets suffice to cover a whole million. It is easy to see that the numbers whose least divisor is 7 or 11 recur in the same order on every following sheet. These divisors could therefore be engraved directly on the copperplate and consequently appeared automatically in their proper places on every sheet. To enter the following divisors, for example 13, Mr. B. took only 13 columns across the width of a spare sheet and, treating it as the beginning of his table, cut out all the squares that had to contain the divisor 13. He therefore needed only to lay this stencil over the first thirteen columns of the first sheet, then over the next thirteen, and so on, to see at once all the places that had to be filled, insofar as they did not already contain 7 or 11, with 13. The same procedure was then used for the divisor 17, and so on. The spare sheets sufficed in this way up to the divisor 73; for the larger divisors 79, 83, and so on, Mr. B. appears to have assembled the frame from two or more pieces. For divisors exceeding 500, however, Mr. B. preferred to find the multiples by addition, needing to take only primes for the other factor. We find this whole procedure highly suitable, and would recommend it for imitation to anyone inclined to extend the table further. For the third and fourth millions, the author himself has meanwhile already carried out a large part of the calculations, so we have good reason to hope to see these too made available in print soon.

Göttingische gelehrte Anzeigen. 1816, November 7.

Tables des diviseurs pour tous les nombres du troisième million, ou plus exactement, depuis 2028000 *à* 3036000, *avec les nombres premiers qui s'y trouvent; par* J. Chr. Burckhardt, *membre de l'académie royale des sciences, du bureau des longitudes de France et de plusieurs autres sociétés savantes. Paris* 1816. *Mme Ve Courcier.* (112 pages in folio.)

Since in our review of the table of factors for the second million we have already described in detail both the method of calculation used by the distinguished author and the arrangement of the table itself, we can here content ourselves with announcing the publication of the table for the third million. Shortly we may also expect from the author the table for the *first* million, presented in the same way, so that the whole table extending beyond three million will then occupy only a moderately sized volume. For this the author deserves the thanks of all those interested in arithmetic, who see this laborious work meeting a need on a scale far exceeding anything one could have dared to hope for only a few years ago.

Göttingische gelehrte Anzeigen. 1817, August 9.

Tables des diviseurs, pour tous les nombres du premier million, ou plus exactement depuis 1 *à* 1020000, *avec les nombres premiers qui s'y trouvent; par* J. Chr. Burckhardt, *membre de l'académie des sciences dans l'institut royal, du bureau des longitudes de France, et de plusieurs autres sociétés savantes. Paris* 1817. *Mme Ve Courcier.* (114 pages in folio.)

Referring here to our reviews of the tables for the second and third millions, we now merely announce the actual · publication of these factor tables for the first million. We thus now possess a connected whole for the first three millions. For the present first million, the author used partly Chernac's *Cribrum Arithmeticum* and partly a manuscript table by Schenmark held by the library of the Royal Institute. The latter had not, however, been constructed with quite all the care one could wish for, and deciding which was right in cases where the two disagreed was often rather laborious. Only a very small number of errors were found in Chernac's table, which Mr. Burckhardt has reported here.

The author also already has most of the materials ready for the fourth, fifth and sixth millions, and offers to supply this continuation if the publisher is encouraged by sufficient sales of the first three millions. It would indeed be very regrettable if the fruits of such laborious and useful work were withheld from the world.

Göttingische gelehrte Anzeigen. December 19, 1825.

A short paper has been presented to the Royal Society on behalf of Mr. Erchinger of Thuningen in the Kingdom of Würtemberg, on the

Geometric Construction of the Regular Seventeen-sided Polygon.

As is well known, the general theory of regular polygons has acquired a new form and a wider scope through its close connection with higher arithmetic. The theory of those polygons that can be constructed geometrically is one part of it, though a comparatively small one. Since the time of the Greeks it had been known that the triangle, pentagon, fifteen-sided polygon and all polygons obtained from these by doubling or repeatedly doubling the number of sides have this property, and it was believed, and sometimes expressly asserted, that these were the only ones. Higher arithmetic has shown this to be an error: by laying open the true sources of the entirely general theory, it revealed of itself that, besides the polygons mentioned, there are countless others that can be constructed geometrically, of which the seventeen-sided polygon is the simplest. This shows in the clearest light the superiority of analysis, which encompasses the most general and the particular with equal ease, over geometry, which must always remain with the particular, is held back by ever greater complications as it advances from simpler cases to more complex ones, and would hardly ever have reached, without help from elsewhere, that next case after the known ones. Nevertheless, it remains important, interesting and desirable that purely geometric treatments should also continue to be cultivated, and that geometry should take possession of at least part of the new fields conquered by analysis. The reviewer knows of no one who has so far publicly treated the construction of the seventeen-sided polygon except Mr. Pauker, in the writings of the Courland Society and in his geometry. Mr. Erchinger's construction differs from this and is carried out more in the purely geometric spirit. It is as follows. (Anyone can draw the accompanying figure: a straight line on which the points $DBGAIFCE$ lie in that order.) Take any straight line AB and extend it backwards and forwards to C and D, so that $AC \times BC = AD \times BD = 4AB \times AB$; next determine the points E, G on the two sides of the extended line CA, so that $AE \times EC = AG \times CG = AB \times AB$, and the point F on the A side of the extended line BA, so that $AF \times DF = AB \times AB$; finally divide AE at I, so that $AI \times EI = AB \times AF$, where AI is the smaller and EI the larger part of AE. Then construct a triangle in which two sides are each $= AB$, and the third $= AI$. If a circle is drawn around this triangle, AI will be the side of the regular seventeen-sided polygon inscribed in that circle.

If one checks the correctness of this construction by comparing it with the theory of the seventeen-sided polygon given as an example in Article 354 of the *Disquisitiones Arithmeticae*, one readily sees that it is simply the geometric translation of the equations to which the application of the general theory leads. Indeed, the distances of the points C, D, E, F, G, I from A are precisely the quantities denoted there by (8 . 1), (8 . 3), (4 . 1), (4 . 3), (4 . 9), (2 . 1), if positive and negative signs are expressed by position, and the distance of the point B from A, taken in the same sense, is set $= -1$. But the real merit of Mr. ERCHINGER's paper lies less in setting out the construction itself, since analysis had already marked out the simplest path, than in giving a purely geometric proof of its correctness. This is carried out with such exemplary, painstaking care to avoid everything that is not purely elementary that it does the author credit, and prompts the wish that his indeed uncommon mathematical talent may receive every encouragement.

Göttingische gelehrte Anzeigen. July 9, 1831.

Investigations into the Properties of Positive Ternary Quadratic Forms, by Ludwig August Seeber, *Doctor of Philosophy, Full Professor of Physics at the University in Freiburg. Freiburg im Breisgau* 1831. (248 pages in 4.)

Functions of two indeterminate quantities x and y of the form $axx+2bxy+cyy$, where a, b, c denote specified integers, are known as *quadratic forms*, or, when a further distinction is needed, *binary quadratic forms*. They form one of the most interesting and richest subjects of higher arithmetic. The problems that arise first are these: to decide whether a given form of this kind contains another, $a'x'x' + 2b'x'y' + c'y'y'$, that is, whether it can be transformed into that form by a substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, in which $\alpha, \beta, \gamma, \delta$ are integers; whether such a relation between two forms is mutual, in which case the forms are called equivalent; further, in both cases, to give all possible transformations of one into the other; and finally, to find all possible representations of a given integer by a given form with integer values of the indeterminate quantities. These problems are completely solved in the *Disquisitiones Arithmeticae*, but constitute by far the smaller part of that work's section on quadratic forms. The finer investigations that follow require in part a preliminary treatment of a field one level higher and presenting much greater difficulties: the theory of similar functions of three indeterminate quantities x, y, z, which therefore have the form $axx + byy + czz+2a'yz+2b'xz+2c'xy$ and are called ternary quadratic forms. The solution of the principal problems concerning these ternary forms is developed in the work mentioned, though only as far as was necessary for the stated purpose. After an interval of thirty years, the author of the present work has now been the first to take up these investigations again and, for one principal kind of ternary form, namely the positive forms, has brought to completion what was left unfinished in the *Disquisitiones Arithmeticae*. For those who have studied higher arithmetic more deeply, we could describe in a few words what is newly achieved in the present work. But to be understood by others too, we must allow ourselves somewhat more detail, and we do this all the more willingly because these investigations have an interest of their own outside higher arithmetic as well.

The properties of a binary form $axx + 2bxy + cyy$ depend chiefly on the number $bb - ac$, which is therefore called the determinant of that form. Two equivalent forms always have equal determinants. But not all forms having a given determinant are therefore equivalent. Rather, such forms fall into a smaller or larger, but always finite, number of classes, with the forms belonging to one class equivalent to one another, and those belonging to different classes not equivalent. Forms whose determinant is positive can represent

positive and negative numbers alike; forms with a negative determinant, however, can represent only numbers having the same sign as a and c, so that positive and negative forms are distinguished here. The simplest forms in each class have definite criteria, are called reduced forms, and can be regarded as representatives of the whole class.

Similar relations concerning ternary forms are established in the *Disquisitiones Arithmeticae*. The determinant of the ternary form

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

is the number

$$aa'a' + bb'b' + cc'c' - abc - 2a'b'c'$$

Here too, equality of determinants is necessary for two forms to be equivalent, but is not sufficient. Rather, all forms with a specified determinant fall into a finite number of classes, in each of which the simplest forms may be called reduced and may, as it were, represent all the others. The distinction between positive and negative forms, however, behaves differently here than for binary forms. For every given determinant, whether positive or negative, there are some forms that can represent positive and negative numbers alike (indifferent forms), and others that can represent either only positive or only negative numbers (positive or negative forms). But positive forms exist only for negative determinants, and negative forms only for positive ones. It is evident, moreover, that a form's character as indifferent, positive or negative belongs at the same time to the whole class to which it belongs. The present work is confined to positive forms, whose determinants must therefore be negative. Everything that holds for these evidently transfers of itself to negative forms, whereas the indifferent forms, entirely excluded from the work, require a quite different treatment.

As already mentioned, the theory of ternary forms in the *Disquisitiones Arithmeticae* was developed only as far as was needed for its purpose there. Consequently, the problem of deciding whether two given ternary forms are equivalent had not yet been solved in full generality. It was indeed shown there how to find, for any given form, an equivalent form of the simplest kind, and that there can be only finitely many such reduced forms for any given determinant. But since each class contains several such reduced forms, which do not in all cases turn out *immediately* to be equivalent, a criterion was still lacking by which their equivalence or non-equivalence could be determined with certainty. The author of the present work has now met this need for positive forms completely and with exemplary thoroughness. His procedure is, however, presented somewhat differently from the account we have just given, and from how the matter would stand if the concept of reduced positive forms included only the essential conditions of greatest simplicity. For positive

forms, these conditions are that the numbers a, b, c, which are positive by their nature, must be no smaller than, respectively, b' or c', a' or c', and a' or b', without regard to signs. Mr. SEEBER has added further qualifications to the concept of reduced forms such that each class can contain only one form of this kind, and must contain one. In view of a beautiful theorem found by Mr. SEEBER from observed cases, to be mentioned further below, we give here the principal conditions that Mr. S. has incorporated into the concept of reduced forms: 1) among the numbers a', b', c', no two may have opposite signs; 2) without regard to sign, $2b'$ and $2c'$ must be no greater than a, further a and $2a'$ no greater than b, and b no greater than c; 3) when a', b', c' are all negative, twice the sum of these numbers must be no greater than $a + b$. We may omit here the remaining qualifications that must be added for certain special cases.

The principal content of the work consists first in solving the problem of finding, for any given positive form, an equivalent form having the character of a reduced form according to the established definition; and then in the rigorous proof of the theorem that two non-identical reduced forms cannot be equivalent, or, what is the same thing, that each class contains only one reduced form. We must do full justice to the spirit of thoroughness with which these matters are carried through. And although we must regret the very great length of treatment involved, perhaps discouraging to some, since the solution of the problem takes 41 pages and the proof of the theorem 91 pages, we would by no means have this taken as a criticism. When a difficult problem or theorem is to be solved or proved, the first step, always to be acknowledged with due thanks, is that a solution or proof should be found at all. The question whether this could have been done more easily and simply remains idle so long as the possibility is not at the same time established by actually doing it. We therefore consider it premature to dwell on this question here. — The remainder of the work chiefly contains equally thorough solutions of the following problems: to decide whether a given form contains another given form not equivalent to it; to find all possible transformations of a given form into a given equivalent form or one merely contained in it; and finally, for a given determinant, to give all possible classes of positive ternary forms.

We must also note that Mr. SEEBER has expressed ternary forms somewhat differently from the *Disquisitiones Arithmeticae*, where the coefficients of the products yz, xz, xy were deliberately assumed to be even integers, whereas Mr. S. also allows odd ones, and therefore denotes by a', b', c' what was denoted above by $2a'$, $2b'$, $2c'$. The greater generality obtained in this way is evidently only apparent, or at least unnecessary, since everything that can be said about such forms with odd coefficients also follows of itself if their doubles are considered instead. We therefore cannot approve this change,

which also entails some loss of simplicity. One consequence has been that what Mr. SEEBER calls the determinant is always four times the number bearing that name in the *Disquisitiones Arithmeticae*. In the present review we have retained the terminology of the *Disquisitiones Arithmeticae*.

For the last-mentioned problem (to give all possible reduced forms for each given determinant), Mr. SEEBER used a theorem to obtain bounds for the first three coefficients. According to this theorem, their product abc cannot exceed three times the determinant. Mr. SEEBER rigorously proves this theorem. In the preface, however, he remarks that among more than 600 cases he examined, he found not a single one in which that product exceeded twice the determinant. He therefore considers it highly probable that this tighter bound holds universally, but says that he did not succeed in finding a rigorous proof. Since this theorem, found by Mr. SEEBER from observed cases, is both remarkable in itself and important for shortening the solution of the stated problem, we wish to add a very simple proof here, so that we too may contribute in this review to the further development of the theory. Two cases must be distinguished.

I. If none of the numbers a', b', c' is negative, put

$$\begin{aligned} b - 2a' &= d, \quad c - 2b' = e, \quad a - 2c' = f \\ c - 2a' &= g, \quad a - 2b' = h, \quad b - 2c' = i \end{aligned}$$

The definition of reduced positive forms immediately implies that if

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

is such a form, none of those six numbers is negative; it is also evident that a, b, c are positive. If we now denote the form's (negative) determinant by $-D$, we have the identity, readily checked by expansion,

$$2D - abc = aa'd + bb'e + cc'f + a'hi + b'gi + c'gh + ghi$$

in which none of the seven terms on the right can be negative, and consequently abc is no greater than $2D$. The same conclusion follows in the same way from the identity

$$2D - abc = aa'g + bb'h + cc'i + a'ef + b'df + c'de + def$$

II. If none of the numbers a', b', c' is positive, put

$$\begin{aligned} b + 2a' &= d, \quad c + 2b' = e, \quad a + 2c' = f \\ c + 2a' &= g, \quad a + 2b' = h, \quad b + 2c' = i \end{aligned}$$

$$\begin{aligned} b + c + 2a' + 2b' + 2c' &= k \\ a + c + 2a' + 2b' + 2c' &= l \\ a + b + 2a' + 2b' + 2c' &= m \end{aligned}$$

and take the determinant of the form, as before, $= -D$. By the definition of reduced positive forms, none of the nine numbers $d, e, f, g, h, i, k, l, m$ can be negative. Thus the identity

$$\begin{aligned} 6D - 3abc = & - aa'(d + 2k) - bb'(e + 2l) - cc'(f + 2m) \\ & - a'hi - b'gi - c'gh + def + 2ghi \end{aligned}$$

in which all terms on the right are positive or zero, since a', b', c' are not positive but negative or zero, shows that $3abc$ cannot exceed $6D$, or abc exceed $2D$. The same conclusion follows likewise from the identity

$$\begin{aligned} 6D - 3abc = & - aa'(g + 2k) - bb'(h + 2l) - cc'(i + 2m) \\ & - a'ef - b'df - c'de + 2def + ghi \end{aligned}$$

Both equations are symmetric. If full symmetry is given up, the proof can be carried out with an even smaller number of terms, for example by the identity

$$\begin{aligned} 8D - 4abc = & - 2aa'(g + k) - 2bb'(e + l) - 4cc'm \\ & + (c + e)df + (c + g)hi \end{aligned}$$

We now wish to add a few remarks on the meaning of positive binary and ternary quadratic forms outside higher arithmetic. It is unnecessary to treat negative forms separately, while indifferent forms lie wholly outside this treatment.

The positive binary form $axx+2bxy+cyy$ represents, in general, the square of the distance between two unspecified points in a plane whose coordinates, relative to two axes inclined to one another at an angle with cosine $= \frac{b}{\sqrt{ac}}$, differ by $x\sqrt{a}$, $y\sqrt{c}$. If x and y are to mean only *integers*, the form therefore refers to a system of points arranged in parallelograms, lying at the intersections of two systems of parallel lines. The lines in each system are equally spaced: the spacings in one, measured parallel to the lines in the second, are $= \sqrt{a}$, and the spacings in the other, measured parallel to the lines in the first, $= \sqrt{c}$; the inclination of the two systems is the one given above. The plane thus appears divided entirely into equal parallelograms whose vertices

make up the system of points, with none of these points lying inside a parallelogram. The determinant taken with positive sign, thus $ac - bb$, is the square of the area of an elementary parallelogram. One and the same system of such points can be divided into parallelograms in infinitely many different ways and thus referred to equally many different forms. All these different forms are, however, what is technically called equivalent, and the area of an elementary parallelogram always remains the same. Two forms that are not equivalent, but of which one contains the other, refer to the same system of points: the first form to the whole system, the second to a part. Two forms that are technically called improperly equivalent (improprie aequivalentes) refer to two equal but oppositely placed systems of points, the plane being thought of as turned over, and so on.

In the same way, the positive ternary form

$$axx + byy + czz + 2a'yz + 2b'xz + 2c'xy$$

represents, in general, the square of the distance between two unspecified points in space whose coordinates relative to three axes (1), (2), (3) give the differences $x\sqrt{a}$, $y\sqrt{b}$, $z\sqrt{c}$: the cosines of the angles between axes (2) and (3), (1) and (3), and (1) and (2) are respectively $\frac{a'}{\sqrt{bc}}$, $\frac{b'}{\sqrt{ac}}$, $\frac{c'}{\sqrt{ab}}$. If x, y, z are to mean only integers, the form refers to a system of points arranged in parallelepipeds, that is, points arising as the intersections of three systems of parallel, equally spaced planes. The whole space thus appears divided into equal parallelepipeds whose vertices make up that system of points, and the square of the volume of an elementary parallelepiped equals the determinant of the ternary form taken with positive sign·. Equivalent forms represent one and the same system of points, referred only to other axes or fundamental planes. In the same way, all the other principal aspects of the theory of ternary forms find their geometric meaning here: one form being contained in another; the representation of a specified number or an indeterminate binary form by a ternary form; the theory of the adjoint ternary forms (formae adiunctae); the disappearance of the distinction between proper and improper equivalence; the nature of reduced forms; and so on. We must, however, confine ourselves to the indications above, especially since the present work, which considers ternary forms solely from a purely arithmetic standpoint, has given only indirect occasion for them. One will at least see from this what a rich field is opened here to investigations that have great theoretical interest in themselves and can also be used for a treatment of all relations among crystal forms that is both convenient and general. This is not the place to enter into the details of this application. We must nevertheless observe that, although a, b, c, a', b', c' were originally assumed to denote integers, the greater part of the theory of ternary forms, and in particular what is required for that application, remains valid independently of this assumption. Indeed, HAÜY's

specifications lead, for most kinds of crystal, to very simple integer values of the coefficients in the ternary forms referring to the corresponding arrangement of the system of points. But the more accurate later measurements of Wollaston, Malus, Biot, Kupffer and others contradict this and make it doubtful whether rational ratios of those coefficients agree with nature in every case. In any case, however, if one does not wish to drop from the theory the restriction to integer values of the coefficients, integers can always be found that come as close as one wishes to the results of measurement, since what matters here is their ratios to one another, rather than their absolute values.

Finally, we wish to give the geometric meaning of Seeber's theorem mentioned above. If a parallelepiped is such that none of its twelve edges (of which four at a time are equal) is greater than any of the twelve face diagonals (which are equal in pairs) or any of the four diagonals of the parallelepiped, then its volume multiplied by $\sqrt{2}$ is no smaller than the volume of a rectangular parallelepiped formed from the same edges.

MANUSCRIPT

PAPERS.

SOLUTION OF THE CONGRUENCE $X^m - 1 \equiv 0$.
ANALYSIS OF RESIDUES. CHAPTER SIX. FIRST PART.

237.

In Chapter III we showed that the congruence $x^n \equiv 1$, when a prime number p is taken as modulus, has μ roots, where μ is the greatest common divisor of the numbers n and $p-1$, and that these roots agree exactly with the roots of the congruence $x^\mu \equiv 1$. It therefore suffices to consider the case in which n is a divisor of $p-1$. That the solution not only of the congruence $x^n - 1 \equiv 0$ but of any other congruence for arbitrary moduli can be derived from its solution for prime moduli has already been shown at various places and will be developed more fully below (Chapter VIII).

238.

But there is no need to stop even here. In the same Chapter III we explained that the solution of the congruence $x^n \equiv 1$ depends on the solution of similar congruences $x^a \equiv 1$, $x^b \equiv 1$, and so on, where a, b, and so on, are primes or powers of primes, and n is the product of these numbers. Namely, if A, B, and so on, are respectively any roots of the congruences $x^a \equiv 1$, $x^b \equiv 1$, and so on, their product $AB\ldots$ will be one of the roots of the congruence $x^n \equiv 1$. Our investigations will therefore be confined to solving the congruence $x^n \equiv 1 \pmod{p}$, where p is a prime, and n a prime or a power of a prime and also a divisor of $p-1$.

239.

Furthermore, Chapter III shows that among the roots of the congruence $x^n \equiv 1$ there are always some whose powers can represent all the others. Thus, if r denotes a root of this kind (we called it *primitive* above when $n = p-1$, and shall retain this expression here, though in a broader sense), all the roots of the proposed congruence will be

$$1,\ r,\ rr,\ r^3 \quad \ldots\ldots \quad r^{n-1}$$

We must therefore direct every effort towards finding roots of this kind, since once they have been found the others will become evident of themselves. For brevity we denote any power of r by its exponent enclosed in parentheses, so that (0) denotes unity, (1) any primitive root of the congruence $x^n \equiv 1$, (2) the square of (1), and so on. Thus the sequence (0), (1), (2), (3), $\ldots$ $(n-1)$ includes all the roots. It is also known that (k) will always be such a primitive root whenever k is coprime to n; that is, in our case, where n is a power of the prime t, $= t^\nu$, whenever t does not divide k. The symbols (1), (2), and so

on, are evidently undetermined in themselves; but as soon as a definite value is assigned to (1), all the others become determined.

240.

Since our aim is to investigate primitive roots before the others, we must first separate them from the rest. This is done by removing from the sequence $(0), (1), (2) \ldots (n-1)$ all terms (k) for which k is divisible by t. If n is prime, or $\nu = 1$, only (0) is to be removed. Before proceeding to investigate the remaining roots, however, we earnestly advise the reader to work out several examples, so as to see concretely everything that might otherwise seem too general. We give one example; but this will not make it unnecessary to work out others independently.

Let $p = 29$; $n = 7$. The seven roots of the congruence $x^7 \equiv 1 \pmod{29}$ will be $1, 7, 16, 20, 23, 24, 25$. Since n is prime, all these roots except 1 will be primitive. Thus, if $7 = (1)$, the symbols will have the following meanings:

(0)	(1)	(2)	(3)	(4)	(5)	(6)
1	7	20	24	23	16	25

Everyone will also remember that the symbols (n) and (0), $(n+1)$ and (1), and so on, and in general (a) and (b), are equivalent whenever $a \equiv b \pmod{n}$.

241.

For our purpose, however, we must proceed in yet another way. We retain only those terms (k) for which k is not divisible by t, whose number is $\frac{t-1}{t}.n = \lambda$. All these numbers, or numbers congruent to them modulo n, can be represented by successive powers of some number. Let this be $= \rho$; then all the primitive roots of the congruence $x^n \equiv 1$ will be denoted as follows:

$$(1) \quad (\rho) \quad (\rho^2) \quad (\rho^3) \quad \ldots. \quad (\rho^{\lambda-1})$$

By this device we completely exclude all nonprimitive roots; the reasons and advantages will become clearer below. In our example we may therefore put $\rho = 3$, and the primitive roots of the congruence $x^7 \equiv 1$ are arranged as follows:

	(1)	(3)	(3^2)	(3^3)	(3^4)	(3^5)
or	(1)	(3)	(2)	(6)	(4)	(5)
which are	7	24	20	25	23	16

242.

To let the reader know the aim of the following investigations, it will be useful to state the theorem that we propose to prove and clarify.

If the number λ, which is $= t^{\nu-1}.t-1$, has prime factors a, b, c, d, and so on, and $\lambda = a^\alpha b^\beta c^\gamma \ldots$, the solution of the congruence $x^n - 1 \equiv 0$ depends on solving $\alpha + \beta + ..$ congruences of lower degree, of which α have degree a, β degree b, γ degree c, and so on.

Thus, in our example, solving the congruence $x^7 \equiv 1$ depends on a congruence of degree two and another of degree three; and it is apparent in general that the degrees of these congruences never depend on the modulus p. To reach the proof of this theorem, however, we must first give some propositions concerning the connection between congruences and their roots, although these investigations properly belong to Chapter eight, where they are to be pursued further.

243.

THEOREM. *Suppose the congruence*

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots. + N \equiv 0 \text{ (prime modulus)}$$

is such that, when the product of the m factors $x-r$, $x-r'$, $x-r''$, $x-r'''\ldots$ is expanded to give $x^m + ax^{m-1} + bx^{m-2} \ldots + n$, we have $A \equiv a$, $B \equiv b$, $C \equiv c$, and so on, modulo p. Then the quantities $r, r', r'' \ldots$ will be roots of the proposed congruence, and it will have no others.

Proof. I. We always have

$$\begin{aligned} x^m + Ax^{m-1} + Bx^{m-2} + \ldots \\ \equiv x^m + ax^{m-1} + bx^{m-2} + \ldots \pmod{p} \end{aligned}$$

But the latter side of the congruence becomes $= 0$ on setting $x = r$, $x = r'$, $x = r''$, and so on; therefore, for these values of x, the former side becomes $\equiv 0 \pmod{p}$. This proves the first part.

II. If another value ρ, congruent to none of r, r', and so on, also satisfied the proposed congruence, we would have

$$\begin{aligned} 0 &\equiv \rho^m + A\rho^{m-1} + B\rho^{m-2} + \ldots \\ &\equiv \rho^m + a\rho^{m-1} + b\rho^{m-2} + \ldots \\ &\equiv (\rho - r)(\rho - r')(\rho - r'')(\rho - r''')\ldots \end{aligned}$$

But since none of the factors $\rho - r$, $\rho - r'$, $\rho - r''$, and so on, is $\equiv 0$, their product being $\equiv 0$ is impossible, because p is prime. There are therefore no roots besides r, r', and so on. This proves the second part.

244.

PROBLEM. *Let $r, r', r'' \ldots$ be unknown quantities, whose number is $= m$, whose sum is $= \alpha$, sum of squares $= \beta$, sum of cubes $= \gamma \ldots$, and sum of powers with exponent m is $= \mu$. Suppose that these numbers, also $= m$ in number, are not themselves given, but instead other numbers α', β', γ', and so on, congruent to them individually modulo p, where this is a prime and $> m$. Find a congruence of degree m whose roots are r, r', r'', and so on.*

Solution. Regard r, r', r'', and so on, as the roots of an equation

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \ldots = 0$$

and determine its coefficients A, B, C, and so on, by the known method, using congruence in place of equality; namely, put

$$\begin{aligned} -A &\equiv \alpha' \\ -2B &\equiv \beta' + A\alpha' \\ -3C &\equiv \gamma' + A\beta' + B\alpha' \\ -4D &\equiv \delta' + A\gamma' + B\beta' + C\alpha' \\ &\text{etc.} \\ -mN &\equiv \mu' + A\lambda' + \text{etc.} \end{aligned}$$

These coefficients cannot be undetermined, since all the numbers $1, 2, 3 \ldots m < p$. I say that the congruence

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots + N \equiv 0$$

is the one required.

Proof. Let the equation whose roots are r, r', r'', r''', and so on, be

$$x^m + ax^{m-1} + bx^{m-2} + \ldots = 0$$

Then

$$\begin{aligned} -a &= \alpha \\ -2b &= \beta + a\alpha \\ -3c &= \gamma + a\beta + b\alpha \\ -4d &= \delta + a\gamma + b\beta + c\alpha \\ &\text{etc.} \end{aligned}$$

It will be evident to everyone from this that

$$a \equiv A, \quad b \equiv B, \quad c \equiv C \text{ etc. } (\text{mod. } p)$$

so, by the preceding section, the numbers r, r', r'', and so on, which are roots of the *equation*

$$x^m + ax^{m-1} + bx^{m-2} + \ldots = 0$$

will also be roots of the *congruence*

$$x^m + Ax^{m-1} + Bx^{m-2} + \ldots \equiv 0 \qquad \text{Q. E. D.}$$

We leave the construction of examples to the readers.

245.

We return to our purpose. Retaining the symbols used in sections 242 and earlier, we undertake to show that, if λ is the product of any factors efg, and so on, the primitive roots of the congruence $x^n \equiv 1$, whose number is λ, can be divided into e classes in such a way that the sums of the roots assigned to each class are given by a congruence of degree e. Once these are taken as known, each class can be subdivided into f groups so that the sum of each group is given by a congruence of degree f. These groups can be subdivided again, and so on, until the individual roots are reached.

246.

Definition. We shall call the collection of *all* terms contained in a form $(\rho^{ke+\alpha})$ of this kind (section 241) a *complete period*, or simply a *period*. Here e denotes any divisor of λ; α any given number; and k all integers from 0 to $\frac{\lambda}{e} - 1$. For brevity we denote such a period by $(e * \alpha)$. Thus, in our example, the terms

	$(1), (2), (4)$	form the periods	$(2 * 0)$,
	$(3), (6), (5)$		$(2 * 1)$
and	$(1), (6)$	form these	$(3 * 0)$
	$(3), (4)$		$(3 * 1)$
	$(2), (5)$		$(3 * 2)$

Now, if all terms are distributed into periods in any way, and each period is again divided into smaller periods, and so on, we say that what we promised in the preceding section is achieved.

Before entering into this exposition itself, however, we shall show that, although the formation of such a period depends on the two somewhat arbitrary quantities r, ρ, it contains nothing indeterminate: however these quantities are chosen, the same terms always come together in the same period, provided that the number of terms the period is to contain has been prescribed.

The criterion that two terms A, B belong to the same period is that each is contained in a form $(\rho^{ke+\alpha})$ of this kind, or that $A \equiv r^{\rho^{ke+\alpha}}$, $B \equiv r^{\rho^{k'e+\alpha}} \pmod{p}$. Here r is a primitive root of the congruence $x^n \equiv 1 \pmod{p}$, and ρ a primitive root of the congruence $x^\lambda \equiv 1 \pmod{n}$; see above.

We must show that, if, in place of the numbers r, ρ, other numbers, say s, σ, are chosen, then A and B are contained in similar forms $s^{\sigma^{le+\beta}}$, $s^{\sigma^{l'e+\beta}}$.

Let $s^m \equiv r \pmod{p}$; $\sigma^\mu \equiv \rho \pmod{n}$ and $m \equiv \sigma^\zeta \pmod{n}$, which is possible because r, ρ are primitive roots. Moreover, m will be coprime to n, and μ to λ (Chapter III). By the appropriate substitutions we obtain

$$A \equiv s^{\sigma^{\mu ke+\mu\alpha+\zeta}}, \qquad B = s^{\sigma^{\mu k'e+\mu\alpha+\zeta}} \qquad \text{Q. E. D.}$$

247.

THEOREM. *The product of two similar periods can be formed, independently of the number p, by adding similar periods and given numbers.*

(We call periods similar when they contain equally many terms, or when the number e is the same.)

Example. Let $n = 7$. The product of the periods $(1)+(6)$ and $(2)+(5)$ is, because $(a)\times(b) = (a+b)$, $(3)+(6)+(8)+(11)$, or it consists of the periods $(3)+(4)$ and $(1)+(6)$.

Proof. Let $\frac{\lambda}{e} = f$, and let the given periods be $(e*\alpha)$ and $(e*\beta)$, or the sums

$$(\rho^\alpha)+(\rho^{\alpha+e})+(\rho^{\alpha+2e})+\ldots+(\rho^{\alpha+(f-1)e}) \;\ldots\ldots\; P$$
$$(\rho^\beta)+(\rho^{\beta+e})+(\rho^{\beta+2e})+\ldots+(\rho^{\beta+(f-1)e}) \;\ldots\ldots\; Q$$

The product PQ consists of f^2 terms. Arrange them as follows. Form f rows, each consisting of f terms. Let the first contain the product of P with (ρ^β), the second the product $P\,.\,(\rho^{\beta+e})$, and so on, and so on. In the first row let the product arising from the term (ρ^α) occupy the first place, that from $(\rho^{\alpha+e})$ the second, and the others follow in succession. In the second row assign the first place to the product arising from $(\rho^{\alpha+e})$, the second to that from $(\rho^{\alpha+2e})$, and so on, and finally the last place to that from (ρ^α). Let the third begin with the product arising from $(\rho^{\alpha+2e})$, and continue in this way, following the product from the last term with the products from the first and second terms, and so on, and so on. Thus, denoting the successive terms of the period P by $1, 2, 3 \ldots z$ and those of the period Q by $\mathrm{I}, \mathrm{II}, \mathrm{III}, \ldots . Z$, arrange the terms of PQ as

$$1\,.\,\mathrm{I}+2\,.\,\mathrm{I}+3\,.\,\mathrm{I}+4\,.\,\mathrm{I}+\ldots+z\,.\,\mathrm{I}$$
$$2\,.\,\mathrm{II}+3\,.\,\mathrm{II}+4\,.\,\mathrm{II}+\ldots.+1\,.\,\mathrm{II}$$
$$3\,.\,\mathrm{III}+4\,.\,\mathrm{III}+\ldots+1\,.\,\mathrm{III}+2\,.\,\mathrm{III}$$
$$\text{etc.} \quad \text{etc.}$$

Now collect all terms occupying the same place in the individual rows into f groups; and I say
1° if any term is $\equiv 1$, all the other terms in the same group will also be $\equiv 1$
2° every group in which no term is $\equiv 1$ forms a period. — Once these statements have been proved, we will evidently have achieved our purpose.

The general form of such a group is

$$(\rho^{\alpha+ke}+\rho^{\beta}),\quad (\rho^{\alpha+(k+1)e}+\rho^{\beta+e}),\quad (\rho^{\alpha+(k+2)e}+\rho^{\beta+2e}),$$
$$\dots\ (\rho^{\alpha+(k+f-1)e}+\rho^{\beta+(f-1)e})$$

Indeed, in place of $\rho^{\alpha+(k-1)e}$ one can also write $\rho^{\alpha+(k+f-1)e}$, since $ef = \lambda$ and $\rho^{\lambda} \equiv 1 \pmod{n}$, and similarly for the preceding terms. Put $\rho^{\alpha+ke}+\rho^{\beta} \equiv \rho^{\chi} \pmod{n}$, which is permissible unless $\rho^{\alpha+ke}+\rho^{\beta}$ happens to be divisible by n[*]. The group can then be represented as (ρ^{χ}), $(\rho^{\chi+e})$, $(\rho^{\chi+2e})\dots(\rho^{\chi+(f-1)e})$, which is evidently the period $(e*\chi)$. But if $\rho^{\alpha+ke}+\rho^{\beta}$ is divisible by n, all terms of the group will be $\equiv (0)$, that is, $\equiv 1$. Q. E. D.

Note. This proof also gives a very easy method of expanding the product. We shall give another below which lacks this advantage, but seems worthy of consideration for its simplicity.

248.

We call all the smaller periods that make up a larger period a system of periods. Thus this name will be given to the periods

$$(ef*\alpha),\quad (ef*f+\alpha),\quad (ef*2f+\alpha)\ \dots.\ (ef*(e-1)f+\alpha)$$

that make up the period $(f*\alpha)$. It will be *properly ordered* if the numbers placed after the sign $*$, here α, $f+\alpha$, $2f+\alpha$, follow an arithmetic progression with difference f. Finally, systems are *similar* if both their smaller and their larger periods are similar.

THEOREM. *If the periods of two similar, properly ordered systems are multiplied together, namely the first by the first, the second by the second, the third by the third, and so on, the sum of all the products can be formed from given numbers and periods similar to the larger period.*

Proof. Let the systems be

$$(ef*\alpha),\quad (ef*\alpha+f),\quad (ef*\alpha+2f)\dots$$
$$(ef*\beta),\quad (ef*\beta+f),\quad (ef*\beta+2f)\dots$$

The products of the individual periods of the first system with the corresponding periods of the second consist, by the preceding section, of integers

[*] The proposition will have to be expressed somewhat differently if n denotes a power of a prime in general; when it is a prime number, however, nothing needs changing.

and similar periods. A little attention to how these periods arise shows that, if $(ef*\alpha)\times(ef*\beta)$ consists of an integer N and periods $(ef*A)$, $(ef*B)$, $(ef*C)$, and so on, the products are then formed as follows:

$$\begin{aligned}&(ef*\alpha+f)\times(ef*\beta+f) \text{ from } N \text{ and periods}\\ &\qquad (ef*A+f),\quad (ef*B+f),\quad (ef*C+f) \text{ etc.}\\ &(ef*\alpha+2f)\times(ef*\beta+2f) \text{ from } N \text{ and periods}\\ &\qquad (ef*A+2f),\quad (ef*B+2f),\quad (ef*C+2f) \text{ etc.}\end{aligned}$$

and in general

$$\begin{aligned}&(ef*\alpha+\mu f)\times(ef*\beta+\mu f) \text{ from } N \text{ and periods}\\ &\qquad (ef*A+\mu f),\quad (ef*B+\mu f),\quad (ef*C+\mu f) \text{ etc.}\end{aligned}$$

It follows directly that the sum of all the periods will be

$$eN+(f*A)+(f*B)+(f*C) \text{ etc.} \qquad \text{Q. E. D.}$$

This proof also supplies a method for finding that sum.

249.

It is easy to make this theorem still more general. Namely, if there are any number of similar, properly ordered systems, and the products of all the first periods, all the second periods, and so on, are formed, the sum of all these products consists of numbers and larger periods. If all these systems are taken to be equal, the sum of powers of all the periods, whatever the exponent, will consist of numbers and periods similar to the larger one. The aim of these results is now apparent. Let $\lambda = efgh\ldots$. Divide all the primitive roots into e periods A, A', A'', and so on, each of these again into f: B, B', B'', and so on, and each of these into g: C, C', C'', and so on. The sum of all the periods is given: it is $\equiv -1$. But according to what we have just said, we shall also have

$$\begin{gathered}(A)^2+(A')^2+(A'')^2+(A''')^2+\text{etc.}\\ (A)^3+(A')^3+(A'')^3+(A''')^3+\text{etc.}\\ \text{etc. etc.}\end{gathered}$$

Hence, by section 244, a congruence of degree e can be found whose roots are A, A', A'', and so on. Taking these as known, let each period be divided into smaller ones:

$$\begin{array}{lllll} A & \text{into} & B, & B', & B''\ldots\\ A' & \text{into} & B^{(n)}, & B^{(n+1)}, & B^{(n+2)}\ldots\\ & \text{etc.} & & & \end{array}$$

Thus $B + B' + B'' + \ldots \equiv A$ is given. But

$$(B)^2 + (B')^2 + (B'')^2 + \ldots$$
$$(B)^3 + (B')^3 + (B'')^3 + \ldots$$
$$\text{etc.}$$

consists of units and the periods A, A', A'', and so on. Therefore B, B', B'', and so on, will be given by a congruence of degree f, from which they can be found; and similarly the periods making up A', A'', and so on, can be determined. Anyone will now see that every period can be subdivided into smaller ones by precisely the same method, until the roots themselves are reached.

250.

But a difficulty occurs in applying these rules, and we must remove it. Since each congruence has several roots, we must decide which label to assign to each, so that they can be properly distinguished from one another. The labels of the periods depend on the numbers r, ρ, which can be chosen at will, so their labelling must also involve something arbitrary. The number ρ must, however, be fixed at the outset. The main feature of our method is that we derive smaller periods from larger ones. But this cannot be done without the proper order of the periods, which we have obtained through their *labels*. We must therefore ensure that all periods are distinguished by their labels as soon as they have been found.

Let the period A be denoted by $(e * \alpha)$ and divided into f periods B, C, D, and so on, which must be labelled. Each is clearly contained in a form $(ef * ke + \alpha)$ of this kind. But I say that, for one of them, B, the number k can be chosen at will, and the placement of the others derived from it.

Let R be any primitive root of the congruence $x^n \equiv 1$, and let B consist of the terms $R^\mu + R^\nu + \text{etc.}$. Put $\frac{1}{\mu}\rho^{ke+\alpha} \equiv \frac{1}{\upsilon} \pmod{n}$, and, since the value of r is arbitrary, provided only that A receives the label $(e * \alpha)$, which evidently happens of itself, put $r \equiv R^\upsilon \pmod{p}$. Then the first term of B will be $r^{\rho^{ke+\alpha}}$, and B may be denoted by $(ef * ke + \alpha)$. If, in place of R^μ, we had considered the term R^ν, we would have obtained a different value of r. But it is readily seen that, for any root ρ, the root r can have $\frac{\lambda}{ef}$ different values.

251.

Let us now see how, once one period is labelled, the others are distinguished by their labels. For this purpose, however, we must seek another method of finding the remaining periods: insofar as they, like A itself, are roots of a congruence, no order is discernible among them. Suppose that A is denoted by $(ef*0)$. It follows from the preceding discussion that

$$\begin{aligned} A^2 &\text{ has the form } M + N(ef*0) + O(ef*1) + P(ef*2) + \dots \\ A^3 &\text{ has the form } M' + N'(ef*0) + O'(ef*1) + \dots \\ &\text{etc.} \\ A^{ef-1} &\text{ has the form } M^* + N^*(ef*0) + O^*(ef*1) + \dots \end{aligned}$$

To these is added the congruence

$$(ef*0) + (ef*1) + \dots + (ef*ef-1) \equiv -1$$

We thus have $cf - 1$ linear congruences and the same number of unknown quantities, which can therefore be determined by elimination.

Note. A case may occur in which the unknown quantities are given by expressions of the form $\frac{V}{Wp}$. We shall show below how this difficulty can be remedied. Since this case can occur only very rarely, we do not wish to dwell on it here.

252.

Let this suffice in general for solving pure congruences. Much more will be said about them at various places below; in particular, many things can be taken over from the solution of pure equations, which we shall not neglect to note in their proper places. We add another example: comparing it with the rules will make everything clearer to those with less experience.

Let $n = 31$, $p = 311$; that is, we seek the roots of the congruence $x^{31} - 1 \equiv 0 \pmod{311}$. We must first find a primitive root of the congruence $y^{30} - 1 \equiv \pmod{31}$, such as $y \equiv 3$. Thus put $\rho \equiv 3$, and first divide all the primitive roots of the proposed congruence into 5 periods, namely

$$\begin{array}{ll} (5*0) & \dots\dots \quad (1)+(26)+(25)+(30)+(5)+(6) \\ (5*1) & \dots\dots \quad (3)+(16)+(13)+(28)+(15)+(18) \\ (5*2) & \dots\dots \quad (9)+(17)+(8)+(22)+(14)+(23) \\ (5*3) & \dots\dots \quad (27)+(20)+(24)+(4)+(11)+(7) \\ (5*4) & \dots\dots \quad (19)+(29)+(10)+(12)+(2)+(21) \end{array}$$

The required calculations give the sum of the periods $\equiv -1$, of their squares $\equiv 25$, cubes $\equiv 26$, fourth powers $\equiv 249$, and fifth powers $\equiv 564$.

Thus the periods will be the roots of the congruence

$$x^5 + x^4 - 12x^3 - 21x^2 + x + 5 \equiv 0$$

Further, one finds

$$(5*0)^2 \equiv 6 + 2(5*0) + 2(5*3) + (5*4)$$
$$(5*0)^3 \equiv 12 + 15(5*0) + 4(5*1) + 3(5*2) + 6(5*3) + 6(5*4)$$
$$(5*0)^4 \equiv 90 + 60(5*0) + 28(5*1) + 26(5*2) + 49(5*3) + 38(5*4)$$

and hence, by elimination,

$$5(5*1) \equiv 3(5*0)^4 - (5*0)^3 - 33(5*0)^2 - 24(5*0) + 15$$
$$5(5*2) \equiv -2(5*0)^4 - (5*0)^3 + 22(5*0)^2 + 31(5*0)$$
$$5(5*3) \equiv (5*0)^4 - 2(5*0)^3$$
$$5(5*4) \equiv -2(5*0)^4 + 4(5*0)^3$$

One root of the congruence found above is $\equiv 17$. Thus, if $(5*0) \equiv 17$, then $(5*1) \equiv 183$, $(5*2) \equiv 263$, $(5*3) \equiv 91$, $(5*4) \equiv 67$.

Now divide each of the periods found into three again, namely

$(5*0)$	into $(15*0),\ (15*5),\ (15*10)$
	or into $(1)+(30),\ (26)+(5),\ (25)+(6)$
$(5*1)$	into $(15*1),\ (15*6),\ (15*11)$
	or into $(3)+(28),\ (16)+(15),\ (13)+(18)$
	etc. etc.

Suppose that the periods into which the following are divided are roots of the respective congruences:

$(5*0)$	are roots of	$x^3 + Ax^2 + Bx + C \equiv 0$
$(5*1)$		$x^3 + A'x^2 + B'x + C' \equiv 0$
$(5*2)$		$x^3 + A''x^2 + B''x + C'' \equiv 0$
	etc.	

Then

$A \equiv -(5*0),$	$B \equiv (5*0) + (5*3),$	$C \equiv -2 - (5*4)$
$A' \equiv -(5*1),$	$B' \equiv (5*1) + (5*4),$	$C' \equiv -2 - (5*0)$
etc.	etc.	etc.

Therefore

$(15*0),\ (15*5),\ (15*10)$	will be roots of congruences	$x^3 - 17x^2 + 108x - 60 \equiv 0$
$(15*1),\ (15*6),\ (15*11)$		
$(15*2),\ (15*7),\ (15*12)$		
$(15*3),\ (15*8),\ (15*13)$		
$(15*4),\ (15*9),\ (15*14)$		

Here, however, we have

$$(15*0)^3 - 3(15*0) \equiv (15*1)$$
$$(15*1)^3 - 3(15*1) \equiv (15*2)$$
$$\text{etc.}$$

Hence, if one of the roots of the first congruence, 10, is taken as $(15*0)$, we have

$$\begin{array}{llll} (15*0) \equiv & 10 & (15*5) \equiv & (15*10) \equiv \\ (15*1) \equiv & 37 & (15*6) \equiv & (15*11) \equiv \\ (15*2) \equiv & -151 & (15*7) \equiv & (15*12) \equiv \\ (15*3) \equiv & -39 & (15*8) \equiv & (15*13) \equiv \\ (15*4) \equiv & -112 & (15*9) \equiv & (15*14) \equiv \end{array}$$

Finally, take the terms making up each of these periods. Then

$$\begin{array}{lll} (1),\ (30) & \text{roots of congruences} & x^2 - (15*0)x + 1 \equiv 0 \\ (3),\ (28) & & x^2 - (15*1)x + 1 \equiv 0 \\ & \text{etc.} & \end{array}$$

The roots of the first congruence are 126 and 195, which will therefore be primitive roots of the congruence $x^{31} \equiv 1$, and from these the remaining roots can readily be derived.

GENERAL INVESTIGATIONS OF CONGRUENCES.

ANALYSIS OF RESIDUES, CHAPTER EIGHT.

330.

The results on congruences presented in the preceding sections concern only the simplest cases and were mostly obtained by particular methods. In this section we shall try to bring the theory of congruences under higher principles, as far as is yet possible, much as the theory of *equations* is usually treated. As we have observed several times, there is a remarkable analogy between the two. Since all algebraic congruences involving a single unknown can be reduced to the form

$$X \equiv 0$$

where X is an algebraic function of the unknown x involving no fractions, functions of this kind must be considered first.

331.

If P, Q are functions of the indeterminate x of the forms

$$A + Bx + Cxx + Dx^3 + \ldots$$
$$H + Ix + Kxx + Lx^3 + \ldots$$

(which we shall henceforth always mean when we simply say *functions*), and the coefficients of like powers of x in the two functions are congruent for any given modulus, the *functions will be called congruent for that modulus.* Congruent functions clearly take congruent values when equal or congruent values are substituted for the indeterminate. Most of what we proved about *numbers* in Chapters I and II also holds for functions. Thus, if $P \equiv P'$, $Q \equiv Q'$, $R \equiv R'$, and so on, we clearly have $P + Q + R$ etc. $\equiv P' + Q' + R' +$ etc.; $P - Q \equiv P' - Q'$; $PQ \equiv P'Q'$; PQR etc. $\equiv P'Q'R'$ etc. The proofs are very easy and can be given in the same way as in Chapter I.

If $PQ \equiv R$, we shall denote the function Q by $\frac{R}{P}$, with the modulus indicated, and say that Q is the quotient when R is divided by P for this modulus. All functions congruent to Q can clearly be taken in its place; we shall regard them all as a *single* value. Below, however, we shall show in which cases such a quotient can have several values, that is, incongruent ones.

332.

If the modulus is a prime number and the divisor Q contains just one term Hx^h whose coefficient H is not divisible by the modulus, that is, provided only that H is not $\equiv 0$, the quotient cannot have several values. For if $QA \equiv P$ and $QB \equiv P$, we would have $Q(A-B) \equiv 0$. Now let

$$Q \equiv .. + Hx^h + Ix^{h+1} + \text{etc.}$$

where H is not divisible by p, and

$$A - B \equiv Lx^l + Mx^{l+1} + \text{etc.}$$

where L is not divisible by p (the function $A-B$ will have this form because we assume that A is not $\equiv B$). We would then have $Q(A-B) \equiv HLx^{h+l} + \text{etc.} \equiv 0$, which is absurd, since HL is not $\equiv 0$.

Rules for dividing the function P by Q, when this is possible, are now easily given. Let

$$P \equiv ax^\alpha + bx^{\alpha+1} + cx^{\alpha+2} + \text{etc.} + kx^\kappa$$
$$Q \equiv mx^\mu + nx^{\mu+1} + qx^{\mu+2} + \text{etc.} + tx^\tau$$

where a, k, m, t are not divisible by the modulus. We must have α not $< \mu$, and κ not $< \tau$. Division can be carried out as in ordinary algebraic calculation, provided that an integer is always taken for the quotient; namely, the quotient will always have the form $\frac{r}{m}$, which must be determined for the modulus. Now, if a remainder is left after $\kappa + \mu - \alpha - \tau + 1$ terms have been found, it will have the form

$$Ax^{\kappa+\mu-\tau+1} + Bx^{\kappa+\mu-\tau+2} + .. + Cx^\kappa$$

and if not all the coefficients $A, B, C..$ are $\equiv 0$, then P cannot be divided by Q.

It is also clear that division could have begun with the terms of highest degree, kx^κ, tx^τ. The calculation will be easier if Q is put in the form

$$mx^\mu(1 + qx + rxx + \text{etc.})$$

which, on putting $mv \equiv 1$, gives

$$\frac{P}{Q} \equiv \frac{vP : x^\mu}{1 + qx + \text{etc.}}$$

Division can then be completed by the usual methods.

333.

THEOREM. *If $x \equiv a$ is a root of the congruence $\xi \equiv 0$, then ξ can be divided by $x - a$ for the modulus of the congruence.*

Proof. For if it could not be divided, we would have $\xi \equiv (x-a)\xi' + b$, where b could not be divided by the modulus. Now, if x is set $\equiv a$, then ξ becomes $\equiv 0$ by hypothesis, so $(x-a)\xi' + b \equiv 0$. But then also $(x-a)\xi' \equiv 0$, and therefore b must be $\equiv 0$.

334.

PROBLEM. *Given two functions, find their common divisor (of greatest degree) for a given modulus.*

Solution. Let the functions be A, B, and let the degree of A be at least that of B. Divide A by B. If this is possible without a remainder, B will be the common divisor sought. If a remainder C is left, it will have lower degree than B. Thus let

$$A \equiv aB + C, \quad B \equiv bC + D, \quad C \equiv cD + E, \quad \text{etc.}$$

where A, B, C, D, a, b, c, and so on, are functions, and the degrees of the functions A, B, C, D, and so on, form a decreasing sequence. If some division eventually succeeds, for example $D \equiv dE$, the last divisor will be the common divisor sought. If none succeeds, a remainder will eventually be reached which has no degree, that is, a *number*; in this case, however, the functions A, B have no common divisor.

Proof. If the divisor E divides the preceding function without a remainder, it is easily seen to divide all the preceding ones. Hence E will be a common divisor of the functions A, B, proving the first assertion. But if there were a divisor of higher degree, say E', then, because $C \equiv A - aB$, it would also divide C, and by the same argument D, and so on, and therefore E: a function of higher degree would divide one of lower degree. This is absurd, proving the second assertion. It is also clear from this that, if a common divisor of any degree exists, a remainder with no degree cannot be reached. Otherwise a function with no degree would be divided by a function of some degree, which is absurd.

335.

THEOREM. *If A, B are coprime functions for the modulus p, and A has degree α, while B has degree β, then functions P, Q can be found whose degrees are respectively $< \beta$, $< \alpha$, such that*

$$PA + QB \equiv 1 \ (mod.\, p)$$

Proof. For in this case we have

$$A \equiv aB + C, \quad B \equiv bC + D, \quad \text{etc.} \quad K \equiv kL + M$$

where the degrees of the functions $A, B, C, D, \ldots K, L, M$ continually decrease, and M has no degree. Now form the sequences

$$\begin{array}{cccccc} a, & a', & a'', & a''', & \ldots & a^{(\kappa)} \\ 1, & b, & b', & b'', & \ldots & b^{(\kappa-1)} \end{array}$$

so that

$$\begin{array}{llll} a' \equiv ba + 1 & a'' \equiv ca' + a & a''' \equiv da'' + a' & \text{etc.} \\ b' \equiv cb + 1 & b'' \equiv db' + b & b''' \equiv eb'' + b' & \text{etc.} \end{array}$$

We then have

$$A - aB \equiv +C, \quad bA - a'B \equiv -D, \quad b'A - a''B \equiv +E, \quad \text{etc.}$$

as is readily seen, and hence, finally,

$$b^{(\kappa-1)}A - a^{(\kappa)}B \equiv \pm M$$

Now let $\frac{1}{\pm M} \equiv \mu$. Then, on putting $P \equiv \mu b^{(\kappa-1)}$, $Q \equiv -\mu a^{(\kappa)}$, we obtain

$$PA + QB \equiv 1$$

Further, it is clear that

$$\begin{array}{c} \text{degree of } B + \text{degree of } a = \text{degree of } A. \\ \text{degree of } C + \text{degree of } b = .\text{degree of } B \\ \text{etc.} \\ \text{degree of } L + \text{degree of } k = \text{degree of } K \end{array}$$

Therefore

$$\text{degree of } L + \text{sum of the degrees of } a, b, \ldots k = \text{degree of } A$$

The degree of $a^{(\kappa)}$ is evident, and hence also

$$\text{degree of } Q = \text{sum of the degrees of } a, b, c, \ldots \text{ that is, } = \alpha - \text{degree of } L$$

Thus

$$\text{degree of } P = \beta - \text{degree of } L \qquad \text{Q. E. D.}$$

336.

It follows that, if M is the common divisor of greatest degree of the functions A, B, we can always put

$$AP + BQ \equiv M$$

For brevity I omit examples of the preceding theorem, but readers will not neglect to gain skill in handling problems of this kind by working through examples. It is also worth pointing out that the preceding theorem holds for functions considered without a modulus, provided their coefficients are rational numbers. This will be evident from the method of proof itself. We cannot, however, dwell on this matter. The reader will observe similar things in what follows even without being prompted.

If A has no common divisor of any degree with either B or C, it will also have no common divisor with the product BC. For let

$$PA + QB \equiv 1, \quad \text{then} \quad PAC + QBC \equiv C$$

Now, if A had with BC a common divisor M, this would also divide C, contrary to the hypothesis. Thus, in general, if a function A is coprime to B, C, D, and so on, it will also be coprime to the product of them all.

If A, B, C, D, and so on, have no divisor common to them all, we can obtain

$$PA + QB + RC + SD + \text{etc.} \equiv 1$$

Let the common divisor of greatest degree of A and B be M; that of M and C be M'; that of M' and D be M'', and so on. The last term of this sequence clearly has no degree, by hypothesis. We can therefore put

$$aA + bB \equiv M, \quad mM + cC \equiv M', \quad m'M' + dD \equiv M'', \quad \text{etc.}$$

and after substitution the truth of the theorem is apparent.

337.

THEOREM. *If A, B, C, and so on, are functions coprime to one another (any two of them having no common divisor) for the modulus p, and the function M is divisible by each of them for the same modulus, it will also be divisible by the product of them all.*

Proof. For we can put $PA + QB \equiv 1$, so that

$$\frac{M}{A}Q + \frac{M}{B}P \equiv \frac{M}{AB}$$

Now, since C is coprime to AB, the function M will also be divisible by ABC, and by the same reasoning by $ABCD$, and so on.

338.

If the congruence $\xi \equiv 0$ has roots $x \equiv a$, $x \equiv b$, $x \equiv c$, and so on, then ξ can be divided by the product of $(x-a)$, $(x-b)$, $(x-c)$, and so on. For, since $a, b, c.$, and so on, are assumed incongruent, the functions $x-a, x-b, x-c$, and so on, will be coprime to one another. Since ξ is divisible by each of them, it will also be divisible by their product. Thus the number of roots cannot exceed the degree of the congruence: this is the proof of the theorem that we promised.

At the same time, however, this shows how the solution of congruences forms only one part of a much deeper investigation, namely the factorization of functions. The congruence $\xi \equiv 0$ clearly has no real roots if ξ has no factors of degree one. Yet nothing prevents ξ from being resolved into factors of degree two, three or more, from which roots that are, as it were, *imaginary* could be attributed to it. Indeed, had we wished to take a freedom similar to that taken by recent mathematicians and to introduce such imaginary quantities, we could have shortened all our following investigations incomparably. Nevertheless, we preferred to derive everything from principles[*)].

339.

Functions are called *prime* for a given modulus when they cannot be divided by any functions of lower degree for that modulus.

Thus all functions of degree one will be prime, while functions of degree two will either be prime or be composed of two of degree one. Hence ξ will be a prime function of degree two if the congruence $\xi \equiv 0$ admits no real roots. For example, $xx + x + 1$ is prime for the modulus 5, because

$$xx + x + 1 \equiv (x-2)^2 - 3 \pmod{5}$$

and 3 is a quadratic nonresidue of 5.

These prime functions demand our attention above all. Although those other than functions of degree one cannot serve to find real roots, a fuller study of them recommends itself both for their remarkable properties and for other excellent truths to be deduced from them.

[*)] Perhaps on another occasion we shall explain our opinion on this matter more fully.

340.

THEOREM. *Every function is either prime or composed of prime functions; in the latter case it can be composed of prime functions in only one way.*

Proof. For unless the proposed function A is prime, it will be divisible by another function B of lower degree. If B is not a prime function, it will be divisible by another function C of lower degree. Continuing in this way, a prime function must eventually be reached. Otherwise this sequence would be infinite, which is absurd, since the degrees continually decrease. Now, if the last prime function is L, it will divide all the preceding ones. Hence $A \equiv LA'$, and A' has lower degree than A. Repeating this, $A' \equiv L'A''$, and so on, a prime function must clearly eventually be reached. Thus A will be $\equiv$ a product of prime functions L, L', L'', and so on. . This proves the first assertion.

Now, if we also had $A \equiv MM'M''$, and so on, and the functions L, L', L'', and so on, were not all the same as M, M', M'', and so on, remove those common to both sequences. Let $\lambda, \lambda', \lambda''$ . .; $\mu, \mu', \mu'', \ldots$ remain. Then μ will be coprime to $\lambda, \lambda', \lambda''$, and so on, and hence also to the product $\lambda\lambda'\lambda''$, and so on. Yet we must have

$$\lambda\lambda'\lambda'' \ldots \equiv \mu\mu'\mu'' \ldots \text{ that is, } \frac{\lambda\lambda'\lambda'' \ldots}{\mu} \equiv \mu'\mu'' \ldots \quad \text{a contradiction}$$

341.

The first main task of these investigations will be to determine the number of prime functions of any given degree. For a given modulus, the number of all different (incongruent) functions of any given degree is finite. Some of these are composed of prime functions of lower degrees, while others are prime; hence the number of the latter is also finite. A rigorous development of this matter is rather delicate; we shall begin with simpler cases.

With the modulus set $= p$, the number of all different functions of degree n of the form

$$x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \text{etc.}$$

will be p^n. For the number of coefficients $.A, B\,.\,C$, and so on, is n, and each can independently of the others be $\equiv 0, 1, 2, 3 \ldots (p-1) (\text{mod.}\, p)$. The theory of combinations therefore gives p^n different combinations, which determine the collection of all different functions of this degree.

Thus there will be p functions of degree one, namely $x, x+1, x+2$ up to $x+p-1$; there will be pp functions of degree two, and so on.

342.

We have already pointed out that all functions of degree one must be regarded as prime. If, therefore, as is sufficient for our purpose, we restrict ourselves to functions whose highest term has coefficient 1, there will be p functions of the first degree, or of one dimension.

All functions of degree two are either composed of two of degree one or are prime. The theory of combinations shows that p different things, with repetitions allowed, can be combined in $\frac{p.p+1}{1.2}$ different ways. Thus there will be that many functions composed of two prime functions of degree one, and hence $pp - \frac{p.p+1}{1.2} = \frac{1}{2}(pp-p)$ prime functions of degree two.

Similarly, from all functions of degree three, whose number is p^3, we must exclude those composed of three prime functions of degree one, whose number is $\frac{p.p+1.p+2}{1.2.3}$, and also those composed of a prime function of degree one and another of degree two, whose number is $p \,.\, \frac{1}{2}(pp-p)$. Removing these leaves $\frac{1}{3}(p^3-p)$; this, then, is the number of prime functions of degree three. Clearly we can always continue in this way.

343.

To carry out these operations more easily and at the same time prepare the way for developing the general law, we shall consider the matter generally. For brevity we denote by (1) the number of prime functions of degree one, by (2) the number of prime functions of degree two, and further by (1^2) the number of functions composed of two prime functions of degree one, and so on, and so on. In general, $(1^\alpha 2^\beta 3^\gamma \ldots)$ denotes the number of all functions composed of prime functions, namely α of degree one, β of degree two, γ of degree three, and so on. Their degree will therefore be $\alpha + 2\beta + 3\gamma + \text{etc.}$ It follows from the preceding results and the theory of combinations that

$$(1^\alpha 2^\beta 3^\gamma 4^\delta \ldots) = (1^\alpha)(2^\beta)(3^\gamma)(4^\delta)\,..$$

$$(1^\alpha) = \frac{(1)\,.\,(1)+1\,.\,(1)+2\,.\,(1)+3\ldots(1)+\alpha-1}{1\,.\,2\,.\,3\,.\,4\ldots\alpha}$$

or, in general,

$$(a^\alpha) = \frac{(a)\,.\,(a)+1\,.\,(a)+2\,.\,(a)+3\ldots(a)+\alpha-1}{1\,.\,2\,.\,3\,.\,4\ldots\alpha}$$

Finally, if all the different ways of composing the number n by addition from the numbers $1, 2, 3, \ldots$ are collected, and these ways are denoted by $\alpha \,.\, 1 + \beta \,.\, 2 + \gamma \,.\, 3 + \text{etc.}$, then the sum of all these expressions $(1^\alpha 2^\beta 3^\gamma \,..)$ is clearly equal to the number of all functions of degree n, that is, $= p^n$. Thus

$$\begin{aligned} p &= (1) \\ pp &= (1^2) + (2) \\ p^3 &= (1^3) + (1 \,.\, 2) + (3) \\ p^4 &= (1^4) + (1^2 \,.\, 2) + (1 \,.\, 3) + (2^2) + (4) \\ &\text{etc.} \end{aligned}$$

The expression p^n clearly contains, besides the quantities $(1), (2), (3)$, and so on, also (n), which shows how all these quantities are to be determined from the preceding ones. Thus we find

$$\begin{array}{lll} (1) = p & (4) = \frac{1}{4}(p^4 - pp) & (7) = \frac{1}{7}(p^7 - p) \\ (2) = \frac{1}{2}(pp - p) & (5) = \frac{1}{5}(p^5 - p) & (8) = \frac{1}{8}(p^8 - p^4) \\ (3) = \frac{1}{3}(p^3 - p) & (6) = \frac{1}{6}(p^6 - p^3 - pp + p) & \text{etc.} \end{array}$$

344–346.

From the beginning of this sequence we observe that the highest term of the expression (n) is $\frac{1}{n}p^n$. If n is prime, $-\frac{1}{n}p$ is added to it; if n is composite, however, the law is less evident. But if we consider the matter more closely, we see that

$$\begin{array}{ll} p = (1) & p^5 = 5(5) + (1) \\ pp = 2(2) + (1) & p^6 = 6(6) + 3(3) + 2(2) + (1) \\ p^3 = 3(3) + (1) & p^7 = 7(7) + (1) \\ p^4 = 4(4) + 2(2) + (1) & p^8 = 8(8) + 4(4) + 2(2) + (1) \text{ etc.} \end{array}$$

Here the law of progression is apparent: if all the divisors of the number n are $\alpha, \beta, \gamma, \delta$, and so on, then

$$p^n = \alpha(\alpha) + \beta(\beta) + \gamma(\gamma) + \delta(\delta) + \text{etc.}$$

We now set out to prove that this observation holds in general.

We showed that the sum of all expressions of the form $(1^\alpha)(2^\beta)(3^\gamma)\ldots$, where always $\alpha + 2\beta + 3\gamma + \ldots = n$, exhausts all functions of degree n and is therefore $= p^n$. It follows that, — — —. If

$$\left(\frac{1}{1-x}\right)^{(1)}\left(\frac{1}{1-xx}\right)^{(2)}\left(\frac{1}{1-x^3}\right)^{(3)}\ldots$$

is expanded into the series $1 + Ax + Bx^2 \ldots = P$, then

$$A = p, \quad B = p^2, \quad C = p^3 \text{ etc.}$$

$$\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x} = \frac{(1)x}{1-x} + \frac{2(2)x^3}{1-x^2} + \frac{3(3)x^3}{1-x^3}\ldots$$

— — — —

[From this, on substituting $\frac{px}{1-px}$ for $\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x}$ and expanding the individual fractions into infinite series, the truth of the theorem follows of itself.]

347.

This theorem can also be expressed in another way. If all the divisors of the number n are $n, 1, \delta, \delta', \delta'', \delta'''$, and so on, the theorem states that

$$p^n = n(n) + (1) + \delta(\delta) + \delta'(\delta') + \text{etc.}$$

Now the product of the (n) prime functions of degree n clearly has degree $n(n)$, and likewise for the others. Hence

The product of all prime functions of degree one and of degrees n, δ, δ', and so on, will have degree p^n.

It is now easy to deduce the value of the expression (n) itself from this theorem, but for brevity we omit the analysis, which is not difficult. Let $n = a^\alpha b^\beta c^\gamma$, and so on, where a, b, c, and so on, are distinct prime numbers. Then

$$n(n) = p^n - \Sigma p^{\frac{n}{a}} + \Sigma p^{\frac{n}{ab}} - \Sigma p^{\frac{n}{abc}} \text{ etc.}$$

Here $\Sigma p^{\frac{n}{abc..}}$ denotes the collection of all expressions similar to $p^{\frac{n}{abc..}}$ when the quantities $a, b, c..$ are permuted among themselves in every way. Thus for $n = 36$ we have $36(36) = p^{36} - p^{18} - p^{12} + p^6$.

Let us add one more observation. If n has the form a^α, and a is prime, then $n(n) = p^n - p^{\frac{n}{a}}$. Since (n) must be an integer, we therefore have, whatever p may be,

$$p^n \equiv p^{\frac{n}{a}} \pmod{n}$$

Thus, if p is coprime to a,

$$p^{n-\frac{n}{a}} \equiv 1 \pmod{n}$$

and for $\alpha = 1$,

$$p^{a-1} \equiv 1 \pmod{a}$$

It is remarkable that these theorems can be obtained in such different ways.

348.

PROBLEM. *Given the equation*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \text{etc.} + M = 0$$

whose roots are $x = a$, $x = b$, $x = c$, and so on, find an equation whose roots are $x = a^\tau$, $x = b^\tau$, $x = c^\tau$, and so on.

First solution. Find, by the known theorem, the sums of the roots of the given equation, of their squares, cubes, and so on, through the power with exponent $m\tau$. This also gives the sums of the roots of the required equation, and of their squares, and so on, namely Σa^τ, $\Sigma a^{2\tau}$, and so on. The coefficients can then be determined by the same theorem.

For practical calculation this solution is easier; but the following is better suited to our purpose, and also to showing that the coefficients of the required equation will be integers if the coefficients of the given equation are integers.

Second solution. Let θ be a primitive root of the equation $x^\tau = 1$, and form the product of

$$\begin{aligned}
&x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.}\\
&x^m + A\theta x^{m-1} + B\theta\theta x^{m-2} + \text{etc.}\\
&x^m + A\theta\theta x^{m-1} + B\theta^4 x^{m-2} + \text{etc.}\\
&\text{etc.}\\
&x^m + A\theta^{\tau-1} x^{m-1} + B\theta^{2\tau-2} x^{m-2} + \text{etc.}
\end{aligned}$$

The roots of this product will therefore be

$$\begin{array}{llll}
a, & \theta a, & \theta\theta a & \text{etc.}\\
b, & \theta b, & \theta\theta b & \text{etc.}\\
c, & \theta c, & \theta\theta c & \text{etc.}
\end{array}$$

that is, the product will equal

$$(x^\tau - a^\tau)(x^\tau - b^\tau)(x^\tau - c^\tau)\ldots$$

and hence have the form

$$x^{\tau m} + A' x^{\tau(m-1)} + B' x^{\tau(m-2)} + \text{etc.}$$

Now, replacing x^τ by x, we have

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{etc.} = (x - a^\tau)(x - b^\tau)(x - c^\tau)\dots$$

and hence

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{etc.} = 0$$

is the required equation. That A', B', and so on, are not only rational numbers but also integers follows easily from the theory of the equation $x^\tau = 1$.

Since we shall often use this operation below, by (P, ρ^τ) we shall denote the function which, on being set equal to zero, gives an equation whose roots are the powers with exponent τ of the roots of the equation $P = 0$.

If $P \equiv Q$ for any modulus, then also $(P, \rho^\tau) \equiv (Q, \rho^\tau)$ for the same modulus.

349.

THEOREM. *The coefficient of the term x^n in (P, ρ^τ) is congruent, modulo τ, to the coefficient of the term $x^{\tau n}$ in P^τ, provided that τ is a prime number* (which, in this case, gives a third solution of the preceding problem).

Proof. It follows from Chapter Six that every coefficient of the product

$$(x^m + Ax^{m-1} + \text{etc.})(x^m + A\theta x^{m-1} + \text{etc.})\dots$$

has the following form after θ^τ is replaced by unity:

$$E + (1 + \theta + \theta\theta + \text{etc.} + \theta^{\tau-1})F$$

Now, if θ is regarded as a primitive root of the equation $x^\tau = 1$, the whole product becomes E; but if $\theta = 1$, the whole product becomes $P^\tau = E + \tau F$. Thus the coefficient of the term $x^{n\tau}$ in P^τ is congruent, modulo τ, to the coefficient of the term $x^{n\tau}$ in E, that is, to the coefficient of the term x^n in (P, ρ^τ).

350.

THEOREM. *If τ is a prime number, then*

$$(P, \rho^\tau) \equiv P \ (mod.\, \tau)$$

Proof. Let the coefficient of the term x^n in (P, ρ^τ) be $= N'$, and let the coefficient of the same term in P be $= N$. Then, on putting

$$P = x^m + Ax^{m-1} + \text{etc.} + Nx^n + \text{etc.}$$

we have

$$P^\tau \equiv x^{m\tau} + A^\tau x^{(m-1)\tau} + \text{etc.} + N^\tau x^{n\tau} + \text{etc.} \ (\text{mod.}\, \tau)$$

and hence, by the preceding article, $N' \equiv N^\tau \ (\text{mod.}\, \tau)$. Thus, since $N^\tau \equiv N$, we obtain $N' \equiv N$. Q. E. D.

It is also clear from this that $(P, \rho^{\alpha}) \equiv (P, \rho^{\alpha\tau})$ and $(P, \rho^{\tau}) \equiv (P, \rho^{\tau\tau})$, whence, in general,

$$(P, \rho^{\alpha}) \equiv (P, \rho^{\alpha\tau^k}) \,(\mathrm{mod.}\, \tau)$$

351.

THEOREM. *There is a value of the number ν less than p^m such that the function $x^{\nu} - 1$ can be divided by the given function P of degree m, whose lowest term does not involve the indeterminate x, modulo p.*

Proof. Divide by P the sequence of functions $1, x, xx \ldots$ through x^{p^m-1} as soon as their degree exceeds m. Since none can be divided by P without a remainder, all the remainders can be put in the form

$$Ax^{m-1} + Bx^{m-2} + \ldots + N$$

with all coefficients positive and $< p$. But since they can never all be $= 0$, there are clearly only $p^m - 1$ functions, one of which each remainder must equal. Since, through the power of x whose exponent is $p^m - 1$, there are p^m remainders, at least two must necessarily be the same. Let the same remainder result when x^a and $x^{a+\nu}$ are divided by P, with $a + \nu < p^m$. Thus $x^{a+\nu} - x^a$ can be divided by P. Since, by hypothesis, x, and hence also x^a, is a function coprime to P, it follows that $x^{\nu} - 1$ can also be divided by P. Q. E. D.

Corollary. If $x^{\nu} - 1$ can be divided by P, then $x^{k\nu} - 1$ can also be divided by P, where k denotes any integer.

352.

THEOREM. *Keeping the notation of the preceding article, if P is a prime function and x^{ν} is the lowest power which, after unity is subtracted, can be divided by P, then ν is either $= p^m - 1$ or a divisor of this number, with the sole exception of the case $P = x$.*

Proof. Since P is a prime function of degree m, there are $p^m - 1$ different functions of degree less than m (excluding the function 0 from the total), all of which are coprime to P. Now, since x^ν is assumed to be the lowest power which leaves unity as remainder on division by P, it is clear that dividing all lower powers, from $1, x, ..$ through $x^{\nu-1}$, by P gives ν different remainders, which we denote generally by A. If these exhaust all possible remainders, the theorem is proved; but if some are still absent from their number, let B be any one of them. It is clear that the function Bx^ν, divided by P, gives remainder B, and that, in general, $Bx^{\nu+k} \equiv Bx^k (\mathrm{mod.}\, P)$. But all the functions from B through $Bx^{\nu-1}$ give remainders different from one another and from the remainders A. For if $Bx^\lambda \equiv Bx^{\lambda+\delta} (\mathrm{mod.}\, P)$, we would also have $1 \equiv x^\delta (\mathrm{mod.}\, P)$, with $\delta < \nu$, contrary to the hypothesis; while if $Bx^\lambda \equiv x^\mu (\mathrm{mod.}\, P)$, we would have $B \equiv x^{\mu+\nu-\lambda} (\mathrm{mod.}\, P)$, and hence B would be one of the remainders A, contrary to the hypothesis. We thus clearly have ν further new remainders. We may proceed in the same way (exactly as above, §. .), and it will become apparent that the number $p^m - 1$ of all possible remainders is either $= \nu$, or $= 2\nu$, or $= 3\nu$, or, in general, a multiple of the number ν. Q. E. D.

353.

It follows from the preceding theorem and the corollary to §. 351 that every prime function of degree n divides the function $x^{p^n-1} - 1$ modulo p. Thus all functions of degree one, except the single one which is $\equiv x$, divide $x^{p-1} - 1$, which is FERMAT'S THEOREM; all prime functions of degree two, that is, of the form $xx + Ax + B$, divide the function $x^{pp-1} - 1$, and so on. Now let all divisors of the number n be $n, \delta, \delta', \delta''$, and so on, . 1. It is clear that $p^n - 1$ is also divisible by $p^\delta - 1$, $p^{\delta'} - 1$, $p^{\delta''} - 1$, and so on, $p - 1$. Hence the function $x^{p^n-1} - 1$ can be divided by *all prime functions of degrees $n, \delta, \delta', \delta''$, and so on, down to the prime functions of degree one (excluding the function x)*, and therefore also, since all these functions are prime in themselves and hence coprime to one another, by *the product of them all.* But this same product has degree $p^n - 1$ (§. 347), because the one function x is absent. Thus it is clear that *this product itself must be congruent to* $x^{p^n-1} - 1 (\mathrm{mod.}\, p)$.

354.

THEOREM. *If the function $x^\nu - 1$ is divisible by the function P, then*

$$(P, \rho^{k\nu+t}) \equiv (P, \rho^t)$$

where k, t denote any integers.

Proof. Let

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.}$$

It is known that, if

$$\frac{mx^{m-1} + (m-1)Ax^{m-2} + \text{etc.}}{x^m + Ax^{m-1} + \text{etc.}}$$

is expanded in an infinite series of the form

$$m\frac{1}{x} + \alpha\frac{1}{xx} + \beta\frac{1}{x^3} + \gamma\frac{1}{x^4} + \text{etc.}$$

then α is the sum of the roots of the equation $P = 0$, β the sum of their squares, and so on. From this it follows without difficulty that the sums of the powers with exponents $\nu + 1$, $\nu + 2$, and so on, are congruent to the sum of the roots, of their squares, and so on. Hence, unless the modulus is equal to or less than the degree of the function P, we have

$$(P, \rho^{\nu+1}) \equiv P, \quad (P, \rho^{\nu+2}) \equiv (P, \rho^2), \quad (P, \rho^{\nu+3}) \equiv (P, \rho^3) \text{ etc.}$$

We shall consider that case below.

355.

THEOREM. *If, in the sequence*

$$(P,\rho^0),\quad (P,\rho)\quad (P,\rho^2),\quad (P,\rho^3)\text{ etc.}$$

the terms following the term in position ν are successively congruent to the first terms, then $x^\nu - 1$ can be divided by P, provided that P contains no factor more than once.

Proof. On putting $\frac{\mathrm{d}P}{\mathrm{d}x} = Q$, Q will be a function coprime to P. Let

$$\frac{Q}{P} \equiv \frac{A}{x} + \frac{B}{xx} + \frac{C}{x^3} + \text{etc.}$$

Then, after the term $\frac{N}{x^\nu}$, there follows, by hypothesis,

$$\frac{A}{x^{\nu+1}} + \frac{B}{x^{\nu+2}} + \frac{C}{x^{\nu+3}} + \text{etc.}$$

Thus

$$\frac{Q}{P} \equiv \frac{Ax^{\nu-1} + Bx^{\nu-2} + \text{etc.}}{x^\nu - 1}$$

which shows that the function $x^\nu - 1$ can be divided by P. Q. E. D.

356.

THEOREM. *If P is a prime function of x of degree m, and X is a function of $x, x^p, x^{pp}, x^{p^3} \,..\, x^{p^{m-1}}$ in which all these quantities occur in the same way, that is, which remains unchanged however they are permuted among themselves, then dividing the function X by P gives a remainder which is a number.*

Proof. Let the remainder be

$$Ax^{m-1} + Bx^{m-2} + \,..\, + N \equiv \xi$$

All coefficients $A, B, C \ldots$ up to, but excluding, N will be $\equiv 0$. This is proved as follows. Since $X - \xi$ is divisible by P, $X^p - \xi^p$ can also be divided by P. But it is easy to see that X^p is what X becomes when x is replaced by x^p, x^p by x^{pp}, and so on, . and $x^{p^{m-1}}$ by x^{p^m}, or, equivalently, x. Thus it is clear that $X^p \equiv X \pmod{P}$; hence, since $X^p \equiv \xi^p$ and $X \equiv \xi (\mathrm{mod.}\, P)$, we also have $\xi^p \equiv \xi (\mathrm{mod.}\, P$, or

$$\xi^p - \xi \equiv 0 (\mathrm{mod.}\, P)$$

But $\xi^p - \xi$ is congruent, modulo p, to the product of $\xi, \xi+1, \xi+2, ..$ through $\xi + p - 1$. These factors are all coprime to P unless ξ is simply a number. Hence $\xi^p - \xi$ cannot be divisible by P in any other way. Q. E. D.

Functions of this kind are the sum of all the quantities, the sum of their squares, cubes, and so on, and the sums of their products taken two at a time, three at a time, and so on. We shall determine what that number is in the following article:

357.

THEOREM. *Let the prime function of the preceding article be*

$$P \equiv x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \text{etc.}$$

Then the remainder when the sum of the quantities x, x^p, *and so on,* $x^{p^{m-1}}$ *is divided by* P *is* $\equiv A$*; for the sum of their products taken two at a time it is* $\equiv B$*; for the sum of their products taken three at a time it is* $\equiv C$*, and so on.*

Proof. Let those functions be X, Y, Z, and so on, and let their remainders be the numbers A', B', C', and so on, in their respective order. It is easy to see that x, x^p, x^{pp}, and so on, are roots of the equation

$$z^m - Xz^{m-1} + Yz^{m-2} - Zz^{m-3} + \text{etc.} = 0$$

Thus, on putting $z = x$, we have

$$x^m - Xx^{m-1} + Yx^{m-2} - Zx^{m-3} + \text{etc.} = 0$$

But the functions $X - A'$, $Y - B'$, $Z - C'$, and so on, are divisible by P, and hence so is the function

$$x^m - A'x^{m-1} + B'x^{m-2} - C'x^{m-3} + \text{etc.}$$

This cannot happen unless $A' \equiv A$, $B' \equiv B$, $C' \equiv C$, and so on. Q. E. D.

It is also known that any other function X of x, x^p, and so on, [in which all these quantities occur in the same way,] can always be derived from these. Thus

$$x^2 + x^{2p} + x^{3pp} + \text{etc.} \equiv AA - 2B(\text{mod.}\, P) \text{ etc. etc.}$$

Example. Let $p = 5$ and $P \equiv x^2 + 2x + 3$. Then the function $x + x^5$, divided by P, gives $\equiv -2$, and $x^6 \equiv 3$, and so on, and so on.

358. 359.

THEOREM. *Let P be a prime function and x^ν the lowest power of x which, divided by P, gives remainder 1. Further, let $P \equiv (P, \rho^n)$. Then n is congruent to some power of the number p modulo ν.*

Proof. We showed above that, if P

$$= x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.}$$

then

$$z^m + Az^{m-1} + Bz^{m-2} + \text{etc.} \\ - (z-x)(z-x^p)\ldots(z-x^{p^{m-1}})$$

is divisible by P. In the same way it would follow that

$$z^m + Az^{m-1} + Bz^{m-3} + \text{etc.} \\ - (z-x^n)(z-x^{np})\ldots(z-x^{np^{m-1}})$$

is divisible by P. Since these factors are coprime to one another, the individual factors must necessarily be congruent to the corresponding individual factors modulo P, p. Thus $z - x^n$ must be $\equiv z - x^{p^\kappa}$, that is, $p^\kappa \equiv n (\text{mod.}\, \nu)$. Q. E. D.*)

Finding the prime divisors of the function $x^\nu - 1$ for a prime modulus.

360.

If ν is divisible by the modulus p or by one of its powers, put $\nu = p^k\lambda$. Then

$$x^\nu - 1 \equiv (x^\lambda - 1)^{p^k} (\text{mod.}\, p)$$

This makes it clear that only the case where ν is not divisible by p needs to be considered.

*) If $(P, \rho^a) \equiv (P, \rho^b) (\text{mod.}\, p)$, then $a \equiv p^\kappa b (\text{mod.}\, \nu)$.

Proof. Let $z^m + Az^{m-1} + Bz^{m-2} + \ldots = \Pi$. Then $(\Pi, \rho^a) \equiv (\Pi, \rho^b) (\text{mod.}\, P)$; but

$$(\Pi, \rho^a) \equiv (z-x^a)(z-x^{ap})(z-x^{app})\ldots(z-x^{ap^{m-1}}),$$
$$(\Pi, \rho^b) \equiv (z-x^b)(z-x^{bp})(z-x^{bpp})\ldots(z-x^{bpm-1})$$

which establishes the proposition.

The product of $\Pi, (\Pi, \rho^2), (\Pi, \rho^3)$, and so on, (Π, ρ^ν) is $\equiv (z^\nu - 1)^m (\text{mod.}\, P)$, for

$$(z-x)(z-x^2)(z-x^3)\ldots(z-x^\nu)$$
$$\equiv (z-x^p)(z-x^{2p})(z-x^{3p})\ldots(z-x^{\nu p}) \equiv \text{etc.} \equiv z^\nu - 1$$

In the sequence $P, (P, \rho^2), (P, \rho^3)$, and so on, $\ldots (P, \rho^\nu)$, all prime divisors of the function $x^\nu - 1$ occur, each m times. It follows that the product of them all is $\equiv (x^\nu - 1)^m$.

If $p^m \equiv 1(\text{mod.}\,\nu)$, with m as small as possible, then $x^{p^m-1}-1$ is clearly divisible by $x^\nu - 1$. Thus $x^\nu - 1$ cannot have any divisors other than those of $x^{p^m-1}-1$. But this expression has prime divisors of degree m and others whose degrees divide the number m. Thus $x^\nu - 1$ also has divisors of these kinds. We shall show how many it has of each kind by an example, from which the general law can easily be deduced.

Let $\nu = 63$ and $p = 13$. Then $m = 6$. Thus $x^{63}-1$ has prime factors of degrees six, three, two and one modulo 13. It is clear that the product of the factors of degree one is the common divisor of greatest degree of the functions $x^{63}-1$ and $x^{12}-1$, that is, x^3-1; hence there are three prime factors of degree one. The product of all prime factors of degrees two and one is the common divisor of the functions $x^{63}-1$ and $x^{168}-1$, that is, $x^{21}-1$; hence there are $\frac{21-3}{2}$, or 9, factors of degree two. The product of the prime factors of degrees three and one is the common divisor of the functions $x^{63}-1$ and $x^{2196}-1$, that is, x^9-1; hence there are $\frac{9-3}{3}$, that is, 2, divisors of degree three. Finally, the remaining ones have degree six, and their number is therefore $= \frac{63-6-18-3}{6}$, that is, 6.

Careful consideration of this matter easily gives the following general rule:

Let δ be a divisor of m, and let all divisors of the number δ less than δ be $\delta', \delta'', \delta'''$, and so on. Let the greatest common divisors of ν with $p^\delta - 1$, $p^{\delta'}-1$, $p^{\delta''}-1$, and so on, be μ, μ', μ'', and so on, respectively. Put $\frac{\mu}{\mu'}; \frac{\mu}{\mu''}, \frac{\mu}{\mu'''}$, and so on, $= \lambda', \lambda'', \lambda'''$, and so on. Then $x^\nu - 1$ has $\frac{1}{\delta}$ times as many prime divisors of degree δ as there are numbers below μ divisible by none of the numbers $\lambda', \lambda'', \lambda'''$, and so on.

361.

THEOREM. *If a function X of the indeterminate x is divisible by another function ξ, and X, when x is replaced by x^k, becomes X', then X' is divisible by $(\xi, \rho^{\frac{1}{k}})$.*

Proof. Let $X \equiv \xi\upsilon$, and let ξ, υ become ξ', υ' when x is replaced by x^k. It is clear that $X' \equiv \xi'\upsilon'$. But ξ' is divisible by $(\xi, \rho^{\frac{1}{k}})$. Hence so is X'. Q. E. D.

362.

With these principles established, we can easily determine the prime divisors of the function $x^\nu - 1$. We assume that all those divisors which also divide some function $x^{\nu'} - 1$, where $\nu' < \nu$, have already been found, and propose to investigate the remaining ones. They can all be included in the expression (P, ρ^k), if P is one of them and k takes all values less than ν and coprime to it.

In Chapter VI we showed how the primitive roots of the equation $x^\nu = 1$ can be divided into classes so that, when all are expressed as powers of one of them, the same division into classes results whichever primitive root is taken as the base; we called such collections of roots *periods*. It is clear that the functions $x, x^\alpha, x^\beta, x^\gamma$, and so on, where α, β, γ, and so on, denote all numbers coprime to ν, can be divided into periods in the same way, and each larger period again into smaller ones, until periods of the form $x^k, x^{kp}, x^{kpp} \ldots x^{kp^{m-1}}$ are finally reached. Once this is done, the following is clear:

1. Since every period is composed of smallest periods of the form $x^k + x^{kp} +$ etc., division by any prime function of degree m gives a remainder which is a number.

2. Since all terms of a period can always be put in the form $x^{\kappa . a^\alpha b^\beta c^\gamma \ldots}$, where $\kappa.\ a, b, c \ldots$ are fixed numbers, while all values may be substituted for $\alpha, \beta, \gamma \ldots$, it is clear that the period becomes itself when x is replaced by x^k and k has the form $a^\alpha b^\beta c^\gamma \ldots (\mathrm{mod.}\, \nu)$. From this it is easy to see that all the functions $P, (P\ \rho^k)$, and so on, with k denoting a number of this kind, give the same remainder when the period is divided by them.

3. Thus, after such a remainder has been subtracted, the period can be divided by the product of all the functions (P, ρ^k).

363.

The main task is to determine these remainders. First, find the remainder that the largest period gives on division by the product of all the appropriate prime functions. If this product is

$$\equiv x^\lambda - Ax^{\lambda-1} + \text{etc.}$$

then this remainder is $\equiv A$. The form of this product is readily found, and Chapter VI shows that $A = 0$ if ν is divisible by a square; otherwise A is either $= +1$ or $= -1$, according as the number of prime factors of ν is even or odd.

Now split this largest period into smaller periods, and represent the terms of any one period by $x^{kp^\pi u}$, so that k is a number fixed within each period but varying between periods, while π and u vary within each period and can take in the other periods the same values that they take in any one period. For the moment, take some prime function P as the base, and let the

periods $\Sigma x^{p^\pi u}$, $\Sigma x^{k' p^\pi u}$, etc., on division by it, give the remainders A, A', etc., respectively. Then $\Sigma x^{p^\pi u} - A$ is divisible by the product of all the functions (P, ρ^u); $\Sigma x^{k' p^\pi u} - A'$ by the product of all the functions $(P, \rho^{k' u})$; etc., etc. It is readily seen that the quantities A, A', etc., are roots of a known congruence. Namely, let the periods of the roots of the equation $x^\nu = 1$ corresponding to the preceding periods be roots of the equation $Q = 0$; then A, A', etc., will be roots of the congruence $Q \equiv 0$. For we have

$$A + A' + \text{etc.} \equiv \text{the sum of the periods},$$
$$AA + A'A' + \text{etc.} \equiv \text{the sum of the squares of the periods}$$

etc., etc. The calculation is entirely similar to the one we set out in Chapter VI, if in place of ρ we substitute x, since here too we can put unity for x^ν, as we did there for ρ^ν.

Once the roots A, A', etc., have been found, choose one as the remainder of the period $\Sigma x^{p^\pi u}$, and use it to order the remainders of the others in the same way as in Chapter VI. This choice is left free here too, since the function P is still entirely undetermined. The subsequent calculation is wholly analogous to the one we treated in Chapter VI; setting out every detail would take us too far. Finally, once we have reached Σx^{p^π}, the main task is complete. For, on putting

$$P \equiv x^m + ax^{m-1} + bx^{m-2} + \text{etc.}$$

we have $-a \equiv \Sigma x^{p^\pi}$. The second coefficient of the other functions (P, ρ^k) is obtained in the same way, and from this the remaining coefficients of P can be determined. It may often happen that we reach identical congruences from which nothing seems to follow. How this difficulty can be met will be shown below.

364.

An example will make all this much clearer. The proposed task is to resolve the function $x^{15} - 1$ into factors modulo 17. We have $m = 4$, and since the product of all the elementary functions is

$$\equiv \frac{x^{15} - 1 \,.\, x - 1}{x^3 - 1 \,.\, x^5 - 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

there will therefore be only two prime factors of degree four, P and P'. Now distribute $x, xx, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}$ into these two periods:

$$\Sigma x^{17^\alpha} \equiv x + xx + x^4 + x^8,$$
$$\Sigma x^{7.17^\alpha} \equiv x^7 + x^{11} + x^{13} + x^{14}$$

Modulo one of the functions P, P', let

$$\Sigma x^{17^\alpha} \equiv A, \quad \Sigma x^{7.17^\alpha} \equiv A'$$

Then

$$\begin{aligned} A + A' &\equiv 1 \\ AA &\equiv \Sigma x^{2.17^\alpha} + \Sigma x^{3.17^\alpha} + \Sigma x^{5.17^\alpha} + \Sigma x^{9.17^\alpha} \\ A'A' &\equiv \Sigma x^{14.17^\alpha} + \Sigma x^{6.17^\alpha} + \Sigma x^{5.17^\alpha} + \Sigma x^{3.17^\alpha} \end{aligned}$$

and hence

$$\begin{aligned} AA + A'A' &\equiv \Sigma x^{17^\alpha} + \Sigma x^{7.17^\alpha} + 4\Sigma x^{3.17^\alpha} + 2\Sigma x^{5.17^\alpha} \\ &\equiv 1 - 4 - 4 \equiv -7 \end{aligned}$$

Thus A and A' will be the roots of the congruence

$$xx - x + 4 \equiv 0 \,(\mathrm{mod.}\, 17)$$

which are $6, 12$. It follows that P divides

$$x^8 + x^4 + xx + x - 6$$

and is

$$\equiv x^4 - 6x^3 - 2xx - 12x + 1$$

Further, P' will be $\equiv (P, \rho^7)$, and will be

$$\equiv x^4 - 12x^3 - 2xx - 6x + 1$$

365.

It is enough for us here to have shown the possibility of these solutions. For brevity, we pass over many devices that can ease these operations. But we cannot omit some very important consequences.

What precedes proves that all the auxiliary equations for solving the equation $x^\nu = 1$, if converted into congruences, have possible roots when the period

$$x + x^p + x^{pp} + \ldots + x^{p^{m-1}}$$

has not yet been split. Let us stay with the case where ν is prime; then m is a divisor of $\nu - 1$. Here, therefore, the auxiliary congruences have real roots if the number of periods found through them is a divisor of $\frac{\nu-1}{m}$. Thus, if $\frac{\nu-1}{m}$ is even, that is, if m is a divisor of $\frac{\nu-1}{2}$, or equivalently if $p^{\frac{\nu-1}{2}} \equiv 1 \,(\mathrm{mod.}\, \nu)$, or equivalently if p is a quadratic residue of the prime ν, the quadratic equation that divides the roots into two periods will have real roots modulo p. But in Chapter VI we showed that, on putting $\nu = 4n \pm 1$, this equation is always $xx + x \mp n = 0$. Hence we have the notable

THEOREM. *If the prime p is a quadratic residue of the prime $4n \pm 1$, the congruence*

$$xx + x \mp n \equiv 0 (\text{mod. } p)$$

will have real roots, and therefore so will the congruence

$$4xx + 4x \mp 4n \equiv 0 \quad \text{or} \quad (2x+1)^2 \mp \nu \equiv 0$$

that is, $\pm\nu$ will be a quadratic residue of p.

366.

This, then, is the third complete proof of the fundamental theorem of Chapter IV, all the more worthy of attention because the principles from which it is drawn are entirely different from those we used for the earlier proofs. .But from this same source, by the opposite route, let us derive a fourth. Namely, let ν be a prime of the form $4n \pm 1$, let p be any other prime, and let $\pm\nu$ be a quadratic residue of the prime p; we shall prove that p is a quadratic residue of ν.

Let p^m be the least power of p that is $\equiv 1 (\text{mod. } \nu)$. The elementary divisors of the function $\frac{x^\nu - 1}{x-1}$ modulo p will have degree m, so their total number will be $= \frac{\nu-1}{m}$. Now, since $\pm\nu Rp$, the congruence

$$xx + x \mp n \equiv 0 (\text{mod. } p)$$

will be solvable; let its roots be A, A'. Distribute the functions $x, xx, .. x^{\nu-1}$ into two classes, denoted by ξ, ξ'. We have

$$\xi + \xi' \equiv A + A' + (1 + x + xx + .. + x^{\nu-1})$$
$$\xi\xi' \equiv AA' + \lambda(1 + x + xx + .. + x^{\nu-1})$$

so that

$$(z - \xi)(z - \xi') - (z - A)(z - A')$$

will be divisible by every elementary divisor of the function $\frac{x^\nu - 1}{x-1}$. Each of these elementary divisors will therefore divide either $\xi - A$ and $\xi' - A'$, or $\xi - A'$ and $\xi' - A$. It follows (since A is not $\equiv A'$) that, if in place of x we substitute x^p, then ξ and ξ' do not change. For if ξ passed into ξ', and conversely, then $\xi - A$ and $\xi - A'$ would be divisible by the same prime function. Q. E. A. Finally, it follows that $\frac{\nu-1}{2}$ is divisible by m, or equivalently that $p^{\frac{\nu-1}{2}} - 1$ is divisible by ν. Thus p is a quadratic residue of ν. Q. E. D.

It is easy to derive all cases of the fundamental theorem from the two theorems.

367.

Although we have restricted ourselves here to the case where ν is prime, analogous theorems can also be determined without much difficulty when ν is composite; brevity does not now allow us to set this out more fully.

It is evident that similar observations can also be made about a greater number of periods. Thus, if $\frac{\nu-1}{m}$ is divisible by 3, that is, if p is a cubic residue of the prime ν, the equation that distributes the roots of the equation $x^\nu = 1$ into three periods, and whose determination a priori we taught in Chapter VI, will be solvable modulo p, and conversely. For example, the congruence $x^3 + xx - 2x - 1 \equiv 0$ can be solved modulo any prime of the form $7n \pm 1$, but cannot if it has another form.

It would not be difficult for us to enrich this chapter with many other observations, if the limits within which we must keep did not prevent it. For those who wish to go further, these principles can at least point the way.

368.

We say that a congruence $S \equiv 0$ has *equal* roots, or more generally equal divisors, if it is divisible by a power of some function.

Whether a given congruence has equal divisors is decided in the same way as in the theory of equations. Put

$$X \equiv \xi^m P$$

Clearly,

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv \xi^{m-1}\left(mP\frac{\mathrm{d}\xi}{\mathrm{d}x} + \xi\frac{\mathrm{d}P}{\mathrm{d}x}\right)$$

so $\frac{\mathrm{d}X}{\mathrm{d}x}$ is divisible by ξ^{m-1}. More generally, let

$$X \equiv A^a B^b C^c \text{ etc.}$$

where A, B, C, etc., denote distinct prime functions. Then

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv X\left(\frac{a\,\mathrm{d}A}{A\,\mathrm{d}x} + \frac{b\,\mathrm{d}B}{B\,\mathrm{d}x} + \frac{c\,\mathrm{d}C}{C\,\mathrm{d}x} + \text{etc.}\right)$$

It follows that, unless one of the numbers a, b, c, etc., is divisible by the modulus, $\frac{\mathrm{d}X}{\mathrm{d}x}$ is divisible by $A^{a-1}B^{b-1}C^{c-1}$, etc., but not by A^a, B^b, C^c, etc. Hence the following

THEOREM. *If the common divisor of greatest degree of the functions X and $\frac{\mathrm{d}X}{\mathrm{d}x}$ is ξ, all the prime factors of ξ will also occur in X, each with a multiplicity $+1$ greater than in ξ. Thus, if X and $\frac{\mathrm{d}X}{\mathrm{d}x}$ are coprime functions, X will have no equal factors.*

369.

Example I. We ask whether the function

$$x^5 + 3x^4 - 6x^3 + 3x - 4 \ldots (X)$$

has equal divisors modulo 17. We have

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 5x^3 - xx + 3$$

From this we find that the functions X and $\frac{\mathrm{d}X}{\mathrm{d}x}$ are coprime, so X has no equal divisors.

Example II. Let

$$X \equiv x^5 + 6x^4 - 3x^3 - 4xx + 2x - 3 (\mathrm{mod.}\, 13)$$

Then

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 2x^3 + 4xx + 5x + 2$$

The greatest common divisor of the functions X, $\frac{\mathrm{d}X}{\mathrm{d}x}$ is $\equiv 5xx + 7x + 7$, or, on multiplication by 8: $xx + 4x + 4$. Since this divisor is $\equiv (x+2)^2$, the function X is divisible by $(x+2)^3$, and the quotient (which is $xx + 11$) contains no further double divisor.

370. 371.

If, by the preceding sections, the function X has been expressed as $A^a B^b C^c$, etc., with A, B, C, etc., coprime and the numbers a, b, c, etc., unequal, the resolution can be carried further. Let X, then, be a function containing no further equal divisors. We saw above that $x^p - x$ is the product of all prime functions of degree one. Let ξ be the common divisor of greatest degree of the functions X and $x^p - x$; then ξ is the product of all divisors of X of degree one, and $\frac{X}{\xi}$ has no further divisors of this kind. If, however, the functions X and $x^p - x$ are found to be coprime, X will have no divisor of degree one, and hence the congruence $X \equiv 0$ will have no real roots. Further, since $x^{pp} - x$ is the product of all prime functions of degrees two and one, the common divisor of greatest degree of the functions $x^{pp} - x$ and $\frac{X}{\xi}$, namely ξ', contains all divisors of X of degree two. Continuing in this way, we see that X is thus resolved into factors ξ, ξ', ξ'', etc., which contain all divisors of degrees one, two, three, etc., respectively.

372.

But if a product of several prime functions of the same degree is given, the individual functions must be found by trial. This problem is closely analogous to that of finding the factors of composite numbers. Here, however, it is determined a priori whether the given function can still be split into factors.

Since here too the number of all possible factors is finite, we can use an aid similar to the one above. But we do not wish to dwell on this matter, for an experienced calculator who has thoroughly grasped the principles will readily find particular devices when needed.

We proceed to another topic, namely the consideration of congruences when the modulus is not a prime number, as we have always assumed up to now. Here the case where the modulus is a power of a prime number especially deserves attention, both in itself and because it is needed to remove certain doubts (§.§. . .).

373.

PROBLEM. *If the function X has been resolved modulo p into coprime factors ξ, ξ', ξ'', etc., resolve X modulo pp into similar factors Ξ, Ξ', Ξ'', etc., so that*

$$\xi \equiv \Xi, \quad \xi' \equiv \Xi', \quad \xi'' \equiv \Xi'', \text{ etc. } (\mathrm{mod.}\, p)$$

Solution. Let $X \equiv \xi\psi (\mathrm{mod.}\, p)$, or equivalently $X = \xi\psi + p\Sigma$. Put

$$\Xi = \xi + p\varphi, \quad \Psi = \psi + p\omega$$

Then

$$\Xi\Psi = X - p\Sigma + (\varphi\psi + \xi\omega)p + pp\varphi\omega$$

Thus, if $\Xi\Psi$ is to be $\equiv X (\mathrm{mod.}\, pp)$, $\varphi\psi + \xi\omega - \Sigma$ must necessarily be divisible by p. But since ψ and ξ are coprime functions modulo p, φ and ω can be determined so that this condition is fulfilled (§. 336), and moreover so that the degrees of φ and ω are respectively one less than the degrees of the functions ξ, ψ. Hence $X \equiv \Xi\Psi (\mathrm{mod.}\, pp)$. It is clear that Ψ can again be split in the same way into factors $\Xi'\Omega$, with the factor Ξ' being $\equiv \xi' (\mathrm{mod.}\, p)$, and so on, until finally

$$X \equiv \Xi\, \Xi'\, \Xi'' \text{ etc. } (\mathrm{mod.}\, pp). \quad \text{Q. E. Fac.}$$

374.

From this it is easy to prove that the function X can also be resolved into factors modulo p^3, p^4, etc. More generally, let

$$X \equiv PQ(\mathrm{mod.}\, p^m) \quad \text{or} \quad X = PQ + p^m R$$

and let the function P be coprime to Q modulo p. On putting

$$P' = P + Ap^m, \quad Q' = Q + Bp^m$$

we have

$$P'Q' = X - p^m R + (AQ + BP)p^m + ABp^{2m}$$

Hence, for any modulus p^ν (with ν being $> m$ and $< 2m + 1$), we have

$$P'Q' \equiv X, \quad \text{if} \quad R \equiv AQ + BP(\mathrm{mod.}\, p^{\nu - m})$$

From this we see that, if the function X has no equal divisors modulo p, it can be split into factors modulo p^k in the same way as modulo p. But if X has equal divisors, the matter becomes much more complicated and cannot even be fully dealt with by the preceding principles. Since we cannot communicate everything belonging to this subject, we shall consider only one case, which occurs very often and whose resolution is needed to settle certain doubts in what precedes. This is the case where only equal factors of degree one are considered. It can also be used directly to find the roots of congruences. We shall treat the matter in general on another occasion.

375.

Let, then, $X \equiv X'(x - a)^m(\mathrm{mod.}\, p)$, and let the function X' be coprime to $x - a$: we seek all divisors of degree one congruent to $x - a$ modulo p that divide X modulo pp, p^3, etc. (We assume that the function X is not divisible by $x - a$ without a modulus; otherwise $x - a$ would divide the function X modulo every modulus.) If we substitute $z + a$ for x, we obtain

$$Z \equiv Z'z^m(\mathrm{mod.}\, p) \quad \text{or} \quad Z = Z'z^m + pA$$

Now, if Z is divisible modulo pp by some divisor of the form $z + \alpha p$, then A must be of the form $zZ'' + pB$. Unless this is so, the investigation is already finished. Let us therefore put

$$Z \equiv Z'z^m + pZ''z(\mathrm{mod.}\, pp)$$
$$\text{or} \quad Z = Z'z^m + pZ''z + ppB$$

It is clear that Z is divisible by z and by every other divisor congruent to it modulo p.

To fix our attention, we put $m = 4$; it is easy to see that every other case can be treated in a similar way. Now, if Z is divisible modulo p^3 by some divisor of the form $z + \alpha p$, we have

$$0 \equiv -\alpha pp Z'' + ppB(\text{modd. } z + \alpha p, p^3)$$
$$\text{or} \quad \alpha Z'' \equiv B(\text{modd. } z, p)$$

There can now be three cases

1) If $Z'' \equiv 0(\text{modd. } z, p)$ and B is not $\equiv 0$, then clearly no value of α satisfies the congruence, and hence Z has, modulo p^3, no divisor of the form $z + \alpha p$. The investigation is therefore finished

2) If neither Z'' nor B is $\equiv 0(\text{modd. } z, p)$, then α has a unique value, namely

$$\alpha \equiv \frac{B}{Z''}(\text{modd. } z, p).$$

Thus there is a unique divisor $\equiv z + \alpha p(\text{mod. } pp)$ of Z modulo p^3, and we have

$$Z \equiv V(z + \alpha p) + p^3 W$$

Now let the divisor of $Z(\text{mod. } p^4)$ be $z + \alpha p + \beta pp$; then

$$0 \equiv$$

REMARKS ON THE ANALYSIS RESIDUORUM.

The two preceding treatises are taken from an extensive manuscript entitled Analysis Residuorum, which probably dates from 1797 or 1798; a complete revision of it later gave rise to the Disquisitiones Arithmeticae. The full title of Chapter Six reads:

Solution of the congruence $x^m - 1 \equiv 0$ and the equation $x^m - 1 = 0$; with elucidations on the theory of regular polygons.

The essential content of its second part (§§. 253–278) passed into the seventh section of the Disqq. Arithm.

Chapter Seven is also partly preserved: Various Applications of Certain Preceding Investigations (§§. 279–302). It is divided into the following subsections:

On Transformations of Common Fractions (§§. 279–281).

On the Conversion of Common Fractions into Decimals (§§. 282–292).

On the Solution of the Indeterminate Equation $xx = a + by$ (§§. 293–297).

On the Solution of the Indeterminate Equation $axx + byy = c$ (§§. 298–301).

On Finding the Divisors of Numbers (§. 302; the following sheets are missing).

All this was incorporated almost word for word into the sixth section of the Disqq. Arithm.

The two sections given here treat the subjects which, as appears from the preface and Articles 11, 44, 61, 62, 65, 84 of the Disqq. Arithm., were intended to form the eighth section of that work. It should, however, be noted that this plan was later changed again: among the manuscripts is a fragment headed Section Eight: A Fuller Consideration of Certain Investigations Concerning the Division of the Circle. This fragment begins with Art. 367 and was therefore intended to continue the Disqq. Arithm.; but the content of the few articles still preserved later passed into the treatise Summatio quarundam serierum singularium, and for this reason the fragment is excluded from the present edition.

In the preceding printing of the two parts of the Analysis Residuorum, the original text has essentially been retained faithfully, although its form cannot be called ready for printing; the following remarks indicate the most important alterations and add some elucidations.

§. 237. Compare Disqq. Arithm. artt. 61, 62.

§. 239. Compare Disqq. Arithm. artt. 53, 54, 65.

§. 241. If $n = 2^\nu$ and $\nu \geqq 3$, there is indeed no number ρ of the stated kind, but this does not substantially change the investigation as a whole.

§. 251. The difficulty noted here was presumably to be removed by introducing higher powers of p as moduli. Compare §§. 363, 372, 373.

§. 332. The assumption that the modulus is a prime number is retained through §. 372 inclusive.

§. 338. The incomplete citation may refer to Disqq. Arithm. art. 44.

§§. 344–346. Of the two proofs present in the manuscript, the first, introduced by the words "we now set about proving" and based on a closer examination of the expressions $(1^\alpha 2^\beta 3^\gamma \ldots)$, has here been omitted entirely in accordance with the author's own instruction ("The whole preceding proof, together with another proof of the preceding theorem which we intended to add, is to be suppressed, because we have discovered another that is infinitely simpler. It rests on this foundation"); moreover, in the printing above the second proof has been shortened by considering the expansion of $\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x}$ instead of that of $\frac{x\,\mathrm{d}P}{\mathrm{d}x}$, thus also avoiding a reference in the original to the suppressed first proof.

§. 348. The expression radix prima is to be understood here in the same sense as radix propria in the treatise Summatio quarundam serierum singularum, art. 11. — The assertion that the coefficients $A'.B'\ldots$ of the expanded product are rational integers refers to Chapter Six, where, however, the theory of the equation $x^\tau - 1 = 0$ is treated only for the case where τ is prime; the form of the proof in §. 349 first leads to the following supplement. If the expanded product is put into the form (valid for all roots of the equation $\theta^\tau = 1$)

$$S = E + F\theta + \ldots + N\theta^{\tau-1}$$

then the coefficients $E, F \ldots N$ are polynomials in x with rational integer coefficients. Further, since the product remains unchanged when θ is replaced by θ^k, where k is any number coprime to τ, the same holds for the expression S. It follows without difficulty that all powers occurring in S of θ whose exponents s have one and the same greatest common divisor with τ must also have identical coefficients. Finally, since every sum of such powers θ^s is always an integer, it is evident that the expression S, and hence also the product in question, is a polynomial in x with integer coefficients, as was to be shown. This consideration also establishes the correctness of the remark at the end of the paragraph. Other reasons nevertheless suggest that the author already knew at that time the general theorem on the transformation of symmetric functions (Demonstratio nova altera theorematis omnem functionem etc. art. 4), from which the propositions above follow immediately.

§. 352. The notation $R \equiv S(\mathrm{mod.}\, P)$, or also $R \equiv S(\mathrm{mod.}\, P, p)$, means here and in what follows that the difference $R - S$ has, modulo p, the divisor P. — The incomplete citation may refer to Disqq. Arithm. art. 49.

§. 354. Multiplication by $x^\nu - 1$ shows that the sums of equal powers of the roots of the two equations $(P, \rho^{k\nu+t}) = 0$, $(P, \rho^t) = 0$ are congruent to one another $(\mathrm{mod.}\, p)$, and from this follows the congruence $(P, \rho^{k\nu+t}) \equiv (P, \rho^t)(\mathrm{mod.}\, p)$ as soon as $m < p$ (compare §. 244). But if $m \geqq p$, the coefficient of the power x^{m-p} in an equation can no longer be determined modulo p from the given power sums of its roots, because it carries the factor p in the formulas of NEWTON used for this purpose. Indeed, from the congruence of each pair of equal power sums of the roots of the equations $A = 0$, $B = 0$, one may in general infer only that $A \equiv \mathfrak{A}^p\mathfrak{C}$, $B = \mathfrak{B}^p\mathfrak{C}(\mathrm{mod.}\, p)$, where $\mathfrak{C}$ denotes the greatest common divisor of the two functions A, B modulo the prime number p, while $\mathfrak{A}$ and $\mathfrak{B}$ are entirely undetermined functions. Presumably the author derived the general validity of the proposition from the theory of the transformation of symmetric functions, and specifically from the following proposition: if, with respect to any modulus p, the difference $R(x) - S(x)$ is divisible by the function $P(x)$, and $a, b, c \ldots$ are the roots of the equation $P(x) = 0$, then the functions

$$(x - R(a))(x - R(b))(x - R(c)) \ldots \quad \text{and}$$
$$(x - S(a))(x - S(b))(x - S(c)) \ldots$$

are congruent to one another modulo p.

§. 355. It is shown in §. 368 that P and $\frac{\mathrm{d}P}{\mathrm{d}x}$ have no common divisor if P contains no factor more than once.

§§. 358, 359. The note placed below the text is taken from a separate sheet, which was probably intended to replace §. 359, already crossed out in the manuscript.

§. 360. An inaccuracy in the manuscript has been corrected in the statement of the theorem.

§. 361. Here the exponent $\frac{1}{k}$ in the notation $(\xi, \rho^{\frac{1}{k}})$ means any positive integer k' such that $kk' \equiv 1(\mathrm{mod.}\, \nu)$, where ν is the least positive integer for which $x^\nu - 1$ is divisible by ξ modulo p; it must be assumed here that ξ is not divisible by x modulo p, and also that k is coprime to ν. The correctness of the assertion that ξ' is divisible by $(\xi, \rho^{\frac{1}{k}})$ $(\mathrm{mod.}\, p)$ follows from §. 354.

§. 363. The concluding remark presumably concerns the introduction of moduli that are powers of the prime number p; compare §§. 251, 372, 373.

§. 367. The roots of the equation $x^3 + xx - 2x - 1 = 0$ are the periods of two terms into which the roots of the equation $\frac{x^7-1}{x-1} = 0$ divide. The same example also occurs on a separate sheet, where the principal result of §§. 362, 363 is stated under the title "the golden theorem".

§. 371. This paragraph was intended to contain an example, but it was not worked out.

R. Dedekind.

FURTHER DEVELOPMENT OF THE INVESTIGATIONS OF PURE EQUATIONS.

1.

The method by which, in Article 360 of the *Disquiss. Arithm.*, we showed how to solve the equation $x^n - 1 = 0$ forms a most fruitful and important theory, of which we could touch on only the first elements in that work. We therefore hope that mathematicians will welcome our taking up this subject here again, treating more fully what was only briefly sketched, in part with the proofs omitted, and pursuing in greater depth the developments made since that time.

The exponent n is assumed to be a prime number, and the number $n-1$ to be resolved into the factors $\alpha \times \beta \times \gamma$; further, we denote by g any primitive root modulo n. Let r denote an arbitrary root of the equation $x^n - 1 = 0$, and R an arbitrary root of the equation $x^\beta - 1 = 0$. Thus, denoting the circumference of the circle whose radius $= 1$ by P, and the imaginary quantity $\sqrt{-1}$ by i, all the roots of the equation $x^\beta - 1 = 0$, or all the values of R, will be represented by the formula

$$\cos \frac{kP}{\theta} + i \sin \frac{kP}{\theta}$$

where k ranges over the integers $0, 1, 2, 3 \ldots \beta - 1$. Further, all powers of any root R are evidently themselves roots, and if R is the root corresponding to a value of k coprime to β, all the powers $R^0, R, R^2, R^3 \ldots R^{\beta-1}$ are distinct from one another and thus exhaust the entire collection of roots. In this case we shall call R a *proper* root of the equation $x^\beta - 1 = 0$; conversely, a root R corresponding to a value of k that is not coprime to β will be called *improper*. It is readily seen that, if δ is the greatest common divisor of the numbers k and β, then $R^{\frac{\beta}{\delta}\cdot} = 1$, while all the powers $R^0, R, R^2, R^3 \ldots R^{\frac{\beta}{\delta}-1}$ are distinct from one another, so that R is a proper root of the equation $x^{\frac{\beta}{\delta}} - 1 = 0$. The same holds for the equation $x^n - 1 = 0$, but all its roots are necessarily proper except for the root 1.

2.

With these preliminaries, our investigation will chiefly concern functions of the following form, consisting of $\beta\gamma$ terms,

$$r + Rr^{g^\alpha} + R^2 r^{g^{2\alpha}} + R^3 r^{g^{3\alpha}} \ldots + R^{\beta\gamma-1} r^{g^{\alpha\beta\gamma-\alpha}}$$

which for brevity we shall denote by the symbol $[r, R]$. The individual terms of such an expression are products of powers of r and powers of R; the exponents of the former form a geometric progression, and those of the latter an arithmetic progression. The exponents

$$1, \quad g^\alpha, \quad g^{2\alpha}, \quad g^{3\alpha} \ldots\ldots g^{\alpha\beta\gamma-\alpha}$$

are all incongruent to one another modulo n, and hence those powers of r are distinct from one another; continued further, however, they would begin the same series again, since $g^{\alpha\beta\gamma} \equiv 1 (\mathrm{mod.}\, n)$, and hence $r^{g^{\alpha\beta\gamma}} = r$. The other factors,

$$1, \quad R, \quad R^2, \quad R^3 \ldots . R^{\beta\gamma-1}$$

form γ equal periods, since $R^\beta = 1$, $R^{\beta-1} = R$, etc. It follows that the function $[r, R]$ can also be represented as

$$\begin{aligned}
&r + r^{g^{\alpha\beta}} + r^{g^{2\alpha\beta}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta}} \\
&+ R\big(r^{g^\alpha} + r^{g^{\alpha\beta+\alpha}} + r^{g^{2\alpha\beta+\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta+\alpha}}\big) \\
&+ R^2\big(r^{g^{2\alpha}} + r^{g^{\alpha\beta+2\alpha}} + r^{g^{2\alpha\beta+2\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha\beta+2\alpha}}\big) \\
&+ \text{etc.} \\
&+ R^{\beta-1}\big(r^{g^{\alpha\beta-\alpha}} + r^{g^{2\alpha\beta-\alpha}} + r^{g^{3\alpha\beta-\alpha}} \ldots\ldots + r^{g^{\alpha\beta\gamma-\alpha}}\big).
\end{aligned}$$

or, introducing the notation of Article 343 of the Disq. Ar.,

$$[r, R] = (\gamma, 1) + R(\gamma, g^\alpha) + R^2(\gamma, g^{2\alpha}) \ldots + R^{\beta-1}(\gamma, g^{\alpha\beta-\alpha})$$

3.

If we take unity for the root r, we have

$$[1, R] = 1 + R + R^2 + R^3 \ldots + R^{\beta\gamma-1} = \gamma(1 + R + R^2 + R^3 \ldots + R^{\beta-1})$$

whose value will be $= \beta\gamma$ if R is also taken to be the root 1, but $= 0$ for every other value of R. Conversely, leaving r indeterminate and putting $R = 1$, we obtain $[r, 1] = r + r^{g^\alpha} + r^{g^{2\alpha}} + r^{g^{3\alpha}} \ldots + r^{g^{\alpha\beta\gamma-\alpha}}$, or, using the notation introduced in the Disq. Ar., $[r, 1] = (\beta\gamma, 1)$; that is, it will consist of a period of $\beta\gamma$ roots, one of which is r itself. Whenever $\alpha = 1$, this period will contain all the roots $r, r^2, r^3 \ldots r^{n-1}$, with only their order changed.

Note also the following relations, whose reason is evident:

$$[r, R] = R[r^{g^\alpha}, R] = R^2[r^{g^{2\alpha}}, R] \quad \text{or generally} \quad = R^k[r^{g^{\alpha k}}, R]$$

where k denotes any positive integer. It follows that the function $[r^m, R]$ either is $= [1, R]$, namely if m is divisible by n, or can be reduced in the remaining cases to the form $R^\mu[r^{g^\nu}, R]$, with $\nu < \alpha$. For if m is not divisible by n, it will be congruent modulo n to some power of g, whose exponent is conveniently expressed by $\text{ind.}\, m$, as in the Disq. Ar.; thus, putting $\text{ind.}\, m = \lambda\alpha + \nu$, which can evidently be done with $\nu < \alpha$, we obtain $[r^m, R] = [r^{g^{\lambda\alpha+\nu}}, R] = R^{-\lambda}[r^{g^\nu}, R]$. We must therefore set $\mu = -\lambda$ or, if you want a positive exponent, $\mu \equiv -\lambda (\text{mod.}\, \beta)$.

4.

THEOREM. *If r', like r, denotes an arbitrary root of the equation $x^n - 1 = 0$, and R', like R, an arbitrary root of the equation $x^\beta - 1 = 0$, the product will be*

$$\begin{aligned}[r, R] \times [r', R'] = \\ [rr', RR'] + R[r^{g^\alpha} r', RR'] + R^2[r^{g^{2\alpha}} r', RR'] \\ + R^3[r^{g^{3\alpha}} r', RR'] \ldots + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}} r', RR']\end{aligned}$$

Proof. By multiplying $[r, R]$ by the individual terms of $[r', R']$, the product can be represented in the form

$$\begin{aligned}&[r, R]r' + RR'[r^{g^\alpha}, R]r'^{g^\alpha} + R^2R'^2[r^{g^{2\alpha}}, R]r'^{g^{2\alpha}} \\ &+ R^3R'^3[r^{g^{3\alpha}}, R]r'^{g^{3\alpha}} \ldots \\ &+ R^{\beta\gamma-1}R'^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}}, R]r'^{g^{\alpha\beta\gamma-\alpha}}\end{aligned}$$

Then collecting the first terms of the individual parts, after duly expanding them, gives $[rr', RR']$; similarly, collecting the second terms gives $R[r^{g^\alpha} r', RR']$, and so on, finally producing the stated form of the product. Q. E. D.

Moreover, simply interchanging r, R with r', R' shows that the same product can also be put in the form

$$[rr', RR'] + R'[rr'^{g^\alpha}, RR'] + R'^2[rr'^{g^{2\alpha}}, RR'] + R'^3[rr'^{g^{3\alpha}}, RR'] \ldots + R'^{\beta\gamma-1}[rr'^{g^{\alpha\beta\gamma-\alpha}}, RR']$$

It follows further that, if r'', r''', etc., also denote arbitrary roots of the equation $x^n - 1 = 0$, and R'', R''', etc., arbitrary roots of the equation $x^\beta - 1 = 0$, the product of the functions $[r, R], [r', R'], [r'', R''], [r''', R'''],$ etc., however many there are, will equal the sum

$$\Sigma R'^{k'} R''^{k''} R'''^{k'''} \text{ etc.}$$
$$[rr'^{g^{\alpha k'}} r''^{g^{\alpha k''}} r'''^{g^{\alpha k'''}} \text{ etc.},\ RR'R''R''' \text{ etc.}]$$

For k', k'', k''', etc., we substitute all the numbers $0, 1, 2, 3 \ldots \beta\gamma - 1$, combined with one another in every possible different way. This gives altogether $\beta^{\mu-1}\gamma^{\mu-1}$ terms, if μ denotes the number of those functions multiplied together.

5.

The formula by which we expressed the product of any number of functions in the preceding article is general and assumes no relation between the roots r, r', r'', r''', etc., or between R, R', R'', R''', etc. We can readily deduce that, if the roots r', r'', r''', etc., may be regarded as powers of r, and the roots R', R'', R''', etc., as powers of R, each term of the product will have the form $R^M[r^m, R^\lambda]$, where the exponent λ is the same for every term, namely $R^\lambda = RR'R''R'''$, etc. Thus, by what we noted in Article 3, such a product reduces to the following form:

$$A[1, R^\lambda] + B[r, R^\lambda] + B'[r^g, R^\lambda] + B''[r^{g^2}, R^\lambda] + B'''[r^{g^3}, R^\lambda] + \text{etc.} + B^{(\alpha-1)}[r^{g^{\alpha-1}}, R^\lambda]$$

where each of the coefficients A, B, B', B'', B''', etc., will have the form

$$h + h'R + h''R^2 + h'''R^3 + \text{etc.} + h^{(\beta-1)}R^{\beta-1}$$

and h, h', h'', h''', etc., denote fixed integers.

The simplest case is that in which we put $r = r' = r'' = r'''$, etc., and also $R = R' = R'' = R'''$, etc.; our product then becomes the power $[r, R]^\lambda$, which therefore always reduces to the form given above.

6.

Thus, putting $\lambda = \beta$, the power $[r, R]^\beta$ takes the form

$$\begin{aligned} &A[1,1] + B[r,1] + B'[r^g,1] + \text{etc.} + B^{\alpha-1)}[r^{g^{\alpha-1}},1] \\ &= \beta\gamma A + B(\beta\gamma,1) + B'(\beta\gamma,g) + B''(\beta\gamma,g^2) + \text{etc.} \\ &\quad + B^{(\alpha-1)}(\beta\gamma,g^{\alpha-1}) = \theta' \end{aligned}$$

If, then, not only the value of the root R (and hence the values of the coefficients A, B, B', etc.) but also the values of the individual sums of $\beta\gamma$ terms $(\beta\gamma,1),(\beta\gamma,g)$, etc., are assumed known, the value of θ' will be known at once, and from it $[r, R]$ can be found by the formula $\sqrt[\beta]{\theta'}$. This expression admits β distinct values, so it might seem doubtful which one should be taken; but it is easily shown that this choice is entirely arbitrary whenever R is a *proper* root of the equation $x^\beta - 1 = 0$. For in this case those β values of the radical expression $\sqrt[\beta]{\theta'}$ are evidently

$$[r,R], \quad [r^{g^\alpha},R], \quad [r^{g^{2\alpha}},R] \ldots . [r^{g^{\alpha\beta-\alpha}},R]$$

since, by Article 3, the powers of these functions with exponent β are equal to one another, while the functions themselves are proportional to the β distinct roots of the equation $x^\beta - 1 = 0$. But as long as only the sums of $\beta\gamma$ terms $(\beta\gamma,1),(\beta\gamma,g)$, etc., are known, the root r itself is determined only to the extent that it must lie in the collection $(\beta\gamma,1)$, and it remains arbitrary which member of this collection we take for r. These roots are $r, r^{g^\alpha}, r^{g^{2\alpha}}$, etc., and therefore we can also take any of the functions $[r,R],[r^{g^\alpha},R],[r^{g^{2\alpha}},R]$, etc., for $[r, R]$.

These conclusions would not hold if R were not a proper root of the equation $x^\beta - 1 = 0$. For if R is assumed to be a proper root of the equation $x^{\beta'} - 1 = 0$, with β' a divisor of β, it is readily seen that

$$[r,R] = [r^{g^{\alpha\beta'}},R], \quad [r^{g^\alpha},R] = [r^{g^{\alpha\beta'+\alpha}},R] \text{ etc.}$$

so that in the collection of β functions $[r,R],[r^{g^\alpha},R] \ldots [r^{g^{\alpha\beta-\alpha}},R]$ only β' distinct functions occur, and therefore among the values of the expression $\sqrt[\beta]{\theta'}$ no more than β' are admissible, while the remaining $\beta - \beta'$ are extraneous. It is readily seen, however, that in this case we need not go as far as the power with exponent β of the function $[r, R]$ since already the power $[r, R]^{\beta'}$ reduces to our form

$$\beta\gamma A + B(\beta\gamma,1) + B'(\beta\gamma,g) + B''(\beta\gamma,g^2) \text{ etc.}$$

Thus we shall obtain $[r, R]$ by an expression such as $\sqrt[\beta']{\theta}$, and it will make no difference which value of this expression we take.

7.

In the same way as $[r, R]$, we can also determine the functions $[r, R^2]$, $[r, R^3]$, etc., or in general $[r, R^k]$. For if substituting in θ', in place of R, the powers R^2, R^3, etc., R^k, is assumed to give the functions θ'', θ''', etc., $\theta^{(k)}$, then evidently $[r, R^2]^\beta = \theta''$, $[r, R^3]^\beta = \theta'''$, etc., and in general $[r, R^k]^\beta = \theta^{(k)}$; hence these functions too can be expressed by radicals, $[r, R^2] = \sqrt[\beta]{\theta''}$, etc. But it is not suitable to use these radical expressions when a quantity is to be expressed by a function of $[r, R]$, $[r, R^2]$, etc. For since their individual values are not fully determined, it would remain doubtful which values could be combined with one another; yet this is evidently by no means arbitrary. It is readily seen that, as soon as a definite value is taken for $[r, R]$, all of $[r, R^2]$, $[r, R^3]$, etc., must also acquire fully determined values, which the radical expressions do not indicate. We must therefore set these expressions aside and seek others by which $[r, R^2]$, $[r, R^3]$, etc., can be expressed *rationally* in terms of $[r, R]$ and known quantities. We readily accomplish this as follows.

By the theorem of Article 4 and what we showed in Article 5, the product $[r, R^k] \times [r, R]^{\beta-k}$ also reduces to a form such as

$$\begin{aligned}&\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \text{etc.}\\ &\quad + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1})\end{aligned}$$

where A, B, B', B'', etc., are rational functions of R. Thus, putting the products

$$\begin{aligned}[r, R^2] \times [r, R]^{\beta-2} &= \vartheta''\\ [r, R^3] \times [r, R]^{\beta-3} &= \vartheta'''\\ [r, R^4] \times [r, R]^{\beta-4} &= \beta''''\\ &\text{etc.}\end{aligned}$$

the quantities $\vartheta'', \vartheta''', \vartheta''''$, etc., can also be determined rationally, and

$$\begin{aligned}[r, R^2] &= \frac{\vartheta''}{\theta'}[r, R]^2\\ [r, R^3] &= \frac{\vartheta'''}{\theta'}[r, R]^3\\ [r, R^4] &= \frac{\vartheta''''}{\theta'}[r, R]^4\\ &\text{etc.}\end{aligned}$$

These expressions therefore give the values of the functions $[r, R^2]$, $[r, R^3]$, etc., rationally, provided that we do not have $[r.R] = 0$; if this equality held, they would become indeterminate. But we can rigorously prove that $[r, R] = 0$ can never occur whenever r denotes a root different from 1, although we must reserve the presentation of this proof for another occasion, so as not to become too lengthy here.

8.

What we set out in the preceding articles is useful when the aim is to descend from periods of $\beta\gamma$ terms to periods of γ terms. For it is readily seen that, if R denotes a proper root, we have

$$\begin{aligned}
\beta(\gamma,1) &= (\beta\gamma,1) + [r,R] + [r,R^2] + [r,R^3] + \text{etc.} + [r,R^{\beta-1}] \\
\beta(\gamma,g^\alpha) &= (\beta\gamma,1) + R^{\beta-1}[r,R] + R^{\beta-2}[r,R^2] \\
&\quad + R^{\beta-3}[r,R^3] + \text{etc.} + R[r,R^{\beta-1}] \\
\beta(\gamma,g^{2\alpha}) &= (\beta\gamma,1) + R^{2\beta-2}[r,R] + R^{2\beta-4}[r,R^2] \\
&\quad + R^{2\beta-6}[r,R^3] + \text{etc.} + R^2[r,R^{\beta-1}] \\
&\text{etc.}
\end{aligned}$$

If here, for the individual $[r,R]$, $[r,R^2]$, etc., we took the radical expressions $\sqrt[\beta]{\theta'}$, $\sqrt[\beta]{\theta''}$, etc., the value of each series would be uncertain among $\beta^{\beta-1}$ values; by contrast, when the rational expressions for $[r,R^2]$, etc., are taken, it will be subject to no ambiguity other than that which is unavoidable by the nature of the matter. This observation seems to have escaped the attention of the illustrious LAGRANGE, who thought he had *simplified* our method given in Article 360 of the Disquis. arithm., where we had deliberately passed over radical expressions and proposed only rational ones, by substituting the former for the latter (Traité de la résolution numérique des équations; edition 2, p. 311).

Moreover, it hardly needs mentioning here that, as soon as the values of the periods $(\gamma,1)$, (γ,g^α), etc., or of just one of them, have been found, the values of all the remaining periods of γ terms can be deduced rationally from them. Thus the descent from periods of $\beta\gamma$ terms to periods of γ terms requires solving the equations $x^\beta = 1$, $x^\beta = \theta'$, and the remaining operations are performed rationally.

9.

All this had already been treated in almost the same way in the Disquis. Ar.; some things, however, had been added there with their proof omitted, and we think it appropriate to supply that proof here. We stated there that finding the value of the radical quantity $\sqrt[\beta]{\theta'}$, which, since θ' is an imaginary quantity, seems to require dividing both a ratio and an angle into β parts, depends on the latter alone, and that the former can always be reduced to extracting a single square root. We prove this as follows.

Denoting the imaginary quantity $\sqrt{-1}$ by i, as above, and writing $\theta' = P + iQ$ and $\sqrt[\beta]{\theta'} = p + iq$, using any one value of the radical and taking P, Q, p, q to be real, it is known that, if the positive quantities E, e and the angles F, f are determined so that $P = E\cos F$, $Q = E\sin F$, $p = e\cos f$, $q = e\sin f$, then $e = \sqrt[\beta]{E}$, and f equals one of the angles

$$\frac{1}{\beta}F, \quad \frac{1}{\beta}(F + 360^0), \quad \frac{1}{\beta}(F + 720^0) \ldots . \frac{1}{\beta}(F + (\beta - 1)360^0)$$

Thus f· ger is determined by division of the angle F into β parts, but we can avoid extracting the root $\sqrt[\beta]{E}$ as follows. Every product $r^k R^K$ has the same real part as $r^{-k}R^{-K}$, while the imaginary parts containing the factor i in these products are equal and opposite. It follows at once that $[r^{-1}, R^{-1}] = p - iq = e(\cos f - i\sin f)$, and hence

$$[r, R] \times [r^{-1}, R^{-1}] = e^2$$

But by the theorem of Article 4 this product becomes

$$\begin{aligned} &= [1,1] + R[r^{g^\alpha - 1}, 1] + R^2[r^{g^{2\alpha}-1}, 1] + \text{etc.} \\ &\quad + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}-1}, 1] \\ &= \beta\gamma + R(\beta\gamma, g^\alpha - 1) + R^2(\beta\gamma, g^{2\alpha} - 1) + \text{etc.} \\ &\quad + R^{\beta\gamma-1}(\beta\gamma, g^{\alpha\beta\gamma-\alpha} - 1) \end{aligned}$$

This quantity can be determined if R and all the periods of $\beta\gamma$ terms are assumed known. Determining e therefore requires only the extraction of a square root.

In the special case $\alpha = 1$, the individual periods $(\beta\gamma, g^\alpha - 1)$, $(\beta\gamma, g^{2\alpha} - 1)$, etc., are evidently $= r + r^2 + r^3 + r^4 + \text{etc.} + r^{n-1}$, and hence

$$\begin{aligned} ee &= \beta\gamma + (R + R^2 + R^3 + \text{etc.} + R^{\beta\gamma-1})(r + r^2 + r^3 + \text{etc.} + r^{n-1}) \\ &= \beta\gamma + 1 = n \end{aligned}$$

provided that r and R are assumed to denote roots different from 1, and therefore we always have $e = \sqrt{n}$ (Disq. arithm., end of Article 360).

10.

So far we have conducted our investigation in the greatest generality, to cover all values of the numbers α, β, γ; from now on, however, we shall pass to the more restricted case $\alpha = 1$, which will open the way to most fruitful and elegant investigations. Thus the symbol $[r, R]$ will denote the function

$$r + Rr^g + R^2 r^{g^2} + R^3 r^{g^3} + \text{etc.} + R^{n-2} r^{g^{n-2}}$$

where n is a prime number, r an arbitrary root of the equation $x^n - 1 = 0$ (the root 1 not excluded), R an arbitrary root of the equation $x^\beta - 1 = 0$, with β denoting a given divisor of $n - 1$, and finally g an integer that is a fixed primitive root modulo n. For brevity we shall also write

$$1 + r + r^2 + r^3 + \text{etc.} + r^{n-1} = s$$
$$1 + R + R^2 + R^3 + \text{etc.} + R^{n-2} = S$$

from which it is evident that s becomes $= n$ for $r = 1$, but $s = 0$ for every other value of r, and similarly $S = n - 1$ for $R = 1$, but $S = 0$ for every other value of R.

By Article 3 we therefore have $[1, R] = S$, $[r, 1] = s - 1$; further, for every integer value of m not divisible by n, $[r^m, R] = R^{-\operatorname{ind} m}[r, R]$, or more generally $[r^m, R^M] = R^{-M \operatorname{ind} m}[r, R^M]$, where $\operatorname{ind} m$ is the exponent of the power of g congruent modulo n to m. Applying this transformation to what we showed in Article 5, we find that a product of two or more functions such as $[r^h, R^H]$ reduces to the form

$$A[1, R^\lambda] + B[r, R^\lambda]$$

where A and B are rational functions of R with integer coefficients, and λ is the sum of all the values of H. It will be of great importance to put such transformations into an efficient algorithm; for this purpose we must first consider more closely the nature of the product of two functions.

11.

The product $[r, R^\mu] \times [r, R^\nu]$ becomes, by the theorem of Article 4, =

$$[r^2, R^{\mu+\nu}] + R^\mu [r^{g+1}, R^{\mu+\nu}] + R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] + R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] + \text{etc.} + R^{(n-2)\mu}[r^{g^{n-2}+1}, R^{\mu+\nu}]$$

Among the $n-1$ exponents $2, g+1, g^2+1, g^3+1$, etc., $g^{n-2}+1$, exactly one is divisible by n, namely $g^{\frac{1}{2}(n-1)}+1$, so that the corresponding term of our sum will be $R^{\frac{1}{2}(n-1)\mu}[1, R^{\mu+\nu}]$. This term will be $= 0$ whenever we do not have $R^{\mu+\nu} = 1$, and $= (n-1)R^{\frac{1}{2}(n-1)\mu} = \pm(n-1)$ for $R^{\mu+\nu} = 1$. The remaining parts of our sum, whose sum we shall put $= \Omega$, are transformed as follows:

$$\begin{aligned}
[r^2, R^{\mu+\nu}] &= R^{-(\mu+\nu)\,\mathrm{ind}\,2}[r, R^{\mu+\nu}] \\
R^\mu[r^{g+1}, R^{\mu+\nu}] &= R^{\mu-(\mu+\nu)\,\mathrm{ind}(g+1)}[r, R^{\mu+\nu}] \\
R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] &= R^{2\mu-(\mu+\nu)\,\mathrm{ind}(g^2+1)}[r, R^{\mu+\nu}] \\
R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] &= R^{3\mu-(\mu+\nu)\,\mathrm{ind}(g^3+1)}[r.R^{\mu+\nu}] \\
&\text{etc.}
\end{aligned}$$

From this we obtain

$$\text{I.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu\,\mathrm{ind}\,x-(\mu+\nu)\,\mathrm{ind}(x+1)}$$

if for x we successively substitute the values $1, g, g^2, g^3 \ldots . g^{n-2}$, except for $g^{\frac{1}{2}(n-1)}$, or, which evidently amounts to the same thing, if for x we substitute the values $1, 2, 3, 4 \ldots . n-2$, since these values are congruent to those modulo n, though their order is changed.

Taking the integer y inverse to x modulo n, that is, determined so that $xy \equiv 1 \pmod{n}$, we have $\mathrm{ind}\,x \equiv -\mathrm{ind}\,y \pmod{n-1}$ and $\mathrm{ind}(x+1)+\mathrm{ind}\,y \equiv \mathrm{ind}(xy+y) \equiv \mathrm{ind}(1+y) \pmod{n-1}$; hence

$$\begin{aligned}
\mu\,\mathrm{ind}\,x - (\mu+\nu)\,\mathrm{ind}(x+1) &\equiv -\mu\,\mathrm{ind}\,y - (\mu+\nu)\{\mathrm{ind}(y+1) - \mathrm{ind}\,y\} \\
&\equiv \nu\,\mathrm{ind}\,y - (\mu+\nu)\,\mathrm{ind}(y+1)
\end{aligned}$$

Therefore, since the inverses of $1, 2, 3 \ldots n-2$ coincide with these same numbers, with only their order changed, we also have

$$\text{II.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\nu\,\mathrm{ind}\,y-(\mu+\nu)\,\mathrm{ind}(y+1)}$$

substituting for y successively the numbers $1, 2, 3 \ldots n-2$. The same formula follows directly from I, since the numbers μ, ν can evidently be interchanged.

Finally, taking the integer z inverse to $x+1$ modulo n, or $xz+z \equiv 1 \pmod{n}$, we have $\operatorname{ind}(1-z) \equiv \operatorname{ind} x + \operatorname{ind} z \pmod{n-1}$, $\operatorname{ind}(x+1) \equiv -\operatorname{ind} z \pmod{n-1}$, and hence

$$\begin{aligned}\mu \operatorname{ind} x - (\mu+\nu)\operatorname{ind}(x+1) &\equiv \mu(\operatorname{ind}(1-z) - \operatorname{ind} z) + (\mu+\nu)\operatorname{ind} z \\ &\equiv \mu \operatorname{ind}(1-z) + \nu \operatorname{ind} z\end{aligned}$$

Thus, as x runs through the values $1, 2, 3 \ldots n-2$, the number z must run through the values $2, 3, 4 \ldots n-1$, though in another order, and we obtain the third expression

$$\text{III.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(1-z) + \nu \operatorname{ind} z}$$

substituting for z successively the values $2, 3, 4 \ldots n-1$, or, if you prefer,

$$\begin{aligned}\text{IV.} \qquad \Omega &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(n+1-z) + \nu \operatorname{ind} z} \\ &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind} z + \nu \operatorname{ind}(n+1-z)}\end{aligned}$$

Since $\operatorname{ind}(1-z) = \frac{1}{2}(n-1) + \operatorname{ind}(z-1)$, our product can also be represented as follows:

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] &= R^{\frac{1}{2}(n-1)\mu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind}(z-1) + \nu \operatorname{ind} z}\} \\ &= R^{\frac{1}{2}(n-1)\nu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind} z + \nu \operatorname{ind}(z-1)}\}\end{aligned}$$

where z is always understood to take the values $2, 3, 4 \ldots . n-1$.

Moreover, in all these formulas the numbers

$$\mu \operatorname{ind} x - (\mu+\nu)\operatorname{ind}(x+1), \quad \nu \operatorname{ind} y - (\mu+\nu)\operatorname{ind}(y+1), \quad \mu \operatorname{ind}(1-z) + \nu \operatorname{ind} z$$

etc., can evidently be replaced by their least residues modulo β.

If $\mu + \nu \equiv 0 \pmod{\beta}$, we have

$$\begin{aligned}[r, R^{\mu}][r, R^{\nu}] = (n-1)R^{\frac{1}{2}(n-1)\mu} &\\ + (r + r^2 + r^3 + \cdots + r^{n-1}) &\\ \times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(n-2)\mu} - R^{\frac{1}{2}(n-1)\mu}) &\end{aligned}$$

12.

The product $[1, R^\mu] \times [r, R^\nu]$ becomes, by the theorem of Article 4,

$$= [r, R^{\mu+\nu}] + R^\mu [r, R^{\mu+\nu}] + R^{2\mu} [r, R^{\mu+\nu}] + \text{etc.} + R^{(n-2)\mu} [r, R^{\mu+\nu}]$$
$$= [r, R^{\mu+\nu}] \times (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{etc.} + R^{(n-2)\mu})$$
$$= [r, R^{\mu+\nu}] \times \frac{n-1}{\beta} (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{etc.} + R^{(\beta-1)\mu})$$

From this the product $[1, R^\mu] \times [1, R^\nu]$ expands into

$$\frac{n-1}{\beta} [1, R^{\mu+\nu}] \times (1 + R^\mu + R^{2\mu} + R^{3\mu} + \text{etc.} + R^{(\beta-1)\mu})$$

The general product $[r^m, R^\mu] \,.\, [r^{m'}, R^{\mu'}]$ can now be found without difficulty. For $[r^m, R^\mu] = R^{-\mu \operatorname{ind} m} [r, R^\mu]$ when the value of m is not divisible by n, and $= [1, R^\mu]$ when it is divisible; and since a similar transformation holds for the other factor $[n^{m'}, R^{\mu'}]$, the multiplication reduces either to the problem of the preceding article or to the cases considered in this article.

13.

Now that we have shown how to expand a product of two factors, expanding a product of more factors will present no difficulty. Once the product $[r, R^\mu] \times [r, R^\nu]$ has been reduced to the form $A[1, R^{\mu+\nu}] + B[r, R^{\mu+\nu}]$, it is evident that, on introducing a third factor $[r, R^\pi]$, the product becomes $= C[1, R^{\mu+\nu+\pi}] + D[r, R^{\mu+\nu+\pi}]$ if we put

$$[r, R^{\mu+\nu}][r, R^\pi] = c[1, R^{\mu+\nu+\pi}] + d[r, R^{\mu+\nu+\pi}]$$

and

$$C = Bc$$
$$D = Bd + A\{1 + R^{\mu+\nu} + R^{2\mu+2\nu} + \text{etc.} + R^{(n-2)(\mu+\nu)}\}$$

Thus $[r, R]^\lambda$ can easily be reduced to the form $A[1, R^\lambda] + B[r, R^\lambda]$.

As an example, we shall expand the powers of the function $[r, R]$ for $n = 11$, $\beta = 5$, setting $g = 2$. The following indices then correspond to the numbers:

numbers	1.2.3.4.5.6.7.8.9.10
indices	0.1.8.2.4.9.7.3.6. 5

Thus, to expand the square $[r, R]^2$ by formula I of Article 11, we have

$$\mu = 1, \quad \nu = 1$$

values of x ...	1. 2.3.4. 5. 6.7. 8. 9
$\operatorname{ind} x$ ...	0. 1.8.2. 4. 9.7. 3. 6
$2 \operatorname{ind}(x+1)$ ...	2.16.4.8.18.14.6.12.10
Least residues of	$\operatorname{ind} x - 2 \operatorname{ind}(x+1)$
modulo 5 ...	3. 0.4.4. 1. 0.1. 1. 1

from which we deduce

$$\Omega = [r, R^2] \times \{2 + 4R + R^3 + 2R^4\}$$

and

$$1^0. \qquad [r, R]^2 = [1, R^2] + [r, R^2] \times \{2 + 4R + R^3 + 2R^4\}$$

The same expression follows from formula III of Article 11, namely

values of z ...	2.3.4.5.6.7.8.9. 10
$\operatorname{ind} z$ ...	1.8.2.4.9.7.3.6. 5
$\operatorname{ind}(n+1-z)$ ...	5.6.3.7.9.4.2.8. 1
least residues of	$\operatorname{ind} z + \operatorname{ind}(n+1-z)$
modulo 5 ...	1.4.0.1.3.1.0.4. 1

In exactly the same way we find

$$2^0. \qquad [r, R^2] \,.\, [r, R] = [1, R^3] + [r, R^3] \times \{2 + R + 4R^2 + 2R^3\}$$
$$3^0. \qquad [r, R^3] \,.\, [r, R] = [1, R^4] + [r, R^4] \times \{2 + 4R + R^3 + 2R^4\}$$

Finally, we obtain

$$4^0. \qquad [r, R^4] \,.\, [r, R] = [1, 1] + [r, 1] \times \{1 + 2R + 2R^2 + 2R^3 + 2R^4\}$$

Multiplying equation 1^0 by $[r, R]$ and substituting for $[r, R^2] \,.\, [r, R]$ its value from 2^0, and using

$$[1, R^2] \,.\, [r, R] = [r, R^3] \,.\, \{2 + 2R + 2R^2 + 2R^3 + 2R^4\}$$

we deduce

$$\begin{aligned}[r, R]^3 = {} & [1, R^3] \times \{2 + 4R + R^3 + 2R^4\} \\ & + [r, R^3] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\}\end{aligned}$$

and in the same way

$$\begin{aligned}[r, R]^4 = {} & [1, R^4] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\} \\ & + [r, R^4] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ [r, R]^5 = {} & [1, 1] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ & + [r, 1] \times \{1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4\} \\ = {} & 1640 + 1700R + 2050R^2 + 1800R^3 + 1900R^4 \\ & + (1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4)(s - 1) \\ = {} & 918Ss - 98S - (6R + 41R^2 + 16R^3 + 26R^4)s \\ & + 66R + 451R^2 + 176R^3 + 286R^4\end{aligned}$$

14.

The calculation in the preceding articles' was carried out so that it could be extended to all values of r and R. It becomes considerably shorter if we regard R from the outset as a proper root of the equation $x^\beta - 1 = 0$. Under this assumption the product $[r, R^\mu] \times [r, R^\nu]$ reduces to the form $B[r, R^{\mu+\nu}]$ whenever $\mu + \nu$ is not divisible by β; but when $\mu + \nu$ is divisible by β, that product becomes $= (n-1)R^{\frac{1}{2}(n-1)\mu} + [r, 1]\Sigma R^{\mu \operatorname{ind} x}$, substituting for $\operatorname{ind} x$ all the numbers $0, 1, 2, 3 \ldots . n-2$ except $\frac{1}{2}(n-1)$. It follows easily that in this case, if μ and therefore also ν are not divisible by β, we have

$$[r, R^\mu] \,.\, [r, R^\nu] = R^{\frac{1}{2}(n-1)\mu}\{n - 1 - [r, 1]\}$$

and hence $= 0$ for $r = 1$, and $= nR^{\frac{1}{2}(n-1)\mu}$ for every other value of r. Moreover, since $R^{\frac{1}{2}(n-1)\mu}$ becomes $= +1$ or $= -1$ according as $\frac{n-1}{\beta} \,.\, \mu$ is even or odd, our product becomes $= n$ in the former case and $= -n$ in the latter.

It further follows that we can put

$$\begin{aligned} [r, R]^2 &= A'[r, R^2] \\ [r, R^2] \,.\, [r, R] &= A''[r, R^3] \\ [r, R^3] \,.\, [r, R] &= A'''[r, R^4] \end{aligned}$$

and so on, up to

$$[r, R^{\beta-2}] \,.\, [r, R] = A^{(\beta-2)}[r, R^{\beta-1}]$$

from which we have

$$\begin{aligned} [r, R]^2 &= A'[r, R^2] \\ [r, R]^3 &= A'A''[r, R^3] \\ [r, R]^4 &= A'A''A'''[r, R^4] \end{aligned}$$

and so on. Finally,

$$[r, R]^\beta = \pm nA'A''A''' \ldots A^{(\beta-2)}$$

where the upper or lower sign is to be taken according as $\frac{n-1}{\beta}$ is even or odd.

It is therefore evident that, once the value of $[r, R]$ has been found, the remaining functions

$$[r, R^2] = \frac{[r, R]^2}{A'}, \quad [r, R^3] = \frac{[r, R]^3}{A'A''} \quad \text{etc.}$$

can be determined here much more readily than in the cases where the condition $\alpha = 1$ does not hold, as we already noted in the *Disq. Ar.* (Article 360, III). A fuller consideration of the nature of the functions A', A'', etc., makes these operations still easier.

15.

In Article 9 we showed that the value of the function $[r, R]$ can be reduced to the form $\sqrt{n}(\cos f + i \sin f)$, and in the same way the functions $[r, R^2]$, $[r, R^3]$, etc., up to $[r, R^{\beta-1}]$, can be reduced to a similar form. Let us put

$$\begin{aligned} [r, R] &= \sqrt{n}(\cos f' + i \sin f') \\ [r, R^2] &= \sqrt{n}(\cos f'' + i \sin f'') \\ [r, R^3] &= \sqrt{n}(\cos f''' + i \sin f''') \\ &\text{etc.} \end{aligned}$$

Then

$$\begin{aligned} A' &= \sqrt{n}(\cos(2f' - f'') + i \sin(2f' - f'')) \\ A'' &= \sqrt{n}(\cos(f' + f'' - f''') + i \sin(f' + f'' - f''')) \\ A''' &= \sqrt{n}(\cos(f' + f''' - f'''') + i \sin(f' + f''' - f'''')) \\ &\text{etc.} \end{aligned}$$

It is evident from this that, if the functions A', A'', A''', etc., are reduced to the forms

$$\begin{aligned} A' &= a'(\cos b' + i \sin b') \\ A'' &= a''(\cos b'' + i \sin b'') \\ A''' &= a'''(\cos b''' + i \sin b''') \\ &\text{etc.} \end{aligned}$$

with all of a', a'', a''', etc., positive, we shall have

$$\begin{aligned} a' &= a'' = a''' \text{ etc.} = \sqrt{n} \\ f' &= \frac{1}{\beta}(b' + b'' + b''' + \text{etc.} + b^{(\beta-2)}) \end{aligned}$$

if $\frac{n-1}{\beta}$ is even, or

$$f' = \frac{1}{\beta}(180^0 + b' + b'' + \text{etc.} + b^{(\beta-2)})$$

if $\frac{n-1}{\beta}$ is odd, and then

$$\begin{aligned} [r, R] &= \sqrt{n}(\cos f' + i \sin f') \\ [r, R^2] &= \sqrt{n}(\cos(2f' - b') + i \sin(2f' - b')) \\ [r, R^3] &= \sqrt{n}(\cos(3f' - b' - b'') + i \sin(3f' - b' - b'')) \\ &\text{etc.} \end{aligned}$$

Finally, by the formulas of Article 8,

$$\left(\frac{n-1}{\beta},1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{\cos f'' + \cos(2f' - b') + \cos(3f' - b' - b'') + \text{etc.}$$
$$+ \cos((\beta-1)f' - b' - b'' - b''' - \text{etc.} - b^{(\beta-2)})\}$$
$$+ \frac{i\sqrt{n}}{\beta}\{\sin f' + \sin(2f' - b') + \sin(3f' - b' - b'') + \text{etc.}\}$$

and similarly we obtain the values of the functions $\left(\frac{n-1}{\beta},g\right)$, $\left(\frac{n-1}{\beta},g^2\right)$, $\left(\frac{n-1}{\beta},g^3\right)$, etc., if in this formula f' is replaced respectively by $f' - \frac{360^0 k}{\beta}$, $f' - 2\frac{360^0 k}{\beta}$, $f' - 3\frac{360^0 k}{\beta}$, etc., assuming $R = \cos\frac{360^0 k}{\beta} + i\sin\frac{360^0 k}{\beta}$.

16.

A further simplification follows from the observation below. Since by Article 14 we have

$$\pm[r,R][r,R^{\beta-1}] = [r,R^2][r,R^{\beta-2}] = \pm[r,R^3][r,R^{\beta-3}] \text{ etc.} = n$$

taking [in the first, third, etc., product] the upper or lower sign according as $\frac{n-1}{\beta}$ is even or odd, in the former case we must have

$$\cos(f' + f^{(\beta-1)}) = \cos(f'' + f^{(\beta-2)}) = \cos(f''' + f^{(\beta-3)}) \text{ etc.} = 1$$

in the latter

$$-\cos(f' + f^{(\beta-1)}) = \cos(f'' + f^{(\beta-2)}) = -\cos(f''' + f^{(\beta-3)}) \text{ etc.} = 1$$

and in both cases

$$\sin(f' + f^{(\beta-1)}) = \sin(f'' + f^{(\beta-2)}) = \sin(f''' + f^{(\beta-3)}) \text{ etc.} = 0$$

We may therefore put, in the former case,

$$f^{(\beta-1)} = -f', \quad f^{(\beta-2)} = -f'', \quad f^{(\beta-3)} = -f''' \quad \text{etc.}$$

in the latter

$$f^{(\beta-1)} = 180^0 - f', \quad f^{(\beta-2)} = -f'', \quad f^{(\beta-3)} = 180^0 - f''' \quad \text{etc.}$$

From this it follows that, in the former case,

$$b^{(\beta-2)} = b', \quad b^{(\beta-3)} = b'', \quad b^{(\beta-4)} = b''' \quad \text{etc.}$$
$$A^{(\beta-2)} = A', \quad A^{(\beta-3)} = A'', \quad A^{(\beta-4)} = A''' \quad \text{etc.}$$

and in the latter

$$b^{(\beta-2)} = b' - 180^0, \quad b^{(\beta-3)} = b'' + 180^0, \quad b^{(\beta-4)} = b''' - 180^0 \quad \text{etc.}$$
$$A^{(\beta-2)} = -A', \qquad A^{(\beta-3)} = -A'', \qquad A^{(\beta-4)} = -A''' \quad \text{etc.}$$

so that the number of functions A', A'', A''', etc., is reduced by half. It further follows that, in the former case,

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{etc.} + 2b^{(\frac{1}{2}\beta-1)})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos f' + 2\cos(2f' - b') \\ &+ 2\cos(3f' - b' - b'') + \text{etc.} \\ &+ 2\cos((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{8}\beta-2)}) \\ &+ \cos(\tfrac{1}{2}\beta f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-1)})\}\end{aligned}$$

(where the last term is evidently $= \cos 0 = 1$) or

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{etc.} + 2b^{(\frac{1}{2}(\beta-3))} + b^{(\frac{1}{2}(\beta-1))})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos f' + 2\cos(2f' - b') \\ &+ 2\cos(3f' - b' - b'') + \text{etc.} \\ &+ 2\cos(\tfrac{1}{2}(\beta - 1)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}(\beta-3))})\}\end{aligned}$$

according as β is even or odd; and in the latter case,

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{etc.} + 2b^{(\frac{1}{2}\beta-1)})$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \text{etc.} \\ &+ 2\cos((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-3)}) \\ &+ \cos(\tfrac{1}{2}\beta f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-1)})\} \\ + i\frac{\sqrt{n}}{\beta}\{&2\sin f' + 2\sin(3f' - b' - b'') + \text{etc.} \\ &+ 2\sin((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-2)})\}\end{aligned}$$

or

$$f' = \frac{1}{\beta}(2b' + 2b'' + \text{etc.} + 2b^{(\frac{1}{2}\beta-1)} + 180^0)$$

$$\begin{aligned}\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \text{etc.}\\ &+ 2\cos((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-2)})\}\\ + i\frac{\sqrt{n}}{\beta}\{&2\sin f' + 2\sin(3f' - b' - b'') + \text{etc.}\\ &+ 2\sin((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-3)})\\ &+ \sin(\tfrac{1}{2}\beta f' - b' - b'' - \text{etc.} - b^{(\frac{1}{2}\beta-1)})\}\end{aligned}$$

according as $\frac{1}{2}\beta$ is even or odd. What we noted above also holds for the remaining periods of $\frac{n-1}{\beta}$ terms. In general, therefore, we conclude that determining these periods requires the division of the whole circle into β parts, on which the construction of the angles b', b'', b''', etc., depends rationally; then the division of the angle $b' + b'' + b''' + \text{etc.}$ into β parts; and finally the square root $\sqrt{n}$. If we set $\beta = \frac{1}{2}(n-1)$ at once, those periods evidently coincide with twice the cosines of the angles $\frac{360^0}{n}$, $2\frac{360^0}{n}$, $3\frac{360^0}{n}$, etc., up to $\frac{1}{2}(n-1)\frac{360^0}{n}$, so that dividing the circle into n parts depends on dividing the whole circle into $\frac{1}{2}(n-1)$ parts, dividing an angle that can be constructed after that division into $\frac{1}{2}(n-1)$ parts, and the radical quantity $\sqrt{n}$. If we intend to proceed as far as the sines of the angles $\frac{360^0}{n}$, etc., one further operation will be needed.

17.

For a clearer illustration, let us return to the example of Article 13, where we found

$$A' = A''' = 2 + 4R + R^3 + 2R^4 = 2R - 2R^2 - R^3$$
$$A'' = 2 + R + 4R^2 + 2R^3 = -R + 2R^2 - 2R^4$$

Taking R to have the value $\cos 72^0 + i \sin 72^0$, we obtain

$$A' = A''' = 2\cos 72^0 - 3\cos 144^0 + i(2\sin 72^0 - \sin 144^0)$$
$$A'' = -3\cos 72^0 + 2\cos 144^0 + i(\sin 72^0 + 2\sin 144^0)$$

The angles b', b'' will therefore be determined by the equations

$$1) \qquad \sin b' = \frac{2\sin 72^0 - \sin 144^0}{\sqrt{11}}$$
$$2) \qquad \cos b' = \frac{2\cos 72^0 - 3\cos 144^0}{\sqrt{11}}$$
$$3) \qquad \operatorname{tang} b' = \frac{2\sin 72^0 - \sin 144^0}{2\cos 72^0 - 3\cos 144^0}$$
$$4) \qquad \sin b'' = \frac{\sin 72^0 + 2\sin 144^0}{\sqrt{11}}$$
$$5) \qquad \cos b'' = \frac{-3\cos 72^0 + 2\cos 144^0}{\sqrt{11}}$$
$$6) \qquad \operatorname{tang} b'' = \frac{\sin 72^0 + 2\sin 144^0}{-3\cos 72^0 + 2\cos 144^0}$$

Any one of the equations $1, 2, 3$ suffices to determine the angle b', provided the quadrant in which it is to be taken is known; this must be decided from the signs of the quantities $2\sin 72^0 - \sin 144^0$, $2\cos 72^0 - 3\cos 144^0$. The same holds for the angle b''. In our case b' is to be taken between 0 and 90^0, and b'' between 90^0 and 180^0. If the numerator and denominator of equation 3 are multiplied by $-3\cos 72^0 + 2\cos 144^0$, it becomes

$$\operatorname{tang} b' = \frac{2}{31}\{-\sin 72^0 + 13\sin 144^0\}$$

Similarly, from equation 6, on multiplying the numerator and denominator by $2\cos 72^0 - 3\cos 144^0$, we obtain

$$\operatorname{tang} b'' = \frac{2}{31}\{-13\sin 72^0 - \sin 144^0\}$$

Numerically, this gives

$$\begin{aligned}\operatorname{tang} b' &= +0{,}4316226944, \quad \log\operatorname{tang} b' = 9{,}6351042715\\ b' &= 23^0 20' 46'' 04603\\ \operatorname{tang} b'' &= -0{,}8355819332, \quad \log\operatorname{tang} b'' = 9{,}9219890411\text{n}\\ b'' &= 140^0 7' 6'' 52441\end{aligned}$$

from which we derive

$$5f' = 186^0 48' 38'' 61647, \qquad f' = 37^0 21' 43'' 723294$$

.We therefore have

$$\begin{aligned}(2,1) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 37^0 21' 43'' 723294 + 2\cos 51^0 22' 41'' 400558\}\\ (2,2) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 325^0 21' 43'' 723294 + 2\cos 267^0 22' 41'' 400558\}\\ (2,4) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 253^0 21' 43'' 723294 + 2\cos 123^0 22' 41'' 400558\}\\ (2,8) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 181^0 21' 43'' 723294 + 2\cos 339^0 22' 41'' 400558\}\\ (2,5) &= -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 109^0 21' 43'' 723294 + 2\cos 195^0 22' 41'' 400558\}\end{aligned}$$

from which we find

$$\begin{array}{lcll}(2,1) & = & +1{,}6825070652 & = 2\cos\frac{360^0}{11}\\ (2,2) & = & +0{,}8308299 & = 2\cos\frac{720^0}{11}\\ (2,4) & = & & = 2\cos\frac{1440^0}{11}\\ (2,8) & = & & = 2\cos\frac{2880^0}{11}\\ (2,5) & = & & = 2\cos\frac{1800^0}{11}\end{array}$$

18.

The equation $x^{17} - 1 = 0$, which we already treated by a different method in the *Disquis. Arithm.*, will provide another example. We shall therefore set $n = 17$, $\beta = 8$, $g = 3$; the following indices then correspond to the numbers:

numbers	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16
indices	0.	14.	1.	12.	5.	15.	11.	10.	2.	3.	7.	13.	4.	9.	6.	8

From this we find

$$\begin{aligned}A' = A'''''' &= 2R + 2R^2 + 3R^4 + 4R^5 + 2R^6 + 2R^7\\ A'' = A'''' &= 2 + 3R + R^3 + R^4 + 3R^5 + 4R^6 + R^7\\ A''' = A'''' &= 3 + 3R + 2R^2 + 3R^3 + R^5 + 2R^6 + R^7\end{aligned}$$

or, since in this case $R^4 + 1 = 0$,

$$A' = A''''' = -3 - 2R - 2R^3$$
$$A'' = A'''' = 1 - 4R^2$$
$$A''' = A'''' = 3 + 2R + 2R^3$$

Putting $R = \cos 45^0 + i \sin 45^0$, we therefore have

$$A' = A''''' = -3 - 2i\sqrt{2},$$
$$A'' = A'''' = 1 - 4i,$$
$$A''' = A'''' = 3 + 2i\sqrt{2}$$

Thus b', b'', b''' will be found from the equations

$$\begin{array}{lll} \sin b' = -\sqrt{\frac{8}{17}} & \sin b'' = -\sqrt{\frac{16}{17}} & \sin b''' = +\sqrt{\frac{8}{17}} \\ \cos b' = -\sqrt{\frac{9}{17}} & \cos b'' = +\sqrt{\frac{1}{17}} & \cos b''' = +\sqrt{\frac{9}{17}} \\ \operatorname{tang} b' = +\sqrt{\frac{8}{9}} & \operatorname{tang} b'' = -4 & \operatorname{tang} b''' = +\sqrt{\frac{8}{9}} \end{array}$$

from which we deduce

$$b' = 223^0 18' 49'', \quad b'' = 284^0 2' 10, \quad b''' = 43^0 18' 49'' = b' - 180^0$$

$$4f' = 550^0 39' 48'', \qquad f' = 137^0 39' 57''$$

$$(2,1) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 137^0 39' 57'' + 2\cos 52^0 1' 5'' + 2\cos 265^0 38' 52'' + 1\}$$
$$(2,4) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 92^0 39' 57'' + 2\cos 322^0 1' 5'' + 2\cos 130^0 38' 52'' - 1\}$$
$$(2,9) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 47^0 39' 57'' + 2\cos 232^0 1' 5'' + 2\cos 355^0 38' 52'' + 1\}$$
$$(2,10) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 2^0 39' 57'' + 2\cos 142^0 1' 5'' + 2\cos 220^0 38' 52'' - 1\}$$
$$(2,13) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 317^0 39' 57'' + 2\cos 52^0 1' 5'' + 2\cos 85^0 38' 52'' + 1\}$$
$$(2,5) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 272^0 39' 57'' + 2\cos 322^0 1' 5'' + 2\cos 310^0 38' 52'' - 1\}$$
$$(2,15) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 227^0 39' 57'' + 2\cos 232^0 1' 5'' + 2\cos 175^0 38' 52'' + 1\}$$
$$(2,11) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 182^0 39' 57'' + 2\cos 142^0 1' 5'' + 2\cos 40^0 38' 52'' - 1\}$$

$$\begin{array}{rcrcl}
\frac{1}{2}(2,1) & = & +0{,}092268 & = & \cos\frac{4}{17}360^0 \\
\frac{1}{2}(2,3) & = & & = & \cos\frac{5}{17}360^0 \\
\frac{1}{2}(2,9) & = & & = & \cos\frac{2}{17}360^0 \\
\frac{1}{2}(2,10) & = & & = & \cos\frac{6}{17}360^0 \\
\frac{1}{2}(2,13) & = & +0{,}93247 & = & \cos\frac{1}{17}360^0 \\
\frac{1}{2}(2,5) & = & & = & \cos\frac{3}{17}360^0 \\
\frac{1}{2}(2,15) & = & & = & \cos\frac{8}{17}360^0 \\
\frac{1}{2}(2,11) & = & & = & \cos\frac{7}{17}360^0
\end{array}$$

* *

From these more general investigations of the functions $[r, R]$, which further clarify and extend the second theory of pure equations begun in Article 360 of the *Disquiss. Ar.*, we proceed to consider certain special cases more closely, namely those in which definite values are taken for β. Several investigations, as fruitful as they are elegant, will emerge from this; some had already been treated in the *Disq. Ar.* (Articles . . .), though by a different method, while others are to be regarded as entirely new. We reserve for another paper, to be published soon, the development of the remarkable connection between these investigations and higher arithmetic, which thereby makes very great and hitherto unexpected advances. — Moreover, throughout the following investigation we shall assume that r is taken to be a *proper* root of the equation $x^n - 1 = 0$, and R a proper root of the equation $R^\beta - 1 = 0$.

19.

We begin with the value $\beta = 2$, so that R must take the value -1. Our function $[r, R]$ therefore becomes

$$= r - r^g + r^{g^2} - r^{g^3} \ldots . - r^{g^{n-2}}$$

and we have

$$[r, R] = -[r^g, R] = +[r^{g^2}, R] = -[r^{g^3}, R] \quad \text{etc.}$$

and, in general, if λ denotes any integer not divisible by n,

$$[r^\lambda, R] = +[r, R] \quad \text{if } \lambda \text{ is a quadratic residue of } n,$$
$$[r^\lambda, R] = -[r, R] \quad \text{if } \lambda \text{ is a quadratic nonresidue of } n.$$

Further, if the quadratic residues of n among $1, 2, 3 \ldots n-1$ are denoted generically by a, and the nonresidues of n within the same limits by b, it is evident that the numbers

$$1, g^2, g^4 \ldots . g^{n-3}$$

with their order disregarded, are congruent modulo n to the numbers a, and similarly the numbers

$$g, g^3, g^5 \ldots . g^{n-2}$$

are congruent to b, so that $[r, R] = \Sigma r^a - \Sigma r^b$.

If, therefore, we put $\frac{360^0}{n} = \omega$ and $r = \cos k\omega + i \sin k\omega$, then $[r, R] = \Sigma \cos ak\omega - \Sigma \cos bk\omega + i\Sigma \sin ak\omega - i\Sigma \sin bk\omega$. Now, by Article 14, the square of the function $[r, R]$ will be $= +n$ or $= -n$ according as n has the form $4z+1$ or $4z-1$, and hence in the former case $[r, R] = \pm\sqrt{n}$, in the latter $[r.R] = \pm i\sqrt{n}$; the sign placed before the radical quantity, however, remains ambiguous. From this we obtain the following sums:

I. If n has the form $4z+1$,

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = \pm\sqrt{n}$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = 0$$

II. If n has the form $4z-1$,

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = 0$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = \pm\sqrt{n}$$

Moreover, since the whole collection of numbers a, b evidently coincides with $1, 2, 3 \ldots n-1$, we have $\Sigma r^a + \Sigma r^b = r + r^2 + r^3 + \text{etc.} + r^{n-1} = -1$, and therefore $\Sigma \cos ak\omega + \Sigma \cos bk\omega = -1$, $\Sigma \sin ak\omega + \Sigma \sin bk\omega = 0$. These identities and the preceding sums give:

I. For the former case,

$$\Sigma \cos ak\omega = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin ak\omega = \Sigma \sin bk\omega = 0$$

II. For the latter case,

$$\Sigma \cos ak\omega = \Sigma \cos bk\omega = -\tfrac{1}{2}$$
$$\Sigma \sin ak\omega = \pm\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin bk\omega = \mp\tfrac{1}{2}\sqrt{n}$$

These sums were already obtained by a method not very different in Article 356 of the *Disquiss. Arr.*; neither method can remove the ambiguity in the sign to be placed before the radical quantity. We have, however, recently overcome this shortcoming in a separate paper, where it was proved that, for the value $k = 1$, the upper signs must be taken in all the formulas given.

Remarks.

Only a few articles remain of the original continuation of this paper from Article 19 onward, which was devoted to special cases. They deal with the quadratic equation whose roots are the two periods of $\frac{n-1}{2}$ terms; the manuscript stops at the beginning of the investigation that was to determine the sign of the square root occurring in its solution. The agreement of this surviving beginning with the paper Summatio quarumdam serierum singularium shows that the author changed his plan to make the determination of the sign just mentioned the subject of a separate paper. Comparison with the citation in Article 8, where the manuscript mistakenly gave the third edition of Lagrange's work instead of the second, shows that this manuscript dates from 1808. That publication of the preceding material had not been abandoned is shown by a leaf evidently inserted later at Article 19, on which a different continuation begins and which already refers to the paper Summatio, etc., for the determination of the sign. This second continuation, which also soon stops, is presented here. In preparing the edition, the text of the manuscript, which was entirely ready for printing, was faithfully retained; only in Article 16 did the formulas for the second case have to be added.

R. Dedekind.

PROOF OF SOME THEOREMS CONCERNING THE PERIODS OF CLASSES OF BINARY QUADRATIC FORMS.

THEOREM. I. *The number of (properly primitive) classes of the same determinant which, when raised to the Pth power, where P is either a prime number or a prime power $= p^\pi$, produce the principal class K, is equal either to* 1 *or to a power of this same prime number p.*

Proof. Let $(\mathfrak{Q})$ be the whole group of all the classes in question, and n their number. Since the principal class K is necessarily contained in $(\mathfrak{Q})$, the theorem is evident if it is the only one there. But if there are others, the number of classes contained in the period of each will be a power of p; let one of them be A, and suppose that its period $(\mathfrak{A})$ contains p^α classes, all of which will be included in $(\mathfrak{Q})$. Now, if the classes of this period $(\mathfrak{A})$ exhaust $(\mathfrak{Q})$, we shall have $p^\alpha = n$, and the theorem will be proved; otherwise, let B be any class of $(\mathfrak{Q})$ not contained in $(\mathfrak{A})$, and suppose its period is developed until we reach a class bB which is also among the classes of $(\mathfrak{A})$. This must necessarily happen, because at least the principal class is common to this period and to $(\mathfrak{A})$. Now, supposing that bB is the *first* class in the period of B common to $(\mathfrak{A})$, or that b is as small as possible, I claim

1^0. That b will be a power of p. For it is evident that, on putting $b = p^\beta h$, $bB = iA$ and $hk \equiv 1 \pmod{p^\pi}$ (which will be possible), we shall have $kbB = p^\beta hkB = p^\beta B = ikA$, that is, $p^\beta B$ will also be among the classes of $(\mathfrak{A})$, from which it follows that $h = 1$ and $b = p^\beta$.

2^0. That, if the classes $K, B, 2B \ldots . (b-1)B$ are denoted by $(\mathfrak{B})$, all the compositions of a class of $(\mathfrak{A})$ with a class of $(\mathfrak{B})$ will give $p^{\alpha+\beta}$ different classes. For, supposing $mA+nB = m'A+n'B$ and $n = n'$, we shall necessarily have $m = m'$; if $n > n'$, we shall have $(n-n')B = (m'-m)A$, which is impossible unless $n = n'$.

3^0. That these $p^{\alpha+\beta}$ different classes will be included in $(\mathfrak{Q})$, which is evident.

Now, if these $p^{\alpha+\beta}$ classes exhaust $(\mathfrak{Q})$, the theorem is proved; otherwise, we shall choose another class of $(\mathfrak{Q})$ not contained among them, namely C; we shall continue its period until we reach a class already included among the classes composed from $(\mathfrak{A})$ and $(\mathfrak{B})$. By reasoning similar to the preceding, we shall prove that the exponent of this class must be a power of p, $= p^\gamma$, and that the composition of the first p^γ classes of the period of C with the $p^{\alpha+\beta}$ classes already found will give $p^{\alpha+\beta+\gamma}$ different classes, all included in $(\mathfrak{Q})$. If these classes still do not exhaust $(\mathfrak{Q})$, we shall treat a fourth class D, etc., in the same way; and it is evident that, since $(\mathfrak{Q})$ consists of a finite number

of classes, these operations will also come to an end, and n will be equal to a power of p. Q. E. D.

THEOREM. II. *If the number of all the classes of the principal genus is expressed by $a^\alpha b^\beta c^\gamma$, etc., where a, b, c denote different prime numbers, there will be in this genus $a^\alpha, b^\beta, c^\gamma$, etc., classes which, when raised respectively to the powers $a^\alpha, b^\beta, c^\gamma$, etc., produce the principal class.*

Proof Let A, A', A'', etc., be all the classes which, when raised to the power a^α, produce K, and let $(\mathfrak{A})$ be their totality; likewise B, B', B'', etc., $(\mathfrak{B})$, C, C', C'', $(\mathfrak{C})$, etc., etc. I claim that the composition of all the classes of $(\mathfrak{A})$ with all the classes of $(\mathfrak{B})$ with all the classes of $(\mathfrak{C})$, etc., will produce classes different from one another. For if $A + B + C \cdots = A' + B' + C' \ldots$, etc., then, on putting $A - A' = A''$, $B - B' = B''$, etc., we shall have

$$A'' + B'' + C'' \text{ etc.} = K$$

and hence, on raising to the power $b^\beta c^\gamma$, etc., $(b^\beta c^\gamma \ldots)A'' = K$, from which it follows readily that $A'' = K$ and $A = A'$, and in the same way we shall have $B = B'$, $C = C'$, etc. Let the totality of these classes be $= (S)$. Further, it is clear that all these classes will belong to the principal genus. Finally, there can be no class in the principal genus which is not included in (S). Let . . .

REMARK.

This fragment, written in 1801, relates to Disq. Arithm., Article 306, IX. The word *dignité* is used here in a sense that is not otherwise customary.

STERN.

[I.]

ON THE CONNECTION BETWEEN THE NUMBER OF CLASSES INTO WHICH BINARY QUADRATIC FORMS ARE DISTRIBUTED AND THEIR DETERMINANT.

FIRST PAPER

PRESENTED TO THE ROYAL SOCIETY 1834 . . . .

1.

Thirty-three years have now passed since we discovered the principles of the remarkable connection to which this paper is devoted, as was already announced at the end of the *Arithmetical Investigations*. Other occupations, however, had long drawn us away from this inquiry, until more recently we were able to return to it and extend it through renewed efforts. Yet, since this new part of higher arithmetic exceeds the bounds of a single paper, this first paper will be devoted to forms with negative determinants; forms with positive determinants, which require an entirely distinct treatment, must remain reserved for another paper.

2.

The basis of the whole subject is a particular investigation of the number of all combinations of integer values taken by two indeterminate integers x, y within a prescribed region. Evidently this problem can also be presented geometrically, by finding the number of *complex numbers* whose representations fall within a prescribed figure. The nature of the figure will depend on that of the line surrounding it, and thus either on a single equation between the coordinates x, y (when the boundary is a curve returning to itself) or on several such equations (when it .consists of several curved or straight parts); it will be at our discretion whether to include in the count, or exclude from it, points corresponding to complex integers that may lie on the boundary itself.

In the analytic presentation of the problem, these conditions of restriction can always be expressed by requiring one or more given functions of the variables x, y, namely P, Q, R, etc., to take positive or nonnegative values (according as the value 0 is excluded or admitted).

Thus, for example, if the prescribed figure is a circle with radius $= \sqrt{A}$, while its centre lies at a point corresponding to a complex integer, the analytic condition will be that $A - xx - yy$ is not negative, provided that, as we shall always suppose, we choose to retain points lying on the boundary itself.

If the figure is a triangle, the three linear functions $ax+by+c$, $a'x+b'y+c'$, $a''x+b''y+c''$ must have nonnegative values, and similarly in other cases.

3.

Generally speaking, an *exact* solution of the problem must proceed by first using the nature of the conditions to confine one variable, for example x, within limits between which the individual integer values are then taken successively. We must find how many integer values of the other variable y correspond to each of them, and then add these numbers together. In special cases there will usually be particular devices for shortening the work.

For example, if the figure is, as above, a circle with radius $=\sqrt{A}$, let r be the integer immediately below $\sqrt{A}$, or $\sqrt{A}$ itself if A is a square. Likewise let r', r'', r''', etc., $r^{(r)}$ be the integers immediately below $\sqrt{(A-1)}$, $\sqrt{(A-4)}$, $\sqrt{(A-9)}$, etc., as far as $\sqrt{(A-rr)}$. The required number will then be

$$\begin{aligned} &= 2r+1+2(2r'+1)+2(2r''+1)+2(2r'''+1)+\text{etc.} \\ &= 1+4r+4r'+4r''+4r'''+\text{etc.}+4r^{(r)} \end{aligned}$$

The following method is shorter in this example. Let q be the integer immediately below $\sqrt{\frac{1}{2}A}$ (or equal to it when it is an integer), and let $r^{(q+1)}$, $r^{(q+2)}$, $r^{(q+3)}$, etc., be the integers immediately below $\sqrt{(A-(q+1)^2)}$, $\sqrt{(A-(q+2)^2)}$, $\sqrt{(A-(q+3)^2)}$, etc., as far as $\sqrt{(A-rr)}$. The required number will then be

$$= 4qq+1+4r+8(r^{(q+1)}+r^{(q+2)}+r^{(q+3)}+\text{etc.}+r^{(r)})$$

This formula gave the following numbers:

A		A		A	
100	317	1000	3149	10000	31417
200	633	2000	6293	20000	62845
300	949	3000	9425	30000	94237
400	1257	4000	12581	40000	125629
500	1581	5000	15705	50000	157093
600	1885	6000	18853	60000	188453
700	2209	7000	21993	70000	219901
800	2521	8000	25137	80000	251305
900	2821	9000	28269	90000	282697
1000	3149	10000	31417	100000	314197

4.

Our purpose does not require an exact determination, but rather the search for an expression that can approach the exact number as closely as desired as the limits are extended to infinity. But first of all, since this involves something vague, the matter must be stated more exactly.

We shall therefore suppose that the functions P, Q, R, etc., besides the variables x, y, involve a constant element k, so that each of P, Q, R, etc., is a homogeneous function of the three quantities x, y, k. In this way the figure determined by the equations $P = 0, Q = 0, R = 0$, etc., will depend on k, so that different values of k correspond to similar figures similarly situated with respect to the origin of coordinates; corresponding linear dimensions will be proportional to the values of k, and areas to the values of kk. Let the number of points within the figure now be denoted by M, and the area by V. It is evident that M and V must increase as k increases; as k increases to infinity, M and V will approach a ratio of equality as closely as desired. Or, if you require elementary clarity, given a quantity λ, however small, a threshold can always be assigned such that, for every value of k exceeding it, $\frac{M}{V}$ must certainly lie between $1 - \lambda$ and $1 + \lambda$. In the customary manner this may be expressed by saying that $M = V$ for an infinite value of k.

In our example the required condition holds on putting $k = \sqrt{A}$, and the curve becomes a circle whose area $= \pi A$, where π denotes the half-circumference of a circle of radius $= 1$. The numbers given above clearly indicate the convergence.

Moreover, if it were worth the effort, we could easily complete the proof of this theorem with the rigour of the ancients; here, however, we have preferred to omit it, hastening on to more difficult matters.

5.

In this paper the boundary will be expressed by a *single* equation of the form $axx + 2bxy + cyy = A$, where a, b, c are integers and $bb - ac$ is a negative number, which we shall put $= -D$. Evidently the curve defining the figure will be an ellipse, and it is readily seen that the squares of the semiaxes are the roots of the equation

$$(ac - bb)qq - (a + c)Aq + AA = 0 \quad \text{or} \quad = A\left(\frac{a + c \pm \sqrt{(4bb + (a - c)^2)}}{2(ac - bb)}\right)$$

The product of these roots is $\frac{AA}{ac-bb} = \frac{AA}{D}$, and hence the area of the ellipse $= \frac{\pi A}{\sqrt{D}}$. We therefore infer that the number of all combinations of integer values of x, y for which $axx + 2bxy + cyy$ does not exceed the value A, as A increases, comes ever closer to $\frac{\pi A}{\sqrt{D}}$, and for infinite A must be set equal to that value. Moreover, it is evident that in this respect it makes no difference whether the combination $x = 0, y = 0$ is counted with the others or excluded.

In this way the required number (in the latter sense) is simply the sum of the numbers of representations of the individual numbers $1, 2, 3 \ldots A$ by the binary quadratic form $axx + 2bxy + cyy$; and since some of those numbers cannot be represented by this form at all, while others admit more or fewer representations, the quantity $\frac{\pi}{\sqrt{D}}$ is to be regarded as the mean value of the number of representations of an indeterminate positive number by any form whose determinant $= -D$.

6.

Before investigating the consequences in general, we have thought it useful to work out some special cases, so that the manner of argument may be understood more easily. Let us therefore first return to the form $xx + yy$, for which the number of representations of an indeterminate number has the mean value $= \pi$. The number of actual representations of a given number is readily determined from the general principles established in the Arithmetical Investigations. Let fA denote the number of representations of the number A; this will be $= 4$ if $A = 1$ or 2 or a power of two; $= 8$ if A is a prime number of the form $4n + 1$, or the product of such a prime and a power of two; $= 0$ if A is a prime number of the form $4n + 3$, or is divisible by such a prime but not by its square; finally, *in general*,

$$\begin{aligned} \text{either} \quad & = 4(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots \\ \text{or} \quad & = 0 \end{aligned}$$

Here the number A is put in the form $2^{\mu} S a^{\alpha} b^{\beta} c^{\gamma} \ldots$, where a, b, c, etc., denote different prime numbers of the form $4n + 1$, and S the product of the primes of the form $4n + 3$ that occur once or more among the factors of the number A, if there are any. The first or second value applies according as the number S is a square or is not a square. It is therefore evident that fA depends solely on the way in which the prime numbers $3, 5, 7, 11, 13$, etc., occur among the factors of the number A, so that in general we must put

$$fA = 4(3) \,.\, (5) \,.\, (7) \,.\, (11) \,.\, (13) \ldots .$$

if we suppose the values of the symbols $(3), (5), (7)$, etc., to be chosen so that, with p denoting a prime number, we have

first $(p) = 1$ if p does not divide A

second $(p) = \alpha + 1$ if p has the form $4n + 1$, and p^α is the highest power dividing A

third $(p) = 0$ if p has the form $4n+3$, and the exponent of the highest power of p dividing A is odd; finally,

fourth $(p) = 1$ if p has the form $4n + 3$, and the exponent of the highest power of p dividing A is even.

Evidently the first case is included in the second and fourth.

The terms of the sequence $f1, f2, f3, f4$, etc., thus proceed very irregularly, although the more terms are taken, the more accurately the mean value $= \pi$ must emerge from them. We shall denote the sum $f1 + f2 + f3 + \ldots + fA$ by FA.

7.

Let us now put, in general, $fm + f3m = f'm$; it is easily seen that

$$f'A = 4(5) \,.\, (7) \,.\, (11) \,.\, (13) \ldots$$

that is, $f'A$ will be independent of the relation of A to the divisor 3, so that the irregularity of the sequence $f'1, f'2, f'3, f'4, f'5, f'6$, etc., will both begin later and be much smaller. Further, if we put

$$f'1 + f'2 + f'3 + f'4 + \text{etc.} + f'm = F'm$$

we shall have

$$\begin{aligned} F'3A &= F3A + f3 + f6 + f9 + \ldots + f9A \\ &= F3A + FA \end{aligned}$$

From this it follows readily that, as A increases to infinity, we must put

$$F'3A = 4\pi A$$

or that the mean value of the terms of the sequence $f'1, f'2, f'3, f'4$, etc., is

$$= \tfrac{4}{3}\pi$$

In the same way, on putting in general $-f'm + f'5m = f''m$, we obtain

$$f''A = 4(7)(11)(13) \ldots$$

that is, the new sequence $f''1$, $f''2$, etc., loses the fluctuations that depend on the relation to the number 5. On setting the sum

$$f''1 + f''2 + f''3 + \ldots + f''m = F''m$$

we obtain

$$F''5m = -F'm + F'5m$$

from which it follows that, as m increases to infinity, we must put

$$F''5m = \tfrac{4}{3}\pi \,.\, 4m$$

or that the mean value of the terms of the sequence is $= \frac{4}{3} \,.\, \frac{4}{5}\pi$.

If we proceed further in the same way, forming new sequences as we successively remove the factors $(7), (11), (13), (17)$, etc., these will approach constancy ever more closely, and their mean values will successively acquire the new factors $\frac{8}{7}, \frac{12}{11}, \frac{12}{13}, \frac{16}{17}, \frac{20}{19}$, etc. The denominators will be the prime numbers in their natural order, and the numerators will be greater or smaller by one according as those primes have the form $4n - 1$ or $\cdot 4n + 1$. Hence, since, on continuing this process to infinity, the constant value 4 must approach the mean value ever more closely, we have

$$4 = \pi \,.\, \tfrac{4}{3} \cdot \tfrac{4}{5} \cdot \tfrac{8}{7} \cdot \tfrac{12}{11} \cdot \tfrac{12}{13} \ldots \text{ to infinity}$$

or

$$\pi = 4 \,.\, \frac{3}{3+1} \cdot \frac{5}{5-1} \cdot \frac{7}{7+1} \cdot \frac{11}{11+1} \cdot \frac{13}{13-1} \cdots$$

If the individual fractions are expanded into infinite series,

$$\begin{aligned}
\frac{3}{3+1} &= 1 - \frac{1}{3} + \frac{1}{9} - \frac{1}{27} + \ldots \\
\frac{5}{5-1} &= 1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \ldots \\
\frac{7}{7+1} &= 1 - \frac{1}{7} + \frac{1}{49} - \frac{1}{343} + \ldots \\
&\text{etc.}
\end{aligned}$$

the product readily expands into

$$1 - \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{7} + \tfrac{1}{9} - \tfrac{1}{11} + \tfrac{1}{13} \ldots .$$

and the sum of this series is generally known to be $= \frac{1}{4}\pi$. In fact, the illustrious Euler had long ago derived from this, in the reverse direction, the equality between $\frac{1}{4}\pi$ and the infinite product $\frac{4}{3} \,.\, \frac{4}{5} \,.\, \frac{8}{7} \,..$ (*Introd. in analys. inf.*, Vol. I, Chap. xv, Article 285).

8.

Let us consider, secondly, the form $xx + 2yy$, for which the number of representations of an indeterminate number will have the mean value $= \frac{\pi}{\sqrt{2}}$. If fA denotes the number of representations of a given number A by this form, this will be $= 2$ for $A = 1$ or $A = 2$, or whenever A is a power of two; further, $fA = 4$ whenever A is one of the primes of which -2 is a quadratic residue, that is, those of the forms $8k + 1, 8k + 3$, for example $A = 3, 11, 17, 19, 41, 43$, etc.; finally, $fA = 0$ whenever A is a prime of which -2 is a quadratic nonresidue, for example one of the sequence $5, 7, 13, 23, 29, 31$, etc., that is, of either the form $8k + 5$ or the form $8k + 7$. In general, however, we must put

$$\begin{aligned} \text{either} \quad & fA = 2(\alpha + 1)(\beta + 1)(\gamma + 1) \dots \\ \text{or} \quad & fA = 0 \end{aligned}$$

Here the number A is put in the form $2^\mu S a^\alpha b^\beta c^\gamma \dots$, where a, b, c, etc., denote different prime numbers of the forms $8k + 1, 8k + 3$, while S is the product of the remaining numbers (of the forms $8k + 5, 8k + 7$), if any occur among the factors of the number A. The first or second value applies according as S is a square or is not a square. From this, by reasoning entirely similar to that in the preceding article, we shall pass from the sequence $f1, f2, f3, f4, f5$, etc., namely $2, 2, 4, 2, 0, 2$, etc., successively to others that remain *constant* for increasingly long stretches. Their *mean* values will be, successively, $\frac{\pi}{\sqrt{2}}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5}$, $\frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5} \cdot \frac{8}{7}$, etc.; we shall proceed in such a way as to arrive at the equation

$$2 = \frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{10}{11} \cdot \frac{14}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} \dots$$

where the denominators form the natural sequence of prime numbers, while the numerators are smaller by one whenever the denominators have the form $8k + 1$ or $8k + 3$, and larger by one whenever the denominators have the form $8k + 5$ or $8k + 7$.

[II.]

ON THE CONNECTION BETWEEN THE NUMBER OF CLASSES INTO WHICH BINARY QUADRATIC FORMS ARE DISTRIBUTED AND THEIR DETERMINANT.

FIRST PAPER

PRESENTED TO THE ROYAL SOCIETY 1837 . . .

1.

Thirty-six years have passed since the principles of the remarkable connection to be treated in this paper were discovered, as was already announced at the end of the *Arithmetical Investigations*. Other occupations, however, had long drawn attention away from this inquiry, until more recently it became possible to return to it and extend it through renewed efforts. Yet, since this new part of higher arithmetic exceeds the bounds of a single paper, this first paper will be devoted to forms with negative determinants; forms with positive determinants, which require an entirely distinct treatment, will remain reserved for another paper.

2.

For our purpose we shall need a theorem which is itself arithmetical, but whose nature can be presented more conveniently and clearly through considerations expressed in geometrical form.

Given a figure in an unbounded plane, enclosed by any line, its area can be determined approximately by dividing the plane into squares and counting both those lying wholly inside the figure and those cut by its boundary. Evidently, the resulting area will be smaller or larger than the true area according as the latter squares are omitted or added to the former. If, however, we choose, by any rule, to exclude some and include others of the latter squares lying on the boundary, the error may be positive or negative, but must be smaller than the total area of all the boundary squares. The smaller the squares are taken, the more accurately the area will be determined in this way. We may carry such an approximation indefinitely further, or take the squares so small that the error becomes smaller than any given quantity. Although this may already seem evident in itself, we shall nevertheless not refuse to support it with a rigorous proof.

Two squares can have one common vertex, two, or none; in the first and second cases they will be called adjacent, and in the third disjoint. Evidently, at most four squares can all be adjacent to one another, and thus among any five distinct squares at least two must be disjoint. Now the distance between two points lying in disjoint squares cannot be smaller than the side of the squares, which we shall denote by a. Hence, if a point starts anywhere in one square, then passes through a second, third and fourth, and finally reaches a fifth, the length of its path certainly cannot be smaller than a. By the same reasoning, if the line continues through further squares, the part between the fifth and ninth, and likewise between the ninth and thirteenth, etc., cannot be smaller than a. We therefore readily conclude that any line returning to itself which has touched n distinct squares in all certainly cannot be shorter than $\frac{(n-4)a}{4}$. Conversely, a closed line whose length is $= l$ certainly cannot have touched more than $4 + \frac{4l}{a}$ distinct squares. Since their area $= 4aa + 4al$ can become smaller than any given quantity as a decreases indefinitely, the same holds all the more for the error in the determination of area discussed above.

3.

The rule for including or excluding squares lying on the boundary of the figure could be chosen in many different ways. The simplest, however, seems to be to consider only the position of the centre of each square, so that squares whose centres lie inside the figure are included, those whose centres lie outside it are excluded, and it is left to our choice whether centres that happen to lie on the boundary itself are counted with the interior or the exterior. Instead of the centres, we could also take any other points situated in the same relative position in each square.

Thus the matter comes down to imagining equally spaced points distributed along equally spaced straight lines in the plane so as to form squares. By the theorem of the preceding article, we can then assert that the number of points contained in the figure, multiplied by the square of the distance between two nearest points, becomes as nearly equal to the area of the figure as desired, provided that distance is taken sufficiently small; or, in the customary manner of speaking, that this product gives the area if the distance is infinitely small.

4.

The curve expressed by the following equation between the rectangular coordinates p, q,

$$app + 2bpq + cqq = 1$$

is a conic section, and specifically an ellipse if a, c and $ac - bb$ are positive quantities. The area enclosed by this ellipse is found to be $. = \frac{\pi}{\sqrt{(ac-bb)}}$.

The value of $app + 2bpq + cqq$ is everywhere greater than 1 outside the ellipse, less than 1 inside it, and nowhere negative.

Suppose a .system of points distributed in the plane containing the ellipse so as to form squares whose sides $= \lambda$ are parallel to the coordinate axes. It makes no difference whether the origin of the coordinates, or centre of the ellipse, coincides with one of these points. Let the number of points inside the ellipse, including any on its boundary, be $= m$. By the theorem of the preceding article, $\frac{\pi}{\sqrt{(ac-bb)}}$ will then be the limit of $m\lambda\lambda$, which approaches it as closely as desired as λ decreases indefinitely.

If we suppose that the origin of the coordinates coincides with a point of the system, then, on putting $p = \lambda x, q = \lambda y$, evidently x and y will be integers for each point of the system; conversely, every combination of integer values of x, y will correspond to a point of the system. Thus the number m is simply the number of all combinations of integer values of x, y for which F is no greater than M, if, for brevity, we denote the function, or quadratic form, $axx + 2bxy + cyy$ by F, and the quantity $\frac{1}{\lambda\lambda}$ by M. The determinant of this form is $bb - ac$, for which we shall write $-D$. Our theorem can now be stated as follows.

THEOREM I. *The number m of all combinations of integer values of the indeterminates x, y for which the value of a form with negative determinant $-D$ does not exceed the bound M becomes $= \frac{\pi M}{\sqrt{D}}$, approximately, indeed, but with the approximation improving indefinitely as M increases indefinitely. It scarcely needs to be mentioned that indefinite approximation here, and likewise in what follows, is not to be understood as saying that the difference between $\frac{\pi M}{\sqrt{D}}$ and m itself decreases indefinitely. Rather, the ratio between these quantities will approach equality indefinitely; that is, $\frac{\pi M}{m\sqrt{D}} - 1$ will decrease indefinitely.*

5.

To carry out the count, we may proceed by computing, for each integer value of x between the bounds $-\sqrt{\frac{cM}{D}}$ and $+\sqrt{\frac{cM}{D}}$, the two values of y satisfying $F = M$; the number of integers lying between them is then obtained directly. Since this number is the same for opposite values of x, almost half the work is saved. The count can also be carried out by counting the values of x corresponding to each value of y between the bounds $-\sqrt{\frac{aM}{D}}$ and $+\sqrt{\frac{aM}{D}}$. A suitable combination of the two methods can reduce the work further, but we do not pursue this here at greater length; it will suffice to add a few observations on the simplest case.

Let the form be $F = xx + yy$, so that the curve is a circle, and let $r, r', r'', r''' \ldots r^{(r)}$ denote the integers immediately below

$$\sqrt{M}, \quad \sqrt{(M-1)}, \quad \sqrt{(M-4)}, \quad \sqrt{(M-9)} \ldots \sqrt{(M-rr)}$$

or these quantities themselves, if any of them are integers. The required number will then be

$$\begin{aligned} m &= 2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \text{etc.} + 2(2r^{(r)} + 1) \\ &= 1 + 4r + 4r' + 4r'' + 4r''' + \text{etc.} + 4r^{(r)} \end{aligned}$$

We obtain the same result more quickly, however, by denoting by q the integer immediately below $\sqrt{\frac{1}{2}M}$ (or this quantity itself, if it is an integer), with the aid of the formula

$$m = 4qq + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \text{etc.} + r^{(r)})$$

The following numbers were obtained in this way.

M	m	M	m	M	m
100	317	1000	3149	10000	31417
200	633	2000	6293	20000	62845
300	949	3000	9425	30000	94237
400	1257	4000	12581	40000	125629
500	1581	5000	15705	50000	157093
600	1885	6000	18853	60000	188453
700	2209	7000	21993	70000	219901
800	2521	8000	25137	80000	251305
900	2821	9000	28269	90000	282697
1000	3149	10000	31417	100000	314197

6.

We give the theorem of Article 4 greater generality in the following way.

THEOREM II. *If we are to collect, not all combinations of integer values of x, y for which F does not exceed the value M, but only those taken at intervals, namely those for which x is congruent to a given number G to a given modulus g, and y is congruent to a given number H to a given modulus h, then the number m' of these combinations will be expressed approximately by $\frac{\pi M}{gh\sqrt{D}}$, with the approximation improving indefinitely as M increases indefinitely.*

Indeed, on putting $x = gx' + G, y = hy' + H$, it is evident that m' is the number of all combinations of integer values of x', y' for which

$$agg(x' + \tfrac{G}{g})^2 + 2bgh(x' + \tfrac{G}{g})(y' + \tfrac{H}{h}) + chh(y' + \tfrac{H}{h})^2$$

does not exceed the value M. Thus, if we suppose a system of points distributed in the plane as in Article 4, but so that the point with coordinates $p = \frac{G\lambda}{g}, q = \frac{H\lambda}{h}$, rather than the origin of the coordinates, coincides with a point of the system, then m' will express the number of points lying inside the ellipse whose equation is

$$aggpp + 2bghpq + chhqq = 1$$

with any points on the boundary itself always included. The area of this ellipse $= \frac{\pi}{gh\sqrt{(ac-bb)}} = \frac{\pi}{gh\sqrt{D}}$ will be the limit which the product $m'\lambda\lambda = \frac{m'}{M}$ approaches indefinitely as λ decreases or M increases indefinitely.

It is also evident that our theorem includes the case where only one of the indeterminates x, y must proceed by intervals, while the value of the other is subject to no condition. Clearly, this is the same as putting either h or $g = 1$.

7.

What has been set out so far is independent of the nature of the coefficients of the form $axx + 2bxy + cyy$; from now on, however, we shall suppose these coefficients to be integers. Thus every combination of integer values of x, y gives the form itself an integer value, or corresponds to a representation of some integer by this form. Hence the collection of all combinations of integer values of x, y for which the form $F = axx + 2bxy + cyy$ takes a value no greater than the bound M is the same as the collection of all representations of integers not exceeding the bound M, or up to and including this bound if it is itself an integer. If, for brevity, we denote the number of distinct representations of a specified integer n by the form F by $F(n)$, or simply by Fn when there is no risk of ambiguity, then the number previously expressed by m will be $= F0 + F1 + F2 + F3 + \text{etc.} + FM$, and the first theorem takes the following form.

THEOREM III. *The sum $F0 + F1 + F2 + etc. + FM$ is expressed approximately by $\frac{\pi M}{\sqrt{D}}$, with the approximation improving indefinitely as M increases indefinitely.*

8.

To the third theorem, which concerns representations of *all* numbers, it is useful to add another concerning odd numbers alone. Evidently, odd numbers cannot be represented by the form F if a and c are both even numbers; the investigation will therefore be restricted to the three remaining cases.

I. Whenever a is odd and c is even, an odd number is represented by giving x an odd value, while the value of y remains arbitrary. Theorem II, on putting $g = 2, G = 1, h = 1$, therefore shows that the number of all combinations of such values of x, y as give the form an odd value no greater than the bound M is expressed, with indefinite approximation, by $\frac{\pi M}{2\sqrt{D}}$, as M increases indefinitely.

II. Whenever a is even and c is odd, the representation of an odd number requires y to be odd. Thus, on putting $g = 1, h = 2, H = 1$, we reach the same conclusion.

III. Whenever both a and c are odd, either an odd value of x must be combined with an even value of y, or an even value of x with an odd value of y, for the formula to produce an odd value. The number of all combinations of each kind for which the value of the form does not exceed the bound M is expressed, with indefinite approximation, by $\frac{\pi M}{4\sqrt{D}}$. Therefore the number of all combinations which give the form odd values not exceeding the bound M is again expressed, with indefinite approximation, by $\frac{\pi M}{2\sqrt{D}}$.

Now the collection of all such combinations is simply the collection of all representations of all the numbers $1, 3, 5, 7 \ldots M$ when M is an odd integer, or $1, 3, 5, 7 \ldots . M - 1$ when M is even. We therefore have

THEOREM IV. *The sum*

$$F1 + F3 + F5 + F7 . . + FM \quad \text{or} \quad F1 + F3 + F5 + F7 . . + F(M-1)$$

(according as M is odd or even) is expressed, with indefinite approximation, by $\frac{\pi M}{2\sqrt{D}}$, provided that F is a form in which one or both of the coefficients a, c are odd.

[III.]

Let C be the collection of representatives of all classes of properly primitive forms for the determinant $-D$. We denote by (n) the number of all representations of the number n by forms in the collection C. Let p be an odd prime. Then

$$\left.\begin{array}{ll} 1. & (pn) = (n) \quad \text{if } p \text{ divides } D \\ 2. & (pn) = (n) + (h) \\ 3. & (pn) = -(n) + (h) \end{array}\right\} \text{ if } p \text{ does not divide } D$$

$$\begin{cases} \text{divides } xx + D \\ \text{does not divide } xx + D \end{cases}$$

where $n = hp^\mu$, μ is arbitrary, and h is not divisible by p.

In case 1. we have $(h) = (ph) = (pph) = (p^3h)$ etc.

2. $(ph) = 2(h),\ (pph) = 3(h),\ (p^3h) = 4(h)$ etc.

3. $(ph) = 0,\ (pph) = (h),\ (p^3h) = 0,\ (p^4h) = (h)$ etc.

* *
*

From each properly primitive class for the determinant $= -D$, the number of these classes being $= \lambda$, choose one form, and let L be the collection of these forms.

Let fA denote the number of all representations of the number A by forms in L.

Further, let $f(A;p) = f\frac{A}{p^\alpha}$ when p^α is the highest power of the prime p that divides A; also $f(A;p,q) = f\frac{A}{p^\alpha q^\beta}$ when q is another prime whose highest power dividing A is $= q^\beta$; and similarly $f(A;p,q,r) = f\frac{A}{p^\alpha q^\beta r^\gamma}$ when r is a third prime whose highest power dividing A is r^γ, and so on.

[IV.]

Let (n) denote the number of values x in the collection

$$0, 1, 2, 3, 4 \ldots . p^n - 1$$

for which $xx - D = xx - ap^\mu$ is divisible by p^n.

1) μ odd, e.g. $= 7$.	2) μ even, e.g. $= 6$	
	aNp	aRp
$(1) = 1$	$(1) = 1$	$(1) = 1$
$(2) = p$	$(2) = p$	$(2) = p$
$(3) = p$	$(3) = p$	$(3) = p$
$(4) = pp$	$(4) = pp$	$(4) = pp$
$(5) = pp$		

$(6) = p^3$	$(5) = pp$	$(5) = pp$
$(7) = p^3$	$(6) = p^3$	$(6) = p^3$
$(8) = 0$	$(7) = 0$	$(7) = 2p^3$
$(9) = 0$	$(8) = 0$	$(8) = 2p^3$
etc.	etc.	etc.

Now put	Then
$(1) - \frac{(2)}{p} = (1)'$	$fp = (1)'$
$(2) - \frac{(3)}{p} = (2)'$	$fpp = 1 + (2)'$
$(3) - \frac{(4)}{p} = (3)'$	$fp^3 = (1)' + (3)'$
$(4) - \frac{(5)}{p} = (4)'$	$fp^4 = 1 + (2)' + (4)'$
etc.	etc.

Consequently, putting $\frac{p-1}{p}(1 + \frac{fp}{p} + \frac{fpp}{pp} + \frac{fp^3}{p^3} + \text{etc.}) = T$, we have

$$\frac{p+1}{p}T = 1 + \frac{(1)'}{p} + \frac{(2)'}{pp} + \frac{(3)'}{p^3} + \frac{(4)'}{p^4} + \text{etc.}$$
$$= 1 + \frac{(1)}{p} = 1 + \frac{1}{p}$$

Thus $T = 1$

[V.]

The average number of classes[*)] near the negative determinant $-D$ is approximately

$$= \frac{\pi\sqrt{D}}{4(1 + \frac{1}{27} + \frac{1}{125} + \text{etc.})}$$

The actual number is expressed by the following formulas, where, for brevity, m stands for the average number and M for the actual number; p, q denote all odd primes that do not divide D, the former being divisors and the latter nondivisors of $\square + D$; r denotes the primes[**)] that divide D:

[*)] [Compare *Disquiss. Arithm.*, Article 302; the formula there differs by a constant δ from the one occurring here in the text.]

[**)] [odd.]

$$\text{I.}\quad M = m \text{ Product of } \frac{p^3+p^2}{p^3-1} \cdot \frac{q^3-q^2}{q^3-1} \cdot \frac{r^3-r}{r^3-1}$$

$$\text{II.}\quad M = \frac{\pi\sqrt{D}}{4} \text{ Product of } \frac{p+1}{p} \cdot \frac{q-1}{q} \cdot \frac{rr-1}{rr}$$

$$\text{III. NB.}\quad M = \frac{2\sqrt{D}}{\pi} \text{ Product of } \frac{p}{p-1} \cdot \frac{q}{q+1}$$

$$\text{IV.}\quad M = \sqrt{\left\{ \frac{D}{2} \cdot \text{Product of } \frac{p+1}{p-1} \cdot \frac{q-1}{q+1} \cdot \frac{rr-1}{rr} \right\}}$$

$$\text{V.}\quad M = \frac{2\sqrt{D}}{\pi}\{1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \pm \tfrac{1}{7} \pm \tfrac{1}{9} \text{ etc.}\}$$

NB. Formula III follows directly by comparing the two ways of counting the representable numbers up to a given bound.

[VI.]

THEOREM. The number of classes, into which all properly primitive binary forms with negative determinant $-D$[*)], is equal to

$$\frac{\pi}{4} \times \sqrt{D} \times \text{Product of } \frac{p-1}{p}\frac{q+1}{q} \times \frac{rr-1}{rr}$$

where

p denotes all primes[**)] for which $-D$ is a nonresidue,

q all primes[**)] for which $-D$ is a residue,

r all primes[**)] that divide D;

$$= \frac{\frac{\pi}{4}\sqrt{D} \text{ Product of } \frac{rr-1}{rr}}{1 \pm \frac{1}{3} \pm \frac{1}{5} \text{ etc.}}$$

in the denominator, the positive sign is put before fractions whose denominators have the form of nondivisors, and the negative sign before those whose denominators have the form of divisors of $xx + D$; fractions whose denominators are not coprime to D are omitted altogether[***)].

[*)] [are divided.]

[**)] [odd.]

[***)] [If m denotes all positive integers coprime to $2D$, and we use LEGENDRE's symbol as generalized by JACOBI, the above rule for determining the signs must be corrected as follows: in the preceding formula the denominator is

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \text{ etc.} = \Sigma \pm \left(\frac{-D}{m}\right)\frac{1}{m}$$

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \ldots)}{\pi}$$
$$= \frac{\operatorname{cotg}\theta \pm \operatorname{cotg} 3\theta \pm \operatorname{cotg} 5\theta \ldots \pm \operatorname{cotg} n\theta}{N : \sqrt{D}}$$

putting $\theta = \frac{\pi}{N}$, $N = \{\frac{1}{4}\} D$, and taking for n all numbers coprime to D, with the sign determined as above*).

For a positive determinant the number of classes will be**)

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \ldots)}{\log .T + U\sqrt{D}}$$

Here T, U denote the smallest values of the quantities t, u that satisfy the equation $tt - Duu = 1$

$$= \frac{\log \sin \frac{1}{2}\theta \pm \log \sin \frac{3}{2}\theta \pm \log \sin \frac{5}{2}\theta \text{ etc.}}{\log T + U\sqrt{D}}$$

[VII.]

For a negative determinant $-p$, which***) is a prime of the form $4n+1$, the number of classes is†) $= (\alpha - \beta)$, where α is the number of quadratic residues in the first quarter

$$1 \,.\, 2 \,.\, 3 \ldots . \tfrac{1}{4}(p-1)$$

and β the number of nonresidues.

---

where the upper or lower sign is to be taken according as the number m is a product of an even or odd number of primes (equal or unequal); in contrast, in the numerator of the following formula we have

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \ldots = \Sigma \left(\frac{-D}{m}\right) \frac{1}{m}$$

]

*)[See the note on this fragment further below.]

**)[In the following formula D denotes the positive determinant, and

$$1 \pm \tfrac{1}{3} \pm \tfrac{1}{5} \ldots = \Sigma \left(\frac{D}{m}\right) \frac{1}{m}$$

]

***)[that is, when p is a positive prime of the form $4n+1$.]

†)[the number of classes is $= 2(\alpha - \beta)$.]

[VIII.]

$$b \equiv 2m + a - 1 \pmod 8$$

where m is [half] the number of classes for the determinant $-p$

p	m	a	b	f	$\frac{2m+a-1-b}{8}$	α	β
17	2	+1	−4	−4	+1	3	2
41	4	+5	+4	+9	+1	3	4
73	2	−3	−8	+27	+1	1	6
89	6	+5	−8	+34	+3	9	2
97	2	+9	+4	+22	+1	5	6
113	4	−7	+8	+15	−1	9	4
137	4	−11	+4	+37	−1	3	8
193	2	−7	+12	+81	−2	11	6
233	6	+13	+8	+144	+2	15	2
241	6	+15	+4	+64	−1	13	6
257	8	+1	+16	+16	0	15	4
281	10	+5	−16	+53	+5	9	10
313	4	+13	−12	−25	+1	5	12
337	4	+9	+16	−148	0	7	12
353	8	+17	+8	+42	+3	15	8
5	.1	+1	+2	+2	0		
13	1	−3	−2	+5	0		
29	3	+5	+2	+12	+1		
37	1	+1	−6	−6	+1		
53	3	−7	−2	+23	0		
61	3	+5	−6	+11	+2		
101	7	+1	−10	−10	+3		
109	3	−3	+10	+33	−1		
149	7	−7	−10	+44	+2		
157	3	−11	−6	−28	0		
173	7	+13	+2	+80	+3		
181	5	+9	+10	−19	+1		
197	5	+1	−14	−14	+3		
229	5	−15	+2	−107	−1		
269	11	+13	+10	−82	+3		
277	3	+9	+14	−60	0		
293	9	+17	+2	+138	+4		
317	5	−11	+14	+114	−2		
349	7	+5	+18	−136	0		
373	5	−7	+18	+104	−2		
389	11	+17	−10	−115	+6		
397	3	−19	−6	+63	−1		

[IX.]

Distribution of Quadratic Residues in Eighths.

p a prime; (r) the number of quadratic residues of p that lie between $(r-1)\frac{p}{8}$ and $r\frac{p}{8}$.

First case; $p = 8n + 1$.

$2t$ number of classes for the determinant $-p$;

$2u$ number of classes for the determinant $-2p$.

$$(1) = (8) = \tfrac{1}{4}(2n + t + u)$$
$$(2) = (4) = (5) = (7) = \tfrac{1}{4}(2n + t - u)$$
$$(3) = (6) = \tfrac{1}{4}(2n - 3t + u)$$

p	$2n$	t	u	(1)	(2)	(3)
17	4	2	2	2	1	0
41	10	4	2	4	3	0
73	18	2	8	7	3	5
89	22	6	4	8	6	2
97	24	2	10	9	4	7
113	28	4	4	9	7	5
137	34	4	6	11	8	7
193	48	2	10	15	10	13
233	58	6	4	17	15	11
241	60	6	10	19	14	13
257	64	8	8	20	16	12
281	70	10	4	21	19	11
313	78	4	18	25	16	21
337	84	4	12	25	19	21
353	88	8	12	27	21	19
401	100	10	6	29	26	19

Second case; $p = 8n + 5$.

$2t$ number of classes for the determinant $-p$;
$2u$ number of classes for the determinant $-2p$.

$$(1) = (3) = (6) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(2) = (7) = \tfrac{1}{4}(2n + 3t - u + 2)$$
$$(4) = (5) = \tfrac{1}{4}(2n - t - u + 2)$$

p	$2n$	t	u	(1)	(2)	(4)
5	0	1	1	0	1	0
13	2	1	3	1	1	0
29	6	3	1	1	4	1
37	8	1	5	3	2	1
53	12	3	3	3	5	2
61	14	3	5	4	5	2
101	24	7	3	5	11	4
109	26	3	5	7	8	5
149	36	7	3	8	14	7
157	38	3	13	12	9	6
173	42	7	5	10	15	8
181	44	5	9	12	13	8
197	58	5	5	12	15	10
229	56	5	13	16	15	10
269	66	11	5	15	24	13
277	68	3	11	19	17	14
293	72	9	9	18	23	14
317	78	5	7	20	22	17
349	86	7	13	23	24	17
373	92	5	13	25	24	19
389	96	11	7	23	31	20
397	98	3	21	29	22	19

Third case; $p = 8n + 3$.

t number of classes for the determinant $-p$

$2u$ number of classes for the determinant $-2p$.

$$(1) = (4) = (7) = \tfrac{1}{4}(2n + t - u)$$
$$(2) = (5) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(3) = \tfrac{1}{4}(2n + t + u + 2)$$
$$(6) = \tfrac{1}{4}(2n - t - u + 2)$$

p	$2n$	t	u	(1)	(2)	(3)	(6)
3	0	1	1	0	0	1	0
11	2	3	1	1	0	2	0
19	4	3	3	1	1	3	0
43	10	3	5	2	3	5	1
59	14	9	3	5	2	7	1
67	16	3	7	3	5	7	2
83	20	9	5	6	4	9	2
107	26	9	3	8	5	10	4
131	32	15	3	11	5	13	4
139	34	9	7	9	8	13	5
163	40	3	11	8	12	14	7
179	44	15	3	14	8	16	7
211	52	9	5	14	12	17	10
227	56	15	7	16	12	20	9
251	62	21	7	19	12	23	9
283	70	9	15	16	19	24	12
307	76	9	17	17	21	26	13
331	82	9	11	20	21	26	16
347	86	15	5	24	19	27	17
379	94	9	11	23	24	29	19

Fourth case; $p = 8n + 7$.

t number of classes for the determinant $-p$;
$2u$ number of classes for the determinant $-2p$.

$$(1) = \tfrac{1}{4}(2n + 2t - u)$$
$$(2) = (3) = (5) = \tfrac{1}{4}(2n + u + 2)$$
$$(4) = (6) = (7) = \tfrac{1}{4}(2n - u + 2)$$
$$(8) = \tfrac{1}{4}(2n - 2t + u)$$

p	$2n$	t	u	(1)	(2)	(4)	(8)
7	0	1	2	0	1	0	0
23	4	3	2	2	2	1	0
31	6	3	4	2	3	1	1
47	10	5	4	4	4	2	1
71	16	7	2	7	5	4	1
79	18	5	4	6	6	4	3
103	24	5	10	6	9	4	6
127	30	5	8	8	10	6	7
151	36	7	6	11	11	8	7
167	40	11	6	14	12	9	6
191	46	13	4	17	13	11	6
199	48	9	10	14	15	10	10
223	54	7	16	13	18	10	14
239	58	15	4	21	16	14	8
263	64	13	6	21	18	15	11
271	66	11	12	19	20	14	14
311	76	19	6	27	21	18	11
359	88	19	6	30	24	21	14
367	90	9	20	22	28	18	23
383	94	17	12	29	27	21	18

[X.]

Distribution of Quadratic Residues in Twelfths.

p a prime; (r) the number of quadratic residues of p that lie between $\frac{r-1}{12}p$ and $\frac{r}{12}p$.

First case; $p = 24n + 1$.

$2t$ number of classes for the determinant $-p$

$4u$ number of classes for the determinant $-3p$

$$(1) = (12) = \tfrac{1}{6}(6n + 3t + 2u)$$
$$(2) = (4) = (6) = (7) = (9) = (11) = \tfrac{1}{6}(6n - 3t + 2u)$$
$$(3) = (5) = (8) = (10) = \tfrac{1}{6}(6n + 3t - 4u)$$

p	n	t	u	(1)	(2)	(3)
73	3	2	3	5	3	2
97	4	2	3	6	4	3
193	8	2	6	11	9	5
241	10	6	3	14	8	11

Second case; $p = 24n + 13$.

$2t$ number of classes for the determinant $-p$;

$4u$ number of classes for the determinant $-3p$.

$$(1) = (3) = (10) = (12) = \tfrac{1}{2}(2n + 1 + t)$$
$$(2) = (6) = (7) = (1.1) = \tfrac{1}{2}(2n + 1 - t)$$
$$(4) = (9) = \tfrac{1}{2}(2n + 1 - t + 2u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 + t - 2u)$$

p	n	t	u	(1)	(2)	(4)	(5)
13	0	1	1	1	0	1	0
37	1	1	2	2	1	3	0
61	2	3	2	4	1	3	2
109	4	3	3	6	3	6	3
157	6	3	4	8	5	9	4
181	7	5	3	10	5	8	7
229	9	5	3	12	7	10	9

Third case; $p = 24n + 5$.

$2t$ number of classes for the determinant $-p$;
$2u$ number of classes for the determinant $-3p$.

$$(1) = (2) = (6) = (7) = (11) = (12) = n$$
$$(3) = (10) = \tfrac{1}{2}(2n + 1 + t)$$
$$(4) = (9) = \tfrac{1}{2}(2n - t + u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 - u)$$

p	n	t	u	(1)	(3)	(4)	(5)
5	0	1	1	0	1	0	0
29	1	3	3	1	3	1	0
53	2	3	5	2	4	3	0
101	4	7	5	4	8	3	2
149	6	7	7	6	10	6	3
173	7	7	9	7	11	8	3
197	8	5	11	8	11	11	3
269	11	11	7	11	17	9	8

Fourth case; $p = 24n + 17$.

$2t$ number of classes for the determinant $-p$;
$2u$ number of classes for the determinant $-3p$.

$$(1) = (2) = (6) = (7) = (11) = (12) = \tfrac{1}{6}(6n + 3 + u)$$
$$(3) = (10) = \tfrac{1}{6}(6n + 6 + 3t - 2u)$$
$$(4) = (9) = \tfrac{1}{6}(6n + 3 - 3t + u)$$
$$(5) = (8) = \tfrac{1}{6}(6n + 6 - 2u)$$

p	n	t	u	(1)	(3)	(4)	(5)
17	0	2	3	1	1	0	0
41	1	4	3	2	3	0	1
89	3	6	3	4	6	1	3
113	4	4	9	6	4	4	2
137	5	4	9	7	5	5	3
233	9	6	15	12	8	9	5
257	10	8	9	12	12	8	8

Remarks on the Paper

On the Connection between the Number of Classes into Which Binary Quadratic Forms Are Distributed and Their Determinant.

On I and II.

The second formula for the number of points inside the circle (I, Article 3, and II, Article 5) follows by considering the square inscribed in the circle, whose sides are parallel to the coordinate axes; comparing the two formulas leads to the theorem

$$r' + r'' + \ldots + r^{(q)} = qq + r^{(q+1)} + r^{(q+2)} + \ldots + r^{(r)}$$

which is also easy to prove arithmetically. This in turn gives the correctness of the first of the following two rules, which were found on a separate sheet:

"Solutions of the equation $xx + yy \leqq A$; formula

$$1 + 4\sqrt{A} + 4\sqrt{\tfrac{1}{2}A} + 8\Sigma(\sqrt{(A - nn)} - n)$$

where the fractional part of each square root is dropped, and the sum is taken from $n = 1$ to $n = \sqrt{A}$ '(should read $\sqrt{\frac{1}{2}A}$)'.

Another formula

$$1 + 4\{A - \tfrac{A}{3} + \tfrac{A}{5} - \tfrac{A}{7} + \tfrac{A}{9} - \tfrac{A}{11}\ldots\}$$

where the fractional part of each term is dropped."

The latter formula follows from the theorem applied later (I, Article 6) concerning the number of all distinct representations of a given number by the form $xx + yy$ (compare Disqq. Arithm., Article 182, note). This theorem can easily be put in the following form: the number of distinct representations of a positive integer m by the form $xx + yy$ is $= 4(a - b)$, where a, b denote the numbers of divisors of m of the respective forms $4n+1$, $4n+3$. By comparing this arithmetical formula with the average number of representations obtained by geometrical considerations (in I, Article 5, or II, Article 4), one easily obtains, with full rigor, the familiar result

$$\frac{\pi}{4} = 1 - \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{7} + \ldots$$

which is derived in the paper (I, Article 7) by a similar comparison, but with the help of infinite products.

On III and IV.

Let C be the collection of all positive, properly primitive forms of negative determinant $-D$ that are not properly equivalent. Assign to the variables of each form two values relatively prime to one another. The total number of representations of a positive integer m is then $\epsilon\psi(m)$, where ϵ denotes the number of solutions of the equation $tt + Duu = 1$, and $\psi(m)$ the number of roots n of the congruence $nn + D \equiv 0 \pmod{m}$ for which the three numbers $m,\ 2n$ and $\frac{nn+D}{m}$ have no common divisor (Disqq. Arithm., art. 180). For the factor, $\epsilon = 4$ when $D = 1$, and $= 2$ in every other case. Further, if $m = p^\pi p'^{\pi'} p''^{\pi''} \ldots$, where $p, p', p'' \ldots$ are distinct primes, then $\psi(m) = \psi(p^\pi)\psi(p'^{\pi'})\psi(p''^{\pi''}) \ldots$; if $\mathfrak{A}(m)$ denotes the number of roots n of the congruence $nn + D \equiv 0 \pmod{m}$, and one uses the symbol introduced by Legendre and generalized by Jacobi, then $\psi(p^\pi) = \mathfrak{A}(p^\pi) = 1 + \left(\frac{-D}{p}\right)$ when p does not divide $2D$, but otherwise $= \mathfrak{A}(p^\pi - \frac{1}{p}\mathfrak{A}(p^{\pi+1})$; the number $\mathfrak{A}(p^\pi)$ is always easy to determine (Disqq. Arithm., art. 104). For what follows, however, it suffices to observe that $\mathfrak{A}(p^\pi)$ always becomes independent of π once π exceeds a certain size.

If the variables of the forms in the collection C are assigned all integer values without exception (Disqq. Arithm., art. 181), the total number (m) of representations of the number m becomes $\epsilon f(m)$, where $f(m) = \Sigma\psi\left(\frac{m}{\mu\mu}\right)$ and the sum extends over all square divisors $\mu\mu$ of the number m. This immediately gives

$$f(m) = f(p^\pi p'^{\pi'} p''^{\pi''} \ldots) = f(p^\pi) f(p'^{\pi'}) f(p''^{\pi''}) \ldots$$

and

$$f(p^\pi) = \psi(p^\pi) + \psi(p^{\pi-2}) + \psi(p^{\pi-4}) + \ldots$$

the series being continued as long as the exponents $\pi,\ \pi - 2,\ \pi - 4 \ldots$ do not become negative. When p does not divide $2D$, this gives

$$f(p^\pi) = 1 + \left(\frac{-D}{p}\right) + \left(\frac{-D}{pp}\right) + \ldots + \left(\frac{-D}{p^\pi}\right)$$

and, in general, when m is relatively prime to $2D$,

$$f(m) = \Sigma\left(\frac{-D}{n}\right)$$

where the sum extends over all divisors n of the number m.

These observations immediately establish the statements in the text (III, 1, 2, 3) about the number (m), provided that the first is supplemented by the condition that D must not be divisible by pp (the determination of the number of classes was already reduced in Disqq. Arithm., art. 256, to the case in which D is divisible by no square). At the same time, even without this restriction, the infinite series

$$1 + \frac{f(p)}{p} + \frac{f(pp)}{pp} + \frac{f(p^3)}{p^3} + \dots$$

is found to have the value

$$\frac{1}{1 - \frac{1}{p}} \quad \text{or} \quad \frac{1}{1 - .\frac{1}{p}} \cdot \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

according as $2D$ is or is not divisible by the prime p.

On V.

The remark appended to formula III indicates how the author arrived at the number k of forms in the collection C. Geometrical considerations (compare I, art. 5, and II, art. 4) give the following limit for the quotient

$$\frac{(1) + (2) + (3) + \dots + (m)}{m}$$

as m grows without bound, that is, the average number of representations of an unspecified positive integer,

$$= k\frac{\pi}{\sqrt{D}}$$

A second expression for this same limit can be derived in several ways from the nature of the number $(m) = \epsilon f(m)$ of representations of the number m, determined above. The surviving fragments (I, arts. 7, 8; III and IV) suggest that the author's first approach was as follows.

Let $\theta(m)$ be any function of the positive integer m, and p any prime. From $\theta(m)$ one can always derive a new function $\theta'(m)$ whose value is independent of whether, and how often, p occurs as a factor in m, and which, whenever p does not divide m, agrees with $\theta(m)$. Such a function is obtained by putting $\theta'(m) = \theta\left(\frac{m}{p^\pi}\right)$, where p^π denotes the highest power dividing m with base p; one may say that the function $\theta'(m)$ arises from $\theta(m)$ by elimination of the prime p. If in this way from $f(m)$ one forms a new function $f'(m)$ by eliminating the prime 2, then forms $f''(m)$ from it by eliminating 3, and so on, each successive function will have a more regular course than its predecessors.

If the primes are eliminated one after another in increasing order, such a function $\theta(m)$ will, for infinitely many values of m, have the value $f(1) = 1$, in particular for all values of m smaller than the last prime eliminated. Continuing this process indefinitely brings one ever closer to the function $f^{\infty}(m)$, which for all values of m has the value 1, and whose average value therefore also $= 1$. If it is possible to express the average value of any function $\theta(m)$ in terms of that of its successor $\theta'(m)$, it will also be possible to find the average value of $f(m)$ through an infinite chain of operations.

If p is the prime whose elimination produces $\theta'(m)$ from $\theta(m)$, then $\theta(m) = \theta'(m)f(p^{\pi})$, where p^{π} again denotes the highest power dividing m with base p. When p does not divide $2D$, this readily gives

$$\theta'(m) = \theta(mp) - \left(\frac{-D}{p}\right)\theta(m)$$

Writing for brevity

$$\Theta(m) = \theta(1) + \theta(2) + \ldots + \theta(m)$$
$$\Theta'(m) = \theta'(1) + \theta'(2) + \ldots + \theta(m)$$

one obtains

$$\Theta'(mp) = \Theta(mp) - \left(\frac{-D}{p}\right)\Theta(m)$$

and hence, using ω, ω' for the respective average values of the functions $\theta(m), \theta'(m)$,

$$\omega = \frac{\omega'}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

If, however, the prime p divides $2D$, the functions $\theta(m)$ and $\theta'(m)$ no longer have so simple a relation in general; nevertheless, a similar argument readily gives $\omega = \omega'$ in this case. The relation between ω and ω' can also be derived in both cases as follows. Put

$$\vartheta(m) = \Sigma\theta(\mu)$$

where the sum extends over all numbers μ that are not divisible by p and are no greater than m. Denote by $m', m'', m''' \ldots$, respectively, the greatest integers contained in $\frac{m}{p}, \frac{m'}{p}, \frac{m''}{p} \ldots$. Then

$$\Theta(m) = \vartheta(m) + \vartheta(m')f(p) + \vartheta(m'')f(pp) + \vartheta(m''')f(p^3) + \ldots$$
$$\Theta'(m) = \vartheta(m) + \vartheta(m') + \vartheta(m'') + \vartheta(m''') + \ldots$$

and this gives

$$\frac{\omega}{\omega'} = (1 - \tfrac{1}{p})\{1 + \frac{f(p)}{p} + \frac{f(pp)}{pp} + \frac{f(p^3)}{p^8} + \ldots\}$$

in agreement with the result found above (compare the note on III and IV).

The average value of the function $f(m)$ is therefore equal to the infinite product

$$\Pi \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

in which p must run through all primes not dividing $2D$, and hence

$$k = \frac{\epsilon\sqrt{D}}{\pi}\Pi \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}$$

There remains, however, a concern about the rigor of this deduction, concerning the method of determining the average value of $f(m)$ by successively eliminating all primes. For it is evident that after elimination of the first n primes, the resulting function $f^{(n)}(m)$ agrees in value with the function $f^{\infty}(m) = 1$ as long as m remains smaller than the last prime eliminated. Thus, by choosing n large enough, this agreement can be extended up to any prescribed size of the number m. But this alone by no means proves that, as n grows without bound, the average value of $f^{(n)}(m)$ approaches without limit the average value of $f^{\infty}(m)$, that is, the value 1. How the author intended to fill this gap cannot be determined with certainty from the surviving papers. Yet the formula already given above (in the note on I),

$$1 + 4\{A - \frac{A}{3} + \frac{A}{5} - \frac{A}{7} + \frac{A}{9} - \frac{A}{11}\ldots\}$$

for the number of pairs of numbers whose sum of squares does not exceed A, suggests that the author bypassed the infinite product and directly found, for the average value of $f(m)$, the infinite series

$$\Sigma \left(\frac{-D}{n}\right)\frac{1}{n}$$

in which n must run in increasing order through all positive integers relatively prime to $2D$. The simplest way of indicating this transition seems to be the following.

Let μ be the greatest divisor of a number m among those relatively prime to $2D$, and put $\theta(m) = f(\mu)$. Then $\theta(m)$ is the function obtained by eliminating all primes dividing $2D$ from $f(m)$; according to the preceding discussion, its average value agrees with that of $f(m)$. Since $\theta(m) = \Sigma\left(\frac{-D}{n}\right)$, where n runs through all divisors of μ, that is, all divisors of m relatively prime to $2D$, one obtains the formula analogous to the one above,

$$\Theta(m) = \theta(1) + \theta(2) + \ldots + \theta(m) = \Sigma\left(\frac{-D}{n}\right)\frac{m}{n}$$

where, in the sum on the right, the letter n runs through all numbers relatively prime to $2D$, and only the greatest integer contained in the quotient $\frac{m}{n}$ is to be retained. Arrange the terms of this series so that the numbers n follow in increasing order. The factor $\frac{m}{n}$ then continually decreases, or at least never increases, and the series terminates as soon as $n > m$. Furthermore, the fundamental theorem in the theory of quadratic residues and its generalization imply that the sum of every $\varphi(4D)$ consecutive values of the factor $\left(\frac{-D}{n}\right)$ vanishes. It follows that the sum of any number of consecutive values of this factor never exceeds, in absolute value, the finite bound depending only on the determinant D, namely $\Delta = \varphi(2D)$. Combining these two observations, one readily finds that the sum of all terms following the term $\left(\frac{-D}{n}\right)\frac{m}{n}$ is smaller in absolute value than $\Delta\frac{m}{n}$, and consequently that the quotient $\Theta(m) : m$, as m grows without bound, has as its limit the convergent infinite series

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$$

ordered in the way specified. Having thus found the common average value of the functions $\theta(m)$ and $f(m)$, one immediately obtains

$$k = \frac{\epsilon\sqrt{D}}{\pi}\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$$

It should also be observed that Articles 6 and 8 of paper II point to an approach to the problem that is simpler in some respects and also easy to carry out, in which only representations of odd numbers, or even only of numbers relatively prime to $2D$, are considered.

On VI and VII.

The way in which the author summed the series $\Sigma\left(\frac{-D}{n}\right)\frac{1}{n}$ can be seen from several particular examples found on separate sheets.

If $D \equiv 3 \pmod 4$, the fundamental theorem in the theory of quadratic residues, together with the series

$$\operatorname{cotang} u = \frac{1}{u} + \frac{1}{u-\pi} + \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} + \dots$$

gives

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \Sigma\left(\frac{n}{D}\right)\frac{1}{n} = \frac{\pi}{2D}\Sigma\left(\frac{\nu}{D}\right)\operatorname{cotang}\frac{\nu\pi}{2D}$$

where ν runs through all numbers relatively prime to $2D$ that are smaller than D. Put

$$\sqrt{-1} = i, \quad \cos\frac{2\pi}{D} + i\sin\frac{2\pi}{D} = r$$

and let μ denote all numbers relatively prime to D that are no greater than D. The preceding sum can then readily be transformed into

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\Sigma\left(\frac{\mu}{D}\right)\frac{r^\mu - 1}{r^\mu + 1}$$

Now apply the formula valid for every root ω of the equation $\omega^D = 1$,

$$\frac{\omega - 1}{\omega + 1} = \Sigma(-1)^{\alpha-1}\omega^\alpha$$

in which α must run through the numbers $1, 2, 3 \dots (D-1)$. Reversing the order of summation gives

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\Sigma(-1)^{\alpha-1}\Sigma\left(\frac{\mu}{D}\right)r^{\alpha\mu}$$

The sum over μ can, as is known, be evaluated by means of the theorems proved in the paper *Summatio quarundam serierum singularium.* Restricting attention to the case in which D is divisible by no square, one finds in general

$$\Sigma\left(\frac{\mu}{D}\right) r^{\alpha\mu} = \left(\frac{\alpha}{D}\right) i^{\left(\frac{D-1}{2}\right)^2} \sqrt{D}$$

where one must put $\left(\frac{\alpha}{D}\right) = 0$ if α is not relatively prime to D. In the case $D \equiv 3 \pmod 4$ one therefore obtains

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{4\sqrt{D}}\left(\frac{2}{D}\right)\Sigma(-1)^{\alpha}\left(\frac{\alpha}{D}\right) = \frac{\pi}{2\sqrt{D}}\Sigma\left(\frac{\alpha'}{D}\right)$$

where α' runs through all numbers relatively prime to D that are smaller than $\frac{1}{2}D$. Finally, since $\epsilon = 2$, the number of classes becomes

$$k = \Sigma\left(\frac{\alpha'}{D}\right)$$

If, on the other hand, $D \equiv 1 \pmod 4$, the series

$$\operatorname{cosec} u = \frac{1}{u} - \frac{1}{u-\pi} - \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} - \dots$$

gives in a similar way

$$\begin{aligned}\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} &= \Sigma(-1)^{\frac{n-1}{2}}\left(\frac{n}{D}\right)\frac{1}{n} = \frac{\pi}{2D}\Sigma(-1)^{\frac{\nu-1}{2}}\left(\frac{\nu}{D}\right)\operatorname{cosec}\frac{\nu\pi}{2D} \\ &= \frac{\pi}{2D}\Sigma\left(\frac{\mu}{D}\right)\frac{r^{\mu}}{r^{2\mu}+1}\end{aligned}$$

where the letters ν and μ have their earlier meanings. Excluding the evident case $D = 1$, apply the formula valid for every root ω of the equation $\omega^D = 1$ (except $\omega = 1$),

$$\frac{\omega}{\omega\omega+1} = 1 + \Sigma\omega^{4\alpha''} + \Sigma\omega^{D-4\alpha''}$$

in which α'' must run through the numbers $1, 2, 3 \dots \frac{1}{4}(D-1)$. Again restricting D to be divisible by no square, one obtains

$$\Sigma\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{\sqrt{D}}\Sigma\left(\frac{\alpha''}{D}\right)$$

and hence, since $\epsilon = 2$,

$$k = 2\Sigma\left(\frac{\alpha''}{D}\right)$$

The cases in which D is even could be treated in a very similar way. —

As for determining the number of classes for *positive* determinants D, apart from the final formula given in the text, only a few geometrical figures survive. They depict hyperbolic sectors of finite dimensions, with inequalities beside them that confine the points whose coordinates are the variables of the quadratic forms to the interior of such a sector. These hyperbolic sectors take the place of the ellipses corresponding to quadratic forms of negative determinant. Determining their area again gives the average number of representations, provided that only representations whose variables satisfy those inequalities are admitted. On the other hand, the inequalities serve to isolate just one representation, excluding all others, from the infinitely many representations of a number m that belong to one and the same root n of the congruence $nn - D \equiv 0 \pmod{\frac{m}{\mu\mu}}$ and correspond to all the solutions of the equation $tt - Duu = 1$ (compare Disqq. Arithm., art. 205). The total number of admitted representations of the number m by the collection of all properly primitive forms that are not properly equivalent is then equal to the value of the function $f(m)$, in which only $-D$ is to be replaced by D. As before for negative determinants, considering its properties gives a second expression for the average number of representations; comparing this with the value previously derived by geometrical considerations then immediately determines the number of classes.

On VIII.

Here p denotes a positive prime of the form $4n + 1$; the notation agrees with that used in the paper *Theoria residuorum biquadraticorum* I, art. 23. Thus

$$f \equiv 1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, \tfrac{1}{2}(p-3) \,.\, \tfrac{1}{2}(p-1) \pmod{p}$$
$$p = aa + bb; \quad a \equiv 1 \pmod{4}; \quad b \equiv af \pmod{p}$$

The numbers denoted by α, β are determined by the decomposition $p = \alpha\alpha + 2\beta\beta$. The column f has been added to the two tables found; some gaps in them have also been filled.

The theorem stated in the text is connected with the biquadratic character of the number 2. For, since (compare *Theoria resid. biqu.* I, art. 21)

$$2^{\frac{p-1}{4}} \equiv f^{\frac{1}{2}b} \pmod{p}$$

the congruence

$$b \equiv 2m + a - 1 \pmod{8}$$

implies

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}$$

and conversely the former follows from the latter. The latter congruence is easily proved as follows. Let μ be the number of quadratic residues α_1 lying between 0 and $\frac{1}{4}p$. Then, by VII,

$$m = 2\mu - \tfrac{1}{4}(p-1)$$

and the number of quadratic residues α_2 lying between $\frac{1}{4}p$ and $\frac{1}{2}p$ is $= \frac{1}{4}(p-1) - \mu$. If now $p \equiv 1 \pmod{8}$, so that the number 2 is a quadratic residue, the numbers $2\alpha_1$ and $p - 2\alpha_2$, taken together, form the same collection as the numbers α_1 and α_2. Denoting the product of these numbers by A, one obtains

$$2^{\frac{p-1}{4}} A \equiv (-1)^{\frac{1}{4}(p-1)-\mu} A \pmod{p}$$

and consequently

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu} \equiv f^{2\mu} \equiv f^{m+\frac{1}{4}(p-1)} \pmod{p}$$

Further, in this case $b \equiv 0 \pmod{4}$, and consequently

$$\frac{p-1}{4} = (a+1)\frac{a-1}{4} + \frac{bb}{4} \equiv 2\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod{4}$$

which gives the congruence to be proved,

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}$$

If, on the other hand, $p \equiv 5 \pmod 8$, so that the number 2 is a quadratic nonresidue, the numbers $2\alpha_1$ and $p - 2\alpha_2$ comprise all the quadratic nonresidues between 0 and $\frac{1}{2}p$. Denote their product by B, and again denote the product of the numbers α_1 and α_2 by A. Then

$$f \equiv AB, \quad (-1)^{\frac{p-1}{4}-\mu} 2^{\frac{p-1}{4}} A \equiv B \pmod p$$

Squaring these two congruences, taking into account that

$$ff \equiv -1, \quad 2^{\frac{p-1}{2}} \equiv -1 \pmod p$$

gives

$$-1 \equiv AABB, \quad -AA \equiv BB$$

and hence $A^4 \equiv +1$. Now A is a product of quadratic residues, so AA is a product of biquadratic residues and is therefore itself a biquadratic residue. Thus $AA \equiv +1$ must hold, because -1 is a biquadratic nonresidue. It follows that

$$(-1)^{\frac{p-1}{4}-\mu} 2^{\frac{p-1}{4}} \equiv AB \equiv f \pmod p$$

and

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu-1} f \equiv f^{2\mu-1} \equiv f^{m+\frac{p-5}{4}} \pmod p$$

Finally, in this case $b \equiv 2 \pmod 4$, and consequently

$$\frac{p-5}{4} = (a+1)\frac{a-1}{4} + \frac{bb-4}{4} \equiv 2\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod 4$$

which again gives the congruence to be proved,

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod p$$

On IX.

Let p be a positive odd number divisible by no square, and put

$$S_r = \Sigma\left(\frac{s_r}{p}\right)$$

where s_r must run through all numbers relatively prime to p that lie between $(r-1)\frac{p}{8}$ and $r\frac{p}{8}$. Denote the numbers of properly primitive forms that are not properly equivalent, for the determinants $-p$ and $-2p$, by C_1 and C_2, respectively. Then (compare DIRICHLET, Recherches sur diverses applications etc., § 11, in CRELLE's Journal XXI)

$$C_1 = 2(S_1 + S_2), \quad C_2 = 2(S_1 - S_4)$$

or

$$C_1 = S_1 + S_2 + S_3 + S_4, \quad C_2 = 2(S_2 + S_3)$$

according as $p \equiv 1$ or $\equiv 3 \pmod 4$. Further, the numbers s_1 and s_2, taken together, form the same collection as the numbers $2s_1$ and $p-2s_4$; likewise the numbers s_3 and s_4 form the same collection as the numbers $2s_2$ and $p-2s_3$. In the case $p \equiv 1 \pmod 4$, the sum $S_1+S_2+S_3+S_4 = 0$. These observations give two further relations between the four sums S_1, S_2, S_3, S_4 in both cases, so that each can be expressed in terms of C_1 and C_2. In this way, when $p \equiv 1 \pmod 4$, one obtains

$$S_1 = S_8 = \tfrac{1}{4}\left(\frac{2}{p}\right) C_1 + \tfrac{1}{4}C_2$$

$$S_2 = S_7 = \tfrac{1}{4}\left(2 - \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

$$S_3 = S_6 = -\tfrac{1}{4}\left(2 + \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_4 = S_5 = \tfrac{1}{4}\left(\frac{2}{p}\right) C_1 - \tfrac{1}{4}C_2$$

and, when $p \equiv 3 \pmod 4$,

$$S_1 = -S_8 = \tfrac{1}{4}\left(3 + \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

$$S_2 = -S_7 = -\tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_3 = -S_6 = \tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 + \tfrac{1}{4}C_2$$

$$S_4 = -S_5 = \tfrac{1}{4}\left(1 - \left(\frac{2}{p}\right)\right) C_1 - \tfrac{1}{4}C_2$$

If p is a prime, the formulas given in the text for the numbers of quadratic residues in the individual eighths follow immediately.

On X.

Let p be a positive number divisible by no square, of the form $6n \pm 1$, and put

$$S_r = \Sigma \left(\frac{s_r}{p} \right)$$

where s_r must run through all numbers relatively prime to p that lie between $(r-1)\frac{p}{12}$ and $r\frac{p}{12}$. Denote the numbers of properly primitive forms that are not properly equivalent, for the determinants $-p$ and $-3p$, by C_1, C_3. One readily finds (compare DIRICHLET, Recherches etc., § 11, or the note on VI and VII)

$$C_1 = 2(S_1 + S_2 + S_3), \quad C_3 = 2(S_1 + S_2 - S_5 - S_6)$$

or

$$C_1 = S_1 + S_2 + S_3 + S_4 + S_5 + S_6, \quad C_3 = 2(S_2 + S_3 + S_4 + S_5)$$

according as $p \equiv 1$ or $\equiv 3 \pmod 4$. Taking into account also that

the	numbers	s_1 and s_2	coincide with	the	numbers	$2s_1$ and $p - 2s_6$
„	„	s_3 and s_4	„	„	„	$2s_2$ and $p - 2s_5$
„	„	s_5 and s_6	„	„	„	$2s_3$ and $p - 2s_4$

and likewise

the	numbers	s_1, s_2, s_3	coincide with	the	numbers	$3s_1,\ 3s_5 - p,\ p - 3s_4$
„	„	s_4, s_5, s_6	„	„	„	$3s_2,\ 3s_6 - p,\ p - 3s_3$

and that, in the case $p \equiv 1 \pmod 4$, the sum $S_1 + S_2 + S_3 + S_4 + S_5 + S_6 = 0$, one obtains four further relations, besides the two above, between the six sums $S_1, S_2 \ldots S_6$, so that all of them can be determined from C_1 and C_3. In this way, when $p \equiv 1 \pmod 4$, one obtains

$$S_1 = S_{12} = \tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_2 = S_{11} = -\tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_3 = S_{10} = \tfrac{1}{2} C_1 - \tfrac{1}{6}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

$$S_4 = S_9 = -\tfrac{1}{2} C_1 - \tfrac{1}{6}\left(2 - \left(\frac{2}{p}\right)\right) C_3$$

$$S_5 = S_8 = \tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 - \tfrac{1}{12}\left(5 - \left(\frac{2}{p}\right)\right) C_3$$

$$S_6 = S_7 = -\tfrac{1}{4}\left(1 + \left(\frac{3}{p}\right)\right) C_1 + \tfrac{1}{12}\left(1 + \left(\frac{2}{p}\right)\right) C_3$$

and, when $p \equiv 3 \pmod 4$,

$$S_1 = -S_{12} = \tfrac{1}{12}\left(9 + 3\left(\frac{2}{p}\right) - \left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1 - \tfrac{1}{4} C_3$$

$$S_2 = -S_{11} = \tfrac{1}{4}\left(-1 + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1 + \tfrac{1}{4} C_3$$

$$S_3 = -S_{10} = \tfrac{1}{6}\left(-\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1$$

$$S_4 = -S_9 = \tfrac{1}{6}\left(3 - 2\left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1$$

$$S_5 = -S_8 = \tfrac{1}{4}\left(-1 - \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right) C_1 + \tfrac{1}{4} C_3$$

$$S_6 = -S_7 = \tfrac{1}{12}\left(3 - 3\left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) - \left(\frac{6}{p}\right)\right) C_1 - \tfrac{1}{4} C_3$$

If p is a prime, the formulas given in the text follow from the first system; for the other cases, similar formulas are obtained from the second system.

R. Dedekind.

GEOMETRICAL ASPECT OF TERNARY FORMS.

Let a point in space (0) be chosen as the origin. Let the displacements from it to three other points P, P', P'', which do not lie in one plane with it, be t, t', t'', respectively; whenever confusion is impossible, the points P, P', P'' themselves may be denoted by (t). (t'), (t'').

Further, let (t, t') generally denote the product of the lengths of the two lines t, t' and the cosine of their inclination, etc.

In general, $(\alpha t + \alpha' t' + \alpha'' t'' + \ldots \quad \beta u + \beta' u' + \beta'' u'' + \ldots)$ is obtained by carrying out the multiplication

$$(\alpha t + \alpha' t' + \alpha'' t'' + \ldots) \times (\beta u + \beta' u' + \beta'' u'' + \ldots)$$

and replacing $tu, tu', tu'', t'u', t'u'' \ldots$ and so on by $(t, u), (t, u'), (t, u''), (t', u')$, (t', u'') and so on.

Every point in space can be represented by a trinomial

$$(xt + x't' + x''t'')$$

For all points in a given plane, an equation

$$\lambda x + \lambda' x' + \lambda'' x'' = L$$

will then hold, where $\lambda, \lambda', \lambda'', L$ are fixed numbers. For a plane through the three points $\mu t, \mu' t', \mu'' t''$,

$$\lambda\mu = \lambda'\mu' = \lambda''\mu'' = L$$

Writing

$$(t, t) = a, \quad (t', t') = a', \quad (t'', t'') = a'',$$
$$(t', t'') = b, \quad (t, t'') = b', \quad (t, t') = b''$$

and

$$a'a'' - bb = A, \quad aa'' - b'b' = A', \quad aa' - b''b'' = A''$$
$$b'b'' - ab = B, \quad bb'' - a'b' = B', \quad bb' - a''b'' = B''$$
$$D = aa'a'' + 2bb'b'' - abb - a'b'b' - a''b''b''$$

gives

$$\begin{array}{rcll} T & = & At + B''t' + B't'' & \text{perpendicular to } t' \text{ and } t'' \\ T' & = & B''t + A't' + Bt'' & t \text{ and } t'' \\ T'' & = & B't + Bt' + A''t'' & t \text{ and } t' \end{array}$$

and, in general, if

$$\lambda x + \lambda' x' + \lambda'' x'' = L$$

is the equation of a plane, the line

$$\lambda T + \lambda' T' + \lambda'' T''$$

will be perpendicular to that plane.

Further,

$$\begin{aligned} aT + b''T' + b'T'' &= Dt \\ b''T + a'T' + bT'' &= Dt' \\ b'T + bT' + a''T'' &= Dt'' \end{aligned}$$

and the lines t, t', t'' are perpendicular to the planes whose equations

$$\begin{aligned} ax + b''x' + b'x'' &= \text{Const} \\ b''x + a'x' + bx'' &= \text{Const} \\ b'x + bx' + a''x'' &= \text{Const} \end{aligned}$$

Twice the area of the triangle through the points $mt, m't', m''t''$ equals the square root of the value of the form

$$F \ldots \begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$$

on substituting $X = m'm'', X' = mm'', X'' = mm'$, while six times the volume of the pyramid formed with the point 0 becomes $= mm'm''\sqrt{D}$; hence the altitude is

$$= \sqrt{\frac{D}{F(\frac{1}{m}, \frac{1}{m'}, \frac{1}{m''})}}$$

T, T', T'' relate to the form $\begin{pmatrix} AD, & A'D, & A''D \\ BD, & B'D, & B''D \end{pmatrix}$ as t, t', t'' do to $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$

The three roots of the equation

$$0 = p^3 - pp(a + a' + a'') + p(A + A' + A'') - D$$

give the squares of the three principal axes of an ellipsoid inscribed in the parallelepiped to which the positive ternary form

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \quad \text{with adjoint} \quad \begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \quad \text{and det.} = -D$$

relates.

Expressing spatial relations relative to a given tetrahedron.

Let $(0), (1), (2), (3)$ denote the four vertices, opposite faces and altitudes. Each point in space P, relative to an arbitrary origin M, then has four coordinates x, x', x'', x''', subject, however, to the relation

$$x + x' + x'' + x''' = 0$$

Here x denotes the quotient obtained by dividing the distance of the point P from a plane drawn through M parallel to the plane (0) by the altitude (0), and so on.

In general,

$$\begin{aligned} -(PM)^2 = {} & xx'(01)^2 + xx''(02)^2 + xx'''(03)^2 \\ & + x'x''(12)^2 + x'x'''(13)^2 + x''x'''(23)^2 \end{aligned}$$

The fundamental law of crystallization can be stated most briefly as follows: any five planes occurring in it satisfy the following relation:

If their normals on the sphere are $(0), (1), (2), (3), (4)$, the products $\sin 102 . \sin 304$, $\sin 103 . \sin 204$, $\sin 203 . \sin 104$ are always in a rational ratio; if this is $\alpha : \beta : \gamma$, then $\beta = \alpha + \gamma$.

If the coordinates of the 5 points on the sphere are

$$\left.\begin{array}{ccc} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \\ a''' & b''' & c''' \\ 0 & 0 & 1 \end{array}\right\} \quad \text{then the products must} \quad \begin{array}{l} (ab' - ba') . (a''b''' - b''a''') \\ (ab'' - ba'') . (a'''b' - b'''a') \\ (ab''' - ba''') . (a'b'' - b'a'') \end{array}$$

be in a rational ratio.

In general, let $1, 2, 3, 4, 5$ be the 5 points on the sphere and 0 its centre; then, if 12 denotes the volume of the tetrahedron 0345,

$$\left.\begin{array}{l} 23 . 45 \\ 24 . 53 \\ 25 . 34 \end{array}\right\} \quad \text{are in a rational ratio}$$

and likewise

$$\left.\begin{array}{l} 12 . 34 \\ 13 . 42 \\ 14 . 23 \end{array}\right\} \quad \text{and so on}$$

Transformations of the form $\left(\begin{smallmatrix}5,&5,&5\\-1,&-1,&-1\end{smallmatrix}\right)$ **Det.** $= 108$

					Chaux carbonatée
$\left\{\begin{smallmatrix}+1&+1&-1\\-1&+1&+1\\+1&-1&+1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}17&17&17\\-7&-7&-7\end{smallmatrix}\right)$		$\left(\begin{smallmatrix}240&240&240\\+168&+168&+168\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10&10&10\\+7&+7&+7\end{smallmatrix}\right)$	equiaxe
	36 . 108		256 . 11664	216	
$\left\{\begin{smallmatrix}+1&+1&0\\0&+1&+1\\+1&0&+1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}8&8&8\\+2&+2&+2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&4&4\\+1&+1&+1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}15&15&15\\-3&-3&-3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&5&5\\-1&-1&-1\end{smallmatrix}\right)$	inverse
	4 . 108	54	27 . 108	54	
$\left\{\begin{smallmatrix}+2&+1&+1\\+1&+2&+1\\+1&+1&+2\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}20&20&20\\+14&+14&+14\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10&10&10\\+7&+7&+7\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}51&51&51\\-21&-21&-21\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}17&17&17\\-7&-7&-7\end{smallmatrix}\right)$	contrastante
	16 . 108	216	432 . 108	16 . 108	
$\left\{\begin{smallmatrix}+1&+2&+2\\+2&+1&+2\\+2&+2&+1\end{smallmatrix}\right\}$	$\left(\begin{smallmatrix}29&29&29\\+23&+23&+23\end{smallmatrix}\right)$		$\left(\begin{smallmatrix}312&312&312\\-138&-138&-138\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}52&52&52\\-23&-23&-23\end{smallmatrix}\right)$	mixte
	25 . 108		67500 . 108	33750	

Writing the original form generally as $\left(\begin{smallmatrix}t,&t,&t\\u,&u,&u\end{smallmatrix}\right)$ and a derived form as $\left(\begin{smallmatrix}T,&T,&T\\U,&U,&U\end{smallmatrix}\right)$ gives

$$\begin{aligned}
1,&\quad T = 3t - 2u \quad U = -t + 2u\\
2,&\quad T = 2t + 2u \quad U = t + 3u\\
3,&\quad T = 6t + 10u \quad U = 5t + 11u\\
4,&\quad T = 9t + 16u \quad U = 8t + 17u
\end{aligned}$$

The form $\left(\begin{smallmatrix}1,&3,&k\\0,&0,&0\end{smallmatrix}\right)$ is transformed by the substitution

$$\begin{aligned}
x &= u + u' - 2u'' \quad \text{inversely} \quad 6u = x + 3y + 2z\\
y &= u - u' \qquad\qquad\qquad\quad 6u' = x - 3y + 2z\\
z &= u + u' + u'' \qquad\qquad\quad 6u'' = -2x + 2z
\end{aligned}$$

$$x \equiv z' \pmod 3, \quad x \equiv y \pmod 2$$

into $\left(\begin{smallmatrix}4+k,&4+k,&4+k\\k-2,&k-2,&k-2\end{smallmatrix}\right)$

To obtain calcite, set $k = 0{,}973103$.

Hind the complex values of the orthographic projection of three straight lines of equal length and perpendicular to one another be a, b, c, then $aa + bb + cc = 0$; in general, with p and q denoting arbitrary complex numbers, one may set

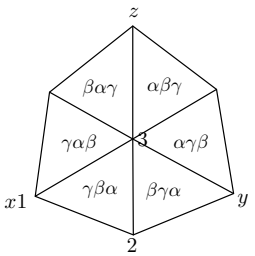
$$a = (p - q)(q - pii), \quad b = (q - qi)(pii - pi),$$
$$c = (qi - p)(pi - q)$$

Hexakisoctahedron.



Equation: $px + qy + rz = 1$

Coordinates.



1.	$\frac{1}{\gamma}$	0	0
2.	$\frac{1}{\beta+\gamma}$	$\frac{1}{\beta+\gamma}$	0
3.	$\frac{1}{\alpha+\beta+\gamma}$	$\frac{1}{\alpha+\beta+\gamma}$	$\frac{1}{\alpha+\beta+\gamma}$

$\alpha < \beta < \gamma$

Six times the volume of an elementary pyramid

$$= \frac{1}{\gamma \,.\, (\beta+\gamma)(\alpha+\beta+\gamma)}$$

All [faces] are circumscribed about a sphere whose radius

$$= \frac{1}{\sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}$$

Twice the area of a triangle

$$= \frac{\sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}{\gamma(\beta+\gamma)(\alpha+\beta+\gamma)}$$

Edge

$$1\,.\,2 = \frac{\sqrt{(\beta\beta+\gamma\gamma)}}{\gamma(\beta+\gamma)},$$

$$1\,.\,3 = \frac{\sqrt{((\alpha+\beta)^2+2\gamma\gamma)}}{\gamma(\alpha+\beta+\gamma)},$$

$$2\,.\,3 = \frac{\sqrt{(2\alpha\alpha+(\beta+\gamma)^2)}}{(\beta+\gamma)(\alpha+\beta+\gamma)}$$

Cosine of the angle between the edges $3\,.\,1\,.\,2$

$$= \frac{\alpha\beta+\beta\beta+\gamma\gamma}{\sqrt{(\beta\beta+\gamma\gamma)((\alpha+\beta)^3+2\gamma\gamma)}}$$

Sine

$$= \frac{\gamma \,.\, \sqrt{(\alpha\alpha+\beta\beta+\gamma\gamma)}}{\sqrt{(\beta\beta+\gamma\gamma)((\alpha+\beta)^2+2\gamma\gamma)}}$$

Values occurring.

	α	β	γ	
7.	0.	0.	1	Hexahedron
3.	0.	1.	1	Rhombic dodecahedron
6.	0.	1.	2	Tetrakishexahedron
	0.	1.	3	
	0.	2.	3	
1.	1.	1.	1	Octahedron
5.	1.	1.	2	Deltoidal icositetrahedron
	1.	1.	3	

	α	β	γ	
2.	1.	2.	2.	Triakisoctahedron
4.	1.	2.	3.	Hexakisoctahedron
	1.	2.	4.	
2.	1.	3.	3.	Triakisoctahedron
4.	1.	3.	5.	Hexakisoctahedron
2.	2.	3.	3	Triakisoctahedron
	2.	3.	4?	
	3.	5.	11	

REMARKS.

Besides the preceding notes, which in part develop the ideas given in the review of SEEBER's investigations of ternary forms, the manuscript records several crystal measurements made by Gauss himself with an eight-inch REICHENBACH theodolite. Each record gives the date of the observation, showing that this investigation belongs to July 1831.

Of the theory of indefinite ternary quadratic forms, the manuscripts left behind contain only the following theorem, probably written down while the Disqu. Arr. were being prepared:

'All transformations of the ternary form

$$\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

into itself are given by the formula

$$\begin{array}{lll} \alpha\delta+\beta\gamma & \alpha\beta-\gamma\delta & \alpha\beta+\gamma\delta \\ \alpha\gamma-\beta\delta & \frac{1}{2}(\alpha\alpha+\delta\delta-\beta\beta-\gamma\gamma) & \frac{1}{2}(\alpha\alpha+\gamma\gamma-\beta\beta-\delta\delta) \\ \alpha\gamma+\beta\delta & \frac{1}{2}(\alpha\alpha+\beta\beta-\gamma\gamma-\delta\delta) & \frac{1}{2}(\alpha\alpha+\beta\beta+\gamma\gamma+\delta\delta) \end{array}$$

with $\alpha, \beta, \gamma, \delta$ chosen so that $\alpha\delta - \beta\gamma = 1$.'

All transformations in which the nine coefficients are integers are obtained by taking for $\alpha, \beta, \gamma, \delta$ both all integers satisfying the condition equation, specifically two even and two odd, and all odd multiples of $\sqrt{\frac{1}{2}}$ satisfying the same condition equation $\alpha\delta - \beta\gamma = 1$.

On page 309. Chaux carbonatée équiaxe, inverse, contrastante and mixte are the names used by HAUY (Traité de Minéralogie 1801, volume II, pp. 132, 137).

The table of transformations of the form $\begin{pmatrix} 5, & 5, & 5 \\ 1, & 1, & 1 \end{pmatrix}$ gives, in the first vertical column, the coefficients of the substitution; in the second, the resulting new form; in the third, the primitive form corresponding to the latter, if it is not already primitive; and in the fourth, its adjoint.

SCHERING.

ON THE THEORY OF BIQUADRATIC RESIDUES.

[I.]

1.

We extend the domain of higher arithmetic by including complex quantities as well. In this investigation, we call every quantity $x + iy$ a complex integer when x, y are real integers.

2.

The infinitely many complex integers are most conveniently represented visually by points in an unbounded plane; we call the point whose horizontal coordinate is x and vertical coordinate y the point $x + iy$; all points representing integers will be called integer points.

3.

To fix a definite convention, the horizontal coordinates shall always be positive to the left, and the vertical coordinates positive upwards.

4.

The straight line drawn from the point $x + iy$ to the point $x' + iy'$ will be called the straight line $(x + iy, x' + iy')$; wherever it matters, we also take its direction into account, and therefore distinguish the straight line $x+iy, x'+iy'$ from $x' + iy', x + iy$.

5.

For brevity, we shall also denote complex quantities such as $x + iy$ by a single letter, such as z.

6.

We call the figure bounded by the straight lines $zz', z'z'', z''z''' \dots z^{n-1}z^n$, $z^n z$ the figure $zz'z''z''' \dots z^n$. We do not exclude the case where some of these lines intersect.

7.

By $S(z, z', z'' \dots z^n)$ we generally denote a sum of as many real integers as there are integer points inside the figure, assigning the number ± 1, ± 2, ± 3, etc., to each point around which the boundary of the figure passes once, twice, three times, and so on; the upper signs apply when the boundary surrounds the point so that it lies on the right side of the figure, and the lower signs in the opposite case. Thus, if no sides of the figure intersect, $S(z, z', z'' \dots)$ is simply the number of points inside the figure, taken positively or negatively.

8.

It is evident that always

$$\begin{aligned} S(z, z', z'' \dots z^n) &= S(z', z'', z''' \dots z^n, z) \\ &= S(z'', z''' \dots z') \text{ etc.} \\ &= -S(z^n, z^{n-1} \dots z'', z', z) \\ &= -S(z^{n-1} \,.\, z^{n-2} \dots z', z, z^n) \text{ etc.} \end{aligned}$$

9.

How points on the boundary itself are to be treated must still be specified more closely. In many cases no integer points can lie on the boundary at all; no convention is then needed. But if such points lie on the boundary zz', inserting between z and z' a $+$ indicates that they are to be treated as if they lay to the right of the boundary, and a $-$ as if they lay to the left. We shall also sometimes insert a 0 or $\frac{1}{2}$ to indicate that they are to be counted either not at all or only at half their value on each side. If any of the points z, z', z'', etc., is itself an integer point, it is not counted at all unless the contrary is expressly stated, except insofar as it may also occur as a point that is not a vertex.

10.

Theorems. If all z, z', z'', etc., are increased by the same integer, S remains unchanged.

If i is replaced by $-i$ and every connecting sign by its opposite, S changes only its sign.

$$\begin{aligned} S(z, z', z'' \ldots z^n) &= S(z, u, u' \,..\, u^n, z', z'', z^n) \\ &\quad - S(z, u, u' \,..\, u^n, z') \\ &= S(z, u, u', u'' \,..\, u^n, z^m, z^{m+1} \,..\, z^n) \\ &\quad - S(z, u, u', u'' \,..\, u^n, z^m, z^{m-1} \,..\, z', z) \end{aligned}$$

Here the connecting signs must correspond, but must be reversed between the terms that run backwards.

If ζ is an integer $= a + bi$, then, when opposite connecting signs are opposite,

$$S(z, z', z' + \zeta, z + \zeta) = [bx' - ay'] - [bx - ay]$$

Here, if $bx' - ay'$ is itself an integer, that integer must be taken for $[bx' - ay']$ when the connecting sign between z' and $z' + \zeta$ is $+$, but 1 or $\frac{1}{2}$ less when this sign is $-$ or $\frac{1}{2}$; the reverse applies to $bx - ay$.

The formula holds only when a and b have no common divisor; if their greatest common divisor is $= h$, the expression to use instead is

$$h\left[\frac{bx' - ay'}{h}\right] - h\left[\frac{bx - ay}{h}\right]$$

11.

Let us now turn more closely to our subject itself. If, for the modulus $m = a + bi$, the numbers f, f', f'', etc., are such that, first, they are all incongruent to one another modulo m, and, second, every integer must necessarily be congruent to one of them, we call the collection of numbers f, f', f'', etc., the system of primitive residues of m. Their number is always $= aa + bb$.

12.

The system of primitive residues can be formed in many ways. The simplest is to choose the points inside the square $0, m, (1 + i)m, im$, but the following must also be included:

I. the point or quantity 0;

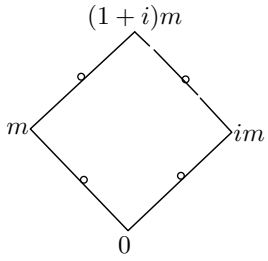
II. all points on two boundary lines that are not opposite one another.

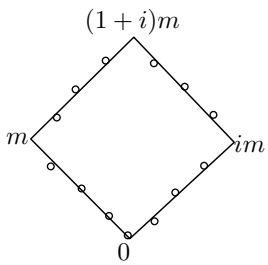
Instead of taking all points on one of the 4 boundary lines, one can also take them on several at once.

This choice of points on the boundary lines, if any lie on them, can be made in several ways that satisfy the above conditions. The following method is the simplest.

On the boundary line $0, m$, take all points between 0 and $\frac{1}{2}m$, inclusive, and on the boundary line $0, im$ all points from $\frac{1}{2}im$ to im, exclusive; proceed similarly on the other two.

These two methods can be represented visually as follows:





13.

If the following are excluded from the primitive points:

I. only the point 0, when a is even and b odd, or the reverse;

II. the points 0 and $\frac{1}{2}(1+i)m$, when a and b are both odd;

III. the four points $0, \frac{1}{2}m, \frac{1}{2}(1+i)m, \frac{1}{2}im$, when a and b are both even,

we call the remaining points proper primitive points and the excluded ones improper. The number of the former is therefore

$$\begin{array}{rrcl} \text{in case} & \text{I} & = & aa+bb-1 \\ & \text{II} & = & aa+bb-2 \\ & \text{III} & = & aa+bb-4 \end{array}$$

and is thus always divisible by 4.

14.

These proper primitive points can be divided into 4 classes F, F', F'', F''' so that

$$\begin{array}{llll} iF \equiv F' & iF' \equiv F'' & iF'' \equiv F''' & iF''' \equiv F \\ -F \equiv F'' & -F' \equiv F''' & -F'' \equiv F & -F''' \equiv F' \\ -iF \equiv F''' & -iF' \equiv F & -iF'' \equiv F' & -iF''' \equiv F'' \end{array}$$

The following extremely important theorem now holds.

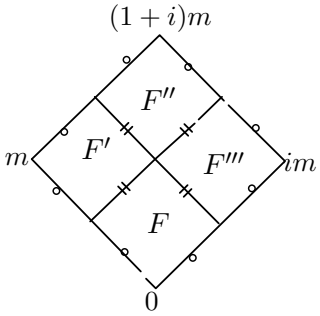
Let M be a number with no factor in common with m. Of the numbers MF, the number belonging to the class F is n,

$$\begin{array}{ll} F' & n' \\ F'' & n'' \\ F''' & n''' \end{array}$$

and let the least residue of $n' + 2n'' + 3n''$ modulo 4 be $= N$, so that N equals one of the 4 numbers $0, 1, 2, 3$. Under this assumption, N is *independent* of the way the primitive residues are distributed into classes. We call it the decident of the biquadratic relation of the number M to m.

15.

The simplest distribution is certainly the following:



In particular cases, however, another distribution may be more advantageous.

16.

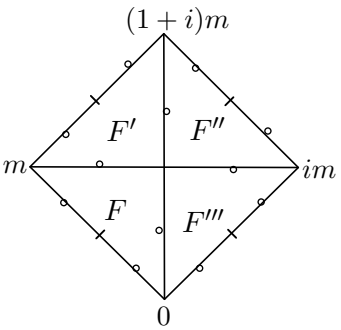
If f, f', f'', etc., are all the primitive residues of the modulus m, then

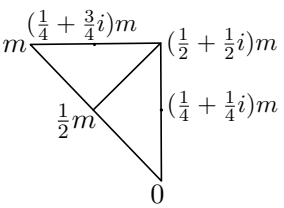
$$\begin{aligned}
&S(z + \tfrac{f}{m},\ z' + \tfrac{f}{m},\ z'' + \tfrac{f}{m},\ \text{etc.}) \\
&+ S(z + \tfrac{f'}{m},\ z' + \tfrac{f'}{m},\ z'' + \tfrac{f'}{m},\ \text{etc.}) \\
&+ S(z + \tfrac{f''}{m},\ z' + \tfrac{f''}{m},\ z'' + \tfrac{f''}{m},\ \text{etc.}) \\
&+ \text{etc.} \\
&= S(mz, mz', mz'',\ \text{etc.}
\end{aligned}$$

17.

Theory of the biquadratic residue $1 + i$.

The modulus must have no divisor in common with the residue. We therefore assume that one of the numbers a and b is even and the other odd. The following diagram shows the distribution of the proper primitive residues into the four classes:





Count towards n all numbers on

$$\text{the line } 0 \ldots \tfrac{1}{2}m \qquad \text{number } = g$$

Towards n', all numbers on

$$\text{the line } 0 \ldots (\tfrac{1}{4} + \tfrac{1}{4}i)m \qquad \text{number } = g'$$

Towards n'', all numbers inside

$$\text{the triangle } \tfrac{1}{2}m, m, (\tfrac{1}{2} + \tfrac{1}{2}i)m \qquad \text{number } = h$$

Towards n''', all numbers inside

$$\text{the triangle } 0, \tfrac{1}{2}m, (\tfrac{1}{2} + \tfrac{1}{2}i)m \qquad \text{number } = h'$$

and also all numbers on

$$\text{the line } (\tfrac{1}{4} + \tfrac{1}{4}i)m \,..\, (\tfrac{1}{2} + \tfrac{1}{2}i)m \qquad \text{number } = g''$$

We always have $g' + g'' = g$, $aa + bb = p$, $\frac{1}{4}(p-1) = g + g' + g'' + h + h'$. The decident is therefore

$$D = S(0_{(+)}, \tfrac{1}{2}m, (\tfrac{1}{2} + \tfrac{1}{2}i)m_{(-)}) + \tfrac{1}{2}(p-1) + 2g''$$

Now suppose that, for the modulus $m + 1 + i$,

g	changes to	G
g'		G'
g''		G''
h		H
h'		H'

then we have

$$\begin{aligned}
&\Delta S(0_{(+)}, \tfrac{1}{2}m, (\tfrac{1}{2} + \tfrac{1}{2}i)m_{(-)}) \\
&\quad = +S(0_{(+)}, (\tfrac{1}{2} + \tfrac{1}{2}i)m, (\tfrac{1}{2} + \tfrac{1}{2}i)m + i_{(-)}) \\
&\qquad - S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m + \tfrac{1}{2} + \tfrac{1}{2}i_{(-)}) \\
&\qquad - S(\tfrac{1}{2}m, (\tfrac{1}{2} + \tfrac{1}{2}i)m, (\tfrac{1}{2} + \tfrac{1}{2}i)m + i,\ \tfrac{1}{2}m + \tfrac{1}{2} + \tfrac{1}{2}i)
\end{aligned}$$

The last of these S is

$$= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] - S((\tfrac{1}{2} + \tfrac{1}{2}i)m, \tfrac{1}{2}m, \tfrac{1}{2}m + \tfrac{1}{2} - \tfrac{1}{2}i)$$

whether a is odd or even

$$\begin{aligned}
&= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] - S(-\tfrac{1}{2} + \tfrac{1}{2}i, \tfrac{1}{2}m - \tfrac{1}{2} + \tfrac{1}{2}i, \tfrac{1}{2}m + i) \\
&= \left[\tfrac{1}{2}(a-b)\right] - \left[\tfrac{1}{2}a\right] + S(0_{(+)}, \tfrac{1}{2}m, \tfrac{1}{2}m + \tfrac{1}{2} + \tfrac{1}{2}i_{(-)}) \\
&\quad - S(0_{(+)}, (\tfrac{1}{2} + \tfrac{1}{2}i)m, (\tfrac{1}{2} + \tfrac{1}{2}i)m + i_{(-)})
\end{aligned}$$

Thus

$$\begin{aligned}\Delta D = & -\left[\tfrac{1}{2}(a-b)\right]+\left[\tfrac{1}{2}a\right]\\ & +2S(0_{(+)},(\tfrac{1}{2}+\tfrac{1}{2}i)m,(\tfrac{1}{2}+\tfrac{1}{2}i)m+i_{(-)})+a+b+1\\ & -2S(0_{(+)},\tfrac{1}{2}m,\tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)})-2g''+2G''\end{aligned}$$

All the connecting signs apply to the case where $a-b$ is positive; otherwise take the opposite signs.

We further split $S(0_{(+)},(\frac{1}{2}+\frac{1}{2}i)m,(\frac{1}{2}+\frac{1}{2}i)m+i_{(-)})$ into

$$\begin{aligned}& S(0_{(+)},(\tfrac{1}{4}+\tfrac{1}{4}i)m,(\tfrac{1}{4}+\tfrac{1}{4}m)+\tfrac{1}{2}i_{(-)})\\ & +\left[\tfrac{1}{2}(a-b)\right]-\left[\tfrac{1}{4}(a-b)\right]\\ & -S((\tfrac{1}{2}+\tfrac{1}{2}i)m_{(-)},(\tfrac{1}{4}+\tfrac{1}{4}i)m,(\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}i_{(-)})\end{aligned}$$

The last part

$$\begin{aligned}&= -S(\tfrac{1}{2}+\tfrac{1}{2}i_{(-)},(-\tfrac{1}{4}-\tfrac{1}{4}i)m+\tfrac{1}{2}+\tfrac{1}{2}i,\ (-\tfrac{1}{4}-\tfrac{1}{4}i)m+\tfrac{1}{2}{}_{(+)})\\ &= -S(-\tfrac{1}{2}-\tfrac{1}{2}i_{(-)},(\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}{}_{(+)})\\ &= -S(-\tfrac{1}{2}-\tfrac{1}{2}i_{(+)},(\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}{}_{(-)})+g''-G''\\ &= S(0_{(+)},(\tfrac{1}{4}+\tfrac{1}{4}i)m,(\tfrac{1}{4}+\tfrac{1}{4}i)m+\tfrac{1}{2}i_{(-)})\\ &\quad -S(0_{(+)},\tfrac{1}{2}m,\tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(-)})+g''-G''\end{aligned}$$

This therefore gives

$$\begin{aligned}\Delta D = & +\left[\tfrac{1}{2}(a-b)\right]+\left[\tfrac{1}{2}a\right]\\ & -4S(-\tfrac{1}{2}-\tfrac{1}{2}i_{(+)},\tfrac{1}{4}+\tfrac{1}{4}im-\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{4}+\tfrac{1}{4}i)m-\tfrac{1}{2}{}_{(-)})\\ & -2\left[\tfrac{1}{4}(a-b)\right]+a+b+1\end{aligned}$$

Increasing the modulus by $1-i,-1+i,-1-i$ requires no separate investigation, because the moduli $m, im, -m, -im$ evidently have equal decidents. We therefore have the following theorems:

If the modulus and its decident are $a+bi, = D$, then the following moduli have the indicated decidents:

$a+1+(b+1)i$	$D+a+b+1+[\frac{1}{2}a]+[\frac{1}{2}(a-b)]-2[\frac{1}{4}(a-b)]$
$a+1+(b-1)i$	$D+a-b+1+[-\frac{1}{2}b]+[-\frac{1}{2}(a+b)]-2[-\frac{1}{4}(a+b)]$
$a-1+(b+1)i$	$D-a+b+1+[\frac{1}{2}b]+[\frac{1}{2}(a+b)]-2[\frac{1}{4}(a+b)]$
$a-1+(b-1)i$	$D-a-b+1+[-\frac{1}{2}a]+[\frac{1}{2}(b-a)]-2[\frac{1}{4}(b-a)]$

This also gives

		or when a is odd
$a+2+bi$	$D-\frac{a-b-3}{2}+2[\frac{1}{2}a]-2[\frac{a-b}{4}]-2[\frac{-a-b-2}{4}]$	$D+\frac{b-a-1}{2}$
$a-2+bi$	$D+\frac{a-b+3}{2}+2[-\frac{1}{2}a]-2[\frac{b-a}{4}]-2[\frac{a+b-2}{4}]$	D
$a+(b+2)i$	$D-\frac{a+b-3}{2}+2[\frac{1}{2}b]-2[\frac{a+b}{4}]-2[\frac{a-b-2}{4}]$	$D+\frac{a+b-3}{2}$
$a+(b-2)i$	$D+\frac{a+b+3}{2}+2[-\frac{1}{2}b]-2[\frac{-a-b}{4}]-2[\frac{b-a-2}{4}]$	

$a+2+(b+2)i$	$2a-b+1+D$	or $D+b-1$
$a+2+(b-2)i$	$-a-2b+1+D$	$D+a-1$
$a-2+(b+2)i$	$a+2b+1+D$	$D-a-1$
$a-2+(b-2)i$	$-2a+b+1+D$	$D-b-1$

$a+4+bi$	$D+a+b$	$a+8+bi$	$D+2$
$a+(b+4)i$	$D-a+b$		
$a-4+bi$	$D-a-b$		
$a+(b-4)i$	$D+a-b$		

$a+4+(b+4)i$	$D+2b$
$a+4+(b-4)i$	$D+2a$
$a-4+(b+4)i$	$D+2a$
$a-4+(b-4)i$	$D+2b$

The result of the preceding investigations is therefore as follows: For the modulus $m=a+bi$, where a is odd and b even, we have

$$D\frac{1+i}{m}=\tfrac{1}{8}(-aa+2ab+bb-8b+1)$$
(and if $a+bi=1+(2+2i)(\alpha+\beta i)$)
$$\text{or } \tfrac{1}{8}(-aa+2ab-3bb+1)\equiv-(\alpha-\beta)^2-\beta$$

$$D\frac{1-i}{m}=\tfrac{1}{8}(+aa+2ab-bb-8b-1)$$
$$\text{or } \tfrac{1}{8}(+aa+2ab+3bb-1)$$

$$D\frac{-1-i}{m}=\tfrac{1}{8}(-aa+2ab+bb+1)$$
$$=\beta+\alpha\alpha+2\alpha\beta-\beta\beta\equiv-\beta+(\alpha+\beta)^2$$

$$D\frac{-1+i}{m}=\tfrac{1}{8}(+aa+2ab-bb-1)$$
$$=\alpha+\alpha\alpha-2\alpha\beta-\beta\beta\equiv-\alpha-(\alpha+\beta)^2$$

$$D\frac{2}{m} = \tfrac{1}{2}ab$$
$$D\frac{i}{m} = \tfrac{1}{4}(aa + bb - 1)$$
$$D\frac{-1}{m} = \tfrac{1}{2}(aa + bb - 1)$$

General theorem on decidents.

Let A, B, C, etc., be distinct (odd complex) prime numbers, none of which divides the number M; then

$$D\frac{M}{A^\alpha B^\beta C^\gamma D^\delta} = \alpha D\frac{M}{A} + \beta D\frac{M}{B} + \gamma D\frac{M}{C} + \text{etc.}$$

$$M^{\frac{1}{4}(aa+bb-1)} \equiv i^{D\frac{M}{a+bi}} \pmod{(a+bi)} \quad \text{if } a+bi \text{ is a prime number}$$

$$\begin{aligned} D\frac{1+i}{m} &= \tfrac{1}{8}(-aa + 2ab - 3bb + 1) \\ &= -\tfrac{1}{8}(3(a-b) \mp 1)(a - b \mp 1) \quad \text{if } a \equiv \tfrac{1}{3} \\ D\frac{1-i}{m} &= \tfrac{1}{8}(+aa + 2ab + 3bb - 1) \\ D\frac{-1-i}{m} &= \tfrac{1}{8}(-aa + 2ab + bb + 1) \\ &= \tfrac{1}{8}(a - b \mp 1)(a - b \mp 3) \quad \text{if } a \equiv \pm 1 \\ D\frac{-1+i}{m} &= \tfrac{1}{8}(+aa + 2ab - bb - 1) \end{aligned}$$

In general, $m \equiv 1 \bmod.(1+i)$

$$D\frac{1+i}{m} = -\text{Real part } \frac{(1+i)(m^4-1)}{16} = \text{Imag. coeff. } \frac{m^4-1}{8+8i}$$
$$D\frac{1-i}{m} = +\text{Real part } \frac{(1-i)(m^4-1)}{16} = \text{Imag. coeff. } \frac{m^4-1}{8-8i}$$

$1 + i \pmod{16}$

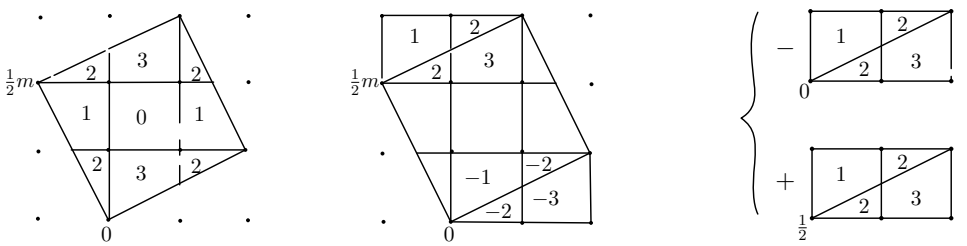
a	b							
	0	2	4	6	8	10	12	14
1	0	3	3	0	2	1	1	2
3	3	3	0	2	1	1	2	0
5	1	2	0	3	3	0	2	1
7	2	0	3	3	0	2	1	1
9	2	1	1	2	0	3	3	0
11	1	1	2	0	3	3	0	2
13	3	0	2	1	1	2	0	3
15	0	2	1	1	2	0	3	3

18.

Theory of the biquadratic residue $-1-2i$.

Let the modulus $= m = a + bi$ be such that a is odd and b even; we also assume that it is a prime number.

The following diagrams represent the decident; their identity is easily seen:



For brevity, we denote $S(x, x+\alpha, x+\alpha+\beta, x+\beta)$ by $[x, \alpha, \beta]$, so that

$$\begin{aligned}[x,\alpha,\beta] &= -[x,\beta,\alpha] = [x+\alpha,\beta,-\alpha] \\ &= -[x+\alpha,-\alpha,\beta] \\ &= [x+\alpha+\beta,-\alpha,-\beta] \\ &= -[x+\alpha+\beta,-\beta,-\alpha]\end{aligned}$$

If we also put

$$\frac{m}{-2-4i} = \frac{-a-2b}{10} + \frac{-b+2a}{10}i = Q$$

then the decident consists of the following eight parts:

$$\begin{aligned}\text{I} &= [0, \tfrac{1}{2}, -iQ] \\ -2\text{II} &= -2[0, \tfrac{1}{2}, Q] \\ \text{III} &= +[Q, \tfrac{1}{2}, -iQ] \\ \text{IV} &= +[-iQ, \tfrac{1}{2}, Q] \\ -3\text{V} &= -3[Q, \tfrac{1}{2}, Q] \\ -3\text{VI} &= -3[2Q, \tfrac{1}{2}, -iQ] \\ +2\text{VII} &= +2[(1-i)Q, \tfrac{1}{2}, Q] \\ +\text{VIII} &= +[0, \tfrac{1}{2}, \tfrac{1}{2}im]\end{aligned}$$

If F denotes an arbitrary elementary residue of the modulus $-1-2i$, then

$$\Sigma[2FQ, \tfrac{1}{2}, iQ] = [0, -\tfrac{1}{2} - i, \tfrac{1}{2}im]$$

Thus, for F substitute $0, 1, i, -1, -i$; we have

$$\begin{aligned} 0 = \quad & [0, \tfrac{1}{2}, iQ] && = \text{IX} \\ & +[2Q, \tfrac{1}{2}, iQ] && = \text{X}. \\ & +[2iQ, \tfrac{1}{2}, iQ] && = \text{XI} \\ & +[-2Q, \tfrac{1}{2}, iQ] && = \text{XII} \\ & +[-2iQ, \tfrac{1}{2}, iQ] && = \text{XIII} \\ & -[0, -\tfrac{1}{2} - i, \tfrac{1}{2}im] && = -\text{XIV} \end{aligned}$$

Add this to the preceding value of the decident. Combining them gives the following results:

(1) Since $(1 + 2i)Q + \frac{1}{2}$ is an integer, we obtain

$$\begin{aligned} \text{XI} &= [-Q - \tfrac{1}{2}, \tfrac{1}{2}, iQ] = -[-Q, -\tfrac{1}{2}, iQ] \\ &= -[Q, \tfrac{1}{2}, -iQ] \end{aligned}$$

and hence

$$\text{III} + \text{XI} = 0$$

(2) We combine $\text{IV}, -3\text{V}, \text{X}, \text{XIII}$ as follows:

$$\begin{aligned} \text{IV} &= +[-2Q + \tfrac{1}{2}i, \tfrac{1}{2}, Q] = [-2iQ - \tfrac{1}{2}, \tfrac{1}{2}i, iQ] \\ \text{V}' &= -[2Q, +\tfrac{1}{2}, -Q] = -[-2iQ, -\tfrac{1}{2}i, iQ] \\ \text{X} &= [+iQ - \tfrac{1}{2}i, \tfrac{1}{2}, iQ] \\ &= [-iQ + \tfrac{1}{2}i, -\tfrac{1}{2}, -iQ] = [-2iQ - \tfrac{1}{2} + \tfrac{1}{2}i, \tfrac{1}{2}, iQ] \\ \text{XIII} &= [-2iQ, \tfrac{1}{2}, iQ] \end{aligned}$$

Thus the entire result from these parts is

$$\begin{aligned} & -4\text{V} \\ & + R(-2iQ) - R(-iQ) - I(-2iQ) + I(-iQ) \\ & - \text{Sq. } [-2iQ - \tfrac{1}{4} + \tfrac{1}{4}i] \\ & + \text{Sq. } [-2iQ + \tfrac{1}{4} - \tfrac{1}{4}i] \end{aligned}$$

(3) Combining $\text{I}, -2\text{II}, -3\text{VI}, +2\text{VII}, +\text{IX}, +\text{XII}$ gives

$$\begin{aligned} \text{I} &= [0, \tfrac{1}{2}, -iQ] \\ \text{II} &= [0, -\tfrac{1}{2}i, -iQ] \\ \text{VI} &= [iQ - \tfrac{1}{2}i, \tfrac{1}{2}, -iQ] = [\tfrac{1}{2} - \tfrac{1}{2}i, -\tfrac{1}{2}, iQ] \\ &= [-\tfrac{1}{2} + \tfrac{1}{2}i, \tfrac{1}{2}, -iQ] \\ \text{VII} &= [-Q - \tfrac{1}{2}i, \tfrac{1}{2}, Q] = [-\tfrac{1}{2} + \tfrac{1}{2}i, -\tfrac{1}{2}, -Q] \\ &= [+\tfrac{1}{2} + \tfrac{1}{2}i, -\tfrac{1}{2}i, -iQ] \\ \text{IX} &= [0, -\tfrac{1}{2}, -iQ] \\ \text{XII} &= [-iQ + \tfrac{1}{2}i, \tfrac{1}{2}, iQ] = [\tfrac{1}{2} + \tfrac{1}{2}i, -\tfrac{1}{2}, -iQ] \end{aligned}$$

$$
\begin{aligned}
&= +4\mathrm{I} - 4\mathrm{II} - 4\mathrm{VI} + 4\mathrm{XII} \\
&\quad - I(\tfrac{1}{2}i) + I(-iQ + \tfrac{1}{2}i) + I0 - I(-iQ) - 2R0 + 2R(-iQ) \\
&\quad + 2\mathrm{Sq.}\ (-iQ + \tfrac{1}{4} + \tfrac{1}{4}i) \\
&= 4\mathrm{I} - 4\mathrm{II} - 4\mathrm{VI} + 4\mathrm{XII} \\
&\quad + R(-1-2i)Q - R(-2iQ) - I(-iQ) + 2R(-iQ) \\
&\quad + 2\mathrm{Sq.}\ (-2iQ + \tfrac{1}{4} + \tfrac{1}{4}i)
\end{aligned}
$$

All this together therefore gives

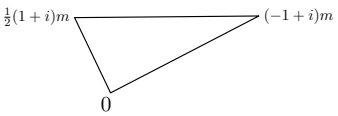
$$
\begin{aligned}
&+ 4\mathrm{I} - 4\mathrm{II} - 4\mathrm{V} - 4\mathrm{VI} + 4\mathrm{XII} + \tfrac{1}{2}(a-1) - \tfrac{1}{2}b \\
&+ \mathrm{Sq.}\ (-2iQ + \tfrac{1}{4} - \tfrac{1}{4}i) \\
&+ 2\mathrm{Sq.}\ (-2iQ + \tfrac{1}{4} + \tfrac{1}{4}i) \\
&- \mathrm{Sq.}\ (-2iQ - \tfrac{1}{4} + \tfrac{1}{4}i)
\end{aligned}
$$

Finally, $\mathrm{VIII} - \mathrm{XIV} = \frac{1}{2}(a-1) + \frac{1}{2}b$. Thus, since the three square parts equal the decident of $\frac{m}{-1-2i}$, we obtain

$$\mathrm{Dec.}\ \frac{-1-2i}{m} \equiv a - 1 + \mathrm{Dec.}\ \frac{m}{-1-2i} \quad \text{Q. E. D.}$$

The proof can probably be simplified considerably further by the fact that

$$\mathrm{Dec.}\ \frac{1+2i}{m} =$$



19.

The following has been found by induction:

$$
\begin{aligned}
\mathrm{Dec.}\ \frac{a-bi}{a+bi} &\equiv \frac{aa+2ab-1}{4}, && a \equiv 1\ (\mathrm{mod.}\ 4) \\
&\equiv \frac{aa+2ab+2bb-1}{4}, && a+bi \equiv 1\ (\mathrm{mod.}\ 2+2i)
\end{aligned}
$$

The following is connected with this: Let $aa + bb = p$ (a prime number), $a \equiv 1$ (mod. 4)

$$
\begin{aligned}
1 \,.\, 2 \,.\, 3 \ldots\ldots\ldots\ldots \tfrac{1}{4}(p-1) &\equiv \alpha \bmod.p \\
\tfrac{1}{4}(p+3) \,.\, \tfrac{1}{4}(p+7) \ldots \tfrac{1}{2}(p-1) &\equiv \beta \\
\tfrac{1}{2}(p+1) \,.\, \tfrac{1}{2}(p+3) \ldots \tfrac{3}{4}(p-1) &\equiv \gamma \\
\tfrac{1}{4}(3p+1) \ldots\ldots\ldots\ldots\ p-1 &\equiv \delta
\end{aligned}
$$

then

$$
\begin{aligned}
&\alpha \equiv \delta, \quad \beta \equiv \gamma \quad \text{if } \tfrac{1}{2}b \text{ is even} \\
&\alpha \equiv -\delta, \quad \beta \equiv -\gamma \quad \text{if } \tfrac{1}{2}b \text{ is odd}
\end{aligned}
$$

$$\pm\alpha\beta \equiv i, \quad \pm\beta\beta \equiv 2b, \quad \frac{\beta}{\alpha} \equiv 2a,$$
$$\frac{\beta}{1+\alpha\beta} \equiv \sqrt{a}, \quad \tfrac{1}{2}\beta(1-\alpha\beta) \equiv \sqrt{a}$$

It therefore remains only to determine the decidents for real residues.

$$a^{\frac{1}{4}bb} \,.\, b^{\frac{1}{4}(aa-1)} \equiv 1 \text{ (mod. } (aa+bb))$$
$$\text{if } a \equiv 1)(\text{mod. } 4) \quad b \text{ even} \quad aa+bb \text{ prime}$$

If only real numbers are to be used, the matter comes down to the following main theorem. Let $a-1$ be divisible by 4, and b by 2; let a and b have no common divisor, and let k denote the numbers $1, 2, 3 \ldots aa+bb-1$. Let

α the number of all values of k for which the least residues of $ak, bk, \quad aak, \quad abk$ all lie between 0 and $\frac{1}{2}(aa+bb)$

β $ak, bk, \quad aak, -abk$

γ $ak, bk, -aak, -abk$

δ $ak, bk, -aak, \quad abk$

Then $\beta + 2\gamma + 3\delta - \frac{1}{4}(aa-1)$ is divisible by 4.

[II.]

PREPARATIONS FOR THE GENERAL THEORY OF BIQUADRATIC RESIDUES.

(1.)

Let $P = x + iy$, where neither x nor y is an integer. We denote the number $+1$ by $LP, L'P, L''P, L'''P$, according as P lies in the first, second, third or fourth quadrant (in the first and second quadrants $[y]$ is even, in the third and fourth odd; in the first and fourth $[x]$ is even, in the second and third odd). In all cases where these symbols are not $= 1$, they are assumed to be $= 0$. We then have the following 24 relations:

$$\begin{array}{lll} L(P \pm 1) = L'P & L(P \pm i) = L'''P & L(P \pm 1 \pm i) = L''P \\ L'(P \pm 1) = LP & L'(P \pm i) = L''P & L'(P \pm 1 \pm i) = L'''P \\ L''(P \pm 1) = L'''P & L''(P \pm i) = L'P & L''(P \pm 1 \pm i) = LP \\ L'''(P \pm 1) = L''P & L'''(P \pm i) = LP & L'''(P \pm 1 \pm i) = L'P \end{array}$$

$$\begin{array}{lll} LiP = L'''P & L(-P) = L''P & L(-iP) = L'P \\ L'iP = LP & L'(-P) = L'''P & L'(-iP) = L''P \\ L''iP = L'P & L''(-P) = LP & L''(-iP) = L'''P \\ L'''iP = L''P & L'''(-P) = L'P & L'''(-iP) = LP \end{array}$$

(2.)

By PP' or z we denote a line beginning at P and ending at P'. It need not be straight. We assign a positive and a negative side to every straight line drawn from $2x + 2iy$ to $2x + (2y+1)i$ (where x, y range over all integers); we choose the right side as positive and the left as negative. By Tz we denote the number of all intersections

of the line z with the lines just described, counting positively those where z passes from the negative side to the positive, and negatively the others. We also put

$$Tz - T(z-1) = Sz$$

($z-1$ is a line parallel to z, going from the point $P-1$ to $P'-1$). Evidently we need only add to the above system the lines drawn from $2x+1+2yi$ to $2x+1+(2y+1)i$, regarding their left sides as positive and their right sides as negative, to recognize in Sz the number of all intersections of z with this double system of straight lines. We further have

$$\begin{aligned}
T(-z) &= -T(z+i) \\
T(z)+T(z+i) &= [\tfrac{1}{2}x]-[\tfrac{1}{2}x'] \\
S(z+1) &= -Sz \\
S(z+i) &= -Sz+LP+L'''P-LP'-L'''P' \\
S(z+1+i) &= Sz-LP+L'''P+LP'+L'''P' \\
Siz &= Sz-LP+LP' \\
S(-z) &= Sz-LP-L'''P+LP'+L'''P' \\
S(-iz) &= Sz+L'P-L'P'
\end{aligned}$$

1.

We consider two kinds of points in the plane: first, those corresponding to integers; second, those determined by multiplying integers by the quantity $Q=\frac{m}{2M}$. We can distinguish them by calling them points of the first order and points of the second order.

2.

Joining each point of the second order to its four neighbours by straight lines, which we shall call *ligatures*, divides the whole plane into infinitely many squares. The points of the first order lie partly inside these squares, partly on the ligatures between their

endpoints, and partly at the endpoints of the ligatures, the last case occurring when they are also points of the second order. If kQ is such a point, then, provided m, M have no common divisor and are both odd, k must be divisible by M.

3.

For ligatures we can also distinguish the starting point from the endpoint, and thus PQ from QP, or in some cases set this distinction aside. We call two such ligatures opposite. In general, the most convenient way to denote ligatures is by their starting points and endpoints, which may if desired be enclosed in brackets. The ligature opposite to a given one shall be indicated by a double overline: $QP=\overline{\overline{PQ}}$.

4.

Each of the squares in question is enclosed by four such ligatures

$$\{kQ, (k+1)Q\},\ \{(k+1)Q, (k+1+i)Q\},$$
$$\{(k+1+i)Q, (k+i)Q\},\ \{(k+i)Q, kQ\} \ldots . \Omega$$

to whose right it lies. Here it is important to consider the form of the number k. We distinguish four kinds of squares according as $k \equiv 0, 1, 1+i, i \pmod 2$, and use the numbers $0, 1, 2, 3$, which we call the respective intensors of the squares.

5.

We assign to the ligatures the same intensors as those of the squares lying to their right.

6.

We must now consider another, larger square Ω', namely the one obtained when the square indicated in 4 for $k = 0$ is multiplied by M: it is therefore bounded by the straight lines μ, μ', μ'', μ'''

$$\{0, \tfrac{1}{2}m\},\ \{\tfrac{1}{2}m, \tfrac{1}{2}(1+i)m\},\ \{\tfrac{1}{2}(1+i)m, \tfrac{1}{2}im\},\ \{\tfrac{1}{2}im, 0\}$$

It consists of complete squares Ω and pieces of such squares. Add up

all points of the first order inside it, taking for each point the intensor of the square Ω in which it lies. This sum, or its least residue modulo 4, is called the decident of M for the modulus m, and determines the biquadratic modality of M with respect to this modulus.

7.

We divide the square Ω' into 5 pieces as follows. Join the point 0 to $\frac{1}{4}(1+i)(m-1)$ by the line λ, which is to run entirely along ligatures inside Ω'. Let

$$\tfrac{1}{2}m + i\lambda = \lambda', \quad \tfrac{1}{2}(1+i)m - \lambda = \lambda'', \quad \tfrac{1}{2}im - i\lambda = \lambda'''$$

These 4 lines therefore run from the corners of the square Ω' into its interior and end at the four corners of the innermost square. Its intensor will be 0 if $m \equiv 1 \pmod{2+2i}$; let the ligatures of this square be ν, ν', ν'', ν'''.

The 5 pieces will therefore be bounded by

I. $\ldots$ $\mu,\ \lambda',\ \overline{\overline{\nu}},\ \overline{\overline{\lambda}}$

II. $\ldots$ $\mu',\ \lambda'',\ \overline{\overline{\nu'}},\ \overline{\overline{\lambda'}}$

III. $\ldots$ $\mu'',\ \lambda''',\ \overline{\overline{\nu''}},\ \overline{\overline{\lambda''}}$

IV. $\ldots$ $\mu''',\ \lambda,\ \overline{\overline{\nu'''}},\ \overline{\overline{\lambda'''}}$

V. the inner square $\nu,\ \nu',\ \nu'',\ \nu'''$

The decident is therefore the enumeration of all points of the first order in I. II. III. IV.

8.

For brevity, the intensor of any point shall mean the intensor of the square in which it lies, and shall be expressed by a prefixed Υ.

9.

The decident is therefore

$$\Sigma\Upsilon P + \Sigma\Upsilon P' + \Sigma\Upsilon P'' + \Sigma\Upsilon P'''$$

where P denotes all points in I., and so on.

10.

We now also consider the region VI $= -i$IV, which lies outside Ω', but adjoins I along μ and together with it forms the region ω, consisting of $AA + BB$ complete squares. If Π denotes all integer points, and Π' all integer points increased by $\frac{1}{2}i$, in this region, it is easy to prove that the decident

$$\begin{aligned} &= \Sigma\Upsilon\Pi - \Sigma\Upsilon\Pi' + \text{number of all integer points inside VI} \\ &\quad - \text{number of all half-points inside VI.} \end{aligned}$$

11.

Imagine straight lines drawn from each integer point k to $k + \frac{1}{2}i$, their right sides regarded as positive and their left sides as negative. Let l be a line, and let Sl denote the sum of all intersections of l with this system of lines, counting positively those where l passes from the negative side to the positive, and negatively the opposite intersections. The decident then has the following expression:

$$\Sigma(\Upsilon l \,.\, Sl) + \Sigma Sl' - S\mu$$

Here l denotes all ligatures of the squares in ω (always taken so that the squares lie to their right), and l' denotes the ligatures on the boundary of the figure ω between 0 and $\frac{1}{2}m$, hence outside Ω'.

All ligatures l consist of

1) l';

2) l'', the boundary ligatures inside Ω', hence $\lambda', \overline{\overline{\nu}}, \overline{\overline{\lambda}}$;

3) l''', which lie in the interior of ω.

If l were allowed to range over all ligatures inside ω or on the boundary of this figure, insofar as they start at points $\frac{km}{2M}$ such that k is divisible by $1+i$, the decident would be

$$= \Sigma\alpha \,.\, Sl - S\mu$$

where $\alpha = 1$ for all ligatures in the interior of ω;

$\alpha = \Upsilon l + 1$ for all boundary ligatures outside Ω' whose direction follows the boundary running from 0 to $\frac{1}{2}m$;

$\alpha = -(\Upsilon\overline{\overline{\lambda}} + 1) = -\Upsilon l$ for all those on this boundary running in the opposite direction;

$\alpha = \Upsilon l$ for all boundary ligatures inside Ω' directed towards 0;

$\alpha = -\Upsilon l + 1$ for all boundary ligatures inside Ω' directed away from 0.

12.

We can now combine all the l that occur (in the last manner) in pairs, namely l with $\overline{\overline{\frac{1}{2}m - l}}$, which we shall call associated ligatures. A single one is excepted, standing isolated or identical with its associated ligature, namely the one running from

$$\tfrac{1}{2}(M-1) \,.\, \frac{m}{2M} \quad \text{to} \quad \tfrac{1}{2}(M+1)\frac{m}{2M}$$

For associated ligatures, α is always the same.

[III.]

Theory of Biquadratic Residues.

1.

The least residues for the modulus $m = a + bi$ are the complex integers $\mu = \alpha + \beta i$ for which $\frac{\mu}{m} = x + yi$ has x and y positive and less than 1. The residue 0 is included as well*). Their number is $= aa + bb$.

2.

If $aa + bb$ is odd, $aa + bb$ is of the form $4n + 1$. On excluding the least residue 0, the others fall into four classes. In the first class f we place those for which x and y are less than $\frac{1}{2}$,

the second	f'	where $x > \frac{1}{2}$,	$y < \frac{1}{2}$
third	f''	$x > \frac{1}{2}$,	$y > \frac{1}{2}$
fourth	f'''	$x < \frac{1}{2}$,	$y > \frac{1}{2}$

All the residues are obtained

f'	from	$if + m$
f''	from	$-f + (1 + i)m$
f'''	from	$-if + im$

3.

Let M be another number with no factor in common with m. Then

$$M^{aa+bb-1} \equiv 1 \text{ (mod. } m)$$

holds; consequently $M^{\frac{1}{4}(aa+bb-1)}$ is either $\equiv 1$, or $\equiv i$, or $\equiv -1$, or $\equiv -i$, that is, $\equiv i^{\varepsilon}$, where ε represents one of the four numbers $0, 1, 2, 3$. In the first case M is a biquadratic residue of m, and hence also a quadratic residue. In the third case M is a quadratic residue but not a biquadratic residue; in the second and fourth cases it is both a quadratic and a biquadratic nonresidue. We call this ε, on which the biquadratic character of the number M with respect to the modulus m depends, the decident of M for the modulus m. Induction gives the following beautiful theorem. "If M and m are odd primes of the form $1 + (2 + 2i)\mu$, where μ is an integer, the difference between the two decidents, that of M for the modulus m and that of m for the modulus M, is either $= 0$ or $= 2$; the former when at least one of the numbers m, M is of the form $1 + 4N$, the latter when both are of the form $1 + 2i + 4N$." This reciprocity theorem is analogous to the one for quadratic residues among real numbers alone.

*) and, if a and b happen to have a common divisor e, the numbers $\frac{m}{e}, \frac{2m}{e}, \frac{3m}{e} \ldots \frac{(e-1)m}{e}$. For now, however, we shall leave this case out of the investigation.

4.

Multiply all the numbers f by M and find their least residues for the modulus m. If among them there are

$$\begin{array}{ll} \alpha & \text{belonging to } f \\ \beta & f' \\ \gamma & f'' \\ \delta & f''' \end{array}$$

then $\varepsilon \equiv \beta + 2\gamma + 3\delta \pmod 4$.

Proof. Let the collection of those numbers in f whose products with M give residues belonging to f be g; let the collection of those whose products give residues from f' be g', and similarly g'' . g'''. Then the least residues of

$$-ig'M, \quad -g''M, \quad ig'''M$$

are all contained in f and are distinct both from one another and from the least residues of the products gM. Consequently the product of all

$$gM, \quad -ig'M, \quad -g''M, \quad +ig'''M$$

is congruent to the product of all f, and hence also to the product of all g, g', g'', g'''. But that product equals the product of all g, g', g'', g''' multiplied by

$$M^\alpha \,.\, (-iM)^\beta \,.\, (-M)^\gamma \,.\, (iM)^\delta$$

so this last product is $\equiv 1$

$$\begin{array}{rl} \text{therefore} & M^{\alpha+\beta+\gamma+\delta}(-i)^\beta(-1)^\gamma i^\delta \equiv 1 \\ \text{or} & M^{\alpha+\beta+\gamma+\delta} \equiv i^\beta(-1)^\gamma(-i)^\delta \equiv i^{\beta+2\gamma+3\delta} \end{array}$$

from which the theorem follows directly.

5.

It is easy to decide whether the least residue of a number N for the modulus m belongs to the class f, f', f'' or f'''. If ω is the integer contained in $\frac{N}{m}$, that residue is $= N - \omega m$ and therefore belongs to f, f', f'', according as, on putting

$$\frac{N}{m} - \omega = x + iy$$

we have

$$\begin{array}{ll} x < \frac{1}{2}, & y < \frac{1}{2} \\ x > \frac{1}{2}, & y < \frac{1}{2} \\ x > \frac{1}{2}, & y > \frac{1}{2} \\ x < \frac{1}{2}, & y > \frac{1}{2} \end{array}$$

In these 4 cases the integer contained in $\frac{2N}{m}$ is, in the same order, as follows:

$$\begin{array}{l} 2\omega \\ 2\omega+1 \\ 2\omega+1+i \\ 2\omega+i \end{array}$$

It follows that the least residue of N for the modulus m belongs to f, f', f'', f''' according as, on writing the integer contained in $\frac{2N}{m}$ as $= \xi + \eta i$, we have

$$\begin{array}{ll} \xi \text{ even} & \eta \text{ even} \\ \xi \text{ odd} & \eta \text{ even} \\ \xi \text{ odd} & \eta \text{ odd} \\ \xi \text{ even} & \eta \text{ odd} \end{array}$$

6.

The decident of M for the modulus m is therefore found as follows. Find the integers contained in each of the individual $\frac{2fM}{m}$. Writing these generally as $x + yi$, disregard entirely those for which x and y are both even; count one for each for which x is odd and y even, take two for each for which x and y are both odd, and three for each for which x is even and y odd. Take the least residue modulo 4 of the sum of all these numbers; it is the required decident. We express this as

$$\text{Dec.}\frac{M}{m} = \Sigma n$$

where $[\frac{2fM}{m}] = x + yi$, and we put $n = 0$ when x is even and y even

$$\begin{array}{lll} 1 & x \text{ odd} & y \text{ even} \\ 2 & x \text{ odd} & y \text{ odd} \\ 3 & x \text{ even} & y \text{ odd} \end{array}$$

For brevity we shall denote n by the characteristic Θ, $n = \Theta\frac{2fM}{m}$ *).

*) To decide which class M belongs to with respect to m, choose those values of k (among the numbers $1, 2, 3 \ldots p-1$) for which $[\frac{2km'M}{p}]$ is even, and add $-\Sigma[\frac{2km'}{p}]^2$. If k is taken only up to $\frac{1}{2}p$, the sum to be taken is

$$-\Sigma\{[\frac{2km'M}{p}]^2 + [\frac{2km'}{p}]^2\}$$

for those values of $[\frac{2km'M}{p}]$ that are divisible by $1+i$.

7. 8.

This rule is general, whatever number M denotes. For the case that will be the immediate subject of our investigation, where M is assumed to be odd and of the form $1 + (2 + 2i)N$, a slightly modified rule is more convenient.

Suppose the numbers f are again divided into 4 classes. In the first we place the (h), whose doubles are also found in f; in the second, h', we count those whose doubles $2h'$ belong to f'; similarly, h'' and h''' denote those whose doubles belong to f'' and f'''. Thus the decident ε is

$$\varepsilon = \Sigma\Theta\frac{2hM}{m} + \Sigma\Theta\frac{2h'M}{m} + \Sigma\Theta\frac{2h''M}{m} + \Sigma\Theta\frac{2h'''M}{m}$$

We call the collection of all $2h$ and $-2h'' + (1 + i)m$ H

and the collection of all $-i(2h' - m)$ and $i(2h''' - im)$ H'

Thus H and H' comprise all f; the former are the even ones, the latter the odd ones.

The following relations must also be applied

$$\begin{aligned}
\Theta iN &= 1 + \Theta N \\
\Theta(-N) &= 2 + \Theta N \\
\Theta(-iN) &= 3 + \Theta N \\
\Theta(N + 1) &= 1 - \Theta N \\
\Theta(N + 1 + i) &= 2 + \Theta N \\
\Theta(N + i) &= 3 - \Theta N
\end{aligned}$$

consequently

$$\begin{aligned}
\Theta\frac{(-2h'i + mi)M}{m} &= 3 - \Theta\frac{-2h'iM}{m} = -\Theta\frac{2h'M}{m} \\
\Theta\frac{(-2h'' + m(1 + i))M}{m} &= 2 + \Theta\frac{-2h''M}{m} = \Theta\frac{2h''M}{m} \\
\Theta\frac{(2h'''i + m)M}{m} &= 1 - \Theta\frac{2h'''iM}{m} = -\Theta\frac{2h'''M}{m}
\end{aligned}$$

and

$$\begin{aligned}
\varepsilon &= \Sigma\Theta\frac{2hM}{m} - \Theta\frac{(-2h'i + mi)M}{m} \\
&\quad + \Theta\frac{(-2h'' + m(1 + i))M}{m} - \Theta\frac{(2h'''i + m)M}{m} \\
&= \Sigma\Theta\frac{HM}{m} - \Sigma\Theta\frac{H'M}{m}
\end{aligned}$$

or

$$\varepsilon = \Sigma \pm \Theta\frac{fM}{m}$$

where the upper sign is to be taken for even f, the lower for odd.

9.

Let, in general, $f = \xi + \eta i$. The numbers ξ, η are restricted within certain bounds by the condition that f be a least residue of m, or that, on putting $\frac{f}{m} = x + yi$, x and y must lie between the bounds 0 and $\frac{1}{2}$. Definite rules for these bounds could easily be given by distinguishing the different cases. If we give η a particular value, ξ will in turn have its particular bounds. For example, if we assume that a is negative and b positive, then, since

$$x = \frac{a\xi + b\eta}{aa + bb}$$
$$y = \frac{a\eta - b\xi}{aa + bb}$$

the following conditions must hold:

I.	for x to be positive	$\xi < -\frac{b}{a}\eta$
II.	for y to be positive	$\xi < \frac{a}{b}\eta$
III.	for $x < \frac{1}{2}$ to hold	$\xi > \frac{aa+bb-2b\eta}{2a}$
IV.	for $y < \frac{1}{2}$ to hold	$\xi > \frac{2a\eta-aa-bb}{2b}$

For positive η, the second condition already includes the first; for negative η, the reverse holds. Likewise, the third condition is already contained in the fourth,

if	$\eta < \frac{1}{2}(a+b)$
and conversely if	$\eta > \frac{1}{2}(a+b)$

We do not, however, need to consider separately all eight cases that can occur here. For a particular value of η, we merely denote the smaller bound of ξ by ξ^0, the larger by ξ^{00}, and remark only that at these boundary values one always has either $x = 0, y = 0, x = \frac{1}{2}, y = \frac{1}{2}$, and specifically that the following must hold:

if	at the *upper* bound	at the *lower* bound
a pos. b positive	$x = \frac{1}{2}$ or $y = 0$	$x = 0$ or $y = \frac{1}{2}$
a neg. b positive	$x = 0$ or $y = 0$	$x = \frac{1}{2}$ or $y = \frac{1}{2}$
a neg. b negative	$x = 0$ or $y = \frac{1}{2}$	$x = \frac{1}{2}$ or $y = 0$
a pos. b negative	$x = \frac{1}{2}$ or $y = \frac{1}{2}$	$x = 0$ or $y = 0$

For brevity we shall distinguish these four cases by saying that, in the first, m belongs to the first quadrant, in the second to the second, and so on.

10.

We now wish to examine more closely the sum of all $\pm\Theta\frac{fM}{m}$ for which η has a particular value. As ξ gradually increases continuously from its smallest value ξ^0 to its largest ξ^{00},

$$\frac{(\xi+\eta i)M}{m} = X + Yi$$

will also change according to the law of continuity. If $\frac{M}{m}$ lies in the first quadrant, both X and Y will keep increasing; if $\frac{M}{m}$ lies in the second quadrant, X will keep decreasing and Y increasing. In the third quadrant the reverse of the first case occurs, and in the fourth the reverse of the second. But the integer contained in $X+iY$ will change in jumps, as either $[X]$ or $[Y]$ changes by one unit. Let the values of ξ at which such a transition occurs, that is, at which either X or Y becomes an integer, be, in order,

$$\xi',\ \xi'',\ \xi'''\ldots.\xi^n$$

Here it must be remarked that neither these values nor ξ^0 and ξ^{00} can be integers, except for $\eta = 0$, when either ξ^0 or $\xi^{00} = 0$. Now let

$$\Theta\frac{(\xi'+\eta i)M}{m} - \Theta\frac{(\xi^0+\eta i)M}{m} = \delta' \quad \text{(to be expressed differently)}$$
$$\Theta\frac{(\xi''+\eta i)M}{m} - \Theta\frac{(\xi'+\eta i)M}{m} = \delta''$$
$$\text{etc.}$$
$$\Theta\frac{(\xi^{00}+\eta i)M}{m} - \Theta\frac{(\xi^{n-1}+\eta i)M}{m} = \delta^n$$

Then it is easy to see, since between ξ^0 and ξ' there lie $[\frac{1}{2}\xi'] - [\frac{1}{2}\xi^0]$ even integers and $[\frac{1}{2}\xi' + \frac{1}{2}] - [\frac{1}{2}\xi^0 + \frac{1}{2}]$ odd integers, and so on, that, considering only the particular value of η,

$$\begin{aligned}(\pm 1)\Sigma\Theta\frac{fM}{m} = {} & \{[\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi^0] - [\tfrac{1}{2}\xi' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi^0 + \tfrac{1}{2}]\} \\ & \quad . \Theta\frac{(\xi^0 + \eta i)M}{m} \\ & + \{[\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi'' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi' + \tfrac{1}{2}]\} \\ & \quad . \{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta'\} \\ & + \{[\tfrac{1}{2}\xi'''] - [\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi''' + \tfrac{1}{2}] + [\tfrac{1}{2}\xi'' + \tfrac{1}{2}]\} \\ & \quad . \{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta' + \delta''\} \\ & + \text{etc.} \\ & + \{[\tfrac{1}{2}\xi^{00}] - [\tfrac{1}{2}\xi^n] - [\tfrac{1}{2}\xi^{00} + \tfrac{1}{2}] + [\tfrac{1}{2}\xi^n + \tfrac{1}{2}]\} \\ & \quad . \{\Theta\frac{(\xi^0 + \eta i)M}{m} + \delta' + \delta'' + \ldots + \delta^n\}\end{aligned}$$

$$\begin{aligned}= {} & -([\tfrac{1}{2}\xi^0] - [\tfrac{1}{2}\xi^0 + \tfrac{1}{2}]) \,.\, \Theta\frac{(\xi^0 + \eta i)M}{m} \\ & -([\tfrac{1}{2}\xi'] - [\tfrac{1}{2}\xi' + \tfrac{1}{2}]) \,.\, \delta' \\ & -([\tfrac{1}{2}\xi''] - [\tfrac{1}{2}\xi'' + \tfrac{1}{2}]) \,.\, \delta'' \\ & - \text{etc.} \\ & -([\tfrac{1}{2}\xi^n] - [\tfrac{1}{2}\xi^n + \tfrac{1}{2}]) \,.\, \delta^n \\ & +([\tfrac{1}{2}\xi^{00}] - [\tfrac{1}{2}\xi^{00} + \tfrac{1}{2}]) \,.\, \Theta\frac{(\xi^{00} + \eta i)M}{m}\end{aligned}$$

(where the upper sign applies for even η, the lower for odd.)

The numbers $\delta', \delta'', \delta'''$, and so on, can have no values other than $+1$ and -1. The value $+1$ is obtained by δ' when, denoting the values of X, Y belonging to ξ' by X', Y',

$\frac{M}{m}$ in quadrant 1.	$\frac{M}{m}$ in quadrant 2.
X' even integer and $[Y]$ odd	X' even integer $[Y]$ even
Y' even integer and $[X]$ even	Y' even integer $[X]$ even

$\frac{M}{m}$ in quadrant 3.	$\frac{M}{m}$ in quadrant 4.
X' even integer and $[Y]$ even	X' even integer $[Y]$ odd
Y' even integer and $[X]$ odd	Y' even integer $[X]$ odd

Whenever one of these conditions changes to its opposite, $\delta = -1$; whenever both change, $\delta = +1$ remains.

11.

The following formulas provide a more convenient overview of these calculations:

$$\begin{aligned} \text{here } m &= a + bi, & aa + bb &= d \\ M &= A + Bi, & AA + BB &= D \\ \frac{dM}{m} &= \alpha + \beta i, & \alpha &= aA + bB, \quad \beta = aB - bA \\ \frac{\xi + i\eta}{m} &= x + iy, & M(x + iy) &= X + iY \end{aligned}$$

If η and X are given, then

$$\begin{aligned} &1. \quad \xi = \tfrac{\beta\eta}{\alpha} + \tfrac{dX}{\alpha} \\ &2. \quad Y = \tfrac{D\eta}{\alpha} + \tfrac{\beta X}{\alpha} \end{aligned}$$

If η and Y are given, then

$$\begin{aligned} &3. \quad \xi = -\tfrac{\alpha\eta}{\beta} + \tfrac{dY}{\beta} \\ &4. \quad X = -\tfrac{D\eta}{\beta} + \tfrac{\alpha Y}{\beta} \end{aligned}$$

If η and x are given, then

$$\begin{aligned} &5. \quad \xi = -\tfrac{b\eta}{a} + \tfrac{dx}{a} \\ &6. \quad X = -\tfrac{B\eta}{a} + \tfrac{\alpha x}{a} \\ &7. \quad Y = \tfrac{A\eta}{a} + \tfrac{\beta x}{a} \end{aligned}$$

If η and y are given, then

$$8. \quad \xi = \frac{a\eta}{b} - \frac{dy}{b}$$
$$9. \quad X = \frac{A\eta}{b} - \frac{\alpha y}{b}$$
$$10. \quad Y = \frac{B\eta}{b} - \frac{\beta y}{b}$$

12.

The rule of Article 10 can now be expressed as follows. Giving η a particular value, we have

$$\Sigma \pm \Theta \frac{fM}{m} = k^0 \Theta(X^0 + Y^0 i) - k^{00} \Theta(X^{00} + Y^{00} i) + \Sigma k$$

Here $k^0 = 0$ when $[\xi^0]$ is even; $k^0 = +1$ when $[\xi^0]$ is odd and η even; $k^0 = -1$ when $[\xi^0]$ is odd and η odd. k^{00} is determined in the same way by $[\xi^{00}]$ and η. Finally, Σk is a sum of as many numbers as there are, between $\xi = \xi^0$ and $\xi = \xi^{00}$, integer values of X or Y; in each case $k = 0$ when the corresponding $[\xi]$ is even, and $= \pm 1$ when $[\xi]$ is odd. The sign is determined as follows. If X is an integer, then $k = 1$ when all the following hold:

η	even
X	even
$[Y]$	even
$\frac{M}{m}$	in the second or third quadrant, i.e. α negative

If one or three of these conditions are absent, then $k = -1$; if two or all four are absent, $k = 1$ remains. If, on the other hand, Y is an integer, then $k = 1$ when all, two, or none of the 4 conditions

η	even
Y	even
$[X]$	even
$\frac{M}{m}$	in the first or second quadrant, i.e. β positive

are satisfied.

13.

We must now consider separately the cases in which ξ^0 or ξ^{00} (or X^0, Y^0, X^{00}, Y^{00}) is an integer. There are four cases to distinguish here, taking a and A to be odd.

I. If m lies in the first quadrant, then for $x = \frac{1}{2}, y = 0$, $\eta = \frac{1}{2}b$ is an integer. Then $Y^{00} = \frac{1}{2}B$ is an integer, and $\Theta(X^{00} + Y^{00} i)$ will be $= \Theta(\frac{1}{2}A + \frac{1}{2}Bi)$ only when β is negative. When β is positive, $\Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i)$ is to be taken instead.

II. If m lies in the second quadrant, then for $x = 0, y = 0$ one has $\eta = 0$. For this value of η, $X^{00} = 0, Y^{00} = 0$. This gives

$$\Theta(X^{00} + Y^{00}i) = \begin{array}{ll} 2, & \text{according as } \frac{M}{m} \text{ lies in quadrant 1.} \\ 3, & 2. \\ 0 & 3. \\ 1 & 4., \text{ and } k^{00} = 1 \end{array}$$

III. If m lies in the third quadrant, then for $x = \frac{1}{2}, y = 0$, $\eta = \frac{1}{2}b$ is an integer, for which $X^0 + Y^0 i = \frac{1}{2}A + \frac{1}{2}Bi$. Then put

$$\Theta(X^0 + Y^0 i) = \Theta(\tfrac{1}{2}A + (\tfrac{1}{2}B - 1)i)$$

whenever β is negative.

IV. If m lies in the fourth quadrant, then for $\eta = 0$ put $\Theta(X^0 + Y^0 i = 0, 1, 2, 3$, according as $\frac{M}{m}$ lies in quadrant 1. 2. 3. 4.; $k^0 = 0$.

14.

The preceding investigations now yield the following determination of the decident.

Collect all values of x and y that lie *within* the bounds 0 and $\frac{1}{2}$ and for which either η and X or η and Y are integers. For each $x + iy$, use the rules of Article 12 to determine the value of k.

Further, collect all values on the boundaries, that is, where either $x = 0$ or $\frac{1}{2}$ while y lies *between* 0 and $\frac{1}{2}$, or $y = 0$ or $= \frac{1}{2}$ while x lies *between* 0 and $\frac{1}{2}$, such that η is an integer and $[\xi]$ odd. Determine the corresponding l as follows. Let $\Theta M(x + yi) = \pm\theta$, with the upper sign for even, the lower for odd η

	then for m in			
for	quadrant 1.	quadrant 2.	quadrant 3.	quadrant 4.
$y = 0$	$l = -\theta$	$l = -\theta$	$l = +\theta$	$l = +\theta$
$x = \frac{1}{2}$	$l = -\theta$	$l = +\theta$	$l = +\theta$	$l = -\theta$
$y = \frac{1}{2}$	$l = +\theta$	$l = +\theta$	$l = -\theta$	$l = -\theta$
$x = 0$	$l = +\theta$	$l = -\theta$	$l = -\theta$	$l = +\theta$

More briefly,

$$l = \pm\theta,$$

the sign is the same as that of a	if $x = 0$
the opposite	if $x = \frac{1}{2}$
the same as that of b	if $y = \frac{1}{2}$
the opposite	if $y = 0$

To $\Sigma k + \Sigma l$ one must then add

$$\left.\begin{array}{l}\text{if } m \text{ lies in the second quadrant: } 2, 1, 0, 3 \\ \text{if } m \text{ lies in the fourth quadrant: } 0,\end{array}\right\} \text{ according as } \frac{M}{m} \text{ lies in quadrant } \begin{array}{l}1.\ 2.\ 3.\ 4.\end{array}$$

if m lies in the first quadrant and $\frac{1}{2}(a-1)$ is odd,

$$\begin{array}{ll}\Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i) & \text{if } \beta \text{ positive} \\ \Theta(\frac{1}{2}A + \frac{1}{2}Bi) & \text{if } \beta \text{ negative}\end{array}$$

if m lies in the third quadrant and $\frac{1}{2}(a-1)$ is odd,

$$\begin{array}{ll}-\Theta(\frac{1}{2}A + \frac{1}{2}Bi) & \text{if } \beta \text{ positive} \\ -\Theta(\frac{1}{2}A + (\frac{1}{2}B - 1)i) & \text{if } \beta \text{ negative.}\end{array}$$

[IV.]

1.

Biquadratic residue? $m = a + bi$; $aa + bb = d$

Modulus $M = A + Bi$, $AA + BB = D$

$$\frac{mD}{M} = \mu \qquad \mu = \alpha + \beta i, \quad \alpha = aA + bB, \quad \beta = Ab - Ba$$

$$\xi + \eta i = \pi; \quad \pi m = x + yi = p; \quad \pi M = X + Yi = P$$

Relations

$$\begin{array}{llll} x = a\xi - b\eta & d\xi = ax + by & D\xi = AX + BY \\ y = b\xi + a\eta & d\eta = -bx + ay & D\eta = -BX + AY \\ X = A\xi - B\eta & dX = \alpha x + \beta y & Dx = \alpha X - \beta Y \\ Y = B\xi + A\eta & dY = -\beta x + \alpha y & Dy = \beta X + \alpha Y \end{array}$$

$$\begin{aligned} \beta\xi &= -Bx + bX = Ay - aY \\ \beta\eta &= -Ax + aX = -By + bY \\ \alpha\xi &= Ax + aY = By + aX \\ \alpha\eta &= -Bx + aY = Ay - bX \end{aligned}$$

Those π for which ξ and η lie between 0 and $\frac{1}{2}$ shall be denoted by π^0, and the corresponding p and P by p^0 and P^0; those π for which $\eta = 0$ and ξ lies between 0 and $\frac{1}{2}$, by π'; those for which $\xi = \frac{1}{2}$ and η lies between 0 and $\frac{1}{2}$, by π''; those π for which $\eta = \frac{1}{2}$ and ξ lies between 0 and $\frac{1}{2}$, by π'''; finally, those for which $\xi = 0$ and η lies between 0 and $\frac{1}{2}$, by π''''.

The decident of $\frac{m}{M}$ is found as follows:

Collect all *integer* P^0; the corresponding x^0 and y^0 will therefore be fractional. Let the respective intensors of p^0 be t^0, that is, the numbers $0, 1.\ 2, 3$, according as

$$\begin{array}{llllll} [x^0] & \text{even}, & \text{odd}, & \text{odd}, & \text{even} \\ [y^0] & \text{even}, & \text{even}, & \text{odd}, & \text{odd} \end{array}$$

The required decident is then $= \Sigma \pm t^0$, where the upper sign is to be taken for even P^0, the lower for odd.

This is the *first* method.

2.

We now wish to arrange the individual P^0 according to the values of Y^0. Restricting ourselves to the case in which a, b, A, B are positive, the smallest value is given by $Y^0 \ldots +1$, the largest by $\frac{1}{2}(A+B-1)$. For each particular value of Y^0, the values of X^0 must lie between certain bounds, namely

I. when $A-B$ is positive

if	between	and
$Y < \frac{1}{2}B$	$-\frac{BY^0}{A}$	$\frac{AY^0}{B}$
$Y = \frac{1}{2}B$	$-\frac{BB}{2A}$	$\frac{1}{2}A$
$Y > \frac{1}{2}B$ and $< \frac{1}{2}A$	$-\frac{BY^0}{A}$	$-\frac{BY^0}{A} + \frac{D}{2A}$
$Y > \frac{1}{2}A$	$\frac{AY^0}{B} - \frac{D}{2B^0}$	$-\frac{BY^0}{A} + \frac{D}{2A}$

II. When $A-B$ is negative,

if	between	and
$Y < \frac{1}{2}A$	$-\frac{BY^0}{A}$	$\frac{AY^0}{B}$
$Y > \frac{1}{2}A$ and $< \frac{1}{2}B$	$\frac{AY^0}{B} - \frac{D}{2B}$	$\frac{AY^0}{B}$
$Y = \frac{1}{2}B$	$\frac{AB-D}{2B}$	$\frac{1}{2}A$
$Y > \frac{1}{2}B$	$\frac{AY^0}{B} - \frac{D}{2B}$	$-\frac{BY^0}{A} + \frac{D}{2A}$

At the lower bounds either $\xi = 0$ or $\eta = \frac{1}{2}$; at the upper bounds, on the other hand, either $\eta = 0$ or $\xi = \frac{1}{2}$. It is easy to prove that the bounds of x are never integers.

3.

We now wish to express the partial sums for each particular Y^0 in another way. At the bounds p will have particular values, which may be denoted by p^*, p^{**}, and while X changes continuously from one bound to the other, p will pass continuously from p^* to p^{**}. But the integer contained in $[p]$ changes here in jumps, with either the real or the imaginary part always changing by one unit. The changes occur at the values of X

$$X',\ X'',\ X'''\ldots X^\mu$$

which are already ordered by size and to which the values of p

$$p',\ p''.\ p'''\ldots$$

correspond.

The last X^μ can also be identical with X^{**} when β is positive, or X' identical with X^*, and so on.

The x are increasing here; thus, when x^{**} is an integer, it is counted as x^μ.

The y are increasing for positive β; then y^{**} is fully included in the count;

decreasing for negative β; then y^* is included in the count.

Let the intensors of p^*, p^{**} be λ^* and λ^{**}

$$\begin{array}{rrl} \text{the intensor from } p' & \text{up to } p''\ldots & \lambda^* + \delta' \\ p'' & \text{up to } p'''\ldots & \lambda^* + \delta' + \delta'' \\ p^\mu & \text{up to } p^{**}\ldots & \lambda^* + \delta' + \delta''\ldots + \delta^\mu = \lambda^{**} \end{array}$$

Then the partial sum, insofar as Y^0 is even, becomes

$$\begin{aligned} &= \lambda^*(g-h) + (\lambda^* + \delta')(g'-h') \\ &\quad + (\lambda^* + \delta' + \delta'')(g''-h'') + \text{etc.} + \lambda^{**}(g^\mu - h^\mu) \end{aligned}$$

where g denotes the number of even X^0 from X^* to X', and h that of the odd ones.

4.

This formula can also be expressed as follows:

$$\begin{aligned}
&\lambda^*\{[\tfrac{1}{2}X^* - \tfrac{1}{2}] - [\tfrac{1}{2}X^*]\}\\
&+\delta'\{[\tfrac{1}{2}X' - \tfrac{1}{2}] - [\tfrac{1}{2}X']\}\\
&+\delta''\{[\tfrac{1}{2}X'' - \tfrac{1}{2}] - [\tfrac{1}{2}X'']\}\\
&+\text{etc.}\\
&+\delta^\mu\{[\tfrac{1}{2}X^\mu - \tfrac{1}{2}] - [\tfrac{1}{2}X^\mu]\}\\
&-\lambda^{**}\{[\tfrac{1}{2}X^{**} - \tfrac{1}{2}] - [\tfrac{1}{2}X^{**}]\}
\end{aligned}$$

or by

$$\lambda^*\varepsilon^* + \delta'\varepsilon' + \delta''\varepsilon'' + \text{etc.} + \delta^\mu\varepsilon^\mu - \lambda^{**}\varepsilon^{**}$$

where in general $\varepsilon = 0$ if $[X]$ odd
and $= -1$ if $[X]$ is even and Y even
$+1$ if $[X]$ even and Y odd.

For δ, on the other hand, the values are

		β	
		positive	negative
if x an even integer,	$[y]$ even	-1	-1
	$[y]$ odd	$+1$	$+1$
x an odd integer,	$[y]$ even	$+1$	$+1$
	$[y]$ odd	-1	-1
y an even integer,	$[x]$ even	-3	$+3$
	$[x]$ odd	-1	$+1$
y an odd integer,	$[x]$ even	$+3$	-3
	$[x]$ odd	$+1$	-1

5.

From this we derive the following second method of determining the decident.

I. Collect all combinations of integer values of Y and x having the following properties:

1. that $\xi = \frac{Ax+bY}{\alpha}$ lies between 0 and $\frac{1}{2}$, with the second bound included;
2. that $\eta = \frac{-Bx+aY}{\alpha}$ lies between 0 and $\frac{1}{2}$, with the first bound included.

II. For these calculate

$$X = \frac{Dx + \beta Y}{\alpha}$$
$$y = \frac{\beta x + dY}{\alpha}$$

III. Omit all those for which $[X]$ is odd, and divide the remaining ones, for which $[X]$ is even, into two classes;

in the first class put those for which, simultaneously,

Y even, x even, $[y]$ even
or where one of these conditions holds;

in the second class, those for which two of these conditions, or none at all, hold,

or in I. where $[Y + x + y]$ even
II. where $[Y + x + y]$ odd

and call the excess of the number in the first class over that in the second c.

IV. Collect all combinations of integer values of Y and y having the following properties:

1. that $\xi = \frac{Ay-aY}{\beta}$ lies between 0 and $\frac{1}{2}$, with the first bound included when β is negative, the second included when β is positive;
2. that $\eta = \frac{-By+bY}{\beta}$ lies between 0 and $\frac{1}{2}$, with the first bound included for positive β, the second for negative.

[V.]

[1.]

$$\begin{array}{ll} \text{Modulus} & M = A + Bi \quad AA + BB = D \\ \text{Residue} & m = a + bi, \quad aa + bb = d \end{array}$$

$$\frac{mD}{M} = \mu = \alpha + \beta i = aA + bB + (Ab - Ba)i$$

$$\xi + \eta i = \pi, \quad \pi m = p = x + yi; \quad \pi M = P = X + Yi$$

ω is an undetermined infinitely small real positive quantity.

[2.]

Preparation.

I. Collect all π for which

ξ nonnegative and no greater than $\frac{1}{2}$
η positive and less than $\frac{1}{2}$
Either x or y is an integer
Either X or Y is an integer

and, for each π, determine the quantity ε by the following rule:

$$\begin{array}{ll} \text{Let } p^0 & \text{be the nearest integer divisible by } 1+i \text{ to } p \\ P^0 & \text{be the nearest integer divisible by } 1+i \text{ to } P \end{array}$$

and put $\varepsilon = \pm 1$, where the sign is always the same as the sign of the imaginary part of the quantity

$$\frac{p - p^0}{P - P^0}(\alpha - \beta i)$$

The following are the special rules. First class, x and X integers

$$\beta\xi = -Bx + bX$$
$$\beta\eta = -Ax + aX$$
$$\beta y = -\alpha x + dX$$
$$\beta Y = -Dx + \alpha X$$

$\varepsilon = -1$ when β is positive, x even, $[y]$ even, X even, $[Y]$ even, or when only an odd number of these conditions holds.

$\varepsilon = +1$ when none or an even number of these conditions holds.

Second class, y and Y integers

$$\begin{aligned}\beta\xi &= +Ay - aY\\ \beta\eta &= -By + bY\\ \beta x &= +\alpha y - dY\\ \beta X &= +Dy - \alpha Y\end{aligned}$$

$\varepsilon = -1$ when β is positive, $[x]$ even, y even, $[X]$ even, Y even, or when an odd number of these conditions holds.

$\varepsilon = +1$ when none or an even number holds.

Third class, y and X integers

$$\begin{aligned}\alpha\xi &= +By + aX\\ \alpha\eta &= +Ay - bX\\ \alpha x &= -\beta y + dX\\ \alpha Y &= +Dy - \beta X\end{aligned}$$

$\varepsilon = -1$ when α is positive, $[x], y, X, [Y]$ are all even, or when an odd number of these conditions holds.

$\varepsilon = +1$ when none or an even number holds.

Fourth class, x and Y integers

$$\begin{aligned}\alpha\xi &= +Ax + bY\\ \alpha\eta &= -Bx + aY\\ \alpha y &= +\beta x + dY\\ \alpha X &= +Dx + \beta Y\end{aligned}$$

$\varepsilon = +1$ when α is positive, $x, [y], [X], Y$ are all even, or when an odd number of these conditions holds.

$\varepsilon = -1$ when none or an even number of them holds.

[3.]

II. Collect all π for which

ξ positive and less than $\frac{1}{2}$
$\eta = \omega$
and either X or Y is an integer,

and put $\varepsilon = \pm 1$, taking the sign of the imaginary part of

$$\frac{M}{P - P^0}$$

Special rule: first class, X an integer

$$\begin{aligned} A\xi &= +X + B\omega \\ Ax &= +aX - \beta\omega \\ Ay &= +bX - \alpha\omega \\ AY &= +BX + D\omega \end{aligned}$$

$\varepsilon = -1$ when A is positive, X and $[Y]$ are even, or when only one condition holds.

$\varepsilon = +1$ when none or two hold.

Second class, Y an integer

$$\begin{aligned} B\xi &= +Y - A\omega \\ Bx &= +aY - \alpha\omega \\ By &= +bY - \beta\omega \\ BX &= +AY - D\omega \end{aligned}$$

$\varepsilon = +1$ when B is positive, $[X]$ and Y are even, or when only one condition holds.

$\varepsilon = -1$ when none or two hold.

[4.]

III. Collect all π for which

ξ and η satisfy the same conditions as in II;

either x or y is an integer,

and put $\varepsilon = \pm 1$ with the sign of the imaginary part of

$$\frac{m}{p - p^0}$$

Special rules: first class, x an integer

$$\begin{aligned} a\xi &= +x + b\omega \\ ay &= +bx + d\omega \\ aX &= +Ax + \beta\omega \\ aY &= +Bx + \alpha\omega \end{aligned}$$

$\varepsilon = -1$ when a is positive, $x, [y]$ are both even, or when only one condition holds.

$\varepsilon = +1$ when none or two hold.

Second class, y an integer

$$\begin{aligned} b\xi &= +y - a\omega \\ bx &= +ay - d\omega \\ bX &= +Ay - \alpha\omega \\ bY &= +By + \beta\omega \end{aligned}$$

$\varepsilon = +1$ when b is positive, $[x]$ and y are even, or when only one condition holds.

$\varepsilon = -1$ when none holds.

[5.]

IV. Collect all π for which

$$\begin{aligned}&\xi = \tfrac{1}{2} + \tfrac{1}{2}\omega\\ &\eta \text{ positive and less than } \tfrac{1}{2}\\ &X \text{ or } Y \text{ is an integer,}\end{aligned}$$

and put $\varepsilon = \pm 1$ with the sign of the imaginary part of

$$\frac{iM}{P - P^0}$$

Special rules: first class, X an integer,

$$\begin{aligned}2B\eta &= +A - 2X + A\omega\\ 2Bx &= -\beta + 2bX - \beta\omega\\ 2By &= +\alpha - 2aX + \alpha\omega\\ 2BY &= +D - 2AX + D\omega\end{aligned}$$

$\varepsilon = +1$ when B is positive, $X, [Y]$ are even, or when one condition holds,
$\varepsilon = -1$ when none or two conditions hold.
Second class, Y an integer

$$\begin{aligned}2A\eta &= -B + 2Y - B\omega\\ 2Ax &= +\alpha - 2bY + \alpha\omega\\ 2Ay &= +\beta + 2aY + \beta\omega\\ 2AX &= +D - 2BY + D\omega\end{aligned}$$

$\varepsilon = +1$ when A is positive, $[X], Y$ are even, or when one holds;
$\varepsilon = -1$ when none or two conditions hold.

[6.]

V. Collect all π for which

$$\xi, \eta \text{ satisfy the same conditions as in IV,}$$
$$\text{and where } x \text{ or } y \text{ is an integer,}$$

and put $\varepsilon = \pm 1$ with the sign of the imaginary part of

$$\frac{im}{p - p^0}$$

Special rules: first class, x an integer

$$\begin{aligned} 2b\eta &= +a - 2x + a\omega \\ 2by &= +d - 2ax + d\omega \\ 2bX &= +\beta + 2Bx + \beta\omega \\ 2bY &= +\alpha - 2Ax + \alpha\omega \end{aligned}$$

$\varepsilon = +1$ when b is positive, $x, [y]$ are even, or when one condition holds;
$\varepsilon = -1$ when none or two conditions hold.

Second class, y an integer

$$\begin{aligned} 2a\eta &= -b + 2y - b\omega \\ 2ax &= +d - 2by + d\omega \\ 2aX &= +\alpha - 2By + \alpha\omega \\ 2aY &= -\beta + 2Ay - \beta\omega \end{aligned}$$

$\varepsilon = +1$ when a is positive, $[x], y$ are even, or when one condition holds;
$\varepsilon = -1$ when none or two conditions hold.

[7.]

The first method now gives the following result:

$$\begin{aligned} 4\ \text{decident} = \text{I}\quad & \Sigma\varepsilon \text{ from all} \\ & -4\Sigma\varepsilon \text{ from those where } y \text{ integer } [x] \text{ even} \\ \text{II.}\quad & -\Sigma\varepsilon \text{ from all} \\ & +4\Sigma\varepsilon \text{ from those where } [x] \text{ even } [y] \text{ odd} \\ \text{IV.}\quad & +4\Sigma\varepsilon \text{ from those where not both } [x] \text{ and } [y] \text{ even} \\ & +Q \end{aligned}$$

Here

for A	B	$Q =$
$+$	$+$	$-\text{Intens.}\ +\mu\omega i + \text{Int.}\ \frac{1}{2}m - \mu\omega$
$+$	$-$	$-\text{Intens.}\ +\mu\omega + \text{Int.}\ \frac{1}{2}mi - \mu\omega i$
$-$	$-$	$-\text{Intens.}\ -\mu\omega i - \text{Int.}\ \frac{1}{2}m + \mu\omega$
$-$	$+$	$-\text{Intens.}\ -\mu\omega - \text{Int.}\ \frac{1}{2}mi + \mu\omega i$

The following table represents this:

α	β	A	B	A	B	A	B	A	B
		$+$	$+$	$+$	$-$	$-$	$-$	$-$	$+$
$+$	$+$	$+2$	0	0	$+2$	-3	-5	-3	-5
$+$	$-$	0	$+2$	-2	0	-5	-3	-1	-3
$-$	$-$	-3	-1	-1	$+1$	-4	-2	0	-2
$-$	$+$	$+1$	-1	-1	$+1$	0	-2	-4	-6
$\frac{m-1}{2}$		even,	odd						

The first part of

$$2Q \ldots -3 - (\alpha\beta AB) + (A\alpha) + (A\beta) + (B\alpha) - (B\beta)$$

The whole $2Q$ for

$$\begin{aligned} \tfrac{m-1}{2} \text{ odd}\quad & -3 + 4(A) - (B) - (\beta) + (\alpha A) + (\alpha B) \\ & + (\beta A) - (\beta B) - (\alpha\beta AB) \\ \tfrac{m-1}{2} \text{ even}\quad & -3 + 2(A) + (B) + (\beta) + (\alpha A) + (\alpha B) \\ & + (\beta A) - (\beta B) + 2(\beta AB) - (\alpha\beta AB) \end{aligned}$$

Example

$$\begin{array}{r|l} m = +3-2i & 13 \\ M = -1-6i & 37 \end{array} \qquad \begin{array}{r} (1+i)M + (-2+i)m = 1 \\ mM = -15-16i \end{array}$$

$$\mu = +9+20i$$

$$\begin{array}{r|r|r|r} +4+13i & +38+31i & +1 & -1 \\ +5+7i & +29+11i & 0 & +0 \\ +6+i & +20-9i & 0-i & -3 \\ +10+14i & +58+22i & +1 & +1 \\ +11+8i & +49+2i & +1 & -1 \\ +12+2i & +40-18i & +1-i & +2 \\ +16+15i & +78+13i & +2 & -0 \\ +17+9i & +69-7i & +1-i & +2 \\ +18+3i & +60-27i & +1-i & -2 \\ \hline & & \multicolumn{2}{r}{\text{decident} = -2} \end{array}$$

$$\begin{array}{lrr} \text{I}\,. & +1 & 0 \\ \text{II}\,. & 0 & -4 \\ \text{IV}\,. & & 0 \\ Q = & -5 & \\ \hline & -8 & \end{array}$$

Good.

I

$$\begin{array}{r|r|r|r|r|r|r} x & X & 20\xi & 20\eta & 20y & 20Y & \varepsilon \\ +1 & 0 & 6 & 1 & -9 & -37 & -1 \\ & +1 & 4 & 4 & +4 & -28 & -1 \\ & +2 & 2 & 7 & +17 & -19 & -1 \\ +2 & +1 & 10 & 5 & -5 & -65 & -1 \\ & +2 & 8 & 8 & +8 & -56 & +1 \\ & & & & & & -3 \end{array}$$

$$\begin{array}{r|r|r|r|r|r|r} y & Y & 20\xi & 20\eta & 20x & 20X & \varepsilon \\ 0 & -1 & 3 & 2 & +13 & +9 & +1^* \\ & -2 & 6 & 4 & +26 & +18 & +1 \\ & -3 & 9 & 6 & +39 & +27 & +1 \\ +1 & -1 & 2 & 8 & +22 & +46 & +1 \\ & & & & & & +4 \\ & & & & & & (+1) \end{array}$$

$$\begin{array}{r|r|r|r|r|r|r} y & X & 9\xi & 9\eta & 9x & 9Y & \varepsilon \\ 0 & +1 & 3 & 2 & +13 & -20 & +1 \\ -2 & +2 & 0 & 3 & +6 & -3 & -1^* \\ & & & & & & 0(-1) \end{array}$$

x	Y	9ξ	9η	$9y$	$9X$	ε
$+1$	-1	1	3	$+7$	$+17$	-1
$+2$	-3	4	3	$+1$	$+14$	$+1$
						0

I . . . $+1(0)$

II

Y	6ξ	$6x$	$6y$	$6X$	ε
-1	$+1$	$+3+9\omega$	-2	-1	-1^*
-2	$+2$	$+6+9\omega$	-4	-2	$+1$
					$0(-1)$

III

x	3ξ	$3y$	$3X$	$3Y$	ε
$+1$	1	-2	-1	$-6+9\omega$	-1

IV

X	12η	$12x$	$12y$	$12Y$	ε
0	$+1$	$+20+20\omega$	-9	-37	-1^*
$+1$	$+3$	$+24+20\omega$	-3	-39	$+1^*$
$+2$	$+5$	$+28+20\omega$	$+3$	-41	-1
					$-1(0)$

V

x	4η	$4y$	$4X$	$4Y$	ε
$+2$	$+1$	-1	$+4-20\omega$	-13	$+1$

y	6η	$6x$	$6X$	$6Y$	ε
0	$+2$	$+13$	$+9$	-20	$+1$

[8.]

We now wish to examine the result of I more closely. There are four combinations:
1^0, when x and X are integers. Here

$$\beta\xi = -Bx + bX$$
$$\beta\eta = -Ax + aX$$
$$\beta y = -\alpha x + dX$$
$$\beta Y = -Dx + \alpha X$$

Let y^0 and Y^0 be the absolutely least residues of $-\alpha x + dX$, $-Dx + \alpha X$ modulo β, and $\beta y = \beta y' + y^0$, $\beta Y = \beta Y' + Y^0$, and put

$$\begin{aligned} \beta u &= -By^0 + bY^0 \qquad & y^0 &= +au - bt \\ \beta t &= -Ay^0 + aY^0 \qquad & Y^0 &= +Au - Bt \end{aligned}$$

Then t, u will be integers, namely

$$\begin{aligned} -u + ti &= M(x + y'i) - m(X + Y'i)\ ^* \\ i(t + ui) &= Mi(y' - y) - mi(Y' - Y) \end{aligned}$$

and then $\varepsilon = -1$ when
$t + u$ is even, β, y^0, Y^0 positive, or when two or none of the conditions holds; otherwise $\varepsilon = +1$.

We put

$$\begin{aligned} t + ui = +\theta &\quad \text{when } y^0 \text{ and } Y^0 \text{ both positive} \\ -\theta &\quad y^0 \text{ and } Y^0 \text{ both negative} \\ +\theta' &\quad y^0 \text{ positive } Y^0 \text{ negative} \\ -\theta' &\quad y^0 \text{ negative } Y^0 \text{ positive} \end{aligned}$$

to each divisible by $1+i$	θ	there then corresponds	$\varepsilon = -1$
to each divisible by $1+i$	θ'		$\varepsilon = +1$
to each not divisible by $1+i$	θ		$\varepsilon = +1$
to each not divisible by $1+i$	θ'		$\varepsilon = -1$

provided that β is positive.

For negative β the rule is reversed.

x	X	y^0	Y^0	$t+ui$	θ	θ'	ε
$+1$	0	-9	$+3$	$0-3i$		$0+3i$	-1
	$+1$	$+4$	-8	$-1+2i$		$-1+2i$	-1
	$+2$	-3	$+1$	$0-i$		$0+i$	-1
$+2$	$+1$	-5	-5	$-1-i$	$+1+i$		-1
	$+2$	$+8$	$+4$	$+1+2i$	$+1+2i$		$+1$

[9.]

2^0, when y and Y are integers. Here let x', X' be the nearest integers to x and X, and

$$x - x' = \frac{x^0}{\beta}, \quad X - X' = \frac{X^0}{\beta}$$

and put

$$\begin{aligned} \beta(t + ui) &= -Mx^0 + mX^0 = -Mp^0 + mP^0, \\ t + ui &= Mp' - mP' \end{aligned}$$

that is,

$$\beta t = -Ax^0 + aX^0 \qquad x^0 = -bt + au$$
$$\beta u = -Bx^0 + bX^0 \qquad X^0 = -Bt + Au$$

Then

$\varepsilon = -1$, when β positive, x^0 positive, X^0 positive, $t+u$ even
etc.

We put

		better
$t+ui = +\theta$	when x^0 and X^0 positive	$+\theta''$
$= -\theta$	when both negative	$-\theta''$
$= +\theta'$	when x^0 positive, X^0 negative	$-\theta$
$= -\theta'$	when x^0 negative, X^0 positive	$+\theta$

where the same rule for ε will hold as above.

y	Y	x^0	X^0	$t+ui$	θ	θ'	ε
0	-1	-7	$+9$	$+1-3i$		$-1+3i$	$+1$
	-2	$+6$	-2	$0+2i$		$0+2i$	$+1$
	-3	-1	$+7$	$+1-i$		$-1+i$	$+1$
$+1$	-1	$+2$	$+6$	$+1$	$+1$		$+1$

It can now be proved

1) That all θ obtained from (1) and from (2) are distinct from one another. Call their collection Θ.

2) That all $\theta = T + Ui$ have the property that

$$-bT + aU$$
$$-BT + AU$$

are positive numbers less than $\frac{1}{2}\beta$.

3) That if T, U are two integers satisfying the conditions just mentioned, $T + Ui$ is certainly in Θ.

(How, then? It is based on the above equation *.)

4) The same holds in a similar way for θ', whose collection Θ' will consist of those numbers $T' + U'i$ for which

$$-bT' + aU'$$
$$-(-BT' + AU')$$

are positive numbers less than $\frac{1}{2}\beta$.

In our case

θ	ε	θ'	ε	θ''	ε	θ'''	ε
$+1$	$+1$	$0+i$	-1	$+2-i$	$+1$	$+1$	-1
$+1+i$	-1	$0+2i$	$+1$	$+3-i$	-1	$+2$	$+1$
$+1+2i$	$+1$	$0+3i$	-1				
		$-1+i$	$+1$				
		$-1+2i$	-1				
		$-1+3i$	$+1$				

Here

$$\theta = -_*M + {}_*m$$
$$\theta' = -_*M - {}_*m$$
$$\theta'' = +_*Mi + {}_*m$$
$$\theta''' = +_*Mi - {}_*m$$

[10.]

3^0. y and X integers. Let x', Y' be the nearest integers to x and Y, and

$$x' + yi = p', \quad X + Y'i = P'; \quad p - p' = \frac{p^0}{\alpha}, \quad P - P' = \frac{P^0}{\alpha}$$

and put

$$i(t+ui) = Mp' - mP' = -\frac{Mp^0}{\alpha} + \frac{mP^0}{\alpha}$$
$$= -\frac{Mx^0}{\alpha} + \frac{miY^0}{\alpha} \quad \text{that is}$$
$$\alpha t = -Bx^0 + aY^0 \quad \text{then} \quad x^0 = -bt + au$$
$$\alpha u = +Ax^0 + bY^0 \qquad\qquad Y^0 = +At + Bu$$

Then

$\varepsilon = -1$, when α positive, x^0 positive, Y^0 positive, $t+u$ even etc.

We put

$$\begin{array}{rll} & & \textit{better} \\ t+ui = +\theta'' & \text{when } x^0 \text{ positive, } Y^0 \text{ positive} & +\theta' \\ = +\theta''' & \text{when } x^0 \text{ positive, } Y^0 \text{ negative} & -\theta''' \\ -\theta'' & \text{when } x^0 \text{ negative, } Y^0 \text{ negative} & -\theta' \\ -\theta''' & \text{when } x^0 \text{ negative, } Y^0 \text{ positive} & +\theta''' \end{array}$$

$$\begin{array}{rl} \text{Thus, for each} & \theta'' \ldots \varepsilon = -1 \\ & \theta''' \ldots \varepsilon = +1 \end{array}$$

provided that θ'' or θ''' is divisible by $1+i$ and α is positive.

y	X	x^0	X^0	$t+ui$	θ''	θ'''	ε
0	+1	+4	−2	+2		+2	+1
+1	+2	−3	−3	$-3+i$	$+3-i$		−1

[11.]

Class 4, x and Y integers. With assumptions similar to those in 3, put

$$-(t+ui) = Mp' - mP' = -\frac{Mp^0}{\alpha} + \frac{mP^0}{\alpha}$$
$$= -\frac{Miy^0}{\alpha} + \frac{mX^0}{\alpha}$$

$$\alpha t = -By^0 - aX^0 \qquad y^0 = -bt + au$$
$$\alpha u = +Ay^0 - bX^0 \qquad X^0 = -At - Bu$$

Then

$\varepsilon = +1$ when α positive, y^0 positive, X^0 positive, $t+u$ even etc.

We put

$$\begin{aligned} t+ui = +\theta'' &\quad \text{when } y^0 \text{ positive } X^0 \text{ negative} \\ +\theta''' &\quad \text{when } y^0 \text{ positive } X^0 \text{ positive} \\ -\theta'' &\quad \text{when } y^0 \text{ negative } X^0 \text{ positive} \\ -\theta''' &\quad \text{when } y^0 \text{ negative } X^0 \text{ negative} \end{aligned}$$

For ε the rule then holds (as above in 3), provided that α is positive:

$$\varepsilon = -1 \text{ for each (divisibility by } 1+i\text{):} \begin{cases} \text{divisible} & \theta'' \\ \text{not divisible} & \theta''' \end{cases}$$

$$\varepsilon = +1 \text{ for each (divisibility by } 1-i\text{):} \begin{cases} \text{divisible} & \theta''' \\ \text{not divisible} & \theta'' \end{cases}$$

x	Y	y^0	X^0	$t+ui$	θ''	θ'''	ε
$+1$	-1	-2	-1	-1		$+1$	-1
$+2$	-3	$+1$	-4	$+2-i$	$+2-i$		$+1$

The collection of all θ'' from 3 and 4, which we denote by Θ'', therefore consists of all numbers $T+Ui$ for which

$$\left.\begin{aligned} -bT + aU \\ \text{and } +AT + BU \end{aligned}\right\} \text{ positive and less than } \frac{1}{2}\alpha$$

the collection of all $\theta''' \ldots$ (Θ''') of those for which

$$\left.\begin{aligned} -bT + aU \\ -AT - BU \end{aligned}\right\} \text{ positive and less than } \frac{1}{2}\alpha$$

[12.]

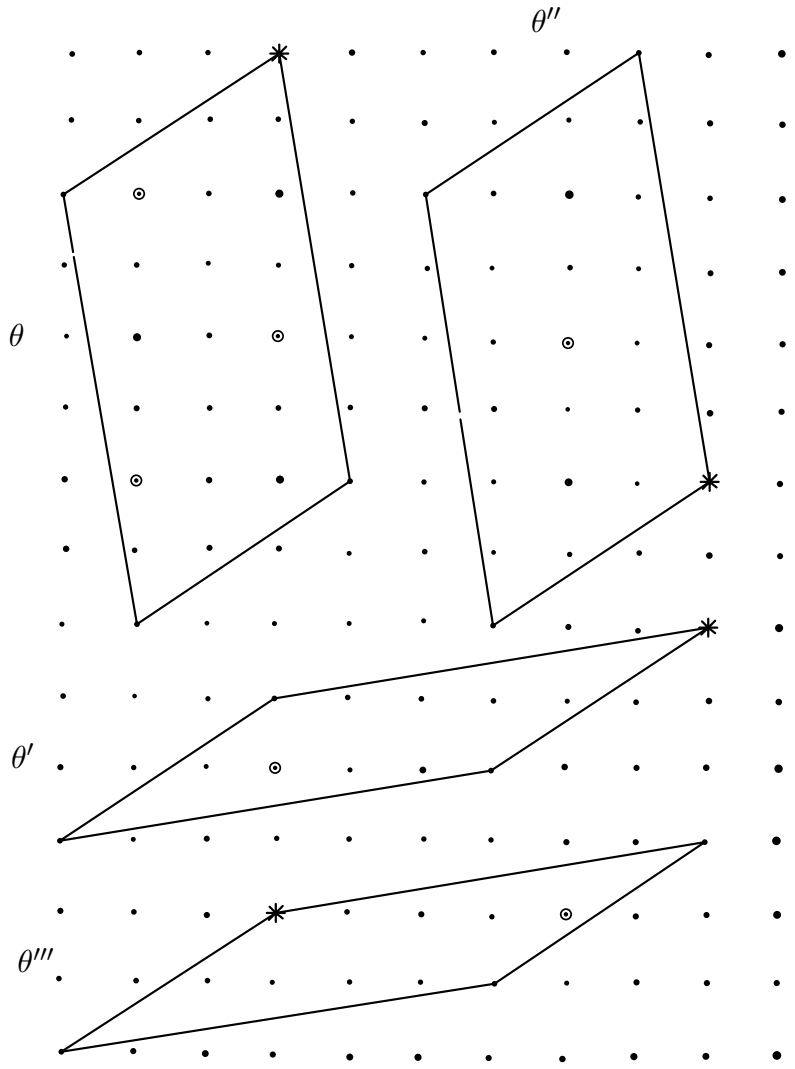
After the above improvement, the rule therefore reads as follows:
Let

$$\begin{aligned}
\Theta &\text{ contain all numbers } T+Ui, \text{ where } +bT-aU \text{ positive} \\
&\quad -BT+AU \text{ positive and } <\tfrac{1}{2}\beta \\
\Theta' &\text{ contain all numbers } T+Ui, \text{ where } -bT+aU \text{ positive} \\
&\quad +AT+BU \text{ positive and } <\tfrac{1}{2}\alpha \\
\Theta'' &\text{ contain all numbers } T+Ui, \text{ where } -bT+aU \text{ positive} \\
&\quad -BT+AU \text{ positive and } <\tfrac{1}{2}\beta \\
\Theta''' &\text{ contain all numbers } T+Ui, \text{ where } +bT-aU \text{ positive} \\
&\quad +AT+BU \text{ positive and } <\tfrac{1}{2}\alpha
\end{aligned}$$

provided that β or α, respectively, is positive.

For all divisible by	then	when
$1+i$	$\varepsilon =$	
θ	$+1$	β positive
θ'	-1	α positive
θ''	-1	β positive
θ'''	$+1$	α positive

Θ		Θ'		Θ''		Θ'''	
$0-i$	-1	$+2-i$	$+1$	$+1$	$+1$	-1	-1
$0-2i$	$+1$	$+3-i$	-1	$+1+i$	-1	-2	$+1$
$0-3i$	-1			$+1+2i$	$+1$		
$+1-i$	$+1$						
$+1-2i$	-1						
$+1-3i$	$+1$						



[13.]

This yields the following rule. Let the results of the instructions be

$$\text{II}\ldots\ G, \quad \text{III}\ldots\ g, \quad \text{IV}\ldots\ H, \quad \text{V}\ldots\ h$$

Then

$$\begin{aligned} 4\Theta &= R = 0 \\ 4\Theta' &= -g + G - h - H + R' \\ 4\Theta'' &= -2g + 2G + R'' \\ 4\Theta''' &= -g + G + h + H + R''' \end{aligned}$$

In our example

$$G = 0, \quad g = -1, \quad H = -1, \quad h = +2,$$
$$R' = 0, \quad R'' = +2, \quad R''' = -2$$
$$4\Theta = 0, \quad 4\Theta' = +1 - 1 + 0 = 0,$$
$$4\Theta'' = +2 + 2 = +4, \quad 4\Theta''' = +1 + 1 - 2 = 0$$

and the corrections R, R' etc. are determined as follows:

$$R = \begin{cases} -(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) - \frac{1}{2}(B) \\ +(\beta) - \frac{1}{2}(\alpha\beta) - \frac{1}{2}(\alpha\beta abAB) \\ +\frac{1}{2}(b) + \frac{1}{2}(B) \end{cases}$$

$$R' = \begin{cases} +(\alpha) - \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) - \frac{1}{2}(A) \\ 0 \\ -\frac{1}{2}(a) + \frac{1}{2}(B) \end{cases}$$

$$R'' = \begin{cases} +(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(B) \\ +(\beta) + \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(B) \end{cases}$$

$$R''' = \begin{cases} -(\alpha) - \frac{1}{2}(\alpha\beta) + \frac{1}{2}(\alpha\beta abAB) \\ -\frac{1}{2}(b) + \frac{1}{2}(A) \\ 0 \\ +\frac{1}{2}(a) + \frac{1}{2}(B) \end{cases}$$

where the quantities in parentheses supply only the signs.

Thus

$$R + R' + R'' + R''' = 2(\alpha\beta abAB) - 2(b) + 2(B) + 2(\beta)$$

consequently

$$\begin{aligned} \Theta + \Theta' + \Theta'' + \Theta''' = & -g + G + \tfrac{1}{2}(\alpha\beta abAB) \\ & + \tfrac{1}{2}(\beta) - \tfrac{1}{2}(b) + \tfrac{1}{2}(B) \\ = & -g + G + S \end{aligned}$$

ab		+	+		−	+		−	−		+	−	
A	B	α	β	S	α	β	S	α	β	S	α	β	S
+	+	+	+	+1	−	+	+1	−	−	+1	+	−	+1
		+	−	−1	+	+	0	−	+	+1	−	−	0
−	+	+	−	0	+	+	+1	−	+	+2	−	−	+1
		−	−	−1	+	−	−1	+	+	+1	−	+	+1
−	−	−	−	−1	+	−	−1	+	+	+1	−	+	+1
		−	+	−1	−	−	−2	+	−	−1	+	+	0
+	−	−	+	0	−	−	−1	+	−	0	+	+	+1
		+	+	−1	−	+	−1	−	−	−1	+	−	−1

[14.]

The first rule now accordingly takes the following form:

$4\,\text{Dec.} =$ I. $-4\Sigma\varepsilon$ from those where y integer, $[x]$ even
II. $+4\Sigma\varepsilon$ from those where $[x]$ even, $[y]$ odd
III. $-\Sigma\varepsilon$ from all
IV. $+4\Sigma\varepsilon$ from those where not both $[x]$ and $[y]$ even
$+Q+S$

In our example

I....	0
II....	−4
III	+1
IV	0
Q	−5
S	0
	−8

Now suppose that in III those for which y is an integer, $[x]$ even, are specially marked. Then

$$\left.\begin{array}{l}\text{III. } \Sigma\varepsilon \text{ from all}\\ \quad -4\Sigma\varepsilon \text{ from the specially marked}\end{array}\right\} = \text{Intensor } (\tfrac{1}{2}-\omega)m - \text{Intens. } \omega m = -W$$

Here

	a	b		
	+	+	−3	−1
	−	+	−2	0
$W=$	−	−	+2	0
	−	+	+3	+1
			$\frac{m-1}{2}$ even	$\frac{m-1}{2}$ odd

Thus

$$\begin{aligned} 4\,\text{decident} = {} & \text{I. } -4\Sigma\varepsilon \quad y \text{ integer, } [x] \text{ even} \\ & \text{II. } +4\Sigma\varepsilon \quad [x] \text{ even, } [y] \text{ odd} \\ & \text{III. } -4\Sigma\varepsilon \quad y \text{ integer, } [x] \text{ even} \\ & \text{IV. } +4\Sigma\varepsilon \quad \text{all where not both } [x], [y] \text{ even} \\ & +Q+S+W \end{aligned}$$

Table for $\frac{1}{4}(Q+S+W)$

a	b	A	B	α	β			a	b	A	B	α	β		
+	+	+	+	+	+	0	0	−	−	+	+	−	−	0	0
				+	−	−1	0					−	+	+1	0
		−	+	+	−	−1	−1			−	+	−	+	0	−1
				−	−	−1	−1					+	+	0	−1
		−	−	−	−	−2	−1			−	−	+	+	0	−1
				−	+	−1	−1					+	−	−1	−1
		+	−	−	+	−1	0			+	−	+	−	0	0
				+	+	−1	0					−	−	0	0
−	+	+	+	−	+	0	0	+	−	+	+	+	−	+1	+1
				+	+	0	0					−	−	0	0
		−	+	+	+	−1	−1			−	+	−	−	+1	0
				+	−	−1	−1					−	+	0	−1
		−	−	+	−	−2	−1			−	−	−	+	+1	0
				−	−	−2	−1					+	+	0	−1
		+	−	−	−	−1	0			+	−	+	+	+1	+1
				−	+	−1	0					+	−	0	0

[15.]

The second method is as follows:

$$\begin{aligned}\text{decident} = \text{I. } &+\Sigma\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even}\\ &-4\Sigma\varepsilon, \text{ among these, where also } y \text{ integer, } [x] \text{ even}\\ \text{II. } &+\Sigma\lambda\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even;}\\ &\quad \lambda \text{ is the intensor of } p\\ \text{II. } &-\Sigma\lambda'\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ odd}\\ &\quad \lambda' \text{ the intensor of } ip = 1,\ 2,\ 3,\ 0\\ &\qquad \text{when } \lambda = 0,\ 1,\ 2,\ 3\\ \text{IV. } &+\Sigma\lambda\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even,}\\ &\quad \lambda \text{ the intensor of } p\\ \text{IV. } &+\Sigma\lambda'\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ even}\\ &\quad \lambda' \text{ the intensor of } im - ip = 0 \quad 3 \quad 2 \quad 1\\ &\qquad \text{when Int. } p = 0 \quad 1 \quad 2 \quad 3\\ &+q\end{aligned}$$

Here $q = 0$ when $\frac{M-1}{2}$ is odd, i.e. divisible only by $1+i$, not by 2, and not at the same time $AB + -$; otherwise,

A	B		α	β	α	β	α	β	α	β
			+	+	−	+	−	−	+	−
+	+	Int. $\frac{1}{2}(m-\omega\mu)$	+3	+1	+3	+1	+0	+2	+0	+2
−	+	0	0		0		0		0	
−	−	−Int. $\frac{1}{2}(m+\omega\mu)$	−0	−2	−0	−2	−3	−1	−3	−1
+	−	−Int. $\omega\mu$	−0		−1		−2		−3	

Where two numbers are given, the first applies to even $\frac{m-1}{2}$, the other to odd.

In our example:

I.	y	Y	$20x$	$20Y$	ε	
	0	−1	+13	+9	+1*	+3
	0	−2	+26	+18	+1	−4
	+1	−1	+22	+46	+1	−1
					+3(+1)	Dec. = −2

II. Absent.

IV.	X	$12x$	$12y$	$12Y$	ε	λ	λ'	$\lambda'\varepsilon$
	0	$+20+20\omega$	−9	−37	−1	2	2	−2
	+1	$+24+20\omega$	−3	−39	+1	3	1	+1
	+2	$+28+20\omega$	+3	−41	−1	0	0	0
								−1

The contributions from II combine into the following result:

$$\begin{aligned}
\text{II. } &-\Sigma\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even}\\
&+4\Sigma\varepsilon, \text{ from these same ones, when also } [x] \text{ even,}\\
&\quad [y] \text{ odd}\\
\text{II. } &+\Sigma\lambda'\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even}\\
&-\Sigma\lambda'\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ odd,}\\
&\quad \lambda' \text{ the intensor of } ip
\end{aligned}$$

The last two parts in turn combine into

$$\begin{aligned}
\text{III. } &+\Sigma\varepsilon, \text{ where } [X] \text{ even, } [Y] \text{ odd}\\
&-4\Sigma\varepsilon, \text{ when also } x \text{ an integer, } [y] \text{ odd}\\
&+r+s
\end{aligned}$$

where $r = 0$ when $AB \ldots\ldots \begin{cases} + & + \\ - & + \\ - & - \end{cases}$

and $r = \text{Int. } \omega mi$ when $AB \ldots + \ -$

$$s = -\text{Int. } (\tfrac{1}{2} - \omega)mi, \quad \text{when } \frac{M-1}{2} \text{ even and } B \text{ positive,}$$
$$\text{in all other cases } = 0$$

In our example

$$\text{III. Drops out.} \quad r = 0, \ s = 0$$

The contributions from IV combine into the following result:

$$\begin{aligned}
\text{IV. } &+4\Sigma\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even and not both}\\
&\quad [x] \text{ even, } [y] \text{ even}\\
&-\Sigma\lambda'\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ even}\\
&+\Sigma\lambda'\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ even}\\
&\quad \text{where } \lambda' \text{ Int. of } im - ip
\end{aligned}$$

The last two parts in turn combine into

$$\begin{aligned}
\text{V. } &+\Sigma\varepsilon, \text{ where not both } [X] \text{ and } [Y] \text{ even}\\
&-4\Sigma\varepsilon, \text{ where also } x \text{ an integer, } [y] \text{ even}\\
&+w
\end{aligned}$$

Here $w = 0$ when $\frac{M-1}{2}$ is even and A positive; in all other cases

$$= -\text{Intensor } (\tfrac{1}{2}i + \omega)m$$

In our example

V.

y	$6x$	$6X$	$6Y$	ε
0	+13	+9	−20	+1

$$w = -2$$

Table for q, r, s, w and their sum.

a b A B α β	$\frac{M-1}{2}$ even $\frac{m-1}{2}$ even	$\frac{M-1}{2}$ odd $\frac{m-1}{2}$ even	$\frac{M-1}{2}$ even $\frac{m-1}{2}$ odd	$\frac{M-1}{2}$ odd $\frac{m-1}{2}$ odd
+ + + + + +	+3 0 0 0 +3	0 0 0 0 0	+1 0 −2 0 −1	0 0 0 −2 −2
+ −	0 0 0 0 0	0 0 0 0 0	+2 0 −2 0 0	0 0 0 −2 −2
− + + −	0 0 0 0 0	0 0 0 0 0	0 0 −2 −2 −4	0 0 0 −2 −2
− −	0 0 0 0 0	0 0 0 0 0	0 0 −2 −2 −4	0 0 0 −2 −2
− − − −	−3 0 0 0 −3	0 0 0 0 0	−1 0 0 −2 −3	0 0 0 −2 −2
− +	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
+ − − +	−1 +1 0 0 0	−1 +1 0 0 0	−1 +1 0 0 0	−1 +1 0 −2 −2
+ +	0 +1 0 0 +1	0 +1 0 0 +1	0 +1 0 0 +1	0 +1 0 −2 −1
− + + + − +	+3 0 0 0 +3	0 0 0 −1 −1	+1 0 −2 0 −1	0 0 0 −3 −3
+ +	+3 0 0 0 +3	0 0 0 −1 −1	+1 0 −2 0 −1	0 0 0 −3 −3
− + + +	0 0 0 −1 −1	0 0 0 −1 −1	0 0 −2 −3 −5	0 0 0 −3 −3
+ −	0 0 0 −1 −1	0 0 0 −1 −1	0 0 −2 −3 −5	0 0 0 −3 −3
− − + −	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
− −	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
+ − − −	−2 +2 0 0 0	−2 +2 0 −1 −1	−2 +2 0 0 0	−2 +2 0 −3 −3
− +	−1 +2 0 0 +1	−1 +2 0 −1 0	−1 +2 0 0 +1	−1 +2 0 −3 −2
− − + + − −	0 0 −1 0 −1	0 0 0 −1 −1	+2 0 −3 0 −1	0 0 0 −3 −3
− +	+3 0 −1 0 +2	0 0 0 −1 −1	+1 0 −3 0 −2	0 0 0 −3 −3
− + − +	0 0 −1 −1 −2	0 0 0 −1 −1	0 0 −3 −3 −6	0 0 0 −3 −3
+ +	0 0 −1 −1 −2	0 0 0 −1 −1	0 0 −3 −3 −6	0 0 0 −3 −3
− − + +	0 0 0 −1 −1	0 0 0 −1 −1	−2 0 0 −3 −5	0 0 0 −3 −3
+ −	−3 0 0 −1 −4	0 0 0 −1 −1	−1 0 0 −3 −4	0 0 0 −3 −3
+ − + −	−3 +3 0 0 0	−3 +3 0 −1 −1	−3 +3 0 0 0	−3 +3 0 −3 −3
− −	−2 +3 0 0 +1	−2 +3 0 −1 0	−2 +3 0 0 +1	−2 +3 0 −3 −2
+ − + + + −	0 0 −1 0 −1	0 0 0 0 0	+2 0 −3 0 −1	0 0 0 −2 −2
− −	0 0 −1 0 −1	0 0 0 0 0	+2 0 −3 0 −1	0 0 0 −2 −2
− + − −	0 0 −1 0 −1	0 0 0 0 0	0 0 −3 −2 −5	0 0 0 −2 −2
− +	0 0 −1 0 −1	0 0 0 0 0	0 0 −3 −2 −5	0 0 0 −2 −2
− − − +	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
+ +	0 0 0 0 0	0 0 0 0 0	−2 0 0 −2 −4	0 0 0 −2 −2
+ − + +	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 −2 −2
+ −	−3 0 0 0 −3	−3 0 0 0 −3	−3 0 0 0 −3	−3 0 0 −2 −5

[16.]

Consequently,

$$\text{Dec. } \frac{m}{M} - \text{Dec. } \frac{M}{m} =$$

I. $-4\Sigma\varepsilon$, where y, Y integer, $[x], [X]$ even

II. $+4\Sigma\varepsilon$, Y integer, $[X]$ even, $[x]$ even, $[y]$ odd

III. $-4\Sigma\varepsilon$, x integer, $[X]$ even, $[Y]$ odd, $[y]$ odd

IV. $+4\Sigma\varepsilon$, Y integer, $[X]$ even, and not both $[x], [y]$ even

V. $-4\Sigma\varepsilon$, x integer, $[y]$ even and not both $[X], [Y]$ even

$+\psi$

Here ψ is represented in the following table:

a	b	A	B	α	β	ψ	a	b	A	B	α	β	ψ
+	+	+	+	+	+	+4 0 0 −2	−	−	+	+	−	−	0 0 0 −2
		+	+	+	−	0 0 0 −2			+	+	−	+	+4 0 0 −2
		−	+	+	−	0 −4 0 −2			−	+	−	+	0 −4 0 −2
		−	+	−	−	0 −4 0 −2			−	+	+	+	0 −4 0 −2
		−	−	−	−	−4 −4 0 −2			−	−	+	+	0 −4 0 −2
		−	−	−	+	0 −4 0 −2			−	−	+	−	−4 −4 0 −2
		+	−	−	+	0 0 0 −2			+	−	+	−	0 0 0 −2
		+	−	+	+	0 0 0 −2			+	−	−	−	0 0 0 −2
−	+	+	+	−	+	+4 0 0 −2	+	−	+	+	+	−	0 0 0 −2
		+	+	+	+	+4 0 0 −2			+	+	−	−	0 0 0 −2
		−	+	+	+	0 −4 0 −2			−	+	−	−	0 −4 0 −2
		−	+	+	−	0 −4 0 −2			−	+	−	+	0 −4 0 −2
		−	−	+	−	−4 −4 0 −2			−	−	−	+	0 −4 0 −2
		−	−	−	−	−4 −4 0 −2			−	−	+	+	0 −4 0 −2
		+	−	−	−	0 0 0 −2			+	−	+	+	0 0 0 −2
		+	−	−	+	0 0 0 −2			+	−	+	−	−4 −4 −4 −6

Here the first two columns apply	to $\frac{1}{2}(M-1)$ even
the last two	to $\frac{1}{2}(M-1)$ odd
the first and third	to $\frac{1}{2}(m-1)$ even
the second and fourth	to $\frac{1}{2}(m-1)$ odd

[17.]

The 128 cases distinguished in the above table in determining ψ can be expressed much more briefly as follows:

$$\psi = k + l$$

$k = -4$ when $a, A, \alpha, b, B, \beta$ have, respectively, the signs $+\ +\ +\ -\ -\ -$; otherwise always

$$k = 0$$

$\frac{1}{2}(M-1)$ even	$\frac{1}{2}(m-1)$ even	$l = +4$,	when $AB\beta$ positive
		-4,	when $AB\beta$ negative
		0,	in all other cases
$\frac{1}{2}(M-1)$ even	$\frac{1}{2}(m-1)$ odd	$l = -4$,	when A negative
		0,	when A positive
$\frac{1}{2}(M-1)$ odd	$\frac{1}{2}(m-1)$ even	$l = 0$	
$\frac{1}{2}(M-1)$ odd	$\frac{1}{2}(m-1)$ odd	$l = -2$	

It remains to be tried whether it is more advantageous to take A and a positive, but $m \equiv 1$, $M \equiv 1$ only modulo 2 (not modulo $2 + 2i$). The final result must be

$$\text{Dec. } \frac{m}{M} - \text{Dec. } \frac{M}{m} \equiv$$

	$M \equiv$			
$m \equiv$	1	$1+2i$	3	$3+2i$
1	0	0	0	0
$1+2i$	0	2	2	0
3	0	2	0	2
$3+2i$	0	0	2	2

Everything modulo 4.

[VI.]

Theory of Biquadratic Residues.

1.

Let a sequence of complex integers $\varphi, \varphi', \varphi''$, and so on, satisfy two conditions: first, they are all pairwise incongruent modulo $\mu = \alpha + \beta i$, where α and β denote real integers; second, every complex integer is congruent to one of them modulo μ. Under this assumption, the collection of numbers $\varphi, \varphi', \varphi''$, and so on, is called a complete residue system for the modulus μ. It has been proved that the number of its members equals the norm of μ, that is, the number $\alpha\alpha + \beta\beta$, which will be denoted by ν.

2.

Among the numbers $\varphi, \varphi', \varphi''$, and so on, one is divisible by μ. If it is excluded and the collection of the others is denoted by χ, then χ forms a complete system of residues not divisible by the modulus, their number being $= \nu - 1$. If we restrict the investigation to odd moduli, $\nu - 1$ is divisible by 4. Furthermore, $f, if, -f, -if$ will then be pairwise incongruent; hence the numbers in χ congruent, respectively, to $if, -f, -if$ are distinct from one another and from f. (Associated and composite numbers.)

This partitions χ into four groups or partial systems $\kappa, \kappa', \kappa'', \kappa'''$. Place any number from χ, for example φ, in the group κ, and the three members of χ congruent to $i\varphi, -\varphi, -i\varphi$ in the groups $\kappa', \kappa'', \kappa'''$, in that order. After removing these four numbers from χ, again place any one of the remaining numbers in κ, and the three that depend on it in the same way in $\kappa', \kappa'', \kappa'''$. Continue until the entire system χ has been distributed. The groups $\kappa, \kappa', \kappa'', \kappa'''$ will be called associated quarter systems. They clearly have the following properties:

1) Each quarter system consists of $\frac{1}{4}(\nu - 1) = \frac{1}{4}(\alpha\alpha + \beta\beta - 1)$ numbers.

2) The characteristic property of a quarter system is that none of its numbers, either itself or multiplied by $i, -1$ or $-i$, is congruent to another number in the same quarter system, whereas every number not divisible by μ, either itself or multiplied by $i, -1$ or $-i$, occurs in it or is congruent to one of its members.

3) Just as multiplying the numbers in κ by $i, -1$ and $-i$ gives, respectively, the numbers in $\kappa', \kappa'', \kappa'''$, or numbers congruent to them, multiplying the numbers in κ' by those factors reproduces, respectively, the numbers

in $\kappa'', \kappa''', \kappa$; multiplying the numbers in κ'' similarly reproduces the numbers in $\kappa''', \kappa, \kappa'$; finally, multiplying the numbers in κ''' reproduces $\kappa, \kappa', \kappa''$.

For brevity, this mutual dependence of the four quarter systems can be expressed as

$$\begin{aligned} \kappa' &\equiv i\kappa, \\ \kappa'' &\equiv -\kappa \equiv i\kappa', \\ \kappa''' &\equiv i\kappa'' \equiv -\kappa' \equiv -i\kappa. \end{aligned}$$

3.

If m denotes a complex integer having no common divisor with μ, and every number of a quarter system κ is multiplied by m, the products, or any numbers congruent to them, themselves form a quarter system. Likewise, multiplying the numbers of the systems $\kappa', \kappa'', \kappa'''$ gives three further quarter systems associated with the first. The proof is easy to give. Denote these four new systems by $m\kappa, m\kappa', m\kappa'', m\kappa'''$, whether the products themselves or only numbers congruent to them are chosen. In the latter case, the choice can always be made from one of the systems $\kappa, \kappa', \kappa'', \kappa'''$. Thus the system χ has been partitioned into quarter systems in two different ways, at least generally speaking. Suppose that $m\kappa$ has in common

$$\begin{aligned} \text{with } \kappa \ldots\ldots &\quad \lambda \text{ numbers} \\ \kappa' \ldots\ldots &\quad \lambda' \text{ numbers} \\ \kappa'' \ldots\ldots &\quad \lambda'' \text{ numbers} \\ \kappa''' \ldots\ldots &\quad \lambda''' \text{ numbers} \end{aligned}$$

Then κ' with $m\kappa'$, κ'' with $m\kappa''$, and κ''' with $m\kappa'''$ will also have λ members in common; κ'' with $m\kappa'$, κ''' with $m\kappa''$, κ with $m\kappa'''$, λ' members, and so on. Let ε be the least residue of $\lambda' + 2\lambda'' + 3\lambda'''$ modulo 4, or let ε be one of the four numbers $0, 1, 2, 3$ according as $\lambda' + 2\lambda'' + 3\lambda'''$ has the form $4n, 4n+1, 4n+2, 4n+3$. I now claim that ε is independent of the arrangement of the quarter system κ.

To make the proof easier, I use the following notation. Let $\Pi\psi$ denote the number $0, 1, 2, 3$ according as the number ψ, not divisible by μ, occurs (itself or through representation by congruence) in the group $\kappa, \kappa', \kappa'', \kappa'''$. The following consequences are therefore immediate:

I. $\Pi(i\psi) \equiv 1 + \Pi\psi \pmod 4$.

II. The number $i^{-\Pi\psi} \,.\, \psi$ occurs, itself or through representation by congruence, in the group κ.

III. $\Sigma\Pi m\varphi \equiv \varepsilon, \pmod 4$, when the sum extends over all members φ occurring in κ.

Now let k be another quarter system, consisting of f, f', f'', and so on, while κ consists of $\varphi, \varphi', \varphi''$, and so on. I assume, as is allowed because the *order* of the members of κ is arbitrary, that f is identical with or associated with φ, f' with φ', f'' with φ'', and so on. Let the quarter groups associated with k be $k'(\equiv ik)$, $k''(\equiv -k)$, $k'''(\equiv -ik)$. Furthermore, let the characteristic P have the same meaning for the groups k, k', k'', k''' as Π has for $\kappa, \kappa', \kappa'', \kappa'''$, so that $\mathrm{P}\psi = 0, 1, 2, 3$ according as ψ belongs to k, k', k'', k'''.

Thus, if the partition of χ into the quarter systems k, k', k'', k''' is used instead of $\kappa, \kappa', \kappa'', \kappa'''$, the least residue of $\mathrm{P}mf + \mathrm{P}mf' + \mathrm{P}mf'' + \mathrm{P}mf'''$, and so on, and so on, or of $\Sigma\mathrm{P}mf$, modulo 4, takes the place of ε; and it remains to prove that $\Sigma\mathrm{P}mf - \Sigma\Pi m\varphi$ is divisible by 4.

We write this quantity as

$$\begin{array}{r} \mathrm{P}mf + \mathrm{P}mf' + \mathrm{P}mf'' + \mathrm{P}mf''' + \text{and so on} \\ -\mathrm{P}m\varphi - \mathrm{P}m\varphi' - \mathrm{P}m\varphi'' - \mathrm{P}m\varphi'''- \\ +\mathrm{P}m\varphi + \mathrm{P}m\varphi' + \mathrm{P}m\varphi'' + \mathrm{P}m\varphi'''+ \\ -\Pi m\varphi - \Pi m\varphi' - \Pi m\varphi'' - \Pi m\varphi'''- \end{array}$$

Since, by assumption, f and φ are congruent or associated, the same holds for mf and $m\psi$, and

$$\left.\begin{array}{r} f \equiv i^{-\mathrm{P}\varphi}\varphi \\ i^{-\mathrm{P}mf}mf \equiv i^{-\mathrm{P}m\varphi}m\varphi \end{array}\right\} \text{ mod. } \mu$$

From this it follows easily that $\mathrm{P}mf - \mathrm{P}m\varphi \equiv -\mathrm{P}\varphi$ (mod. 4) and that the sum of the top two rows $\equiv -\Sigma\mathrm{P}\varphi$. Furthermore, since $\mathrm{P}m\varphi - \Pi m\varphi \equiv \mathrm{P}(i^{-\Pi m\varphi}m\varphi)$, $m\varphi \,.\, i^{-\Pi m\varphi}$ belongs to κ, and the collection of *all* $m\varphi \,.\, i^{-\Pi m\varphi}$, regardless of order, agrees with all φ, the sum of *all* $\mathrm{P}(m\varphi \,.\, i^{-\Pi m\varphi})$ will equal the sum of all $\mathrm{P}\varphi$. Thus the sum of the third and fourth rows $\equiv \Sigma\mathrm{P}\varphi$ (mod. 4), and hence the sum of all four rows $\equiv 0$ (mod. 4). Which was to be proved.

Since ε thus depends only on m and μ, independently of the choice of quarter systems, we shall call ε the character of the number m in relation to the modulus μ and denote it by Ch. m (mod. μ). It is easy to see that this only generalizes, or includes, the definition given (Art. ...) for the case in which μ is prime.

4.

I now turn to *specific* arrangements of the quarter systems, and set the modulus, to be denoted by m, $= ea + ebi$, so that the positive integer e denotes the greatest real divisor, or the greatest divisor common to the two components of m; thus a, b are relatively prime. The quarter system with the simplest arrangement will be the one whose members $x + iy$ are such that $ax + by$ is positive and less than $\frac{1}{2}e(aa + bb)$, while $ay - bx$ is nonnegative and likewise less than $\frac{1}{2}e(aa + bb)$; the latter condition is deliberately expressed so as to include the cases in which $ay - bx = 0$. It is easy to see that there will be $\frac{1}{2}(e-1)$ such cases in all, namely

$$\begin{array}{llll} x & = a, & y & = b \\ x & = 2a, & y & = 2b \\ x & = 3a, & y & = 3b \\ & \text{and so on, up to} & & \\ x & = \frac{1}{2}(e-1)a, & y & = \frac{1}{2}(e-1)b \end{array}$$

and hence none at all if the components of m have no common divisor. Let us call this quarter system k, and let k', k'', k''' be those obtained by multiplying the numbers belonging to k by $i, -1, -i$; or one may also put

$$k' = m + ik, \quad k'' = (1+i)m - k, \quad k''' = im - ik$$

This gives the following rule for deciding whether any given integer $x + iy$ not divisible by m is congruent to a member of k, k', k'' or k'''. Namely, $2(ax + by)$ can be put in the form $Pe(aa + bb) + Q$, and $2(ay - bx)$ in the form $Re(aa + bb) + S$, with P, Q, R, S real integers satisfying the following conditions:

if $x + iy$ is congruent to a number from

so that	k	k'	k''	k'''
P	even	odd	odd	even
R	even	even	odd	odd
Q	positive	positive	positive	nonnegative
$e(aa+bb) - Q$	positive	nonnegative	positive	positive
S	nonnegative	positive	positive	positive
$e(aa+bb) - S$	positive	positive	nonnegative	positive

The matter is easier to survey if the cases in which neither of the numbers $ax + by$, $ay - bx$ is divisible by $e(aa + bb)$ are distinguished from the rest.

I. In the first case, simply take for P the (algebraically) smaller of the two integers between which $\frac{2(ax+by)}{e(aa+bb)}$ lies strictly, and likewise for R the smaller of the two between which $\frac{2(ay-bx)}{e(aa+bb)}$ lies.

II. If $ax + by$ is divisible by $e(aa + bb)$, then $ay - bx$ will be divisible by $aa + bb$, but not by $e(aa + bb)$ (since otherwise $x + iy$ would be divisible by $ea + ebi$). If now R, that is, the integer immediately below $\frac{2(ay-bx)}{e(aa+bb)}$, is even, then $x + iy$ will be congruent modulo $ea + ebi$ to a number from k', but to one from k''' if R is odd.

III. If $ay + bx$ is divisible by $e(aa + bb)$, but $ax + by$ is not, then $x + iy$ will be congruent to a number from k or from k'', according as the integer algebraically immediately below $\frac{2(ax+by)}{e(aa+bb)}$ is even or odd.

5.

The following method for determining the character of a given integer $M = A + Bi$ relative to the odd modulus $m = ea + ebi$ that does not divide it is readily derived from the above.

For brevity we use the following notation. If p denotes any nonintegral real number, let $[p]$ denote the integer that makes both $p - [p]$ and $1 + [p] - p$ positive. This definition therefore excludes applying the notation to integers. If the definition required neither $p - [p]$ nor $1 + [p] - p$ to be negative, the symbol $[p]$ would be ambiguous when p is an integer. One could also, as was done in an earlier paper, require $1 + [p] - p$ to be positive and $p - [p]$ merely to be nonnegative. For our purpose it is somewhat more convenient to keep to the first definition.

Accordingly, the quarter system k consists of all integers f for which, on putting $\frac{2f}{m} = \xi + \eta i$, ξ lies strictly between 0 and 1, while η lies between 0 and 1, with 0 included; or

$$\begin{aligned} & [\xi] = 0, \quad [\eta] = 0 \\ \text{or} \quad & [\xi] = 0, \quad \eta = 0 \end{aligned}$$

If now, for every f, we put $\frac{2fM}{m} = \xi + i\eta$ and take

$\Psi f = 0$ if both $[\xi]$ even and either $[\eta]$ even or η integer
1 $[\eta]$ even and either $[\xi]$ odd or ξ integer
2 $[\xi]$ odd and either $[\eta]$ odd or η integer
3 $[\eta]$ odd and either $[\xi]$ even or ξ integer

or, in tabular form,

	$[\eta]$ even	$[\eta]$ odd	η integer
$[\xi]$ even	0	3	0
$[\xi]$ odd	1	2	2
ξ integer	1	3	− .

which may be denoted by $\nabla(\xi+i\eta)$, then the required character of the number M relative to the modulus m equals the least residue of $\Sigma\Psi f$ modulo 4.

6.

The rule given in the preceding article is general; for the case in which M is odd, however, we shall give it another form. At the same time we shall assume that the real parts of m and M are odd, and hence their imaginary parts even.

To each number f belonging to the quarter system k we assign another number g, derived from f as follows. On putting $\frac{2f}{m} = \xi + i\eta$, four cases are distinguished:

I. If $[2\xi] = 0$ and either $[2\eta] = 0$ or $\eta = 0$
II. If $[2\xi] = 1$ and either $[2\eta] = 0$ or $\eta = 0$
III. If $[2\xi] = 0$ and $[2\eta] = 1$
IV. If $[2\xi] = 1$ and $[2\eta] = 1$

In the first case put $g = 2f$, in the second $g = im - 2if$, in the third $g = m + 2if$, and in the fourth $g = (1+i)m - 2f$. It is easy to see that the collection of all g forms a complete quarter system l; its defining property is that, on putting $\frac{g}{m} = \xi + i\eta$, the following conditions hold together:

either	$[\xi] = 0,$	$[\eta] = 0$	
or	$\eta = 0,$	$[\xi] = 0$	and g divisible by $1+i$
or	$\xi = 0,$	$[\eta] = 0$	and g not divisible by $1+i$

It follows that l differs from k only in that the numbers in k for which $\eta = 0$ and which are not divisible by $1+i$, namely

$$a+bi, \quad 3(a+bi), \quad 5(a+bi) \ldots \frac{e-3}{2}(a+bi)$$
$$\text{or up to } \frac{e-1}{2}(a+bi)$$

according as e has the form $4n+1$ or $4n+3$, are absent from l, while their products by i occur in the latter collection instead. At the same time one sees that, for $e = 1$, that is, when m is divisible by no real integer, k and l are entirely the same.

It now remains to derive Ψf directly from the g corresponding to f. The result is that, for the above 4 cases,

I. $\Psi f = \nabla \frac{gM}{m}$

II. $\Psi f = \begin{cases} -\nabla \frac{gM}{m} & \text{if neither the real nor imaginary part of } \frac{gM}{m} \text{ is an integer} \\ 1 - \nabla \frac{gM}{m} & \text{if either is an integer} \end{cases}$

III. as II. IV. as I.

Remarks.

Judging by the position of the manuscripts in a notebook, the fragments designated I and II in this printed edition date from 1811 or the time immediately following. Of the preceding attempts to prove the fundamental theorem for biquadratic residues by the methods applied here to the residue $1+i$, a record survives that settles the special case of the residue $1+2i$ and starts from the determination of the biquadratic character appended as a note to Article 6 of Fragment III. The manuscripts also supplement the historical information published by Gauss in the notices of his arithmetical papers: the theorems included in Articles 15 to 20 of the *Theoria residuorum biquadrat.* were written down before the *Theoria motus corporum coel.* was worked out. The investigations of cubic residues mentioned in those notices were probably never worked up in full; what is recorded consists of proofs of the reciprocity theorems for two primes, one of them real, carried out with the methods provided by the paper *Disquisitionum circa aequationes puras ulterior evolutio.*

Fragments III to VI form separate booklets in the manuscripts. For the first three, the handwriting points to a date not far from that of Fragments I and II, while a considerably later date must be assumed for the last, No. VI.

[I.] Art. 10. The number of lattice points in $(z, z', z'+\zeta, z+\zeta)$ is determined by the theorem: if a and b are relatively prime, the straight line drawn from $\xi+\eta i$ to $\xi+\eta i+a+bi$ passes through one lattice point when the imaginary part of $(\xi+\eta i)\,.\,(-a+bi)$ is an integer.

[I.] Art. 17. The first transformation of the last S in the expression for ΔS is obtained by dividing the region in question into three parts such that this S becomes

$$\begin{aligned} &S\big(\tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i,\ (\tfrac{1}{2}+\tfrac{1}{2}i)m,\\ &\qquad (\tfrac{1}{2}+\tfrac{1}{2}i)m+i,\ \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(+)}\big)\\ &-S\big(\tfrac{1}{2}m,\ \tfrac{1}{2}m+\tfrac{1}{2}+\tfrac{1}{2}i_{(+)},\ \tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i\big)\\ &-S\big((\tfrac{1}{2}+\tfrac{1}{2}i)m,\ \tfrac{1}{2}m,\ \tfrac{1}{2}m+\tfrac{1}{2}-\tfrac{1}{2}i\big) \end{aligned}$$

then counting the lattice points in the first part by means of the theorem in Article 10, and further noting that the second part contains no lattice point.

The second transformation is obtained by multiplying the quantities corresponding to the vertices of the third part by i and increasing them by the integer $(1-i)\frac{m-1}{2}$; finally, the third is obtained by comparing the resulting figure, according to the rule of Article 16, with the figure displaced from it by $\frac{-1}{1+i}$.

[I.] Art. [18.] An explanation of the first scheme is found in Articles 1 to 6 of the fragment written later and designated here by [II.].

[I.] Art. [18.] (2.) The geometric interpretation, with the aid of the two systems of lattice points

$$[-2iQ - \tfrac{1}{2}, \tfrac{1}{2}, iQ] = [-2iQ + \tfrac{1}{2}, \tfrac{1}{2}, iQ] = \mathrm{IV}^*$$

and

$$-[-2iQ + \tfrac{1}{2}i, -\tfrac{1}{2}i, iQ] = -[-2iQ - \tfrac{1}{2}i, -\tfrac{1}{2}i, iQ] = \mathrm{X}^*$$

gives the equations

$$\begin{aligned} \mathrm{IV} - \mathrm{IV}^* + [-2iQ, \tfrac{1}{2}i, -\tfrac{1}{2}] &= -\mathrm{X} + \mathrm{X}^* + [-iQ, \tfrac{1}{2}i, -\tfrac{1}{2}] \\ \mathrm{XIII} + \mathrm{IV}^* &= [-2iQ, 1, iQ] = -I(-2iQ) + I(-iQ) \\ \mathrm{V} + \mathrm{X}^* &= -[-2iQ, -i, iQ] = R(-2iQ) - R(-iQ) \end{aligned}$$

where, in general, Rx and Ix denote the greatest integers contained in the real part and in the coefficient of the imaginary part of x, respectively.

But $[-2iQ, \frac{1}{2}i, -\frac{1}{2}]$ is the number of lattice points in the square whose centre is at $-2iQ - \frac{1}{4} + \frac{1}{4}i$ and whose endpoints have the displacements $\frac{1}{2}$ and $\frac{1}{2}i$ between them.

$[-iQ, \frac{1}{2}i, -\frac{1}{2}]$ or $[-2iQ, -\frac{1}{2}i, \frac{1}{2}]$ is the number of lattice points in an equal square with centre $-2iQ + \frac{1}{4} - \frac{1}{4}i$.

[I.] Art. [18.] (3.) With the aid of the lattice points $[0, \frac{1}{2}i, -iQ] = -[-\frac{1}{2}i, -\frac{1}{2}i, -iQ] = \mathrm{I}^*$ one obtains

$$\begin{aligned} \mathrm{VII} - \mathrm{XII} &= \mathrm{I} - \mathrm{I}^* + [-iQ, \tfrac{1}{2}, \tfrac{1}{2}i] - [0, \tfrac{1}{2}, \tfrac{1}{2}i] \\ &= \mathrm{I} - \mathrm{I}^* + [-2iQ, \tfrac{1}{2}, \tfrac{1}{2}i] \\ \mathrm{II} - \mathrm{I}^* &= [0, -i, -iQ] = -R0 + R(-iQ) \\ \mathrm{IX} - \mathrm{I} &= [0, -1, -iQ] = I0 - I(-iQ) \\ \mathrm{VI} - \mathrm{XII} &= -[\tfrac{1}{2}i, -1, -iQ] = -I(\tfrac{1}{2}i) + I(-iQ + \tfrac{1}{2}i) \\ \mathrm{VIII} - \mathrm{XIV} &= -[\tfrac{1}{2}, -1 - i, \tfrac{1}{2}im_{(-)}] = \frac{a-1}{2} + \frac{b}{2} \end{aligned}$$

[II.] Art. 10. We have

$$\begin{aligned} \Upsilon P' &\equiv -\Upsilon(-iP' + \tfrac{1}{2}im), \\ \Upsilon P'' &\equiv -1 - \Upsilon(P'' - \tfrac{1}{2}im), \\ \Upsilon P''' &\equiv 1 + \Upsilon(-iP''') \pmod 4 \end{aligned}$$

and $-iP' + \frac{1}{2}im$, $P'' - \frac{1}{2}im$ are the lattice points in I and VI, respectively, increased by $\frac{1}{2}i$.

[III.] Art. 6. I have added to the present paper the rules given in the note for determining $\mathrm{Dec.}\frac{M}{m}$, taking them from another place in the manuscripts.

The first of these two rules, which, as is easy to see, agrees with the second, follows from that of Article 6, because

$$k \equiv f \,.\, i^{-n} \text{ (mod. } m), \quad n = \Theta\frac{2fM}{m}, \quad p = mm',$$
$$\left[\frac{2km'}{p}\right]^2 \equiv \Theta\frac{2km'}{p} \text{ (mod. } 2+2i)$$

holds.

[III.] Art. 8 contains in the manuscript an example for Article 7, namely the determination of the decident of $-1+2i$ for the modulus $-11+4i$.

[III.] Art. 10. For the remark 'to be expressed differently', compare Article 3 of the following fragment [IV].

[IV.] Articles 1. 2. 4 contain in the manuscript, besides what is printed here, the application to the two examples for $m = 5+8i$, $M = 9+4i$ and for $m = 9+4i$, $M = 5+8i$. [V.] Art. [7.] Here, as in Article 1 of the preceding fragment [IV], Dec.$\frac{m}{M}$ denotes the value of

$$\Sigma(-1)^X \Sigma(-1)^Y \text{Int.}\, p$$

where the summation extends over all integers X and Y for which the corresponding ξ and η lie within the bounds 0 and $\frac{1}{2}$.

The text states that the formulas for the decident in Articles 7 and 15 were found in two distinct ways. To keep these explanations from becoming too long, however, they are derived here from a common source.

For any fixed integer value of X, let Y^* be the smaller and Y^{**} the larger of the two values of Y corresponding to the boundary values of ξ, η. Let the values of p corresponding to Y^* and Y^{**} be p^* and p^{**}. Like Y^* and Y^{**}, they cannot be equal to one another, since the sum Σ does not extend over the boundary values of ξ and η.

Sum over all values of Y occurring for the same X, in the same way as in the preceding two papers [III] and [IV]. Put $[\frac{1}{2}Y'' - \frac{1}{2}] - [\frac{1}{2}Y' - \frac{1}{2}]$ for the number of odd integers between Y' and Y'', and add the intensors referring to the bounds $\xi = 0$ and $= \frac{1}{2}$ twice, with opposite signs. This gives for $\Sigma(-1)^Y \text{Int.}\, p$ the expression consisting of seven parts

$$-\Sigma[-\text{Int.}(p - \mu\omega i) + \text{Int.}(p + \mu\omega i)]$$
taking all p for which $[Y]$ even,
x or y integer, incl. $\xi = 0$ and $\frac{1}{2}$, excl. $\eta = 0$ and $\frac{1}{2}$

$$\left.\begin{array}{l} -\text{Int.}(p^* - \mu\omega i) \text{ if } [Y^*] \text{ even} \\ +\text{Int.}(p^{**} + \mu\omega i) \text{ if } [Y^{**}] \text{ even} \end{array}\right\} \; \xi = 0 \text{ or } \tfrac{1}{2}, \quad 0 < \eta < \tfrac{1}{2}$$

$$\left.\begin{array}{l} -\text{Int.}(p^* + \mu\omega i) \text{ if } [Y^*] \text{ even} \\ +\text{Int.}(p^{**} - \mu\omega i) \text{ if } [Y^{**}] \text{ even} \end{array}\right\} \; 0 < \xi < \tfrac{1}{2}, \quad \eta = 0 \text{ or } \tfrac{1}{2}$$

$$\left.\begin{array}{l} -\text{Int.}(p^* + \mu\omega i) \text{ if } [Y^*] \text{ even} \\ +\text{Int.}(p^{**} - \mu\omega i) \text{ if } [Y^{**} - \omega] \text{ even} \end{array}\right\} \; \xi = 0 \text{ or } \tfrac{1}{2}, \quad \eta = 0 \text{ or } \tfrac{1}{2}$$

which, multiplied by $(-1)^X$ and summed over all integer values of X, gives the decident $\frac{m}{M}$.

In this way, the first part of the expression gives, from the ε formed according to Article 2, Rule I,

$$\begin{array}{c} \Sigma\varepsilon \text{ where } X \text{ integer, } [Y] \text{ even} \\ -\Sigma\varepsilon \text{ where also } y \text{ integer, } [x] \text{ even} \end{array}$$

For the following parts one may put

$$\left.\begin{array}{l} -(B)\text{Int.}(p - B\mu\omega i) \text{ if } \xi = 0 \\ +(B)\text{Int.}(p + B\mu\omega i) \text{ if } \xi = \frac{1}{2} \end{array}\right\} \; X \text{ integer, } [Y] \text{ even, } 0 < \eta < \tfrac{1}{2}$$

$$\left.\begin{array}{l} -(A)\text{Int.}(p + A\mu\omega i) \text{ if } \eta = 0 \\ +(A)\text{Int.}(p - A\mu\omega i) \text{ if } \eta = \frac{1}{2} \end{array}\right\} \; X \text{ integer, } [Y] \text{ even, } 0 < \xi < \tfrac{1}{2}$$

$$\begin{array}{c} -\frac{1}{2}[(A') + (B')]\text{Int.}(p + A'\mu\omega i) \\ \text{if } X \text{ integer, } [Y + A'\omega] \text{ even, } \xi \text{ and } \eta = 0 \text{ or } \frac{1}{2} \end{array}$$

where $A' = +A$ or $-A$ when $\eta = 0$ or $\frac{1}{2}$, and $B' = +B$ or $-B$ when $\xi = 0$ or $\frac{1}{2}$; here, for example, the notation $(A) : +1$ or -1 is used according as A is positive or negative.

Multiply by $(-1)^X$ and sum over X, making the following substitutions in these expressions, namely in the

$$\begin{array}{rl} \text{first} & p - B\mu\omega i,\ P - BD\omega i,\ \pi - AB\omega i - BB\omega,\ X,\ [Y] \\ & \text{respectively into } ip,\ iP,\ i\pi,\ -Y,\ [X] \\ \text{second} & p + B\mu\omega i,\ P + BD\omega i,\ \pi + AB\omega i + BB\omega,\ X,\ [Y] \\ & \ldots \quad p,\ P,\ \pi \quad X,\ [Y] \\ \text{third} & p + A\mu\omega i,\ P + AD\omega i,\ \pi + AA\omega i + AB\omega,\ X,\ [Y] \\ & \ldots \quad p,\ P,\ \pi \quad X,\ [Y] \\ \text{fourth} & p - A\mu\omega i,\ P - AD\omega i,\ \pi - AA\omega i - AB\omega,\ X,\ [Y] \\ & \ldots \text{ into } im - ip,\ iM - iP,\ i - i\pi,\ Y - B,\ A - 1 - [X] \end{array}$$

and denote the result from the fifth expression by Q_1. One then obtains

$$
\begin{aligned}
&- \Sigma(-1)^{Y}(B)\text{Int.}\, ip, \\
&\qquad \text{where } Y \text{ integer, } [X] \text{ even, } \eta = \omega,\ 0 < \xi < \tfrac{1}{2} \\
&+ \Sigma(-1)^{X}(B)\text{Int.}\, p, \\
&\qquad \text{where } X \text{ integer, } [Y] \text{ even, } \xi = \tfrac{1}{2} + \omega,\ 0 < \eta < \tfrac{1}{2} \\
&- \Sigma(-1)^{X}(A)\text{Int.}\, p, \\
&\qquad \text{where } X \text{ integer, } [Y] \text{ even, } \eta = \omega,\ 0 < \xi < \tfrac{1}{2} \\
&+ \Sigma(-1)^{Y}(A)\text{Int.}(im - ip), \\
&\qquad \text{where } Y \text{ integer, } [X] \text{ even, } \xi = \tfrac{1}{2} + \omega,\ 0 < \eta < \tfrac{1}{2} \\
&+ Q_1
\end{aligned}
$$

Examining the individual cases shows that, under the assumption $M \equiv 1 \pmod{2 + 2i}$,

$$
\begin{aligned}
Q_1 = \ & - \text{Int.}\, \mu\omega i \text{ if } M \text{ in quadrant 1} \\
& - \text{Int.}(\tfrac{1}{2}mi + \mu\omega i), \quad \text{if } M \text{ in quadrant 2 and } \frac{M-1}{2} \text{ even} \\
& + \text{Int.}(\tfrac{1}{2}mi - \mu\omega i), \quad \text{if } M \text{ in quadrant 4 and } \frac{M-1}{2} \text{ even}
\end{aligned}
$$

where a complex number is called even or odd according as it is divisible by 2 or not.

Thus, using the ε specified in Rules II and IV, one obtains

$$
\begin{aligned}
\text{Dec.}\frac{m}{M} = \text{I}, \quad & \Sigma\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ even} \\
& - 4\Sigma\varepsilon, \text{ where also } y \text{ integer, } [x] \text{ even} \\
\text{II}, \quad & - \Sigma\varepsilon\text{Int.}\, ip, \text{ where } Y \text{ integer, } [X] \text{ even} \\
\text{IV}, \quad & + \Sigma\varepsilon\text{Int.}\, p, \text{ where } X \text{ integer, } [Y] \text{ even} \\
\text{II}, \quad & + \Sigma\varepsilon\text{Int.}\, p, \text{ where } X \text{ integer, } [Y] \text{ even} \\
\text{IV}, \quad & + \Sigma\varepsilon\text{Int.}(im - ip), \text{ where } Y \text{ integer, } [X] \text{ even} \\
& + Q_1
\end{aligned}
$$

The expression for the decident takes another form if one first sums over X, expressing the number of odd integers between X' and X'' by $[\frac{1}{2}X''+\frac{1}{2}]-[\frac{1}{2}X'+\frac{1}{2}]$, namely

$$\begin{aligned}\text{Dec.}\frac{m}{M} = \text{I}, \quad & \Sigma\varepsilon, \text{ where } Y \text{ integer, } [X] \text{ odd}\\ & -4\Sigma\varepsilon, \text{ where also } y \text{ integer, } [x] \text{ even}\\ \text{II}, \quad & -\Sigma\varepsilon\text{Int.}\, ip, \text{ where } X \text{ integer, } [Y] \text{ even}\\ \text{IV}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ where } Y \text{ integer, } [X] \text{ odd}\\ \text{II}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ where } Y \text{ integer, } [X] \text{ odd}\\ \text{IV}, \quad & +\Sigma\varepsilon\text{Int.}(im-ip), \text{ where } X \text{ integer, } [Y] \text{ odd}\\ & +Q_2\end{aligned}$$

$$\begin{aligned}Q_2 = & -\text{Int.}(-\mu\omega), \quad \text{if } M \text{ in quadrant 2}\\ & +\text{Int.}(\tfrac{1}{2}m-\mu\omega), \quad \text{if } M \text{ in quadrant 1 and } \frac{M-1}{2} \text{ odd}\\ & -\text{Int.}(\tfrac{1}{2}m+\mu\omega), \quad \text{if } M \text{ in quadrant 3 and } \frac{M-1}{2} \text{ odd}\end{aligned}$$

If one sums over Y first, but uses the second method just applied for determining the number of odd integers between two values, one obtains

$$\begin{aligned}\text{Dec.}\frac{m}{M} = \text{I}, \quad & \Sigma\varepsilon, \text{ where } X \text{ integer, } [Y] \text{ odd}\\ & -4\Sigma\varepsilon, \text{ where also } y \text{ integer, } [x] \text{ even}\\ \text{II}, \quad & -\Sigma\varepsilon\text{Int.}\, ip, \text{ where } Y \text{ integer, } [X] \text{ odd}\\ \text{IV}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ where } X \text{ integer, } [Y] \text{ odd}\\ \text{II}, \quad & +\Sigma\varepsilon\text{Int.}\, p, \text{ where } X \text{ integer, } [Y] \text{ odd}\\ \text{IV}, \quad & +\Sigma\varepsilon\text{Int.}(im-ip), \text{ where } Y \text{ integer, } [X] \text{ odd}\\ & +Q_3\end{aligned}$$

$$\begin{aligned}Q_3 = & -\text{Int.}(-\mu\omega i), \quad \text{if } M \text{ in quadrant 3}\\ & -\text{Int.}(\tfrac{1}{2}mi+\mu\omega i), \quad \text{if } M \text{ in quadrant 2 and } \frac{M-1}{2} \text{ odd}\\ & +\text{Int.}(\tfrac{1}{2}mi-\mu\omega i), \quad \text{if } M \text{ in quadrant 4 and } \frac{M-1}{2} \text{ odd}\end{aligned}$$

If one also sums over X first and uses the first method for expressing the number of odd integers between two values, one obtains the form for the

decident given in [V], Article 15, where the quantity q can also be defined by the following equation:

$$\begin{aligned} q = & -\text{Int.}\,\mu\omega, \quad \text{if } M \text{ in quadrant 4} \\ & +\text{Int.}(\tfrac{1}{2}m - \mu\omega), \quad \text{if } M \text{ in quadrant 1 and } \frac{M-1}{2} \text{ even} \\ & -\text{Int.}(\tfrac{1}{2}m + \mu\omega), \quad \text{if } M \text{ in quadrant 3 and } \frac{M-1}{2} \text{ even} \end{aligned}$$

Combining these four expressions for the decident gives the result stated in [V], Article 7, since $\text{Int.}\,ip - \text{Int.}\,p$ equals 3 when $[x]$ is even and $[y]$ odd, and otherwise equals 1; furthermore, $\text{Int.}(im - ip) + \text{Int.}\,p$ equals 0 when $[x]$ and $[y]$ are even, and equals 4 in all other cases.

[V.] Art. [7.] In the first column, the first table for the example gives the values of $\frac{37.P}{M}$ or $37(\xi + \eta i)$ corresponding to each integer P, when $0 < \xi < \frac{1}{2}$, $0 < \eta < \frac{1}{2}$; in the second, $\frac{37.Pm}{M}$ or $37\,.\,p$; in the third, the greatest integer contained in p; and in the fourth, $\pm\text{Int.}\,p$, where the upper sign applies when P is divisible by $1 + i$, and the lower when P is not divisible by $1 + i$.

[V.] Art. [9.]. [12.] The improved notation for the θ is indicated only for the second and third classes, Articles 9. 10, but is also to be extended to the first and fourth, Articles 8. 11. Accordingly, a $\theta^\lambda = T + Ui$ has the index $\lambda, = 0, 1, 2$ or 3 for which the quantities φ^0 and Φ^0, determined by the equations

$$\begin{aligned} & i^\lambda M = \mathfrak{A} + \mathfrak{B}i, \quad i^{-\lambda}\mu = \rho + \sigma i \\ & \sigma\varphi^0 = -\text{Coeff. Imag. } \theta^\lambda(a - bi) = +bT - aU \\ & \sigma\Phi^0 = +\text{Coeff. Imag. } \theta^\lambda(\mathfrak{A} - \mathfrak{B}i) = -\mathfrak{B}T + \mathfrak{A}U \end{aligned}$$

lie between 0 and $\frac{1}{2}$.

To prove, following the indications in Article 9 (3), that if T, U are two real integers satisfying the conditions just stated, then $T + Ui$ also belongs to the collection θ^λ determined in one of the four combinations, Articles 8. 11, let φ', Φ' denote the complex integers for which the equation

$$T + Ui = \varphi' i^\lambda M + \Phi' m$$

holds, and for which one of the four quantities $\pm\frac{\varphi' - \varphi^0}{m}$, $\pm i\frac{\varphi' - \varphi^0}{m}$ has its real part and the coefficient of its imaginary part between 0 and $\frac{1}{2}$ (*Theoria residuorum biquadr. artt.* 45, 46). As is readily seen by examining the sixteen individual cases in the four combinations, the quantity in question is then $\frac{p}{m}$, and the corresponding quantity among $\pm\frac{\Phi' - \Phi^0}{m}$, $\pm i\frac{\Phi' - \Phi^0}{M}$ is $\frac{P}{M}$, since $\frac{\Phi' - \Phi^0}{M} = -\frac{\varphi' - \varphi^0}{m} i^\lambda$.

This way of representing the quantities $\frac{p}{m}$ or $\frac{P}{M}$ also shows that the sum I, $\Sigma\varepsilon$, over all, equals $\Theta + \Theta' + \Theta'' + \Theta'''$, where Θ^λ denotes the sum of

the ε which, for each lattice point θ inside the parallelogram $0,\ \frac{1}{2}m,\ \frac{1}{2}m + \frac{1}{2}i^\lambda M,\ \frac{1}{2}i^\lambda M$, are to be put

$= +1$ if θ is divisible by $1+i$ and Coeff. Imag. $\mu i^{-\lambda}$ is positive, or if neither condition holds; but

$= -1$ if only one holds.

[V.] Art. 13. The quantity Θ^λ can be determined either by the four different ways of summing used above for Dec.$\frac{m}{M}$, or, what is essentially the same, by the methods indicated in [II], Article 11. These are to be based on the four constructions obtained by joining the points whose θ is a multiple of $1+i$ to the points $\theta+1$, $\theta+i$, $\theta-1$ and $\theta-i$, respectively.

On the boundary of the parallelogram just mentioned, let a θ correspond to every point for which the real or imaginary part of θ is an integer. Denote by θ^0 the nearest integer divisible by $1+i$ to θ, and by l the displacement from a point on the straight boundary segment containing θ to any following point on the same straight line; thus, for example, for this parallelogram, the quantities $m,\ Mi^\lambda,\ -m,\ -Mi^\lambda$, in order. If one puts

$$\varepsilon = \pm 1 \text{ with the sign of the imaginary part of } \frac{l}{\theta - \theta^0}$$

then combining the four results obtained in either way gives $4\Theta^\lambda = -\Sigma\varepsilon$.

One avoids determining the θ and ε at the vertices separately by replacing this parallelogram with another whose boundaries are infinitely near those of the former and which does not include the two points 0 and $\frac{1}{2}m + \frac{1}{2}i^\lambda M$. The boundary of such a parallelogram is obtained by placing it on the positive sides of the lines

$$0 \ldots . \tfrac{1}{2}m, \quad \tfrac{1}{2}m + \tfrac{1}{2}i^\lambda M \ldots . \tfrac{1}{2}m,$$
$$\tfrac{1}{2}m + \tfrac{1}{2}i^\lambda M \ldots . \tfrac{1}{2}i^\lambda M, \quad 0 \ldots . \tfrac{1}{2}i^\lambda M$$

Assign the infinitely small positive quantities $\omega_1, \omega_2, \omega_3, \omega_4$ to the four resulting straight lines, in order. For the points θ on them one may then put

$$\begin{aligned}
\theta = p &= m(\xi + \omega_1 i),\\
-\theta i^\lambda + \tfrac{1}{2}mi^\lambda + \tfrac{1}{2}M = P &= M(\xi + \omega_2 i),\\
-\theta + \tfrac{1}{2}m + \tfrac{1}{2}Mi^\lambda = p &= m(\xi + \omega_3 i),\\
\theta i^{-\lambda} = P &= M(\xi + \omega_4 i) \quad \text{if } \lambda \text{ even}
\end{aligned}$$

$$\begin{aligned}
\theta = p &= m(\xi + \omega_1 i),\\
\theta i^{1-\lambda} - \tfrac{1}{2}mi^{1-\lambda} + \tfrac{1}{2}M = P &= M(\tfrac{1}{2} + \omega_2 + \eta i),\\
\theta i + \tfrac{1}{2}m - \tfrac{1}{2}Mi^{1+\lambda} = p &= m(\tfrac{1}{2} + \omega_3 + \eta i),\\
\theta i^{-\lambda} = P &= M(\xi + \omega_4 i) \quad \text{if } \lambda \text{ odd}
\end{aligned}$$

where, in part, ξ and η also extend beyond the range of real values from 0 to $\frac{1}{2}$ by infinitely small quantities, to close the figure.

Let G, g, H, h denote the sums of the ε formed according to Rules II, III, IV, V, respectively (in Articles 3 to 6). Let G' or $G_{\prime}$, and g' or $g_{\prime}$, include the ε arising for the infinitely small values of ξ that may occur in the second parallelogram, but otherwise formed according to Rules II and III, respectively. Further, let G'' or $G_{\prime\prime}$, and g'' or $g_{\prime\prime}$, similarly refer to the same rules, but to the infinitely small values of $\frac{1}{2} - \xi$; and finally let $H', h_{\prime}, H'', h_{\prime\prime}$ refer to Rules IV, V, IV, V and the infinitely small values $\frac{1}{2} - \eta, \frac{1}{2} - \eta, \eta, \eta$, respectively. Then

$$\begin{aligned} 4\Theta^{\lambda} = & -(g + g' + g'') - i^{\lambda}(G + G' + G'') \\ & + i^{\lambda}(g + g_{\prime} + g_{\prime\prime}) + (G + G_{\prime} + G_{\prime\prime}) \quad \text{if } \lambda \text{ even} \\ 4\Theta^{\lambda} = & -(g + g' + g'') - i^{1-\lambda}(H + H' + H'') \\ & - i^{\lambda-1}(h + h_{\prime} + h_{\prime\prime}) + (G + G_{\prime} + G_{\prime\prime}) \quad \text{if } \lambda \text{ odd} \end{aligned}$$

For the vertex θ of the parallelogram nearest to 0, let ξ_1 denote the corresponding value of the ξ of the first side, and ξ_4 the corresponding value of the ξ of the fourth side, so that

$$\theta = m(\xi_1 + \omega_1 i) = i^{\lambda} M(\xi_4 + \omega_4 i)$$

Then the ξ corresponding to a point p on the first side or its extension with real part equal to 0 is given by

$$(\text{Real. } p = 0), \quad \xi - \xi_1 = \sigma a \mathfrak{A} \omega_1 - \sigma \omega_4$$

where the positive factors of the infinitely small positive quantities have been replaced by unity, and σ, $\mathfrak{A}$ denote the real quantities determined by

$$\rho + \sigma i = i^{-\lambda}(\alpha + \beta i), \quad \mathfrak{A} + \mathfrak{B} i = i^{\lambda}(A + Bi)$$

This point p lies on the first side itself if $\xi - \xi_1$ is positive; hence, taking ω_1 infinitely small compared with ω_4, if σ is negative. The point p^0 nearest to p whose representing number is divisible by $1 + i$ is 0; thus $\text{Imag.}\frac{m}{p - p^0}$ or $\text{Imag.}\frac{1}{\xi + \omega_1 i}$ has the minus sign. Therefore, for $\text{Real. } p = 0$, one obtains

$$\varepsilon = -1 \text{ if } (\sigma) = -1, \quad \varepsilon = 0 \text{ if } (\sigma) = +1, \quad \text{i.e. } \varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}(\sigma)$$

and in the same way, for $\text{Imag. } p = 0$,

$$\xi - \xi_1 = \sigma b \mathfrak{B} \omega_1 - \sigma \omega_4, \quad \text{Imag.}\frac{m}{p - p^0} = \text{Imag.}\frac{1}{\xi + \omega_1 i},$$
$$\varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}(\sigma) \quad \text{thus } g' = -1 + (\sigma)$$

For the fourth side, $P^0 = 0$, $\text{Imag.}\frac{M}{P-P^0} = \text{Imag.}\frac{1}{\xi+\omega_4 i}$,

$$\begin{aligned} \text{thus for Real.}(i^\lambda P) = 0; \quad & \xi - \xi_4 = -\sigma a\mathfrak{A}\omega_4 + \sigma\omega_1, \\ & \varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}(\sigma a\mathfrak{A}) \\ \text{and for Imag.}(i^\lambda P) = 0; \quad & \xi - \xi_4 = -\sigma b\mathfrak{B}\omega_4 + \sigma\omega_1, \\ & \varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}(\sigma b\mathfrak{B}) \end{aligned}$$

and consequently $G_{\prime} = -1 + \frac{1}{2}(\sigma a\mathfrak{A}) + \frac{1}{2}(\sigma b\mathfrak{B})$, or, since $\rho = a\mathfrak{A} + b\mathfrak{B}$, $G_{\prime} = -1 + \frac{1}{2}(\rho\sigma) + \frac{1}{2}(\rho\sigma ab\mathfrak{A}\mathfrak{B})$.

The part R_1^λ of $4\Theta^\lambda$ arising from the portion of the boundary infinitely near 0 is therefore

$$R_1^\lambda = +G_{\prime} - g' = -(\sigma) + \tfrac{1}{2}(\rho\sigma) + \tfrac{1}{2}(\rho\sigma ab\mathfrak{A}\mathfrak{B})$$

Similar considerations give, for the parts R_2^λ, R_3^λ, R_4^λ, which have the same relations to the points $\frac{1}{2}m$, $\frac{1}{2}m + \frac{1}{2}Mi^\lambda$, $\frac{1}{2}Mi^\lambda$, respectively, as R_1^λ has to 0, when λ is even,

$$\begin{aligned} R_2^\lambda &= -g'' - i^\lambda G'' = -\tfrac{1}{2}(b) - \tfrac{1}{2}(\mathfrak{B}), \\ R_3^\lambda &= -i^\lambda G' + i^\lambda g_{\prime} = i^\lambda(\sigma) - \tfrac{1}{2}i^\lambda(\rho\sigma) - \tfrac{1}{2}i^\lambda(\rho\sigma ab\mathfrak{A}\mathfrak{B}) \\ R_4^\lambda &= +i^\lambda g_{\prime\prime} + G_{\prime\prime} = \tfrac{1}{2}i^\lambda(b) + \tfrac{1}{2}i^\lambda(\mathfrak{B}) \end{aligned}$$

and when λ is odd,

$$\begin{aligned} R_2^\lambda &= -g'' - i^{1-\lambda}H'' = -\tfrac{1}{2}(b) - \tfrac{1}{2}(\mathfrak{B}), \\ R_3^\lambda &= -i^{1-\lambda}H' - i^{\lambda-1}h_{\prime} = 0, \\ R_4^\lambda &= -i^{\lambda-1}h_{\prime\prime} + G_{\prime\prime} = \tfrac{1}{2}i^{\lambda+1}(a) + \tfrac{1}{2}i^{\lambda+1}(\mathfrak{A}) \end{aligned}$$

[V.] Art. [14.] The sums of the ε formed according to Rule III are evaluated by means of the equation

$$\begin{aligned} &\text{III,} \quad \Sigma\varepsilon \text{ from all } -4\Sigma\varepsilon \text{ from those where } y \text{ integer, } [x] \text{ even} \\ &= \text{III,} \quad \Sigma[-\text{Int.}(p - m\omega) + \text{Int.}(p + m\omega)] \end{aligned}$$

which is readily verified from the definition of the ε. Here p takes all values satisfying the conditions stated under Rule III. Except for the two intensors corresponding to the smallest (ξ^*) and the greatest admissible value (ξ^{**}) of ξ, respectively, which equal

$$\begin{gathered} -\text{Int.}(p^* - m\omega) \text{ and } +\text{Int.}(p^{**} + m\omega) \text{ or} \\ -\text{Int.}(\omega m) \text{ and } +\text{Int.}(\tfrac{1}{2} - \omega)m \end{gathered}$$

these intensors can always be paired as $+\text{Int.}(p' + m\omega)$ and $-\text{Int.}(p'' - m\omega)$, so that between ξ' and ξ'', corresponding to p' and p'', there is no value of

ξ making the real or imaginary part of p an integer. Thus the two intensors always cancel one another.

[V.] Art. [15.] We have

$$\begin{aligned}
\text{II}, \quad & + \Sigma\varepsilon \text{Int.}\, ip \text{ where } Y \text{ integer } [X] \text{ even}, \\
& - \Sigma\varepsilon \text{Int.}\, ip \text{ where } X \text{ integer } [Y] \text{ odd} \\
= \Sigma[& -\text{Int.}\, i(p - m\omega) + \text{Int.}\, i(p + m\omega)] \\
& \text{for those } p, \text{ for which } x \text{ or } y \text{ integer, } [X] \text{ even} \\
& Y \text{ odd, } 0 < \xi < \tfrac{1}{2}, \quad \eta = \omega \\
& + \text{Int.}\, i(p^* - m\omega) \text{ if } [X^*] \text{ even } [Y^*] \text{ odd} \\
& - \text{Int.}\, i(p^{**} + m\omega) \text{ if } [X^{**}] \text{ even } [Y^{**}] \text{ odd}
\end{aligned}$$

as one readily verifies by performing the summation on the second side of the equation, by the method used in the preceding note, over each interval from $\xi_\prime$ to $\xi_{\prime\prime}$ so small that between $\xi_\prime$ and $\xi_{\prime\prime}$ there is no ξ making the real or imaginary part of the corresponding P an integer. Using the ε formed according to Rule III gives the second side of this equation the form stated in Article 15.

[V.] Art. [15.] The sums of the $\lambda'\varepsilon$ formed according to Rule IV are transformed into the sums of the ε from V by considerations of the same kind as in the last note, also using the equation

$$\begin{aligned}
\text{V}, \quad & \Sigma\varepsilon \text{ from all}, \ -4\Sigma\varepsilon \text{ where } x \text{ integer } [y] \text{ even}, \\
= & +\text{Int.}(\tfrac{1}{2}im + m\omega) - \text{Int.}(\tfrac{1}{2}im + \tfrac{1}{2} - \omega m)
\end{aligned}$$

which corresponds to the preceding evaluation of the sum of the ε in Rule III.

[V.] Art. [17.] Define the auxiliary quantities U, T, L, V by the equations

$$\begin{aligned}
U &= 1 - 2(B) - (AB) + (\alpha a) + (\beta b) + (\alpha b) - (\beta a) \\
&\quad + (\alpha\beta ab) - (\alpha\beta abAB) \quad \text{or} \\
U &= (1 + (A))(1 - (B))(1 - (a\beta) + (b\beta) + (\alpha\beta))
\end{aligned}$$

$$\begin{gathered}
\text{since } (\alpha a) + (\beta b) = (A) + (A\alpha\beta ab), \\
(\alpha b) - (\beta a) = (B) - (B\alpha\beta ab),
\end{gathered}$$

$$\begin{aligned}
T &= -2 + (a) + (b) - (\beta) - 2(B) - (\alpha ab) \quad \text{or} \\
T &= -2 + (a) + (b) - (\beta) - 2(B) - (aA) + (bB) - (\beta AB) \\
L &= (1 + (A))(1 + (B))(1 + (\beta)) - (1 - (A))(1 - (B))(1 - (\beta)) \\
V &= (1 + (A))(1 - (B))(-2(a) + 2(\beta) + (ab) + (\alpha\beta)) \quad \text{or} \\
V &= (1 + (A))(1 - (B))(-(a) + (b) + (\beta) + (ab) - (\beta ab) + (\alpha\beta))
\end{aligned}$$

$$\text{since } (a) + (b) = (\beta) + (\beta ab) \text{ if } A \text{ positive } B \text{ negative}$$

and denote by W', S', Q' the quantities into which W, S, Q in the expression for Dec.$\frac{m}{M}$ in Article 14 pass when m and M, and hence $\alpha+\beta i$ and $\alpha-\beta i$, are interchanged. Then

$$\begin{aligned}
2W' &= -5(B)-(AB) \quad \text{if } \frac{M-1}{2} \text{ even}\\
2W' &= -(B)-(AB) \quad \text{if } \frac{M-1}{2} \text{ odd}\\
2S' &= -(\alpha\beta abAB)-(\beta)-(B)+(b)\\
2Q'+2S'+2W' &= 2T+U \quad \text{if } \frac{M-1}{2} \text{ even}\\
2Q'+2S'+2W' &= -4+4(a)+U \quad \text{if } \frac{M-1}{2} \text{ odd}\\
8\psi &= 8(q+r+s+w)-(2Q'+2S'+2W')
\end{aligned}$$

If one replaces $8(q+r+s+w)$ here by its value stated in Article 15, but writes it in the form

$$\begin{array}{llll}
2T+4L+V & \text{if } \frac{M-1}{2} \text{ even} & \frac{m-1}{2} \text{ even}\\
2T-16+16(A)+V & \text{if } \frac{M-1}{2} \text{ even} & \frac{m-1}{2} \text{ odd}\\
-4+4(a)+V & \text{if } \frac{M-1}{2} \text{ odd} & \frac{m-1}{2} \text{ even}\\
-20+4(a)+V & \text{if } \frac{M-1}{2} \text{ odd} & \frac{m-1}{2} \text{ odd}
\end{array}$$

and notes that

$$V-U=-\tfrac{1}{2}(1+(a))(1+(A))(1+(\alpha))(1-(b))(1-(B))(1-(\beta))$$

holds, one obtains for ψ the method of determination given in Article 17.

[VI.] Art. 3. The incomplete reference may be taken to refer to Article 4 of Fragment III.

Schering.

ON THE THEORY OF COMPLEX NUMBERS.

[I.]

NEW THEORY OF THE DECOMPOSITION OF CUBES.

I. We assume that the equation $x^3 + y^3 + z^3 = 0$ has a solution, namely $x = a,\ y = b,\ z = c$, where a, b, c have no common divisor and are therefore also pairwise coprime. We set

$$\begin{aligned} b + c &= \alpha \\ c + a &= \beta \\ a + b &= \gamma \end{aligned}$$

where α, β, γ must also be pairwise coprime. For if α and β had a common divisor, it would also divide a^3 and b^3, so a and b would have to have a common divisor too.

We now have

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = 0$$

but the identity

$$\begin{aligned} &(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 \\ &= (\alpha + \beta + \gamma)^3 - 24\alpha\beta\gamma \end{aligned}$$

holds. Consequently,

$$(\alpha + \beta + \gamma)^3 = 24\alpha\beta\gamma$$

If α, β, γ are real numbers, then $\alpha + \beta + \gamma$ will be divisible by 3, hence $\alpha+\beta+\gamma)^3$ by 27, and therefore $\alpha\beta\gamma$ by 9. Thus one of the numbers α, β, γ, for example γ, must be divisible by 9, and so must c^3; consequently c is divisible by 3.

If, however, α, β, γ are imaginary numbers, we conclude that $\alpha + \beta + \gamma$ must be divisible by $1 - \varepsilon$, hence $24\alpha\beta\gamma$ by $(1 - \varepsilon)^3$, and therefore $\alpha\beta\gamma$ by $1 - \varepsilon$. Thus one of the numbers α, β, γ is divisible by $1 - \varepsilon$, and consequently so is one of the numbers a, b, c.

II. In general, we have the identity

$$\begin{aligned} &(p + q + r)^3 + (p + q\varepsilon + r\varepsilon\varepsilon)^8 + (p + q\varepsilon\varepsilon + r\varepsilon)^3 \\ &= 27pqr + 3(p + q + r)(p + q\varepsilon + r\varepsilon\varepsilon)(p + q\varepsilon\varepsilon + r\varepsilon) \end{aligned}$$

Consequently, if $p+q+r=0$, then

$$(p+q\varepsilon+r\varepsilon\varepsilon)^3+(p+q\varepsilon\varepsilon+r\varepsilon)^3-27pqr=0$$

If p,q,r, are themselves cubes, namely $=a^3,b^3,c^3$ respectively, that is, if the equation $x^3+y^3+z^3=0$ has a solution, then, on setting

$$\begin{aligned} a^3+b^3\varepsilon+c^3\varepsilon\varepsilon &= a' \\ a^3+b^3\varepsilon\varepsilon+c^3\varepsilon &= b' \\ -3abc &= c' \end{aligned}$$

we also have $a'^3+b'^3+c'^3=0$. From this new solution a third can be derived in the same way, and so on. It is easy to see that if the first solution consists of real numbers, the third will too.

It should also be noted that if a,b,c have no common factor, the same will hold for a',b',c', apart from the factor $1-\varepsilon$. For

$$\begin{aligned} \frac{a'}{1-\varepsilon} &= -\varepsilon\varepsilon a^3+\varepsilon b^3=a^2-\varepsilon c^3=-b^3+\varepsilon\varepsilon c^3 \\ \frac{b'}{1-\varepsilon} &= a^3-\varepsilon b^3=-\varepsilon\varepsilon a^3+\varepsilon c^3=\varepsilon\varepsilon b^3-c^3 \\ \frac{c'}{1-\varepsilon} &= (\varepsilon\varepsilon-1)abc \end{aligned}$$

The first two numbers therefore have no factor in common with a, b, or c, and cannot be divisible by $1-\varepsilon$ either, unless a,b,c are all divisible by $1-\varepsilon$; thus they also have no factor in common with the third.

III. But the reverse path is also open. We have seen that one of the quantities is divisible by $1-\varepsilon$; let it be c. Since we can substitute $a\varepsilon$ or $a\varepsilon\varepsilon$ for a, and likewise $b\varepsilon$ or $b\varepsilon\varepsilon$ for b, we may assume that a is either $\equiv 1$ or $\equiv -1$. We shall assume the former, since in the other case $b\equiv 1$ would hold, and it would only need to be interchanged with a. Accordingly, we set

$$\begin{aligned} a &= 1+3\alpha \\ b &= -1+3\beta \end{aligned}$$

and

$$\begin{aligned} \frac{a\varepsilon+b\varepsilon\varepsilon}{\varepsilon-\varepsilon\varepsilon} &= 1+(\varepsilon\varepsilon-\varepsilon)(\alpha\varepsilon+\beta\varepsilon\varepsilon)=A \\ \frac{a\varepsilon\varepsilon+b\varepsilon}{\varepsilon-\varepsilon\varepsilon} &= -1+(\varepsilon\varepsilon-\varepsilon)(\alpha\varepsilon\varepsilon+\beta\varepsilon)=B \\ \frac{a+b}{\varepsilon-\varepsilon\varepsilon} &= (\varepsilon\varepsilon-\varepsilon)(\alpha+\beta)=C \end{aligned}$$

where $A+B+C=0$, and $ABC=\frac{a^3+b^3}{(\varepsilon-\varepsilon\varepsilon)^3}=\left(\frac{c}{\varepsilon\varepsilon-\varepsilon}\right)^3$

Since here

$$a = -\varepsilon A + \varepsilon\varepsilon B$$
$$b = \varepsilon\varepsilon A - \varepsilon B$$

A and B cannot have a common factor, because it would otherwise also be a common factor of a and b. Since $A + B + C = 0$, C consequently cannot have a factor in common with either A or B. It follows easily that A and B, and hence also C, are cubes. For $\left(\frac{c}{\varepsilon\varepsilon-\varepsilon}\right)^3$ will be divisible by $\varepsilon - \varepsilon\varepsilon$, hence also by $(\varepsilon - \varepsilon\varepsilon)^3$, or $\alpha + \beta$ by 3; therefore $A \equiv 1$, $B \equiv -1$ (mod. 3).

If we now set

$$A = a'^3$$
$$B = b'^3$$
$$C = c'^3$$

we have derived from the solution of the equation $x^3 + y^3 + z^3 = 0$

$$x = a$$
$$y = b$$
$$z = c$$

another solution,

$$x = a'$$
$$y = b'$$
$$z = c'$$

$$\text{where } a'^3 b'^3 c'^3 = \frac{c^3}{(\varepsilon\varepsilon - \varepsilon)^3}$$

so c' will contain the factor $1 - \varepsilon$ one fewer time than c. But this is absurd if c is divisible only by a fixed power of $1 - \varepsilon$, that is, if c differs from 0. For by continuing these operations we would otherwise eventually reach a solution in which z was not divisible by $1 - \varepsilon$ at all, contrary to (I).

We can take a similar path for powers with exponent 5. Namely, if $a^5 + b^5 + c^5 = 0$, we set $b + c = \alpha$, $c + a = \beta$, $a + b = \gamma$, and then

$$\begin{aligned} 0 &= (2a)^5 + (2b)^5 + (2c)^5 \\ &= (\beta + \gamma - \alpha)^5 + (\gamma + \alpha - \beta)^5 + (\alpha + \beta - \gamma)^5 \\ &= (\alpha + \beta + \gamma)^5 - 80\alpha\beta\gamma(\alpha\alpha + \beta\beta + \gamma\gamma) \end{aligned}$$

But $(\alpha+\beta+\gamma)^5 = 80\alpha\beta\gamma(\alpha\alpha+\beta\beta+\gamma\gamma)$ cannot hold unless one of the numbers α, β, γ is divisible by $1-\varepsilon$. For if none of them were divisible, both $\alpha+\beta+\gamma$ and $\alpha\alpha+\beta\beta+\gamma\gamma$ would have to be divisible by $1-\varepsilon$, and consequently so would $2(\alpha\alpha+\beta\beta+\gamma\gamma)+2(\alpha+\beta+\gamma)(\alpha+\beta-\gamma) = (2\alpha+\beta)^2+3\beta\beta$, which is impossible.

We can also present this as follows. If $a^5+b^5+c^5=0$, then

$$\begin{aligned} 4(a+b+c)^5 &= 5(b+c)(c+a)(a+b) \\ &\qquad [(a+2b+3c)^2+3(a+c)^2-8(a+b+c)c] \\ &= 5(b+c)(c+a)(a+b) \\ &\qquad [(b-c)^2+3(b+c)^2+4(a+b+c)a] \end{aligned}$$

$$4(a+b+c)^5+5abc[(b-c)^2+3(b+c)^2] = 5(a+b+c)\{\dots\}$$

The rest of the proof would be very similar to the preceding one.

But if we try the same procedure with seventh powers, we cannot prove that for a given solution

$$a^7+b^7+c^7=0$$

one of the quantities a, b, c must be divisible by 7. For we obtain only

$$\begin{aligned} (\alpha+\beta+\gamma)^7 = 5\alpha\beta\gamma\{&3(\alpha^4+\beta^4+\gamma^4) \\ &+10(\alpha\alpha\beta\beta+\alpha\alpha\gamma\gamma+\beta\beta\gamma\gamma)\} \end{aligned}$$

which can hold without α, β, γ being divisible by $1-\varepsilon$.

Hopefully, however, this can in future be derived from the nature of the determinants and the units.

[II.]

DETERMINATION OF THE NEAREST INTEGER.

Let

$$\begin{aligned} \varepsilon^3 = 1, \quad m &= a+b\varepsilon+c\varepsilon\varepsilon \\ 2a-b-c &= A+\alpha \\ 2b-c-a &= B+\beta \\ 2c-a-b &= C+\gamma \end{aligned}$$

where A, B, C are integers and α, β, γ are positive proper fractions. We then have

$$A+B+C+\alpha+\beta+\gamma=0$$

so there are three cases to distinguish:

I. $\alpha + \beta + \gamma = 0$, hence $\alpha = 0$, $\beta = 0$, $\gamma = 0$

1, $A \equiv B \equiv C \pmod 3$. Here m itself is an integer.

2, $A - B \equiv B - C \equiv C - A \equiv \pm 1 \pmod 3$. Here $m \pm \frac{\varepsilon - \varepsilon\varepsilon}{3} \cdot \varepsilon^n$ is an integer.

II. $\alpha + \beta + \gamma = 1$.

Here each of

$$A + B\varepsilon + C\varepsilon\varepsilon + 1$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon\varepsilon$$

is divisible by $1 - \varepsilon$, and one of these numbers by 3. The quotient, or

$$m + \frac{\varepsilon^n - \alpha - \beta\varepsilon - \gamma\varepsilon\varepsilon}{3}$$

is the required integer.

III. $\alpha + \beta + \gamma = 2$

Here

$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon + \varepsilon\varepsilon$$
$$A + B\varepsilon + C\varepsilon\varepsilon + \varepsilon\varepsilon + 1$$
$$A + B\varepsilon + C\varepsilon\varepsilon + 1 + \varepsilon$$

are divisible by $1 - \varepsilon$, and one of these numbers by 3. The quotient, or

$$m + \frac{\varepsilon^n(\varepsilon + \varepsilon\varepsilon) - \alpha - \beta\varepsilon - \gamma\varepsilon\varepsilon}{3}$$

is the required integer.

In all three cases the remainder has the form

$$x + y\varepsilon + z\varepsilon\varepsilon$$

so that x, y, z are smaller than $\frac{1}{3}$ in absolute value, and $x + y + z = 0$. This necessarily gives

$$xx + yy + zz = 2xx - 2yz = 2yy - 2xz = 2zz - 2xy < \tfrac{2}{9}$$

because two of the three quantities x, y, z must have the same sign. Consequently, the determinant of the remainder is

$$= \tfrac{3}{2}(xx + yy + zz) < \tfrac{1}{3} \qquad \text{Q. E. D.}$$

The nearest integer is found *more conveniently* as follows. Given $a + b\varepsilon + c\varepsilon\varepsilon = m$, set

$$b - a = C + \gamma$$
$$c - b = A + \alpha$$
$$a - c = B + \beta$$

where A, B, C are the next smaller integers and α, β, γ are positive fractions. There are three cases to distinguish:

I. $\alpha + \beta + \gamma = 0$; then m itself is an integer

II. $\alpha + \beta + \gamma = 1$; then the nearest integer is

$$\begin{array}{lll} B + (B+C)\varepsilon & & \text{if } \alpha \text{ is the largest fraction.} \\ \quad C\varepsilon + (A+C)\varepsilon\varepsilon & & \beta \\ A + B \quad . \quad +A\varepsilon\varepsilon & & \gamma \end{array}$$

II. $\alpha + \beta + \gamma = 2$; then the nearest integer is

$$\begin{array}{lll} B + 1 + (B+C+2)\varepsilon & & \text{if } \alpha \text{ is the smallest fraction.} \\ \quad (C+1)\varepsilon + (A+C+2)\varepsilon\varepsilon & & \beta \\ A + B + 2 \quad . \quad +(A+1)\varepsilon\varepsilon & & \gamma \end{array}$$

In II, 1, the remainder is $\beta + (\beta+\gamma)\varepsilon$, whose determinant is

$$\begin{aligned} &= \beta\beta + \beta\gamma + \gamma\gamma \\ &= \tfrac{1}{3} - \tfrac{1}{6}[(\alpha-\beta)(1+3\beta) + (\alpha-\gamma)(1+3\gamma)] \end{aligned}$$

More simply still:

Arrange the fractions $a - [a], b - [b], c - [c]$ by size, and call them p, q, r in that order. If all three are equal, m is an integer. If they are unequal, let t be any fraction between

$$\begin{array}{llll} p \text{ and } q, & \text{according as} & q - p & \text{is largest} \\ q \text{ and } r & & r - q & \\ r \text{ and } 1 + p & & 1 + p - r & \end{array}$$

Then

$$[a-t] + [b-t]\varepsilon + [c-t]\varepsilon\varepsilon$$

is the nearest integer.

[III.]

Let $\varepsilon^5 = 1$

$$a + b\varepsilon + c\varepsilon\varepsilon + d\varepsilon^2 + e\varepsilon^4 = q'$$

$$a + b\varepsilon^{-1} + c\varepsilon^{-2} + d\varepsilon^{-3} + e\varepsilon^{-4} = q''''$$

$$(a-b)^2 + (b-c)^2 + (c-d)^2 + (d-e)^2 + (e-a)^2 = 2p'$$

$$(a-c)^2 + (b-d)^2 + (c-e)^2 + (d-a)^2 + (e-b)^2 = 2p''$$

$$q'q'''' = -p'\varepsilon - p''\varepsilon\varepsilon - p''\varepsilon^3 - p'\varepsilon^4 = P'$$

$$q''q''' = -p'\varepsilon\varepsilon - p''\varepsilon^4 - p''\varepsilon - p'\varepsilon^3 = P''$$

$$\text{Determinant} = P'P'' = -p'p' + 3p'p'' - p''p''$$
$$\text{Measure} = 2p' + 2p'' = 2P' + 2P''$$
$$= 5(aa + bb + cc + dd + ee) - (a + b + c + d + e)^2$$

Multiplication by $1 - \varepsilon$ gives the new measure $= 8p'$

$$\text{Maximum measure} = 2\left(\frac{\sin 72^\circ}{\sin 36^\circ} + \frac{\sin 36^\circ}{\sin 72^\circ}\right)\sqrt{D} = 4{,}472\sqrt{D}$$

Modulus $= 1 - \varepsilon$

$$1 - \varepsilon = x$$
$$\varepsilon = 1 - x$$
$$\varepsilon\varepsilon = 1 - 2x + xx$$
$$\varepsilon^3 = 1 - 3x + 3xx - x^3$$
$$\varepsilon^4 = 1 - 4x + 6xx - 4x^3 + x^4$$
$$= -4 + 6x - 4xx + x^3$$

Thus

$$\frac{1 - \varepsilon^n}{1 - \varepsilon} \equiv n \text{ mod. } (1 - \varepsilon)$$
$$\varepsilon^n \equiv 1 - nx \text{ mod. } (1 - \varepsilon)^2$$
$$\left(\frac{\varepsilon + \varepsilon^4}{\varepsilon\varepsilon + \varepsilon^3}\right)^n \equiv 1 + nxx \text{ mod. } (1 - \varepsilon)^3$$

Thus a number that is $\equiv 1$ mod. $(1 - \varepsilon)^3$ can be a unit *only* if it is also $\equiv 1$ (mod. 5).

[IV.]

SOME REMARKS ON THE MEASURE OF NUMBERS.

Let $\varepsilon^n = 1$, with n prime,

$$m = a + a'\varepsilon + a''\varepsilon\varepsilon + a'''\varepsilon^3 + \ldots + a^{(n-1)}\varepsilon^{n-1} = f\varepsilon$$
$$D = f\varepsilon \,.\, f\varepsilon\varepsilon \,.\, f\varepsilon^3 \ldots f\varepsilon^{n-1}$$
$$f\varepsilon \,.\, f\varepsilon^{n-1} = -b'(\varepsilon + \varepsilon^{n-1}) - b''(\varepsilon^2 + \varepsilon^{-2})$$
$$- b'''(\varepsilon^3 + \varepsilon^{-3}) \ldots$$

then

$$2b' = (a - a')^2 + (a' - a'')^2 + (a'' - a''')^2 + \text{etc.}$$
$$2b'' = (a - a'')^2 + (a' - a''')^2 + (a'' - a'''')^2 + \text{etc.}$$
$$\text{etc.}$$

Here $b', b'', b''' \ldots$ are therefore all positive quantities; they are called the *partial measures* of m, and their sum

$$b' + b'' + b''' + \text{etc.} = n(aa + a'a' + a''a'' + \ldots) - (a + a' + a'' + \text{etc.})^2$$

the *general measure*. If we set

$$f\varepsilon \,.\, f\varepsilon^{n-1} = c', \quad f\varepsilon\varepsilon \,.\, f\varepsilon^{n-2} = c'' \quad \text{etc.}$$

then

$$c' + c'' + c''' + \text{etc.} + c^{\frac{1}{2}(n-1)} = b' + b'' + b''' + \text{etc.} + b^{\frac{1}{2}(n-1)}$$

$$c'(\varepsilon + \varepsilon^{n-1}) + c''(\varepsilon\varepsilon + \varepsilon^{n-2}) + c'''(\varepsilon^3 + \varepsilon^{n-3}) + \text{etc.} = 2(b' + b'' + b''' + \text{etc.} + b^{\frac{1}{2}(n-1)}) - nb'$$

$$c'(2 - \varepsilon - \varepsilon^{n-1}) + c''(2 - \varepsilon\varepsilon - \varepsilon^{n-2}) + c'''(2 - \varepsilon^3 - \varepsilon^{n-3}) + \text{etc.} = nb'$$

$$b' > \frac{n-1}{2n}(nD)^{\frac{2}{n-1}}, \quad b' + b'' + b''' + \text{etc.} > \frac{n-1}{2} \,.\, D^{\frac{2}{n-1}}$$

If, in general,

$$f\varepsilon \,.\, f\varepsilon^{n-1} = A + A'\varepsilon + A''\varepsilon\varepsilon + A'''\varepsilon^3 + \ldots$$

then the general measure is $\triangle = -A - A' - A'' - \text{etc.} + nA$

Measure of $(1 + \varepsilon) f\varepsilon \ldots$

$$\triangle' = 4\triangle - 2n(A - A') = 4\triangle - 2nb'$$

If $a + a' + a'' + \ldots = 0$, then $\triangle = n(aa + a'a' + a''a'' + \text{etc.})$

and if $A + A' + A'' + \ldots = 0$, then $\triangle = nA$, $\triangle' = n(2A + 2A')$

Thus, if one of the coefficients A', A'', etc., is negative and greater in absolute value than $\frac{1}{2}A$, the measure can be reduced without changing the determinant.

[V.]

If it should be confirmed that every unit is composed solely of factors of the form

$$\frac{\varepsilon^{\alpha} - \varepsilon^{\beta}}{\varepsilon^{\gamma} - \varepsilon^{\delta}}$$

the following theorem would be proved:

If $f(\varepsilon)$ is a unit, then

$$\frac{f(\varepsilon)}{f(\varepsilon^{-1})} = \varepsilon^{n}$$

Even without *assuming that* theorem, the conclusion is easy to prove. Let

$$\frac{f\varepsilon}{f\varepsilon^{-1}} = F\varepsilon$$

then

$$F\varepsilon \,.\, F\varepsilon^{-1} = 1$$

from which the theory of measure readily gives

$$F\varepsilon = \pm\varepsilon^{n}$$

The lower sign is impossible, however, since otherwise $f\varepsilon$ would have to be divisible by $1 - \varepsilon$.

It is easy to prove that the determinant of a number different from 0 cannot be $= 0$. If the determinant is divisible by m, the number itself is divisible by $1 - \varepsilon$. Consequently, if the determinant is divisible by m^{m-1}, the number itself must be divisible by m. This is absurd: with determinant 0, the number could first be divided by m, without changing its determinant, until it was no longer divisible. The first assertion follows as follows. Let the given number be

$$a + b\varepsilon + c\varepsilon\varepsilon + \text{etc.} \equiv a + b + c\,.\,. \mod 1 - \varepsilon$$

so its determinant is $\equiv (a + b + c\,.\,.)^{m-1} \mod 1 - \varepsilon$.

[VI.]

Let $\varepsilon^{n} = 1$

$$\begin{aligned} f\varepsilon &= a + b\varepsilon + c\varepsilon\varepsilon + d\varepsilon^{3} + \text{etc.} \\ m &= \text{determinant of this number} \\ \frac{m}{f\varepsilon} &= f\varepsilon\varepsilon \,.\, f\varepsilon^{3} \ldots f\varepsilon^{n-1} \\ &= A + B\varepsilon + C\varepsilon\varepsilon + \text{etc.} = F\varepsilon \end{aligned}$$

The number $f\varepsilon$ corresponds to a root of the congruence $x^n \equiv 1$ (mod. m.) Let it be r. We have

$$\begin{aligned} nA &= F1 + F\varepsilon + F\varepsilon\varepsilon + \ldots \\ nB &= F1 + \varepsilon^{-1}F\varepsilon + \varepsilon^{-2}F\varepsilon\varepsilon + \ldots \\ nC &= F1 + \varepsilon^{-2}F\varepsilon + \varepsilon^{-4}F\varepsilon\varepsilon + \ldots \\ &\text{etc.} \end{aligned}$$

Thus, since $F\varepsilon\varepsilon, F\varepsilon^3, F\varepsilon^4$, etc., are divisible by $f\varepsilon$,

$$\begin{gathered} nA - F1 - \varepsilon(nB - F1) \\ nA - F1 - \varepsilon\varepsilon(nC - F1) \\ nA - F1 - \varepsilon^3(nD - F1) \\ \text{etc.} \end{gathered}$$

are all divisible by $f\varepsilon$, or also

$$\begin{gathered} n(A - B) - \varepsilon n(B - C) \\ n(B - C) - \varepsilon n(C - D) \\ \text{etc.} \end{gathered}$$

are divisible by $f\varepsilon$; consequently [if $f\varepsilon$ is not divisible by $1 - \varepsilon$, and $F\varepsilon$ is not divisible by a real integer]

$$\varepsilon \equiv \frac{A-B}{B-C} \equiv \frac{B-C}{C-D} \equiv \frac{C-D}{D-E} \text{ etc. (mod. } f\varepsilon)$$

REMARKS.

The investigations collected here under the common heading On the Theory of Complex Numbers are scattered notes in the manuscript. They contain the essential steps of the proof of FERMAT's theorem for the third and fifth powers. In incomplete notes that are not printed here, numbers composed of cube roots of unity are studied by means of both the theory of binary quadratic forms and the division of the circle. When applying the latter, during the preparation of the paper *Disquisitionum circa aequationes puras ulterior evolutio*, the ternary cubic form into which $27\frac{x^n-1}{x-1}$ can be transformed for a prime $n \equiv 1 \bmod. 3$ was also set out, and the theory of composition of the related form $X^3 + mY^3 + mmZ^3 - 3mXYZ$ was developed at the same time.

The property of integers formed from cube roots of unity that is assumed in the investigations of Fragment [I], namely that each can be decomposed into prime factors in only one way, follows from EUCLID's procedure for finding the common divisors of two numbers, if one applies the theorem derived in [II] on the nearest integer to any given fraction.

That the same fundamental property holds for numbers composed of fifth roots of unity follows from this: the fractional remainder formed by a rule entirely analogous to that in [II], either for m or else for m multiplied by a suitable unit E, is such that subtracting it from the given number mE produces an integer, and its determinant does not exceed unity. As indicated in [III], the units can be derived from the theory of binary quadratic forms of determinant 5, in conjunction with the decomposition of a real prime into four factors (for example, $11 = \text{Det. } (2 + \varepsilon)$), namely as products of powers of ε and $1 + \varepsilon$.

SCHERING.

TABLE

OF THE QUADRATIC CHARACTER

OF THE PRIMES FROM 2 TO 997 AS RESIDUES

WITH RESPECT

TO THE PRIMES FROM 3 TO 503 AS DIVISORS.

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	
3		−		−		−		−			−	−		−				3
5			−		−			−		−	−		−				−	5
7	−			−	−				−	−		−		−		−		7
11		−	−		−				−		−	−			−	−	−	11
13		−				−	−		−	−				−		−		13
17	−					−	−	−						−	−	−	−	17
19			−	−	−		−	−	−					−	−			19
23	−	−				−			−	−	−		−		−		−	23
29			−	−		−			−	−						−	−	29
31	−		−	−				−			−		−		−		−	31
37		−		−	−							−	−		−	−		37
41	−		−						−		−	−	−	−			−	41
43					−	−	−		−		−		−	−	−	−	−	43
47	−	−		−			−					−			−	−	−	47
53				−	−	−	−			−		−		−	−	−	−	53
59		−	−	−			−	−		−			−			−	−	59
61		−	−			−		−					−		−			61
67							−	−	−	−		−			−		−	67
71	−	−	−					−		−		−		−				71
73	−	−						−	−			−	−					73
79	−		−		−	−		−	−		−							79
83		−		−	−		−		−	−	−	−	−				−	83
89	−		−		−		−								−	−		89
97	−	−			−						−			−	−	−		97
101			−			−	−	−	−		−	−		−	−			101
103	−			−		−	−	−	−	−			−				−	103
107		−			−	−		−	−	−		−	−		−	−		107
109		−	−	−						−	−			−				109
113	−			−	−	−					−		−			−		113
127	−				−	−	−	−			−	−	−		−			127
131		−	−	−	−	−							−	−		−	−	131
137	−			−	−		−	−				−					−	137
139			−	−	−	−				−	−	−	−		−			139
149			−	−			−	−		−	−	−			−	−		149
151	−		−		−		−	−		−	−	−		−	−		−	151
157		−			−	−	−	−			−	−			−			157
163													−	−	−	−		163
167	−	−		−	−			−		−	−				−			167
173						−			−	−	−	−	−	−	−			173
179		−	−			−	−	−		−	−			−	−		−	179
181		−	−		−	−				−		−		−			−	181
191	−	−	−			−	−		−					−			−	191
193	−	−		−					−		−			−			−	193
197				−				−	−	−		−	−	−	−	−	−	197
199	−		−	−		−			−	−	−			−	−	−		199
211			−		−	−		−				−		−	−	−	−	211
223	−			−			−	−		−	−	−	−	−	−	−		223
227		−		−	−			−	−	−				−	−	−	−	227
	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	

	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	
3	−	−		−	−			−		−		−		−			−	3
5	−		−		−		−		−			−			−		−	5
7		−	−		−						−	−	−	−		−		7
11		−	−				−	−		−			−			−		11
13	−				−				−	−	−		−	−	−		−	13
17		−				−	−		−	−				−		−		17
19	−			−		−			−						−	−	−	19
23			−	−					−					−	−		−	23
29		−	−			−				−	−	−					−	29
31		−	−					−	−	−	−	−	−		−			31
37		−	−	−		−			−		−			−		−	−	37
41	−			−		−				−	−		−	−	−		−	41
43		−			−	−		−	−	−	−	−		−			−	43
47	−		−		−	−	−	−	−	−					−			47
53							−	−			−		−		−			53
59			−		−						−			−		−	−	59
61	−			−		−		−		−	−	−	−	−	−	−		61
67		−	−	−		−	−			−	−			−	−			67
71			−	−	−	−	−		−	−	−	−			−			71
73	−	−	−	−	−		−	−				−		−		−		73
79		−		−	−	−	−	−	−						−			79
83	−					−						−	−	−	−			83
89		−	−	−	−		−	−			−	−			−		−	89
97	−			−	−		−	−	−	−		−	−					97
101			−		−			−	−		−				−	−		101
103	−				−	−		−		−	−				−	−	−	103
107	−				−	−	−		−		−					−		107
109	−		−	−		−	−	−				−	−		−	−		109
113	−					−		−				−	−	−	−		−	113
127	−		−	−	−					−	−		−	−	−			127
131	−						−		−		−	−	−		−			131
137	−			−					−	−	−	−				−	−	137
139		−	−		−	−	−				−		−	−	−	−	−	139
149	−	−		−						−	−		−	−				149
151								−		−				−		−	−	151
157		−	−				−		−			−	−	−				157
163	−		−			−		−					−		−			163
167	−						−	−			−			−		−		167
173		−		−		−	−					−	−			−	−	173
179	−	−				−	−		−		−						−	179
181		−		−	−				−							−	−	181
191		−			−			−		−	−	−						191
193		−				−		−	−		−	−			−	−	−	193
197	−					−		−	−		−	−		−		−		197
199	−				−		−			−					−		−	199
211			−	−	−	−			−	−	−	−	−			−	−	211
223				−		−	−		−			−		−	−		−	223
227			−	−	−		−	−	−	−		−	−		−		−	227
	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	
229		–	–		–		–	–				–		–		–		229
233	–			–		–		–	–	–	–	–						233
239	–	–	–		–		–			–	–							239
241	–	–	–							–			–		–	–	–	241
251		–	–	–		–	–		–		–		–					251
257	–				–	–	–		–	–	–						–	257
263	–	–			–	–	–		–		–	–		–				263
269			–		–	–			–			–	–	–	–	–		269
271	–		–	–	–		–				–	–	–			–		271
277		–		–		–		–	–	–			–		–		–	277
281	–		–	–			–			–	–			–		–	–	281
283				–	–	–			–	–			–				–	283
293							–				–	–		–		–	–	293
307				–	–		–	–				–	–			–		307
311	–	–	–	–		–									–	–		311
313	–	–			–	–		–		–								313
317				–	–				–		–	–		–		–	–	317
331			–				–	–			–			–		–		331
337	–	–		–		–						–	–	–	–			337
347		–			–	–				–	–			–		–	–	347
349		–	–				–	–	–	–	–	–	–					349
353	–				–		–	–	–	–			–	–	–			353
359	–	–	–		–		–		–			–	–		–			359
367	–			–		–			–		–	–	–		–	–	–	367
373		–		–		–	–			–	–	–	–				–	373
379			–					–	–			–	–					379
383	–	–		–			–	–	–	–	–			–				383
389			–	–	–	–	–	–					–				–	389
397		–			–			–	–	–	–	–		–	–			397
401	–		–	–	–					–			–	–	–			401
409	–	–	–				–		–				–			–		409
419		–	–	–		–			–	–		–	–	–	–		–	419
421		–	–	–	–		–				–							421
431	–	–	–		–			–	–	–			–			–	–	431
433	–	–			–	–	–					–	–			–	–	433
439	–		–	–	–	–		–		–						–		439
443		–				–	–					–	–		–		–	443
449	–		–	–	–				–				–			–	–	449
457	–	–		–			–	–		–					–			457
461			–				–	–	–				–	–		–	–	461
463	–						–			–	–			–	–		–	463
467		–		–		–	–		–				–	–	–	–	–	467
479	–	–	–	–	–				–									479
487	–							–		–	–		–			–		487
491		–	–		–	–	–				–	–	–	–				491
499			–							–	–			–	–			499
503	–	–		–	–	–			–					–	–		–	503
	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	

	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	
229	–		–			–		–		–								229
233			–				–		–		–	–	–		–			233
239	–	–	–			–			–			–	–	–				239
241	–	–			–	–		–			–		–					241
251		–		–	–	–	–		–	–			–		–			251
257	–	–		–	–		–						–			–	–	257
263	–					–	–			–		–				–		263
269	–	–		–	–		–	–		–				–	–			269
271	–	–			–	–	–			–							–	271
277		–	–		–	–	–						–		–			277
281					–				–			–				–		281
283	–		–	–		–	–	–	–	–			–	–		–		283
293	–	–	–	–		–		–			–	–				–		293
307			–		–	–	–	–	–	–	–	–	–	–				307
311		–		–	–	–	–				–	–	–	–		–	–	311
313			–		–	–		–		–	–		–			–	–	313
317	–	–		–	–	–	–		–	–			–		–			317
331		–	–		–	–	–			–		–	–	–	–		–	331
337					–					–	–		–		–	–		337
347	–	–	–	–		–	–				–	–	–	–	–	–		347
349		–		–		–						–					–	349
353	–			–		–		–				–	–	–	–			353
359				–	–				–		–			–	–			359
367	–	–		–		–	–		–		–		–			–		367
373			–	–		–	–		–	–	–	–				–		373
379	–	–			–	–		–	–	–	–			–		–	–	379
383		–	–	–					–	–			–			–	–	383
389		–		–	–			–					–	–		–		389
397		–		–	–	–		–			–			–	–	–		397
401				–		–	–			–		–	–					401
409			–			–	–		–	–		–			–	–	–	409
419				–	–			–			–				–	–	–	419
421		–			–			–	–	–	–	–	–		–		–	421
431	–							–				–					–	431
433					–							–		–		–	–	433
439	–		–	–		–				–		–	–	–		–	–	439
443	–	–	–		–		–			–	–	–	–		–	–	–	443
449	–	–					–	–	–					–		–		449
457		–		–	–						–	–		–	–			457
461	–	–		–			–			–	–	–	–			–	–	461
463	–	–		–	–		–	–		–		–	–		–			463
467			–			–	–	–				–	–	–		–	–	467
479	–		–	–			–	–		–	–	–			–	–	–	479
487	–	–	–	–		–	–	–		–	–			–		–	–	487
491	–		–		–	–		–	–		–			–	–		–	491
499		–		–					–	–	–	–		–	–	–	–	499
503	–	–		–	–	–		–					–		–			503
	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	

	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	
3		–	–	–				–		–		–	–	–		–		3
5	–	–					–	–	–			–	–			–		5
7	–	–		–			–		–	–	–		–				–	7
11			–	–			–	–	–			–		–		–		11
13			–			–	–	–	–			–	–				–	13
17	–	–	–				–		–					–		–		17
19	–		–	–					–		–	–				–	–	19
23		–		–	–	–	–			–	–		–	–			–	23
29	–	–			–	–	–	–			–	–		–	–		–	29
31	–		–	–		–			–	–			–		–		–	31
37	–	–	–			–		–			–		–	–		–	–	37
41				–		–					–			–				41
43					–	–		–		–	–					–		43
47	–		–			–			–		–							47
53	–			–							–	–	–	–	–	–		53
59				–	–			–		–	–	–		–				59
61	–			–	–		–				–	–				–		61
67	–	–	–	–	–	–		–		–		–	–	–	–			67
71		–	–		–		–		–			–		–		–	–	71
73	–					–		–					–	–	–			73
79		–		–	–		–	–						–				79
83		–			–	–			–	–	–	–			–	–		83
89			–		–	–	–					–		–	–		–	89
97		–		–	–				–	–	–				–	–		97
101			–				–	–		–	–		–	–	–		–	101
103	–			–	–		–							–		–		103
107	–	–		–						–	–	–		–	–		–	107
109			–			–			–	–	–		–	–	–		–	109
113	–		–	–		–							–		–		–	113
127	–		–	–			–		–		–	–	–		–			127
131		–			–		–		–	–			–				–	131
137		–			–	–		–		–	–		–					137
139				–	–	–		–	–	–								139
149	–					–	–		–							–		149
151		–			–	–			–	–				–	–	–		151
157			–		–	–				–	–	–					–	157
163		–		–	–	–	–				–	–		–	–			163
167			–		–	–	–	–	–			–	–	–		–	–	167
173	–	–	–	–	–	–	–				–		–		–	–	–	173
179	–	–				–	–		–	–		–			–			179
181					–			–		–	–			–	–	–	–	181
191	–			–					–	–	–	–	–	–	–			191
193		–	–				–	–	–	–	–	–	–			–		193
197			–	–		–		–	–	–	–			–			–	197
199		–	–							–		–			–			199
211		–		–		–	–			–		–	–		–			211
223							–	–			–	–	–	–	–			223
227					–	–		–							–			227
	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	

	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	
3		–					–	–		–		–		–		–	–	3
5	–	–	–			–	–		–				–			–		5
7	–				–			–	–						–	–	–	7
11			–	–		–							–	–	–	–		11
13			–	–	–	–		–		–			–	–			–	13
17	–		–	–	–		–		–		–	–				–		17
19	–		–		–		–	–		–			–	–				19
23	–			–		–	–	–				–	–		–	–		23
29	–	–		–				–	–	–				–				29
31				–					–	–	–	–	–		–			31
37					–	–	–				–	–			–		–	37
41		–	–			–	–	–		–		–					–	41
43	–		–			–	–		–	–	–	–	–		–		–	43
47	–	–	–		–	–	–	–		–		–				–	–	47
53		–				–	–		–		–	–	–		–	–		53
59	–	–	–	–	–		–	–	–		–	–	–		–	–		59
61	–	–		–	–	–	–			–	–				–			61
67		–		–	–	–		–		–	–	–			–			67
71			–		–		–	–			–		–	–				71
73			–	–		–				–	–		–		–			73
79	–	–		–	–	–		–	–	–				–	–		–	79
83		–						–			–			–	–			83
89			–	–	–	–	–	–		–		–	–		–	–		89
97		–				–				–	–	–		–				97
101	–		–						–	–		–			–			101
103	–					–							–	–	–		–	103
107	–	–	–		–		–			–	–			–		–	–	107
109	–				–				–		–	–	–			–		109
113	–	–	–	–				–		–		–	–	–	–	–	–	113
127			–		–	–	–											127
131	–				–	–	–	–		–		–	–		–		–	131
137				–	–				–	–	–		–	–			–	137
139	–		–	–	–					–		–		–				139
149			–		–	–			–		–	–			–	–	–	149
151	–	–	–			–						–	–	–		–		151
157	–			–	–			–	–	–			–	–	–	–		157
163			–		–				–			–		–				163
167	–		–		–				–	–	–		–		–		–	167
173			–	–	–	–							–	–	–	–	–	173
179	–														–		–	179
181		–	–		–				–	–		–		–	–		–	181
191	–	–	–		–	–	–	–	–	–	–		–					191
193	–	–		–				–			–		–		–	–	–	193
197	–		–	–							–		–	–		–		197
199	–		–	–	–	–	–				–		–	–		–		199
211		–		–	–	–		–	–		–	–	–			–	–	211
223	–	–	–	–					–	–					–			223
227	–			–	–		–						–		–	–	–	227
	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	

	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	
229	–	–			–	–		–		–						–	–	229
233			–		–	–		–			–					–	–	233
239			–	–						–	–		–					239
241		–						–	–	–			–	–		–	–	241
251	–					–	–	–			–		–		–		–	251
257			–			–				–	–	–	–	–	–			257
263	–	–	–			–	–	–						–			–	263
269	–	–				–			–			–	–				–	269
271		–		–	–		–						–	–		–	–	271
277			–						–	–			–			–		277
281	–		–	–	–			–	–				–	–				281
283		–	–	–			–	–				–	–		–		–	283
293	–				–				–	–	–	–	–			–	–	293
307	–				–		–	–	–			–		–	–	–	–	307
311			–	–		–	–			–	–			–		–		311
313		–	–	–		–		–			–	–						313
317	–		–		–	–	–	–		–				–	–			317
331	–		–	–	–	–	–		–	–	–			–			–	331
337	–				–	–	–	–		–			–		–	–	–	337
347	–		–		–	–		–			–	–				–		347
349		–	–					–	–					–	–		–	349
353			–		–			–	–		–			–			–	353
359	–	–				–		–	–	–						–	–	359
367	–	–				–		–	–			–	–		–	–		367
373				–			–	–								–		373
379	–	–			–	–	–		–	–	–		–		–			379
383	–					–				–				–	–	–		383
389			–			–	–	–		–			–	–				389
397		–		–	–	–	–		–							–		397
401	–	–				–	–	–			–			–		–		401
409				–	–		–		–	–	–				–	–		409
419	–	–	–			–			–		–	–						419
421	–			–	–			–	–			–				–		421
431	–	–	–	–		–	–				–			–	–	–		431
433					–		–		–		–	–	–	–		–	–	433
439					–				–			–	–	–		–		439
443	–	–		–	–			–	–		–				–	–	–	443
449					–			–	–	–	–	–			–	–		449
457		–	–	–					–		–				–	–	–	457
461		–	–	–	–			–	–	–		–		–	–	–		461
463	–			–	–	–	–	–					–			–		463
467	–	–	–	–		–	–			–		–		–	–	–	–	467
479		–		–	–	–		–		–	–		–				–	479
487			–		–			–	–	–	–							487
491				–			–	–			–	–		–	–	–	–	491
499		–			–			–			–	–	–		–		–	499
503						–					–	–		–		–	–	503
	149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	

	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	
229		–					–	–			–	–	–				–	229
233		–	–		–	–	–			–	–	–				–	–	233
239	–	–	–	–	–	–	–			–	–	–	–				–	239
241	–	–	–	–			–	–	–					–		–	–	241
251		–	–		–		–						–		–	–	–	251
257	–	–		–						–	–	–			–			257
263					–	–	–		–			–	–	–	–	–	–	263
269	–				–	–				–	–	–		–		–		269
271		–					–		–		–	–	–					271
277		–						–	–		–	–	–	–	–			277
281		–			–		–	–	–	–				–	–	–	–	281
283			–	–	–	–	–		–	–	–	–	–		–		–	283
293	–			–		–	–	–		–	–	–			–	–		293
307			–	–		–		–			–	–	–	–	–	–		307
311								–					–	–	–	–	–	311
313		–			–	–		–	–			–	–	–	–	–	–	313
317			–	–	–			–	–	–	–	–	–	–	–			317
331	–	–				–	–		–	–	–			–		–	–	331
337	–	–	–		–				–	–			–	–		–	–	337
347		–	–		–	–	–	–	–		–							347
349	–	–		–	–	–	–		–	–	–	–		–			–	349
353						–	–	–	–	–	–	–	–		–	–	–	353
359		–							–	–		–			–	–		359
367			–				–	–	–	–				–				367
373	–		–	–						–		–					–	373
379	–		–	–	–		–	–	–			–	–	–		–	–	379
383			–		–			–			–			–	–	–		383
389	–					–		–		–	–		–	–		–	–	389
397				–			–	–	–		–	–						397
401	–	–		–	–							–	–	–		–	–	401
409	–						–		–			–	–	–	–		–	409
419			–	–		–			–		–						–	419
421	–	–				–		–	–	–		–		–	–		–	421
431					–			–		–		–					–	431
433		–		–		–	–	–		–	–					–	–	433
439			–			–	–		–	–		–				–		439
443					–		–		–		–	–	–			–		443
449			–		–	–	–				–					–	–	449
457	–	–		–		–				–		–	–	–		–		457
461					–				–				–		–	–		461
463	–		–				–	–		–	–		–	–			–	463
467	–	–	–					–		–					–	–		467
479		–	–	–			–	–			–	–		–		–		479
487		–	–		–	–	–	–				–	–	–			–	487
491	–	–		–	–	–		–			–					–		491
499	–		–	–	–			–	–		–	–			–	–	–	499
503				–	–		–		–	–	–				–			503
	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	

	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	
3		–			–	–	–			–		–		–		–	–	3
5		–		–			–		–		–	–	–	–	–		–	5
7	–			–		–	–		–		–			–	–			7
11			–		–		–	–	–	–	–		–	–		–		11
13	–				–	–			–				–			–	–	13
17		–	–	–		–		–	–			–		–		–		17
19	–	–	–	–	–				–	–			–					19
23	–	–	–							–		–					–	23
29	–	–	–			–		–		–	–		–		–		–	29
31		–		–		–	–			–			–	–	–		–	31
37		–		–	–	–	–			–			–			–		37
41		–	–	–	–	–	–		–		–	–	–		–	–		41
43			–	–	–		–			–	–				–		–	43
47	–		–				–	–		–	–				–		–	47
53	–				–							–			–	–	–	53
59				–		–	–	–	–							–	–	59
61	–		–		–		–								–		–	61
67		–		–					–	–			–	–	–		–	67
71				–	–	–	–					–	–		–			71
73	–	–	–	–	–	–		–	–	–	–		–				–	73
79	–				–			–	–	–				–	–	–	–	79
83		–	–	–		–		–		–	–	–	–		–			83
89	–				–	–					–	–						89
97			–				–		–	–			–	–	–			97
101				–	–	–	–	–				–		–				101
103	–			–	–	–					–	–	–	–	–			103
107						–		–		–				–	–		–	107
109	–	–	–			–					–	–		–	–	–	–	109
113	–		–		–			–	–		–			–			–	113
127			–		–			–	–	–			–		–	–		127
131			–		–		–	–		–		–		–	–		–	131
137	–				–	–	–	–	–	–		–	–			–	–	137
139	–	–		–	–							–		–		–		139
149	–			–	–		–	–			–		–	–	–			149
151	–	–						–		–	–						–	151
157	–	–	–						–				–		–			157
163	–			–	–	–	–	–		–		–	–	–			–	163
167			–	–	–			–		–		–	–	–	–	–		167
173	–			–	–		–	–	–	–	–		–		–			173
179	–			–	–	–		–	–	–	–	–	–			–	–	179
181	–	–	–	–	–	–			–		–			–				181
191	–	–	–					–		–		–		–	–	–		191
193				–			–	–	–			–						193
197	–		–				–				–	–	–		–	–		197
199				–			–	–						–	–	–		199
211	–			–				–	–				–		–	–		211
223	–	–	–	–	–		–		–		–		–			–		223
227	–	–		–								–	–				–	227
	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	

	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	
3			–		–			–		–				–	–	–		3
5		–		–			–		–	–		–	–		–			5
7	–	–	–		–			–	–	–					–	–	–	7
11	–	–			–	–		–		–		–	–					11
13	–					–			–		–		–	–		–		13
17	–		–	–	–	–			–			–		–			–	17
19	–		–	–	–	–	–		–	–	–				–		–	19
23	–	–		–	–			–	–	–		–			–	–		23
29			–		–			–		–		–	–	–		–	–	29
31	–					–	–				–		–		–	–		31
37	–								–			–	–					37
41	–	–		–		–		–	–					–	–			41
43	–			–			–	–				–			–	–	–	43
47			–				–	–	–				–	–	–			47
53		–		–		–		–					–	–	–	–		53
59		–		–			–	–	–	–			–	–		–	–	59
61	–	–		–	–		–	–	–		–							61
67		–	–	–		–	–		–			–		–			–	67
71					–					–	–	–	–			–	–	71
73			–	–	–		–	–		–	–	–		–		–	–	73
79			–			–	–	–		–				–	–	–	–	79
83	–						–			–		–	–	–		–	–	83
89	–	–		–	–	–	–	–				–		–				89
97		–		–	–	–	–	–	–		–	–	–			–	–	97
101		–							–	–		–	–		–		–	101
103				–		–			–		–	–		–	–	–		103
107			–	–	–	–					–	–				–		107
109	–		–	–	–	–	–			–		–		–	–		–	109
113	–			–	–	–					–	–	–			–	–	113
127	–	–	–		–		–				–	–	–	–			–	127
131			–			–		–									–	131
137	–	–		–		–	–	–		–		–		–	–	–	–	137
139				–	–						–			–	–		–	139
149	–				–	–								–		–	–	149
151			–	–	–			–	–		–		–		–	–		151
157			–	–		–		–						–		–	–	157
163			–	–				–		–	–			–		–		163
167		–		–		–			–		–	–		–			–	167
173					–	–	–				–	–		–	–		–	173
179	–						–	–		–	–	–			–		–	179
181	–	–		–	–		–	–	–	–		–		–		–	–	181
191		–	–	–	–	–	–		–	–	–							191
193		–		–		–	–	–						–		–		193
197	–	–	–				–	–	–	–	–		–				–	197
199	–	–		–	–		–	–				–	–	–				199
211	–					–		–	–		–	–	–	–	–	–		211
223	–			–	–		–	–		–		–				–		223
227		–	–	–	–		–	–			–			–	–		–	227
	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	

	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	
229	–			–	–	–		–		–	–	–		–	–	–	–	229
233		–	–	–												–		233
239	–	–		–	–	–		–	–		–	–	–	–	–		–	239
241	–	–		–							–			–		–		241
251				–		–									–			251
257		–				–	–			–	–		–			–		257
263		–		–	–						–		–				–	263
269	–	–	–						–				–	–		–	–	269
271		–	–	–				–		–		–	–		–	–		271
277	–		–		–		–	–	–	–				–	–	–		277
281	–	–	–	–	–		–			–		–	–	–			–	281
283	–	–	–			–	–	–	–				–	–		–		283
293	–	–	–					–	–	–			–			–		293
307	–	–	–		–	–		–		–	–	–	–	–				307
311	–		–	–	–			–	–		–	–	–		–		–	311
313		–			–		–	–	–		–	–		–				313
317			–	–				–				–		–				317
331	–		–		–				–		–		–		–	–		331
337		–	–			–	–		–		–	–	–	–	–	–		337
347	–			–				–	–					–				347
349		–	–							–		–	–					349
353		–	–					–	–	–				–	–		–	353
359				–	–		–	–	–			–	–		–	–	–	359
367	–				–			–		–			–		–	–	–	367
373						–		–	–		–	–	–	–			–	373
379	–				–		–	–			–	–				–		379
383			–			–		–	–	–	–		–	–	–	–	–	383
389	–		–	–		–		–	–			–	–		–	–		389
397		–	–		–			–		–	–	–			–	–	–	397
401						–	–	–		–	–	–	–	–		–		401
409		–		–		–	–		–	–	–	–	–	–		–	–	409
419	–	–				–	–		–		–	–	–		–		–	419
421	–		–			–		–			–	–		–		–		421
431	–		–				–		–	–					–	–	–	431
433				–	–		–	–	–	–	–	–		–	–	–	–	433
439	–		–			–	–			–		–				–	–	439
443	–	–		–	–	–		–	–			–	–					443
449	–	–		–	–		–					–		–	–	–	–	449
457	–	–		–		–			–		–	–	–	–		–	–	457
461	–			–	–	–				–					–		–	461
463				–	–	–		–	–			–	–				–	463
467		–				–			–					–		–		467
479		–				–				–	–			–				479
487						–	–	–		–	–		–		–	–	–	487
491		–					–		–		–	–	–					491
499			–	–						–	–	–		–	–	–	–	499
503					–	–	–	–	–	–	–			–		–		503
	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	

	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	
229	–	–	–	–	–	–			–		–	–			–		–	229
233	–		–			–	–		–	–	–		–			–	–	233
239	–		–				–	–			–	–		–				239
241			–			–	–	–	–			–		–	–		–	241
251	–	–							–		–	–		–	–	–		251
257			–				–		–	–	–			–				257
263		–		–	–	–	–						–				–	263
269		–	–					–	–							–		269
271		–				–			–	–		–	–	–		–		271
277					–	–	–	–	–	–					–	–	–	277
281	–			–						–	–	–		–			–	281
283	–		–				–	–	–	–			–	–		–		283
293	–	–			–		–		–	–	–	–	–			–		293
307			–		–	–			–		–			–	–	–	–	307
311			–	–		–	–		–	–	–		–	–				311
313			–		–		–	–				–	–	–	–	–		313
317				–		–				–	–		–			–	–	317
331		–	–	–	–			–			–					–		331
337		–			–			–		–		–					–	337
347		–	–	–	–	–	–	–	–	–	–			–	–			347
349	–	–	–			–	–		–						–	–		349
353										–		–	–		–	–		353
359		–	–	–		–	–	–	–		–	–	–	–	–	–	–	359
367		–		–		–	–	–	–	–					–		–	367
373	–		–	–	–	–	–	–			–		–				–	373
379	–	–			–	–	–			–		–	–	–			–	379
383						–	–		–	–		–	–				–	383
389	–		–		–	–			–		–	–					–	389
397				–			–	–		–	–		–	–	–		–	397
401			–				–	–	–	–	–				–	–	–	401
409	–	–	–		–				–	–		–				–		409
419			–			–	–			–	–		–		–			419
421		–	–			–	–			–	–		–					421
431	–	–		–	–	–	–		–		–		–	–	–	–		431
433		–	–			–		–		–	–		–		–			433
439	–	–	–	–		–	–		–		–	–			–			439
443	–		–				–		–	–		–					–	443
449		–	–		–	–				–			–		–	–		449
457	–	–	–	–	–				–	–			–		–		–	457
461			–	–		–		–	–					–	–		–	461
463	–	–	–		–	–	–			–			–	–	–	–	–	463
467	–	–		–		–	–				–				–		–	467
479							–	–	–	–	–	–	–	–				479
487	–			–	–	–		–	–		–			–		–	–	487
491			–	–	–	–			–		–					–		491
499		–	–			–		–	–	–	–		–	–				499
503	–				–						–	–	–			–	–	503
	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	

	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	
3			–	–				–	–	–		–	–		–			3
5		–	–				–	–				–	–	–				5
7		–	–				–			–	–		–	–			–	7
11				–	–		–				–	–	–	–	–	–	–	11
13	–	–	–				–	–	–					–		–	–	13
17	–	–		–	–	–	–			–			–			–		17
19			–	–	–	–				–	–	–	–		–	–	–	19
23				–	–	–	–	–	–							–	–	23
29			–		–	–				–			–		–	–		29
31	–			–		–	–		–		–						–	31
37			–			–	–	–		–	–	–		–				37
41		–					–		–	–	–	–	–			–		41
43	–	–					–			–	–	–			–			43
47			–					–		–	–	–			–	–	–	47
53				–	–	–	–		–			–			–	–	–	53
59				–		–	–		–		–	–	–	–	–	–	–	59
61	–	–	–					–	–	–		–						61
67		–	–					–	–	–	–	–			–			67
71		–	–	–	–	–				–	–			–	–	–		71
73					–	–			–			–		–			–	73
79	–	–	–			–	–				–			–	–		–	79
83	–					–			–		–	–						83
89					–			–	–	–		–	–	–	–			89
97			–			–			–	–	–		–		–	–		97
101	–	–			–	–		–	–			–	–		–		–	101
103			–		–				–	–		–	–	–	–	–		103
107		–	–	–	–		–								–		–	107
109			–			–						–				–	–	109
113	–	–			–	–		–			–					–	–	113
127		–		–	–				–						–		–	127
131	–	–		–	–		–	–		–			–	–		–	–	131
137	–				–				–	–	–			–		–	–	137
139	–	–			–	–		–	–	–		–				–		139
149	–		–	–	–			–		–			–	–	–			149
151	–	–	–	–				–		–				–	–	–	–	151
157			–	–		–		–			–	–	–	–		–	–	157
163	–			–		–			–					–		–	–	163
167	–			–			–	–		–	–		–					–	167
173			–						–			–		–	–			173
179						–		–	–	–	–	–			–	–	–	179
181	–			–	–		–		–	–					–			181
191				–		–	–		–	–		–		–			–	191
193	–		–	–	–	–			–					–	–			193
197	–	–			–			–	–	–	–	–	–				–	197
199	–						–	–	–	–	–				–	–	–	199
211						–		–	–				–			–	–	211
223				–			–				–				–	–		223
227	–				–	–		–		–			–		–			227
	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	

	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	
3		–	–			–		–		–	–	–		–	–		3
5	–	–				–	–	–	–			–		–		–	5
7	–		–		–		–	–				–	–	–	–		7
11		–			–	–		–	–	–				–	–		11
13	–		–	–			–		–	–				–	–		13
17	–	–					–			–	–	–			–	–	17
19						–	–	–	–	–	–	–			–	–	19
23			–		–	–			–			–				–	23
29		–	–		–	–	–	–	–							–	29
31	–	–			–	–	–			–	–			–			31
37	–		–	–		–			–		–	–	–	–		–	37
41		–		–			–				–	–	–			–	41
43	–	–			–		–	–	–								43
47	–	–			–			–	–		–	–				–	47
53		–	–		–					–	–		–	–	–		53
59		–		–				–		–	–		–		–	–	59
61	–				–	–			–	–	–			–	–		61
67	–					–		–	–				–	–		–	67
71	–			–					–			–					71
73	–	–	–							–	–	–			–		73
79				–	–				–	–	–		–	–	–	–	79
83	–		–			–	–			–	–	–		–	–		83
89	–		–			–	–				–			–	–	–	89
97		–	–	–	–	–	–			–	–		–	–			97
101				–	–	–	–			–			–			–	101
103	–		–	–			–	–				–		–	–		103
107		–		–	–	–				–			–			–	107
109	–	–			–					–			–	–			109
113				–		–		–	–	–		–				–	113
127		–	–	–				–	–		–	–			–		127
131	–				–	–	–		–			–			–		131
137				–	–		–		–						–	–	137
139			–	–	–		–		–		–	–				–	139
149	–			–		–		–	–			–		–		–	149
151	–		–				–	–		–			–		–		151
157	–	–		–				–		–	–	–	–				157
163		–	–	–		–	–	–			–	–	–				163
167				–			–				–		–		–	–	167
173	–	–		–	–	–	–			–	–	–	–				173
179		–			–			–	–		–		–			–	179
181	–					–		–	–	–	–	–		–	–	–	181
191	–		–	–		–	–	–		–	–		–		–		191
193				–		–		–						–			193
197		–			–	–				–	–	–		–			197
199	–	–		–	–	–	–	–	–	–					–		199
211				–		–		–			–						211
223	–		–	–	–		–		–	–	–		–	–			223
227	–	–	–			–		–					–	–	–		227
	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	

	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	
229		–			–	–			–		–	–	–	–	–			229
233			–		–		–	–	–					–	–	–	–	233
239	–	–	–	–	–		–			–			–	–	–	–		239
241	–	–						–	–		–			–	–			241
251		–	–	–	–	–			–		–	–						251
257	–		–		–	–				–			–		–	–	–	257
263	–	–		–	–			–	–			–	–		–	–		263
269	–				–	–	–				–	–	–	–	–		–	269
271				–	–		–					–	–	–				271
277	–			–		–		–		–	–			–	–			277
281	–	–	–		–	–		–	–			–	–	–	–	–		281
283	–			–					–		–				–	–		283
293		–	–	–	–			–	–		–	–		–	–	–	–	293
307	–	–	–		–	–		–					–				–	307
311	–		–			–	–						–		–	–		311
313		–		–	–	–	–	–	–	–	–						–	313
317		–	–	–								–		–	–			317
331	–	–			–		–	–	–							–		331
337	–		–			–	–					–	–			–	–	337
347		–	–			–					–		–		–	–	–	347
349	–			–	–				–	–	–		–	–		–	–	349
353			–			–			–	–				–				353
359	–						–	–		–			–	–		–	–	359
367	–	–	–	–	–	–		–	–			–	–	–				367
373		–	–	–		–	–						–		–		–	373
379				–				–		–				–		–		379
383		–			–		–		–				–	–	–			383
389		–					–		–			–		–			–	389
397		–			–	–	–						–		–	–	–	397
401	–			–	–		–	–	–			–			–		–	401
409	–	–	–		–	–		–		–								409
419	–		–				–		–		–							419
421	–				–		–	–		–	–			–	–		–	421
431	–	–				–			–	–			–		–	–		431
433		–		–									–	–	–			433
439		–		–		–	–	–				–			–	–		439
443	–	–			–		–		–	–	–		–	–		–		443
449	–		–	–		–				–					–	–	–	449
457		–	–		–	–		–	–			–	–				–	457
461	–		–		–	–	–				–	–		–				461
463	–			–	–	–	–	–	–		–	–	–	–			–	463
467					–			–		–		–	–	–			–	467
479	–	–	–	–	–		–	–	–		–	–		–		–		479
487	–	–	–		–	–			–		–	–	–	–	–		–	487
491			–				–				–				–	–		491
499	–	–			–		–				–	–	–	–	–			499
503		–			–		–	–	–				–	–		–	–	503
	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	

	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	
229		–	–		–	–	–				–		–	–	–		229
233		–	–		–	–	–			–				–	–	–	233
239		–				–			–	–	–	–		–	–	–	239
241	–		–		–	–			–	–	–	–	–				241
251				–	–	–		–	–	–		–	–	–	–		251
257			–		–		–	–	–	–		–					257
263	–		–	–	–			–			–			–		–	263
269	–									–			–	–			269
271		–			–			–	–	–						–	271
277				–			–	–	–			–	–		–	–	277
281			–		–				–	–			–		–		281
283	–	–		–	–		–	–		–				–		–	283
293	–		–	–	–		–	–	–	–		–					293
307				–	–	–	–		–	–	–		–				307
311		–					–			–		–	–		–	–	311
313	–	–			–		–	–			–	–	–				313
317	–		–	–	–	–	–		–		–	–			–		317
331	–				–		–				–	–	–	–	–		331
337		–	–	–	–		–										337
347			–	–					–	–	–		–			–	347
349		–	–		–		–			–		–	–				349
353	–			–	–	–				–							353
359	–	–			–				–	–	–		–	–			359
367	–					–							–		–		367
373	–		–		–	–		–	–		–	–	–				373
379	–		–		–		–			–			–	–			379
383	–	–		–	–				–	–	–			–		–	383
389	–	–			–	–	–	–	–		–		–			–	389
397			–		–		–	–	–	–				–	–	–	397
401				–		–		–	–		–	–		–	–	–	401
409	–				–			–		–	–		–				409
419	–		–		–				–			–	–			–	419
421		–	–	–							–	–	–		–	–	421
431	–	–	–	–			–	–	–		–			–	–	–	431
433									–	–	–	–	–	–	–	–	433
439	–	–	–		–	–			–	–			–				439
443						–	–			–			–	–	–	–	443
449		–	–	–		–	–								–	–	449
457		–	–	–				–	–			–	–	–	–	–	457
461	–		–	–				–	–	–	–			–	–		461
463	–				–	–		–	–	–	–	–	–	–		–	463
467	–		–	–					–		–	–	–	–			467
479	–		–	–				–	–				–		–		479
487					–	–	–	–	–	–			–	–	–	–	487
491	–		–		–		–	–						–			491
499			–	–	–					–	–				–		499
503	–	–	–			–	–		–	–		–				–	503
	659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	

	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	
3	–		–			–		–		–		–		–		–		3
5	–				–	–	–			–	–			–			–	5
7					–		–	–	–						–	–		7
11		–		–				–		–	–			–	–		–	11
13				–	–			–		–			–	–			–	13
17	–	–		–						–				–	–			17
19	–				–		–	–				–		–			–	19
23					–	–	–	–		–		–	–	–	–	–		23
29			–			–	–						–		–	–		29
31	–					–					–	–	–			–		31
37		–	–			–	–	–			–				–	–	–	37
41	–		–	–		–	–			–		–	–	–	–	–	–	41
43	–		–	–	–		–	–	–			–	–			–	–	43
47	–	–				–		–	–			–			–			47
53						–		–			–		–	–	–	–		53
59			–						–	–		–				–		59
61		–		–	–				–	–	–	–	–	–	–		–	61
67		–		–			–	–	–	–	–	–		–	–	–	–	67
71			–	–		–	–			–	–	–	–			–	–	71
73			–	–	–	–	–		–		–	–	–			–		73
79		–	–		–	–	–				–		–		–	–		79
83		–	–			–					–	–	–	–	–		–	83
89	–			–	–	–	–	–									–	89
97		–	–		–	–		–		–			–			–	–	97
101			–		–		–		–	–	–	–	–					101
103		–	–	–			–				–	–	–					103
107				–		–					–		–	–			–	107
109				–	–	–		–	–	–			–		–	–	–	109
113	–	–	–		–		–	–	–			–			–			113
127		–	–	–	–	–		–								–		127
131	–		–	–		–	–		–	–	–				–	–		131
137		–		–		–	–	–		–	–			–			–	137
139		–				–					–			–	–		–	139
149	–	–	–		–		–		–				–	–	–	–		149
151		–	–	–				–	–	–	–	–						151
157	–	–		–			–		–	–		–						157
163		–	–	–			–			–	–	–				–		163
167					–						–	–	–	–	–	–		167
173	–	–	–		–	–			–	–				–			–	173
179		–		–	–	–		–					–		–	–		179
181	–	–		–		–		–				–	–	–	–			181
191	–	–	–		–			–		–	–						–	191
193	–	–		–			–		–		–	–	–				–	193
197	–	–	–	–		–	–		–	–	–	–					–	197
199	–			–	–		–		–	–	–	–	–	–		–		199
211	–		–		–	–	–		–	–		–	–		–		–	211
223	–			–			–						–				–	223
227		–		–								–	–		–	–		227
	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	

	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	
3	–		–		–		–				–				–	–	3
5				–	–	–		–				–			–		5
7	–		–	–	–				–	–	–		–		–		7
11	–		–	–		–			–			–	–	–	–		11
13	–	–	–	–	–		–			–		–			–	–	13
17	–				–		–			–	–	–	–				17
19	–				–	–	–		–		–					–	19
23	–	–				–			–		–				–	–	23
29	–				–	–	–	–		–			–		–		29
31		–	–		–		–					–	–			–	31
37		–				–	–	–		–		–		–			37
41			–	–				–	–	–				–			41
43	–		–		–			–	–		–	–	–				43
47	–		–	–		–		–	–		–		–		–		47
53			–	–		–	–	–	–	–	–	–		–	–	–	53
59	–		–	–					–	–		–				–	59
61				–	–	–	–				–	–	–		–		61
67		–	–	–					–	–	–	–	–			–	67
71						–		–	–	–		–	–	–		–	71
73				–			–	–	–	–	–					–	73
79		–	–	–	–			–		–	–	–				–	79
83			–	–		–		–		–			–	–	–	–	83
89			–	–		–	–		–			–	–	–		–	89
97							–				–	–				–	97
101		–				–					–		–		–	–	101
103	–	–	–			–		–		–			–	–	–		103
107	–						–	–			–		–			–	107
109		–	–						–	–			–			–	109
113				–	–	–				–	–				–		113
127	–		–	–	–			–		–		–	–	–			127
131		–	–	–		–	–			–			–		–	–	131
137	–	–				–	–	–			–		–		–	–	137
139	–			–				–	–			–	–			–	139
149		–		–	–	–		–	–		–					–	149
151	–		–	–			–			–					–	–	151
157			–	–		–		–		–	–		–		–		157
163				–	–			–	–		–	–					163
167	–		–	–	–	–			–		–					–	167
173		–			–	–				–		–		–	–	–	173
179		–	–	–			–	–	–			–	–	–			179
181					–			–	–	–	–						181
191				–				–			–	–			–		191
193				–	–	–	–	–	–	–	–	–	–	–		–	193
197															–		197
199		–	–	–	–			–	–	–		–		–		–	199
211		–					–		–	–	–			–			211
223		–	–	–		–		–	–							–	223
227				–	–	–	–	–			–	–	–	–		–	227
	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	

	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	
229	–		–				–							–	–			229
233		–		–	–	–		–	–							–	–	233
239				–					–		–	–		–		–		239
241		–	–				–	–		–	–		–			–	–	241
251	–	–				–	–		–		–	–		–	–	–		251
257	–	–	–	–			–	–		–	–			–	–			257
263	–			–		–	–	–			–	–	–	–	–	–	–	263
269	–	–	–			–	–	–	–					–	–	–		269
271			–				–	–	–	–		–	–		–	–	–	271
277	–			–	–		–		–			–		–				277
281		–	–		–	–		–	–	–	–	–	–	–	–	–		281
283	–	–						–	–	–		–		–		–		283
293				–		–	–	–			–	–	–		–			293
307	–			–				–		–	–							307
311	–			–	–	–		–					–	–				311
313	–	–	–	–		–		–			–				–		–	313
317	–				–				–		–		–	–			–	317
331		–	–			–		–	–	–	–	–	–	–		–	–	331
337	–		–	–		–	–	–		–	–	–			–			337
347	–		–		–	–	–	–	–			–			–	–		347
349		–			–		–	–				–						349
353			–	–					–					–	–	–		353
359	–	–	–	–	–					–	–	–		–				359
367			–	–			–	–		–	–				–			367
373		–	–	–	–		–		–	–	–	–	–		–			373
379				–	–						–	–		–	–	–		379
383	–	–	–	–	–		–	–		–	–	–		–				383
389	–	–	–	–				–	–				–	–	–	–		389
397	–			–			–	–	–	–				–	–	–	–	397
401		–		–	–	–			–			–	–	–				401
409	–	–			–		–	–	–					–	–			409
419			–				–		–		–	–		–	–	–	–	419
421			–	–	–	–	–		–		–	–	–	–	–	–		421
431	–	–		–		–		–	–						–	–	–	431
433			–						–	–	–	–	–		–	–		433
439		–				–	–				–		–		–			439
443			–				–	–		–		–	–		–		–	443
449	–	–	–	–	–	–	–				–	–	–	–	–			449
457		–	–						–		–		–	–	–			457
461	–			–	–	–			–	–					–	–	–	461
463	–		–	–	–		–		–		–				–		–	463
467					–			–	–	–			–			–		467
479		–	–		–					–	–		–		–			479
487	–	–			–	–	–	–	–	–			–				–	487
491		–			–	–		–							–	–		491
499	–			–				–	–				–		–		–	499
503				–		–			–		–	–	–				–	503
	769	773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	

	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	
229	–		–	–	–			–		–	–	–	–		–	–	229
233	–		–		–			–	–					–			233
239	–	–			–		–				–	–		–			239
241	–	–		–	–		–				–				–		241
251			–						–		–	–					251
257		–	–	–		–			–		–	–				–	257
263		–		–		–	–				–					–	263
269		–	–									–	–	–		–	269
271	–	–		–	–		–	–	–	–	–	–	–	–	–		271
277	–		–		–		–		–	–	–		–		–		277
281	–		–	–		–		–			–	–		–			281
283	–	–		–	–			–						–			283
293	–				–		–		–		–			–			293
307	–	–	–		–		–		–		–			–	–	–	307
311		–		–			–	–	–	–				–		–	311
313		–	–				–	–	–			–	–	–	–	–	313
317		–	–	–				–	–		–		–		–		317
331		–	–					–		–					–	–	331
337	–		–	–		–	–		–					–		–	337
347			–		–	–	–			–		–		–	–		347
349	–					–	–	–	–	–	–	–	–	–	–		349
353	–	–	–		–	–	–				–	–	–	–	–		353
359	–	–		–			–		–	–		–			–		359
367	–		–			–		–	–			–					367
373	–			–							–	–				–	373
379	–	–	–			–	–		–	–		–	–	–		–	379
383		–			–		–	–			–	–		–	–		383
389			–	–	–		–		–	–		–		–	–		389
397		–						–			–						397
401	–			–					–	–		–	–	–		–	401
409		–	–		–			–		–		–	–			–	409
419	–	–	–	–	–	–				–	–		–	–			419
421		–			–			–	–		–		–		–	–	421
431		–	–	–	–		–			–		–	–	–		–	431
433	–		–		–			–	–			–	–	–			433
439	–	–	–			–		–	–			–	–		–		439
443		–		–			–	–	–	–	–				–	–	443
449		–	–				–		–	–					–	–	449
457		–	–	–				–				–	–				457
461	–							–	–		–	–		–			461
463			–		–			–	–					–	–		463
467					–	–	–	–	–				–	–		–	467
479			–	–	–	–		–			–			–	–		479
487		–		–		–	–		–		–	–		–			487
491		–			–	–			–	–				–	–	–	491
499	–			–	–		–					–		–	–		499
503	–	–			–			–		–		–	–		–		503
	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	

TABLE

FOR CONVERTING

COMMON FRACTIONS WITH DENOMINATORS FROM THE FIRST THOUSAND

INTO DECIMAL FRACTIONS.

3 (1)..6; (0)..3

7 (0)..428571

9 (1)..2; (2)..4; (3)..8; (4)..7; (5)..5; (0)..1

11 (1)..81; (2)..63; (3)..27; (4)..54; (0)..90

13 (1)..615384; (0)..769230

17 (0)..5882352941 176470

19 (0)..5263157894 73684210

23 (0)..4347826086 9565217391 30

27 (1)..740; (2)..481; (3)..962; (4)..925; (5)..851; (0)..370

29 (0)..3448275862 0689655172 41379310

31 (1)..4838709677 41935; (0)..3225806451 61290

37 (1)..351; (2)..756; (3)..783; (4)..918; (5)..594; (6)..972; (7)..864; (8)..324; (9)..621; (10)..108; (11)..540; (0)..270

41 (1)..46341; (2)..78048; (3)..68292; (4)..09756; (5)..58536; (6)..51219; (7)..07317; (0)..24390

43 (1)..5116279069 7674418604 6; (0)..2325581395 3488372093 0

47 (1)..2127659574 4680851063 8297872340 4255319148 936170

49 (0)..2040816326 5306122448 9795918367 3469387755 10

53 (1)..9056603773 584; (2)..5471698113 207; (3)..2264150943 396; (0)..1886792452 830

59 (0)..1694915254 2472881355 9322033898 3050847457 6271186440 67796610

61 (0)..1639344262 2950819672 1311475409 8360655737 7049180327 8688524590

67 (1)..7910447761 1940298507 4626865671 641; (0)..1492537313 4328358208 9552238805 970

71 (1)..7323943661 9718309859 1549295774 64788; (0)..1408450704 2253521126 7605633802 81690

73 (1)..68493150; (2)..42465753; (3)..12328767; (4)..61643835; (5)..08219178; (6)..41095890 (7)..05479452; (8)..27397260; (0)..13698630

79 (1)..6708860759 493; (2)..4556962025 316; (3)..2151898734 177; (4)..2405063291 139; (5)..9746835443 037; (0)..1265822784 810

81 (1)..358024691; (2)..938271604; (3)..320987654; (4)..530864197; (5)..839506172; (0)..123456790

83 (1)..0240963855 4216867469 8795180722 8915662650 6; (0)..1204819277 1084337349 3975903614 4578313253 0

89 (1)..3707865168 5393258426 9662921348 3146067415 7303;
(0)..1123595505 6179775280 8988764044 9438202247 1910

97 (0)..1030927835 0515463917 5257731958 7628865979 3814432989
6907216494 8453608247 4226804123 7113402061 855670

101 (1)..1980; (2)..3960; (3)..7920; (4)..5841; (5)..1683; (6)..3366;
(7)..6732; (8)..3465; (9)..6930; (10)..3861; (11)..7722;
(12)..5445; (13)..0891; (14)..1782; (15)..3564; (16)..7128;
(17)..4257; (18)..8514; (19)..7029; (20)..4059; (21)..8118;
(22)..6237; (23)..2475; (24)..4950; (0)..0990

103 (1)..5825242718 4466019417 4757281553 3980; (2)..4951456310
6796116504 8543689320 3883 (0)..0970873786 4077669902
9126213592 2330

107 (1)..8878504672 8971962616 8224299065 4205607476 6355140186 915
(0)..0934579439 2523364485 9813084112 1495327102 8037383177 570

109 (0)..0917431192 6605504587 1559633027 5229357798 1651376146
7889908256 8807339449 5412844036 6972477064 2201834862 38532110

113 (0)..0884955752 2123893805 3097345132 7433628318 5840707964
6017699115 0442477876 1061946902 6548672566 3716814159
2920353982 30

121 (1)..8925619834 7107438016 52; (2)..2396694214 8760330578 51;
(3)..3884297520 6611570247 93; (4)..5950413223 1404958677 68;
(0)..0826446280 9917355371 90;

127 (1)..3464566929 1338582677 1653543307 0866141732 28;
(2)..7244094488 1889763779 5275590551 1811023622 04;
(0)..0787401574 8031496062 9921259842 5196850393 70

131 (0)..0763358778 6259541984 7328244274 8091603053 4351145038
1679389312 9770992366 4122137404 5801526717 5572519083
9694656488 5496183206 1068702290

137 (1)..87591240; (2)..51094890; (3)..13138686; (4)..57664233;
(5)..91970802; (6)..03649635; (7)..43795620; (8)..25547445;
(9)..06569343; (10)..78832116; (11)..45985401; (12)..51824817;
(13)..21897810; (14)..62773722; (15)..53284671; (16)..39416058;
(0)..07299270

139 (1)..6187050359 7122302158 2733812949 6402877697 841726;
(2)..9208633093 5251798561 1510791366 9064748201 438848;
(0)..0719424460 4316546762 5899280575 5395683453 237410

149 (0)..0671140939 5973154362 4161073825 5033557046 9798657718
1208053691 2751677852 3489932885 9060402684 5637583892
6174496644 2953020134 2281879194 6308724832 21476510

151 (1)..5496688741 7218543046 3576158940 3973509933 7748344370
8609271523 1788079470 19867 (0)..0662251655 6291390728
4768211920 5298013245 0331125827 8145695364 2384105960 26490

157 (1)..1464968152 8662420382 1656050955 4140127388 5350318471
3375796178 3439490445 85987261 (0)..0636942675 1592356687
8980891719 7452229299 3630573248 4076433121 0191082802 54777070

163 (1)..2944785276 0736196319 0184049079 7546012269 9386503067
4846625766 8711656441 7177914110 4 (0)..0613496932 5153374233
1288343558 2822085889 5705521472 3926380368 0981595092
0245398773 0

167 (0)..0598802395 2095808383 2335329341 3173652694 6107784431
1377245508 9820359281 4371257485 0299401197 6047904191
6167664670 6586826347 3053892215 5688622754 4910179640
7185628742 514970

169 (1)..1065088757 3964497041 4201183431 9526627218 9349112426
0355029585 7988165680 47337278 (0)..0591715976 3313609467
4556213017 7514792899 4082840236 6863905325 4437869822 48520710

173 (1)..7398843930 6358381502 8901734104 0462427745 664;
(2)..6705202312 1387283236 9942196531 7919075144 508;
(3)..9826589595 3757225433 5260115606 9364161849 710;
(0)..0578034682 0809248554 9132947976 8786127167 630

179 (0)..0558659217 8770949720 6703910614 5251396648 0446927374
3016759776 5363128491 6201117318 4357541899 4413407821
2290502793 2960893854 7486033519 5530726256 9832402234
6368715083 7988826815 64245810

181 (0)..0552486187 8453038674 0331491712 7071823204 4198895027
6243093922 6519337016 5745856353 5911602209 9447513812
1546961325 9668508287 2928176795 5801104972 3756906077
3480662983 4254143646 4088397790

191 (1)..2198952879 5811518324 6073298429 3193717277 4869109947
6439790575 9162303664 9214659685 8638743455 49738;
(0)..0523560209 4240837696 3350785340 3141361256 5445026178
0104712041 8848167539 2670157068 0628272251 30890

193 (0)..0518134715 0259067357 5129533678 7564766839 3782383419
6891191709 8445595854 9222797927 4611398963 7305699481
8652849740 9326424870 4663212435 2331606217 6165803108
8082901554 4041450777 2020725388 6010362694 30

197 (1)..7055837563 4517766497 4619289340 1015228426 3959390862
9441624365 4822335025 3807106598 9847715736 04060913;
(0)..0507614213 1979695431 4720812182 7411167512 6903553299
4923857868 0203045685 2791878172 5888324873 09644670

199 (1) . . 3819095477 3869346733 6683417085 4271356783 9195979899 4974874371 8592964824 1206030150 7537688442 211055276; (0) . . 0502512562 8140703517 5879396984 9246231155 7788944723 6180904522 6130653266 3316582914 5728643216 080402010

211 (1) . . 3317535545 0236966824 6445497630; (2) . . 3222748815 1658767772 5118483412; (3) . . 2559241706 1611374407 5829383886; (4) . . 7914691943 1279620853 0805687203; (5) . . 5402843601 8957345971 5639810426; (6) . . 7819905213 2701421800 9478672985; (0) . . 0473933649 2890995260 6635071090

223 (0) . . 0448430493 2735426008 9686098654 7085201793 7219730941 7040358744 3946188340 8071748878 9237668161 4349775784 7533632286 9955156950 6726457399 1031390134 5291479820 6278026905 8295964125 5605381165 9192825112 1076233183 8565022421 5246636771 30

227 (1) . . 1806167400 8810572687 2246696035 2422907488 9867841409 6916299559 4713656387 6651982378 8546255506 6079295154 1850220264 317; (0) . . 0440528634 3612334801 7621145374 4493392070 4845814977 9735682819 3832599118 9427312775 3303964757 7092511013 2158590308 370

229 (0) . . 0436681222 7074235807 8602620087 3362445414 8471615720 5240174672 4890829694 3231441048 0349344978 1659388646 2882096069 8689956331 8777292576 4192139737 9912663755 4585152838 4279475982 5327510917 0305676855 8951965065 5021834061 1353711790 39301310

233 (0) . . 0429184549 3562231759 6566523605 1502145922 7467811158 7982832618 0257510729 6137339055 7959914163 0901287553 6480686695 2789799570 8154506437 7682403433 4763948497 8540772532 1888412017 1673819742 4892703862 6609442060 0858369098 7124463519 3133047210 30

239 (1) . . 4644351; (2) . . 2552301; (3) . . 9330543; (4) . . 6569037; (5) . . 9916317; (6) . . 7071129; (7) . . 7489539; (8) . . 2133891; (9) . . 4686192; (10) . . 4016736; (11) . . 0585774; (12) . . 0502092; (13) . . 7573221; (14) . . 5062761; (15) . . 7196652; (16) . . 1882845; (17) . . 5899581; (18) . . 6485355; (19) . . 6987447; (20) . . 4560669; (21) . . 9623430; (22) . . 6820083; (23) . . 8702928; (24) . . 4602510; (25) . . 1087866; (26) . . 8075313; (27) . . 2635983; (28) . . 2259414; (29) . . 9079497; (30) . . 7782426; (31) . . 2384937; (32) . . 3472803; (33) . . 1548117; (0) . . 0418410

241 (1)..5809128630 7053941908 7136929460; (2)..1327800829 8755186721 9917012448; (3)..8589211618 2572614107 8838174273; (4)..0248962655 6016597510 3734439834; (5)..3485477178 4232365145 2282157676; (6)..8796680497 9253112033 1950207468; (7)..3153526970 9543568464 7302904564; (0)..0414937759 3360995850 6224066390

243 (1)..6748971193 4156378600 8230452; (3)..8683127572 0164609053 4979423; (3)..4403292181 0699588477 3662551; (4)..6213991769 5473251028 8065843; (5)..3909465020 5761316872 4279835; (0)..0411522633 7448559670 7818930

251 (1)..4223107569 7211155378 4860557768 9243027888 4462151394; (2)..8764940239 0438247011 9521912350 5976095617 5298804780; (3)..2908366533 8645418326 6932270916 3346613545 8167330677; (4)..2828685258 9641434262 9482071713 1474103585 6573705179; (0)..0398406374 5019920318 7250996015 9362549800 7968127490

257 (0)..0389105058 3657587548 6381322957 1984435797 6653696498 0544747081 7120622568 0933852140 0778210116 7315175097 2762645914 3968871595 3307392996 1089494163 4241245136 1867704280 1556420233 4630350194 5525291828 7937743190 6614785992 2178988326 8482490272 3735408560 3112840466 926070

263 (0)..0380228136 8821292775 6653992395 4372623574 1444866920 1520912547 5285171102 6615969581 7490494296 5779467680 6083650190 1140684410 6463878326 9961977186 3117870722 4334600760 4562737642 5855513307 9847908745 2471482889 7338403041 8250950570 3422053231 9391634980 9885931558 9353612167 30

269 (0)..0371747211 8959107806 6914498141 2639405204 4609665427 5092936802 9739776951 6728624535 3159851301 1152416356 8773234200 7434944237 9182156133 8289962825 2788104089 2193308550 1858736059 4795539033 4572490706 3197026022 3048327137 5464684014 8698884758 3643122676 5799256505 5762081784 38661710

271 (1)..22140; (2)..32841; (3)..97047; (4)..82287; (5)..93726;
(6)..62361; (7)..74169; (8)..45018; (9)..70110; (10)..20664;
(11)..23985; (12)..43911; (13)..63468; (14)..80811; (15)..84870;
(16)..09225; (17)..55350; (18)..32103; (19)..92619; (20)..55719;
(21)..34317; (22)..05904; (23)..35424; (24)..12546; (25)..75276;
(26)..51660; (27)..09963; (28)..59778; (29)..58671; (30)..52029;
(31)..12177; (32)..73062; (33)..38376; (34)..30258; (35)..81549;
(36)..89298; (37)..35793; (38)..14760; (39)..88560; (40)..31365;
(41)..88191; (42)..29151; (43)..74907; (44)..49446; (45)..96678;
(46)..80073; (47)..80442; (48)..82656; (49)..95940; (50)..75645;
(51)..53874; (52)..23447; (53)..39483; (0)..03690

277 (1)..8880866425 9927797833 9350180505 4151624548 7364620938
6281588447 653429602 (2)..0469314079 4223826714 8014440433
2129963898 9169675090 2527075812 274368231 (3)..7545126353
7906137184 1155234657 0397111913 3574007220 2166064981
949458483 (0)..0361010830 3249097472 9241877256 3176895306
8592057761 7328519855 595667870

281 (1)..9217081850 5338078291 81494661; (2)..7722419928 8256227758
00711743; (3)..7010676156 5836298932 38434163; (4)..8576512455
5160142348 75444839; (5)..3131672597 8647686832 74021352;
(6)..9110320284 6975088967 97153024; (7)..1957295373 6654804270
46263345; (8)..5693950177 9359430604 98220640; (9)..7473309608
5409252669 03914590; (0)..0355871886 1209964412 81138790

283 (1)..1519434628 9752650176 6784452296 8197879858 6572438162
5441696113 0742049469 9646643109 5406360424 0282685512
3674911660 7773851590 1060070671 3780918727 9 (0)..0353356890
4593639575 9717314487 6325088339 2226148409 8939929328
6219081272 0848056537 1024734982 3321554770 3180212014
1342756183 7455830388 6925795053 0

289 (0)..0346020761 2456747404 8442906574 3944636678 2006920415
2249134948 0968858131 4878892733 5640138408 3044982698
9619377162 6297577854 6712802768 1660899653 9792387543
2525951557 0934256055 3633217993 0795847750 8650519031
1418685121 1072664359 8615916955 0173010380 6228373702
4221453287 1972318339 10

293 (1)..0375426621 1604095563 1399317406 1433447098 9761092150
1706484641 6382252559 7269624573 3788395904 4368600682
5938566552 9010238907 8498293515 3583617747 440273
(0)..0341296928 3276450511 9453924914 6757679180 8873720136
5187713310 5802047781 5699658703 0716723549 4880546075
0853242320 8191126279 8634812286 6894197952 218430

307 (1) . . 4951140065 1465798045 6026058631 9218241042 3452768729 6416938110 7491856677 5244299674 2671009771 9869706840 3908794788 2736156351 7915309446 2540716612 3778501628 664
(0) . . 0325732899 0228013029 3159609120 5211726384 3648208469 0553745928 3387622149 8371335504 8859934853 4201954397 3941368078 1758957654 7231270358 3061889250 8143322475 570

311 (1) . . 2958199356 9131832797 4276527331 1897106109 3247588424 4372990353 6977491961 4147909967 8456591639 8713826366 5594855305 4662379421 2218649517 6848874598 0707395498 39228
(0) . . 0321543408 3601286173 6334405144 6945337620 5787781350 4823151125 4019292604 5016077170 4180064308 6816720257 2347266881 0289389067 5241157556 2700964630 2250803858 52090

313 (0) . . 0319488817 8913738019 1693290734 8242811501 5974440894 5686900958 4664536741 2140575079 8722044728 4345047923 3226837060 7028753993 6102236421 7252396166 1341853035 1437699680 5111821086 2619808306 7092651757 1884984025 5591054313 0990415335 4632587859 4249201277 9552715654 9520766773 1629392971 2460063897 7635782747 6038338658 1469648562 30

317 (1) . . 2397476340 6940063091 4826498422 7129337539 4321766561 5141955835 9621451104 100946372 (2) . . 0220820189 2744479495 2681388012 6182965299 6845425867 5078864353 3123028391 167192429 (3) . . 5678233438 4858044164 0378548895 8990536277 6025236593 0599369085 1735015772 870662460 (0) . . 0315457413 2492113564 6687697160 8832807570 9779179810 7255520504 7318611987 381703470

331 (1) . . 1178247734 1389728096 6767371601 2084592145 0151057401 8126888217 5226586102 7190332326 2839879154 0785498489 4259818731 (2) . . 3595166163 1419939577 0392749244 7129909365 5589123867 0694864048 3383685800 6042296072 5075528700 9063444108 7613293051 (0) . . 0302114803 6253776435 0453172205 4380664652 5679758308 1570996978 8519637462 2356495468 2779466193 3534743202 4169184290

337 (0) . . 0296735905 0445103857 5667655786 3501483679 5252225519 2878338278 9317507418 3976261127 5964391691 3946587537 0919881305 6379821958 4569732937 6854599406 5281899109 7922848664 6884272997 0326409495 5489614243 3234421364 9851632047 4777448071 2166172106 8249258160 2373887240 3560830860 5341246290 8011869436 2017804154 3026706231 4540059347 1810089020 7715133531 157270

343. (0) . . 0291545189 5043731778 4256559766 7638483965 0145772594 7521865889 2128279883 3819241982 5072886297 3760932944 6064139941 6909620991 2536443148 6880466472 3032069970 8454810495 6268221574 3440233236 1516034985 4227405247 8134110787 1720116618 0758017492 7113702623 9067055393 5860058309 0379008746 3556851311 9533527696 7930

347 (1) . . 6023054755 0432276657 0605187319 8847262247 8386167146 9740634005 7636887608 0691642651 2968299711 8155619596 5417867435 1585014409 2219020172 9106628242 0749279538 9048991354 4668587896 253 (0) . . 0288184438 0403458213 2564841498 5590778097 9827089337 1757925072 0461095100 8645533141 2103746397 6945244956 7723342939 4812680115 2737752161 3832853025 9365994236 3112391930 8357348703 170

.349 (1) . . 3037249283 6676217765 0429799426 9340974212 0343839541 5472779369 6275071633 2378223495 7020057306 5902578796 5616045845 272206 (2) . . 8194842406 8767908309 4555873925 5014326647 5644699140 4011461318 0515759312 3209169054 4412607449 8567335243 5530085959 885386 (0) . . 0286532951 2893982808 0229226361 0315186246 4183381088 8252148997 1346704871 0601719197 7077363896 8481375358 1661891117 478510

353 (1) . . 7932011331 4447592067 9886685552 40; (2) . . 2096317280 4532577903 6827195467 42; (3) . . 8696883852 6912181303 1161473087 81; (4) . . 3512747875 3541076487 2521246458 92; (5) . . 8356940509 9150141643 0594900849 85; (6) . . 3994334277 6203966005 6657223796 03; (7) . . 1841359773 3711048158 6402266288 95; (8) . . 1558073654 3909348441 9263456090 65; (9) . . 3626062322 9461756373 9376770538 24; (10) . . 1529745042 4929178470 2549575070 82; (0) . . 0283286118 9801699716 7138810198 30;

359 (1) . . 3286908077 9944289693 5933147632 3119777158 7743732590 5292479108 6350974930 3621169916 4345403899 7214484679 6657381615 5988857938 7186629526 4623955431 7548746518 1058485821 7270194986 072423398 (0) . . 0278551532 0334261838 4401114206 1281337047 3537604456 8245125348 1894150417 8272980501 3927576601 6713091922 0055710306 4066852367 6880222841 2256267409 4707520891 3649025069 6378830083 565459610

361 (0)..0277008310 2493074792 2437673130 1939058171 7451523545
7063711911 3573407202 2160664819 9445983379 5013850415
5124653739 6121883656 5096952908 5872576177 2853185595
5678670360 1108033240 9972299168 9750692520 7756232686
9806094182 8254847645 4293628808 8642659279 7783933518
0055401662 0498614958 4487534626 0387811634 3490304709
1412742382 2714681440 4432132963 9889196675 90

367 (0)..0272479564 0326975476 8392370572 2070844686 6485013623
9782016348 7738419618 5286103542 2343324250 6811989100
8174386920 9809264305 1771117166 2125340599 4550408719
3460490463 2152588555 8583106267 0299727520 4359673024
5231607629 4277929155 3133514986 3760217983 6512261580
3814713896 4577656675 7493188010 8991825613 0790190735
6948228882 8337874659 4005449591 2806539509 5367847411
4441416893 732970

373 (1)..1983914209 1152815013 4048257372 6541554959 7855227882
0375335120 6434316353 8873994638 0697050938 3378016085
7908847184 9865951742 6273458445 0402144772 1179624664
8793565683 6461126005 3619302949 061662 (0)..0268096514
7453083109 9195710455 7640750670 2412868632 7077747989
2761394101 8766756032 1715817694 3699731903 4852546916
8900804289 5442359249 3297587131 3672922252 0107238605
8981233243 9678284182 305630

379 (0)..0263852242 7440633245 3825857519 7889182058 0474934036
9393139841 6886543535 6200527704 4854881266 4907651715
0395778364 1160949868 0738786279 6833773087 0712401055
4089709762 5329815303 4300791556 7282321899 7361477572
5593667546 1741424802 1108179419 5250659630 6068601583
1134564643 7794722955 1451187335 0923482849 6042216358
8390501319 2612137203 1662269129 2875989445 9102902374
6701846965 6992084432 71767810

383 (0)..0261096605 7441253263 7075718015 6657963446 4751958224
5430809399 4778067885 1174934725 8485639686 6840731070
4960835509 1383812010 4438642297 6501305483 0287206266
3185378590 0783289817 2323759791 1227154046 9973890339
4255874673 6292428198 4334203655 3524804177 5456919060
0522193211 4882506527 4151436031 3315926892 9503916449
0861618798 9556135770 2349869451 6971279373 3681462140
9921671018 2767624020 8877284595 30

389 (0)..0257069408 7403598971 7223650385 6041131105 3984575835
4755784061 6966580976 8637532133 6760925449 8714652956
2982005141 3881748071 9794344473 0077120822 6221079691
5167095115 6812339331 6195372750 6426735218 5089974293
0591259640 1028277634 9614395886 8894601542 4164524421
5938303341 9023136246 7866323907 4550128534 7043701799
4858611825 1928020565 5526992287 9177377892 0308483290
4884318766 0668380462 7249357326 47814910

397 (1)..3501259445 8438287153 6523929471 0327455919 3954659949
6221662468 5138539042 8211586901 7632241813 602015113;
(2)..5667506297 2292191435 7682619647 3551637279 5969773299
7481108312 3425692695 2141057934 5088161209 068010075;
(3)..3778337531 4861460957 1788413098 2367758186 3979848866
4987405541 5617128463 4760705289 6725440806 045340050;
(0)..0251889168 7657430730 4785894206 5491183879 0931989924
4332493702 7707808564 2317380352 6448362720 303022670

401 (1)..7381546134 6633416458 8528678304 2394014962 5935162094
7630922693 2668329177 0573566084 7880299251 8703241895
2618453865 3366583541 1471321695 7605985037 4064837905
2369077306 7331670822 9426433915 2119700748 1296758104
(0)..0249376558 6034912718 2044887780 5486284289 2768079800
4987531172 0698254364 0897755610 9725685785 5361596009
9750623441 3965087281 7955112219 4513715710 7231920199
5012468827 9301745635 9102244389 0274314214 4638403990

409 (1)..2542787286 0635696821 5158924205 3789731051 3447432762
8361858190 7090464547 6772616136 9193154034 2298288508
5574572127 1393643031 7848410757 9462102689 4865525672
3716381418 0929095354 5232273838 6308068459 6577017114 9144
(0)..0244498777 5061124694 3765281173 5941320293 3985330073
3496332518 3374083129 5843520782 3960880195 5990220048
8997555012 2249388753 0562347188 2640586797 0660146699
2665036674 8166259168 7041564792 1760391198 0440097799 5110

419 (0)..0238663484 4868735083 5322195704 0572792362 7684964200
4773269689 7374701670 6443914081 1455847255 3699284009
5465393794 7494033412 8878281622 9116945107 3985680190
9307875894 9880668257 7565632458 2338902147 9713603818
6157517899 7613365155 1312649164 6778042959 4272076372
3150357995 2267303102 6252983293 5560859188 5441527446
3007159904 5346062052 5059665871 1217183770 8830548926
0143198090 6921241050 1183317422 4343675417 6610978520
2863961813 84248210

421 (1)..2826603325 4156769596 1995249406 1757719714 .9643705463 1828978622 3277909738 7173396674 5843230403 8004750593 8242280285 0356294536 8171021377 6722090261 (2)..2636579572 4465558194 7743467933 4916864608 0760095011 8764845605 7007125890 7363420427 5534441805 2256532066 5083135391 9239904988 1235154394 2992874109 (0)..0237529691 2114014251 7814726840 8551068883 6104513064 1330166270 7838479809 9762470308 7885985748 2185273159 1448931116 3895486935 8669833729 2161520190

431 (1)..4872389791 1832946635 7308584686 7749419953 5962877030 1624129930 3944315545 2436194895 5916473317 8654292343 3874709976 7981438515 0812064965 1972197772 6218097447 7958236658 9327146171 6937354988 3990719257 5406032482 5986078886 31090 (0)..0232018561 4849187935 0348027842 2273781902 5522041763 3410672853 8283062645 0116009280 7424593967 5174013921 1136890951 2761020881 6705336426 9141531322 5058004640 3712296983 7587006960 5568445475 6380510440 8352668213 4570765661 25290

433 (0)..0230946882 2170900692 8406466512 7020785219 3995381062 3556581986 1431870669 7459584295 6120092378 7528868360 2771362586 6050808314 0877598152 4249422632 7944572748 2678983833 7182448036 9515011547 3441108545 0346420323 3256351039 2609699769 0531177829 0993071593 5334872979 2147806004 6189376443 4180138568 1293302540 4157043879 9076212471 1316397228 6374133949 1916859122 4018475750 5773672055 4272517321 0161662817 5519630484 9884526558 8914549653 5796766743 6489607390 30

439 (1)..4920273348 5193621867 8815489749 4305239179 9544419134 3963553530 7517084282 4601366742 5968109339 4077448747 1526195899 7722095671 9817767653 7585421412 3006833712 9840546697 0387243735 7630979498 8610478359 9088838268 7927107061 503416856 (0)..0227790432 8018223234 6241457858 7699316628 7015945330 2961275626 4236902050 1138952164 0091116173 1207289293 8496583143 5079726651 4806378132 1184510250 5694760820 0455580865 6036446469 2482915717 5398633257 4031890660 5922551252 847380410

443 (1)..4176072234 7629796839 7291196388 2618510158 0135440180 5869574492 0993227990 9706546275 3950338600 4514672686 2302483069 9774266365 6884875846 5011286681 7155756207 6749435665 9142212189 6162528216 7042889390 5191873589 1647855530 4740406320 5 (0)..0225733634 3115124153 4988713318 2844243792 3250564334 0857787810 3837471783 2957110609 4808126410 8352144469 5259593679 4582392776 5237020316 0270880361 1738148984 1986455981 9413092550 7900677200 9029345372 4604966139 9548532731 3769751693 0

449 (1)..7572383073 4966592427 6169265033 40; (2)..7461024498 8864142538 9755011135 85; (3)..3674832962 1380846325 1670378619 15; (4)..4944320712 6948775055 6792873051 22; (5)..8106904231 6258351893 0957683741 64; (6)..5634743875 2783964365 2561247216 03; (7)..1581291759 4654788418 7082405345 21; (8)..3763919821 8262806236 0801781737 19; (9)..7973273942 0935412026 7260579064 58; (10)..1091314031 1804008908 6859688195 99; (11)..7104677060 1336302895 3229398663 69; (12)..1559020044 5434298440 9799554565 70; (13)..3006681514 4766146993 3184855233 85; (0)..0222717149 2204899777 2828507795 10

457 (1)..7768052516 4113785557 9868708971 5536105032 8227571115 9737417943 1072210065 6455142231 9474835886 2144420131 2910284463 8949671772 4288840262 5820568927 7899343544 85 (2)..0765864332 6039387308 5339168490 1531728665 2078774617 0678336980 3063457330 4157549234 1356673960 6126914660 8315098468 2713347921 2253829321 6630196936 5426695842 45 (0)..0218818380 7439824945 2954048140 0437636761 4879649890 5908096280 0875273522 9759299781 1816192560 1750547045 9518599562 3632385120 3501094091 9037199124 7264770240 70

461 (0)..0216919739 6963123644 2516268980 .4772234273 3188720173 5357917570 4989154013 0151843817 7874186550 9761388286 3340563991 3232104121 4750542299 3492407809 1106290672 4511930585 6832971800 4338394793 9262472885 0325379609 5444685466 3774403470 7158351409 9783080260 3036876355 7483731019 5227765726 6811279826 4642082429 5010845986 9848156182 2125813449 0238611713 6659436008 6767895878 5249457700 6507592190 8893709327 5488069414 3167028199 5661605206 0737527114 9674620390 4555314533 6225596529 2841648590

463 (1) . . 7580993520 5183585313 1749460043 1965442764 5788336933
0453563714 9028077753 7796976241 9006479481 6414686825
0539956803 4557235421 1663066954 6436285097 1922246220 3023
(2) . . 9092872570 1943844492 4406047516 1987041036 7170626349
8920086393 0885529157 6673866090 7127429805 6155507559
3952483801 2958963282 9373650107 9913606911 4470842332 6133
(0) . . 0215982721 3822894168 4665226781 8574514038 8768898488
1209503239 7408207343 4125269978 4017278617 7105831533
4773218142 5485961123 1101511879 0496760259 1792656587 4730

Divisor	3 9 11 13 27 31 37 41 43 53 67 71 73 79 81 83 89 101
Primitive root . .	2 2 2 6 2 17 5 6 28 26 12 62 5 29 11 50 30 2

Divisor	103 107 121 127 137 139 151 157 163 169 173 191 197 199 211
Primitive root . .	6 63 35 106 12 92 114 18 70 137 82 157 73 127 7

Divisor	227 239 241 243 251 271 277 281 283 293 307 311 317 331 347
Primitive root . .	163 35 14 65 111 6 80 54 259 89 138 258 71 37 125

Divisor	349 353 359 373 397 401 409 421 431 439 443 449 457 463
Primitive root . .	220 28 299 82 133 190 174 54 21 285 240 34 264 174

467 2141327623 1263383297 6445396145 6102783725 9100642398
2869379014 9892933618 8436830835 1177730192 7194860813
7044967880 0856531049 2505353319 0578158458 2441113490
3640256959 3147751605 9957173447 5374732334 0471092077
0877944325 4817987152 0342612419 700<u>2141327</u> . . . . .

479 2087682672 2338204592 9018789144 0501043841 3361169102
2964509394 5720250521 9206680584 5511482254 6972860125
2609603340 2922755741 1273486430 0626304801 6701461377
8705636743 2150313152 4008350730 6889352818 3716075156
5762004175 3653444676 4091858037 5782881002 . . . . .

487 2053388090 3490759753 5934291581 1088295687 8850102669
4045174537 9876796714 5790554414 7843942505 1334702258
7268993839 8357289527 7207392197 1252566735 1129363449
6919917864 4763860369 6098562628 3367556468 1724845995
8932238193 0184804928 1314163377 8234086242 2997946611
9096509240 2464065708 4188911704 3121149897 3305954825
4620123203 2854209445 5852156057 4948665297 7412731006
1601642710 4722792607 8028747433 2648870636 5503080082
1355236139 6303901437 3716632443 5318275154 0041067761
8069815195 0718685831 6221765913 757700<u>2053</u> . . .

491 2036659877 8004073319 7556008146 6395112016 2932790224
0325865580 4480651731 1608961303 4623217922 6069246435
8452138492 8716904276 9857433808 5539714867 6171079429
7352342158 8594704684 3177189409 3686354378 8187372708
7576374745 4175152749 4908350305 4989816700 6109979633
4012219959 2668024439 9185336048 8798370672 0977596741
3441955193 4826883910 3869653767 8207739307 5356415478
6150712830 9572301425 6619144602 8513238289 2057026476
5784114052 9531568228 1059063136 4562118126 2729124236
2525458248 4725050916 4969450101 8329938900 . . .

499 2004008016 0320641282 5651302605 2104208416 8336673346
6933867735 4709418837 6753507014 0280561122 2444889779
5591182364 7294589178 3567134268 5370741482 9659318637
2745490981 9639278557 1142284569 1382765531 0621242484
9699398797 5951903807 6152304609 2184368737 4749498997
9959919839 6793587174 3486973947 8957915831 6633266533
0661322645 2905811623 2464929859 7194388777 5551102204
4088176352 7054108216 4328657314 6292585170 3406813627
2545090180 3607214428 8577154308 6172344689 3787575150
3006012024 0480961923 8476953907 8156312625 2505010020 . . . .

503 1988071570 5765407554 6719681908 5487077534 7912524850
8946322067 5944333996 0238568588 4691848906 5606361829
0258449304 1749502982 1073558648 1113320079 5228628230
6163021868 7872763419 4831013916 5009940357 8528827037
7733598409 5427435387 6739562624 2544731610 3379721669
9801192842 9423459244 5328031809 1451292246 5208747514
9105367793 2405566600 3976143141 1530815109 3439363817
0974155069 5825049701 7892644135 1888667992 0477137176
9383697813 1212723658 0516898608 3499005964 2147117296
2226640159 0457256461 2326043737 5745526838 9662027833
00<u>19880715</u> . . . . .

509 1964636542 2396856581 5324165029 4695481335 9528487229
8624754420 4322200392 9273084479 3713163064 8330058939
0962671905 6974459724 9508840864 4400785854 6168958742
6326129666 0117878192 5343811394 8919449901 7681728880
1571709233 7917485265 2259332023 5756385068 7622789783
8899803536 3457760314 3418467583 4970530451 8664047151
2770137524 5579567779 9607072691 5520628683 6935166994
1060903732 8094302554 0275049115 9135559921 4145383104
1257367387 0333988212 1807465618 8605108055 0098231827
1119842829 0766208251 4734774066 7976424361 4931237721
021611001<u>9</u> . . . . .

521 1919385796 5451055662 1880998080 6142034548 9443378119
00191938 57 ....

523 1912045889 1013384321 2237093690 2485659655 8317399617
5908221797 3231357552 5812619502 8680688336 5200764818
3556405353 7284894837 4760994263 8623326959 8470363288
7189292543 0210325047 8011472275 3346080305 9273422562
1414913957 9349904397 7055449330 7839388145 3154875717
0172084130 01912045 88 .....

529 1890359168 2419659735 3497164461 2476370510 3969754253
3081285444 2344045368 6200378071 8336483931 9470699432
8922495274 1020793950 8506616257 0888468809 0737240075
6143667296 7863894139 8865784499 0548204158 7901701323
2514177693 7618147448 0151228733 4593572778 8279773156
8998109640 8317580340 2646502835 5387523629 4896030245
7466918714 5557655954 6313799621 9281663516 0680529300
5671077504 7258979206 0491493383 7429111531 1909262759
9243856332 7032136105 8601134215 5009451795 8412098298
6767485822 3062381852 5519848771 2665406427 2211720226
84310018 90 ....

541 1848428835 4898336414 0480591497 2273567467 6524953789
2791127541 5896487985 2125693160 8133086876 1552680221
8114602587 8003696857 6709796672 8280961182 9944547134
9353049907 5785582255 0831792975 9704251386 3216266173
7523105360 4436229205 1756007393 7153419593 3456561922
3659889094 2698706099 8151571164 5101663385 9519408502
7726432532 3475046210 7208872458 4103512014 7874306839
1866913123 8447319778 1885397412 1996303142 3290203327
1719038817 0055452865 0646950092 4214417744 9168207024
0295748613 6783733826 2476894639 5563770794 8243992606
2846580406 6543438077 6340110905 7301293900 1848428835 ....

547 1828153564 8994515539 3053016453 3820840950 6398537477
1480804387 5685557586 8372943327 2394881170 01828153 56 ....

557 1795332136 4452423698 3842010771 9928186714 5421903052
0646319569 1202872531 4183123877 9174147217 2351885098
7432675044 8833034111 3105924596 0502692998 2046678635
5475763016 1579892280 0718132854 5780969479 3536804308
7971274685 8168761220 8258527827 6481149012 5673249551
1669658886 8940754039 4973070017 ....

563 1776198934 2806394316 1634103019 5381882770 8703374777
9751332149 2007104795 7371225577 2646536412 0781527531
0834813499 1119005328 5968028419 1829484902 3090586145
6483126110 1243339253 9964476021 3143872113 6767317939
6092362344 5825932504 4404973357 0159857904 0852575488
4547069271 7584369449 3783303730 01̲77619893̲ . . . . .

569 1757469244 2882249560 6326889279 4376098418 2776801405
9753954305 7996485061 5114235500 8787346221 4411247803
1634446397 1880492091 3884007029 8769771528 9982425307
5571177504 3936731107 2056239015 8172231985 9402460456
9420035149 3848857644 9912126537 7855887521 9683655536
0281195079 0861159929 7012302284 7100175746̲ . . . .

571 1751313485 1138353765 3239929947 4605954465 8493870402
8021015761 8213660245 1838879159 3695271453 5901926444
8336252189 1418563922 9422066549 9124343257 4430823117
3380035026 2697022767 0753064798 5989492119 0893169877
4080560420 3152364273 2049036777 5831873905 4290718038
5288966725 0437828371 2784588441 3309982486 8651488616
4623467600 7005253940 4553415061 2959719789 8423817863
3975481611 2084063047 2854640980 7355516637 4781085814
3607705779 3345008756 5674255691 7688266199 6497373029
7723292469 3520140105 0788091068 3012259194 3957968476
3572679509 6322241681 2609457092 8196147110 3327495621
7162872154 1155866900 1̲751313485 . . . .

577 1733102253 0329289428 0762564991 3344887348 3535528596
1871750433 2755632582 3223570190 6412478336 2218370883
8821490467 9376083188 9081455805 8925476603 1195840554
5927209705 3726169844 0207972270 3639514731 3691507798
9601386481 8024263431 5424610051 9930675909 8786828422
8769497400 3466204506 0658578856 1525129982 6689774696
7071057192 3743500866 5511265164 6447140381 2824956672
4436741767 7642980935 8752166377 8162911611 7850953206
2391681109 1854419410 7452339688 0415944540 7279029462
7383015597 9202772963 6048526863 0849220103 9861351819
7573656845 7538994800 6932409012 1317157712 3050259965
3379549393 4142114384 7487001̲733 . . . .

587 1703577512 7768313458 2623509369 1763202725 7240204429
3015332197 6149914821 1243611584 3270868824 5315161839
8637137989 7785349233 3901192504 2589437819 4207836456
5587734241 9080068143 1005110732 5383304940 3747870528
1090289608 1771720613 2879045996 5928449744 4633730834
7529812606 4735945485 5195911413 9693356047 7001703577 ....

593 1686340640 8094435075 8853288364 2495784148 3979763912
3102866779 0893760539 6290050590 2192242833 0522765598
6509274873 5244519392 9173693086 0033726812 8161888701
5177065767 2849915682 9679595278 2462057335 5817875210
7925801011 8043844856 6610455311 9730185497 4704890387
8583473861 7200674536 2563237774 0303541315 3456998313
6593591905 5649241146 7116357504 2158516020 2360876897
1332209106 2394603709 9494097807 7571669477 2344013490
7251264755 4806070826 3069139966 2731871838 1112984822
9342327150 0843170320 4047217537 9426644182 1247892074
1989881956 1551433389 5446880269 8145025295 1096121416
5261382799 3254637436 7622259696 4586846543 0016863406 ....

599 1669449081 8030050083 4724540901 5025041736 2270450751
2520868113 5225375626 0434056761 2687813021 7028380634
3906510851 4190317195 3255425709 5158597662 7712854757
9298831385 6427378964 9415692821 3689482470 7846410684
4741235392 3205342237 0617696160 2671118530 8848080133
5559265442 4040066777 9632721202 0033388981 6360601001 ....

601 1663893510 8153078202 9950083194 6755407653 9101497504
1597337770 3826955074 8752079866 8885191347 7537437603
9933444259 5673876871 8801996672 2129783693 8435940099
8336106489 1846921797 0049916805 3244592346 0898502495
8402662229 6173044925 1247920133 1114808652 2462562396
0066555740 4326123128 1198003327 7870216306 1564059900
1663893510 ...

607 1647446457 9901153212 5205930807 2487644151 5650741350
9060955518 9456342668 8632619439 8682042833 6079077429
9835255354 2009884678 7479406919 2751235584 8434925864
9093904448 1054365733 1136738056 0131795716 6392092257
0016474464 ....

613 1631321370 3099510603 5889070146 8189233278 9559543230
0163132137 ....

617 1620745542 9497568881 6855753646 6774716369 5299837925
4457050243 1118314424 6353322528 3630470016 ....

619 1615508885 2988691437 8029079159 9353796445 8804523424
8788368336 0258481421 6478190630 0484652665 5896607431
3408723747 9806138933 7641357027 4636510500 8077544426
4943457189 0145395799 6768982229 4022617124 3941841680
1292407108 2390953150 2423263327 9483037156 7043618739
9030694668 8206785137 3182552504 0387722132 4717235945
0726978998 3844911147 0113085621 9709208400 6462035541
1954765751 2116316639 7415185783 5218093699 5153473344
1033925686 5912762520 1938610662 3586429725 3634894991
9224555735 0565428109 8546042003 2310177705 9773828756
0581583198 7075928917 6090468497 5767366720 5169628432
9563812600 9693053311 7932148626 8174474959 6122778675
2827140549 2730210016 . . . .

631 1584786053 8827258320 1267828843 1061806656 1014263074
4849445324 8811410459 5879556259 9049128367 6703645007
9239302694 1362916006 3391442155 3090332805 0713153724
2472266244 0570522979 3977812995 2456418383 5182250396
1965134706 8145800316 9572107765 4516640253 5657686212
3613312202 8526148969 8890649762 2820919175 9112519809
8256735340 7290015847 . . . .

641 1560062402 4960998439 9375975039 0015600624 . .

643 1555209953 3437013996 8895800933 1259720062 2083981337
4805598755 8320373250 3888024883 3592534992 2239502332
8149300155 . . . .

647 1545595054 0958268933 5394126738 7944358578 0525502318
3925811437 4034003091 1901081916 5378670788 2534775888
7171561051 0046367851 6228748068 0061823802 1638330757
3415765069 5517774343 1221020092 7357032457 4961360123
6476043276 6615146831 5301391035 5486862442 0401854714
0649149922 7202472952 0865533230 2936630602 7820710973
7248840803 7094281298 2998454404 9459041731 0664605873
2612055641 4219474497 6816074188 5625965996 9088098918
0834621329 2117465224 1112828438 9489953632 1483771251
9319938176 1978361669 2426584234 9304482225 6568778979
9072642967 5425038639 8763523956 7233384853 1684698608
9644513137 5579598145 2859350850 0772797527 0479134466
7697063369 3972179289 0262751159 1962905718 7017001545 . . . .

653 1531393568 1470137825 4211322312 4042879019 9081163859
1117917304 7473200612 5574272588 0551301684 5329249617
1516079632 4655436447 1669218989 2802450229 7090352220
5206738131 6998468606 4318529862 1745788667 6875957120
9800918836 1408882082 6952526799 3874425727 4119448698
3154670750 3828483920 3675344563 5528330781 0107197549
7702909647 7794793261 868300<u>1531</u> . . . .

659 1517450682 · 8528072837 6327769347 4962063732 9286798179
0591805766 3125948406 6767830045 5235204855 8421851289
8330804248 8619119878 6039453717 7541729893 7784522003
0349013657 0561456752 6555386949 9241274658 5735963581
1836115326 2518968133 5356600910 4704097116 8437025796
6616084977 2382397572 0789074355 0834597875 5690440060
6980273141 1229135053 1107738998 4825493171 4719271623
6722306525 0379362670 7132018209 4081942336 8740515933
2321699544 7647951441 5781487101 6691957511 3808801213
9605462822 4582701062 2154779969 6509863429 4385432473
4446130500 7587253414 2640364188 1638846737 4810318664
6433990895 2959028831 5629742033 3839150227 6176024279
2109256449 1654021244 3095599393 0197268588 7708649468
892261001<u>5</u> . . . .

661 1512859304 0847201210 2874432677 7609682299 5461422087
7458396369 1376701966 7170953101 3615733736 7624810892
5869894099 8487140695 9152798789 7125567322 2390317700
4538577912 2541603630 8623298033 2829046898 6384266263
2375189107 4130105900 <u>15</u>12859304 . . . .

673 1485884101 0401188707 2808320950 9658246656 7607726597
3254086181 2778603268 9450222882 6151560178 3060921248
1426448736 9985141158 9895988112 9271916790 4903417533
4323922734 0267459138 1872213967 3105497771 1738484398
2169390787 5185735512 6300148588 . . . .

677 1477104874 4460856720 8271787296 8980797636 6322008862
6292466765 1403249630 7237813884 7858197932 0531757754
8005908419 4977843426 8833087149 1875923190 5465288035
4505169867 0605612998 5228951255 5391432791 7282127031
0192023633 6779911373 7075332348 5967503692 7621861152
1418020679 4682422451 9940915805 0221565731 1669128508
1240768094 5347119645 4948301329 394387001<u>4</u> . . . .

683 1464128843 3382137628 1112737920 9370424597 3645680819
9121522693 9970717423 1332357247 4377745241 5812591508
0527086383 6017569546 1200585651 5373352855 0512445095
1683748169 8389458272 3279648609 0775988286 9692532942
8989751098 0966325036 6032210834 5534407027 8184480234
2606149341 1420204978 0380673499 2679355783 3089311859
4436310395 3147877013 1771595900 4392386530 0146412884 ....

691 1447178002 8943560057 8871201157 7424023154 8480463096
9609261939 2185238784 3704775687 4095513748 1910274963
8205499276 4109985528 2199710564 3994211287 9884225759
7684515195 3690303907 3806078147 6121562952 2431259044
8625180897 2503617945 0072358900 1447178022 ....

701 1426533523 5378031383 7375178316 6904422253 9229671897
2895863052 7817403708 9871611982 8815977175 4636233951
4978601997 1469329529 2439372325 2496433666 1911554921
5406562054 2082738944 3651925820 2567760342 3680456490
7275320970 0427960057 0613409415 1212553495 0071326676
1768901569 1868758915 8345221112 6961483594 8644793152
6390870185 4493580599 1440798858 7731811697 5748930099
8573466476 4621968616 2624821683 3095577746 0770328102
7104136947 2182596291 0128388017 1184022824 5363766048
5021398002 8530670470 7560627674 7503566333 8088445078
4593437945 7917261055 6348074179 7432239657 6319543509
2724679029 9572039942 9386590584 8787446504 9928673323
8231098430 8131241084 1654778887 3038516405 1355206847
3609129814 5506419400 8559201141 2268188302 4251069900 ....

709 1410437235 5430183356 8406205923 8363892806 7700987306
0648801128 3497884344 1466854724 9647390691 1142454160
7898448519 0409026798 3074753173 4837799717 9125528913
9633286318 7588152327 2214386459 8025387870 2397743300
4231311706 6290550070 5218617771 5091678420 3102961918
1946403385 0493653032 4400564174 8942172073 3427362482
3695345557 1227080394 9224259520 4513399153 7376586741
8899858956 2764456981 6643159379 4076163610 7193229901
2693935119 8871650211 5655853314 5275035260 9308885754
5839210155 1480959097 3201692524 6826516220 0282087447
1086036671 3681241184 7672778561 3540197461 2129760225
6699576868 8293370944 9929478138 2228490832 1579689703
8081805359 6614950634 6967559943 5825105782 7926657263
7517630465 4442877291 9605077574 0479548660 0846262341
3258110014 ....

719 1390320584 1446453407 5104311543 8108484005 5632823365
7858136300 4172461752 4339360222 5312934631 4325452016
6898470097 3574408901 2517385257 3018080667 5938803894
2976356050 0695410292 0723226703 7552155771 9054242002
7816411682 8929068150 2086230876 2169680111 2656467315
7162726008 3449235048 6787204450 6258692628 6509040333
7969401947 1488178025 0347705146 0361613351 8776077885
9527121001 ....

727 1375515818 4319119669 8762035763 4112792297 1114167812
9298486932 5997248968 3631361760 6602475928 4731774415
4057771664 3741403026 1348005502 0632737276 4786795048
1430536451 1691884456 6712517193 9477303988 9958734525
4470426409 9037138927 0976616231 0866574965 6121045392
0220082530 9491059147 1801925722 1458046767 5378266850
0687757909 2159559834 9381017881 7056396148 5557083906
4649243466 2998624484 1815680880 3301237964 2365887207
7028885832 1870701513 0674002751 0316368638 2393397524
0715268225 5845942228 3356258596 9738651994 4979367262
7235213204 9518569463 5488308115 5433287482 8060522696
0110041265 4745529573 5900962861 0729023383 7689133425
0343878954 6079779917 4690508940 8528198074 2778541953
2324621733 1499312242 0907840440 1650618982 1182943603
8514442916 0935350756 5337001375 ....

729 1371742112 4828532235 9396433470 5075445816 1865569272
9766803840 8779149519 8902606310 0137174211

733 1364256480 2182810368 3492496589 3587994542 9740791268
7585266030 0136425648 ....

739 1353179972 9364005412 7198917456 0216508795 6698240866
0351826792 9634641407 3071718538 5656292286 8741542625
1691474966 1705006765 8998646820 0270635994 5872801082
5439783491 2043301759 1339648173 2070365358 5926928281
4614343707 7131258457 3748308525 0338294993 2341001353 ....

743 1345895020 1884253028 2637954239 5693135935 3970390309
5558546433 3781965006 7294751009 4212651413 1897711978
4656796769 8519515477 7927321668 9098250336 4737550471
0632570659 4885598923 2839838492 5975773889 6366083445
4912516823 6877523553 1628532974 4279946164 1991924629
8788694481 8304172274 5625841184 3876177658 1426648721
3997308209 9596231493 9434724091 5208613728 1292059219
3808882907 1332436069 9865410497 9811574697 1736204576
0430686406 4602960969 0444145356 6621803499 3270524899
0578734858 6810228802 1534320323 0148048452 2207267833
1090174966 3526244952 8936742934 0511440107 6716016150
7402422611 0363391655 4508748317 6312247644 6837146702
5572005383 5800807537 0121130551 8169582772 5437415881
5612382234 1857335127 8600269179 0040376850 6056527590
8479138627 1870794078 0619111709 2866756393 0013458950 ....

751 1331557922 7696404793 6085219707 0572569906 7909454061
2516644474 0346205059 9201065246 3382157123 8348868175
7656458055 9254327563 2490013315 ....

757 1321003963 0118890356 6710700132 ....

761 1314060446 7805519053 8764783180 0262812089 3561103810
7752956636 0052562417 8712220762 1550591327 2010512483
5742444152 4310118265 4402102496 7148488830 4862023653
0880420499 3429697766 0972404730 6176084099 8685939553
2194480946 1235216819 9737187910 6438896189 2247043363
9947437582 1287779237 8449408672 7989487516 4257555847
5689881734 5597897503 2851511169 5137976346 9119579500
6570302233 9027595269 3823915900 1314060446 ....

769 1300390117 0351105331 5994798439 5318595578 6736020806
2418725617 6853055916 7750325097 5292587776 3328998699
6098829648 8946684005 2015604681 4044213263 9791937581
2743823146 9440832249 6749024707 4122236671 0013003901 ....

773 1293661060 8020698576 9728331177 2315653298 8357050452
7813712807 2445019404 9159120310 4786545924 9676584734
7994825355 7567917205 6921096675 2910737386 8046571798
1888745148 7710219922 3803363518 7580853816 3001293661 ....

787 1270648030 4955527318 9326556543 8373570520 9656925031
7662007623 8881829733 1639135959 3392630241 4231257941
5501905972 0457433290 9783989834 8157560355 7814485387
5476493011 4358322744 5997458703 9390088945 3621346886
9123252858 9580686149 9364675984 7522236340 5336721728
0813214739 5171537484 1168996188 0559085133 4180432020
3303684879 2884371029 2249047013 9771283354 5108005082
5921219822 1092757306 2261753494 2820838627 700$\underline{12}$70648 ....

797 1254705144 2910915934 7553324968 6323713927 2271016311
1668757841 9071518193 2245922208 2810539523 2120451693
8519447929 7365119196 9887076537 0138017565 8720200752
8230865746 5495608531 9949811794 2283563362 6097867001 ....

809 1236093943 1396786155 7478368355 9950556242 2744128553
7700865265 7601977750 3090234857 8491965389 3695920889
9876390605 6860321384 4252163164 4004944375 7725587144
6229913473 4239802224 9690976514 2150803461 0630407911
00$\underline{12360939}$ ....

811 1233045622 6880394574 5992601726 2638717632 5524044389
6424167694 2046855733 6621454993 8347718865 5980271270
0369913686 8064118372 3797780517 8791615289 7657213316
8927250308 2614056720 0986436498 1504315659 6794081381
0110974106 0419235511 7139334155 3637484586 9297163995
0678175092 4784217016 0295930949 4451294697 9038224414
3033292231 8125770653 5141800246 6091245376 0789149198
5203452527 7435265104 8088779284 8335388409 3711467324
2909987669 5437731196 0542540073 9827373612 8236744759
5561035758 3230579531 4426633785 4500616522 8113440197
2872996300 8631319358 8162762022 1948212083 8471023427
8668310727 4969173859 4327990135 6350184956 8434032059
1861898890 2589395807 6448828606 6584463625 1541307028
3600493218 2490752157 8298397040 6905055487 0530209617
7558569667 0776818742 2934648581 9975339087 5462392108
5080147965 4747225647 3489519112 2071516646 1159062885
3267570900 123$\underline{304}5\underline{662}$ ....

821 1218026796 5895249695 4933008526 1875761266 7478684531
0596833130 3288672350 7917174177 8319123020 7064555420
2192448233 8611449451 8879415347 1376370280 1461632155
9074299634 5919610231 4250913520 0974421437 2716199756
3946406820 9500609013 3982947624 8477466504 2630937880
6333739342 2655298416 5651644336 1753958587 0889159561
5103532277 7101096224 1169305724 7259439707 6735688185
1400730816 0779537149 8172959805 1157125456 7600487210
7186358099 8781973203 4104750304 5066991473 8124238733
2521315468 9403166869 6711327649 2082825822 1680876979
2935444579 7807551766 1388550548 1120584652 8623629719
8538367844 0925700365 4080389768 5749086479 9025578562
7283800243 6053593179 0499390986 6017052375 1522533495
7369062119 3666260657 7344701583 4348355663 8246041412
9110840438 4896467722 2898903775 8830694275 2740560292
3264311814 8599269183 9220462850 1827040194 8842874543
2399512789 2813641900 1218026796 ....

823 1215066828 6755771567 4362089914 9453219927 0959902794
6537059538 2746051032 8068043742 4058323207 7764277035
2369380315 9173754556 5006075334 1433778857 8371810449
5747266099 6354799513 9732685297 6913730255 1640340218
7120291616 0388821385 1761846901 5795868772 7825030376
6707168894 2891859052 2478736330 4981773997 5698663426
4884568651 2758201701 0935601458 0801944106 9258809234
5078979343 8639125151 8833535844 4714459295 2612393681
6524908869 9878493317 1324422843 2563791008 5054678007
2904009720 5346294046 1725394896 7193195625 7594167679
2223572296 4763061968 4082624544 3499392466 5856622114
2162818955 0425273390 0364520048 6026731470 2308626974
4835965978 1287970838 3961117861 4823815309 8420413122
7217496962 3329283110 5710814094 7752126366 9501822600
2430133657 3511543134 8724179829 8906439854 1919805589
3074119076 5492102065 6136087484 8116646415 5528554070
4738760631 8347509113 0012150668 ....

827 1209189842 8053204353 0834340991 5356711003 6275695284
1596130592 5030229746 0701330108 8270858524 7883917775
0906892382 1039903264 8125755743 6517533252 7206771463
1197097944 3772672309 5525997581 6203143893 5912938331
3180169286 5779927448 6094316807 7388149939 5405078597
3397823458 2829504232 1644498186 2152357920 1934703748
4885126964 9334945586 4570737605 8041112454 6553808948
0048367593 7122128174 1233373639 6614268440 1451027811
3663845223 700$\underline{1209189}$ ....

829 1206272617 6115802171 2907117008 4439083232 8106151990
3498190591 0735826296 7430639324 4873341375 1507840772
0144752714 1133896260 5548854041 0132689987 9372738238
8419782870 9288299155 6091676718 9384800965 0180940892
6417370325 6936067551 2665862484 9215922798 5524728588
6610373944 5114595898 6731001206 ....

839 1191895113 2300357568 5339690107 2705601907 0321811680
5721096543 5041716328 9630512514 8986889153 7544696066
7461263408 8200238379 0226460071 5137067938 0214541120
3814064362 3361144219 3087008343 2657926102 5029797377
8307508939 2133492252 6817640047 6758045292 0143027413
5876042908 2240762812 8724672228 8438617401 6686531585
2205005959 4755661501 7878426698 4505363528 0095351609
0584028605 4827175208 5816448152 5625744934 4457687723
4803337306 3170441001 ....

841 1189060642 0927467300 8323424494 6492271105 8263971462
5445897740 7847800237 8121284185 4934601664 6848989298
4542211652 7942925089 1795481569 5600475624 2568370986
9203329369 7978596908 4423305588 5850178359 0963139120
0951248513 6741973840 6658739595 7193816884 6611177170
0356718192 6278240190 2497027348 3947681331 7479191438
7633769322 2354340071 3436385255 6480380499 4054696789
5362663495 8382877526 7538644470 8680142687 2770511296
0760998810 9393579072 5326991676 5755053507 7288941736
0285374554 1022592152 1997621878 7158145065 3983353151
0107015457 7883472057 0749108204 5184304399 5243757431
6290130796 6706302021 4030915576 6944114149 8216409036
8608799048 7514863258 0261593341 2604042806 1831153388
8228299643 2818073721 7598097502 9726516052 3186682520
8085612366 2306777645 6599286563 6147443519 6195005945
3032104637 3365041617 1224732461 3555291319 8573127229
4887039239 00$\underline{11890}\underline{606}$ ....

853 1172332942 5556858147 7139507620 1641266119 5779601406
7995310668 2297772567 4091441969 5193434935 5216881594
3728018757 3270808909 7303634232 1219226260 2579132473
6225087924 9706916764 3610785463 0715123094 9589683470
1055099648 300$\underline{1172}$33$\underline{2}$ ....

857 1166861143 5239206534 4224037339 5565927654 6091015169
1948658109 6849474912 4854142357 0595099183 1971995332
5554259043 1738623103 8506417736 2893815635 9393232205
3675612602 1003500583 4305717619 6032672112 0186697782
9638273045 5075845974 3290548424 7374562427 0711785297
5495915985 9976662777 1295215869 3115519253 2088681446
9078179696 6161026837 8063010501 7502917152 8588098016
3360560093 3488914819 1365227537 9229871645 2742123687
2812135355 8926487747 9579929988 3313885647 6079346557
7596266044 3407234539 0898483080 5134189031 5052508751
4585764294 0490081680 2800466744 4574095682 6137689614
9358226371 0618436406 0676779463 2438739789 9649941656
9428238039 6732788798 1330221703 6172695449 2415402567
0945157526 2543757292 8821470245 0408401400 2333722287
0478413068 8448074679 1131855309 2182030338 3897316219
3698949824 9708284714 1190198366 3943990665 1108518086
3477246207 7012835472 5787631271 8786464410 7351225204
200700$\underline{1166}$ ....

859 1164144353 8998835855 6461001$\underline{1164}$ ....

863 1158748551 5643105446 1181923522 5955967555 0405561993
0475086906 1413673232 9084588644 2641946697 5666280417
1494785631 5179606025 4924681344 1483198146 0023174971
0312862108 9223638470 4519119351 1008111239 8609501738
1228273464 6581691772 8852838933 9513325608 3429895712
6303592120 5098493626 8829663962 9200463499 4206257242
1784472769 4090382387 0220162224 7972190034 7624565469
2931633835 4577056778 6790266512 1668597914 2526071842
4101969872 5376593279 2584009269 9884125144 8435689455
3881807647 7404403244 4959443800 6952491309 3858632676
7091541135 5735805330 2433371958 2850521436 8482039397
4507531865 5851680185 3997682502 8968713789 1077636152
9548088064 8899188876 0139049826 1877172653 5341830822
7114716106 6048667439 1657010438 7369640787 9490150637
3117033603 7079953650 0579374275 7821552723 0590961761
2977983777 5202780996 5237543453 0706836616 4542294322
1320973348 7833140208 5747392815 7589803012 7462340672
0741599073 00$\underline{11587485}$ ....

877 1140250855 1881413911 0604332953 2497149372 8620296465
2223489167 6168757126 5678449258 8369441277 0809578107
1835803876 8529076396 8072976054 7320410490 3078677309
0079817559 8631698973 7742303306 7274800456 1003420752
5655644241 7331812998 8597491448 1185860889 3956670467
5028506271 3797035347 7765108323 8312428734 3215507411
6305587229 1904218928 1641961231 4709236031 9270239452
6795895096 9213226909 9201824401 3683010262 2576966932
7251995438 9965792474 3443557582 668187011 ....

881 1135073779 7956867196 3677639046 5380249716 2315550510
7832009080 5902383654 9375709421 1123723041 9977298524
4040862656 0726447219 0692395005 6753688989 7843359818
3881952326 9012485811 5777525539 1600454029 5119182746
8785471055 6186152099 8864926220 2043132803 6322360953
4619750283 7684449489 2167990919 4097616345 0624290578
8876276958 0022701475 5959137343 9273552780 9307604994
3246311010 2156640181 6118047673 0987514188 4222474460
8399545970 4880817253 1214528944 3813847900 1135073779 ....

883 1132502831 2570781426 9535673839 1845979614 9490373725
9343148357 8708946772 3669309173 2729331823 3295583238
9580973952 4348810872 0271800679 5016987542 4688561721
4043035107 5877689694 2242355605 8890147225 3680634201
5855039637 5990939977 3499433748 5843714609 2865232163
0804077010 1925754813 1370328425 8210645526 6138165345
4133635334 0883352208 3805209513 0237825594 5639864099
6602441506 2287655719 1392978482 4462061155 1528878822
1970554926 3873159682 8992072480 1812004530 0113250283 ....

887 1127395715 8962795941 3754227733 9346110484 7801578354
0022547914 3179255918 8275084554 6786922209 6956031567
0800450958 2863585118 3765501691 0935738444 1939120631
3416009019 1657271702 3675310033 8218714768 8838782412
6268320180 3833145434 0473506200 6764374295 3776775648
2525366403 6076662908 6809470124 0135287485 9075535512
9650507328 0721533258 1736189402 4802705749 7181510710
2593010146 5614430665 1634723788 0496054114 9943630214
2051860202 9312288613 3032694475 7609921082 2998872604
2841037204 0586245772 2660653889 5152198421 6459977452
0856820744 0811724915 4453213077 7903043968 4329199549
0417136414 8816234498 3089064261 5558060879 3686583990
9808342728 2976324689 9661781285 2311161217 5873731679
8196166854 5659526493 7993235625 7046223224 3517474633
5963923337 0913190529 8759864712 5140924464 4870349492
6719278466 7418263810 5975197294 2502818489 2897406989
8534385569 3348365276 2119503945 8850056369 7857948139
7970687711 3866967305 5242390078 9177001127 ....

907 1102535832 4145534729 8787210584 3439911797 1334068357
2216097023 1532524807 0562293274 5314222712 2381477398
0154355016 5380374862 1830209481 8081587651 5986769570
0110253583 ....

911 1097694840 8342480790 3402854006 5861690450 0548847420
4171240395 1701427003 2930845225 0274423710 2085620197
5850713501 6465422612 5137211855 1042810098 7925356750
8232711306 2568605927 5521405049 3962678375 4116355653
1284302963 7760702524 6981339187 7058177826 5642151481
8880351262 3490669593 8529088913 2821075740 9440175631
1745334796 9264544456 6410537870 4720087815 5872667398
4632272228 3205268935 2360043907 7936333699 2316136114
1602634467 6180021953 8968166849 6158068057 0801317233
8090010976 ....

919 1088139281 8280739934 7116430903 1556039173 0141458106
6376496191 5125136017 4102285092 4918389553 8628944504
8966267682 2633297062 0239390642 0021762785 6365614798
6942328618 0631120783 4602829162 1327529923 8302502720
3482045701 8498367791 0772578890 0979325353 6452665941
2404787812 8400435255 7127312295 9738846572 3612622415
6692056583 2426550598 4766050054 4069640914 0369967355
8215451577 8019586507 0729053318 8248095756 2568008705
1142546245 9194776931 4472252448 3133841131 6648531011
9695321001 ....

929 1076426264 8008611410 1184068891 2809472551 1302475780
4090419806 2432723358 4499461786 8675995694 2949407965
5543595263 7244348762 1097954790 0968783638 3207750269
1065662002 1528525296 0172228202 3681377825 6189451022
6049515608 1808396124 8654467168 9989235737 3519913885
8988159311 0871905274 4886975242 1959095801 9375672766
4155005382 1313240043 0570505920 3444564047 3627556512
3789020452 0990312163 6167922497 3089343379 9784714747
0398277717 9763186221 7438105489 7739504843 9181916038
7513455328 3100107642 ....

937 1067235859 1248665955 1760939167 5560298826 0405549626
4674493062 9669156883 6712913553 8954108858 0576307363
9274279615 7950907150 4802561366 0618996798 2924226254
0021344717 1824973319 1035218783 3511205976 5208110992
5293489861 2593383137 6734258271 0779082177 1611526147
2785485592 3159018143 0096051227 3212379935 9658484525
0800426894 3436499466 3820704375 6670224119 5304162219
8505869797 2251867662 7534685165 4215581643 5432230522
9455709711 8463180362 8601921024 5464247598 7193169690
5016008537 8868729989 3276414087 5133404482 3906083244
3970117395 9445037353 2550693703 3084311632 8708644610
4589114194 2369263607 2572038420 4909284951 9743863393
8100320170 7577374599 7865528281 7502668089 6478121664
8879402347 9188900747 0651013874 0661686232 6574172892
2091782283 8847385272 1451440768 4098185699 0394877267
8762006403 4151547491 9957310565 6350053361 7929562433
2977588046 9583778014 9413020277 4813233724 6531483457
8441835645 6776947705 4429028815 3681963713 9807897545
3575240128 0683030949 8399146211 3127001067 ....

941 1062699256 1105207226 3549415515 4091392136 0255047821
4665249734 3251859723 6981934112 6461211477 1519659936
2380446333 6875664187 0350690754 5164718384 6971307120
0850159404 8884165781 0839532412 3273113708 8204038257
1732199787 4601487778 9585547290 1168969181 7215727948
9904357066 9500531349 6280552603 6131774707 7577045696
0680127523 9107332624 8671625929 8618490967 0563230605
7385759829 9681190223 1668437832 0935175345 3772582359
1923485653 5600425079 7024442082 8905419766 2061636556
8544102019 1285866099 8937300743 8894792773 6450584484
5908607863 9744952178 5334750265 6748140276 3018065887
3538788522 8480340063 7619553666 3124335812 9649309245
4835281615 3028692879 9149840595 1115834218 9160467587
6726886291 1795961742 8267800212 5398512221 0414452709
8831030818 2784272051 0095642933 0499468650 3719447396
3868225292 2422954303 9319872476 0892667375 1328374070
1381509032 9436769394 2614240170 0318809776 8331562167
9064824654 6227417640 8076514346 4399574920 2975557917
1094580233 7938363443 1455897980 8714133900 1062699256 ....

947 1055966209 0813093980 9926082365 3643083421 3305174234
4244984160 5068637803 5902851108 7645195353 7486800422
3864836325 2375923970 4329461457 2333685322 0696937697
9936642027 4551214361 1404435058 0781414994 7201689545
9345300950 3695881731 7845828933 4741288278 7750791974
6568109820 4857444561 7740232312 5659978880 6758183738
1203801478 3526927138 3315733896 5153115100 3167898627
2439281942 9778247096 0929250263 9915522703 2734952481
5205913410 7708553326 2935586061 2460401267 1594508975
7127771911 2988384371 7001055966 ....

953 1049317943 3368310598 1112277019 9370409233 9979013641
1332633788 0377754459 6012591815 3200419727 1773347324
2392444910 8079748163 6935991605 4564533053 5152151101
7838405036 7261280167 8908709338 9296956977 9643231899
2654774396 6421825813 2214060860 4407135362 0146904512
0671563483 7355718782 7911857292 7597061909 7586568730
3252885624 3441762854 1448058761 8048268625 3934942287
5131164742 9171038824 .7639034627 4921301154 2497376705
1416579223 5047219307 4501573976 9150052465 8971668415
5299055613 8509968520 4616998950 6820566631 6894018887
7229800629 5907660020 9863588667 3662119622 2455403987
4081846799 5802728226 6526757607 5550891920 2518363064
0083945435 4669464847 8488982161 5949632738 7198321091
2906610703 0430220356 7681007345 2256033578 1741867785
9391395592 8646379853 0954879328 4365162644 2812172088
1427072402 9380902413 4312696747 1143756558 2371458551
9412381951 7313746065 0577124868 8352570828 9611752360
9653725078 6988457502 6232948583 4207764952 7806925498
4260230849 9475341028 3315844700 9443861490 0314795383
00<u>10493179</u> . . . .

961 1040582726 3267429760 6659729448 4911550468 2622268470
3433922996 8782518210 1977107180 0208116545 2653485952
1331945889 6982310093 6524453694 0686784599 3756503642
0395421436 0041623309 0530697190 4266389177 9396462018
7304890738 8137356919 8751300728 4079084287 2008324661
8106139438 0853277835 5879292403 7460978147 7627471383
9750260145 6815816857 4401664932 3621227887 6170655567
1175858480 7492195629 5525494276 7950052029 1363163371
4880332986 4724245577 5234131113 4235171696 1498439125
9105098855 3590<u>10405</u> . . . .

967 1034126163 3919338159 2554291623 5780765253 3609100310
2378490175 8014477766 2874870734 2295760082 7300930713
5470527404 3433298862 4612202688 7280248190 2792140641
1582213029 9896587383 6608066184 0744570837 6421923474
6639089968 9762150982 4198552223 3712512926 5770423991
7269966928 6452947259 5656670113 7538779731 1271975180
9720785935 8841778697 00<u>10341261</u> . . . .

971 1029866117 4047373841 4006179196 7044284243 0484037075
1802265705 4582904222 4510813594 2327497425 3347064881
5653964984 5520082389 2893923789 9073120494 3357363542
7394438722 9660144181 2564366632 3377960865 0875386199
7940267765 1905252317 1987641606 5911431513 9031925849
6395468589 0834191555 0978372811 5345005149 3305870236
8692070030 8959835221 4212152420 1853759011 3285272914
5211122554 0679711637 4871266735 3244078269 8249227600
4119464469 6189495365 6024716786 8177136972 1936148300
7209062821 8331616889 8043254376 9309989701 3388259526
2615859938 2080329557 1575695159 6292481977 3429454170
9577754891 8640576725 0257466529 3511843460 3501544799
1761071060 7621009268 7950566426 3645726055 6127703398
5581874356 3336766220 3913491246 1380020597 3223480947
4768280123 5839340885 6848609680 7415036045 3141091658
0844490216 2718846549 9485066941 2976313079 2996910401
6477857878 4757981462 4098867147 2708547888 7744593202
8836251287 3326467559 2173017507 7239958805 3553038105
0463439752 8321318228 6302780638 5169927909 3717816683
8311019567 4562306900 1029866117 . . . .

977 1023541453 4288638689 8669396110 5424769703 1729785056
2947799385 8751279426 8167860798 3623336745 1381780962
1289662231 3203684749 2323439099 2835209825 9979529178
9314227226 2026612077 7891504605 9365404298 8741044012
2824974411 4636642784 0327533265 0972364380 7574206755
3735926305 0153531218 0143295803 4800409416 5813715455
4759467758 4442169907 8812691914 0225179119 7543500511
7707267144 3193449334 6980552712 3848515864 8925281473
8996929375 6397134083 9303991811 6683725690 8904810644
8311156601 8423746161 7195496417 6049129989 7645854657
1136131013 3060388945 7523029682 7021494370 5220061412
4872057318 3213920163 7666325486 1821903787 1033776867
9631525076 7656090071 6479017400 2047082906 8577277379
7338792221 0849539406 3459570112 5895598771 7502558853
6335721596 7246673490 2763561924 2579324462 6407369498
4646878198 5670419651 9959058341 8628454452 4053224155
5783009211 8730808597 7482088024 5649948822 9273285568
0655066530 1944728761 5148413510 7471852610 0307062436
0286591606 9600818833 1627430910 9518935516 8884339815
7625383828 0450358239 5087001023 . . . .

983 1017293997 9654120040 6917599186 1648016276 7039674465
9206510681 5869786368 2604272634 7914547304 1709053916
5818921668 3621566632 7568667344 8626653102 7466937945
0661241098 6775178026 4496439471 0071210579 8575788402
8484231943 0315361159 3692777212 6144455747 7110885045
7782299084 4354018311 2919633774 1607324516 7853509664
2929806714 1403865717 1922685656 1546286876 9074262461
8514750762 9704984740 5900305188 1993896236 0122075279
7558494404 8830111902 3397761953 2044760935 9104781281
7904374364 1912512716 1749745676 5005086469 9898270600
2034587995 9308240081 3835198372 3296032553 4079348931
8413021363 1739572736 5208545269 5829094608 3418107833
1637843336 7243133265 5137334689 7253306205 4933875890
1322482197 3550556052 8992878942 0142421159 7151576805
6968463886 0630722278 7385554425 2288911495 4221770091
5564598168 8708036622 5839267548 3214649033 5707019328
5859613428 2807731434 3845371312 3092573753 8148524923
7029501525 9409969481 1800610376 3987792472 0244150559
5116988809 7660223804 6795523906 4089521871 8209562563
5808748728 3825025432 3499491353 00<u>10172939</u> ....

991 1009081735 6205852674 0665993945 5095862764 8839556004 0363269424
8234106962 6639757820 3834510595 3582240161 4530776992 9364278506
5590312815 3380423814 3289606458 1231079717 4571140262 3612512613
5216952573 1584258324 9243188698 9845610494 4500504540 8678102926
3370332996 9727547931 3824419778 0020181634 7124117053 4813319878
9101917255 2976791120 0807265388 4964682139 2532795156 4076690211
9071644803 2290615539 8587285570 1311806256 3067608476 2865792129
1624621594 3491422805 2472250252 2704339051 4631685166 4984863773
9656912209 88900<u>10090</u> ....

997 1003009027 0812437311 9358074222 6680040120 3610832497 4924774322
9689067201 6048144433 2998996990 9729187562 6880641925 7773319959
8796389167 5025075225 6770310932 7983951855 566700<u>1003</u> ....

TABLE OF THE FREQUENCY OF PRIME NUMBERS.

1	168	51	89	101	81	151	85	201	77	251	71	301	85	351	74	401	70	451	92
2	135	52	97	102	93	152	90	202	87	252	88	302	83	352	80	402	71	452	76
3	127	53	89	103	87	153	88	203	78	253	78	303	72	353	82	403	76	453	63
4	120	54	92	104	80	154	77	204	78	254	81	304	84	354	79	404	75	454	72
5	119	55	90	105	91	155	84	205	77	255	76	305	88	355	87	405	70	455	74
6	114	56	93	106	82	156	85	206	85	256	87	306	80	356	79	406	83	456	82
7	117	57	99	107	92	157	76	207	83	257	72	307	82	357	67	407	67	457	73
8	107	58	91	108	76	158	88	208	87	258	78	308	73	358	80	408	81	458	77
9	110	59	90	109	91	159	87	209	85	259	86	309	76	359	83	409	79	459	75
10	112	60	94	110	88	160	85	210	88	260	76	310	80	360	71	410	82	460	68
11	106	61	88	111	83	161	85	211	84	261	77	311	79	361	68	411	73	461	77
12	103	62	87	112	84	162	84	212	86	262	73	312	69	362	79	412	81	462	69
13	109	63	88	113	81	163	81	213	69	263	79	313	86	363	76	413	74	463	74
14	105	64	93	114	88	164	83	214	81	264	84	314	86	364	84	414	69	464	77
15	102	65	80	115	82	165	77	215	86	265	80	315	76	265	77	415	90	465	85
16	108	66	98	116	93	166	80	216	74	266	78	316	77	366	77	416	80	466	74
17	98	67	84	117	81	167	81	217	76	267	87	317	84	367	85	417	67	467	69
18	104	68	99	118	90	168	83	218	80	268	94	318	84	368	79	418	82	468	83
19	94	69	80	119	79	169	73	219	84	269	75	319	81	369	72	419	85	469	85
20	102	70	81	120	87	170	87	220	91	270	78	320	86	370	68	420	75	470	72
21	98	71	98	121	88	171	87	221	78	271	84	321	79	371	70	421	75	471	87
22	104	72	95	122	86	172	81	222	80	272	78	322	80	372	76	422	73	472	78
23	100	73	90	123	88	173	89	223	81	273	83	323	81	373	81	423	77	473	73
24	104	74	83	124	88	174	79	224	80	274	71	324	71	374	73	424	83	474	78
25	94	75	92	125	83	175	83	225	83	275	80	325	87	375	82	425	81	475	80
26	98	76	91	126	84	176	75	226	84	276	83	326	85	376	85	426	74	476	86
27	101	77	83	127	83	177	95	227	76	277	83	327	73	377	80	427	71	477	75
28	94	78	95	128	86	178	73	228	80	278	74	328	86	378	71	428	78	478	69
29	98	79	84	129	89	179	89	229	89	279	81	329	73	379	77	429	71	479	85
30	92	80	91	130	83	180	94	230	88	280	73	330	81	380	83	430	89	480	71
31	95	81	88	131	85	181	71	231	84	281	87	331	80	381	72	431	76	481	77
32	92	82	92	132	83	182	79	232	78	282	85	332	82	382	76	432	79	482	78
33	106	83	89	133	87	183	91	233	76	283	77	333	72	383	74	433	84	483	82
34	100	84	84	134	82	184	79	234	71	284	72	334	80	384	81	434	80	484	75
35	94	85	87	135	80	185	83	235	87	285	90	335	77	385	78	435	85	485	65
36	92	86	85	136	89	186	91	236	73	286	77	336	77	386	80	436	82	486	63
37	99	87	88	137	96	187	79	237	76	287	71	337	84	387	78	437	73	487	82
38	94	88	93	138	80	188	87	238	73	288	71	338	80	388	69	438	70	488	78
39	90	89	76	139	85	189	80	239	87	289	85	339	77	389	75	439	75	489	83
40	96	90	94	140	84	190	88	240	79	290	84	340	68	390	84	440	75	490	78
41	88	91	89	141	87	191	75	241	80	291	84	341	84	391	81	441	79	491	78
42	101	92	85	142	87	192	81	242	91	292	77	342	77	392	79	442	72	492	76
43	102	93	97	143	82	193	89	243	76	293	78	343	77	393	86	443	85	493	67
44	85	94	86	144	77	194	84	244	77	294	68	344	80	394	87	444	88	494	82
45	96	95	87	145	79	195	74	245	78	295	85	345	80	395	75	445	82	495	80
46	86	96	95	146	85	196	85	246	80	296	75	346	76	396	72	446	68	496	87
47	90	97	84	147	84	197	76	247	84	297	82	347	80	397	75	447	68	497	68
48	95	98	82	148	83	198	87	248	79	298	73	348	82	398	75	448	73	498	81
49	89	99	87	149	83	199	96	249	88	299	73	349	77	399	82	449	70	499	72
50	98	100	87	150	91	200	77	250	80	300	78	350	82	400	81	450	80	500	81

501 78	551 79	601 75	651 61	701 75	751 68	801 85	851 70	901 74	951 76
502 74	552 75	602 73	652 74	702 71	752 85	802 66	852 77	902 73	952 70
503 67	553 71	603 83	653 85	703 81	753 73	803 70	853 74	903 70	953 78
504 76	554 80	604 76	654 69	704 71	754 71	804 69	854 66	904 63	954 65
505 76	555 77	605 73	655 78	705 87	755 83	805 78	855 71	905 81	955 73
506 83	556 61	606 74	656 73	706 68	756 70	806 79	856 73	906 70	956 76
507 76	557 88	607 72	657 71	707 82	757 66	807 68	857 78	907 80	957 58
508 71	558 68	608 78	658 70	708 74	758 68	808 70	858 76	908 80	958 69
509 76	559 74	609 78	659 79	709 77	759 79	809 69	859 69	909 79	959 77
510 75	560 77	610 80	660 73	710 77	760 77	810 78	860 71	910 82	960 69
511 72	561 86	611 73	661 83	711 78	761 77	811 78	861 77	911 62	961 68
512 82	562 61	612 71	662 70	712 76	762 80	812 72	862 74	912 81	962 88
513 70	563 83	613 76	663 74	713 72	763 68	813 69	863 83	913 71	963 71
514 77	564 67	614 79	664 77	714 73	764 79	814 72	864 60	914 54	964 74
515 81	565 77	615 71	665 77	715 66	765 72	815 78	865 80	915 73	965 74
516 66	566 78	616 75	666 77	716 83	766 82	816 69	866 80	916 70	966 70
517 85	567 72	617 85	667 73	717 69	767 78	817 75	867 68	917 72	967 73
518 83	568 72	618 81	668 73	718 65	768 68	818 75	868 78	918 79	968 66
519 76	569 71	619 67	669 66	719 67	769 77	819 62	869 80	919 75	969 75
520 78	570 80	620 73	670 74	720 74	770 74	820 83	870 73	920 71	970 73
521 73	571 85	621 77	671 75	721 78	771 77	821 75	871 79	921 72	971 76
522 83	572 72	622 70	672 76	722 77	772 75	822 72	872 58	922 72	972 78
523 79	573 85	623 74	673 76	723 73	773 70	823 84	873 76	923 72	973 74
524 69	574 72	624 75	674 77	724 86	774 76	824 78	874 65	924 81	974 63
525 77	575 70	625 68	675 69	725 75	775 72	825 71	875 75	925 76	975 85
526 79	576 77	626 69	676 75	726 69	776 67	826 81	876 80	926 80	976 70
527 84	577 78	627 70	677 74	727 76	777 70	827 78	877 75	927 74	977 66
528 72	578 77	628 70	678 63	728 75	778 76	828 69	878 67	928 63	978 60
529 70	579 76	629 71	679 82	729 76	779 81	829 69	879 68	929 70	979 80
530 78	580 77	630 75	680 83	730 75	780 71	830 68	880 75	930 80	980 65
531 80	581 73	631 67	681 75	731 69	781 70	831 76	881 80	931 69	981 67
532 68	582 79	632 81	682 78	732 76	782 82	832 79	882 69	932 69	982 75
533 79	583 73	633 77	683 66	733 71	783 68	833 82	883 72	933 76	983 70
534 74	584 78	634 70	684 78	734 75	784 74	834 68	884 73	934 68	984 70
535 72	585 72	635 82	685 72	735 74	785 75	835 67	885 69	935 81	985 74
536 71	586 81	636 78	686 74	736 79	786 77	836 73	886 77	936 68	986 76
537 87	587 79	637 73	687 74	737 69	787 70	837 71	887 76	937 71	987 76
538 67	588 87	638 74	688 82	738 78	788 73	838 64	888 71	938 71	988 63
539 78	589 73	639 59	689 74	739 70	789 80	839 80	889 77	939 72	989 71
540 71	590 68	640 72	690 79	740 81	790 68	840 69	890 68	940 68	990 72
541 73	591 71	641 77	691 60	741 67	791 78	841 70	891 68	941 74	991 71
542 77	592 67	642 71	692 79	742 74	792 71	842 69	892 80	942 79	992 79
543 78	593 80	643 68	693 77	743 73	793 82	843 83	893 69	943 72	993 65
544 81	594 77	644 70	694 73	744 67	794 71	844 68	894 72	944 76	994 68
545 68	595 78	645 86	695 76	745 64	795 73	845 78	895 74	945 73	995 78
546 68	596 77	646 75	696 77	746 67	796 79	846 70	896 80	946 66	996 69
547 73	597 79	647 74	697 73	747 76	797 77	847 69	897 64	947 72	997 69
548 76	598 73	648 79	698 79	748 71	798 72	848 77	898 75	948 66	998 83
549 77	599 72	649 73	699 62	749 76	799 71	849 75	899 76	949 67	999 74
550 78	600 73	650 84	700 72	750 72	800 81	850 68	900 61	950 75	1000 65

1000000 . . . 1100000

	0	1	2	3	4	5	6	7	8	9	
1	1										1
2		1				1		1	1		4
3		4	2	2	3	1	2	3	3	1	21
4	2	8	5	4	3	6	9	4	5	8	54
5	11	10	8	18	12	10	10	12	15	8	114
6	14	14	18	21	16	22	19	15	17	15	171
7	26	17	23	23	24	24	17	22	20	21	217
8	19	19	21	7	14	15	20	17	15	17	164
9	11	13	9	13	14	14	12	13	11	16	126
10	8	6	8	5	9	5	5	9	7	9	71
11	6	6	4	6	3	1	3	1	4	5	39
12	1	1	2	1	1	1	2	2	1		12
13	1	1			1		1	1	1		6
14											
15											
16											
	752	719	732	700	731	698	713	722	706	737	7210

$$\int \frac{\mathrm{d}x}{\log x} = 7212{,}99$$

1100000 . . . 1200000

	0	1	2	3	4	5	6	7	8	9	
0											0
1					1						1
2			1				1	1		2	5
3	4	3	3	3	3	3	3	2		1	25
4	5	6	7	5	9	4	4	5	6	6	57
5	8	13	10	12	11	11	9	12	12	9	107
6	14	20	17	20	17	17	18	16	17	14	170
7	21	19	22	19	21	21	20	18	29	27	217
8	22	13	10	12	18	20	17	19	9	20	160
9	13	14	16	17	7	11	16	14	12	11	131
10	9	6	10	10	8	9	6	8	3	8	77
11	1	4	2	2	2	1	4	5	9	2	32
12	1	1	1		2	3	1		2		11
13	1	1	1				1		1		5
14	1				1						2
	736	710	716	713	697	725	729	723	735	710	7194

$$\int \frac{\mathrm{d}x}{\log x} = 7165{,}911$$

1200000 . . . 1300000

	0	1	2	3	4	5	6	7	8	9	
0											
1								1	1		2
2	2		2	1						1	6
3	3	2	4	5	4	3	1	4	3	3	32
4	7	7	7	3	5	7	12	2	3	10	63
5	15	12	12	15	10	14	9	15	6	12	120
6	16	14	13	19	17	16	16	15	20	14	160
7	24	15	25	24	21	20	15	22	24	24	214
8	17	19	16	11	17	15	22	18	19	14	168
9	8	12	7	10	12	13	14	13	13	9	111
10	3	11	10	8	10	4	5	3	9	10	73
11	3	6	3	2	3	5	3	6	1	3	35
12	1	1	1			1	3	1	1		9
13	1	1		1		2					5
14				1							1
16					1						1
	676	744	693	693	724	713	718	709	722	689	7081

$$\int \frac{\mathrm{d}x}{\log x} = 7123{,}35$$

1300000 . . . 1400000

	0	1	2	3	4	5	6	7	8	9	
1						1					1
2		1	1		1	1	1	2	1	1	9
3	3	1	1	3	2	2	2		5		19
4	3	10	7	11	6	8	7	6	6	5	69
5	17	13	11	11	15	12	8	8	14	10	119
6	15	14	17	14	20	18	23	17	16	19	173
7	22	18	26	18	21	16	16	28	19	23	207
8	14	22	14	16	14	13	21	17	15	15	161
9	17	11	12	14	12	9	12	7	13	13	120
10	5	6	2	11	5	15	5	8	6	7	70
11	4	2	7	1	1	3	3	6	3	3	33
12		1	2	1	2	2	2	1	1	3	15
13		1			1				1		3
14										1	1
	709	702	713	705	692	713	709	723	695	737	7098

$$\int \frac{\mathrm{d}x}{\log x} = 7084{,}48$$

1400000 . . . 1500000

	141	142	143	144	145	146	147	148	149	150	
0											0
1			1		1	1	1			1	5
2		1	1		2				2	1	7
3	3	3	0	2	1	2	2	4	2	0	19
4	8	8	8	4	6	7	9	9	5	8	72
5	17	9	7	14	13	11	14	15	16	13	129
6	21	23	20	18	20	19	11	16	16	19	183
7	17	23	18	18	13	24	18	11	15	22	179
8	12	16	28	17	24	14	17	18	23	14	183
9	12	11	4	15	6	10	13	12	7	8	98
10	7	2	7	7	9	7	8	9	8	9	73
11	2	2	2	4	2	3	6	5	4	4	34
12	1	2	3	1	2	2	1	1	2	1	16
13			1		1						2
	679	680	717	723	703	701	716	705	706	698	7028

$$\int \frac{\mathrm{d}x}{\log x} = 7048{,}78186$$

1500000 . . . 1600000

	151	152	153	154	155	156	157	158	159	160	
0											0
1						1	1				2
2			1	1	2		2		1	3	10
3	2		4	2	2	3	5	3	6	1.	28
4	8	5	5	7	9	13	6	10	7	7	77
5	8	19	9	13	11	9	12	15	11	17	124
6	16	20	25	21	20	12	26	14	23	22	199
7	19	21	18	19	18	15	12	19	11	20	172
8	19	12	15	18	15	17	10	17	15	11	149
9	16	14	16	12	8	17	15	6	11	9	124
10	8	3	5	4	9	7	5	10	10	2	63
11		5	2	2	3	3	3	2	4	5	29
12	4			1	3	1	1	4	1	2	17
13		1				2	2			1	6
	731	702	691	686	698	714	680	701	693	675	6971

$$\int \frac{\mathrm{d}x}{\log x} = 7015{,}78776$$

1600000 . . . 1700000

	161	162	163	164	165	166	167	168	169	170	
0								1			1
1						2					2
2	1	3	1		1	1	2			2	11
3	3	3	3	4	4	2	2	4	4		29
4	7	4	9	7	7	10	4	4	10	6	68
5	10	11	8	12	11	11	13	12	18	14	120
6	18	22	15	19	15	11	14	19	10	16	159
7	22	15	14	21	25	18	22	24	24	18	203
8	14	23	25	15	17	16	17	15	13	19	174
9	8	12	18	12	12	21	12	8	14	13	130
10	7	2	5	8	4	6	11	7	4	9	63
11	7	3	1	1	3	1	3	2	2	3	26
12	2	1	1	1				4			9
13	1				1				1		3
14		1									1
15						1					1
	719	694	710	692	692	700	716	702	675	712	7012

$$\int \frac{\mathrm{d}x}{\log x} = 6985{,}13714$$

1700000 . . . 1800000

	171	172	173	174	175	176	177	178	179	180	
0											0
1				1							1
2	1					2	1			1	5
3	3	4		3	3	4	3	5	3	2	30
4	7	9	6	6	5	8	6	6	10	7	70
5	13	15	19	16	12	15	21	13	13	15	152
6	17	16	22	22	20	14	15	13	18	17	174
7	23	21	22	15	22	19	19	21	17	15	194
8	11	16	11	15	16	15	13	18	19	13	147
9	18	11	8	11	15	10	12	14	10	15	124
10	3	1	8	7	2	9	6	9	5	11	61
11	1	3	3	1	3	4	4	1	4	2	26
12	2	3		1	1				1	2	10
13	1	1	1	2							5
14											
15											1
	695	685	691	689	706	684	679	700	689	713	6931

$$\int \frac{\mathrm{d}x}{\log x} = 6956{,}53562$$

1800000 . . . 1900000

	181	182	183	184	185	186	187	188	189	190	
0											
1											
2	1	1	2	1		2				3	10
3	3	2	1	5	1	1	1	2	3	3	22
4	6	5	10	12	7	6	5	5	8	7	71
5	14	15	10	11	11	12	19	17	12	14	135
6	13	20	14	15	21	19	16	19	23	15	175
7	25	26	18	17	21	21	20	22	19	17	206
8	15	19	13	18	22	15	19	15	11	14	161
9	10	7	19	13	9	8	10	12	10	15	113
10	9	4	8	6	6	13	4	6	8	10	74
11	2		4			3	5	2	5	2	23
12	2	1	1	2	2		1		1		10
13											
14											
	704	672	718	674	700	707	703	689	697	691	6955

$$\int \frac{\mathrm{d}x}{\log x} = 6929{,}73917$$

1900000 . . . 2000000

	191	192	193	194	195	196	197	198	199	200	
0											
1	1										1
2			1			1	2		1		5
3	4	3	1	2	10	1	3	4	4	2	34
4	5	4	4	6	4	9	7	10	11	7	67
5	12	18	15	18	11	12	11	16	11	12	136
6	19	20	18	16	17	24	20	20	18	10	182
7	21	20	23	27	20	16	25	17	21	31	221
8	16	10	16	14	14	18	17	15	8	20	148
9	15	14	8	8	9	12	8	8	15	6	103
10	5	6	8	6	11	4	5	5	6	6	62
11	2	4	6	2	3	2	1	3	2	5	30
12		1		1				2	1		5
13					1		1		1		3
14						1			1	1	3
	689	697	711	683	692	685	673	670	688	714	6902

$$\int \frac{\mathrm{d}x}{\log x} = 6904{,}54424$$

2000000 . . . 2100000

	201	202	203	204	205	206	207	208	209	210	
0											
1					2	1					3
2			2	2	1			2	2	1	10
3	3	3	5	2	2	3	4	5	2	3	32
4	7	8	9	4	8	5	6	7	9	6	69
5	13	10	9	15	13	10	12	13	9	15	119
6	25	20	13	16	26	23	25	14	17	18	197
7	10	22	23	25	13	23	18	23	25	22	204
8	13	17	15	22	12	13	12	16	18	19	157
9	16	15	11	4	11	12	11	14	11	10	115
10	10	2	8	6	11	7	7	3	3	6	63
11	2	1	5	3		1	3	3	3		21
12		2			1	2	2		1		8
13	1			1							2
	705	691	693	690	671	696	694	674	686	674	6874

$$\int \frac{\mathrm{d}x}{\log x} = 6880{,}780$$

2100000 . . . 2200000

	211	212	213	214	215	216	217	218	219	220	
0											
1		1					1				2
2	1	1	1			1	1	1	1	2	9
3	5	3	3	1	4		2	3	2	4	27
4	7	7	2	13	5	3	9	6	9	8	69
5	12	14	20	16	16	12	17	13	12	14	146
6	12	20	17	14	16	25	16	23	21	19	183
7	19	14	18	23	26	22	18	22	22	17	201
8	22	21	20	20	12	16	20	10	12	15	168
9	12	10	8	7	9	10	7	13	16	17	109
10	6	5	6	2	7	7	8·	5	2	4	52
11	3	2	3	1	4	2	1		2		18
12	1	1	1	1	1	2		2			9
13		1	1	1					1		4
14				1				2			3
	699	683	697	673	693	712	666	691	679	664	6857

$$\int \frac{\mathrm{d}x}{\log x} = 6858{,}292$$

2200000 . . . 2300000

	221	222	223	224	225	226	227	228	229	230	
1					1				1		2
2			1	1		2			3	2	9
3	5	2	4	7	2	1	2	2	2	2	29
4	8	9	5	5	10	7	7	7	6	9	73
5	12	24	16	13	11	10	14	14	15	9	138
6	17	18	12	18	18	20	16	17	21	22	179
7	19	17	25	21	18	20	23	25	19	18	205
8	12	12	19	15	18	24	13	17	16	22	168
9	14	9	6	9	19	11	16	9	13	7	113
10	7	6	6	6	1	3	7	5		3	44
11	5	2	4	4	2	2	2	2	2	5	30
12	1	1	2	1				2	2	1	10
	701	660	695	680	683	688	701	694	662	685	6849

$$\int \frac{\mathrm{d}x}{\log x} = 6836{,}977$$

2300000 . . . 2400000

	231	232	233	234	235	236	237	238	239	240	
1	1	1	1		1						4
2			1		2	2	1	2	1	2	11
3	4	1	2	3	4	3	2	6	4	3	32
4	8	12	10	9	8	7	3	13	7	9	86
5	13	18	13	14	17	12	10	13	10	16	136
6	15	16	21	20	16	21	26	11	14	16	176
7	22	25	20	20	13	16	26	18	19	15	194
8	13	9	16	21	17	15	15	15	21	16	158
9	13	9	6	7	14	14	8	13	14	14	112
10	7	5	3	2	5	5	8	7	8	5	55
11	3	3	4	3	3	5	1	2	2	2	28
12	1		3	1·						2	7
13		1									1
	690	662	672	671	666	690	691	660	705	680	6787

$$\int \frac{\mathrm{d}x}{\log x} = 6816{,}706$$

2400000 . . . 2500000

	241	242	243	244	245	246	247	248	249	250	
1									1		1
2	2						1	1	2	3	9
3	4	6	4	4	1	5	3	5	3	2	37
4	12	8	7	7	9	7	10	8	6	4	78
5	13	14	17	19	15	12	18	11	11	17	147
6	18	16	21	20	18	22	18	18	20	22	193
7	21	16	19	20	17	17	21	22	19	17	189
8	10	16	14	14	21	17	10	17	16	16	151
9	8	13	9	11	7	12	6	11	12	13	102
10	9	6	5	4	6	4	8	6	7	3	58
11	2	4	3	1	4	1	4	1	2	1	23
12	1		1		1	1	1			2	7
13		1			1	2			1		5
	660	690	672	657	701	687	666	672	687	674	6766

$$\int \frac{\mathrm{d}x}{\log x} = 6797{,}394$$

2500000 . . . 2600000

	251	252	253	254	255	256	257	258	259	260	
1		1	1							1	3
2	1	2		1	1						5
3	4		6	6	2	2	1	2	8	4	35
4	7	18	9	7	8	6	10	7	8	8	88
5	10	11	7	15	15	23	16	16	10	13	136
6	22	14	20	21	20	15	18	19	20	25	194
7	24	17	12	20	22	22	23	15	13	12	180
8	18	15	20	9	16	18	16	20	19	19	170
9	8	10	13	7	9	7	6	12	6	10	88
10	2	5	8	10	5	4	7	4	9	4	58
11	1	5	3	2	2	1	2	3	5		24
12	1	1	1	2		2	1	2	1	2	13
13	2	1							1	2	6
	677	675	696	670	670	671	678	698	693	676	6804

$$\int \frac{\mathrm{d}x}{\log x} = 6778{,}960$$

2600000 . . . 2700000

	261	262	263	264	265	266	267	268	269	270	
0				1							1
1			2					2			4
2	1	2	1		2		1	2	1		10
3	3	6	2	2	4		3	3	3	2	28
4	9	6	6	12	3	7	7	8	6	7	71
5	11	15	14	11	13	17	22	16	18	21	158
6	26	17	14	18	23	19	20	24	19	15	195
7	23	11	27	20	21	21	21	14	22	21	201
8	14	23	16	13	15	16	12	8	12	13	142
9	9	10	13	16	10	10	5	10	5	8	96
10	3	6	5	4	2	8	2	5	8	10	53
11	1	1		1	3	1	4	4	5	2	22
12		3		2	4	1	1	4	1	1	17
13							1				1
14							1				1
	653	681	672	680	689	695	660	665	681	686	6762

$$\int \frac{\mathrm{d}x}{\log x} = 6761{,}332$$

2700000 . . . 2800000

	271	272	273	274	275	276	277	278	279	280	
1						1			1		2
2	2		2			2			1		7
3	4	5	6	5	4	4	4	3	3	5	43
4	9	7	16	7	8	9	8	8	12	11	95
5	10	14	13	14	13	12	13	17	11	18	135
6	24	18	15	28	19	20	15	21	18	17	195
7	18	22	15	20	24	16	23	19	22	9	188
8	13	10	13	12	15	13	20	19	15	15	145
9	9	9	10	4	11	12	9	7	8	8	87
10	6	9	6	7	5	8	7	2	7	10	67
11	3	3	4	2		2		3	1	6	24
12	1	3		1	1	1			1	1	9
13							1	1			2
14											
15											
16											
17	1										1
	679	695	644	657	672	671	684	666	662	684	6714

$$\int \frac{\mathrm{d}x}{\log x} = 6744{,}430$$

2800000 . . . 2900000

	281	282	283	284	285	286	287	288	289	290	
1					1		1				2
2		2	4		5	2		1	1		15
3	2	4	4	3	4	3	1	3	2	4	30
4	9	7	6	9	7	8	10	11	10	8	85
5	14	7	14	14	7	16	19	16	18	15	140
6	18	17	20	13	23	18	16	18	15	21	179
7	24	22	21	20	20	27	22	23	21	22	222
8	13	18	9	20	13	12	9	12	12	14	132
9	10	17	12	12	8	6	14	9	10	11	109
10	7	4	6	3	5	7	5	5	8	3	53
11		1	3	3	5		1	2	1	2	18
12	2	1				1	2		2		8
13			1	2	2						5
14	1			1							2
	690	695	667	704	671	654	672	653	676	662	6744

$$\int \frac{\mathrm{d}x}{\log x} = 6728{,}220$$

2900000 . . . 3000000

	291	292	293	294	295	296	297	298	299	300	
1		1							1		2
2		1	2	1	2	2		1	1	3	13
3	3	3	5	2	8	6	4	4	5	4	44
4	7	7	6	6	7	9	6	6	6	4	64
5	20	11	14	18	12	15	17	19	16	11	153
6	17	21	22	18	18	16	11	26	21	17	187
7	19	30	18	22	22	25	27	13	15	23	214
8	14	11	12	12	17	11	13	11	14	19	134
9	10	9	12	13	9	6	12	12	9	11	103
10	6	4	5	6	3	6	8	7	9	4	58
11	2	1	3	1		2	1		1	4	15
12	2	1		1	2	2		1	2		11
13			1								1
14											
15							1				1
	680	663	671	680	649	652	694	658	671	687	6705

$$\int \frac{\mathrm{d}x}{\log x} = 6712{,}64$$

1000000 . . . 2000000

	110	120	130	140	150	160	170	180	190	200	
0							1				1
1	1	1	2	1	5	2	2	1		1	16
2	4	5	6	9	7	10	11	5	10	5	72
3	21	25	32	19	19	28	29	30	22	34	259
4	54	57	63	69	72	77	68	70	71	67	668
5	114	107	120	119	129	124	120	152	135	136	1256
6	171	170	160	173	183	199	159	174	175	182	1746
7	217	217	214	207	179	172	203	194	206	221	2030
8	164	160	168	161	183	149	174	147	161	148	1615
9	126	131	111	120	98	124	130	124	113	103	1180
10	71	77	73	70	73	63	63	61	74	62	687
11	39	32	35	33	34	29	26	26	23	30	307
12	12	11	9	15	16	17	9	10	10	5	114
13	6	5	5	3	2	6	3	5		3	38
14		2	1	1			1			3	8
15							1	1			2
16			1								1
	7210	7194	7081	7098	7028	6971	7012	6931	6955	6902	70382

$$\int \frac{\mathrm{d}x}{\log x} = 70427{,}78$$

2000000 . . . 3000000

	210	220	230	240	250	260	270	280	290	300	
0							1				1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	11	9	5	10	7	15	13	98
3	32	27	29	32	37	35	28	43	30	44	337
4	69	69	73	86	78	88	71	95	85	64	778
5	119	146	138	136	147	136	158	135	140	153	1408
6	197	183	179	176	193	194	195	195	179	187	1878
7	204	201	205	194	189	180	201	188	222	214	1998
8	157	168	168	158	151	170	142	145	132	134	1525
9	115	109	113	112	102	88	96	87	109	103	1034
10	63	52	44	55	58	58	53	67	53	58	561
11	21	18	30	28	23	24	22	24	18	15	223
12	8	9	10	7	7	13	17	9	8	11	99
13	2	4		1	5	6	1	2	5	1	27
14		3					1		2		6
15										1	1
16											
17								1			1
	6874	6857	6849	6787	6766	6804	6762	6714	6744	6705	67862

The group of one hundred numbers at position 26379 contains no prime number

The group of one hundred numbers at position 27050 contains 17 prime numbers.

$$\int \frac{\mathrm{d}x}{\log x} = 67915{,}733$$

GAUSS TO ENKE.

Highly esteemed friend!

— — The remarks on the frequency of prime numbers that you kindly sent me interested me in more than one way. They reminded me of my own work on this subject, whose beginnings lie far in the past, in 1792 or 1793, when I acquired LAMBERT's supplements to the logarithm tables. Even before I had begun the finer investigations of higher arithmetic, one of my first tasks was to turn my attention to the decreasing frequency of prime numbers. For this purpose I counted them in each group of a thousand and wrote the results on one of the attached blank leaves. I soon saw that, despite all its fluctuations, this frequency was on average approximately inversely proportional to the logarithm, so that the number of all primes below a given bound n would be approximately expressed by the integral

$$\int \frac{\mathrm{d}n}{\log n}$$

with the natural logarithm understood. Later, when I learned of the list printed in VEGA's tables (of 1796), extending up to 400031, I extended my count, which confirmed that relationship. In 1811 the appearance of CHERNAC's cribrum gave me great pleasure, and (since I had no patience for a sustained count in sequence) I very often spent an otherwise free quarter of an hour counting a group of a thousand, here or there; eventually, however, I gave it up altogether without quite finishing the million. Only later did I make use of GOLDSCHMIDT's diligence, partly to fill the remaining gaps in the first million and partly to continue the count using BURCKHARDT's tables Thus the first three millions have been counted (for many years now) and compared with the value of the integral. Here I give only a short extract:

Below	there are prime numbers	Integral $\int \frac{\mathrm{d}n}{\log n}$	Deviation	Your formula	Deviation
500000	41556	41606,4	+50,4	41596,9	+40,9
1000000	78501	79627,5	+126,5	78672,7	+171,7
1500000	114112	114263,1	+151,1	114374,0	+264,0
2000000	148883	149054,8	+171,8	149233,0	+350,0
2500000	183016	183245,0	+229,0	183495,1	+479,1
3000000	216745	216970,6	+225,6	217308,5	+563,5

I did not know that LEGENDRE had also concerned himself with this subject. Your letter prompted me to look in his *Théorie des Nombres*, and in the second edition I found some pages on it that I must have overlooked earlier (or forgotten since). LEGENDRE uses the formula

$$\frac{n}{\log n - A}$$

where A is supposed to be a constant, for which he takes 1,08366. A quick calculation then gives me the deviations in the above cases as

$$\begin{gathered} -23{,}3 \\ +42{,}2 \\ +68{,}1 \\ +92{,}8 \\ +159{,}1 \\ +167{,}6 \end{gathered}$$

These differences are even smaller than those with the integral, but they seem to grow faster as n increases, so it is quite possible that, if continued much further, they would exceed the latter. To bring the count and the formula into agreement, one would have to set, respectively, in place of $A = 1{,}08366$

$$\begin{gathered} 1{,}09040 \\ 1{,}07682 \\ 1{,}07582 \\ 1{,}07529 \\ 1{,}07179 \\ 1{,}07297 \end{gathered}$$

It seems that, as n grows, the (average) value of A decreases, but I venture no conjecture as to whether the limit as n grows to infinity will be 1 or a quantity different from 1. I cannot say that there are grounds for expecting a very simple limiting value; on the other hand, the excess of A over 1 could quite well be a quantity of order $\frac{1}{\log n}$. I would be inclined to believe that the differential of the function in question must be simpler than the function itself. Whereas I have assumed $\frac{\mathrm{d}n}{\log n}$ for it, LEGENDRE's formula would assume a differential function that would be approximately $\frac{\mathrm{d}n}{\log n-(A-1)}$. Your formula, moreover, could for a very large n be regarded as agreeing with

$$\frac{n}{\log n - \frac{1}{2k}}$$

where k is the modulus of BRIGGS's logarithms, and hence with LEGENDRE's formula if

$$A = \tfrac{1}{2k} = 1{,}1513 \text{ is set.}$$

Finally, I should mention that I have noticed a couple of differences between your counts and mine.

Between	59000	and	60000	you have	95	I	94
	101000		102000		94		93

The first difference may be due to the prime number 59023 appearing twice in LAMBERT's supplements. The group of a thousand from 101000—102000 teems with errors in LAMBERT's supplements: in my copy I have marked 7 numbers that are not prime and inserted 2 that were missing. Could you not persuade the young DASE to count the primes in the following millions from the tables at the Academy, which, I fear, the public is not meant to possess? In that case I should mention that, in the 2nd and 3rd millions, the count was made at my direction according to a special scheme that I had already used myself for part of the first million. The counts for each 100000 occupy one (small) octavo page in 10 columns, each referring to one group of ten thousand; there is also a column before them (on the left) and another after them on the right. As an example, here is one vertical column and the two additional columns from the interval $1000000 \ldots 1100000$ — — —

For an explanation, take the 1st vertical column, for example. The group of ten thousand from 1000000 to 1010000 contains 100 groups of a hundred; among these there is 1 containing only one prime; none at all with 2 or 3; 2 with 4 primes each; 11 with 5 each, and so on. Together they give $752 = 1 \,.\, 1 + 4 \,.\, 2 + 5 \,.\, 11 + 6 \,.\, 14 + \,.\,.$ The last column contains the aggregates from the 10 individual columns. The numbers 14. 15. 16 in the first vertical column are superfluous here, since no groups of a hundred contain so many primes; but they come into use on the following sheets. Finally, the 10 pages are again combined into 1, and thus cover the entire 2nd million.

But it is time to break off. — — — With heartfelt wishes for your well-being

Always yours

Göttingen, 24 December 1849. C. F. GAUSS.

TABLE
OF THE NUMBER OF CLASSES
OF BINARY QUADRATIC FORMS.

Hundred 1.
G. I. . . .(17). .(61)
1. 1. 2. 3.
4. 7
3 11. 19. 23.
27. 31. 43.
67
5 47. 79
7 71
9 59. 83
G. II. .(58). .(280)
1 5. 6. 8.
9. 10. 12.
13. 15. 16.
18. 22. 25.
28. 37. 58.
2 14. 17. 20.
32. 34. 36.
39. 46. 49.
52. 55. 63.
64. 73. 82.
97. 100
3 26. 29. 35.
38. 44. 50.
51. 53. 54.
61. 75. 76.
81. 87. 91.
92. 99
4 41. 62. 68.
94. 95. 98
5 74. 86
6 89
G. IV. .(25). .(136)
1 21. 24. 30.
33. 40. 42.
45. 48. 57.
60. 70. 72.
78. 85. 88.
93
2 56. 65. 66.
69. 77. 80.
84. 90. 96

Total 233. . .477
Irreg. 0 Impr. 74

Hundred 2.
G. I. . . . .(11). .(101)
3 163
5 103. 127
7 151
9 107. 139. 199
11 167
13 191
15 131. 179
G. II. . . . .(46). .(406)
2 142. 148. 193
3 106. 108. 109.
115. 118. 121.
123. 124. 135.
147. 157. 162.
169. 172. 175.
187
4 111. 113. 128.
137. 158. 178.
183. 196
5 119. 122. 125.
143. 159. 166.
181. 188. 197
6 116. 155. 171
7 101. 134. 149.
173
8 146. 164
10 194
G. IV. . . .(39). .(356)
1 102. 112. 130.
133. 177. 190
2 114. 117. 126.
132. 136. 138.
141. 144. 145.
150. 153. 154.
156. 160. 180.
184. 192. 198
3 104. 110. 129.
140. 152. 170.
174. 176. 182.
186. 189. 195.
200
4 161. 185
G. VIII. . .(4). . .(32)
1 105. 120. 165.
168

Total 291. . .895
Irreg. 0

Hundred 3.
G. I. . . . . (9). . . . . (109)
7 223
9 211. 243(*3*). 283
11 271
13 263
15 227. 239
21 251
G. II. . . . . (42). . . . . (482)
3 202. 207. 214. 235. 247. 262. 267. 268. 277. 298
4 226. 256. 289. 292. 295
5 218. 229. 242. 250
6 203. 212. 219. 233. 241. 244. 259. 274. 275. 279. 291
7 215. 278. 284. 287
8 254. 257
9 236. 293
10 206. 281
11 269
12 299
G. IV. . . . . (43). . . . . (512)
1 232. 253
2 205. 208. 213. 217. 220. 225. 228. 238. 252. 258. 265. 282. 288
3 201. 204. 216. 222. 231. 234. 237. 245. 246. 249. 255. 261. 270. 286. 294. 297. 300
4 221. 224. 248. 260. 272. 276
5 209. 230. 266. 290. 296
G. VIII. . . . (6). . . . . (64)
1 210. 240. 273. 280.
2 264. 285

Total 313. 1167
Irreg. 1 Impr. 183.

Hundred 4.
G. I. . . . . (9). . . . . (113)
7 343
9 307(*3*). 331. 367. 379
15 347
17 383
19 311. 359
G. II. . . . . (40). . . . . (554)
3 358. 397
4 313. 337. 382. 388
5 303. 316. 317. 319. 346. 361. 373. 375. 394
6 302. 323. 324. 327. 334. 351. 355. 363. 387
7 338. 349. 391
8 353
9 332. 335. 339(*3*). 362
10 386. 398
11 326. 389
12 356. 371. 395
13 314
G. IV. . . . . (43). . . . . (608)
2 301. 310. 322. 328. 333. 340. 352. 372. 400
3 304. 309. 315. 318. 325. 342. 348. 364. 366. 368. 370. 378. 393. 396
4 305. 306. 308. 320. 350. 354. 369. 376. 377. 380. 384. 392. 399
5 321. 344. 365. 381.
6 329
7 341. 374
G. VIII. . . . (8). . . . . (88)
1 312. 330. 345. 357. 385
2 336. 360. 390

Total 325. 1363
Irreg. 2 Impr. 229

NEGATIVE DETERMINANTS.

Hundred 5.
G. I. . . . .(10). .(174)
7 463. 487
9 499
15 439. 443
21 431. 467
25 479
27 419. 491
G. II. . . .(33). .(512)
3 403. 427
4 457. 466. 478
5 412. 415. 421. 422. 423
6 433. 436. 475. 484
7 447. 454
8 407. 409. 452. 471
9 411. 428. 451. 459(*). 486
10 401. 449. 482. 500
13 458
14 404
15 461
16 446
G. IV. . . .(49). .(760)
2 418. 438. 442. 445. 448. 498
3 405. 417. 424. 430. 432. 435. 450. 453. 460. 472. 473. 477. 483. 490. 492. 493. 496
4 402. 406. 410. 414. 441. 444. 468. 469. 481. 485. 495
5 413. 437. 455. 470. 474. 476. 488. 489
6 416. 425. 426. 434. 464. 497
7 494
G. VIII. . .(8). .(120)
1 408. 462
2 420. 429. 456. 465. 480
3 440

Total 336. . .1566
Irreg. 1

Hundred 6.
G. I. . . . . .(7). .(133)
9 547
15 523. 571
21 503. 587
25 599
27 563
G. II. . . .(40). .(724)
4 562. 577. 583
5 508. 538. 541
6 507. 526. 529. 543. 567
7 502. 511. 535
8 512. 514. 548. 559. 578
9 515. 519. 527. 531. 556. 557. 575. 586
11 551. 554. 591
12 539. 542. 579. 593
14 596
15 509. 524. 566
16 521. 569
G. IV. . . .(41). .(672)
2 505. 522. 532. 553. 568. 592. 598
3 513. 517. 533. 537. 540. 550. 555. 565. 588. 595. 597
4 501. 518. 544. 558. 564. 573. 574. 576(*2*). 580(*2*). 582. 589
5 534. 572. 590
6 516. 549. 594
7 506. 530. 536. 581
8. . . 545. 584
G. VIII. .(12). .(200)
1 520
2 504. 510. 525. 528. 552. 561. 570. 585. 600
3 546. 560

Total 347. . .1729
Irreg. 2

Hundred 7.
G. I. . . . .(8). . .(138)
9 643
13 607. 631
15 619. 683. 691
25 647
33 659
G. II. . . .(37). .(718)
3 652
5 613. 625. 694
6 603. 617. 622. 628. 655. 667. 673. 676. 687
7 604. 634. 639. 653
9 661. 675(*3*). 679
10 601
11 623. 662. 668
12 674. 695
13 698
14 641. 686. 692
16 611. 635. 671. 677. 699
17 614
18 626
G. IV. . . .(43). .(812)
2 658. 697
3 606. 610. 618. 627. 637. 648. 669. 670. 682. 685. 688. 700
4 612. 632. 640. 642. 646. 657. 663
5 615. 633. 636. 638. 649. 664. 666. 678. 681
6 602. 605. 608. 620. 621. 650. 651. 684
7 654
8 644. 656
9 629
10 689
G. VIII. .(12). .(216)
2 609. 616. 624. 630. 645. 660. 672. 690. 693.
3 665. 680. 696.

Total 350. .1884
Irreg. 1

Hundred 8.
G. I. . . . . .(6). . .(110)
13 727
15 739. 751. 787
21 743
31 719
G. II. . . . . .(39). . .(860)
4 772
5 709. 757
6 718. 723. 763. 775
7 703. 733. 778
8 799
9 707. 722. 729. 747. 771. 783. 796
10 711. 724. 769. 788
11 758. 767
12 706. 766
13 746. 764. 773
15 716. 779. 797
16 791
17 701
18 731. 755(*3*)
20 734. 761
21 794
G. IV. . . . . .(42). . .(792)
2 708. 742. 793
3 702. 715. 730. 748. 753. 762. 795
4 712. 717. 721. 732. 735. 736. 738. 745. 768. 784. 785. 786. 790
5 726. 737. 750. 752. 754. 774. 781
6 704. 713. 725. 756. 759. 782. 800
8 710. 740. 749. 789
10 776
G. VIII. . . . .(13). . .(264)
1 760
2 720. 765. 777. 792. 798
3 705. 714. 728. 741. 744. 780
4 770

Total 356. . .2026
Irreg. 1

Hundred 9.
G. I. . . . . (8). . . . (164)
9 823. 883
21 811. 827. 859. 863.
29 887
33 839
G. II. . . . . (34). . . . (750)
4 862
5 847. 853. 877
6 802. 898
7 807. 838. 841. 892.
8 895
9 835. 843. 844. 867. 886. 891(*3*)
10 878
11 829. 871. 879
13 842
14 818. 831
15 803. 815. 821. 851. 875
16 809. 857
20 881
21 899
22 866
G. IV. . . . (47). . . (1024)
3 808. 813. 814. 817. 826. 828. 837. 856
4 820(*2*). 832. 834. 850. 852. 855. 865. 868. 873. 882. 889. 900(*2*)
5 822. 830. 872. 874
6 801. 804. 810. 812. 819. 833. 848. 864. 876. 890. 894
7 806. 845. 849. 860. 893
8 846. 869. 884(*2*). 896
10 824. 836
11 854
G. VIII. . . (10). . . . (200)
2 805. 858. 870. 880. 897
3 816. 825. 861. 885. 888
G. XVI. . . . (1). . . . (16)
1 840

Total 360. 2154
Irreg. 4

Hundred 10.
G. I. . . . . (8). . . . (174)
9 907
11 967
15 947
17 991
19 919
27 983
31 911
45 971
G. II. . . . . (33). . . (810)
5 982
6 955
7 997
8 943. 958. 961
9 922. 931. 963. 972
10 916. 927. 937. 977
12 932. 939. 964. 979. 995. 999
13 934. 951. 998
15 908. 923. 956
16 953
18 914. 929. 959. 974(*3*)
20 926
23 941
G. IV. . . . (45). . . . (976)
2 928
3 913. 918. 925. 933. 940. 942. 949. 970. 973. 988
4 903. 904. 993. 938. 946. 975. 994
5 917. 921. 968. 1000
6 901. 905. 915. 948. 954. 976. 978. 980. 981. 985. 987. 996
7 902. 906. 909. 935. 962
8 992
9 944. 950. 989
11 965. 986
G. VIII. . . (14). . . . (312)
2 910. 912. 952. 957. 960
3 924. 930. 936. 945. 966. 969. 984. 990
5 920

Total 366. 2272
Irreg. 1

Hundred 11.
G. I. . . . . .(7). . . . .(191)
9 1087
15 1051
19 1063
23 1039
35 1031
39 1019
51 1091
G. II. . . . . .(35). . . .(880)
5 1093
6 1003. 1027. 1033. 1042
8 1024. 1047
9 1018. 1059. 1075(*3*). 1083. 1099
10 1006. 1009
11 1021. 1082. 1084
12 1043. 1058
13 1013. 1052. 1061. 1094.
15 1007. 1069
16 1028
17 1079
18 1011. 1055. 1067. 1097
21 1004. 1046
22 1049. 1076
G. IV. . . . . .(44). . . . .(984)
2 1012
3 1030. 1038. 1048. 1068 1072. 1090
4 1002. 1015. 1017. 1023. 1054. 1057. 1060. 1078. 1081
5 1037. 1066. 1071. 1098
6 1026. 1035. 1036. 1044. 1053. 1062. 1073. 1077. 1089. 1096. 1100
7 1010. 1014. 1029. 1086. 1095
8 1016. 1022. 1025. 1074. 1088(*2*)
9 1041. 1070
11. . . 1034
G. VIII. . . . . .(14). . . .(344)
2 1005. 1008. 1032. 1045. 1065. 1092
3 1020. 1050. 1080
4 1040. 1056. 1085
5 1001. 1064

Total 365. 2399
Irreg. 2

Hundred 12.
G. I. . . . . .(6). . . . .(148)
15 1123
21 1163. 1171
23 1103
27 1187(*3*)
41 1151
G. II. . . . . .(36). . . .(924)
6 1108. 1138. 1198
7 1117. 1183
8 1129. 1153. 1156. 1159
9 1107(*3*). 1132. 1135. 1142. 1147
10 1143
11 1111. 1114. 1126. 1167
12 1127. 1186. 1191. 1195
15 1115. 1174. 1175. 1179
16 1119
18 1172. 1193
19 1199
20 1124
23 1181
24 1139
25 1109
28 1154
G. IV. . . . . .(40). . . .(1064)
3 1162. 1177. 1192
4 1149. 1150. 1152. 1168. 1178. 1180
5 1102. 1125. 1137. 1165. 1182. 1189
6 1131. 1134. 1141. 1145. 1158. 1164. 1188
7 1101. 1112. 1133. 1136. 1148. 1157. 1194
8 1146
9 1116. 1118. 1161. 1166
10 1184
11 1121. 1130
12 1106. 1169. 1196
G. VIII. . . . .(18). . . . .(408)
2 1105. 1110. 1113. 1120. 1122. 1128. 1170. 1185. 1197
3 1144. 1155. 1173. 1176 1200
4 1104. 1140
5 1160. 1190

Total 382. 2544
Irreg. 2

Hundred 13.
G. I. . . . . .(6). . . . . .(190)
23 1279
27 1231. 1291
33 1283
35 1223
45 1259(*3*)
G. II. . . . . .(38). . . . . .(986)
5 1213
6 1227. 1243. 1255. 1282. 1297
7 1237
8 1201. 1252
9 1203. 1207. 1215. 1219. 1228(*3*). 1267(*3*)
10 1261. 1263. 1268.
12 1202. 1234. 1299
13 1247
14 1294
15 1250
16 1217. 1249
17 1277
18 1251. 1262. 1289
19 1229. 1244
20 1214. 1271
21 1211. 1226. 1238
29 1286
G. IV. . . . . .(40). . . . .(1008)
3 1222. 1258. 1285
4 1204. 1225. 1233. 1246. 1278
5 1210. 1212. 1257. 1264. 1270. 1273. 1276. 1287
6 1208. 1216. 1236. 1242. 1269. 1275. 1292. 1293. 1296. 1300
7 1206
8 1220(*2*). 1239. 1241. 1253. 1266. 1280. 1298
9 1235. 1274. 1295
10 1205. 1284
13 1256
VIII. . . . .(16). . . . . .(416)
2 1240. 1248. 1288. 1290
3 1218. 1230. 1254. 1260. 1272. 1281
4 1221. 1224. 1232. 1245
5 1209. 1265

Total 370. 2600
Irreg. 4

Hundred 14.
G. I. . . . . .(7). . . . . .(191)
11 1303
15 1327
27 1367. 1399
33 1307. 1331
45 1319
G. II. . . . . .(32). . . . . .(846)
5 1318
6 1387
7 1372
8 1348
9 1306. 1315(*3*). 1323(*3*). 1324. 1347. 1363. 1366. 1369. 1373. 1383
10 1375
11 1354
12 1321. 1339. 1351
13 1381
14 1346. 1359
15 1388
17 1343
18 1355. 1371
19 1382
21 1322
22 1391
24 1379
25 1301
30 1361
G. IV. . . . . .(46). . . . . .(1340)
4 1312(*2*). 1332(*2*). 1345. 1357. 1393
5 1317. 1333. 1338. 1342. 1378. 1384. 1390. 1398
6 1308. 1313. 1336. 1337. 1350. 1358. 1362. 1377. 1395. 1397
7 1311. 1335. 1341. 1352. 1374. 1389. 1396
8 1314. 1334
9 1310. 1325. 1328. 1329. 1340. 1356(*3*)
10 1376
11 1304. 1370
12 1316. 1385. 1394
14 1349. 1364
G. VIII. . . . . .(13). . . . . .(328)
2 1302. 1353. 1360. 1380
3 1309. 1330. 1368. 1392
4 1305. 1344. 1386. 1400
5 1326
G. XVI. . . . . .(2). . . . . .(32)
1 1320. 1365

Total 391. 2737
Irreg. 5 Progr. 3192

Hundred 15.
G. I. . . . . .(10). . . . . .(308)
9 1423
21 1483
23 1447. 1471
33 1459
37 1487
39 1439. 1451. 1499
45 1427
G. II. . . . . .(26). . . . . .(746)
6 1411. 1467
7 1402. 1453
8 1438
9 1458. 1468
10 1444. 1486. 1489. 1492.
11 1429. 1493
15 1431. 1478
16 1412
17 1415. 1418
18 1409. 1433. 1475
19 1436
21 1403
26 1481
29 1466
30 1454
G. IV. . . . . .(49). . . . . .(1348)
3 1432. 1435. 1450
4 1408. 1417. 1422. 1462. 1465. 1474. 1477. 1498
5 1495. 1497. 1500
6 1404. 1405. 1407. 1413. 1420. 1437. 1442. 1443. 1452. 1457. 1472
7 1401. 1414. 1441. 1455. 1461. 1473. 1479
8 1426. 1434. 1446. 1463. 1476
9 1419. 1445. 1448. 1490. 1491
10 1460. 1494
11 1406
12 1421. 1424. 1484
14 1469
G. VIII. . . . .(15). . . . . .(424)
2 1428. 1488
3 1425. 1456. 1464. 1480. 1482. 1485
4 1410. 1416. 1430. 1440(*2*). 1449. 1470
7 1496

Total 378. 2826
Irreg. 1 Propr. 3282

Hundred 16.
G. I. . . . . .(9). . . . . .(299)
15 1567
19 1543
21 1523
27 1579
33 1531. 1583
49 1511
51 1559. 1571
G. II. . . . . .(24). . . . . .(656)
6 1507. 1555. 1588
7 1527. 1597
9 1516. 1519. 1549. 1563
10 1522
11 1503. 1591
12 1502. 1587
17 1532. 1546. 1594
18 1539(*3*)
19 1535
20 1553
22 1538. 1556
25 1514
27 1574
G. IV. . . . . .(53). . . . . .(1564)
3 1558. 1593
4 1510. 1513(*2*). 1528. 1537. 1552. 1578. 1582(*2*). 1600(*2*)
5 1534, 1542. 1570. 1573. 1576
6 1501. 1506. 1521. 1525. 1548. 1572. 1575. 1585
7 1557. 1562. 1564. 1565. 1569. 1577
8 1504. 1508. 1536. 1551. 1561. 1568(*2*). 1598
9 1515. 1541. 1547. 1566. 1599
10 1509. 1524. 1544. 1592
11 1586
12 1517. 1526. 1550. 1580. 1595
13 1529. 1589
G. VIII. . . . .(13). . . . . .(360)
2 1540
3 1512. 1518. 1530. 1533. 1545. 1554. 1584
4 1520. 1590(*2*). 1596
5 1505. 1581
G. XVI. . . . . .(1). . . . . .(32)
2 1560

Total 389. 2911
Irreg. 6 Propr. 3416

Hundred 17.
G. I. . . . . .(6). . . . . .(182)
17 1663
21 1627
27 1607
33 1699
39 1667
45 1619
G. II. . . . . .(37). . . .(1116)
6 1618
7 1642
8 1657
9 1603. 1621. 1675(*). 1683. 1687
10 1678. 1681. 1684
11 1639. 1654. 1693
12 1647. 1651
13 1669
14 1609. 1623. 1697
15 1611. 1622. 1643. 1682
16 1636
19 1637. 1671
20 1604
21 1613. 1658
22 1631. 1646. 1655
26 1679
27 1676. 1691
28 1601
G. IV. . . . . .(41). . . . . .(1312)
3 1612
4 1633. 1660. 1698
5 1626. 1648. 1660. 1662. 1688. 1692. 1695
6 1615. 1620. 1635. 1659. 1666. 1668. 1690. 1696
7 1606. 1614. 1630. 1670
8 1602. 1628. 1673
9 1644. 1674. 1689
10 1625. 1629. 1652
11 1641. 1686
12 1649. 1661. 1664. 1694
13 1685
14 1616
16 1634
G. VIII. . . .(15). . . . . .(368)
2 1605. 1632. 1645. 1653 1672. 1677
3 1617. 1638
4 1608. 1610. 1624. 1640. 1650. 1656. 1665
G. XVI. . . . . .(1). . . . . .(32)
2 1680

Total 380. 3010
Irreg. 1 Impr. 513

Hundred 18.
G. I. . . . . .(5). . . . . .(95)
15 1723. 1747
17 1783
21 1787
27 1759
G. II. . . . . .(35). . . . .(1182)
10 1714. 1753. 1774
12 1726. 1731. 1732. 1762. 1777. 1795
13 1719. 1735. 1741. 1789
14 1703. 1711. 1775
15 1707. 1756. 1772. 1779
17 1733
18 1727. 1763(*3*). 1791
19 1754
21 1709. 1715. 1724
23 1718
24 1751
25 1766. 1799
26 1721
29 1706
30 1739
G. IV. . . . .(41). . . . .(1260)
3 1708
4 1717. 1737. 1738. 1780. 1792
5 1702. 1750. 1758. 1761. 1765. 1773. 1786. 1798
6 1728. 1743. 1744. 1771. 1782. 1797
7 1757. 1788
8 1764(*2*). 1767
9 1701. 1712. 1713. 1730. 1734. 1755(*). 1793
10 1745. 1746. 1748. 1778. 1796
11 1742
13 1790
16 1769. 1784
17 1781
G. VIII. . . . .(18). . . . .(536)
2 1705. 1710. 1752. 1768
3 1720. 1722. 1729. 1740. 1800
4 1716. 1725. 1776. 1794
5 1749. 1770
6 1704. 1736. 1760
G. XVI. . . . .(1). . . . . .(32)
2 1785

Total 399. 3105
Irreg. 3 Impr. 525

Hundred 19.
G. I. . . . . (7) . . . . . (263)
15 1867
19 1831
27 1879
43 1847
45 1823. 1871
69 1811
G. II. . . . . (31) . . . . . (994)
6 1807. 1873
7 1852
8 1822. 1828
9 1843. 1863. 1882
10 1858
11 1849
12 1803
14 1801. 1838
15 1819. 1835. 1875. 1891. 1894
17 1877
18 1899
19 1861
20 1839
21 1851. 1859. 1868. 1883
23 1814
24 1895
28 1874
30 1844
36 1889
G. IV. . . . . (45) . . . . . (1416)
4 1813. 1842. 1864. 1897
5 1810. 1857. 1887. 1893
6 1812. 1815. 1818. 1825. 1827. 1837. 1878. 1888. 1892. 1900
7 1816. 1846. 1855. 1898
8 1802. 1808. 1866. 1876. 1884
9 1804. 1809. 1821. 1834. 1836. 1853. 1862
10 1805. 1817. 1829. 1841. 1850. 1854
12 1856. 1865
13 1832
14 1826
16 1886(*2*)
G. VIII. . . . . (16) . . . . . (496)
2 1870. 1885
3 1830. 1833. 1840. 1890
4 1824. 1845. 1860. 1872
5 1806. 1820. 1869. 1880. 1881. 1896
G. XVI. . . . . (1) . . . . . (16)
1 1848

Total 393. 3185
Irreg. 1 Impr. 513

Hundred 20.
G. I. . . . . (6) . . . . . (252)
21 1987
27 1999
33 1951.
39 1907
63 1931(*3*)
69 1979
G. II. . . . . (33) . . . . . (1090)
7 1948
8 1983
9 1915. 1927. 1933. 1963. 1996
10 1906. 1975
11 1903. 1942
12 1939. 1982. 1993
14 1954
15 1923
16 ·1922. 1943
18 1913. 1966. 1967. 1971(*3*)
21 1901. 1959. 1973. 1997
22 1919
25 1916
26 1934
27 1964. 1994
28 1991
35 1949
G. IV. . . . . (43) . . . . . (1356)
3 1978
4 1912. 1918(*2*). 1945. 1957
5 1930. 1962. 1969. 1981
6 1908. 1917. 1926. 1936. 1941. 1947. 1972. 1984. 1990
7 1909. 1929. 1935
8 1911. 1924. 1940. 1958. 1961
9 1902. 1944. 1955. 1977. 1998
10 1921. 1928. 1952. 1956. 1985. 2000
12 1982. 1986. 1988
13 1970
14 1910
17 1946
G. VIII. . . . . (18) . . . . . (584)
2 1992
3 1905. 1932. 1950. 1960. 1968. 1995
4 1920. 1938. 1953. 1974. 1980. 1989
5 1904. 1965,
6 1914. 1925
7 1976

Total 388. 3282
Irreg. 3 Impr. 556

Hundred 21.
G. I. . . . . .(8). . . . . .(284)
21 2011. 2083
27 2003
33 2027
35 2087
45 2039. 2063
57 2099
G. II. . . . . .(30). . . . . .(1054)
6 2017. 2062
8 2095
9 2023. 2038. 2047. 2053
12 2059. 2098
14 2007. 2018
15 2043. 2071. 2092
16 2048
17 2026. 2029
19 2031. 2069
20 2078
21 2012
22 2089
24 2019
25 2042
27 2051. 2075(*3*)
28 2066
30 2036. 2081
32 2084
G. IV. . . . . .(42). . . . . .(1376).
4 2020. 2077
5 2032. 2073. 2074
6 2022. 2025. 2028. 2035. 2050. 2052. 2067. 2068. 2082. 2086. 2096
7 2008. 2033. 2044. 2055. 2058. 2094
8 2004. 2005. 2034. 2041. 2056
9 2014. 2049. 2060. 2076. 2079. 2091
10 2057. 2061
12 2006. 2009. 2045
13 2015
15 2096
17 2021
18 2054
G. VIII. . . . . .(19). . . . . .(632)
2 2002. 2013. 2080. 2088
3 2037. 2065
4 2010. 2016. 2046. 2072. 2100.
5 2030. 2070. 2085. 2093
6 2001. 2064. 2090
7 2024
G. XVI. . . . . .(1). . . . . .(32)
2 2040

Total 404. 3378
Irreg. 1 Impr. 560

Hundred 2
G. I. . .(5). .(149)
13 2143
21 2179
27 2187(*3*)
39 2131
49 2111
G. II. . .(33).(1174)
8 2113. 2137
9 2122. 2167. 2188
10 2164
11 2182
12 2107. 2116
13 2102. 2197
14 2127
15 2151. 2191
16 2153. 2194
17 2103. 2119
18 2155. 2161. 2199
21 2123. 2138. 2147. 2171. 2183. 2186
24 2195
28 2129
30 2126. 2159
32 2174
39 2141
G. IV.(46).(1592)
5 2101. 2118. 2125. 2152. 2158. 2173. 2178
6 2104. 2115. 2132. 2139. 2148. 2157. 2163. 2172.
7 2110. 2140. 2146. 2149. 2165
8 2134. 2176(*2*) 2192
9 2106. 2108. 2117. 2124. 2133(*3*). 2175. 2181. 2198
10 2150. 2154. 2166. 2177
11 2135
12 2105. 2156. 2168. 2169. 2196
14 2114. 2144. 2162
15 2189
16 2180
G. VIII.(14).(424)
2 2128. 2170
3 2160. 2185. 2190. 2193. 2200
4 2112(*2*). 2130. 2142
5 2109. 2121. 2136
7 2120
G. XVI.(2). . .(80)
2 2145
3 2184

Total 399. . .3419
Irreg. 4 Impr. 585

Hundred 23.
G. I. . . .(7). .(217)
15 2203
21 2251
29 2287
33 2267
35 2239
39 2207
45 .2243(*3*)
G. II. .(29).(1084)
7 2293
9 2221. 2227. 2283
10 2281
11 2215. 2263
12 2209
13 2218
14 2258
15 2237. 2269. 2284. 2299
16 2206
17 2234
18 2228
20 2297
21 2213. 2259
22 2271
24 2273
27 2252. 2291
28 2279
29 2231
32 2276
36 2219(*3*)
39 2246
G. IV.(46).(1612)
4 2212. 2242. 2248. 2272
5 2202. 2230. 2247. 2290
6 2223. 2257. 2260. 2268. 2275. 2278
7 2217. 2238. 2270
8 2236. 2245. 2254(*2*). 2286. 2292. 2298
9 2214. 2221. 2235(*3*). 2241. 2253. 2266. 2295. 2300.
10 2249. 2250. 2255. 2282
11 2204. 2216
12 2211. 2225. 2229
13 2222
14 2274
15 2264. 2285
16 2201
19 2294
G. VIII.(17).(584)
2 2233. 2277
3 2205. 2220. 2262
4 2208. 2232. 2244. 2256. 2265. 2289. 2296

5 2226. 2288
6 2240
7 2210
9 2261
G. XVI.(1)..(32)
2 2280

Total 401...3529
Irreg. 4 Impr. 571

Hundred 24
G. I....(7)..(291)
15 2347
29 2311. 2383
39 2371
57 2339
59 2399
63 2351
G. II..(32).(1106)
7 2335
8 2302. 2308. 2377
11 2326. 2374
12 2307. 2323. 2395
13 2362. 2367
14 2359
15 2303. 2319. 2341. 2363
16 2386
17 2333. 2389. 2391
19 2381
20 2375
21 2342. 2348. 2357
24 2327. 2372
25 2396
27 2315(*3*)
30 2393
32 2306
33 2309
G. IV..(40).(1520)
4 2332. 2353. 2368
5 2398
6 2305. 2317. 2322. 2338. 2358. 2388
7 2314. 2382
8 2304. 2312. 2313. 2329(*2*). 2343. 2350. 2356
9 2318. 2344. 2349. 2355. 2361. 2387
11 2334. 2364.
12 2316. 2331. 2376. 2379(*2*). 2390
14 2324. 2354. 2384
15 2321. 2330. 2378
16 2336
18 2369

G. VIII.(20).(648)
2 2392
3 2325. 2346. 2352. 2370. 2373. 2380
4 2320. 2328. 2337. 2340. 2365. 2385(*2*). 2397. 2400(*2*).
5 2360. 2394.
6 2301. 2376
7 2345
G. XVI. .(1). .(32)
2 2310

Total 407. . .3597
Irreg. 5 Impr. 611

Hundred 25.
G. I. . .(5). .(217)
21 2467
33 2423
37 2447
57 2459
69 2411
G. II. .(35).(1250)
9 2403(*3*). 2437(*3*).
2443. 2458
10 2407. 2452. 2473. 2487. 2500
12 2419. 2468. 2479
13 2428
14 2401. 2446. 2455
15 2476
16 2434. 2462
17 2463
18 2417. 2491
19 2477
20 2402. 2404. 2498
21 2427
22 2439
27 2426
28 2495
30 2483
31 2471
33 2435
38 2441
39 2474
G. IV.(38).(1472)
4 2410
5 2422. 2433. 2494
6 2412. 2413. 2425. 2451. 2475.
2482. 2488. 2493
7 2416. 2431. 2438. 2497
8 2454
9 2430(*3*). 2461
10 2449
11 2421. 2489. 2492
12 2420(*2*). 2432. 2450.
2466. 2484. 2499
13 2453. 2469. 2481
14 2429. 2486
15 2406. 2444
17 2456
18 2414
G. VIII.(22).(720)
3 2418. 2424. 2440. 2457. 2472.
2485
4 2436. 2442. 2445. 2448(*2*).
2464. 2465. 2470. 2478. 2490.
2496
5 2405. 2409. 2415. 2460
6 2408. 2480

Total 403. .3659
Irreg. 5 Impr. 595

Hundred 26.
G. I. . .(7). .(301)
21 2503
33 2539
35 2543
41 2551
51 2531
57 .2591
63 2579
G. II. .(29).(1028)
8 2578
9 2515. 2557. 2563(*3*).
2566. 2572
10 2527
12 2587. 2593
13 2524
15 2523. 2575. 2518. 2599
16 2521
18 2511. 2547
19 2554
20 2559
21 2507. 2571
22 2567. 2594
25 2582. 2588
28 2564
32 2519. 2558
35 2549
G. IV.(45).(1752)
4 2533. 2542(*2*)
5 2577
6 2512. 2517. 2538. 2545. 2548.
2592. 2598
7 2502. 2509. 2535. 2536. 2556.
2583
8 2506. 2513. 2528. 2560. 2569.
2589
9 2522. 2555. 2581. 2595
10 2514. 2529. 2532. 2596
11 2570. 2573
12 2597
13 2510
14 2501. 2525. 2586
15 2526. 2534. 2537. 2540
16 2546. 2561
18 2504. 2516
G. VIII.(18).(648)
3 2508. 2530. 2550. 2553. 2562.
2590
4 2568. 2580. 2584
5 2505. 2541. 2544. 2552 2585

6 2565. 2574. 2600
8 2576
G. XVI.(1)..(32)
2 2520

Total 405..3761
Irreg. 2 Impr. 641

Hundred 27.
G. I. . .(7). . .(231)
15 2647. 2683
23 2671
39 2659
43 2663
45 2699(*3*)
51 2687
G. II. .(29).(1196)
10 2638
11 2623. 2662. 2677
12 2611. 2689. 2692
14 2612
15 2602. 2643
16 2617. 2633. 2657
18 2619(*3*). 2627. 2644
21 2693
23 2614. 2615
24 2631. 2654
26 2642
27 2675(*3*)
30 2603. 2606
31 2621
33 2636
39 2651
42 2609
G. IV.(46).(1776)
3 2608
4 2605
5 2641
6 2620. 2629. 2650. 2653. 2658.
2667. 2668. 2676. 2682. 2695.
2698
7 2607
8 2601. 2628(*2*). 2655.
2674. 2686
9 2626. 2634. 2635. 2637.
2646(*3*). 2673. 2700(*3*)
10 2656. 2678
11 2645. 2648. 2649. 2672
12 2681. 2691. 2696
13 2679
15 2630. 2684. 2690. 2694
16 2624(*3*). 2639. 2669
17 2666
18 2681
G. VIII.(17).(584)
2 2632
3 2613. 2622. 2680. 2685. 2697
4 2652. 2665. 2688
5 2610. 2618. 2625. 2664. 2670.
6 2604. 2660
7 2616

G. XVI. .(1). .(32)
2 2640

Total 401. . .3819
Irreg. 7 Impr. 625

Hundred 28.
G. I. . .(6). .(208)
21 2707 2767
33 2731
39 2791
41 2719
53 2711
G. II.(29).(1190)
9 2787. 2797
10 2722. 2743
12 2713
13 2762
14 2734. 2753
15 2727. 2732. 2764
18 2723. 2763(*3*). 2783
19 2738. 2746. 2799
20 2777
21 2749. 2779
22 2798
27 2747. 2759
29 2741
30 2708.
31 2735
39 2771
40 2729
41 2789
G. IV.(47).(1864)
4 2773. 2788
5 2776
6 2704. 2710. 2715. 2718. 2725. 2740. 2748. 2752. 2755. 2758. 2794
7 2703. 2761. 2766. 2782
8 2733. 2742. 2775. 2785
9 2716. 2770. 2778. 2781. 2795
10 2724. 2751
11 2757
12 2701. 2702(*2*). 2739. 2754 2780
13 2721. 2792
14 2744. 2768. 2774
15 2750. 2796
17 2726
18 2705. 2786
20 2714. 2756(*2*)
G. VIII.(16).(568)
2 2737
3 2728. 2800

4 2706. 2709. 2717. 2745. 2772.
2790. 2793
5 2712. 2769
6 2720. 2736. 2784
7 2765
G. XVI.(2)..(64)
2 2730. 2760

Total 412. .3894
Irreg. 3 Impr. 644

Hundred 29.
G. I. .(6). .(250)
25 2887
27 2803
33 2851
45 2843
57 2879
63 2819
G. II. .(32).(1298)
8 2878
10 2818. 2836. 2857
11 2815. 2863
12 2827
13 2809. 2823. 2839. 2854
15 2875. 2883. 2899
16 2833
18 2867. 2897
19 2858
20 2866
23 2837
24 2811
26 2807
27 2859. 2891(*3*)
30 2801. 2855
31 2876
33 2861
34 2804. 2831. 2894
36 2846
G. IV.(43).(1680)
4 2842. 2893
5 2830. 2853
6 2802. 2872. 2892
7 2812. 2881
8 2817. 2845. 2847: 2848(*2*).
2868. 2884
9 2806. 2828. 2835(*3*).
2862. 2887. 2888. 2890. 2895
10 2810. 2844. 2869. 2871. 2874.
2896
11 2841
12 2816. 2822. 2824. 2825. 2852.
2873. 2900.
13 2826.
15 2813. 2864. 2889
16 2882
21 2834
G. VIII.(17).(648)
2 2832
3 2808. 2860
4 2821. 2829. 2850(*2*).
2865. 2880. 2898
5 2814. 2838. 2877. 2886
6 2820
7 2870

8 2840. 2849
G. XVI.(2)..(96)
3 2805. 2856

Total 410..3972
Irreg. 4 Impr. 636

Hundred 30.
G. I..(6)..(322)
31 2927
33 2971
39 2963
59 2903
73 2999
87 2939
G. II..(33).(1266)
8 2962
9 2902. 2923. 2998
10 2983
11 2917. 2935
12 2947. 2953. 2995
13 2908
14 2932
15 2956. 2986
17 2918
18 2916. 2943. 2979
20 2942. 2959
21 2911. 2931. 2972
24 2974. 2991
26 2969
27 2951. 2957
30 2978. 2987
33 2906
35 2909
43 2966
G. IV.(37).(1588)
5 2965
6 2907. 2914. 2938. 2977. 2997
7 2913. 2930. 2941. 2973
8 2944. 2946. 2949. 2980(*2*)
9 2950. 2955. 2988. 2989
10 2919. 2929. 2948. 2975
11 2922. 2933. 2934. 2967
12 2993(*2*)
13 2901. 2984
16 2921. 2994. 2996.
18 2915. 2924
20 2936. 2954. 2981
G. VIII.(24).(888)
2 2968
3 2905. 2920. 2937. 2970. 2982. 2992
4 2928. 2940. 2952. 2958. 2985
5 2904. 2910. 2926. 2990. 3000

6 2912. 2925. 2961. 2964. 2976
8 2945. 2960

Total 412. .4064
Irreg. 2 Impr. 714

Hundred 43.
G. I. . .(7). .(425)
27 4243
45 4219
51 4231
63 4283
65 4271
69 4211
105 4259
G. II.(32).(1592)
12 4222. 4258. 4267. 4273
13 4207. 4282
14 4279
15 4204. 4227
17 4261
18 4201. 4291(*3*). 4297
19 4252
21 4203. 4253
22 4223
24 4239. 4287. 4295
26 4217. 4244
27 4262. 4299
30 4276
31 4247
39 4229
40 4286
42 4274
54 4226. 4241
56 4289
G. IV.(38).(1780)
6 4225. 4237. 4288
7 4210. 4213
8 4228. 4249
9 4236. 4246. 4255. 4263. 4285. 4293. 4294. 4300(*3*)
11 4215. 4238. 4281. 4298
12 4212(*2*). 4232. 4251. 4275(*2*). 4292
13 4202. 4206. 4208. 4234
14 4205
15 4235. 4250. 4266
17 4269
18 4220. 4265. 4268
19 4254
20 4214
G. VIII(22). .(976)
3 4218. 4257. 4272
4 4216. 4240. 4260. 4270. 4278
5 4230. 4233. 4242. 4264. 4284
6 4245. 4248. 4277
7 4209
8 4221. 4224. 4296
9 4280
10 4256

G. XVI.(1)..(48)
3 4290
Total 415....4821
Irreg. 4

Hundred 51.
G. I...(8)..(546)
25 5023
45 5003
57 5059
63 5011
69 5087
83 5039
87 5051
117 5099
G. II..(22).(1104)
11 5077. 5098
15 5047. 5062
16 5086
18 5007. 5041. 5042. 5063
21 5027. 5043. 5091
24 5095
25 5071
27 5067. 5078
30 5009
32 5079
39 5021
42 5006
45 5036(*3*)
58 5081
G. IV.(51).(2728)
6 5020. 5065. 5083
7 5038
8 5002. 5008. 5017. 5058. 5089
9 5013. 5014. 5035. 5050. 5055. 5068(*3*). 5097
10 5026. 5028. 5044. 5052. 5053. 5056. 5072. 5092
11 5093
12 5022. 5076
13 5029. 5090
14 5046. 5074
15 5019. 5030. 5094
16 5012. 5031(*2*)
18 5004. 5033. 5034. 5048. 5054. 5069(*3*). 5075(*3*)
19 5001. 5018
20 5057. 5084
22 5015
26 5024. 5045
30 5066
G. VIII(16).(784)
3 5032

4 5037
5 5061. 5080
6 5010. 5025. 5049. 5070. 5073.
5082. 5085. 5088. 5100
8 5064
9 5096
10 5060
G. XVI.(3).(128)
2 5005
3 5016. 5040

Total 424. . .5290
Irreg. 5

Hundred 61.
G. I. . .(7). .(353)
27 6007. 6043
45 6067(*3*). 6091(*3*)
57 6079
71 6047
81 6011(*3*)
G. II. .(22).(1440)
12 6073
15 6022
17 6037
18 6087
22 6082. 6092
24 6098
25 6031. 6053
27 6075(*3*)
28 6046
31 6038
33 6019
35 6029
39 6059
41 6023
42 6051
46 6002
48 6071
49 6044
58 6089
63 6074
G. IV.(53).(3012)
7 6013. 6028
8 6001(*2*). 6052(*2*)
9 6015. 6021(*3*). 6055. 6063. 6064. 6070. 6076. 6078. 6085(*3*)
10 6010. 6034. 6049. 6058. 6088.
11 6012
12 6003. 6004. 6008. 6025. 6027. 6057. 6066. 6077. 6084. 6099. 6100(*2*)
13 6033. 6094
14 6062
15 6017. 6039. 6050. 6081. 6093.
16 6016
18 6065. 6083(*3*)
19 6009
20 6036. 6054
21 6035. 6095
24 6014(*2*). 6068. 6086
25 6056
26 6005
28 6026
30 6041
G. VIII.(14).(768)
3 6097

4 6040. 6042
6 6018. 6024. 6030. 6048
8 6032. 6061. 6069. 6080
9 6060
10 6020. 6096
G. XVI.(4).(208)
3 6045. 6072. 6090
4 6006

Total 439. .5781
Irreg. 11 Impr. 933

Hundred 62.
G. I. . .(5). .(265)
33 6163
39 6199
41 6143
59 6151
93 6131
G. II. .(28).(1704)
11 6127
14 6103
15 6115. 6147
16 6178
18 6183. 6187. 6196
19 6172·
21 6133
22 6121
27 6122
29 6166
30 6139
33 6124. 6167
34 6113
35 6134. 6197
37 6173
40 6159
41 6119
42. 6155. 6158
45 6107
49 6191
53 6101
60 6179
G. IV.(44).(2568)
6 6157
7 6108. 6142. 6193
8 6112. 6148
9. 6130. 6154. 6175
10 6106. 6117. 6169. 6198
11 6182. 6190
12 6123(*2*). 6181
14 6145. 6174. 6185
15 6102. 6109. 6125. 6126. 6129. 6171
16 6144. 6189

17 6128. 6184
18 6111. 6135. 6156(*3*).
6164
19 6140
20 6114. 6137. 6161. 6176. 6186
22 6152. 6194
25 6170
28 6146
G. VIII(20).(1200)
4 6118
5 6136. 6153. 6162. 6168
6 6132. 6138. 6150. 6165. 6177.
6180. 6192. 6195
7 6141
9 6188
10 6110
12 6104. 6200
13 6116
15 6149
G. XVI(3)..(128)
2 6160
3 6105. 6120

Total 445...5865
Irreg. 2 Impr. 975

Hundred 63.
G. I. . .(7). .(447)
43 6247
45 6211
51 6203. 6271. 6287
77 6263
129 6299
G. II. .(28).(1678)
12 6238. 6295
15 6259. 6268
16 6217
18 6267(*3). 6283(*3*)
20 6223. 6241. 6274
23 6218. 6277
25 6207. 6250
27 6227(*3*)
29 6229
30 6212. 6219
33 6243
36 6242
38 6257
42 6275
45 6239. 6291(*3*)
51 6236. 6284
57 6269
63 6221(*3*)
G. IV.(39).(2428)
6 6220. 6262
7 6253
8 6202. 6208(*2*)
9 6235. 6252. 6297.
10 6246. 6292
11 6298
12 6255 6286(*2*)
13 6282
14 6228. 6245. 6260. 6276
15 6214. 6234. 6249
16 6231. 6233. 6244. 6272(*4*)
17 6294
18 6226(*3*). 6251
19 6281. 6289
20 6261
21 6266
22 6224
23 6278
24 6209. 6215
25 6206
27 6296
35 6254
G. VIII(23).(1176)
3 6232
4 6273
5 6205. 6213. 6258. 6280. 6285
6 6210. 6222. 6225. 6237. 6288.

6290. 6300
7 6248. 6256. 6265. 6279. 6293
8 6204
9 6264
10 6201
11 6230
G. XVI(3)..(176)
3 6216
4 6240. 6270

Total 451..5905
Irreg. 9

Hundred 91.
G. I...(6)..(386)
27 9067
35 9007
45 9043
63 9091
99 9011
117 9059
G. II..(26).(1960)
15 9013
18 9003(*3*). 9055
19 9034
21 9004. 9046
26 9079
27 9031. 9094
29 9098
30 9001. 9076
33 9068
36 9049. 9083
40 9023
42 9041
44 9047
45 9019(*3*)
46 9038
48 9092
54 9099(*3*)
57 9029
69 9014. 9071
80 9026
G. IV.(42).(2928)
8 9087. 9088
9 9022. 9037. 9073. 9097
10 9025. 9058
11 9052
12 9018. 9027. 9028
13 9082
14 9017. 9032. 9066
15 9033. 9051. 9063
17 9002. 9057. 9070
18 9012. 9015. 9069(*)..
9075(*3*)

19 9053. 9095
20 9039. 9054. 9062. 9081
21 9036
22 9084
27 9008. 9050. 9074
28 9089
30 9005. 9035. 9056. 9077

G. VIII(23).(1640)
5 9010
6 9040. 9042. 9045. 9072. 9085. 9100
7 9078. 9080. 9090. 9093
8 9016(*2*). 9024. 9060
9 9061. 9074
10 9020
11 9006
12 9021. 9065
14 9096
17 9086
18 9044

G. XVI(3)..(176)
3 9030. 9048
5 9009

Total 45..7090
Irreg. 6 Impr. 1122

Hundred 92.
G. I. . .(5). .(295)
51 9199
57 9103. 9127
63 9187
67 9151
G. II. .(30).(2208)
13 9157
14 9172
19 9133
20 9124. 9183
21 9115
23 9181
27 9109. 9123. 9167. 9175
28 9137
29 9148
30 9147
32 9111
34 9122. 9166
36 9143
39 9107. 9171
40 9188
47 9173
54 9134. 9155
56 9182
57 9179
60 9131
62 9119
63 9194
72 9161
G. IV.(36).(2652)
7 9178
8 9118(*2*). 9193
9 9132. 9139. 9162. 9163(*3*)
10 9190
12 9121. 9142. 9153. 9186
13 9117
15 9106. 9136. 9195. 9196
17 9158
18 9154
19 9146
20 9169
21 9126. 9197
22 9138. 9189
24 9113. 9159
25 9101. 9125
27 9164.
28 9116
30 9140
31 9191
32 9104(*2*)
33 9149
34 9110

G. VIII(26).(1752)
4 9108
5 9102. 9160
6 9112. 9130. 9145. 9150
7 9174
8 9135. 9144. 9156. 9168. 9184. 9192. 9198
9 9105. 9114. 9180. 9185. 9200
10 9128. 9152
11 9129. 9170
12 9141
19 9176
G. XVI(3)..(176)
3 9177
4 9120. 9165

Total 465...7083
Irreg. 3 Impr. 1207

Hundred 93.
G. I...(4)..(340)
33 9283
75 9227
93 9203
139 9239
G. II..(27).(2092)
13 9277
17 9223
18 9241. 9298
21 9235
25 9293
27 9211. 9247
29 9244
30 9271
31 9263
33 9267
35 9279
36 9259
37 9274
39 9242. 9286. 9287
40 9278
45 9251(*3*)
49 9221
54 9209
60 9257.
63 9206
66 9236
75 9299
80 9281
G. IV.(47).(3216)
7 9262
8 9202. 9208. 9232
10 9238. 9289
11 9237. 9258

12 9207. 9219. 9220(*2*).
9228. 9243(*2*). 9268.
9292. 9259. 9297
13 9249. 9255
14 9217. 9226. 9253
15 9212. 9250. 9276
16 9214(*2*). 9216.
9248(*2*). 9252
17 9254
18 9234
21 9201. 9229. 9261
22 9233. 9245
24 9275. 9291
25 9231. 9294
26 9218. 9290
27 9260(*3*)
29 9215
30 9284
32 9224
36 9266(*2*)
G. VIII(20).(1440)
6 9205. 9213. 9265. 9270. 9288.
9300
7 9256
8 9222. 9225. 9273. 9280(*2*).
9285
9 9272
10 9210
11 9230
12 9204. 9264
14 9269. 9296
15 9246
G. XVI.(1)..(48)
3 9282
G. XXXII(1).(64)
2 9240

Total 454...7200
Irreg. 9 Ingr. 1145

Hundred 94.
G. I. . .(6). . .(478)
41 9319
51 9343
55 9391
87 9323
97 9311
147 9371
G. II. .(27).(1894)
15 9307. 9388
18 9355
21 9397
23 9382
25 9375
26 9337
27 9349
28 9327
30 9346. 9358. 9363. 9364
32 9377
34 9326. 9332
36 9347. 9379. 9395
41 9302
46 9351
49 9335
51 9383
52 9359
56 9314
57 9356
69 9341
G. IV.(39).(2848)
7 9340. 9367
9 9342(*3*). 9370
11 9304. 9322
12 9378. 9387
13 9313. 9318
14 9353. 9394
15 9325. 9331. 9339
16 9301. 9316(*2*)
17 9303
18 9315(*3*). 9357. 9362. 9376. 9385(*3*). 9396. 9398
21 9334. 9368. 9392
22 9305. 9317.
23 9365
24 9308. 9399
27 9369. 9374.
30 9386
32 9344(*2)
33 9329. 9389
G. VIII(25).(1752)
4 9310. 9328. 9373
5 9333
6 9352

7 9321. 9361. 9381.
8 9312(*2*). 9348. 9372.
9393. 9394. 9400
9 9390
10 9330. 9338. 9366
11 9306. 9309. 9336
12 9324
14 9350. 9380
13 9320
G. XVI.(3)..(176)
3 9384
4 9345. 9360

Total 464...7148
Irreg. 6 Impr. 1210

Hundred 95.
G. I....(8)..(708)
33 9403
45 9463
75 9439
91 9431
101 9479
105 9419
123 9467
135 9491
G. II..(24).(1706)
16 9433
18 9475
19 9466. 9487
20 9442
21 9427
24 9406. 9409. 9423
30 9459
33 9421
34 9458
36 9451. 9497(*3*)
39 9484
40 9473
42 9428
45 9411. 9437
46 9407
51 9413
57 9461
63 9404
71 9446
G. IV.(41).(2988)
8 9412(*2*). 9457(*2*).
9472
9 9493
11 9402. 9447. 9496
12 9445. 9469. 9483. 9498
13 9415. 9418. 9448. 9454. 9468.
9478

14 9436
15 9443. 9452
17 9410
18 9444. 9477. 9482. 9495
20 9500
21 9414. 9481. 9489. 9499
22 9441
24 9422(*2*). 9426. 9474.
9488
28 9494
29 9449
30 9455
35 9470
36 9476
42 9434

G. VIII(25).(1744)
4 9430
5 9417
6 9408. 9432. 9438. 9465. 9492
7 9453. 9462
8 9424. 9460. 9485. 9486. 9490
9 9420. 9450(*3*). 9471
.10 9440
11 9429. 9456
12 9425. 9435. 9464
14 9416
16 9401

G. XVI.(2)..(112)
3 9480
4 9405

Total 452..7258
Irreg. 5

Hundred 96.
G. I. . . .(5). .(471)
39 9547
69 9511. 9587
129 9551
165 9539
G. II. .(28).(1964)
16 9508
17 9535
18 9523. 9583
20 9598
24 9502. 9507
25 9559
26 9543
27 9531(*3*). 9563.
9574(*3*)
29 9532
30 9571
33 9527
34 9556. 9586
38 9524. 9567
42 9518
43 9578
48 9566
49 9599
51 9575
59 9596
60 9572
61 9533
64 9521
G. IV.(38).(2700)
8 9538. 9562. 9577
10 9517. 9553. 9573
12 9505. 9522. 9526. 9550. 9580.
9595(*2*)
13 9514. 9549. 9557
14 9501. 9529. 9542
15 9582
16 9544
17 9564
18 9558
19 9565
20 9503(*2*). 9589. 9591.
9593
21 9515. 9561
24 9519. 9579
25 9530. 9584
27 9509
28 9536
30 9506
38 9569
40 9554
G. VIII(26).(1960)
4 9568

5 9592
6 9552. 9585. 9597
7 9528
8 9510(*2*). 9513(*2*).
9537. 9540(*2*). 9588.
9600(*2*).
9 9541. 9548. 9555(*3*)
10 9525. 9534. 9594
12 9504. 9516(*2*). 9560
13 9545. 9594
14 9581
15 9512. 9590
G. XVI.(3).(176)
3 9520. 9570
5 9576

Total 469. .7271
Irreg. 10

Hundred 97
G. I. . . .(5). .(333)
33 9643
57 9619
71 9679
77 9631
95 9623
G. II. .(29).(2108)
12 9667
19 9661
20 9697
21 9607. 9613
24 9601
26 9655
27 9627(*3*). 9663.
9683(*3*)
28 9604. 9634. 9649
30 9687. 9691
32 9662
33 9692
36 9668
42 9651
43 9647
44 9602
45 9626
49 9677
52 9689
55 9629
57 9659
63 9671
66 9611
69 9644
G. IV. .(41).(3108)
9 9612(*3*). 9615. 9622.
9678

10 9628
11 9670
12 9652. 9673(*2*). 9676.
9682. 9700
13 9637
14 9642. 9658. 9664
15 9639
16 9610
17 9606
18 9603. 9675(*3*).
9693(*3*).
19 9638. 9694
20 9608. 9616. 9650. 9653
21 9699
22 9654. 9684
23 9695
24 9641. 9666
25 9609
29 9617. 9674. 9698
30 9621
32 9665
33 9635
42 9686
G. VIII(22).(1600)
4 9640
5 9618. 9625. 9685. 9688
6 9648. 9696
7 9633. 9646
8 9645. 9669
9 9630. 9657
10 9620. 9636
11 9681
12 9605. 9632. 9680(*2*)
15 9624
16 9614
18 9656
G. XVI.(3)..(192)
3 9672
4 9690
5 9660

Total 451..7341
Irreg. 7

Hundred 98.
G. I. . .(6). .(524)
39 9739. 9787
89 9767
105 9743
119 9791
133 9719
G. II.(24).(1646)
17 9703
18 9748(*3*). 9783
19 9727
21 9733
22 9742
24 9763
25 9781
26 9769. 9778
27 9747(*3*). 9751
30 9755
33 9799
35 9754
37 9788
39 9707. 9771
43 9722
46 9721. 9759
48 9731
76 9764
81 9749
G. IV.(43).(3292)
7 9718
9 9772
10 9732. 9793
11 9738. 9753
12 9706. 9745. 9762
13 9712. 9713
14 9757. 9775. 9784
15 9766. 9777. 9795
16 9736. 9797
17 9711
18 9715. 9723. 9782
19 9773
20 9714. 9796
21 9708. 9710. 9770. 9774
22 9725. 9756
24 9728
26 9794
27 9704. 9726
28 9716. 9734
29 9761
30 9746
33 9740
36 9779
38 9701
G. VIII(24).(1752)
5 9717. 9730

6 9760. 9790
7 9724. 9752
8 9702(*2*). 9729. 9735.
9758. 9780. 9792(*2*)
9 9725. 9709. 9720(*3*)
10 9741. 9750. 9798
11 9737. 9786
12 9800
14 9789
15 9776. 9785
G. XVI(3)..(192)
4 9744. 9765. 9768

Total 466..7406
Irreg. 5

Hundred 99.
G. I...(8).(638)
49 9871
51 9883
63 9811(*3*). 9859
75 9887
91 9839
111 9803
135 9851
G. II..(22).(1700)
20 9892
21 9829. 9862. 9868
22 9847
24 9817. 9874
26 9838
28 9886. 9895
30 9857
34 9826
42 9827
45 9899(*3*)
48 9863
49 9818
51 9819
52 9833
57 9836
60 9875
70 9806
77 9866
G. IV.(43).(3164)
6 9823
7 9802
8 9865
9 9832. 9843. 9853. 9898
10 9808. 9837. 9850
11 9813
12 9872. 9835
13 9846
14 9820. 9878

15 9822. 9882
16 9807. 9814. 9848
17 9852. 9893. 9897
18 9801(*3*). 9844. 9873.
9891
19 9815. 9879
21 9855
22 9841
25 9830
26 9812. 9876
27 9831
28 9881(*2*)
31 9884
32 9809(*2*)
34 9824
37 9854
39 9896
41 9869

G. VIII(24).(1712)
5 9877
6 9804. 9810. 9828. 9867. 9888.
9900
7 9805. 9858. 9885
8 9816. 9856. 9860
9 9825(*3*). 9849(*3*).
9889
10 9821. 9834
11 9894
12 9861. 9864
13 9842
16 9845
17 9890

G. XVI(3). .(192)
3 9870
4 9880
5 9840

Total 464. .7406
Irreg. 7

Hundred 100.
G. I. . .(4). .(228)
39 9967
45 9907(*3*)
69 9931
75 9923
G. II.(28).(2302)
16 9991
18 9934(*3*)
23 9927. 9973
25 9949
27 9963(*3*)
28 9903. 9943
30 9938. 9979
31 9901
32 9986
34 9998
38 9908
39 9914. 9987
42 9939. 9947
46 9983
47 9935. 9946
50 9902
60 9995
63 9971
65 9959
67 9941
76 9929
85 9974
G. IV.(46).(3248)
7 9937
9 9925. 9958. 9997
10 9913. 9942. 9948. 10000
11 9970
12 9916. 9922. 9952. 9955(*2*).
9972(*2*)
13 9993
14 9988
15 9904. 9921. 9969. 9978
16 9961. 9985
17 9919. 9965
18 9910. 9915. 9964
19 9951. 9957. 9977
20 9992
21 9909
22 9953. 9956. 9962. 9999
23 9917. 9994
25 9981
26 9924
27 9989
28 9926. 9980
30 9932. 9950
34 9911

G. VIII(18).(1328)
4 9982
5 9976
6 9928. 9940. 9990
7 9906
8 9930. 9975. 9984
10 9918
11 9968
12 9905. 9920. 9936. 9954. 9996
13 9966
14 9944
G. XVI(4)..(240)
3 9933
4 9912. 9945. 9960

Total 452..7346
Irreg. 5

Hundred 117.
G. I...(1)..(147)
147 11699
G. II..(35).(2896)
16 11617
18 11698
19 11677
20 11614
22 11668
26 11647
27 11643. 11683(*3*)
29 11663
30 11602. .11623. 11659
35 11686
36 12603. 11631. 11633. 11667.
11671. 11689. 11691. 11695
37 11642
42 11657
43 11626
45 11611
51 11621
54 11619
56 11678
59 11612
63 11675
67 11639
70 11636
73 11654
81 11651(*3*)
90 11681
G. IV..(35).(2672)
8 11650
9 11608. 11692
11 11638. 11653
12 11635. 11641. 11673
13 11632. 11674

14 11652. 11662
15 11607. 11694
16 11629. 11665
17 11672
18 11601. 11627. 11637. 11664
19 11687
21 11644
23 11618
24 11615
25 11693
26 11604. 11669. 11679
28 11646
29 11630
32 11666. 11684
33 11624
35 11606

G. VIII(27).(2248)
6 11610. 11620. 11628. 11656. 11680. 11697
8 11605. 11622. 11658. 11670. 11682
9 11613. 11655
10 11616. 11625. 11676
11 11688
12 11648. 11661. 11700(*2*)
13 11634. 11645. 11649
14 11690
18 11660. 11696
21 11609

G. XVI.(2).(128)
3 11685
5 11640

Total 459. . .8091
Irreg. 3 Impr. prim. 1339

Hundred 118.
G. I. . . .(5). .(319)
39 11743
41 11719
63 11731
81 11779(*3*)
95 11783
G. II. .(28).(2560)
18 11707
21 11767
22 11727. 11758
25 11734
29 11722
30 11755
31 11701. 11708
33 11702. 11763
36 11762
39 11747. 11787
40 11791
49 11789
50 11794
53 11751
54 11723
60 11711. 11771. 11777
61 11735. 11738
65 11759
73 11717
87 11756
98 .11714
G. IV.(40).(3100)
8 11797
9 11782
10 11785
11 11740. 11757
12 11733. 11737. 11788
14 11728. 11746. 11764
15 11710. 11773. 11793
16 11705. 11775. 11776. 11796
17 11761
18 11754. 11772
19 11706
20 11716. 11768
21 11724. 11799
22 11703. 11732. 11749
25 11709. 11769. 11780
27 11795(*3*). 11798.
28 11786
29 11721. 11741.
30 11774
34 11729
40 11744
G. VIII(23).(1744)
4 11713(*3*)
6 11715. 11718. 11748. 11752

7 11720. 11742. 11778
8 11712. 11725(*2*). 11753.
11770. 11784. 11790
9 11800
10 11792
11 11736
12 11739. 11745
15 11766
16 11780
18 11726. 11765
G. XVI.(4)..(320)
4 11760
5 11704. 11730
6 11781

Total 469...8043
Irreg. 4 Impr. prim. 1369

Hundred 119.
G. I....(7)..(505)
31 11863
39 11827
47 11887
61 11839
75 11867
113 11807
139 11831
G. II...(23).(1990)
21 11878
24 11806. 11812. 11854
27 11851(*3*). 11881
30 11875
33 11884
39 11852
40 11833. 11897
43 11821
45 11871. 11899(*3*)
49 11813. 11846
52 11876
54 11828. 11843(*.3*)
58 11855
70 11801
72 11819
75 11879
G. IV.(44).(3608)
8 11848
9 11803. 11818. 11893
10 11860. 11862
11 11815
12 11823
13 11838
14 11842. 11892
15 11824. 11853. 11883
16 11857

18 11809. 11811. 11835(*3*).
11873. 11874
19 11841
20 11822(*2*). 11836. 11847.
11858. 11866
21 11859. 11888. 11898
23 11829
24 11826. 11889. 11896
26 11834. 11894
27 11804. 11810. 11861
29 11882
35 11870
36 11849
37 11885
42 11891
43 11864

G. VIII(22).(1688)
4 11872
6 11817. 11845. 11869. 11895
7 11830. 11890
8 11805. 11808(*2*). 11877
9 11802. 11820. 11825
10 11850. 11900
11 11837. 11868
12 11844. 11886
16 11814. 11840
20 11816

G. XVI.(4)..(304)
2 11880
4 11832
6 11856. 11865

Total 469...8095
Irreg. 6 Impr. 1337

Hundred 120.
G. I. . .(7). .(547)
39 11923
45 11971(*3*)
81 11903. 11939(*3*)
83 11927
95 11959
123 11987
G. II. .(22).(1912)
20 11953
21 11962
24 11995
27 11907(*9*). 11911. 11967
30 11943. 11947
31 11983
33 11974. 11979
41 11941
48 11963
49 11933. 11999
50 11975
57 11915
66 11906
69 11909
71 11981
73 11996
80 11969
G. IV.(45).(3564)
9 11992
10 11922. 11932. 11938. 11958
11 11902. 11965
12 11905. 11908. 11917. 11929. 11950. 11980. 11988(*2*). 11998
13 11986
15 11944. 11955
17 11982
18 11916. 11956. 11991
19 11918. 11993. 11994
20 11978
21 11901. 11957
23 11989
24 11926. 11964. 11972(*2*)
26 11936. 11945
27 11919. 11930. 11942. 11961(*3*)
29 11951
30 11912. 11948
32 11966(*2*)
33 11931
40 11924
42 11954

G. VIII(22).(1832)
6 11914. 11937. 11968. 11977
7 11973
8 11920(*2*). 11940. 11946
9 11913. 11925. 11935. 11949. 11952
10 11997. 12000
12 11904. 11910
15 11934
16 11976. 11984
17 11990
21 11921
G. XVI.(4)..(288)
3 11928
4 11985
5 11960
6 11970

Total 471...8143
Irreg. 8 Impr. prim. 1361

Thousand I.
G. I...(93)..(1277)

1	1. 2. 3. 4. 7 ..	5
3	11. 19. 23. 27. 31. 43. 67. 163 ..	8
5	47. 79. 103. 127 ..	4
7	71. 151. 223. 343. 463. 487 ..	6
9.	59. 83. 107. 139. 199. 211. 243(*3*). 283. 307(*3*). 331. 367. 379. 499. 547. 643. 823. 883. 907	18
11	167. 271. 967	3
13	191. 263. 607. 631. 727	5
15	131. 179. 227. 239. 347. 439. 443. 523. 571. 619. 683. 691. 739. 751. 787. 947 ..	16
17	383. 991 ..	2
19	311. 359. 919	3
21	251. 431. 467. 503. 587. 743. 811. 827. 859. 863 ..	10
25	479. 599. 647	3
27	419. 491. 563. 983 ..	4
29	887	1
31	719. 911 ..	2
33	659. 839 ..	2
45	971	1

Irreg. 2 pr. 2130

G. II.....(402).....(6068)
1 5. 6. 8. 9. 10. 12. 13. 15. 16. 18. 22. 25. 28. 37. 58 .. 15

2	14. 17. 20. 32. 34. 36. 39. 46. 49. 52. 55. 63. 64. 73. 82. 97. 100. 142. 148. 193 . .	20
3	26. 29. 35. 38. 44. 50. 51. 53. 54. 61. 75. 76. 81. 87. 91. 92. 99. 106. 108. 109. 115. 118. 121. 123. 124. 135. 147. 157. 162. 169. 172. 175. 187. 202. 207. 214. 235. 247. 262. 267. 268. 277. 298. 358. 397. 403. 427. 541. 652	49
4	41. 62. 68. 94. 95. 98. 111. 113. 128. 137. 158. 178. 183. 196. 226. 256. 289. 292. 295. 313. 337. 382. 388. 415. 457. 466. 478. 562. 577. 583. 772. 862	32
5	74. 86. 119. 122. 125. 143. 159. 166. 181. 188. 197. 218. 229. 242. 250. 303. 316. 317. 319. 346. 361. 373. 375. 394. 412. 421. 422. 423. 508. 538. 613. 625. 694. 709. 757. 847. 853. 877. 982	39
6	89. 116. 155. 171. 203. 212. 219. 233. 241. 244. 259. 274. 275. 279. 291. 302. 323. 324. 327. 334. 351. 355. 363. 387. 433. 436. 475. 484. 507. 526. 529. 543. 567. 603. 617. 622. 628. 655. 667. 673. 676. 687. 718. 723. 763. 775. 802. 898. 955	49
7	101. 134. 149. 173. 215. 278. 284. 287. 338. 349. 391. 447. 454. 502. 511. 535. 604. 634. 639. 653. 703. 733. 778. 807. 838. 841. 892. 997	28
8	146. 164. 254. 257. 353. 407. 409. 452. 471. 512. 514. 527. 548. 559. 578. 722. 799. 895. 943. 958. 961	22
9	194. 236. 293. 332. 335. 339(*3*). 362. 411. 428. 451. 459. 486. 515. 519. 531. 556. 557. 575. 586. 661. 675(*3*). 679. 707. 729. 747. 771. 783. 796. 835. 843. 844. 867. 886. 891(*3*). 922. 931. 963. 972	37
10	206. 281. 386. 398. 401. 449. 482. 500. 601. 711. 724. 769. 788. 878. 916. 927. 937. 977	18
11	269. 326. 389. 551. 554. 591. 623. 662. 668. 758. 767. 829. 842. 871. 879 .	15
12	299. 356. 371. 395. 539. 542. 579. 593. 674. 695. 706. 766. 932. 939. 964. 979. 995. 999	18
13	314. 458. 698. 746. 764. 773. 934. 951. 998	9
14	404. 596. 641. 686. 692. 818. 831	7
15	461. 509. 524. 566. 611. 635. 671. 677. 699. 716. 779. 797. 803. 815. 821. 851. 875. 908. 923. 956 .	20
16	446. 521. 569. 791. 809. 857. 953	7
17	614. 701	2
18	626. 731. 755(*3*). 914. 929. 959. 974(*3*) . . .	7
20	734. 761. 881. 926 . . .	4
21	794. 899	2
22	866	1
23	941	1

Irreg. 5 all *3* pr. 7394

G. IV. . .(417). . . . .(6620)

1	21. 24. 30. 33. 40. 42. 45. 48. 57. 60. 70. 72. 78. 85. 88. 93. 102. 112. 130. 133. 177. 190. 232. 253 . . .	24
2	56. 65. 66. 69. 77. 80. 84. 90. 96. 114. 117. 126. 132. 136. 138. 141. 144. 145. 150. 153. 154. 156. 160. 180. 184. 192. 198. 205. 208. 213. 217. 220. 225. 228. 238. 252. 258. 265. 282. 288. 301. 310. 322. 328. 333. 340. 352. 372. 400. 418. 438. 442. 445. 448. 498. 505. 522. 553. 568. 592. 598. 658. 697. 708. 742. 793. 928 :	67
3	104. 110. 129. 140. 152. 170. 174. 176. 182. 186. 189. 195. 200. 201. 204. 216. 222. 231. 234. 237. 245. 246. 249. 255. 261. 270. 286. 294. 297. 300. 304. 309. 315. 318. 325. 342. 348. 364. 366. 368. 370. 378. 393. 396. 405. 417. 424. 430. 432. 435. 450. 453. 460. 472. 473. 477. 483. 490. 492. 493. 496. 513. 517. 533. 537. 540. 550. 555. 565. 588. 595. 597. 606. 610. 618. 627. 637. 648. 669. 670. 682. 685. 688. 700. 702. 715. 730. 748. 753. 762. 784. 795. 808. 813. 814. 817. 826. 827. 837. 856. 913. 918. 925. 933. 940. 942. 949. 970. 973. 988 .	110
4	161. 185. 221. 224. 248·. 260. 272. 276. 305. 306. 308. 320. 350. 354. 369. 376. 377. 380. 384. 392. 399. 402. 406. 410. 414. 441. 444. 468. 469. 481. 485. 495. 501. 518. 532. 544. 558. 564. 573. 574. 576(*2*). 580(*2*). 582. 589. 612. 632 640. 642. 646. 657. 663. 712. 717. 721. 732. 735. 736. 738. 745. 768. 785. 786. 790. 820(*2*). 832. 834. 850. 852. 855. 865. 868. 873. 882. 889. 900(*2*). 903. 904. 933. 938. 946. 975. 994	82
5	209. 230. 266. 290. 296. 321. 344. 365. 381. 413. 425. 437. 455. 470. 474. 476. 488. 489. 534. 572. 590. 608. 615. 629. 633. 636. 638. 649. 664. 666. 678. 681. 726. 737. 750. 752. 754. 774. 781. 822. 830. 872. 874. 917. 921. 968. 1000	47
6	329. 416. 426. 434. 464. 497. 516. 549. 594. 602. 605. 620. 621. 650. 651. 684. 704. 713. 725. 756. 759. 782. 800. 801. 804. 810. 812. 819. 833. 848. 864. 876. 890. 894. 901. 905. 915. 948. 954. 976. 978. 980. 981. 985. 987. 996	46
7	341. 374. 494. 506. 530. 536. 581. 654. 806. 845. 849. 860. 893. 902. 906. 909. 935. 962	18
8	545. 584. 644. 656. 710. 740. 749. 789. 846. 869. 884(*2*). 896. 992 . . .	13
9	944. 950. 989	3
10	689. 776. 824. 836	4
11	854. 965. 986	3

pr. 6904

G. VIII. . .(87). . . . .(1496)

1	105. 120. 165. 168. 210. 240. 273. 280. 312. 330. 345. 357. 385. 408. 462. 520. 760	17

2	264. 285. 336. 360. 390. 420. 429. 456. 465. 480. 504. 510. 525. 528. 552. 561. 570. 585. 600. 609. 616. 624. 630. 645. 660. 672. 690. 693. 720. 765. 777. 792. 798. 805. 858. 870. 880. 897. 910. 912. 952. 957. 960	43
3	440. 546. 560. 665. 680. 696. 705. 714. 728. 741. 744. 780. 816. 825. 861. 885. 888. 924. 930. 936. 945. 966. 969. 984. 990 .	25
4	770	1
5	920	1

G. XVI.....(1).....(16)

1	840	1

Total number of all

$$\begin{aligned} \text{genera} &= 3277 \\ \text{classes } p.p.p &= 15467 \\ \sqrt{1} + \sqrt{2} + \ldots + \sqrt{1000} &= 21097{,}661 \\ \text{Quotient} &= 0{,}733 \end{aligned}$$

Irreg. 11, 5(*2*), 6(*3*)

Thousand III.

G. I.....(64).....(2470)

13	2143	1
15	2203. 2347. 2647. 2683 ..	4
21	2011. 2083. 2179. 2251. 2467. 2503. 2707. 2767 ..	8
23	2671	1
25	2887	1
27	2003. 2187*. 2803	3
29	2287. 2311. 2383	3
31	2927	1
33	2027. 2267. 2423. 2539. 2731. 2851. 2971	7
35	2087. 2239. 2543	3
37	2447	1
39	2131. 2207. 2371. 2659. 2791. 2963	6
41	2551. 2719	2
43	2663	1
45	2039. 2063. 2243*. 2699*. 2843	5
49	2111	1
51	2531. 2687	2
53	2711	1
57	2099. 2339. 2459. 2591. 2879	5
59	2399. 2903	2
63	2351. 2579. 2819	3

69	2411	1
73	2999	1
87	2939	1

Irreg. 3

G. II. . . .(311). . . . .(11646)

6	2017. 2062	2
7	2293. 2335	2
8	2095. 2113. 2137. 2302. 2308. 2377. 2578. 2878. 2962	9
9	2023. 2038. 2047. 2053. 2122. 2167. 2188. 2221. 2227. 2283. 2403(*3*). 2437(*3*). 2443. 2458. 2515. 2557. 2563(*3*). 2566. 2572. 2787. 2797. 2902. 2923. 2998, ...	24
10	2164. 2281. 2407. 2452. 2473. 2487. 2500. 2527. 2638. 2722. 2743. 2818. 2836. 2857. 2983	15
11	2182. 2215. 2263. 2326. 2374. 2623. 2662. 2677. 2815. 2863. 2917. 2935 . .	12
12	2059. 2098. 2107. 2116. 2209. 2307. 2323. 2395. 2419. 2468. 2479. 2587. 2593. 2611. 2689. 2692. 2713. 2827. 2947. 2953. 2995	21
13	2102. 2197. 2218. 2362. 2367. 2428. 2524. 2762. 2809. 2823. 2839. 2854. 2908	13
14	2007. 2018. 2127. 2258. 2359. 2401. 2446. 2455. 2612. 2734. 2753. 2932 . .	12
15	2043. 2071. 2092. 2151. 2191. 2237. 2269. 2284. 2299. 2303. 2319. 2341. 2363. 2476. 2523. 2575. 2578. 2599. 2602. 2643. 2727. 2732. 2764. 2875. 2883. 2899. 2956. 2986 . .	28
16	2048. 2153. 2194. 2206. 2386. 2434. 2462. 2521. 2617. 2633. 2657. 2833 . .	12
17	2026. 2029. 2103. 2119. 2234. 2333. 2389. 2391. 2463. 2918	10
18	2155. 2161. 2199. 2228. 2417. 2491. 2511. 2547. 2619(*3*). 2627. 2644. 2723. 2763(*3*). 2783. 2867. 2897. 2916. 2943. 2979	19
19	2031. 2069. 2381. 2477. 2554. 2738. 2746. 2799. 2858	9
20	2078. 2297. 2375. 2402. 2404. 2498. 2559. 2777. 2866. 2942. 2959	11
21	2012. 2123. 2138. 2147. 2171. 2183. 2186. 2213. 2259. 2342. 2348. 2357. 2427. 2507. 2571. 2693. 2749. 2779. 2911. 2931. 2972	21
22	2089. 2271. 2439. 2567. 2594. 2798	6
23	2614. 2615. 2837	3
24	2019. 2195. 2273. 2327. 2372. 2631. 2654. 2811. 2974. 2991	10
25	2042. 2396. 2582. 2588 . .	4
26	2642. 2807. 2969	3

27	2051. 2075(*3*). 2252. 2291. 2315(*3*). 2426. 2675(*3*). 2747. 2759. 2859. 2891(*3*). 2951. 2957	13
28	2066. 2129. 2279. 2495. 2564	5
29	2231. 2741	2
30	2036. 2081. 2126. 2159. 2393. 2483. 2603. 2606. 2708. 2801. 2855. 2978. 2987	13
31	2471. 2621. 2735. 2876 ..	4
32	2084. 2174. 2276. 2306. 2519. 2558	6
33	2309. 2435. 2636. 2861. 2906	5
34	2804. 2831. 2894	3
35	2549. 2909	2
36	2219(*3*). 2846	2
38	2441	1
39	2141. 2246. 2474. 2651. 2771	5
40	2729	1
41	2789	1
42	2609	1
43	2966	1

Irreg. 10

G. IV...(430).....(16232)

3	2608	1
4	2020. 2077. 2212. 2242. 2248. 2272. 2332. 2353. 2368. 2410. 2533. 2542(*2*) 2605. 2773. 2788. 2842. 2893	17
5	2032. 2073. 2074. 2101. 2118. 2125. 2152. 2158. 2173. 2178. 2202. 2230. 2247. 2290. 2398. 2422. 2433, 2494. 2577. 2641. 2776. 2830. 2853. 2965 ..	24
6	2022. 2025. 2028. 2035. 2050. 2052. 2067. 2068. 2082. 2086. 2096. 2104. 2115. 2132. 2139. 2148. 2157. 2163. 2172. 2223. 2257. 2260. 2268. 2275. 2278. 2305. 2317. 2322. 2338. 2358. 2388. 2412. 2413. 2425. 2451. 2475. 2482. 2488. 2493. 2512. 2517. 2538. 2545. 2548. 2592. 2598. 2620. 2629. 2650. 2653. 2658. 2667. 2668. 2676. 2682. 2695. 2698. 2704. 2710. 2715. 2718. 2725. 2740. 2748. 2752. 2755. 2758. 2794.	
	2802. 2872. 2892. 2907. 2914. 2938. 2977. 2997 ..	76
7	2008. 2033. 2044. 2055. 2058. 2094. 2110. 2140. 2146. 2149. 2165. 2217. 2238. 2270. 2314. 2382. 2416. 2431. 2438. 2497. 2502. 2509. 2535. 2536. 2556. 2583. 2607. 2703. 2761. 2766. 2782. 2812. 2881. 2913. 2930.. 2941. 2973	37
8	2004. 2005. 2034. 2041. 2056. 2134. 2176(*2*). 2192. 2236. 2245. 2254(*2*). 2286. 2292. 2298. 2304. 2312. 2313. 2329(*2*). 2343. 2350. 2356. 2454. 2506. 2513. 2528. 2560. 2569. 2589. 2601. 2628(*2*). 2655. 2674. 2686. 2733. 2742. 2775. 2785. 2817. 2845. 2847. 2848(*2*) 2868. 2884. 2944. 2946. 2949. 2980(*2*)	47

9	2014. 2049. 2060. 2076. 2079. 2091. 2106. 2108. 2117. 2124. 2133(*3*). 2175. 2181. 2198. 2214. 2221. 2235(*3*). 2241. 2253. 2266. 2295. 2300. 2318. 2344. 2349. 2355. 2361. 2387. 2430(*3*). 2461. 2522 2555. 2581. 2595. 2626. 2634. 2635. 2637. 2646(*3*). 2673. 2700(*3*). 2716. 2770. 2778. 2781. 2795. 2806. 2828. 2835(*3*). 2862. 2887. 2888. 2890. 2895. 2950. 2955. 2988. 2989 . .	58
10	2057. 2061. 2150. 2154. 2166. 2177. 2249. 2250. 2255. 2282. 2449. 2514. 2529. 2532. 2596. 2656. 2678. 2724. 2751. 2810. 2844. 2869. 2871. 2874. 2896. 2919. 2929. 2948. 2975	29
11	2135. 2204. 2216. 2334. 2364. 2421. 2489. 2492. 2570. 2573. 2645. 2648. 2649. 2672. 2757. 2841. 2922. 2933. 3934. 2967 . .	20
12	2006. 2009. 2045. 2105. 2156. 2168. 2169. 2196. 2211. 2225. 2229. 2316. 2331. 2366. 2379(*2*). 2390. 2420(*2*). 2432. 2450. 2466. 2484. 2499. 2597. 2661. 2691. 2696. 2701. 2702(*2*). 2739. 2754. 2780· 2816. 2822. 2824. 2825. 2852. 2873. 2900. 2993(*2*)	39
13	2015. 2222. 2453. 2469. 2481. 2510. 2679. 2721. 2792. 2826. 2901. 2984 . .	12
14	2114. 2144. 2162. 2274. 2324. 2354. 2384. 2429. 2486. 2501. 2525. 2587. 2744. 2768. 2774	15
15	2096. 2189. 2264. 2285. 2321. 2330. 2378. 2406. 2444. 2526. 2534. 2537. 2540. 2630. 2684. 2690. 2694. 2750. 2796. 2813. 2864. 2889	22
16	2180. 2201. 2336. 2546. 2561. 2624(*2*). 2639. 2669. 2882. 2921. 2994. 2996	12
17	2021. 2456. 2666. 2726 . .	4
18	2054. 2369. 2414. 2504. 2516. 2681. 2705. 2786. 2915. 2924	10
19	2294	1
20	2714. 2756(*2*). 2936. 2954. 2981	5
21	2834	1

Irreg. 13 (2). 6 (3). Sa..19

G. VIII. . .(184). . . .(6344)

2	2002. 2013. 2080. 2088. 2128. 2170. 2233. 2277. 2392. 2632. 2737. 2832. 2068	13
3	2037. 2065. 2160. 2185. 2190. 2193. 2200. 2205. 2220. 2262. 2325. 2346. 2352. 2370. 2373. 2380. 2418. 2424. 2440. 2457. 2472. 2485. 2508. 2530. 2550. 2553. 2562. 2590. 2613. 2622. 2680. 2685. 2697. 2728. 2800. 2808. 2860. 2905. 2920. 2937. 2970. 2982. 2992	43
4	2010. 2016. 2046. 2072. 2100. 2112(*2*). 2130. 2142. 2208. 2232. 2244. 2256. 2265. 2289. 2296. 2320. 2328. 2337. 2340. 2365. 2385(*2*). 2397. 2400(*2*). 2436. 2442. 2445. 2448(*2*). 2464. 2465. 2470. 2478. 2490. 2496. 2568. 2580. 2584. 2652. 2665. 2688. 2706. 2709. 2717. 2745. 2772. 2790. 2793. 2821. 2829. 2850(*2*). 2865. 2880. 2898. 2928. 2940. 2952. 2958. 2985	57

5	2030. 2070. 2085. 2093. 2109. 2121. 2136. 2226. 2288. 2360. 2394. 2405. 2409. 2415. 2460. 2505. 2541. 2544. 2552. 2585. 2610. 2618. 2625. 2664. 2670. 2712. 2769. 2814. 2838. 2877. 2886. 2904. 2910. 2926. 2990: 3000 . .	36
6	2001. 2064. 2090. 2240. 2301. 2376. 2408. 2480. 2564. 2574. 2600. 2604. 2660. 2720. 2736. 2784. 2820. 2912. 2925. 2961. 2964. 2976	22
7	2024. 2120. 2210. 2345. 2616. 2765. 2870	7
8	2576. 2840. 2849. 2945. 2960	5
9	2261	1

Irreg. 5 (2)

G. XVI. . . .(11). . . . .(400)

2	2040. 2145. 2280. 2310. 2520. 2640. 2730. 2760 . .	8
3	2184. 2805. 2856	3

Total of all

genera *p.p.p*	= 4054	expected	4051,3
classes *p.p.p*	= 37092	. .	37074,3
. . impr. *p.p*	= 6182		

Irreg. 18(*2*). 19(*3*). Sa= 37

Thousand X.

Genera I.

27	9067
33	9283. 9403. 9643
35	9007
39	9547. 9739. 9787. 9967
41	9319
45	9043. 9463. 9907(*3*)
49	9871
51	9199. 9343. 9883
55	9391
57	9103. 9127. 9619'
63	9091. 9187. 9811(*3*). 9859
67	9151
69	9511. 9587. 9931
71	9679
75	9227. 9439. 9887. 9923
77	9631
87	9323
89	9767
91	9431. 9839

93 9203
95 9623
97 9311
99 9011
101 9479
105 9419. 9743
111 9059. 9803
119 9791
123 9467
129 9551
133 9719
135 9491. 9851
139 9239
147 9371
165 9539

.57. . .4401.

Genera II.

12 9667 1
13 9157. 9277 2
14 9172 1
15 9013. 9307. 9388 3
16 9433. 9508. 9991 3
17 9223. 9535. 9703 3
18 9003(*3*). 9055. 9241. 9298. 9355. 9475. 9523. 9583. 9748(*3*). 9783. 9934(*3*) 11
19 9034. 9133. 9466. 9487. 9661. 9727 6
20 9124. 9183. 9442. 9598. 9697. 9892 6
21 9004. 9046. 9115. 9235. 9397. 9427. 9607. 9613. 9733. 9829. 9862. 9868 . . 12
22 9742. 9847 2
23 9181. 9382. 9927. 9973 . . 4
24 9406. 9409. 9423. 9502. 9507. 9601. 9763. 9817. 9874 9
25 9293. 9375. 9559. 9781. 9949 5
26 9079. 9337. 9543. 9655. 9769. 9778. 9838 7
27 9031. 9094. 9109. 9123. 9167. 9175. 9211. 9247. 9349. 9531(*3*). 9563. 9574(*3*). 9627(*3*). 9663. 9683(*3*). 9747(*3*). 9751. 9963(*3*) 18
28 9137. 9327. 9604. 9634. 9649. 9886. 9895. 9903. 9943 9
29 9098. 9148. 9244. 9532 . . 4
30 9001. 9076. 9147. 9271. 9346. 9358. 9363. 9364. 9459. 9571. 9687. 9691. 9755. 9857. 9938. 9979 . . 16
31 9263. 9901 2
32 9111. 9377. 9662. 9986 . . 4
33 9068. 9267. 9421. 9527. 9692. 9799 6
34 9122. 9166. 9326. 9332. 9458. 9556. 9586. 9826. 9998 9

35	9279. 9754	2
36	9049. 9083. 9143. 9259. 9347. 9379. 9395. 9451. 9497(*3*). 9668	10
37	9274. 9788	2
38	9524. 9567. 9908	3
39	9107. 9171. 9242. 9286. 9287. 9484. 9707. 9771. 9914. 9987	10
40	9023. 9188. 9278. 9473 ..	4
41	9302	1
42	9041. 9428. 9518. 9651. 9827. 9939. 9947	7
43	9578. 9647. 9722	3
44	9047. 9602	2
45	9019(*3*). 9251(*3*). 9411. 9437. 9626. 9899(*3*).	6
46	9038. 9351. 9407. 9721. 9759. 9983	6
47	9173. 9935. 9946	3
48	9092. 9566. 9731. 9863 ..	4
49	9221. 9335. 9599. 9677. 9818	5
50	9902	1
51	9383. 9413. 9575. 9819 ..	4
52	9359. 9689. 9833	3
54	9099(*3*). 9134. 9155. 9209	4
55	9629	1
56	9182. 9314	2
57	9029. 9179. 9356. 9461. 9659. 9836	6
59	9596	1
60	9131. 9257. 9572. 9875. 9995	5
61	9533	1
62	9119	1
63	9194. 9206. 9404. 9671. 9971	5
64	9521	1
65	9959	1
66	9236. 9611	2
67	9941	1
69	9014. 9071. 9341. 9644 ..	4
70	9806	1
71	9446	1
72	9161	1
75	9299	1
76	9764. 9929	2
77	9866	1
80	9026. 9281	2
81	9749	1
85	9974	1

Total 265. .19580
Irreg. 14.

Genera IV.

6	9823	1
7	9178. 9262. 9340. 9367. 9718. 9802. 9937	7
8	9087. 9088. 9118(*2*). 9193. 9202. 9208. 9232. 9412(*2*). 9457(*2*). 9472. 9538. 9562. 9577. 9865	14
9	9022. 9037. 9073. 9097. 9132. 9139. 9162. 9163(*3*). 9342(*3*). 9370. 9493. 9612(*3*). 9615. 9622. 9678. 9772. 9832. 9843. 9853. 9898. 9925. 9958. 9997	23
10	9025. 9058. 9190. 9238. 9289. 9517. 9553. 9573. 9628. 9732. 9793. 9808. 9837. 9850. 9913. 9942. 9948. 10000	18
11	9052. 9237. 9258. 9304. 9322. 9402. 9447. 9496. 9670. 9738. 9753. 9813. 9970	13
12	9018. 9027. 9028. 9121. 9142. 9153. 9186. 9207. 9219. 9220(*2*). 9228. 9243(*2*). 9268. 9292. 9295. 9297. 9378. 9387. 9445. 9469. 9483. 9498. 9505. 9522. 9526. 9550. 9580. 9595(*2*). 9652. 9673(*2*). 9676. 9682. 9700. 9706. 9745. 9762. 9835. 9872. 9916. 9922. 9952. 9955(*2*). 9972(*2*)	43
13	9082. 9117. 9249. 9255. 9313. 9318. 9415. 9418. 9448. 9454. 9468. 9478. 9514. 9549. 9557. 9637. 9712. 9713. 9846. 9993 . .	20
14	9017. 9032. 9066. 9217. 9226. 9253. 9353. 9354. 9436. 9501. 9529. 9542. 9642. 9658. 9664. 9757. 9775. 9784. 9820. 9878. 9988	21
15	9033. 9051. 9063. 9106. 9136. 9195. 9196. 9212. 9250. 9276. 9325. 9331. 9339. 9443. 9452. 9582. 9639. 9766. 9777. 9795. 9822. 9882. 9904. 9921. 9969. 9978	26
16	9214(*2*). 9216(*2*). 9248(*2*). 9252. 9301. 9316(*2*). 9544. 9610. 9736. 9797. 9807. 9814. 9848. 9961. 9985	15
17	9002. 9057. 9070. 9158. 9254. 9303. 9410. 9564. 9606. 9711. 9852. 9893. 9897. 9919. 9965	15
18	9012. 9015. 9069(*3*). 9075(*3*). 9154. 9234. 9315(*3*). 9357. 9362. 9376. 9385(*3*). 9396. 9398. 9444. 9477. 9482. 9495. 9558. 9603. 9675(*3*). 9693(*3*). 9715. 9723. 9782. 9801(*3*). 9844. 9873. 9891. 9910. 9915. 9964	31
19	9053. 9095. 9146. 9565. 9638. 9694. 9773. 9815. 9879. 9951. 9957. 9977 . .	12
20	9039. 9054. 9062. 9081. 9169. 9500. 9503(*2*). 9589. 9591. 9593. 9608. 9616. 9650. 9653. 9714. 9796. 9992	17
21	9036. 9126. 9197. 9201. 9229. 9261. 9334. 9368. 9392. 9414. 9481. 9489. 9499. 9515. 9561. 9699. 9708. 9710. 9770. 9774. 9855. 9909	22
22	9084. 9138. 9189. 9233. 9245. 9305. 9317. 9441. 9654. 9684. 9725. 9756. 9841. 9953. 9956. 9962. 9999	17
23	9365. 9695. 9917. 9994 . .	4
24	9113. 9159. 9275. 9291. 9308. 9399. 9422(*2*). 9426. 9474. 9488. 9519. 9579. 9641. 9666. 9728 . .	15

25	9101. 9125. 9231. 9294. 9530. 9584. 9609. 9830. 9981	9
26	9218. 9290. 9794. 9812. 9876. 9924	6
27	9038. 9050. 9074. 9164. 9260(*3*). 9369. 9374. 9509. 9704. 9726. 9831. 9989	12
28	9089. 9116. 9494. 9536. 9716. 9734. 9881(*2*). 9926. 9980	9
29	9215. 9449. 9617. 9674. 9698. 9761	6
30	9005. 9035. 9056. 9077. 9140. 9284. 9386. 9455. 9506. 9621. 9746. 9932. 9950	13
31	9191. 9884	2
32	9104(*2*). 9224. 9344(*2*). 9665. 9809(*2*)	5
33	9149. 9329. 9389. 9635. 9740	5
34	9110. 9824. 9911	3
35	9470	1
36	9266(*2*). 9476. 9779 ..	3
37	9854	1
38	9569. 9701	2
39	9896	1
40	9554	1
41	9869	1
42	9434. 9686	2

Total 416...30144
Irreg. 20(*2*). 11(*3*)

Genera VIII.

4	9108. 9310. 9328. 9373. 9430. 9568. 9640. 9982.	
5	9010. 9102. 9160. 9333. 9417. 9592. 9618. 9625. 9685. 9688. 9717. 9730. 9877. 9976	14
6	9040. 9042. 9045. 9072. 9085. 9100. 9112. 9130. 9145. 9150. 9206. 9213. 9265. 9270. 9288. 9300. 9352. 9408. 9432. 9438. 9465. 9492. 9552. 9585. 9597. 9648. 9696. 9760. 9790. 9804. 9810. 9828. 9867. 9888. 9900. 9928. 9940. 9990	38
7	9078. 9080. 9090. 9093. 9174. 9256. 9321. 9361. 9381. 9453. 9462. 9528. 9633. 9646. 9724. 9752. 9805. 9858. 9885. 9906 ..	20
8	9016(*2*). 9024. 9060. 9135. 9144. 9156. 9168. 9184. 9192. 9198. 9222. 9225. 9273. 9280(*2*). 9285. 9312(*2*). 9348. 9372. 9393. 9394. 9400. 9424. 9460. 9485. 9486. 9490. 9510(*2*). 9513(*2*). 9537. 9540(*2*). 9588. 9600(*2*). 9645. 9669. 9702(*2*). 9729. 9735. 9758. 9780. 9792(*2*). 9816. 9856. 9860. 9930. 9975. 9984	46
9	9061. 9064. 9105. 9114. 9180. 9185. 9200. 9272. 9390. 9420. 9450(*3*). 9471. 9541. 9548. 9555(*3*). 9630. 9657. 9705. 9709. 9720(*3*). 9825(*3*). 9849(*3*). 9889 ...	23
10	9020. 9128. 9152. 9210. 9330. 9338. 9366. 9440. 9525. 9534. 9594. 9620. 9636. 9741. 9750. 9798. 9821. 9834. 9918	19
11	9006. 9129. 9170. 9230. 9306. 9309. 9336. 9429. 9456. 9681. 9737. 9786. 9894. 9968	14

12	9021. 9065. 9141. 9204. 9264. 9324. 9425. 9435. 9461. 9504. 9516(*2*).	
	9560. 9605. 9632. 9680(*2*). 9900. 9861. 9864. 9905. 9920. 9936. 9954. 9996 ..	23
13	9545. 9594. 9842. 9966 ..	4
14	9096. 9269. 9296. 9350. 9380. 9416. 9581. 9789. 9944	9
15	9246. 9320. 9512. 9590. 9624. 9776. 9785	7
16	9401. 9614. 9845	3
17	9086. 9890	2
18	9044. 9656	2
19	9176	1
Total 233..16680		

Irreg. 11(*2*), 5(*3*)

Genera XVI.

3	9030. 9048. 9177. 9281. 9384. 9480. 9520. 9570. 9672. 9870. 9933	11
4	9120. 9165. 9345. 9360. 9405. 9690. 9744. 9765. 9768. 9880. 9912. 9945. 9960	13
5	9009. 9576. 9660. 9840 ..	4
28...1680.		

Genera XXXII.

2	9240	1
1...64		

Sum of all

classes *p.p.p.*	72549
expected	72572
$\Sigma\gamma\sqrt{D}$	72775
genera *p.p.p.*	4595
expected	4594,9

Irreg. 31(*2*). 32(*3*)...63

Greatest quotient

1,729662 from 9434. IV, 42

least

0,2421048 from 9823. IV, 6

Number of classes

less than half the root	244
less than the root greater than half	566
greater than the root	199

Eight hundred negative determinants.
of the form $-(15n + 7)$.

G. I. . . . . (93). . . . . (2793)

1	7	1
3	67	1
5	127	1
7	487	1
9	307(*3*). 367. 547. 907. 1087	5
11	967	1
13	607. 727	2
15	787. 1327. 1567. 1747. 1867. 2347. 2647	7
17	4447	1
19	3607. 4327. 5527	3
21	1627. 1987. 2467. 2707. 2767. 3067. 3187. 3907. 5107. 5647	10
23	1447. 3847	2
25	2887	1
27	3307. 3547(*3*). 4027(*3*). 4987. 6007. 6427. 7027. 9067. 10627	9
29	2287. 7207. 7687	3
31	3727. 8647	2
33	3967. 4567. 5167. 6547. 6967. 7867. 8167. 10987 .	8
35	9007	1
37	6367	1
39	4507. 5347. 7507. 9547. 9787. 9967. 10567. 11467. 11587. 11827	10
41	11047	1
43	5407. 6247. 8527. 8887 . .	4
45	5227(*3*). 5827. 6067(*3*). 6607. 8287. 8467. 8707. 9907(*3*). 10267	9
47	7927. 11887	2
51	6907. 10687	2
53	11287	1
57	9127	1
61	11527	1
63	9187	1
69	10867	1

Irreg. 6

G. II. . . . .(343). . . .(10010)

1	22. 37	2
2	52. 82. 97. 142	4
3	157. 172. 187. 202. 247. 262. 277. 397. 427. 652 . .	10
4	292. 337. 382. 457. 562. 577. 772. 862	8
5	412. 757. 847. 877. 982 . .	5
6	622. 667. 802. 1027. 1042. 1282. 1297. 1387. 1507. 1807. 2017. 2062	12
7	502. 892. 997. 1117. 1237. 1372. 1402. 1597. 1642. 1852	10
8	1252. 1657. 1822. 2137. 2302. 2377. 2962. 3217. 4687	9
9	922. 1132. 1147. 1207. 1267(*3*). 1687. 1882. 1927. 2047. 2122. 2167. 2227. 2437(*3*). 2557. 2572. 2797. 2902. 3037. 3292. 3427. 3532. 5692 . .	22
10	937. 1492. 1522. 2407. 2452. 2527. 2722. 2857. 3007. 3412. 3697. 4057. 4162. 4372. 4852	15
11	1942. 2182. 2662. 2677. 2917. 3637. 3802. 4957. 5077. 5212. 6127. 6637 . .	12
12	1732. 1762. 1777. 2107. 2587. 2692. 2827. 2947. 3127. 3202. 3742. 3787. 4132. 4222. 4267. 4387. 4657. 4747. 4867. 4882. 5182. 5587. 5707. 5947. 7417. 7492. 7522. 7987. 8002. 9667	30
13	2197. 2362. 3622. 3862. 4207. 4282. 5482. 6742. 6847. 6997. 8422. 8572. 8842. 9157. 9277. 10207. 11302	17
14	2932. 3022. 3457. 3487. 5422. 5602. 5812. 5887. 6337. 8017. 8782. 9172 . .	12
15	2092. 2602. 3142. 3517. 3667. 3877. 4087. 4357. 4492. 4627. 5047. 5062. 5437. 6022. 6442. 6667. 6727. 6892. 6922. 7087. 7162. 7387. 7477. 7627. 8227. 8677. 8812. 8947. 9307. 10147. 10732. 10957	32
16	2617. 3247. 4612. 4702. 6217. 7177. 8452. 8962. 10327. 10462. 11617 . . .	11
17	4762. 4927. 5197. 5287. 5557. 6037. 6502. 6652. 6982. 7132. 7327. 7402. 7642. 7702. 8047. 8317. 10042. 11482	18
18	4297. 5737. 5767. 5857(*3*). 6187. 6382. 6577. 6787. 7057. 7267(*3*). 7732. 7807. 8107(*3*). 8212. 8347. 8407. 8482. 8737. 8767. 10747(*3*). 10882. 11257. 11347. 11707 . . .	24
19	4252. 4597. 4822. 5722. 6172. 9487. 9727. 10597. 10837. 11062. 11197. 11677	12
20	3442. 4177. 7012. 8542. 9442. 9697. 9892. 10162. 10177	9
21	5242. 5932. 6487. 7147. 7447. 8182. 8332. 9397. 9427. 9607. 9862. 10012. 10102. 10342. 10927. 11002. 11227. 11317. 11767. 11962	20
22	6082. 6772. 7297. 7537. 7822. 9742. 9847. 11167 .	8
23	6277. 6397. 7237. 7717. 8902. 9382. 10522. 10762 .	8
24	7747. 7972. 8377. 9502. 9817. 10372. 10657. 10807. 10852. 10942. 11107. 11422. 11812	13
25	10477	1
26	7342. 7762. 9337. 11647 .	4

27	8587. 9247. 10357. 10447. 11212	5
28	11497	1
29	9532. 11722	2
30	10027. 11182. 11602. 11947	4
32	11332	1
34	10702	1
35	11437	1

Irreg. 6

G. IV....(310)....(9688)

1	112. 232	2
2	217. 322. 352. 442. 532. 592. 697. 742. 1012 ...	9
3	472. 517. 637. 682. 817. 1072. 1162. 1177. 1192. 1222. 1432. 1612	12
4	712. 832. 1057. 1312(*2*). 1357. 1417. 1462. 1477. 1537. 1552. 1582(*2*). 1717. 1792. 1897. 1912. 1957. 2077. 2212. 2242. 2272. 2332. 2542(*2*). 2842. 3172(*2*). 3322. 3502(*2). 3712	27
5	1102. 1342. 1702. 2032: 2152. 2422. 3082. 3367. 3382. 3397. 3817. 3922. 4102. 4342. 5272. 5377 ..	16
6	1837. 1972. 2257. 2317. 2482. 2512. 2752. 2872. 2977. 3052. 3232. 3337. 3577. 3592. 3652. 3892. 3937. 3997. 4012. 4117. 4192. 4237. 4417. 4432. 4477. 4537. 4552. 4642. 4717. 4792. 4942. 4972. 5317. 5362. 5467. 5497. 5842. 6157. 6262. 6307. 6352. 6472. 6682. 6862. 7282. 7837. 10432	47
7	2497. 2782. 2812. 3097. 3112. 3277. 3352. 3562. 3982. 4582. 4732. 5122. 5137. 5302. 5902. 5977. 6142. 6517. 7792. 9262. 9367. 9802. 9937	23
8	3262(*2*). 3682. 3757. 3772. 3832. 4402. 4672(*2*). 4777(*2*). 5002. 5017.. 5257. 5392. 5572. 5632. 5752. 5917. 5962. 6052(*2*). 6112. 6202. 6532. 6697. 6757. 6817. 7252. 7312. 7357. 7582(*2*). 7597. 8122. 8197. 8257. 8497. 8992(*2*). 9202. 9232. 9412(*2*). 9457(*2*). 9472. 9562. 9577. 10132(*2*). 10312. 10537. 10642. 11092. 11377. 11512. 11572. 11797	50
9	4042. 4072. 4147. 4837. 4897. 4912(*3*). 5452. 5542. 5677. 5782. 5872. 6322. 6412. 6457. 7102. 7117. 7372. 7852. 7942. 8062. 8092. 8152. 8242(*3*). 8752. 8827(*3*). 9022. 9037. 9097. 9622. 9772. 9832. 9997. 10222. 10252(*3*). 10717. 10822. 11407. 11692. 11782. 11992	40
10	4462. 4807. 5092. 5332. 6292. 6592. 6712. 6802. 6937. 7432. 7897. 8077. 8137. 8302. 8557. 8617. 8692. 8857. 8977. 9517. 10057. 10087. 10297. 10402. 10552. 10777. 10972. 11122. 11272. 11932	30
11	5662. 7222. 7567. 7612. 7882. 8362. 8662. 8917. 9052. 9322. 10417. 10492. 11452. 11902	14

12	5617. 6562. 6877. 7042. 7552. 7957. 8392. 8722. 9142. 9292. 9652. 9682. 9922. 9952. 10237. 10387. 10612. 10672. 11017. 11542. 11737. 11917	22
13	8872. 9082. 9637. 9712. 10117. 11632	6
14	8032. 9217. 9757. 11662. 11842	5
15	8797. 10072. 10507 ...	3
16	10282. 10897. 11392(*2*). 11857	4

Irreg. 19

G. VIII....(54)....(1856)

2	952. 1672. 2002. 2392. 2632. 2737	6
3	2992. 3157. 3952. 4522. 5032. 5797. 6097. 6232. 6832. 7912	10
4	3472. 4312. 5152(*2*). 5992. 6622. 6952. 7072(*2*). 7672(*2*). 8437. 8512. 8932. 9982. 11152. 11872	14
5	5512. 7192. 7462. 7657. 7777. 8632. 9592. 9877. 11242. 11362. 11557 ...	11
6	8272. 9112. 9352. 10192. 10582. 10792. 10912. 11032. 11077. 11137. 11752. 11977	12
7	8602	1

Irreg. 3

All genera 2451 expected 2445,10
all classes 24347 expected 24358,82

$$\left.\begin{array}{l}\left.\begin{array}{ll}8n\ldots.. & 3068\\ 8n+4\,.. & 3010\end{array}\right\}6078\\ \left.\begin{array}{ll}8n+2\,.. & 3062\\ 8n+6\,.. & 3034\end{array}\right\}6096\end{array}\right\}12174$$

$$\left.\begin{array}{l}\left.\begin{array}{ll}8n+1\,.. & 3076\\ 8n+5\,.. & 3026\end{array}\right\}6102\\ \left.\begin{array}{ll}8n+3\,.. & 3033\\ 8n+7\,.. & 3038\end{array}\right\}6071\end{array}\right\}12173$$

$7n\ldots..$	$115\,..$	3411
$7n+1\,..$	$115\,..$	3009
$7n+2\,..$	$114\,..$	2975
$7n+4\,..$	$114\,..$	2993
$R\,7\ldots$	$343\,..$	8977
$7n+3\,..$	$114\,..$	3979
$7n+5\,..$	$114\,..$	3998
$7n+6\,..$	$114\,..$	3982
$N\,7\ldots$	$342\,..$	11959

Impr. classes 4049
Proper together with improper
28396 expected 28418,62

Eight hundred negative determinants.
of the form $-(15n + 13)$

G. I. . . .(91). . . . .(2561)

3	43. 163	2
5	103	1
7	223. 343. 463	3
9	283. 643. 823. 883. 1423 .	5
11	1303	1
13	2143	1
15	523. 1123. 1723. 2203. 2683	5
17	1663. 1783	2
19	1063. 1543. 3343. 3463 . .	4
21	1483. 2083. 2503. 4603. 5923	5
23	4783. 6703	2
25	5023. 5503	2
27	2803. 3163. 3643. 3943. 4243. 4363. 4483. 4723. 4903. 5443(*3*). 6043. 6763. 6883. 7723(*3*). 8563. 8803(*3*). 11383 .	17
29	2383. 3583. 3823. 5743. 8863	5
31	11863	1
33	4423. 4663. 5623. 5683. 6163. 6343. 6823. 7603. 8443. 9283. 9403. 9643 . .	12
35	11503	1
39	4003. 7243. 7963. 11743. 11923	5
41	10903	1
43	8263	1
45	5323. 5563(*3*). 9043. 9463. 10243. 10663. 10723(*3*). 11083 . . .	8
51	8623. 9343. 9883. 10303. 11443	5
57	8923. 9103	2

G. II. . . .(340). . . .(10110)

1.	13. 28. 58	3
2	73. 148. 193	3
3	118. 268. 298. 358. 403 .	5
4	178. 313. 388. 478. 583 .	5
5	373. 508. 538. 613. 853. 1093. 1213. 1318	8
6	433. 628. 673. 718. 763. 898. 1003. 1033. 1108. 1138. 1198. 1243. 1588. 1618. 1873	15
7	703. 733. 778. 838. 1183. 1453. 1948. 2293	8
8	943. 958. 1153. 1348. 1438. 1828. 2113. 2308. 2578. 2878	10

9	1018. 1228(*3*). 1363. 1468. 1603. 1843. 1933. 1963. 2023. 2038. 2053. 2188. 2443. 2458. 2563(*3*). 2923. 2998. 3238. 3523. 3628. 3733. 3763. 4348. 4678. 5413	25
10	1678. 1753. 1858. 2473. 2638. 2743. 2818. 2983. 3028. 3103. 3118. 3508. 4153	13
11	1693. 1903. 2263. 2623. 2863. 3418. 3703. 3868. 3958. 4918. 5098. 8023. 8143	13
12	1993. 2098. 2323. 2593. 2713. 2953. 3283. 3313. 3403. 3433. 3778. 3883. 4063. 4258. 4273. 4513. 4843. 5188. 5233. 5758. 5938. 6073. 6238. 8068 . .	24
13	2218. 2428. 2908. 3373. 3613. 3853. 3898. 4093. 4618. 4933. 5383. 5818. 5878. 6598. 7078. 8383. 8743. 10333. 10543	19
14	3673. 3988. 4078. 4183. 4468. 4948. 5218. 5263. 6103. 6388. 6658. 6673. 7438. 7753. 7858. 8233. 8353. 11113. 11278	19
15	2518. 3148. 3223. 4138. 4813. 5203. 5398. 5653. 5803. 6268. 6403. 6463. 6778. 6988. 7123. 7303. 7363. 7468. 7483. 8053. 8458. 8698. 9013. 9388. 10483. 10588	26
16	2833. 4993. 6178. 6628. 7183. 7393. 8548. 8578. 9433. 9508. 10558	11
17	3253. 4303. 5308. 5578. 7333. 7558. 8038. 9223. 9703	9
18	3043. 3793. 4963. 5458. 5998. 6283(*3*). 6418. 6553. 6583(*3*). 6793. 7543. 9298. 9523. 9583. 9748(*3*). 10003. 10018. 10228. 10603. 10753. 10798(*3*). 11698 . . .	22
19	5158. 5638. 6373. 6733. 7573. 7933. 8983. 9133. 10198. 11173	10
20	3748. 5143. 6223. 6718. 6898. 7063. 7423. 8098. 8158. 9598. 10063. 10513. 10993. 11428. 11953 . . .	15
21	4198. 6133. 6508. 6523. 7213. 7318. 7948. 7978. 8518. 9613. 9733. 9868. 10093. 10123. 10363. 10378. 10453. 10828. 11023. 11068. 11263. 11323. 11878	23
22	5113. 5953. 5983. 7663. 7783. 7873. 7903. 7993. 8713. 10273. 10708. 11668. 11758	13
23	5788. 8278. 8293. 8893. 9973. 10423. 10618	7
24	4798. 6943. 7003. 7108. 8083. 8503. 8683. 8818. 9763. 10843. 10963. 11143. 11203 11353. 11563	15
25	10783. 11548	2
26	8788. 9778. 9838	3
27	8203. 11683(*3*)	2
28	9943. 10078. 11038. 11593 .	4
29	9148	1
30	9358. 11623	2
31	11983	1
32	10183. 10468	2
33	11338	1
40	11833	1

G. IV....(320)....(10088)

1	88. 133. 253	3
2	208. 238. 328. 418. 448. 553. 568. 598. 658. 793. 928	11
3	493. 688. 748. 808. 913. 973. 988. 1048. 1258. 1558. 1708. 1978. 2608 ..	13
4	868. 1078. 1168. 1393. 1408. 1498. 1513(*2*). 1528. 1633. 1738. 1813. 1918(*2*). 2248. 2353. 2368. 2533. 2773. 2788(*2*). 2893. 3088. 3193. 3298. 3448	23
5	1273. 1333. 1378. 1573. 1648. 1798. 2158. 2173. 2398. 3133. 3178. 3388. 3928. 3973. 4558. 4873 ..	16
6	1888. 2068. 2278. 2338. 2413. 2488. 2548. 2653. 2668. 2698. 2758. 2938. 3073. 3208. 3268. 3478.	
	3598. 3658. 3718. 4018. 4033. 4108. 4123. 4168. 4288. 4393. 4438. 4453. 4708. 4753. 4768. 4978. 5083. 5128. 5173. 5293. 5338. 5518. 5548. 5713. 5728. 6028. 6433. 6493. 6913. 7018. 7093. 7228. 7813. 8248. 9823	51
7	2008. 3538. 3568. 3838. 4213. 4333. 4498. 4543. 4573. 5038. 5488. 5608. 5833. 5863. 6013. 6193. 6253. 6538. 6568. 6973. 7198. 7408. 9178. 9718. 10858. 10873	26
8	2848(*2*). 3013. 3058. 3328. 3358(*2*). 3493. 4228. 4318(*2*). 4633(*2*). 4738. 5008. 5248(*2*). 5428. 5533. 5668. 5908. 6148(*2*). 6208(*2*). 6868(*2*). 6958(*2*). 7033. 7168. 7288. 7588. 7648. 7828. 8308. 8338. 8638(*2*). 8653. 8878(*2*). 9088. 9118(*2*). 9193. 9208. 9538. 10033. 10138. 11533. 11848	40
9	3688. 4378. 4528. 4588. 4693. 4828. 5068(*3*). 5773. 6313. 6359. 6643. 6748. 7258. 7513. 7528. 7678. 7693(*3*). 7708. 7738. 7918. 8188. 8218. 8323(*3*). 8488. 8668. 8908. 8998. 9073. 9163(*3*). 9493. 9853. 9898. 9958. 10213. 10288. 10393. 10693. 11158. 11188. 11608. 11803. 11818. 11893	43
10	4858. 5053. 5473. 5968. 6058. 6088. 6613. 7153. 7273. 7453. 7498. 7798. 8128. 8173. 8473. 8593. 8608. 8758. 8773. 8833. 8953. 9058. 9238. 9553. 9628. 9793. 9808. 9913. 10108. 10438. 10888. 10978. 11053. 11293. 11398. 11458. 11938	37
11	6298. 7618. 7768. 8413. 8728. 10648. 11638. 11653	8
12	5353. 5893. 6838. 6928. 7048. 7348. 7633. 7843. 8428. 9028. 9268. 9673(*2*). 10048. 10258. 10348. 10768. 11008. 11218. 11308. 11488. 11578. 11788. 11908. 11998	24
13	8938. 9313. 9418. 9448. 9478. 10498. 10678. 10918. 11098. 11518	10
14	6478. 7138. 9253. 9658. 9988. 10573. 10633. 10933. 11233. 11728	10
15	8368. 10408. 10813. 11413. 11773	5

G. VIII. . . .(48). . . .(1600)

2	1288. 1768. 2128. 2233. 2968. 4048	6
3	2728. 3553. 3913. 4648. 4888. 5278. 6448	7
4	3808. 5593. 5698. 5848. 6118. 6328(*2*). 6688(*2*). 6853. 7378. 8398. 8848. 8968. 9328. 9373. 9568. 10168(*2*). 10528(*2*). 10948. 11368. 11713(*2*)	20
5	4408. 5368. 6808. 9688. 10153. 10738	6
6	7888. 8533. 9928. 10318. 11473. 11968	6
7	8113. 11128. 11248	3

G. XVI. . . .(1). . . . . (32)

2	8008	1

Total G. 2451 Cl. 24391

Irreg. 37 impr. 4075

			$15n+7$,13	
$7n$	115 . .	3435 . . .	230 . .	6846
$7n+1$ . .	114 . .	2988 . . .	229 . .	5997
$7n+2$ . .	114 . . .	2987 . . .	228 . .	5962
$7n+4$ . .	114 . .	2994 . . .	228 . .	5987
$R\,7$ . . .	342 . .	8969 . . .	685 . .	17946
$7n+3$ . .	114 . .	4005 . . .	228 . .	7984
$7n+5$ . .	114 . .	3975 . . .	228 . .	7973
$7n+6$ . .	115 . .	4007 . . .	229 . .	7989
$N\,7$ . . .	343 . .	11987 . . .	685 . .	23946
All .	800.	24391 . .	1600 . .	48738

Quot. min. 0,2349782 from 163,2608

max. 0,7354322 from 11833

Det. of the form

$-(15n+13)$ . .	68	305	271	128	27
$-(15n+7)$ . . .	69	316	264	130	21
	0,3	0,4	0,5	0,6	

[Det. in hundred 10000 of the form $15n$]

G. VIII. . . .(3). . . . .(1464)

48	999975
63	999945
72	999930

G. XVI. . . .(3). . . . .(2224)

39	999915
*44	999900
56	999990(*2*)

G. XXXII. .(1). . . . . .(576)
18 999960
104. 4264
Impr. 592

[Quotient $< \frac{1}{2} <$ $< 1 <$]

in hundred	11	Det.	24.	1.	56. . 19
	12		28		51 21
	13		21		58 21
	14		27		57 16
	15		21		62 17
	16		22		56 22
	17		29		52 19
	18		25.		57 18
	19		22		64 14
	20		21		61 18
	21		18		62 20
	22		18		63 19
	23		19		61 20
	24		27		55 18
	25		31		51 18
	26		26		54 20
	27		30		51 19
	28		27		53 20
	29		23		57 20
	30		24		58 18
	117		24		56 20
	118		20		61 19
	119		24		61 15
	120		29		52 19

Negative determinants.

in hundred	Quotient			
1	max.	1,271998	from det.	89
	min.	0,2626128		58
2		1,435917		194
		0,2349782		163

22	1,685723	2141
	0,2808228	2143
23	1,645848	2246
	0,2923654	2293
24	1,479278	2369
	0,2897240	2335
27	1,6445315	2609
	0,2895883	2683
28	1,5527075	2789
	0,3030216	2783
29	1,5778996	2834
	0,2974718	2893
30	1,604748	2939
	0,2936893	2968
91	1,684117	9026
	0,2835515	9067
92	1,586777	9176
	0,2717044	9157
93	1,660820	9281
	0,2699414	9277
94	1,518533	9371
	0,2893063	9367
95	1,729662	9434
	0,3287980	9472
96	1,689400	9539
	0,3269906	9577
97	1,707014	9686
	0,2440986	9667
99	1,650848	9869
	0,2420048	9823
100	1,702214	9974
	0,2808862	9937
117	1,6654535	11681
	0,2964744	11650
118	1,810938	11714
	0,294621	11797
119	1,579112	11864
	0,2846194	11863
120	1,5326965	11921
	0,3287433	11992

Positive determinants.

Hundred 1.
Square determinants excluded: 10.

G. I. . . .(12)
1 2. 5. 13. 17. 29. 41. 53. 61. 73. 89. 97
3 37
G. II. . . .(51)
1 3. 6. 7. 8. 10. 11. 12. 14. 18. 19. 20. 21. 22. 23. 26. 27. 28. 31. 32. 33. 38. 43. 44. 45. 46. 47. 50. 52. 54. 57. 58. 59. 62. 65. 67. 68. 69. 71. 74. 76. 77. 83. 85. 86. 92. 93. 94. 98
2 34. 82
3 79
G. IV. . .(27)
1 15. 24. 30. 35. 39. 40. 42. 48. 51. 55. 56. 60. 63. 66. 70. 72. 75. 78. 80. 84. 87. 88. 90. 91. 95. 96. 99

Hundred 2.
Excluded: 4.

G. I. . . .(11)
1 109. 113. 125. 137. 149. 157. 173. 181. 193
3 101. 197
G. II. . . .(41)
1 103. 106. 107. 108. 116. 117. 118. 122. 124. 127. 128. 129. 131. 133. 134. 139. 142. 151. 153. 158. 161. 162. 163. 164. 166. 167. 172. 174. 177. 179. 185. 188. 191. 199
2 145. 146. 178. 194
3 141. 148. 189
G. IV. . .(40)
1 102. 104. 105. 110. 111. 112. 114. 115. 119. 123. 126. 130. 132. 135. 136. 138. 140. 143. 147. 152. 154. 155. 156. 159. 160. 165. 170. 171. 175. 176. 180. 182. 183. 184. 186. 187. 190. 192. 198. 200
G. VIII. . .(4)
1 120. 150. 168. 195

Hundred 3.

G. I
1 233. 241. 277. 281. 293
3 229. 257. 269
G. II
1 201. 202. 206. 211. 212. 213. 214. 217. 218. 229. 236. 237. 239. 242. 243. 244. 245. 249. 250. 251. 253. 261. 262. 263. 265. 268. 271. 278. 283. 284. 292. 297. 298
2 205. 221. 274

3 223. 226. 254. 291
G. IV
1 203. 204. 207. 215. 216. 222. 228. 230. 232. 234. 238. 246. 247. 248. 252. 258. 259. 260. 266. 267. 270. 272. 273. 275. 276. 279. 282. 285. 286. 287. 290. 294. 295. 296. 299. 300
2 219. 220. 224. 288
3 235
G. VIII
1 210. 231. 240. 255. 264. 280

Hundred 9.

G. I. . . . .(7)
1 809. 821. 853. 857. 881
3 829. 877
G. II. . . .(32)
1 801. 811. 823. 827. 833. 838. 844. 845. 849. 859. 862. 863. 865. 869. 873. 878. 883. 886. 887. 889. 893
2 802. 818. 866
3 813. 837. 839. 842. 892
5 817
6 898
14 (841)
G. IV. . . .(52)
1 803. 804. 805. 806. 807. 808. 810. 814. 815. 822. 824. 825. 826. 830. 831. 832. 834. 835. 836. 843. 846. 847. 848. 850. 851. 852. 854. 856. 860. 861. 864. 867. 868. 871. 872. 875. 879. 882. 885
2 812. 820. 828. 876. 884. 890. 891. 896. 897
3 874. 894. 895. 899
G. VIII. . .(8)
1 816. 819. 855. 858. 888
2 870. 880. (900)
G. XVI. . .(1)
1 840

Hundred 10.

G. I. . . .(6). . . . .(8)
1 929. 937. 941. 953. 977
3 997
G. II. . .(38). . . .(130)
1 907. 908. 911. 913. 917. 919. 921. 922. 926. 932. 947. 949. 956. 958. 964. 965. 967. 971. 972. 974. 981. 983. 989. 991. 998
2 914
3 905. 909. 916. 925. 933. 934. 973. 985. 993
5 982
6 901

[15 961]
G. IV....(40)...(224)
1 902. 918. 923. 927. 928. 931. 938. 942. 944. 945. 946. 948. 950. 951. 954. 955. 957. 962. 968. 969. 970. 976. 978. 980. 986. 988. 995. 996. 999. 1000
2 939. 943. 959. 963. 979. 992
3 906. 940
4 904. 994
G. VIII...(16)...(144)
1 903. 912. 915. 920. 924. 930. 935. 936. 952. 966. 975. 984. 987. 990
2 910. 960

Total 370

G. I
1 313. 317
3 349. 373. 389. 397. 557. 677. 701. 709. 733. 757. 761
5 401
7 577
G. II
1 301. 302. 307. 309. 311. 314.
2 305
3 316. 321. 325. 326
5 727
G. IV
1 303. 304. 308. 310. 318. 319. 320. 327
2 306. 322. 323
G. VIII
1 312. 315

TABLE
FOR
CIRCLE DIVISION.

2	5	3	5
4	17	5	13
6	37	7	5 . 5
8	5 . 13	9	41
10	101	11	61
12	5 . 29	13	5 . 17
14	197	15	113
17	5 . 29	18	5 . 5 . 13
19	181	21	13 . 17
22	5 . 97	23	5 . 53
27	5 . 73	28	5 . 157
30	17 . 53	31	13 . 37
32	5 . 5 . 41	33	5 . 109
34	13 . 89	37	5 . 137
38	5 . 17 . 17	41	29 . 29
43	5 . 5 . 37	44	13 . 149
46	29 . 73	47	5 . 13 . 17
50	41 . 61	55	17 . 89
57	5 . 5 . 5 . 13	68	5 . 5 . 5 . 37
70	13 . 13 . 29	72	5 . 17 . 61
73	5 . 13 . 41	75	29 . 97
76	53 . 109	80	37 . 173
81	17 . 193	83	5 . 13 . 53
91	41 . 101	93	5 . 5 . 173
98	5 . 17 . 113	99	13 . 13 . 29
100	73 . 137	105	37 . 149
111	61 . 101	112	5 . 13 . 193
117	5 . 37 . 37	119	73 . 97
123	5 . 17 . 89	128	5 . 29 . 113
129	53 . 157	132	5 . 5 . 17 . 41
133	5 . 29 . 61	142	5 . 37 . 109
157	5 . 5 . 17 . 29	162	5 . 29 . 181
172	5 . 61 . 97	173	5 . 41 . 73
174	13 . 17 . 137	182	5 . 5 . 5 . 5 . 53
183	5 . 17 . 197	185	109 . 157
191	17 . 29 . 37	192	5 . 73 . 101
193	5 . 5 . 5 . 149	200	13 . 17 . 181
211	113 . 197	212	5 . 89 . 101
216	13 . 37 . 97	233	5 . 61 . 89
237	5 . 41 . 137	239	13 . 13 . 13 . 13
242	5 . 13 . 17 . 53	251	17 . 17 . 109
253	5 . 37 . 173	255	13 . 41 . 61

265	13 . 37 . 73	268	5 . 5 . 13 . 13 . 17
278	5 . 13 . 29 . 41	293	5 . 5 . 17 . 101
294	13 . 61 . 109	302	5 . 17 . 29 37
307	5 . 5 . 5 . 13 . 29	313	5 . 97 . 101
319	17 . 41 . 73	327	5 . 17 . 17 . 37
342	5 . 149 . 157	343	5 . 5 . 13 . 181
360	29 . 41 . 109	378	5 . 17 . 41 . 41
394	29 . 53 . 101	401	37 . 41 . 53
403	5 . 109 . 149	408	5 . 13 . 13 . 197
411	13 . 73 . 89	437	5 . 13 . 13 . 113
438	5 . 17 . 37 . 61	443	5 . 5 . 5 . 5 . 157
447	5 . 13 . 29 . 53	463	5 . 13 . 17 . 97
467	5 . 113 . 193	499	13 . 61 . 157
500	53 . 53 . 89	507	5 . 5 . 53 . 97
512	5 . 13 . 37 . 109	515	13 . 101 . 101
524	37 . 41 . 181	538	5 . 13 . 61 . 73
557	5 . 5 . 5 . 17 . 73	560	53 . 61 . 97
568	5 . 5 . 5 . 29 . 89	577	5 . 13 . 13 . 197
599	17 . 61 . 173	606	13 . 13 . 41 . 53
616	13 . 17 . 17 . 101	621	29 . 61 . 109
657	5 . 5 . 89 . 97	660	37 . 61 . 193
682	5 . 5 . 5 . 61 . 61	684	13 . 17 . 29 . 73
693	5 . 5 . 5 . 17 . 113	697	5 . 13 . 37 . 101
701	17 . 97 . 149	743	5 . 5 . 61 . 181
746	13 . 13 . 37 . 89	757	5 . 5 . 73 . 157
772	5 . 13 . 53 . 173	776	73 . 73 . 113
785	13 . 137 . 173	798	5 . 13 . 97 . 101
818	5 . 5 . 5 . 53 . 101	829	17 . 17 . 29 . 41
853	5 . 13 . 29 . 193	882	5 . 5 . 29 . 29 . 37
905	13 . 17 . 17 . 109	919	37 . 101 . 113
922	5 . 17 . 73 . 137	924	53 . 89 . 181
931	13 . 17 . 37 . 53	945	29 . 89 . 173
948	5 . 17 . 97 . 109	993	5 . 5 . 13 . 37 . 41
999	17 . 149 . 197	1032	5 . 5 . 13 . 29 . 113
1057	5 . 5 . 5 . 41 . 109	1067	5 . 17 . 37 . 181
1068	5 . 5 . 5 . 5 . 5 . 5 . 73	1087	5 . 13 . 61 . 149
1118	5 . 5 . 17 . 17 . 173	1123	5 . 13 . 89 . 109
1143	5 . 5 . 17 . 29 . 53	1148	5 . 29 . 61 . 149
1196	53 . 137 . 197	1228	5 . 17 . 113 . 157
1239	41 . 97 . 193	1270	61 . 137 . 193
1303	5 . 41 . 41 . 101	1341	73 . 109 . 113
1385	41 . 149 . 157	1393	5 . 5 . 197 . 197
1407	5 . 5 . 17 . 17 . 137	1432	5 . 5 . 5 . 5 . 17 . 193
1433	5 . 29 . 73 . 97	1467	5 . 29 . 41 . 181
1477	5 . 13 . 97 . 173	1560	17 . 37 . 53 . 73
1567	5 . 41 . 53 . 113	1568	5 . 5 . 5 . 13 . 17 . 89
1597	5 . 37 . 61 . 113	1607	5 . 5 . 13 . 29 . 137
1636	17 . 29 . 61 . 89	1744	137 . 149 . 149

1772	5 . 17 . 17 . 41 . 53	1818	5 . 5 . 5 . 137 . 193
1823	5 . 17 . 113 . 173	1832	5 . 5 . 17 . 53 . 149
1893	5 . 5 . 13 . 37 . 149	1918	5 . 5 . 37 . 41 . 97
1929	13 . 13 . 101 . 109	1955	13 . 29 . 37 . 137
1984	13 . 29 . 53 . 197	2010	13 . 17 . 101 . 181
2013	5 . 29 . 89 . 157	2018	5 . 5 . 29 . 41 . 137
2042	5 . 29 . 149 . 193	2059	13 . 41 . 41 . 97
2153	5 . 13 . 181 197	2163	5 . 13 . 17 . 29 . 73
2191	89 . 149 . 181	2309	13 . 53 . 53 . 73
2350	17 . 17 . 97 . 197	2428	5 . 41 . 149 . 193
2436	13 . 13 . 13 . 37 . 73	2515	101 . 173 . 181
2540	13 . 29 . 109 . 157	2547	5 . 37 . 89 . 197
2621	13 . 37 . 37 . 193	2673	5 . 13 . 17 . 53 . 61
2697	5 41 . 113 . 157	2738	5 . 13 . 29 . 41 . 97
2801	17 . 29 . 73 . 109	2818	5 . 5 . 5 . 17 . 37 . 101
2917	5 . 13 . 29 . 37 . 61	2943	5 . 5 . 5 . 5 . 13 . 13 . 41
3039	17 . 61 . 61 . 73	3112	5 . 13 . 13 . 73 . 157
3141	13 . 13 . 17 . 17 . 101	3149	17 . 29 . 89 . 113
3166	17 . 41 . 73 . 197	3207	5 . 5 . 29 . 41 . 173
3323	5 . 13 . 29 . 29 . 101	3362	5 . 13 . 17 . 53 . 193
3405	29 . 29 . 61 . 113	3458	5 . 73 . 181 . 181
3521	29 . 37 . 53 . 109	3532	5 . 5 . 17 . 149 . 197
3583	5 . 13 . 17 . 37 . 157	3740	41 . 41 . 53 . 157
3782	5 . 5 . 29 . 109 . 181	3793	5 . 5 . 53 . 61 . 89
3957	5 . 5 . 13 . 13 . 17 . 109	4193	5 . 5 . 5 . 5 . 5 . 29 . 97
4217	5 . 13 . 29 . 53 . 89	4232	5 . 5 . 41 . 101 . 173
4246	13 . 17 . 29 . 29 . 97	4327	5 . 89 . 109 . 193
4484	17 . 89 . 97 . 137	4535	17 . 53 . 101 . 113
4545	13 . 37 . 109 . 197	4581	13 . 53 . 97 . 157
4594	13 . 17 . 29 . 37 . 89	4662	5 . 13 . 13 . 17 . 17 . 89
4747	5 . 17 . 41 . 53 . 61	4906	13 . 53 . 181 . 193
4937	5 . 73 . 173 . 193	4952	5 . 37 . 41 . 53 . 61
5052	5 . 13 . 41 . 61 . 157	5087	5 . 17 . 29 . 29 . 181
5257	5 . 5 . 13 . 17 . 41 . 61	5283	5 . 13 . 17 . 73 . 173
5357	5 . 5 . 61 . 97 . 97	5443	5 . 5 . 5 . 5 . 137 . 173
5507	5 . 5 . 13 . 13 . 37 . 97	5648	5 . 17 . 53 . 73 . 97
5667	5 . 29 . 37 . 41 . 73	5701	29 . 53 . 97 . 109
5767	5 . 13 . 17 . 101 . 149	5928	5 . 29 . 29 . 61 . 137
5962	5 . 13 . 29 . 109 . 173	6065	17 . 53 . 137 . 149
6107	5 . 5 . 17 . 17 . 29 89	6118	5 . 5 . 13 . 41 . 53 . 53
6252	5 . 17 . 29 . 101 . 157	6481	17 . 37 . 173 . 193
6682	5 . 5 . 5 . 29 . 109 . 113	6898	5 . 13 . 17 . 17 . 17 . 149
6908	5 . 13 . 73 . 89 113	6943	5 . 5 . 5 . 29 . 61 . 109
6962	5 . 37 . 37 . 73 . 97	7093	5 . 5 . 13 . 17 . 29 . 157
7161	17 . 101 . 109 . 137	7443	5 . 5 . 5 . 37 . 53 . 113
7697	5 . 17 . 29 . 61 . 197	7782	5 . 5 . 13 . 17 . 97 . 113
8224	13 . 17 . 29 . 61 . 173	8307	5 . 5 . 5 . 5 . 5 . 61 . 181
8368	5 . 5 . 17 . 37 . 61 . 73		

8393	5 . 5 . 13 . 29 . 37 . 101
8578	5 . 37 . 41 . 89 . 109
9152	5 . 29 . 41 . 73 . 193
9298	5 . 41 . 53 . 73 . 109
9466	29 . 37 . 37 . 37 . 61
9703	5 . 13 . 13 . 17 . 29 . 113
9872	5 . 13 . 13 . 29 . 41 . 97
10298	5 . 17 . 61 . 113 . 181
10833	5 . 17 . 41 . 113 . 149
11471	13 . 17 . 41 . 53 . 137
12332	5 . 5 . 13 . 41 . 101 . 113
12882	5 . 5 . 17 . 37 . 61 . 173
13043	5 . 5 . 17 . 17 . 61 . 193
13241	29 . 101 . 173 . 173
13545	17 . 17 . 53 . 53 . 113
14140	17 . 29 . 37 . 97 . 113
14573	5 . 17 . 73 . 109 . 157
14773	5 . 13 . 13 . 29 . 61 . 73
14958	5 . 13 . 101 . 173 . 197
16513	5 . 29 . 53 . 113 . 157
17191	13 . 17 . 61 . 97 . 113
17766	13 . 37 . 73 . 89 . 101
18258	5 . 29 . 97 . 137 . 173
18543	5 . 5 . 13 . 17 . 29 . 29 . 37
19283	5 . 37 . 37 . 157 . 173
19534	13 . 13 . 13 . 29 . 53 . 113
19703	5 . 13 . 13 . 29 . 89 . 89
19911	13 . 17 . 29 . 157 . 197
20457	5 . 5 . 13 . 29 . 149 . 149
21705	13 . 17 . 61 . 101 . 173
22008	5 . 41 . 109 . 149 . 157
22231	29 . 37 . 41 . 41 . 137
24331	13 . 17 . 89 . 101 . 149
24816	17 . 17 . 61 . 181 . 193
25523	5 . 53 . 73 . 113 . 149
25793	5 . 5 . 17 . 29 . 137 . 197
26018	5 . 5 . 13 . 97 . 109 . 197
28205	13 . 29 . 73 . 97 . 149
28862	5 . 17 . 17 . 53 . 73 . 149
30027	5 . 29 . 89 . 181 . 193
30383	5 . 17 . 17 . 37 . 89 . 97
32258	5 . 13 . 37 . 41 . 61 . 173
32807	5 . 5 . 5 . 13 . 61 . 61 . 89
32973	5 . 13 . 37 . 37 . 41 . 149
34208	5 . 13 . 13 . 17 . 29 . 53 . 53
35857	5 . 5 . 17 . 61 . 137 . 181
37057	5 . 5 . 5 . 5 . 73 . 101 . 149
37770	13 . 17 . 29 . 41 . 61 . 89
8457	5 . 5 . 53 . 137 . 197
9133	5 . 17 . 37 . 89 . 149
9193	5 . 5 . 5 . 5 . 17 . 41 . 97
9431	17 . 97 . 149 . 181
9667	5 . 13 . 41 . 89 . 197
9762	5 . 17 . 37 . 157 . 193
9901	13 . 13 . 29 . 73 . 137
10312	5 . 29 . 53 . 101 . 137
11018	5 . 5 . 157 . 157 . 197
11981	13 . 17 . 41 . 89 . 89
12433	5 . 13 . 61 . 101 . 193
12943	5 . 5 . 5 . 5 . 13 . 13 . 13 . 61
13068	5 . 5 . 5 . 53 . 149 . 173
13252	5 . 13 . 13 . 37 . 41 . 137
13918	5 . 5 . 13 . 37 . 89 . 181
14318	5 . 5 . 5 . 13 . 17 . 41 . 181
14646	13 . 37 . 41 . 73 . 149
14942	5 . 13 . 13 . 37 . 37 . 193
15075	13 . 17 . 53 . 89 . 109
16928	5 . 17 . 109 . 157 . 197
17557	5 . 5 . 5 . 17 . 29 . 41 . 61
17923	5 . 61 . 61 . 89 . 97
18432	5 . 5 . 5 . 17 . 29 . 37 . 149
19123	5 . 29 . 37 . 173 . 197
19326	13 . 29 . 61 . 109 . 149
19653	5 . 37 . 61 . 109 . 157
19902	5 . 73 . 89 . 89 . 137
20080	13 . 29 . 61 . 89 . 197
21124	29 . 41 . 53 . 73 . 97
21907	5 . 5 . 29 . 29 . 101 . 113
22157	5 . 5 . 13 . 37 . 137 . 149
24263	5 . 13 . 17 . 41 . 73 . 89
24778	5 . 29 . 149 . 157 . 181
25462	5 . 13 . 17 . 37 . 101 . 157
25683	5 . 13 . 17 . 17 . 97 . 181
25943	5 . 5 . 5 . 13 . 29 . 37 . 193
27493	5 . 5 . 17 . 17 . 17 . 17 . 181
28322	5 . 13 . 13 . 13 . 13 . 41 . 137
29757	5 . 5 . 41 . 61 . 73 . 97
30103	5 . 13 . 17 . 41 . 73 . 137
31752	5 . 17 . 17 . 37 . 109 . 173
32406	17 . 17 . 17 . 37 . 53 . 109
32885	13 . 13 . 109 . 149 . 197
33307	5 . 5 . 5 . 5 . 17 . 53 . 197
34367	5 . 13 . 37 . 41 . 53 . 113
36673	5 . 17 . 29 . 37 . 73 . 101
37448	5 . 13 . 13 . 53 . 173 . 181
38326	29 . 37 . 41 . 173 . 193

38807	5 . 5 . 5 . 17 . 37 . 61 . 157	39082	5 . 5 . 41 . 73 . 137 . 149
39307	5 . 5 . 5 . 13 . 13 . 13 . 29 97	39818	5 . 5 . 5 . 5 . 17 . 37 . 37 . 109
40188	5 . 13 . 37 . 61 . 101 . 109	40515	17 . 53 . 61 . 109 . 137
40568	5 . 5 . 5 . 13 . 53 . 97 . 197	41187	5 . 17 . 37 . 37 . 37 . 197
41319	13 . 41 . 101 . 101 . 157	41688	5 . 17 . 41 . 53 . 97 . 97
42658	5 . 13 . 13 . 97 . 149 . 149	42932	5 . 5 . 5 . 29 . 29 . 89 . 197
43633	5 . 13 . 29 . 41 . 109 . 113	43932	5 . 5 . 5 . 5 . 13 . 17 . 89 . 157
44179	13 . 13 . 13 . 17 . 17 . 29 . 53	44507	5 . 5 . 13 . 113 . 149 . 181
44733	5 . 89 . 101 . 113 . 197	45050	13 . 41 . 109 . 181 . 193
45068	5 . 5 . 5 . 41 . 61 . 73 . 89	46444	13 . 41 . 149 . 157 . 173
46617	5 . 53 . 137 . 173 . 173	47403	5 . 13 . 29 . 37 . 89 . 181
47783	5 . 13 . 17 . 53 . 101 . 193	48187	5 . 97 . 101 . 137 . 173
48737	5 . 29 . 29 . 53 . 73 . 73	49083	5 . 13 . 17 . 73 . 109 . 137
50052	5 . 17 . 41 . 41 . 89 . 197	51115	17 . 17 . 17 . 29 . 53 . 173
51387	5 . 17 . 37 . 53 . 89 . 89	51412	5 . 17 . 61 . 61 . 61 . 137
51917	5 . 13 . 37 . 53 . 97 . 109	52571	37 . 41 . 61 . 109 . 137
54193	5 . 5 . 5 . 5 . 5 . 41 . 73 . 157	54358	5 . 13 . 29 . 73 . 109 . 197
54507	5 . 5 . 37 . 53 . 157 . 193	57532	5 . 5 . 17 . 41 . 41 . 41 . 113
66347	5 . 13 . 13 . 17 . 37 . 41 . 101	67333	5 . 17 . 53 . 61 73 . 113
67852	5 . 13 . 37 . 89 . 137 . 157	68463	5 . 13 . 17 . 113 . 137 . 137
71564	37 . 61 . 97 . 149 . 157	71700	13 . 29 . 37 . 41 . 89 . 101
72662	5 . 13 . 17 . 29 . 37 . 61 . 73	74043	5 . 5 . 13 . 37 . 37 . 61 . 101
75382	5 . 5 . 13 . 17 . 73 . 73 . 193	78629	13 . 17 . 41 . 41 . 53 . 157
80593	5 . 5 . 17 . 17 . 17 . 137 . 193	80802	5 . 37 . 41 . 53 . 109 . 149
81141	13 . 61 . 137 . 157 . 193	81749	13 . 17 . 17 . 53 . 97 . 173
83071	37 . 61 . 89 . 89 . 193	83247	5 . 13 . 13 . 13 . 29 . 73 . 149
84141	13 . 29 . 29 . 41 . 53 . 149	85353	5 . 13 . 17 . 37 . 41 . 41 . 53
86143	5 . 5 . 13 . 17 . 61 . 101 . 109	88668	5 . 5 . 13 . 17 . 73 . 101 . 193
88699	29 . 53 . 89 . 149 . 193	88733	5 . 13 . 41 . 97 . 97 . 157
88868	5 . 5 . 29 . 37 . 37 . 73 . 109	89361	29 . 37 . 137 . 157 . 173
89471	13 . 13 . 41 . 41 . 73 . 193	90212	5 . 13 . 37 . 89 . 193 . 197
90657	5 . 5 . 13 . 17 . 61 . 89 . 137	93020	13 . 13 . 17 . 17 . 29 . 41 . 149
93197	5 . 37 . 53 . 53 . 61 . 137	99557	5 . 5 . 5 . 5 . 41 . 41 . 53 . 89
99893	5 . 5 . 29 . 181 . 193 . 197	101343	5 . 5 . 13 . 29 . 41 . 97 . 137
102163	5 . 37 . 41 . 41 . 97 . 173	104818	5 . 5 . 5 . 5 . 17 . 29 181 . 197
106242	5 . 53 . 53 . 73 . 101 . 109	109637	5 . 13 . 17 . 29 . 37 . 37 . 137
112595	17 . 29 . 41 . 53 . 61 . 97	112782	5 . 5 . 17 . 37 . 41 . 109 . 181
114669	17 . 37 . 53 . 53 . 61 . 61	117251	41 . 97 . 101 . 109 . 157
117307	5 . 5 . 5 . 13 . 149 . 157 . 181	117372	5 . 13 . 17 . 17 . 53 . 101 . 137
128482	5 . 5 . 17 . 29 . 89 . 101 . 149	129553	5 . 13 . 13 . 17 . 61 . 61 . 157
133749	13 . 13 . 37 . 53 . 137 . 197	136293	5 . 5 . 17 . 41 . 53 . 89 . 113
136404	13 . 17 . 29 . 97 . 173 . 173	137717	5 . 13 . 53 . 89 . 157 . 197
137883	5 . 13 . 17 . 29 . 29 . 53 . 193	141743	5 . 5 . 89 . 149 . 157 . 193
143382	5 . 5 . 13 . 13 . 17 . 17 . 113 . 149	145046	13 . 29 . 37 . 101 . 109 . 137
145231	13 . 37 . 37 . 41 . 97 . 149	148158	5 . 53 . 61 . 61 . 113 . 197
148582	5 . 5 . 13 . 53 . 73 . 97 . 181	150522	5 . 13 . 17 . 29 . 37 . 97 . 197
155317	5 . 41 . 61 . 73 . 73 . 181	157308	5 . 13 . 29 . 29 . 41 . 61 . 181
157318	5 . 5 . 5 . 5 . 5 . 5 . 13 . 37 37 . 89	159772	5 . 37 . 53 . 101 . 149 . 173

160590	29 . 29 . 29 . 89 . 109 . 109
162014	13 . 17 . 73 . 89 . 101 . 181
174118	5 . 5 . 17 . 41 . 89 . 113 . 173
180107	5 . 5 . 13 . 29 . 97 . 113 . 157
181743	5 . 5 . 17 . 17 . 73 . 173 . 181
161832	5 . 5 . 13 . 13 . 29 . 37 . 53 . 109
173932	5 . 5 . 5 . 5 . 5 . 13 . 73 . 101 . 101
177144	17 . 29 . 73 . 89 97 . 101
181343	5 . 5 . 17 . 37 . 53 . 109 . 181

184133	5 . 29 . 73 . 101 . 101 . 157
189782	5 . 5 . 13 . 61 . 89 . 137 . 149
190393	5 . 5 . 13 . 13 . 137 . 173 . 181
191407	5 . 5 . 13 . 13 . 17 . 37 . 61 . 113
191807	5 . 5 . 5 . 13 . 17 . 41 . 109 . 149
194708	5 . 5 . 29 . 41 . 73 . 101 . 173
201106	17 . 17 . 61 . 89 . 149 . 173
208048	5 . 53 . 89 . 109 . 113 . 149
210195	61 . 113 . 137 . 149 . 157
210943	5 . 5 . 5 . 13 . 37 . 37 . 73 . 137
211765	13 . 17 . 53 . 89 . 137 . 157
216676	13 . 29 . 41 . 97 . 173 . 181
219602	5 . 17 . 17 . 53 . 53 . 109 . 109
221382	5 . 5 . 13 . 73 . 101 . 113 . 181
228068	5 . 5 . 5 . 17 . 29 . 61 . 101 . 137
232643	5 . 5 . 13 . 13 . 13 . 41 . 61 . 197
236151	17 . 17 . 41 . 89 . 137 . 193
247643	5 . 5 . 17 . 29 . 73 . 173 . 197
249501	13 . 53 . 53 . 61 . 89 . 157
251103	5 . 13 . 17 . 17 . 89 . 109 . 173
256638	5 . 13 . 29 . 37 . 61 . 113 . 137
260359	13 . 13 . 17 . 41 . 53 . 61 . 89
262433	5 . 17 . 29 . 29 . 53 . 61 . 149
263317	5 . 17 . 17 . 17 . 89 . 101 . 157
263557	5 . 5 . 5 . 13 . 37 . 41 . 73 . 193
265842	5 . 13 . 17 . 17 . 101 . 193 . 193
267657	5 . 5 . 41 . 41 . 61 . 89 . 157
281897	5 . 13 . 29 . 37 . 37 . 89 . 173
286018	5 . 5 . 13 . 13 . 53 . 53 . 61 . 113
287228	5 . 17 . 17 . 29 . 73 . 149 . 181
289038	5 . 17 . 17 . 37 . 89 . 97 . 181
292362	5 . 13 . 17 . 41 . 61 . 157 . 197
298307	5 . 5 . 5 . 5 . 41 . 53 . 181 . 181
307939	13 . 29 . 61 . 101 . 137 . 149
309070	13 . 29 . 101 . 113 . 149 . 149
320078	5 . 13 . 41 . 61 . 73 . 89 . 97
322392	5 . 13 . 17 . 41 . 89 . 149 . 173
330182	5 . 5 . 5 . 5 . 5 . 13 . 29 . 37 . 41 . 61
331068	5 . 5 . 5 . 5 . 53 . 101 . 181 . 181
383807	5 . 5 . 5 . 13 . 37 . 73 . 97 . 173
385692	5 . 13 . 17 . 61 . 89 . 137 . 181

389163	5 . 13 29 . 41 . 89 . 101 . 109
390112	5 . 13 . 17 . 17 . 17 . 17 . 17 . 17 . 97
403639	29 . 29 . 37 . 97 . 137 . 197
409557	5 . 5 . 5 . 5 . 13 . 13 . 73 . 73 . 149
411787	5 . 17 . 17 . 53 . 97 . 101 . 113
418048	5 . 97 . 97 . 109 . 173 . 197
444753	5 . 53 . 109 . 113 . 157 . 193
447342	5 . 17 . 29 . 41 . 97 . 137 . 149
464307	5 . 5 . 5 . 29 . 37 . 73 . 101 . 109
465525	13 . 13 . 29 . 89 . 97 . 113 . 197
465694	13 . 13 . 17 . 29 . 73 . 181 . 197
478707	5 . 5 . 13 . 13 . 13 . 17 . 41 . 41 . 73
485298	5 . 13 . 13 13 . 13 . 29 . 29 . 37 . 53
494607	5 . 5 . 29 . 89 . 101 . 137 . 137
500150	41 . 61 . 73 . 73 . 137 . 137
508929	13 . 13 . 37 . 53 . 53 . 73 . 101
518734	13 . 17 . 37 . 37 . 53 . 97 . 173
520463	5 . 13 . 41 . 61 . 73 . 101 . 113
534568	5 . 5 . 5 . 13 . 89 . 89 . 149 . 149
538275	17 . 61 . 73 . 97 . 109 . 181
548630	37 . 41 . 89 . 109 . 113 . 181
566793	5 . 5 . 17 . 29 . 29 . 41 . 97 . 113
567923	5 . 13 . 17 . 17 . 17 . 41 . 109 . 113
571459	13 . 13 . 13 . 13 . 17 . 37 . 61 . 149
586455	29 . 41 . 73 . 89 . 113 . 197
606325	13 . 37 . 97 . 137 . 149 . 193
607533	5 . 17 . 29 . 73 . 97 . 97 . 109
617427	5 . 13 . 13 . 17 . 29 . 53 . 89 . 97
623888	5 . 13 . 37 . 41 . 113 . 181 . 193
627391	41 . 41 . 53 . 113 . 113 . 173
662843	5 . 5 . 17 . 113 . 137 . 173 . 193
672717	5 . 89 . 97 . 157 . 173 . 193
683982	5 . 5 . 17 . 29 . 61 . 61 . 101 . 101
700107	5 . 5 . 13 . 17 . 41 . 53 . 137 . 149
703175	13 . 17 . 17 . 29 . 97 . 149 . 157
704683	5 . 13 . 29 . 61 . 97 . 113 . 197
721068	5 . 5 . 5 . 5 . 17 . 29 . 109 . 113 . 137
780262	5 . 17 . 17 . 29 . 37 . 41 . 61 . 157
783568	5 . 5 . 5 . 5 . 17 . 29 . 101 . 109 . 181
791532	5 . 5 . 53 . 89 . 149 . 181 . 197
793921	17 . 17 . 17 . 29 . 73 . 157 . 193
812447	5 . 29 . 29 . 41 . 89 . 137 . 157
832902	5 . 13 . 13 . 13 . 17 . 109 . 173 . 197
848871	29 . 53 . 73 . 113 . 157 . 181
899168	5 . 5 . 17 . 37 . 53 . 73 . 97 . 137
907567	5 . 29 . 37 . 41 . 89 . 109 . 193
911111	17 . 41 . 101 . 173 . 173 . 197
936513	5 . 37 . 37 . 41 89 . 97 . 181

1000193	5 . 5 . 5 . 29 . 53 . 101 . 149 . 173
1010027	5 . 13 . 61 . 89 . 89 . 109 . 149
1024240	37 . 61 . 109 . 157 . 157 . 173
1031675	13 . 13 . 17 . 53 . 73 . 113 . 157 . 197
1049433	5 . 13 . 61 . 89 . 89 . 89 . 197
1059193	5 . 5 . 5 . 5 . 13 . 13 . 13 . 37 . 61 . 181
1067157	5 . 5 . 41 . 113 . 157 . 173 . 181
1068182	5 . 5 . 5 . 17 . 17 . 41 . 61 . 73 . 173
1083493	5 . 5 . 13 . 61 . 61 . 61 . 73 . 109
1089593	5 . 5 . 61 . 89 . 149 . 149 . 197
1131527	5 . 41 . 53 . 53 . 73 . 97 . 157
1139557	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 37 . 73 . 181
1143007	5 . 5 . 13 . 41 . 61 . 73 . 101 . 109
1197943	5 . 5 . 5 . 5 . 5 . 17 . 17 . 37 . 109 . 197
1264557	5 . 5 . 5 . 5 . 5 . 13 . 13 . 29 . 53 . 197
1306143	5 . 5 . 29 . 37 . 37 . 61 . 73 . 193
1351742	5 . 17 . 53 . 109 . 137 . 157 . 173
1373307	5 . 5 . 5 . 5 . 17 . 29 . 101 . 157 . 193
1387203	5 . 29 . 41 . 41 . 113 . 181 . 193
1402232	5 . 5 . 17 . 37 . 41 . 113 . 137 . 197
1413443	5 . 5 . 13 . 29 . 37 . 41 . 89 . 157
1477034	37 . 37 . 41 . 53 . 53 . 101 . 137
1518057	5 . 5 . 5 . 13 . 13 . 41 . 61 . 113 . 193
1528649	13 . 37 . 53 . 61 . 61 . 109 . 113
1615463	5 . 13 . 17 . 37 . 53 . 73 . 73 . 113
1618855	17 . 29 . 37 . 53 . 89 . 97 . 157
1635786	29 . 29 . 41 . 89 . 89 . 97 . 101
1664957	5 . 5 . 13 . 37 . 73 . 89 . 113 . 157
1750507	5 . 5 . 13 . 53 . 53 . 89 . 109 . 173
1766693	5 . 5 . 5 . 5 . 5 . 5 . 29 . 97 . 157 . 173
1824257	5 . 5 . 17 . 29 . 97 . 109 . 113 . 113
1909461	13 . 13 . 17 . 17 . 41 . 53 . 89 . 193
1954207	5 . 5 . 13 . 61 . 61 . 89 . 113 . 157
1984933	5 . 17 . 37 . 37 . 37 . 53 . 89 . 97
2036069	17 . 41 . 41 . 61 . 61 . 101 . 193
2050706	13 . 17 . 17 . 17 . 41 . 53 . 157 . 193
2052057	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 29 . 73 . 97 . 193
2126007	5 . 5 . 17 . 29 . 29 . 181 . 181 . 193
2277387	5 . 13 . 29 . 29 . 53 . 89 . 89 . 113
2298668	5 . 5 . 13 . 13 . 17 . 17 . 29 . 37 . 37 . 109
2343692	5 . 17 . 41 . 41 . 61 . 73 . 89 . 97
2353918	5 . 5 . 13 . 17 . 29 . 29 . 61 . 113 . 173
2379723	5 . 13 . 29 . 37 . 53 . 53 . 97 . 149
2457057	5 . 5 . 5 . 5 . 13 . 17 . 41 . 53 . 89 . 113
2471717	5 . 37 . 41 . 109 . 137 . 149 . 181
2475918	5 . 5 . 17 . 53 . 61 . 157 . 157 . 181
2478328	5 . 13 . 29 . 37 . 89 . 97 . 101 . 101
2484968	5 . 5 . 13 . 61 . 97 . 113 . 157 . 181

2680168	5 . 5 . 29 . 61 . 73 . 109 . 137 . 149
2733307	5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 13 . 17 . 37 . 173
2809305	13 . 17 . 29 . 37 . 37 . 61 . 73 . 101
2923783	5 . 13 . 17 . 37 . 41 . 109 . 149 . 157
2959007	5 . 5 . 17 . 37 . 97 . 101 . 157 . 181
3014557	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 41 . 53 . 53 . 101
3025001	13 . 13 . 17 . 17 . 61 . 73 . 109 . 193
3136570	13 . 13 . 29 . 37 . 53 . 61 . 97 . 173
3139557	5 . 5 . 5 . 5 . 5 . 5 . 13 . 29 . 73 . 73 . 157
3272693	5 . 5 . 5 . 13 . 37 . 41 . 101 . 137 . 157
3370437	5 . 13 . 13 . 13 . 13 . 41 . 73 . 97 . 137
3449051	13 . 13 . 13 . 53 . 61 . 89 . 97 . 97
3637197	5 . 13 . 17 . 29 . 61 . 89 . 193 . 197
3800438	5 . 13 . 29 . 29 . 97 . 101 . 149 . 181
3801448	5 . 29 . 37 . 53 . 61 . 73 . 101 . 113
3815076	13 . 13 . 17 . 37 . 53 . 109 . 137 . 173
3894873	5 . 13 . 13 . 37 . 89 . 101 . 137 . 197
3911450	29 . 29 . 41 . 97 . 137 . 173 . 193
3931663	5 . 13 . 29 . 37 . 41 . 109 . 137 . 181
4000300	13 . 13 . 13 . 17 . 17 . 73 . 137 . 181 . 181
4079486	13 . 17 . 17 . 53 . 61 . 73 . 137 . 137
4218932	5 . 5 . 5 . 5 . 29 . 41 . 41 . 61 . 61 . 157
4466678	5 . 13 . 17 . 73 . 97 . 109 . 149 . 157
4650839	17 . 17 . 89 . 113 . 137 . 157 . 173
4697282	5 . 5 . 13 . 113 . 113 . 137 . 197 . 197
4751232	5 . 5 . 13 . 17 . 29 . 73 . 97 . 101 . 197
4773557	5 . 5 . 5 . 29 . 29 . 41 . 113 . 149 . 157
5033696	13 . 17 . 37 . 37 . 89 . 89 . 97 . 109

5982670	13 . 13 . 13 . 17 . 41 . 53 . 53 . 53 . 157
6151956	13 . 17 . 29 . 29 . 73 . 97 . 113 . 149
6208047	5 . 17 . 17 . 17 . 17 . 29 . 41 . 41 . 197 . 197
6225244	29 . 37 . 41 . 53 . 53 . 53 . 61 . 97
6315768	5 . 5 . 17 . 17 . 53 . 61 . 73 . 149 . 157
6356150.	13 . 29 . 37 . 37 . 61 . 61 . 109 . 193
6367252	5 . 13 . 17 . 29 . 29 . 61 . 73 . 97 . 101
6656382	5 . 5 . 13 . 29 . 41 . 41 . 137 . 137 . 149
6817837	5 . 17 . 17 . 53 . 61 . 149 . 173 . 193
6829610	13 . 17 . 17 . 53 . 61 . 101 . 193 . 197
6981694	13 . 41 . 97 . 137 . 181 . 193 . 197
7138478	5 . 29 . 37 . 41 . 73 . 89 . 181 . 197
7620661	5 . 17 . 37 . 73 . 101 . 101 . 137 . 181
7691443	5 . 5 . 5 . 37 . 53 . 97 . 101 . 109 . 113
8082212	5 . 13 . 17 . 17 . 37 . 53 . 97 . 101 . 181
8571779	13 . 13 . 29 . 41 . 73 . 101 . 137 . 181
8809432	5 . 5 . 5 . 13 . 89 . 101 . 149 . 181 . 197
9407318	5 . 5 . 5 . 5 . 5 . 5 . 37 . 41 . 53 . 73 . 193

9548768	5 . 5 . 13 . 13 . 17 . 41 . 53 . 61 . 61 . 157
9614382	5 . 5 . 29 . 37 . 53 . 61 . 61 . 101 . 173
9639557	5 . 5 . 5 . 5 . 5 . 5 . 13 . 17 . 17 . 53 . 109 . 137
9689961	13 . 29 . 29 . 37 . 61 . 113 . 113 . 149
10328193	5 . 5 . 5 . 13 . 17 . 29 . 53 . 53 . 137 . 173
10669731	17 . 89 . 97 . 101 . 101 . 193 . 197
11131086	13 . 13 . 17 . 17 . 37 . 61 . 73 . 89 . 173
12477035	17 . 17 . 17 . 29 . 29 . 29 . 37 . 97 . 181
12514913	5 . 13 . 41 . 53 . 137 . 149 . 157 . 173
12750353	5 . 13 . 17 . 17 . 41 . 61 . 73 . 137 . 173
14698000	13 . 13 . 17 . 17 . 29 . 61 . 97 . 149 . 173
15165443	5 . 5 . 5 . 5 . 37 . 53 . 61 . 97 . 101 . 157
15986082	5 . 5 . 13 . 17 . 109 . 109 . 137 . 157 . 181
16317267	5 . 13 . 17 . 17 . 61 . 61 . 101 . 109 . 173
18378313	5 . 13 . 13 . 17 . 37 . 61 . 137 . 193 . 197
18975991	13 . 17 . 17 . 17 . 53 . 61 . 89 . 97 . 101
20198495	13 . 17 . 41 . 89 . 101 . 101 . 137 . 181
22866693	5 . 5 . 5 . 5 . 41 . 61 . 73 . 101 . 113 . 197
23747457	5 . 5 . 17 . 17 . 17 . 17 . 17 . 17 . 37 . 73 . 173
24208144	29 . 29 . 29 . 37 . 37 . 53 . 61 . 61 . 89
24280807	5 . 5 . 5 . 5 . 13 . 13 . 17 . 53 . 109 . 157 . 181
24310918	5 . 5 . 13 . 13 . 37 . 41 . 53 . 89 . 113 . 173
31011557	5 . 5 . 5 . 13 . 17 . 61 . 97 . 109 . 137 . 197
32944452	5 . 13 . 13 . 29 . 29 . 41 . 53 . 53 . 89 . 149
34436768	5 . 5 . 17 . 61 . 97 . 101 . 137 . 173 . 197
34602875	13 . 17 . 17 . 29 . 37 . 53 . 113 . 137 . 181
45500682	5 . 5 . 5 . 37 . 53 . 53 . 61 . 89 . 149 . 197
53365057	5 . 5 . 5 . 13 . 37 . 89 . 97 . 101 . 157 . 173
58305593	5 . 5 . 13 . 17 . 37 . 37 . 101 . 109 . 137 . 149
75505943	5 . 5 . 5 . 37 . 37 . 53 . 89 . 137 . 149 . 173
95665578	5 . 13 . 37 . 41 . 73 . 181 . 181 . 197 . 197
111530944	13 . 13 . 13 . 13 . 13 . 17 . 37 . 37 . 53 . 157 . 173
121042733	5 . 17 . 41 . 73 . 97 . 97 . 101 . 157 . 193
160007778	5 . 13 . 13 . 17 . 17 . 29 . 29 . 73 . 73 . 149 . 157
167207057	5 . 5 . 5 . 5 . 17 . 17 . 17 . 29 . 73 . 109 . 109 . 181
168623905	13 . 13 13 . 13 . 17 . 29 . 29 . 37 . 89 . 97 . 109
185507821	13 . 13 . 17 . 29 . 29 . 53 . 61 . 101 . 113 . 193
193788912	5 . 13 . 17 . 17 . 37 . 37 . 37 . 53 . 73 . 101 . 101
201229582	5 . 5 . 13 . 13 . 17 . 17 . 17 . 17 . 17 . 53 . 97 . 101
211823957	5 . 5 . 17 . 17 . 53 . 101 . 137 . 149 . 157 . 181
284862638	5 . 13 . 17 . 17 . 17 . 17 . 29 . 29 . 41 . 41 . 97 . 109
299252491	13 . 29 . 37 . 97 . 109 . 109 . 113 . 157
317742693	5 . 5 . 5 . 13 . 29 . 41 . 73 . 89 . 137 . 149 . 197
327012132	5 . 5 . 13 . 17 . 17 . 29 . 89 . 109 . 149 . 157 . 173
599832943	5 . 5 . 5 . 5 . 13 . 17 . 29 . 37 . 37 . 41 . 73 97 . 113
830426722	5 . 13 . 13 . 61 . 97 . 149 . 157 . 173 . 173 . 197
1112115023	5 . 17 . 17 . 61 . 73 . 113 . 157 . 173 . 173 . 181
1282794079	13 . 17 . 29 . 29 . 73 . 89 . 97 . 113 . 181 . 197 . 197

2189376182	5 . 5 . 5 . 17 . 17 . 29 . 29 . 53 . 61 . 61 . 89 . 89 . 101
2971354082	5 . 5 . 13 . 17 . 29 . 41 . 53 . 53 . 113 . 149 . 157 . 181
3955080927	5 . 13 . 17 . 17 . 17 . 17 . 53 . 53 . 61 . 61 . 101 . 149 . 173 . 197
8193535810	13 . 13 . 29 . 29 . 61 . 109 . 109 . 137 . 157 . 157 . 193
14033378718	5 . 5 . 13 . 13 . 17 . 17 . 61 . 61 . 61 . 61 . 73 . 73 . 157 . 181

5	2. 3. 7
13	5. 8. 18. 57. 239
17	4. 13. 21. 38. 47. 268
29	12. 17. 41. 70. 99. 157. 307
37	6. 31. 43. 68. 117. 191. 302. 327. 882. 18543*
41	9. 32. 73. 132. 278. 378. 829. 993. 2943
53	23. 30. 83. 182. 242. 401. 447. 606. 931. 1143*. 1772. 6118. 34208. 44179. 85353. 485298
61	11. 50. 72. 133. 255. 438. 682. 2673. 2917. 4747*. 4952. 5257. 9466. 12943. 17557. 114669. 330182
73	27. 46. 173. 265. 319. 538. 557. 684. 1068. 1560*. 2163. 2309. 2436. 3039. 5667. 8368. 14773. 48737. 72662. 478707*
89	34. 55. 123. 233. 411. 500. 568. 746. 1568. 1636*. 3793. 4217. 4594. 4662. 6107. 11981. 19703. 24263. 32807. 37770*. 45068. 51387. 99557. 157318. 260359. 24208144
97	22. 75. 119. 172. 216. 463. 507. 560. 657. 1433*. 1918. 2059. 2738. 4193. 4246. 5357. 5507. 5648. 6962. 9193*. 9872. 17923. 21124. 29757. 30383. 39307. 41688. 112595. 320078. 390112*. 617427. 1984933. 2343692. 3449051. 6225244
101	10. 91. 111. 192. 212. 293. 313. 394. 515. 616*. 697. 798. 818. 1303. 2818. 3141. 3323. 8393. 17766. 36673*. 66347. 71700. 74043. 173932. 177144. 508929. 683982. 1635786. 2478328. 2809305*. 3014557. 6367252. 18975991. 193788912. 201229582. 2189376182
109	33. 76. 142. 251. 294. 360. 512. 621. 905. 948*. 1057. 1123. 1929. 2801. 3521. 3957. 5701. 6943. 8578. 9298*. 15075. 32406. 39818. 40188. 51917. 86143. 88868. 106242. 160590. 161832*. 219602. 389163. 464307. 607533. 1083493. 1143007. 2298668. 5033696. 168623905. 284862638*
113	15. 98. 128. 437. 693. 776. 919. 1032. 1341. 1567*. 1597. 3149. 3405. 4535. 6682. 6908. 7443. 7782. 9703. 12332*. 13545. 14140. 17191. 19534. 21907. 34367. 43633. 57532. 67333. 136293*. 191407. 286018. 411787. 520463. 566793. 567923. 1528649. 1615463. 1824257. 2277387*. 2457057. 3801448. 7691443. 599832943
137	37. 100. 174. 237. 922. 1407. 1607. 1955. 2018. 4484*. 5928. 7161. 9901. 10312. 11471. 13252. 19902. 22231. 28322. 30103*. 40517. 49083. 51412. 52571. 68463. 90657. 93197. 101343. 109637. 117372*. 145046. 210943. 228068. 256638. 494607. 500150. 721068. 899168. 1477034. 3370434*. 4079486. 9639557

149	44. 105. 193. 403. 701. 1087. 1148. 1744. 1832. 1893*. 5767. 6065. 6898. 9133. 10833. 14646. 18432. 19326. 20457. 22157*. 24331. 25523. 28205. 28862. 32973. 37057. 39082. 42658. 80802. 83247*. 84141. 93020. 128482. 143382. 145231. 189782. 191807. 208048. 262433. 307939*. 309070. 409557. 447342. 534568. 571459. 700107. 1010027. 2379723. 2680168. 6151956*. 6656382. 9689961. 32944452. 58305593
157	28. 129. 185. 342. 443. 499. 757. 1228. 1385. 2013*. 2540. 2697. 3112. 3583. 3740. 4581. 5052. 6252. 7093. 14573*. 16513. 19653. 22008. 25462. 38807. 41319. 43932. 54193. 67852. 71564*. 78629. 88733. 117251. 129553. 180107. 184133. 210195. 211765. 249503. 263317*. 267657. 703175. 780262. 812447. 1131527. 1413443. 1618855. 1664957. 1954207. 2923783*. 3139557. 3272693. 4218932. 4466678. 4773557. 5982670. 6315768. 9548768. 15165443. 160007778*. 299252491
173	80. 93. 253. 599. 772. 785. 945. 1118. 1477. 1823*. 3207. 4232. 5283. 5443. 5962. 8224. 12882. 13068. 13241. 18258*. 19283. 21705. 31752. 32258. 46444. 46617. 48187. 51115. 81749. 89361*. 102163. 136404. 159772. 174118. 194718. 201106. 251103. 281897. 322392. 383807*. 518734. 627391. 1000193. 1024240. 1068182. 1351742. 1750507. 1766693. 2353918. 2733307*. 3136570. 3815076. 4650839. 9614382. 10328193. 11131086. 12514913. 12750353. 14698000. 16317267*. 23747457. 24310918. 53365057. 75505943. 111530944. 327012132
181	19. 162. 200. 343. 524. 743. 924. 1067. 1467. 2010*. 2191. 2515. 3458. 3782. 5087. 8307. 9431. 10298. 13918. 14318*. 24778. 25683. 27493. 35857. 37448. 44507. 47403. 112782. 117307. 148582*. 155317. 157308. 162014. 181343. 181743. 190393. 216676. 221382. 287228. 289038*. 298307. 331068. 385692. 538275. 548630. 783568. 848871. 936513. 1059193. 1067157*. 1139557. 2471717. 2475918. 2484968. 2959007. 3800438. 3931663. 4000300. 7620662. 8082212*. 8571779. 12477035. 15986092. 20198495. 24280807. 34602875. 167207057. 211823957. 1112115023. 2971354082*. 14033378718
193	81. 112. 467. 660. 853. 1239. 1270. 1432. 1818. 2042*. 2428. 2621. 3362. 4327. 4906. 4937. 6481. 9152. 9762. 12433*. 13043. 14942. 24816. 25943. 30027. 28326. 45050. 47783. 54507. 75382*. 80593. 81141. 83071. 88668. 88699. 89471. 137883. 141743. 236151. 263557*. 265842. 444753. 606385. 623888. 662843. 672717. 793921. 907567. 1306143. 1373307*. 1387203. 1518057. 1909461. 2036069. 2050706. 2052057. 2126007. 3025001. 3911450. 6356150*. 6817837. 9407318. 121042733. 185507821. 8193535810
197	14. 183. 211. 408. 577. 999. 1196. 1393. 1984. 2153*. 2350. 2547. 3166. 3532. 4545. 7697. 8457. 9667. 11018. 14958*. 16928. 19123. 19911. 20080. 25793. 26018. 32885. 33307. 40568. 41187*. 42932. 44733. 50052. 54358. 90212. 99893. 104818. 133749. 137719. 148158*. 150522. 232643. 247643. 292362. 403639. 418048. 465525. 465694. 586455. 704683*. 791532. 832902. 911111. 1031675. 1049433. 1089593. 1197943. 1264557. 1402232. 3637197*. 3894873. 4697282. 4751232. 6208047. 6829610. 6981694. 7138478. 8809432. 10669731. 18378313*. 22866693. 31011557. 34436768. 45500682. 95665578. 317742693. 830426722. 1282794079. 3955080927

Factorable $aa + 4$.

1	5	3	13
5	29	7	53
9	5 . 17	11	5 . 5 . 5
13	173	19	5 . 73
21	5 . 89	23	13 . 41
25	17 . 37	29	5 . 13 . 13
31	5 . 193	39	5 . 5 . 61
43	17 . 109	49	5 . 13 . 37
53	29 . 97	59	5 . 17 . 41
61	5 . 5 . 149	63	29 . 137
81	5 . 13 . 101	83	61 . 113
99	5 . 37 . 53	101	5 . 13 . 157
111	5 . 5 . 17 . 29	121	5 . 29 . 101
127	13 . 17 . 73	141	5 . 41 . 97
143	113 . 181	161	5 . 5 . 17 . 61
169	5 . 29 . 197	179	5 . 13 . 17 . 29
199	5 . 89 . 89	205	13 . 53 . 61
211	5 . 5 . 13 . 137	213	17 . 17 . 157
219	5 . 53 . 181	237	13 . 29 . 149
247	17 . 37 . 97	261	5 . 5 . 5 . 5 . 109
283	13 . 61 . 101	309	5 . 13 . 13 . 113
311	5 . 5 . 53 . 73	335	13 . 89 . 97
359	5 . 149 . 173	393	13 . 109 . 109
417	17 . 53 . 193	419	5 . 13 . 37 . 73
469	5 . 29 . 37 . 41	485	17 . 101 . 137
527	29 . 61 . 157	535	17 . 113 . 149
611	5 . 5 . 109 . 137	679	5 . 13 . 41 . 173
691	5 . 29 . 37 . 89	705	13 . 13 . 17 . 173
749	5 . 29 . 53 . 73	759	5 . 29 . 29 . 137
761	5 . 5 . 5 . 41 . 113	829	5 . 13 . 97 . 109
841	5 . 17 . 53 . 157	943	17 . 17 . 17 . 181
961	5 . 5 . 17 . 41 . 53	1011	5 . 5 . 5 . 13 . 17 . 37
1043	13 . 13 . 41 . 157	1047	89 . 109 . 113
1089	5 . 5 . 13 . 41 . 89	1131	5 . 17 . 101 . 149
1159	5 . 37 . 53 . 137	1305	97 . 97 . 181
1351	5 . 17 . 109 . 197	1371	5 . 41 . 53 . 173
1381	5 . 13 . 13 . 37 . 61	1499	5 . 41 . 97 . 113
1581	5 . 41 . 89 . 137	1745	13 . 29 . 41 . 197
1801	5 . 37 . 89 . 197	1899	5 . 37 . 101 . 193
2025	13 . 29 . 73 . 149	2343	13 . 37 . 101 . 113
2355	17 . 41 . 73 . 109	2441	5 . 13 . 29 . 29 . 109

2677	17 . 17 . 137 . 181
3039	5 . 5 . 13 . 157 . 181
3339	5 . 5 . 41 . 73 . 149

3351	5 . 13 . 13 . 97 . 137
3377	13 . 61 . 73 . 197
3717	29 . 53 . 89 . 101
3749	5 . 17 . 37 . 41 . 109
4021	5 . 17 . 37 . 53 . 97
4123	17 . 29 . 29 . 29 . 41
4215	13 . 73 . 97 . 113
4761	5 . 5 . 5 . 13 . 13 . 29 . 37
4989	5 . 5 . 5 . 13 . 17 . 17 . 53
5041	5 . 13 . 13 . 17 . 29 . 61
5567	13 . 17 . 17 . 73 . 113
5573	29 . 61 . 97 . 181
5717	13 . 13 . 41 . 53 . 89
5821	5 . 13 . 37 . 73 . 193
6061	5 . 5 . 13 . 17 . 61 . 109
6261	5 . 5 . 5 . 53 . 61 . 97
6989	5 . 5 . 5 . 53 . 73 . 101
7319	5 . 17 . 73 . 89 . 97
7745	13 . 13 . 37 . 53 . 181
8049	5 . 17 . 53 . 73 . 197
8579	5 . 29 . 53 . 61 . 157
8879	5 . 29 . 41 . 89 . 149
9801	5 . 17 . 73 . 113 . 137
9817	17 . 37 . 37 . 41 . 101
9947	73 . 89 . 97 . 157
10039	5 . 5 . 13 . 17 . 17 . 29 . 37
12383	37 . 109 . 193 . 197
12605	17 . 37 . 41 . 61 . 101
12815	13 . 13 . 41 . 137 . 173
13251	5 . 17 . 101 . 113 . 181
13489	5 . 5 . 5 . 5 . 5 . 5 . 5 . 17 . 137
13507	17 . 17 . 41 . 89 . 173
14261	5 . 5 . 5 . 89 . 101 . 181
14901	5 . 13 . 13 . 13 . 17 . 29 . 41
16041	5 . 73 . 89 . 89 . 89
20511	5 . 5 . 5 . 13 . 17 . 97 . 157
20769	5 . 29 . 37 . 37 . 41 . 53
20875	13 . 29 . 53 . 113 . 193
21139	5 . 5 . 17 . 37 . 157 . 181
21161	5 . 5 . 13 . 89 . 113 . 137
21189	5 . 5 . 37 . 61 . 73 . 109
22805	13 . 17 . 89 . 137 . 193
23311	5 . 5 . 29 . 41 . 101 . 181
23901	5 . 29 . 137 . 149 . 193
23915	13 . 29 . 73 . 113 . 173
25689	5 . 5 . 29 . 41 . 149 . 149
27355	13 . 37 . 53 . 149 . 197
27411	5 . 5 . 41 . 61 . 61 . 197

27429	5 . 17 . 29 . 37 . 73 . 113
27611	5 . 5 . 41 . 61 . 89 . 137
29169	5 . 13 . 29 . 41 . 101 . 109
29691	5 . 17 . 17 . 29 . 109 . 193
29929	5 . 13 . 17 . 61 . 97 . 137
31351	5 . 37 . 149 . 181 . 197
32003	13 . 17 . 17 . 41 . 61 . 109
32139	5 . 5 . 13 . 17 . 73 . 197
32239	5 . 5 . 5 . 5 . 5 . 37 . 89 . 101
37579	5 . 17 . 29 . 41 . 89 . 157
44301	5 . 13 . 37 . 53 . 89 . 173.
47389	5 . 5 . 53 . 97 . 101 . 173
47761	5 . 5 . 5 . 5 . 17 . 17 . 73 . 173
47829	5 . 17 . 37 . 41 . 113 . 157
49813	13 . 53 . 101 . 181 . 197
57989	5 . 5 . 5 . 53 . 53 . 61 . 157
63911	5 . 5 . 13 . 13 . 17 . 29 . 37 . 53
66361	5 . 5 . 41 . 113 . 193 . 197
79011	5 . 5 . 5 . 5 . 13 . 89 . 89 . 97
79871	5 . 29 . 37 . 61 . 101 . 193
81487	13 . 13 . 73 . 73 . 73 . 101
81669	5 . 13 . 29 . 113 . 173 . 181
86487	17 . 17 . 41 . 41 . 89 . 173
91587	17 . 29 . 29 . 37 . 101 . 157
95963	13 . 13 . 41 . 89 . 109 . 137
99011	5 . 5 . 5 . 5 . 5 . 13 . 29 . 53 . 157
99407	17 . 29 . 37 . 41 . 73 . 181
108111	5 . 5 . 13 . 17 . 97 . 113 . 193
110211	5 . 5 . 13 . 37 . 73 . 101 . 137
114611	5 . 5 . 13 . 13 . 89 . 181 . 193
115983	13 . 17 . 37 . 61 . 149 . 181
117281	5 . 29 . 61 . 89 . 101 . 173
128359	5 . 13 . 17 . 29 . 53 . 89 . 109
139701	5 . 13 . 53 . 149 . 193 . 197
140489	5 . 5 . 5 . 41 . 113 . 173 . 197
140871	5 . 13 . 17 . 37 . 61 . 73 . 109
142047	29 . 29 . 41 . 53 . 61 . 181
148939	5 . 5 . 29 . 29 . 73 . 97 . 149
183739	5 . 5 . 5 . 13 . 29 41 . 101 . 173
191279	5 . 13 . 13 . 29 . 73 . 113 . 181
203091	5 . 17 . 17 . 41 . 61 . 101 . 113
205111	5 . 5 . 13 . 73 . 97 . 101 . 181
206707	29 . 37 . 53 . 61 . 109 . 113
207171	5 . 13 . 17 . 29 . 89 . 101 . 149
211221	5 . 13 . 13 . 37 . 61 . 149 . 157
228179	5 . 13 . 13 . 61 . 73 . 101 . 137
234333	37 . 37 . 37 . 41 . 137 . 193
234881	5 . 13 . 13 . 17 . 17 . 17 . 97 . 137

241511	5 . 5 . 5 . 5 . 13 . 17 . 37 . 101 . 113
244299	5 . 13 . 17 . 37 . 97 . 101 . 149
245293	109 . 113 . 137 . 181 . 197
247699	5 . 13 . 17 . 41 . 61 . 149 . 149
257665	13 . 17 . 101 . 109 . 157 . 173
263489	5 . 5 . 5 . 5 . 5 . 5 . 29 . 37 . 41 . 101
269459	5 . 17 . 37 . 37 . 53 . 61 . 193
289589	5 . 5 . 29 . 61 . 97 . 113 . 173
302111	5 . 5 . 41 . 61 . 97 . 101 . 149
306757	17 . 29 . 53 . 101 . 181 . 197
313489	5 . 5 . 5 . 5 . 5 . 5 . 17 . 17 . 17 . 37 . 173
317039	5 . 5 . 53 . 61 . 89 . 89 . 157
326957	37 . 37 . 41 . 101 . 109 . 173
349835	17 . 41 . 73 . 97 . 137 . 181
355989	5 . 5 . 5 . 5 . 13 . 17 . 37 . 137 . 181
387921	5 . 61 . 101 . 137 . 181 . 197
396783	13 . 13 . 29 . 61 . 61 . 89 . 97
408489	5 . 5 . 5 . 5 . 13 . 29 . 73 . 89 . 109
466489	5 . 5 . 5 . 13 . 17 . 29 . 61 . 61 . 73
563235	13 . 17 . 41 . 61 . 61 . 97 . 97
567629	5 . 13 . 37 . 73 . 109 . 113 . 149
582997	37 . 41 . 73 . 113 . 157 . 173
588489	5 . 5 . 5 . 5 5 . 61 . 89 . 137 . 149
628261	5 . 5 . 5 . 13 . 17 . 29 . 41 . 61 . 197
634205	37 . 53 . 73 . 109 . 149 . 173
637855	13 . 37 . 41 . 41 . 61 . 73 . 113
834267	17 . 17 . 17 . 29 . 137 . 181 . 197
840421	5 . 13 . 17 . 137 . 149 . 173 . 181
851929	5 . 17 . 53 . 73 . 89 . 137 . 181
922769	5 . 13 . 13 . 17 . 41 . 61 . 137 . 173
966391	5 . 13 . 17 . 29 29 . 37 . 157 . 173
1029353	61 . 61 . 89 . 109 . 149 . 197
1165689	5 . 5 . 29 . 41 . 41 . 53 . 109 . 193
1230349	5 . 13 . 13 . 17 . 17 . 29 . 37 . 53 . 109
1299241	5 . 13 . 13 . 37 . 89 . 89 . 173 . 197
1341429	5 . 29 . 61 . 73 . 89 . 173 . 181
1362611	5 . 5 . 13 37 . 89 . 89 . 101 . 193
1493911	5 . 5 . 13 . 29 . 101 . 109 . 137 . 157
1499001	5 . 13 . 13 . 17 . 73 . 73 . 149 . 197
1780489	5 . 5 . 5 . 29 . 37 . 41 . 53 . 73 . 149
1996199	5 . 13 . 13 . 17 . 17 . 37 . 53 53 . 157
2028211	5 . 5 . 13 . 17 . 41 . 41 . 53 . 61 . 137
2050005	17 . 29 . 61 . 73 . 89 . 137 . 157
2159739	5 . 5 . 5 . 5 . 13 . 17 . 37 . 41 . 113 . 197
3376311	5 . 5 . 13 . 13 . 13 . 17 . 17 . 61 . 61 . 193
3666653	13 . 13 . 17 . 41 . 53 . 97 . 149 . 149
3872099	5 . 13 . 13 . 17 . 37 . 41 . 41 . 97 . 173
4370811	5 . 5 . 13 . 17 . 53 . 61 . 89 . 197

4490249	5 . 13 . 29 . 61 . 73 . 89 . 137 . 197
4705711	5 . 5 . 13 . 17 . 17 . 17 . 17 . 41 . 101 . 197
5125339	5 . 5 . 17 . 17 . 29 . 37 . 97 . 181 . 193
5472411	5 . 5 . 17 . 29 . 41 . 41 . 89 . 109 . 149
6101547	13 . 13 . 13 . 17 . 29 . 37 . 61 . 97 . 157
6489011	5 . 5 . 5 . 5 . 17 . 37 . 41 . 89 . 149 . 197
8175989	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 97 . 149 . 181
8649761	5 . 5 . 5 . 13 . 17 . 37 . 61 . 101 . 109 . 109
8812979	5 . 17 . 17 . 17 . 29 . 73 . 89 . 97 . 173
9530277	13 . 13 . 17 . 17 . 17 . 73 . 89 . 113 . 149
10126399	5 . 13 . 17 . 29 . 29 . 53 . 89 . 149 . 157
10251621	5 . 13 . 17 . 17 29 . 61 . 101 . 173 . 181
10763489	5 . 5 . 5 . 5 . 5 . 5 . 61 . 61 . 101 . 109 . 181
10831321	5 . 17 . 29 . 29 . 41 . 61 . 73 . 89 . 101
11398611	5 . 5 . 13 . 17 . 53 . 97 . 137 . 173 . 193
11483821	5 . 29 . 53 . 61 . 101 . 113 . 157 . 157
15035789	5 . 5 . 37 . 41 . 41 . 53 . 101 . 157 . 173
17363031	5 . 13 . 13 . 41 . 73 . 89 . 89 . 101 . 149

23866411	5 . 5 . 13 . 17 . 17 . 17 . 61 . 157 . 193 . 193
25252451	5 . 13 . 29 . 37 . 41 . 97 . 97 . 137 . 173
31456571	5 . 13 . 17 . 41 . 97 . 101 . 109 . 113 . 181
34411159	5 . 13 . 37 . 41 . 61 . 73 . 89 . 157 . 193
35272357	13 . 13 . 13 . 13 . 17 . 29 . 61 . 97 . 101 . 137
35944451	5 . 13 . 17 . 17 . 17 . 29 . 73 . 89 109 . 197
61017271	13 . 13 . 13 . 17 . 29 . 37 . 61 . 97 . 157
107402539	5 . 5 . 13 . 29 . 37 . 61 . 109 . 149 . 173 . 193
143828743	29 . 29 . 37 . 37 . 53 . 97 . 113 . 157 . 197
148757489	5 . 5 . 5 . 13 . 13 . 17 . 37 . 41 . 41 . 61 . 109 . 149
150446761	5 . 5 . 5 . 13 . 17 . 37 . 53 . 113 . 137 . 137 . 197
322564791	5 . 13 . 17 . 29 . 29 . 29 . 37 . 53 . 101 . 101 . 193
657182319	5 . 17 . 17 . 61 . 97 . 97 . 113 . 149 . 157 . 197
1359685525	13 . 17 . 53 . 61 . 61 . 97 . 113 . 157 . 157 . 157
4949475989	5 . 5 . 5 . 5 . 5 . 13 . 13 . 29 . 29 . 37 . 37 . 41 . 61 . 89 . 181
28608252345	13 . 29 . 29 . 29 . 37 . 53 . 61 . 73 . 97 . 113 . 149 . 181
112899039159	5 . 13 . 13 . 17 . 17 . 17 . 17 . 29 . 37 . 41 . 61 . 73 . 73 . 73 . 173

5	1. 11
13	3. 29
17	9
29	5. 111. 179
37	25. 49. 1011. 4761. 10039
41	23. 59. 469. 4123. 14901
53	7. 99. 961. 4989. 20769. 63911
61	39. 61. 205. 1381. 5041

73	19. 127. 311. 419. 749. 466489
89	21. 199. 691. 1089. 5717. 16041
97	53. 141. 247. 335. 4021. 6261. 7319. 79011. 396783. 563235*
101	81. 121. 283. 3717. 6989. 9817. 12605. 32239. 81487. 263489*. 10831321
109	43. 261. 393. 829. 2355. 2441. 3749. 6061. 21189. 29169*. 32003. 128359. 140871. 408489. 1230349. 8649761
113	83. 309. 761. 1047. 1499. 2343. 5567. 27429. 203091. 206707*. 244299. 637855
137	63. 211. 485. 611. 759. 1159. 1581. 3351. 9801. 13489*. 21161. 27611. 29929. 95963. 110211. 228179. 234881. 2028211. 35272357
149	61. 237. 535. 1131. 2025. 3339. 8879. 25689. 148939. 207171*. 244299. 247699. 302111. 567629. 588489. 1780489. 3666653. 5472411. 9530277. 17363031*. 148757489
157	101. 213. 527. 841. 1043. 8579. 9947. 20511. 37579. 47829*. 57989. 91587. 99011. 211221. 317039. 1493911. 1996199. 2050005. 6101547. 10126399*. 11483821. 61017271. 1359685525
173	13. 359. 679. 705. 1371. 12815. 13507. 23915. 44301. 47389*. 47761. 86487. 117281. 183739. 257665. 289589. 313489. 326957. 582997. 634205*. 922769. 966391. 3872099. 8812979. 15035789. 25252451. 112899039159
181	143. 219. 943. 1305. 2677. 3039. 5573. 7745. 13251. 14261*. 21139. 23311. 81669. 99407. 115983. 142047. 191279. 205111. 349835. 355989*. 840421. 851929. 1341429. 8175989. 10251621. 10763489. 31456571. 4949475989. 28608252345
193	31. 417. 1899. 4215. 5821. 20875. 22805. 23901. 29691. 79871*. 108111. 114611. 234333. 269459. 1165689. 1362611. 3376311. 5125339. 11398611. 23866411*. 34411159. 107402539. 322564791
197	169. 1351. 1745. 1801. 3377. 8049. 12383. 27355. 27411. 31351*. 32139. 49813. 66361. 139701. 140489. 245293. 306757. 387921. 628261. 834267*. 1029353. 1299241. 1499001. 2159739. 4370811. 4490249. 4705711. 6489011. 35944451. 143828743*. 150446761. 657182319

Factorable $aa + 9$

1	5	2	13
4	5 . 5	5	17
7	29	8	73
10	109	11	5 . 13
13	89	14	5 . 41
16	5 . 53	17	149
19	5 . 37	22	17 . 29
26	5 . 137	28	13 . 61
29	5 . 5 . 17	31	5 . 97
37	13 . 53	41	5 . 13 . 13
46	5 . 5 . 5 . 17	50	13 . 193
55	37 . 41	56	5 . 17 . 37
65	29 . 73	67	13 . 173
68	41 . 113	71	5 . 5 . 101
73	17 . 157	76	5 . 13 . 89

79	5 . 5 . 5 . 5 . 5	80	13 . 17 . 29
89	5 . 13 . 61	94	5 . 29 . 61
106	5 . 13 . 173	109	5 . 29 . 41
119	5 . 13 . 109	124	5 . 17 . 181
128	13 . 13 . 97	131	5 . 17 . 101
143	53 . 193	154	5 . 5 . 13 . 73
155	61 . 197	158	13 . 17 . 113
163	97 . 137	166	5 . 37 . 149
167	13 . 29 . 37	175	17 . 17 . 53
181	5 . 29 . 113	191	5 . 41 . 89
196	5 . 5 . 29 . 53	211	5 . 61 . 73
232	13 . 41 . 101	239	5 . 29 . 197
241	5 . 37 . 157	254	5 . 5 . 29 . 89
271	5 . 5 . 13 . 113	281	5 . 53 . 149
284	5 . 13 . 17 . 73	301	5 . 13 . 17 . 41
314	5 . 13 . 37 . 41	352	17 . 37 . 197
379	5 . 5 . 13 . 13 . 17	413	17 . 29 . 173
419	5 . 97 . 181	430	17 . 73 . 149
436	5 . 193 . 197	437	17 . 41 . 137
446	5 . 5 . 73 . 109	454	5 . 5 . 5 . 17 . 97
464	5 . 17 . 17 . 149	521	5 . 5 . 61 . 89
529	5 . 5 . 29 . 193	535	13 . 101 . 109
544	5 . 13 . 29 . 157	547	41 . 41 . 89
574	5 . 13 . 37 . 137	610	37 . 89 . 113
629	5 . 5 . 41 . 193	704	5 . 5 . 5 . 5 . 13 . 61
722	37 . 73 . 193	746	5 . 5 . 113 . 197
796	5 . 5 . 5 . 37 . 137	811	5 . 17 . 53 . 73
821	5 . 5 . 13 . 17 . 61	848	29 . 137 . 181
869	5 . 13 . 37 . 157	943	37 . 61 . 197
971	5 . 5 . 109 . 173	991	5 . 17 . 53 . 109
1015	17 . 157 . 193	1042	13 . 17 . 17 . 17 . 17
1055	13 . 13, 37 . 89	1070	61 . 137 . 137
1081	5 . 13 . 89 . 101	1129	5 . 5 . 13 . 37 . 53

1144	5 . 17 . 89 . 173
1175	41 . 113 . 149
1259	5 . 13 . 89 . 137
1298	13 . 29 . 41 . 109
1309	5 . 53 . 53 . 61
1324	5 . 13 . 149 . 181
1421	5 . 5 . 5 . 41 . 197
1559	5 . 17 . 17 . 29 . 29
1618	97 . 137 . 197
1627	13 . 17 . 53 . 113
1646	5 . 5 . 29 . 37 . 101
1675	13 . 29 . 61 . 61
1687	73 . 101 . 193

1805	13 . 29 . 29 . 149
1831	5 . 13 . 17 . 37 . 41
1909	5 . 13 . 17 . 17 . 97
1979	5 . 5 . 29 . 37 . 73
2069	5 . 13 . 13 . 17 . 149
2182	13 . 29 . 73 . 173
2351	5 . 13 . 17 . 41 . 61
2528	17 . 41 . 53 . 173
2596	5 . 5 . 17 . 101 . 257
2719	5 . 13 . 29 . 37 . 53
2839	5 . 61 . 73 . 181
2953	13 . 17 . 109 . 181
3038	17 . 29 . 97 . 193
3089	5 . 17 . 37 . 37 . 41
3458	29 . 41 . 89 . 113
3496	5 . 5 . 37 . 73 . 181
3571	5 . 5 . 37 . 61 . 113
3677	13 . 13 . 13 . 17 . 181
4136	5 . 13 . 17 . 113 . 137
4171	5 . 5 . 5 . 13 . 53 . 101
4196	5 . 5 . 41 . 89 . 193
4237	37 . 41 . 61 . 97
4459	5 . 17 . 29 . 37 . 109
4489	5 . 53 . 193 . 197
4496	5 . 5 . 13 . 37 . 41 . 41
4565	13 41 . 113 . 173
4786	5 . 13 . 53 . 61 . 109
5029	5 . 5 . 13 . 13 . 41 . 73
5111	5 . 13 . 13 . 13 . 29 . 41
5125	37 . 37 . 53 . 181
5198	13 . 13 . 29 . 37 . 149
5401	5 . 17 . 29 . 61 . 97
5549	5 . 13 . 41 . 53 . 109
5579	5 . 5 . 5 . 13 . 61 . 157
5605	13 . 17 . 17 . 37 . 113
5921	5 . 5 . 5 . 17 . 73 . 113
6329	5 . 5 . 5 . 5 . 5 . 13 . 17 . 29
6346	5 . 5 . 13 . 17 . 37 . 197
6421	5 . 5 . 5 . 17 . 89 . 109
6494	5 . 37 . 37 . 61 . 101
6641	5 . 13 . 37 . 53 . 173
6821	5 . 5 . 53 . 97 . 181
7196	5 . 5 . 17 . 37 . 37 . 89
7271	5 . 5 . 17 . 37 . 41 . 41
7489	5 . 29 . 41 . 53 . 89
7616	5 . 13 . 53 . 113 . 149
7646	5 . 5 . 13 . 13 . 101 . 137
7729	5 . 5 . 97 . 109 . 113

7934	5 . 17 . 53 . 89 . 157
9650	29 . 113 . 157 . 181
10012	13 . 13 . 29 . 113 . 181
10154	5 . 5 . 17 . 41 . 61 . 97
10447	29 . 73 . 149 . 173
10736	5 . 13 . 97 . 101 . 181
11074	5 . 13 . 61 . 157 . 197
11671	5 . 5 . 5 . 41 . 97 . 137
12109	5 . 17 . 41 . 109 . 193
12191	5 . 37 . 41 . 97 . 101
13561	5 . 13 . 13 . 17 . 37 . 173
14029	5 . 5 . 13 . 29 . 53 . 197
15004	5 . 5 . 13 . 37 . 97 . 193
16096	5 . 5 . 13 . 13 . 13 . 53 . 89
16291	5 . 13 . 17 . 29 . 41 . 101
17029	5 . 5 . 17 . 41 . 53 . 157
17357	13 . 41 . 41 . 61 . 113
17668	17 . 29 . 37 . 109 . 157
18671	5 . 5 . 5 . 5 . 5 . 17 . 17 . 193
19504	5 . 5 . 17 . 89 . 89 . 113
20651	5 . 61 . 61 . 73 . 157
20813	17 . 37 . 53 . 73 . 89
22085	13 . 41 . 53 . 89 . 97
22367	17 . 17 . 37 . 149 . 157
22700	13 . 17 . 29 . 37 . 41 . 53
23425	29 . 29 . 41 . 73 . 109
23671	5 . 5 . 5 . 5 . 13 . 29 . 29 . 41
23879	5 . 5 . 13 . 61 . 73 . 197
24001	5 . 61 . 61 . 113 . 137
24311	5 . 53 . 61 . 101 . 181
25645	89 . 137 . 149 . 181
26141	5 . 13 . 17 . 37 . 61 . 137
27341	5 . 13 . 17 . 17 . 101 . 197
27731	5 . 13 . 29 . 37 . 37 . 149
27805	13 . 37 . 73 . 101 . 109
27844	5 . 13 . 13 . 13 . 13 . 61 . 89
28804	5 . 5 . 29 . 37 . 157 . 197
28973	17 . 41 . 73 . 73 . 113
30544	5 . 17 . 29 . 37 . 53 . 193
33629	5 . 5 . 13 . 89 . 113 . 173
34010	13 . 13 . 29 . 53 . 61 . 73
38608	13 . 41 . 137 . 137 . 149
39704	5 . 5 . 5 . 13 . 73 . 97 . 137
40030	17 . 41 . 97 . 137 . 173
40304	5 . 5 . 73 . 73 . 89 . 137
42173	29 . 29 . 89 . 109 . 109
42421	5 . 5 . 5 . 5 . 13 . 37 . 41 . 73
43864	5 . 13 . 37 . 89 . 89 . 101

47296	5 . 5 . 5 . 13 . 73 . 109 . 173
47335	13 . 29 . 89 . 173 . 193
48046	5 . 5 . 5 . 5 . 13 . 29 . 97 . 101
48829	5 . 5 . 5 . 5 . 17 . 29 . 53 . 73
49883	13 . 17 . 17 . 41 . 41 . 197
49924	5 . 17 . 41 . 73 . 97 . 101
54871	5 . 5 . 13 . 17 . 53 . 53 . 97
54926	5 . 37 . 41 . 41 . 89 . 109
55709	5 . 97 . 109 . 149 . 197
57701	5 . 37 . 41 . 41 . 53 . 101
57839	5 . 13 . 13 . 13 . 13 . 13 . 17 . 53
62402	13 . 13 . 17 . 89 . 97 . 157
66584	5 . 13 . 17 . 17 . 53 61 . 73
70171	5 . 5 . 5 . 17 . 37 . 173 . 181
71021	5 . 5 . 13 . 13 . 13 . 17 . 37 . 73
71276	5 . 17 . 61 . 89 . 101 . 109
71354	5 . 5 . 17 . 37 . 41 . 53 . 149
73972	13 . 17 . 29 . 53 . 89 . 181
78829	5 . 5 . 5 . 5 . 29 . 37 . 41 . 113
79051	5 . 13 . 13 . 37 . 37 . 37 . 73
84563	13 . 17 . 17 . 17 . 17 . 37 . 89
84818	17 . 29 . 29 . 61 . 73 . 113
86221	5 . 5 . 61 . 73 . 173 . 193
88411	5 . 13 . 37 . 73 . 113 . 197
95071	5 . 5 . 13 . 37 . 61 . 61 . 101
95188	13 . 13 . 13 . 17 . 41 . 61 . 97
105274	5 . 41 . 53 . 73 . 89 . 157
109279	5 . 5 . 29 . 37 . 41 . 61 . 89
109991	5 . 13 . 53 . 89 . 109 . 181
112171	5 . 5 . 5 . 17 . 109 . 157 . 173
114499	5 . 29 . 29 . 41 . 193 . 197
114896	5 . 5 . 13 . 41 . 61 . 109 . 149
115079	5 . 5 . 5 . 5 . 29 . 53 . 61 . 113
116881	5 . 13 . 53 . 73 . 157 . 173
127114	5 . 17 . 29 . 29 . 37 . 41 . 149
133523	17 . 29 . 41 . 53 . 53 . 157
134764	5 . 17 . 97 . 101 . 113 . 193
137659	5 . 13 . 37 . 137 . 149 . 193
141581	5 . 13 . 13 . 17 . 37 109 . 173
146794	5 . 13 . 41 41 . 53 . 61 . 61
147409	5 . 13 . 13 . 41 . 53 . 61 97
154679	5 . 5 . 29 . 37 . 41 . 73 . 149
154729	5 . 5 . 17 . 17 . 61 . 157 . 173
157454	5 . 5 . 5 . 13 . 37 . 41 . 89 . 113
167689	5 . 13 . 13 . 13 . 73 . 89 . 197
170107	13 . 17 . 17 . 29 . 37 . 37 . 97
174427	61 . 89 . 113 . 137 . 181
178336	5 . 13 . 13 . 41 . 61 . 101 . 149

178988	17 . 37 . 37 . 73 . 109 . 173
180416	5 . 13 . 17 . 29 . 89 . 101 . 113
190021	5 . 5 . 17 . 41 . 53 . 113 . 173
190541	5 . 17 . 41 . 137 . 193 . 197
193546	5 . 5 . 5 . 13 . 13 . 97 . 101 . 181
193829	5 . 5 . 5 . 5 . 5 . 29 . 89 . 137
219754	5 . 5 . 13 . 17 . 17 . 53 . 89 . 109
249871	5 . 5 . 13 . 17 . 17 . 29 . 73 . 157
250250	37 . 41 . 53 . 61 . 113 . 113
252328	13 . 41 . 89 . 97 . 101 . 137
263681	5 . 13 . 13 . 37 . 101 . 101 . 109
265256	5 . 17 . 29 . 41 . 61 . 101 . 113
280750	13 . 13 . 17 . 61 . 61 . 73 . 101
286904	5 . 5 . 17 . 29 . 29 . 41 . 41 . 137
293687	17 . 37 . 61 . 73 . 89 . 173
311921	5 . 5 . 5 . 17 . 53 . 61 . 73 . 97
313454	5 . 5 . 5 . 13 . 13 . 13 . 13 . 13 . 29 . 73
314257	17 . 17 . 73 . 109 . 109 . 197
316739	5 . 17 . 37 . 41 . 73 . 73 . 73
324952	29 . 37 . 41 . 89 . 149 . 181
341569	5 . 17 . 29 . 29 . 53 . 89 . 173
347543	17 . 29 . 41 . 113 . 137 . 193
356809	5 . 13 . 29 . 37 . 41 . 113 . 197
377804	5 . 5 . 13 . 109 . 113 . 181 . 197
386722	13 . 29 . 109 . 109 . 173 . 193
393079	5 . 5 . 5 . 13 . 17 . 137 . 137 . 149
415825	17 . 37 . 37 . 109 . 173 . 197
419246	5 . 5 . 29 . 53 . 137 . 173 193
423475	17 . 41 . 89 . 89 . 109 . 149
448280	41 . 41 . 41 . 89 . 181 . 181
496004	5 . 5 . 13 . 17 . 37 . 41 . 149 . 197
512579	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 53 . 97
520921	5 . 5 . 5 . 13 . 53 . 97 . 109 . 149
524704	5 . 5 . 5 . 13 . 13 . 29 . 41 . 97 . 113
528967	17 . 29 . 101 . 109 . 149 . 173
539996	5 . 5 . 13 . 13 . 37 . 109 . 109 . 157
541829	5 . 5 . 5 . 13 . 17 . 29 . 41 . 41 . 109
550985	37 . 41 . 61 . 101 . 109 . 149
554279	5 . 5 . 13 . 13 . 37 . 61 . 89 . 181
599510	13 . 17 . 29 . 29 . 109 . 113 . 157
693775	17 . 17 . 17 . 41 . 97 . 109 . 113
700061	5 . 13 . 41 . 53 . 89 . 101 . 193
713291	5 . 17 . 29 . 29 . 29 . 41 . 41 . 73
744421	5 . 5 . 5 . 13 37 . 149 . 157 . 197
745249	5 . 13 . 13 . 29 . 29 . 53 . 73 . 101
792113	29 . 61 . 89 . 101 . 109 . 181
847319	5 . 17 . 37 . 73 . 101 . 113 . 137
859379	5 . 5 . 17 . 29 . 29 . 53 . 101 . 193

895208	13 . 17 . 17 . 17 . 29 . 41 . 61 . 173
895861	5 . 17 . 29 . 89 . 97 . 109 . 173
937766	5 . 13 . 17 . 29 . 41 . 53 . 73 . 173
947329	5 . 5 . 5 . 37 . 73 . 89 . 109 . 137
970454	5 . 5 . 5 . 37 . 73 . 97 . 149 . 193
984934	5 . 13 . 17 . 29 . 29 . 61 . 109 . 157
987406	5 . 17 . 53 . 73 . 101 . 149 . 197
1196173	53 . 89 . 97 . 101 . 113 . 137
1202704	5 . 5 . 5 . 17 . 17 . 37 . 61 . 113 . 157
1256084	5 . 13 . 17 . 29 . 53 . 61 . 97 . 157
1297090	13 . 29 . 37 . 41 . 109 . 137 . 197
1460288	13 . 13 . 13 . 17 . 29 . 101 . 101 . 193
1717025	13 . 29 41 . 53 . 73 . 157 . 157
1799921	5 . 5 . 5 . 5 . 5 . 17 . 29 . 37 . 157 . 181
1800254	5 . 5 . 17 . 37 . 97 . 101 . 109 . 193
2153956	5 . 17 . 101 . 101 . 157 . 173 . 197
2253046	5 . 5 . 5 . 5 . 5 . 29 . 41 . 53 . 149 . 173
2347195	17 . 29 . 41 . 53 . 137 . 137 . 137
2362579	5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 29 . 37 . 197
2382560	13 . 29 . 37 . 101 . 113 . 181 . 197
2454779	5 . 5 . 13 . 41 . 73 . 109 . 157 . 181
2473954	5 . 5 . 5 . 13 . 17 . 17 . 29 . 41 . 97 . 113
2579296	5 . 5 . 5 . 5 . 17 . 29 . 41 . 61 . 89 . 97
2710934	5 . 17 . 17 . 17 . 37 . 41 . 53 . 61 . 61
2867521	5 . 5 . 17 . 61 . 73 . 101 . 137 . 157
2960596	5 . 5 . 13 . 17 . 41 . 53 . 73 . 73 . 137
3045079	5 . 5 . 5 . 5 . 13 . 17 . 17 . 101 . 113 . 173
3287839	5 . 17 . 17 . 17 . 29 . 53 . 53 . 73 . 73
3386888	13 . 13 . 17 . 29 . 37 . 137 . 157 . 173
3569269	5 . 13 . 29 . 41 . 53 . 89 . 101 . 173
4046131	5 . 13 . 17 . 29 . 89 . 101 . 157 . 181
4546271	5 . 5 . 13 . 17 . 41 . 53 . 53 . 109 . 149
4699704	5 . 5 . 5 . 13 . 61 . 73 . 113 . 137 . 197
4889605	37 . 41 . 53 . 61 . 73 . 173 . 193
8026096	5 . 5 . 17 . 37 . 37 . 89 . 101 . 109 . 113
8182343	17 . 17 . 29 . 41 . 73 . 73 . 101 . 181
8931226	5 . 37 . 53 . 61 . 89 . 89 . 113 . 149
9237421	5 . 5 . 5 . 5 . 5 . 13 . 17 . 17 . 29 . 29 . 29 . 149
9250762	41 . 89 . 97 . 101 . 101 . 137 . 173
10419736	5 . 13 . 13 . 29 . 37 . 73 . 101 . 109 . 149
11077571	5 . 5 . 13 . 13 . 41 . 109 . 113 . 149 . 193
12519856	5 . 13 . 37 37 . 41 . 53 . 61 . 97 . 137
13237028	17 . 29 . 37 . 41 . 61 . 149 . 149 . 173
13382956	5 . 13 . 17 . 29 . 29 . 37 . 137 . 193 . 197
14937769	5 . 13 . 17 . 37 . 53 . 61 . 61 . 101 . 137
19912579	5 . 5 . 5 . 5 . 5 . 13 . 41 . 41 . 97 . 173 . 173
20620229	5 . 5 . 37 . 37 . 61 . 73 . 73 . 97 . 197
22181629	5 . 5 . 13 . 13 . 13 . 17 . 29 . 37 . 41 . 53 . 113

23504986	5 . 13 . 13 . 13 . 29 . 29 . 29 . 41 . 53 . 73
25674911	5 . 13 . 29 . 37 . 41 . 73 . 89 . 113 . 157
26999399	5 . 13 . 13 . 29 . 37 . 97 . 109 . 193 . 197
33399844	5 . 17 . 17 . 29 . 37 . 37 . 41 . 73 . 73 . 89
33753059	5 . 13 . 13 . 41 . 89 . 97 . 101 . 109 . 173
34618846	5 . 5 . 13 . 13 . 13 . 17 . 17 . 37 . 97 . 109 . 193
34792409	5 . 13 . 13 . 13 . 17 . 29 . 41 . 101 . 137 . 197
40103726	5 . 17 . 37 . 41 . 109 . 109 . 197
41494546	5 . 5 . 5 . 13 . 61 . 61 . 89 . 109 . 149 . 197
48279454	5 . 5 . 5 . 5 . 13 . 29 . 41 . 41 . 41 . 61 . 181
60740461	5 . 13 . 17 . 17 . 17 . 41 . 73 . 97 . 101 . 197
64370954	5 . 5 . 5 . 13 . 17 . 37 . 53 . 61 . 73 . 89 . 193
96499349	5 . 13 . 17 . 29 37 . 41 . 61 . 73 . 137 . 157
105742171	5 . 5 . 5 . 13 . 17 . 29 . 29 . 37 . 41 . 41 . 53 . 73
110518796	5 . 5 . 5 . 13 . 37 . 53 . 53 . 61 . 73 . 109 . 149
111009121	5 . 5 . 13 . 17 . 17 . 37 . 37 . 37 . 73 . 113 . 157
113737804	5 . 5 . 13 . 13 . 29 . 29 . 53 . 73 . 89 . 97 . 109
117290203	17 . 29 . 37 . 41 . 53 . 73 . 109 . 113 . 193
149574656	5 . 29 . 41 . 61 . 73 . 137 . 173 . 181 . 197
163030454	5 . 5 . 5 . 13 . 13 . 17 . 37 . 37 . 53 . 73 . 89 . 157
165242573	13 . 29 . 37 . 41 . 73 . 97 . 109 . 157 . 197
178643779	5 . 5 . 13 . 41 . 41 . 61 . 113 . 137 . 157 . 197
200760094	5 . 13 . 17 . 17 . 37 . 37 . 37 . 41 . 53 . 101 . 193
323643829	5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 37 . 61 . 73 . 73 . 97
401580454	5 . 5 . 5 . 13 . 53 . 61 . 73 . 73 . 97 . 137 . 137 . 193
478666540	17 . 17 . 29 . 37 . 41 . 61 . 73 . 149 . 157 . 173
1411168679	5 . 5 . 13 . 17 . 17 . 89 . 113 . 157 . 173 . 197 . 197

5	1. 4. 79
13	2. 11. 41
17	5. 29. 46. 379. 1042
29	7. 22. 80. 1559. 6329
37	19. 56. 167
41	14. 55. 109. 301. 314. 1831. 3089. 4496. 5111. 7271*. 23671
53	16. 37. 175. 196. 1129. 2719. 22700. 57839
61	28. 89. 94. 704. 821. 1309. 1675. 2351. 146794. 2710934*
73	8. 65. 154. 211. 284. 811. 1979. 5029. 34010. 42421*. 48829. 66584. 71021. 79051. 313454. 316739. 713291. 3287839. 23504986. 105742171*
89	13. 76. 191. 254. 521. 547. 1055. 7196. 7489. 16096*. 20813. 27844. 84563. 109279. 33399844
97	31. 128. 454. 1909. 4237. 5401. 10154. 22085. 54871. 95188*. 147409. 170107. 311921. 512579. 2579296. 323643829
101	71. 131. 232. 1081. 1646. 4171. 6494. 12191. 16291. 43864*. 48046. 49924. 57701. 95071. 280750. 745249
109	10. 119. 446. 535. 991. 1298. 4459. 4786. 5549. 6421*. 23425. 27805. 42173. 54926. 71276. 219754. 263681. 541829. 113737804

113	68. 158. 181. 271. 610. 1627. 3458. 3571. 5605. 5921*. 7729. 17357. 19504. 28973 78829. 84818. 115079. 157454. 180416. 250250*. 265256. 524704. 693775. 2473954. 8026096. 22181629
137	26. 163. 437. 574. 796. 1070. 1259. 4136. 7646. 11671*. 24001. 26141. 39704. 40304. 193829. 252328. 286904. 847319. 947329. 1196173*. 2347195. 2960596. 12519856. 14937769
149	17. 166. 281. 430. 464. 1175. 1805. 2069. 5198. 7616*. 27731. 38608. 71354. 114896. 127114. 154679. 178336. 393079. 423475. 520921*. 550985. 4546271. 8931226. 9237421. 10419736. 110518796
157	73. 241. 544. 869. 2596. 5579. 7934. 17029. 17668. 20651*. 22367. 62402. 105274. 133523. 249871. 539996. 599510. 984934. 1202704. 1256084*. 1717025. 2867521. 25674911. 96499349. 111009121. 163030454
173	67. 106. 413. 971. 1144. 2182. 2528. 4565. 6641. 10447*. 13561. 33629. 40030. 47296. 112171. 116881. 141581. 154729. 178988. 190021*. 293687. 341569. 528967. 895208. 895861. 937766. 2253046. 3045079. 3386888. 3569269*. 9250762. 13237028. 19912579. 33753059. 478666540
181	124. 419. 848. 1324. 2839. 2953. 3496. 3677. 5125. 6821*. 9650. 10012. 10736. 24311. 25645. 70171. 73972. 109991. 174427. 193546*. 324952. 448280. 554279. 792113. 1799921. 2454779. 4046131. 8182343. 48279454
193	50. 143. 529. 629. 722. 1015. 1687. 3038. 4196. 12109*. 15004. 18671. 30544. 47335. 86221. 134764. 137659. 347543. 386722. 419246*. 700061. 859379. 970454. 1460288. 1800254. 4889605. 11077571. 34618846. 64370954. 117290203*. 200760094. 401580454
197	155. 239. 352. 436. 746. 943. 1421. 1618. 4489. 6346*. 11074. 14029. 23879. 27341. 28804. 49883. 55709. 88411. 114499. 167689*. 190541. 314257. 356809. 377804. 415825. 496004. 744421. 987406. 1297090. 2153956*. 2362579. 2382560. 4699704. 13382956. 26620229. 26999399. 34792409. 40103726. 41494546. 60740461*. 149574656. 165242573. 178643779. 1411168679

Factorable $aa + 16$**.**

1	17
3	5 . 5
5	41
7	5 . 13
9	97
11	137
13	5 . 37
17	5 . 61
19	13 . 29
23	5 . 109
27	5 . 149
33	5 . 13 . 17
35	17 . 73

39	29 . 53
45	13 . 157
47	5 . 5 . 89
53	5 . 5 . 113
61	37 . 101
67	5 . 17 . 53
77	5 . 29 . 41
87	5 . 37 . 41
97	5 . 5 . 13 . 29
103	5 . 5 . 5 . 5 . 17
105	61 . 181
131	89 . 193
135	17 . 29 . 37
137	5 . 13 . 17 . 17
141	101 . 197
147	5 . 5 . 5 . 173
173	5 . 53 . 113
227	5 . 13 . 13 . 61
241	13 . 41 . 109
253	5 . 5 . 13 . 197
257	5 . 73 . 181
263	5 . 101 . 137
271	17 . 29 . 149
279	13 . 53 . 113
309	29 . 37 . 89
357	5 . 13 . 37 . 53
383	5 . 13 . 37 . 61
397	5 . 5 . 5 . 13 . 97
403	5 5 . 73 . 89
487	5 . 13 . 41 . 89
505	37 . 61 . 113
545	17 . 101 . 173
569	41 . 53 . 149
579	13 . 17 . 37 . 41
619	29 . 73 . 181
647	5 . 5 . 5 . 17 . 197
677	5 . 29 . 29 . 109
747	5 . 5 . 13 . 17 . 101
851	13 . 17 . 29 . 113
897	5 . 5 . 5 . 41 . 157
903	5 . 5 . 13 . 13 . 193
987	5 . 17 . 73 . 157
1021	13 . 17 . 53 . 89
1203	5 . 5 . 13 . 61 . 73
1237	5 . 29 . 61 . 173
1293	5 . 13 . 17 . 17 . 89
1353	5 . 5 . 5 . 5 . 29 . 101
1359	13 . 17 . 61 . 137

1463	5 . 13 . 13 . 17 . 149
1553	5 . 5 . 13 . 41 . 181
1717	5 . 41 . 73 . 197
1837	5 . 17 . 29 . 37 . 37
1929	137 . 157 . 173
2203	5 . 5 . 13 . 109 . 137
2223	5 . 29 . 173 . 197
2243	5 . 13 . 17 . 29 . 157
2301	29 . 41 . 61 . 73
2447	5 . 5 . 17 . 37 . 193
2455	29 . 37 . 41 . 137
2477	5 . 13 . 13 . 53 . 137
2593	5 . 13 . 13 . 73 . 109
2687	5 . 17 . 29 . 29 . 101
2823	5 . 17 . 29 . 53 . 61
2957	5 . 13 . 17 . 41 . 193
3095	17 . 37 . 97 . 157
3113	5 . 13 . 29 . 53 . 97
3153	5 . 5 . 13 . 13 . 13 . 181
3247	5 . 5 . 53 . 73 . 109
3293	5 . 101 . 109 . 197
3603	5 . 5 . 5 . 17 . 41 . 149
3607	5 . 13 . 13 . 89 . 173
3777	5 . 13 41 . 53 . 101
3847	5 . 5 . 29 . 137 . 149
4453	5 . 5 . 17 . 37 . 97
4497	5 . 5 . 61 . 89 . 149
4505	13 . 13 . 29 . 41 . 101
4601	29 . 37 . 109 . 181
4647	5 . 5 . 5 . 13 . 97 . 137
4853	5 5 . 5 . 29 . 73 . 89
4897	5 . 5 . 5 . 5 . 17 . 37 . 61
5337	5 . 13 . 17 . 149 . 173
5473	5 . 17 . 53 . 61 . 109
5635	13 . 13 . 13 . 97 . 149
5897	5 . 5 . 5 . 29 . 53 . 181
5921	13 . 89 . 157 . 193
6051	13 . 17 . 29 . 29 . 197
6081	37 . 53 . 109 . 173
6427	5 . 17 . 53 . 53 . 173
6605	61 . 73 . 97 . 101
6727	5 . 13 . 61 . 101 . 113
7345	17 . 89 . 181 . 197
7413	5 . 17 . 37 . 101 . 173
7547	5 . 5 . 13 . 13 . 13 . 17 . 61
7683	5 . 17 . 37 . 137 . 137
7703	5 . 5 . 13 . 41 . 61 . 73
7963	5 . 13 . 89 . 97 . 113

8141	73 . 89 . 101 . 101
8523	5 . 37 . 41 . 61 . 157
8747	5 . 5 . 101 . 157 . 193
9133	5 . 13 . 61 . 109 . 193
9353	5 . 5 . 5 . 13 . 13 . 41 . 101
10003	5 . 5 . 13 . 37 . 53 . 157
11967	5 . 13 . 17 . 29 . 41 . 109
12045	13 . 29 . 53 . 53 . 137
12257	5 . 29 . 53 . 113 . 173
12603	5 . 5 . 5 . 5 . 13 . 113 . 173
12667	5 . 37 . 73 . 109 . 109
13397	5 . 5 . 5 . 13 . 17 . 73 . 89
16897	5 . 5 . 5 . 17 . 29 . 41 . 113
17477	5 . 17 . 17 . 29 . 37 . 197
17635	13 . 41 . 53 . 101 . 109
17853	5 . 5 . 5 . 109 . 149 . 157
19991	17 . 29 . 61 . 97 . 137
20167	5 . 41 . 97 . 113 . 181
23677	5 . 53 . 97 . 113 . 193
24447	5 . 5 . 13 . 13 . 17 . 53 . 157
24785	13 . 13 . 17 . 29 . 73 . 101
25617	5 . 13 . 29 . 37 . 97 . 97
28581	13 . 53 . 73 . 109 . 149
29217	5 . 13 . 37 . 37 . 53 . 181
29853	5 . 5 . 5 . 17 . 41 . 53 . 193
36107	5 . 13 . 17 . 53 . 113 . 197
36823	5 . 13 . 17 . 41 . 173 . 173
37579	5 . 17 . 29 . 41 . 89 . 157
38863	5 . 13 . 17 . 17 . 37 . 41 . 53
39653	5 . 5 . 29 . 101 . 109 . 197
40853	5 . 5 . 5 . 13 . 61 . 113 . 149
41373	5 . 13 . 29 . 29 . 173 . 181
44269	17 . 53 . 61 . 181 . 197
44947	5 . 5 . 13 . 17 . 17 . 137 . 157

45793	5 . 13 . 37 . 89 . 97 . 101
52157	5 . 17 . 17 . 17 . 37 . 41 . 73
52379	37 . 73 . 89 . 101 . 113
52393	5 . 17 . 29 . 41 . 157 . 173
57323	5 . 13 . 17 29 41 . 41 . 61
57803	5 . 5 . 89 . 97 . 113 . 137
66333	5 . 13 . 17 . 17 . 29 . 41 . 197
67327	5 . 37 . 41 . 61 . 97 . 101
68215	37 . 61 . 101 . 137 . 149
69347	5 . 5 . 101 . 101 . 109 . 173
73467	5 . 29 . 41 . 89 . 101 . 101
74133	5 . 13 . 13 . 41 . 41 . 53 . 73

81413	5 . 13 . 29 . 29 . 29 . 37 . 113
82817	5 . 13 . 73 . 89 . 109 . 149
82893	5 . 17 . 37 . 73 . 173 . 173
103317	5 . 13 . 13 . 29 . 37 . 61 . 193
104293	5 . 13 . 61 . 101 . 157 . 173
113699	29 . 29 . 29 . 53 . 73 . 137
126497	5 . 5 . 13 . 53 . 61 . 97 . 157
130553	5 . 5 . 13 . 53 . 97 . 101 . 101
132143	5 . 29 . 53 . 193 . 193
139477	5 . 37 . 41 . 97 . 137 . 193
150897	5 . 5 . 5 . 13 . 29 . 61 . 89 . 89
154821	29 . 37 . 41 . 41 . 97 . 137
158373	5 . 13 . 17 . 37 . 61 . 89 . 113
158509	17 . 17 . 53 . 101 . 109 . 149
161399	17 . 17 . 53 . 89 . 97 . 197
162383	5 . 17 . 89 . 149 . 149 . 157
171293	5 . 17 . 29 . 41 . 41 . 73 . 97
172569	13 . 29 . 29 . 101 . 149 . 181
174727	5 . 13 . 17 . 37 . 53 . 73 . 193
232147	5 . 5 . 5 . 13 . 41 . 41 . 109 . 181
239387	5 . 53 . 97 . 109 . 113 . 181
240347	5 . 5 . 17 . 41 . 89 . 193 . 193
242897	5 . 5 . 5 . 17 . 17 . 97 . 113 . 149
251817	5 . 13 . 29 . 41 . 53 . 113 . 137
260033	5 . 13 . 13 . 17 . 29 . 29 . 29 . 193
260575	17 . 29 . 61 . 73 . 157 . 197
300527	5 . 13 . 17 . 37 . 113 . 113 . 173
374203	5 . 5 . 17 . 89 . 113 . 181 . 181
378671	13 . 13 . 37 . 41 . 53 . 61 . 173
434441	13 . 13 . 37 . 37 . 41 . 101 . 197
577603	5 . 5 . 5 . 5 . 29 . 29 . 41 . 113 . 137
648447	5 . 5 . 13 . 17 . 61 . 61 . 113 . 181
650103	5 . 5 . 5 . 5 . 29 . 37 . 73 . 89 . 97
658783	5 . 17 . 17 . 29 . 41 . 41 . 61 . 101
696353	5 . 5 . 5 . 5 17 . 17 . 37 . 37 . 37 . 53
748853	5 . 5 . 5 . 5 . 5 . 61 . 109 . 137 . 197
870487	5 . 13 . 61 . 73 . 97 . 137 . 197
873503	5 . 5 . 13 . 13 61 . 109 . 157 . 173
970497	5 5 . 17 . 37 . 53 . 73 . 113 . 137
1193679	13 29 . 41 . 41 . 101 113 . 197
1229533	5 . 13 . 13 . 53 . 53 . 53 . 61 . 197
1259837	5 . 13 . 13 . 13 . 17 . 29 . 37 . 89 . 89
1335487	5 . 17 . 89 . 97 . 113 . 137 . 157
1404163	5 . 13 . 13 . 37 . 41 . 97 . 101 . 157
1626475	13 . 29 . 41 . 73 . 109 . 137 . 157
2008103	5 . 5 . 5 . 13 . 41 . 53 . 61 . 97 . 193
2083893	5 . 13 . 17 . 53 . 73 . 89 . 101 . 113
2116091	17 . 29 . 37 . 101 . 113 . 137 . 157

2373167	5 . 17 . 29 . 37 . 41 . 53 . 157 . 181
2960653	5 . 5 . 13 . 13 . 17 . 17 . 17 . 101 . 113
3258603	5 . 5 . 5 . 37 . 41 . 61 . 61 . 101 . 149
3611583	5 . 17 . 29 . 37 . 61 . 109 . 137 . 157
3898603	5 . 5 . 5 . 13 . 13 . 37 . 41 . 73 . 73 . 89
4945505	13 . 13 . 17 . 17 . 17 . 29 . 89 . 101 . 113
5431603	5 . 5 . 5 . 17 . 17 . 29 . 41 . 73 . 97 . 97
8180243	5 . 13 . 29 . 29 . 37 . 37 . 41 . 53 . 53 . 113 . 193
8268383	5 . 13 . 13 . 29 . 41 . 73 . 73 . 113 . 113
9993613	5 . 13 . 29 . 37 . 53 . 53 . 61 . 61 . 137
10311423	5 . 41 . 41 . 61 . 109 . 113 . 113 . 149
15305803	5 . 5 . 13 . 37 . 53 . 101 . 109 . 173 . 193
16626883	5 . 17 . 73 . 101 . 109 . 149 . 157 . 173
17545053	5 . 5 . 13 . 17 . 17 . 41 . 53 . 101 . 109 . 137
17916571	17 . 37 . 37 . 61 . 73 . 109 . 157 . 181
18500917	5 . 13 . 29 . 41 . 41 . 61 . 89 . 101 . 197
19344643	5 . 13 . 13 . 29 . 41 . 73 . 73 . 113 . 113
20278927	5 . 13 . 17 . 29 . 53 . 73 . 113 . 149 . 197
22858302	5 . 5 . 17 . 17 . 17 . 17 . 17 . 29 . 53 . 61 . 157
38648107	5 . 17 . 17 . 29 . 97 . 109 . 109 . 157 . 197
40473647	5 . 5 . 5 . 5 . 13 . 37 . 41 . 73 . 97 . 137 . 137
46113113	5 . 13 . 13 . 17 . 29 . 37 . 53 . 73 . 181 . 197
1082687431	13 . 17 . 29 53 . 61 . 97 . 109 157 . 173 . 197
1254102921	13 . 13 . 17 . 17 . 41 . 53 . 61 . 97 . 101 . 137 . 181

5	3
13	7
17	1. 33. 103. 137
29	19. 97
37	13. 135. 1837
41	5. 77. 87. 579
53	39. 67. 357. 38863. 696353
61	17. 227. 383. 2823. 4897. 7547. 57323
73	35. 1203. 2301. 7703. 52157. 74133
89	47. 309. 403. 487. 1021. 1293. 4853. 13397. 150897. 1259837*. 3898603
97	9. 397. 3113. 4453. 25617. 171293. 650103. 5431603
101	61. 747. 1353. 2687. 3777. 4505. 6605. 8141. 9353. 24785*. 45793. 67327. 73467. 130553. 658783
109	23. 241. 677. 2593. 3247. 5473. 11967. 12667. 17635
113	53. 173. 279. 505. 851. 6727. 7963. 16897. 52379. 81413*. 158373. 2083893. 2960653. 4945505. 8268383. 19344643
137	11. 263. 1359. 2203. 2455. 2477. 4647. 7683. 12045. 19991*. 57803. 113699. 154821. 251817. 577603. 970497. 9993613. 17545053. 40473647
149	11. 271. 569. 1463. 3603. 3849. 4497. 5635. 28581. 40853*. 68215. 82817. 158509. 242897. 3258603. 10311423

157	45. 897. 987. 2243. 3095. 8523. 10003. 17853. 24447. 37579*. 44947. 126497. 162384. 1335487. 1404163. 1626475. 2116091. 3611583. 22858302
173	147. 545. 1237. 1929. 3607. 5337. 6081. 6427. 7413. 12257*. 12603. 36823. 52393. 69347. 82893. 104293. 300527. 378671. 873503. 16626883*
181	105. 257. 619. 1553. 3153. 4601. 5897. 20167. 29217. 41373*. 172569. 232147. 239387. 374203. 648447. 2373167. 17916571. 1254102921
193	131. 903. 2447. 2957. 5921. 8747. 9133. 23677. 29853. 103317. 132143 139477. 174727. 240347. 260033. 2008103. 8180243 15305803
197	141. 253. 647. 1717. 2223. 3293. 6051. 7345. 17477. 36107*. 39653. 44269. 66333. 161399. 260575. 434441. 748853. 870487. 1193679. 1229533*. 18500917. 20278927. 38648107. 46113113. 1082687431

Factorable $aa + 25$**.**

1	13
2	29
3	17
4	41
6	61
7	37
8	89
9	53
11	73
12	13 . 13
13	97
14	13 . 17
17	157
19	193
27	13 . 29
31	17 . 29
37	17 . 41
38	13 . 113
44	37 . 53
48	17 . 137
51	13 . 101
53	13 . 109
54	17 . 173
56	29 . 109
62	53 . 73
67	37 . 61
71	17 . 149
78	41 . 149
81	37 . 89
84	73 . 97
86	41 . 181

89	29 . 137
97	53 . 89.
99	17 . 17 . 17
116	13 . 17 . 61
118	13 . 29 . 37
119	41 . 173
127	41 . 197
151	101 . 113
157	13 . 13 . 73
168	13 . 41 . 53
174	157 . 193
181	13 . 13 . 97
201	17 . 29 . 41
207	13 . 17 . 97
209	13 . 41 . 41
227	149 . 173
252	17 . 37 . 101
259	13 . 29 . 89
267	181 . 197
274	13 . 53 . 109
303	17 . 37 . 73
309	17 . 53 53
311	13 . 61 . 61
324	13 . 41 . 197
326	13 . 13 . 17 . 37
354	17 . 73 . 101
363	13 . 37 . 137
376	13 . 73 . 149
377	17 . 37 . 113
414	37 . 41 . 113
433	29 . 53 . 61
437	29 . 37 . 89
454	13 . 101 . 157
488	37 . 41 . 157
521	13 . 53 . 197
573	13 . 73 . 173
611	29 . 41 . 157
636	13 . 29 . 29 . 37
638	13 . 173 . 181
677	13 . 17 . 17 . 61
733	37 . 53 . 137
753	13 . 113 . 193
768	13 . 17 . 17 . 157
816	41 . 109 . 149
819	17 . 109 . 181
857	13 . 13 . 41 . 53
858	37 . 101 . 197
898	13 . 17 . 41 . 89

959	29 . 101 . 157
984	29 . 173 . 193
1092	61 . 113 . 173
1104	13 . 29 . 53 . 61
1177	37 . 97 . 193
1252	73 . 109 . 197
1364	13 . 13 . 101 . 109
1431	13 . 17 . 41 . 113
1442	13 . 17 . 97 . 97
1544	17 . 17 . 73 . 113
1561	13 . 17 . 37 . 149
1733	97 . 113 . 137
1767	13 . 29 . 41 . 101
1887	29 . 29 . 29 . 73
2128	17 . 41 . 73 . 89
2144	13 . 29 . 89 . 137
2341	13 . 41 . 53 . 97
2434	17 . 29 . 61 . 197
2751	17 . 41 . 61 . 89
2887	13 . 17 . 109 . 173
2989	13 . 17 . 17 . 29 . 41
3199	13 . 13 . 13 . 17 . 137
3323	37 . 37 . 37 . 109
3471	17 . 37 . 61 . 157
3522	13 . 17 . 37 . 37 . 41
3654	13 . 61 . 113 . 149
3686	17 . 41 . 101 . 193
3788	17 . 61 . 101 . 137.
4219	17 . 41 . 113 . 113
4264	17 . 61 . 89 . 197
4458	13 . 89 . 89 . 193
4798	13 . 89 . 101 . 197
4814	17 . 17 . 17 . 53 . 89
5154	17 . 89 . 97 . 181
5251	13 . 13 . 29 . 29 . 97
5706	13 . 101 . 137 . 181
5927	13 . 13 . 37 53 . 53
6001	29 . 73 . 97 . 173
6157	17 . 53 . 109 . 193
6581	29 . 53 . 73 . 193
6616	13 . 17 . 37 53 . 101
7359	13 . 97 . 109 . 197
7676	53 . 73 . 97 . 157
7753	41 . 61 . 61 . 197
8147	29 . 37 . 157 . 197
8231	17 . 101 . 109 . 181
8776	13 . 13 . 37 . 109 113
9209	73 . 73 . 73 . 109

10049	41 . 89 . 101 . 137
10061	13 . 17 . 29 . 53 . 149
10501	37 . 73 . 137 . 149
12468	13 . 29 . 41 . 89 . 113
12526	17 . 17 . 29 . 97 . 193
13786	73 . 101 . 149 . 173
13787	89 97 . 101 . 109
14067	13 . 29 37 . 41 . 173
14756	13 . 37 . 41 . 61 . 181
15807	13 . 17 . 29 . 101 . 193
17057	13 . 13 . 53 . 109 . 149
18123	13 . 29 . 37 . 61 . 193
18771	13 . 13 . 13 17 . 53 . 89
18823	13 . 29 . 41 . 73 . 157
19553	13 . 17 . 17 . 17 . 41 . 73
19751	17 . 17 . 17 . 29 . 37 . 37
20502	13 . 53 . 61 . 73 . 137
21009	13 . 17 . 37 . 137 . 197
21319	13 . 37 . 37 . 113 . 113
21527	13 . 53 . 61 . 137 . 149
21644	13 . 13 . 17 . 41 . 41 . 97
23488	29 . 37 . 53 . 89 . 109
24101	13 . 29 . 61 . 73 . 173
24358	17 . 29 . 41 . 149 . 197
25401	13 . 17 . 97 . 101 . 149
26707	29 . 29 . 37 . 73 . 157
30467	17 . 41 . 41 . 109 . 149
31226	17 . 53 . 61 . 113 . 157
33381	29 . 37 . 53 . 97 . 101
38011	13 . 41 . 89 . 97 . 157
38134	17 . 41 . 97 . 137 . 157
40559	13 . 17 . 17 . 37 . 61 . 97
41037	29 . 41 . 73 . 89 . 109
41891	17 . 37 . 73 . 97 . 197
44407	13 . 17 . 17 37 . 41 . 173
48062	13 . 17 . 53 . 53 . 61 . 61
49943	17 . 37 . 73 . 157 . 173
50051	13 . 17 . 173 . 181 . 181
56913	13 . 17 . 37 . 37 . 53 . 101
60347	13 . 17 . 29 . 29 . 97 . 101
68626	13 . 13 17 . 53 . 157 . 197
85699	37 . 61 89 . 101 . 181
87989	17 . 53 . 113 . 193 . 197
93469	13 . 13 . 13 . 17 . 29 . 37 . 109
95473	13 . 13 . 13 . 73 . 157 . 181
101151	37 . 41 . 101 . 173 . 193
108871	17 . 53 173 . 193 . 197
121479	17 . 17 . 29 . 41 . 109 . 197

141777	13 . 17 . 37 . 73 . 113 . 149
144808	13 . 41 . 61 . 61 . 97 . 109
152762	13 . 41 . 41 . 97 . 101 . 109
152803	13 . 29 . 37 . 41 . 137 . 149
155187	73 . 97 . 101 . 113 149
160314	29 . 37 41 . 61 . 61 . 157
172561	13 . 13 . 13 . 13 . 37 . 73 . 193
183971	17 . 37 . 41 . 73 . 89 . 101
188618	13 . 17 . 17 29 53 . 61 . 101
214482	29 . 37 . 53 . 61 . 89 . 149
214631	13 . 29 . 41 . 73 . 137 . 149
234852	17 . 41 . 53 . 73 . 113 . 181
249014	13 . 73 . 73 . 89 . 89 . 113
257841	13 . 29 . 61 . 89 . 101 . 149
279007	13 . 13 . 17 . 29 . 29 . 89 . 181
329219	17 . 37 . 73 . 89 . 89 . 149
329848	13 . 17 . 17 . 29 . 37 . 137 . 197
382537	13 . 17 . 17 . 29 . 61 . 101 . 109
422419	17 . 17 . 17 . 41 . 53 . 61 . 137
458742	17 . 17 . 113 . 173 . 193 . 193
484041	13 . 29 . 37 . 37 . 61 . 61 . 61
546534	13 . 13 . 37 . 41 . 41 . 157 . 181
564812	13 . 37 . 37 . 41 . 53 . 73 . 113
735331	13 . 13 . 37 . 41 . 53 . 101 197
743781	13 . 13 . 13 . 13 . 17 . 37 . 89 . 173
867847	17 . 89 . 89 . 137 . 137 . 149
938003	13 . 29 . 53 . 61 . 61 . 61 . 97
1000154	13 . 13 . 29 . 29 . 37 . 37 53 . 97.
1964806	13 . 13 . 17 . 29 . 41 . 73 . 113 . 137
2144583	13 . 41 . 53 . 61 . 73 . 101 . 181
3589859	17 . 17 . 73 . 109 . 113 . 137 . 181
3879591	13 . 37 . 53 . 89 . 113 . 149 . 197
5693622	13 . 13 . 13 . 53 . 97 . 101 . 157 . 181
6991009	13 17 . 17 . 37 . 53 . 113 . 149 . 197
7062082	13 . 29 . 29 . 41 . 53 . 73 . 149 193
8489259	13 . 17 . 29 . 29 . 29 . 41 . 41 . 41 . 97
8717008	13 . 13 17 . 17 . 37 . 37 . 89 . 113 . 113
9707868	13 . 29 . 29 . 37 . 101 . 113 . 137 . 149
10305788	13 . 17 . 37 . 53 101 . 109 . 113 . 197
17462342	13 . 37 . 61 . 61 . 89 . 89 . 137 157
38722306	13 . 13 . 29 . 37 . 61 . 89 . 89 . 109 . 157
48162204	13 . 17 . 37 . 37 . 41 . 53 . 101 . 181 . 193
60920523	13 . 17 . 17 . 53 . 61 . 61 . 101 . 137 . 181

63769026	17 . 29 . 37 . 41 . 53 . 89 . 101 . 101 . 113
111771087	13 . 17 . 37 . 61 . 61 . 89 . 113 . 137 . 149
141757784	13 . 17 . 53 . 61 . 89 . 113 . 137 . 137 . 149

172642653	13 . 17 . 29 . 73 . 89 . 89 . 137 . 149 . 197
190067607	73 . 89 . 97 . 101 . 101 . 109 . 149 . 173
308956283	13 . 29 . 29 . 37 . 41 . 53 . 61 . 73 . 89 . 137
569329071	13 . 13 . 29 . 37 . 41 . 97 . 101 . 109 . 137 . 149

13	1. 12
17	3. 14. 99
29	2. 27. 31
37	7. 118. 326. 636. 19751
41	4. 37. 201. 209. 2989. 3522
53	9. 44. 168. 309. 857. 5927
61	6. 67. 116. 311. 433. 677. 1104. 48062. 484041
73	11. 62. 157. 303. 1887. 19553
89	8. 81. 97. 259. 437. 898. 2128. 2751. 4814. 18771*
97	13. 84. 181. 207. 1442. 2341. 5251. 21644. 40559. 938203*. 1000154. 8489259
101	51. 252. 354. 1767. 6616. 33381. 56913. 60347. 183971. 188618*
109	53. 56. 274. 1364. 3323. 9209. 13787. 23488. 41037. 93469*. 144808. 152762. 382537
113	38. 151. 377. 414. 1431. 1544. 4219. 8776. 12468. 21319*. 249014. 564812. 8717008. 63769026
137	48. 89. 363. 733. 1733. 2144. 3199. 3788. 10049. 20502*. 422419. 1964806. 308956283
149	71. 78. 376. 816. 1561. 3654. 10061. 10501. 17057. 21527*. 25401. 30467. 14777. 152803. 155187. 214482. 214631. 257841. 329219. 867847*. 9707868. 111771087. 141757784. 569329071
157	17. 454. 488. 611. 768. 959. 3471. 7676. 18823. 26707*. 31226. 38011. 38134. 160314. 17462342. 38722306
173	54. 119. 227. 573. 1092. 2887. 6001. 13786. 14067. 24101*. 44407. 49943. 743781. 190067607
181	86. 638. 819. 5154. 5706. 8231. 14756. 50051. 85699. 95473*. 234852. 279007. 546534. 2144583. 3589859. 5693622. 60920523
193	19. 174. 753. 984. 1177. 3686. 4458. 6157. 6581. 12526*. 15807. 18123. 101151. 172561. 458742. 7062082. 48162204
197	127. 267. 324. 521. 858. 1252. 2434. 4264. 4798. 7359*. 7753. 8147. 21009. 24358. 41891. 68626. 87989. 108871. 121479. 329848*. 735331. 3879591. 6991009. 10305788. 172642653

Factorable $aa + 36$.

1	37
5	61
7	5 . 17
11	157
13	5 . 41
17	5 . 5 . 13
23	5 . 113
35	13 . 97
41	17 . 101
43	5 . 13 . 29
61	13 . 17 . 17
67	5 . 5 . 181
73	5 . 29 . 37
85	53 . 137
89	73 . 109
95	13 . 17 . 41
113	5 . 13 . 197
115	89 . 149
127	5 . 53 . 61
191	13 . 53 . 53
203	5 . 73 . 113
217	5 . 5 . 5 . 13 . 29
233	5 . 5 . 41 . 53
293	5 . 89 . 193
295	13 . 37 . 181
307	5 . 109 . 173
347	5 . 13 . 17 . 109
445	37 . 53 . 101
479	29 . 41 . 193
517	5 . 5 . 17 . 17 . 37
565	29 . 101 . 109
617	5 . 5 . 97 . 157
667	5 . 5 . 13 . 37 . 37
673	5 . 17 . 73 . 73
737	5 . 13 . 61 . 137
763	5 . 13 . 13 . 13 . 53
953	5 . 13 . 89 . 157
971	13 . 29 . 41 . 61
1183	5 . 5 . 17 . 37 . 89
1333	5 . 5 . 17 . 37 . 113
1463	5 . 41 . 53 . 197
1517	5 . 5 . 13 . 73 . 97
1673	5 . 13 . 17 . 17 . 149
1717	5 . 5 . 5 . 5 . 53 . 89
1873	5 . 41 . 109 . 157

2201	13 . 41 . 61 . 149
2251	17 . 17 . 89 . 197
2383	5 . 5 . 13 . 101 . 173
2557	5 . 13 . 17 . 61 . 97
2567	5 . 5 . 29 . 61 . 149
2963	5 . 89 . 109 . 181
3181	13 . 37 . 109 . 193
3553	5 . 13 . 29 . 37 . 181
3767	5 . 5 . 17 . 173 . 193
4031	41 . 61 . 73 . 89
4277	5 . 17 . 29 . 41 . 181
4883	5 . 5 . 37 . 149 . 173
5009	13 . 97 . 101 . 197
5321	13 . 13 . 29 . 53 . 109
5467	5 . 5 . 5 . 5 . 17 . 29 . 97
5495	13 . 13 . 29 . 61 . 101
5497	5 . 173 . 181 . 193
6217	5 . 5 . 5 . 37 . 61 . 137
6221	29 . 73 . 101 . 181
6655	29 . 41 . 193 . 193
6827	5 . 17 . 61 . 89 . 101
7547	5 . 37 . 37 . 53 . 157
7717	5 . 5 . 5 . 53 . 89 . 101
7813	5 . 17 . 61 . 61 . 193
7861	13 . 17 . 137 . 157
7919	37 . 97 . 101 . 173
8459	13 . 17 . 41 . 53 . 149
10261	13 . 17 . 53 . 89 . 101
10565	13 . 13 . 41 . 89 . 181
13763	5 . 13 . 17 . 37 . 41 . 113
13823	5 . 13 . 109 . 149 181
14543	5 . 13 . 29 . 29 . 53 . 73
15245	13 . 37 . 61 . 89 . 89
15733	5 . 5 . 29 . 29 . 61 . 193
17617	5 . 5 . 29 . 41 . 53 . 197
18659	13 . 17 . 97 . 109 . 149
22345	17 . 29 . 53 . 97 . 197
22481	13 . 17 . 17 . 17 . 41 . 193
22583	5 . 5 . 17 . 101 . 109 . 109
22733	5 . 5 . 13 . 13 . 13 . 97 . 97
22867	5 . 5 29 . 37 . 101 . 193
23753	5 . 37 . 113 . 137 . 197
29129	13 . 53 . 89 . 101 . 137
29995	13 . 13 . 13 . 13 . 17 . 17 . 109
30845	13 . 13 . 17 . 41 . 41 . 197
31885	13 . 17 29 . 41 . 53 . 73
32647	5 . 13 . 17 . 73 . 73 . 181
38893	5 . 73 . 109 . 193 . 197

38923	5 . 17 . 37 . 53 . 61 . 149
39347	5 . 13 . 41 . 53 . 97 . 113
42133	5 . 5 . 17 . 17 . 17 . 97 . 149
44327	5 . 29 . 29 . 37 . 73 . 173
48967	5 . 5 . 5 . 13 . 17 . 29 . 41 . 73

49517	5 . 5 . 29 . 113 . 173 . 173
54167	5 . 5 . 13 . 13 . 37 . 137 . 137
61117	5 . 5 . 13 . 29 . 61 . 73 . 89
62825	13 . 17 . 37 . 41 . 61 . 193
74603	5 . 13 . 17 . 29 . 29 . 53 . 113
87217	5 . 5 . 5 . 17 . 17 . 29 . 53 . 137
96227	5 . 17 . 53 . 109 . 109 . 173
125909	13 . 17 . 61 . 73 . 89 . 181
130613	5 . 41 . 53 . 73 . 137 . 157
141709	13 . 13 . 29 . 37 . 37 . 41 . 73
151163	5 . 29 . 61 . 109 . 137 . 173
161035	13 . 41 . 53 . 61 . 101 . 149
171655	89 . 97 . 109 . 173 . 181
174565	29 . 37 . 37 . 41 . 97 . 193
182743	5 . 17 . 29 . 29 . 29 . 89 . 181
189353	5 . 17 . 109 . 157 . 157 . 157
191203	5 . 53 . 53 . 73 . 181 . 197
206407	5 . 17 . 17 . 29 . 41 . 137 . 181
256693	5 . 17 . 17 . 29 . 61 . 149 . 173
387833	5 . 13 . 37 . 53 . 53 . 61 . 73
427795	13 . 17 . 37 . 37 . 53 . 101 . 113
429347	5 . 13 . 13 . 37 . 173 . 173 . 197
449921	13 . 29 . 37 . 41 . 41 . 89 . 97
533789	13 . 13 . 29 . 29 . 113 . 113 . 157
726029	17 . 17 . 29 . 29 . 101 . 109 . 197
837533	5 . 5 . 5 . 37 . 97 . 101 . 113 . 137
1097105	13 . 17 . 17 . 97 . 109 . 157 . 193
1396529	13 . 13 . 13 . 37 . 41 . 53 . 61 . 181
2390717	5 . 5 . 5 . 13 . 17 . 29 . 29 . 37 . 61 . 109
2525527	5 . 13 . 17 . 61 . 89 97 . 97 . 113
5318933	5 . 5 . 13 . 17 . 29 . 89 . 97 . 113 . 181
6920333	5 . 5 . 13 . 17 . 17 . 17 . 37 . 61 . 97 . 137
9439957	5 . 17 . 17 . 17 . 17 . 17 . 37 . 37 . 53 . 173
11776417	5 . 5 . 17 . 41 . 73 . 73 . 89 . 97 . 173
45435967	5 . 5 . 5 . 29 . 41 . 53 . 61 . 113 . 193 . 197
70145903	5 . 13 . 13 . 17 . 41 . 53 . 73 . 97 . 113 . 197
90115783	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 13 . 13 . 17 . 61 . 73
716295433	5 . 5 . 13 . 13 . 29 . 29 . 37 . 41 . 61 . 89 89 . 197
2009136133	5 . 5 . 13 . 17 . 41 . 61 . 73 . 89 . 97 . 113 . 181 . 197

5	.
13	17
17	7. 61
29	43. 217
37	1. 73. 517. 667
41	13. 95
53	191. 233. 763
61	5. 127. 971
73	673. 14543. 31885. 48967. 141709. 387833. 90115783
89	1183. 1717. 4031. 15245. 61117
97	35. 1517. 2557. 5467. 22733. 449921
101	41. 445. 5495. 6827. 7717. 10261
109	89. 347. 565. 5321. 22583. 29995. 2390717
113	23. 203. 1333. 13763. 39347. 74603. 427795. 2525527
137	85. 737. 6217. 29129. 54167. 87217. 837533. 6920333
149	115. 1673. 2201. 2567. 8459. 18659. 38923. 42133. 161035
157	11. 617. 953. 1873. 7547. 7861. 130613. 189353. 533789
173	307. 2383. 4883. 7919. 44327. 49517. 96227. 151163. 256693. 9439957*. 11776417
181	67. 295. 2963. 3553. 4277. 6221. 10565. 13823. 32647. 125909*. 171655. 182743. 206407. 1396529. 5318933
193	293. 479. 3181. 3767. 5497. 6655. 7813. 15733. 22481. 22867*. 62825. 174565. 1097105
197	113. 1463. 2251. 5009. 17617 22345. 23753. 30845. 38893. 191203*. 429347. 726029. 45435967. 70145903. 716295433. 2009136133

Factorable $aa + 49$.

1	5 . 5
2	53
3	29
4	5 . 13
5	37
6	5 . 17
8	113
9	5 . 13
10	149
11	5 . 17
12	193
13	109
15	137
16	5 . 61
17	13 . 13
19	5 . 41
22	13 . 41

23	17 . 17
24	5 . 5 . 5 . 5
26	5 . 5 . 29
29	5 . 89
30	13 . 73
31	5 . 101
32	29 . 37
39	5 . 157
40	17 . 97
41	5 . 173
43	13 . 73
45	17 . 61
48	13 . 181
51	5 . 5 . 53
55	29 . 53
57	17 . 97
60	41 . 89
61	5 . 13 . 29
69	5 . 13 . 37
74	5 . 5 . 13 . 17
79	5 . 17 . 37
96	5 . 17 . 109
99	5 . 5 . 197
101	5 . 5 . 5 . 41
103	73 . 73
104	5 . 41 . 53
106	5 . 37 . 61
108	13 . 17 . 53
113	13 . 17 . 29
116	5 . 37 . 73
118	89 . 157
121	5 . 13 . 113
122	109 . 137
132	101 . 173
137	97 . 97
139	5 . 13 . 149
142	17 . 29 . 41
149	5 . 5 . 5 . 89
152	13 . 13 . 137
159	5 . 17 . 149
171	5 . 29 . 101
176	5 . 5 . 17 . 73
181	5 . 17 . 193
186	5 . 13 . 13 . 41
199	5 . 5 . 13 . 61
205	109 . 193
214	5 . 53 . 173
227	17 . 37 . 41

229	5 . 29 . 181
234	5 . 97 . 113
249	5 . 5 . 17 . 73
251	5 . 5 . 13 . 97
264	5 . 13 . 29 . 37
289	5 . 61 . 137
295	13 . 17 . 197
296	5 . 89 . 197
314	5 . 109 . 181
316	5 . 13 . 29 . 53
321	5 . 13 . 13 . 61
331	5 . 97 . 113
334	5 . 13 . 17 . 101
347	13 . 41 . 113
351	5 . 5 . 5 . 17 . 29
373	13 . 53 . 101
374	5 . 5 . 29 . 193
449	5 . 5 . 37 . 109
474	5 . 5 . 89 . 101
533	17 . 61 . 137
550	13 . 17 . 37 . 37
554	5 . 29 . 29 . 73
555	13 . 17 . 17 . 41
589	5 . 13 . 17 . 157
591	5 . 181 . 193
594	5 . 13 . 61 . 89
601	5 . 5 . 5 . 5 . 17 . 17
606	5 . 17 . 29 . 149
634	5 . 37 . 41 . 53
641	5 . 13 . 29 . 109
667	13 . 109 . 157
676	5 . 5 . 101 . 181
691	5 . 17 . 53 . 53
719	5 . 13 . 41 . 97
776	5 . 5 . 13 . 17 . 109
799	5 . 5 . 113 . 113
809	5 . 29 . 37 . 61
824	5 . 5 . 157 . 173
839	5 . 17 . 41 . 101
844	5 . 17 . 17 . 17 . 29
899	5 . 5 . 5 . 53 . 61
906	5 . 13 . 73 . 173
919	5 . 13 . 73 . 89
979	5 . 13 . 73 . 101
992	13 . 17 . 61 . 73
1009	5 . 17 . 53 . 113
1031	5 . 13 . 13 . 17 . 37
1041	5 . 29 . 37 . 101

1111	5 . 17 . 53 . 137
1128	17 . 29 . 29 . 89
1179	5 . 13 . 17 . 17 37
1186	5 . 29 . 89 . 109
1221	5 . 29 . 53 . 97
1252	13 . 17 . 41 . 173
1364	5 . 37 . 89 . 113

1374	5 . 5 . 13 . 37 . 157
1395	13 . 29 . 29 . 89
1556	5 . 13 . 193 . 193
1592	17 . 29 . 53 . 97
1609	5 . 17 . 97 . 157
1621	5 . 13 . 17 . 29 . 41
1629	5 . 13 137 . 149
1649	5 . 5 . 5 . 73 . 149
1689	5 . 17 . 97 . 173
1751	5 . 5 . 13 53 . 89
1766	5 . 29 . 137 . 157
1929	5 . 37 89 . 113
1949	5 5 . 17 . 41 . 109
2069	5 . 41 . 53 . 197
2076	5 . 5 . 13 . 89 . 149
2151	5 5 . 37 . 41 . 61
2374	5 . 5 . 17 . 89 . 149
2381	5 . 29 . 113 . 173
2521	5 37 . 89 . 193
2578	13 . 17 . 17 . 29 . 61
2595	17 . 37 . 53 101
2607	17 . 29 . 61 . 113
2659	5 . 37 . 97 . 197
2817	13 . 37 . 73 . 113
2851	5 5 . 5 . 13 41 . 61
2930	17 . 41 . 109 . 113
2944	5 61 . 157 . 181
2999	5 . 5 . 13 . 101 . 137
3100	17 . 29 101 . 193
3156	5 . 17 . 17 . 61 . 113
3251	5 5 . 29 . 37 . 197
3501	5 . 5 . 13 . 109 . 173
3547	17 . 37 . 73 . 137
3709	5 . 13 . 29 . 41 . 89
3753	13 . 41 . 73 . 181
4034	5 . 13 . 29 . 89 . 97
4065	13 . 37 . 89 . 193
4211	5 . 97 . 101 . 181
4286	5 . 13 . 41 . 61 . 113

4324	5 . 5 . 17 . 29 . 37 . 41
4399	5 . 5 . 5 . 5 . 113 . 137
4556	5 . 29 37 . 53 . 73
4629	5 . 73 . 149 . 197
4630	17 . 37 . 173 197
4657	37 . 37 . 89 . 89
4715	13 . 13 . 17 . 53 . 73
4749	5 . 5 . 13 . 13 . 17 . 157
4754	5 . 13 . 17 . 113 . 181
4778	37 . 41 . 101 . 149
4918	13 . 13 . 13 . 101 . 109
4927	29 . 53 . 53 . 149
5024	5 . 5 . 5 . 5 . 41 . 197
5101	5 . 5 . 5 . 29 . 37 . 97
5191	5 . 13 . 17 . 89 . 137
5221	5 . 101 . 137 . 197
5226	5 . 5 . 5 . 41 . 73 . 73
5841	5 . 13 . 37 . 41 . 173
6008	41 . 41 . 109 . 197
6029	5 . 17 . 29 . 73 . 101
6309	5 . 13 . 53 . 53 . 109
6381	5 . 17 . 17 . 73 . 193
6574	5 . 5 . 13 13 . 53 . 193
6899	5 5 . 5 . 5 . 13 . 29 . 101
6998	13 . 17 . 37 . 53 . 113
7276	5 . 5 . 13 . 29 . 41 . 137
7316	5 . 17 . 53 . 109 . 109
7440	13 . 17 . 41 . 41 . 149
7914	5 . 29 . 61 . 73 97
8149	5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 5 . 17
8219	5 . 37 . 41 . 61 . 73
8251	5 . 5 . 13 . 17 . 61 . 101
8515	37 . 89 . 101 . 109
8753	13 . 137 137 . 157
8919	5 . 17 . 41 . 101 . 113
9161	5 . 13 . 29 . 113 . 197
9301	5 . 5 . 73 . 137 . 173
9546	5 . 13 . 97 . 97 . 149
9616	5 . 13 . 13 . 17 . 41 . 157
9837	13 . 17 . 37 . 61 . 97
9993	13 149 149 . 173
10291	5 . 17 . 37 . 113 . 149
10630	13 . 13 . 61 . 97 . 113
10651	5 . 5 . 13 . 37 . 53 . 89
10727	29 . 97 . 113 . 181
10761	5 . 41 . 53 . 73 . 73
10887	41 . 89 . 109 . 149
11185	53 . 89 . 89 . 149

11632	29 . 149 . 173 . 181
12151	5 . 5 . 13 . 13 . 101 . 173
12489	5 . 13 . 13 . 17 . 61 . 89
13101	5 . 5 . 5 . 5 . 17 . 41 . 197
13329	5 . 13 . 73 . 97 . 113
14351	5 . 5 . 5 . 5 . 37 61 . 73
14656	5 . 41 . 61 . 89 . 193
14811	5 . 13 . 109 . 113 . 137
15356	5 41 . 61 . 109 . 173
15425	17 . 29 . 29 . 53 . 157
15661	5 . 13 . 61 . 157 . 197
16393	61 . 101 . 113 193
16446	5 . 29 . 109 . 109 157
17247	13 . 37 37 . 61 137
18099	5 . 5 . 17 . 29 . 97 . 137
18976	5 . 5 . 5 . 13 . 37 . 53 . 113
19743	13 . 17 . 41 . 137 . 157
20297	13 . 13 . 13 . 29 . 53 . 61
20999	5 . 13 . 29 . 149 . 157
21768	97 . 137 . 181 . 197
21834	5 . 17 . 29 . 41 . 53 . 89
22156	5 . 13 . 13 . 53 . 97 . 113
22569	5 . 41 . 41 . 157 . 193
25726	5 . 5 . 5 . 29 . 41 . 61 . 73.
25931	5 . 13 . 17 . 41 . 41 . 181
26016	5 . 17 . 29 . 37 . 41 . 181
26337	113 . 113 . 157 . 173
27200	13 . 37 . 97 . 101 . 157
27564	5 . 13 . 13 . 73 . 109 . 113
27721	5 . 17 . 17 . 29 . 53 . 173
29254	5 . 13 . 13 . 53 . 97 . 197
29501	5 . 5 . 13 . 17 . 17 . 41 . 113
30179	5 . 61 . 73 . 113 . 181.
30424	5 . 5 . 13 . 17 . 29 . 53 . 109
31274	5 . 5 . 5 . 5 . 13 . 17 . 73 . 97
32491	5 . 13 . 37 . 41 . 53 . 101
33258	13 . 17 . 17 . 37 . 73 . 109
34134	5 . 13 . 41 . 53 . 73 . 113
35303	17 . 37 . 61 . 109 . 149
35361	5 . 41 . 113 . 137 . 197
35524	5 . 5 . 5 . 17 . 17 . 181 . 193
36149	5 . 5 . 5 . 13 . 13 . 157 . 197
37409	5 . 61 . 89 . 149 . 173
37836	5 . 17 . 17 . 61 . 109 . 149
38601	5 . 5 . 5 . 13 . 17 . 149 . 181
39901	5 . 5 . 13 . 13 . 29 . 73 . 89
41801	5 . 5 . 41 . 61 . 89 . 157
41859	5 . 73 . 89 . 149 . 181

43416	5 . 13 . 13 . 13 . 29 . 61 . 97
44677	13 . 53 . 97 . 109 . 137
44976	5 . 5 . 5 . 5 . 5 13 . 17 . 29 . 101
46229	5 . 17 . 29 . 41 . 97 . 109
48317	13 . 13 . 29 . 37 . 41 . 157
49099	5 . 5 . 41 . 73 . 89 . 181
50632	17 . 73 . 101 . 113 . 181
51176	5 . 5 . 17 . 17 . 37 . 97 . 101
54274	5 . 5 . 5 . 37 . 53 . 61 . 197
55774	5 . 5 . 5 . 13 . 89 . 137 . 157
58881	5 . 13 . 53 . 61 . 73 . 113
64051	5 . 5 . 73 . 73 . 89 . 173
64644	5 . 29 . 37 . 61 . 113 . 113
67785	17 . 53 . 109 . 149 . 157
69983	13 . 13 . 17 . 61 . 89 . 157
72851	5 . 5 . 5 . 17 . 17 . 17 . 29 . 149
73043	13 . 17 . 37 . 41 . 73 . 109
73672	17 . 17 . 37 . 53 . 61 . 157
73721	5 . 29 . 29 53 . 89 137
76534	5 . 29 . 53 . 53 . 197
80841	5 . 17 . 61 . 73 . 89 . 97
82307	13 . 53 . 157 . 173 . 181
83430	13 . 17 . 29 . 37 . 149 197
87369	5 . 13 . 17 . 89 . 197 . 197
88213	37 . 41 . 97 . 137 . 193
88406	5 . 17 . 53 . 89 . 101 . 193
88989	5 . 13 . 17 . 17 . 41 . 53 . 97
89149	5 . 5 . 5 . 29 . 89 . 109 . 113
92049	5 . 5 . 13 . 17 . 29 . 137 . 193
102735	13 . 13 . 13 . 89 . 137 . 197
124029	5 . 13 . 13 . 37 . 37 . 61 . 109
131863	13 . 17 . 37 . 97 . 97 . 113
133149	5 . 5 . 5 . 5 . 5 . 41 101 . 137
138199	5 . 5 . 13 . 17 . 101 . 109 . 157
139551	5 . 5 . 13 . 29 . 53 . 101 . 193
141633	17 . 17 . 17 . 17 . 29 . 41 . 101
148439	5 . 37 . 41 . 73 101 . 197
150410	17 . 37 . 41 . 61 . 73 . 197
150681	5 . 29 . 53 . 97 . 97 . 157
154876	5 . 5 . 17 . 41 . 73 . 109 . 173
157995	29 . 37 . 41 . 53 . 53 . 101
160168	17 . 37 . 41 . 53 . 137 . 137
163609	5 . 13 . 13 . 37 . 41 . 53 . 137
166851	5 . 5 . 5 . 5 . 5 . 13 . 41 . 61 . 137
167124	5 . 5 . 13 . 13 . 29 . 37 . 61 . 101
174074	5 . 5 . 13 . 17 . 157 . 181 . 193
178149	5 . 5 . 5 . 5 . 17 . 89 . 97 . 173
179565	13 . 17 . 29 . 113 . 113 . 197

187249	5 . 5 . 17 . 17 . 109 . 113 . 197
189538	73 . 109 . 149 . 157 . 193
207814	5 . 13 . 17 . 17 . 97 . 137 . 173
213263	29 . 37 . 41 . 73 . 73 . 97
217351	5 . 5 . 5 . 13 . 13 . 17 . 17 . 53 . 73
231755	13 . 17 . 17 . 17 . 61 . 61 . 113
273694	5 . 17 . 37 . 41 . 53 . 97 . 113
281226	5 . 5 . 5 . 5 . 61 . 73 . 157 . 181
288901	5 . 5 . 29 . 37 . 53 . 149 . 197
299399	5 . 5 . 5 . 5 . 13 . 29 . 37 . 53 . 97
307519	5 . 13 . 17 . 17 . 29 . 29 . 41 . 73
343066	5 . 13 . 17 . 17 . 17 . 41 . 89 . 101
345094	5 . 13 17 . 37 . 113 . 149 . 173
361409	5 . 13 . 17 . 53 . 61 . 101 . 181
375967	5 . 17 . 37 . 53 . 61 . 149
401444	5 . 13 . 17 . 17 . 29 . 29 . 101 . 101
408628	41 . 53 . 89 . 89 . 89 . 109
415848	13 . 17 . 17 . 37 . 101 . 109 . 113
417317	13 . 41 . 61 . 113 . 137 . 173
428021	5 . 13 . 37 . 41 . 61 . 97 . 157
448976	5 . 5 . 5 . 17 . 61 . 89 . 101 . 173
462953	29 . 41 . 53 . 101 . 113 . 149
521044	5 . 13 . 13 . 17 . 17 . 73 . 97 . 157
527329	5 . 17 . 37 . 61 . 61 . 109 . 109
658576	5 . 5 . 13 . 13 . 13 . 13 . 53 . 73 . 157
689601	5 . 5 . 5 . 37 . 41 . 73 . 89 . 193
788493	13 . 41 . 109 . 157 . 173 . 197
935601	5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 29 . 41 . 41
979976	5 . 5 . 5 . 5 . 17 . 17 . 137 . 197 197
1055864	5 . 13 . 17 . 29 . 37 . 53 . 113 . 157

1538221	5 . 13 . 13 . 29 . 53 . 61 . 109 . 137
1686759	5 . 13 . 29 . 29 . 41 . 41 . 113 . 137
2001229	5 . 13 . 17 . 29 . 41 . 53 . 149 . 193
2446492	13 . 41 . 73 . 89 . 101 . 109 . 157
3254151	5 . 5 . 13 . 17 . 29 . 41 . 61 . 73 . 181
3297075	37 . 41 . 53 . 53 . 73 . 101 . 173
3643774	5 . 5 . 5 . 13 . 17 . 41 . 109 . 137 . 157
4515359	5 . 13 . 13 . 13 . 17 . 17 . 113 . 157 . 181
5307581	5 . 17 . 37 . 53 . 73 . 73 . 101 . 157
5456999	5 . 5 . 41 . 73 . 73 . 101 . 137 . 197
7936717	13 . 29 . 37 . 41 . 41 . 41 . 181 . 181
8555207	13 . 17 . 41 . 53 61 . 73 . 109 . 157
12448726	5 . 5 5 . 5 . 13 . 13 . 13 . 41 . 89 . 157 . 197
21432319	5 . 17 . 37 . 73 . 149 . 173 . 197 . 197
40407039	5 . 17 . 37 . 41 . 53 . 89 . 97 . 101 . 137
41719774	5 . 5 . 5 . 17 . 17 . 29 . 29 . 41 . 41 . 173 . 197

118135085 | 17 17 . 37 . 41 . 61 . 101 . 109 . 137 . 173

5	1. 24
13	4. 9. 17
17	6. 11. 23. 74. 601. 8149
29	3. 26. 61. 113. 351. 844
37	5. 32. 69. 79. 264. 550. 1031. 1179
41	19. 22. 101. 142. 186. 227. 555. 1621. 4324. 935601*
53	2. 51. 55. 104. 108. 316. 634. 691
61	16. 45. 106. 199. 321. 809. 899. 2151. 2578. 2851*. 20297
73	30. 43. 103. 116. 176. 249. 554. 992. 4556. 4715*. 5226. 8219. 10761. 14351. 25726. 217351. 307519
89	29. 60. 149. 594. 919. 1128. 1395. 1751. 3709. 4657*. 10651. 12489. 21834. 39901
97	40. 57. 137. 251. 719. 1221. 1592. 4034. 5101. 7914*. 9837. 31274. 43416. 80841. 88989. 213263. 299399
101	31. 171. 334. 373. 474. 839. 979. 1041. 2595. 6029*. 6899. 8251. 32491. 44976. 51176. 141633. 157995. 167124. 343066. 401444*
109	13. 96. 449. 641. 776. 1186. 1949. 4918. 6309. 7316*. 8515. 30424. 33258. 46229. 73043. 124029. 408628. 527329
113	8. 121. 234. 331. 347. 799. 1009. 1364. 1929. 2607*. 2817. 2930. 3156. 4286. 6998. 8919. 10630. 13329. 18976. 22156. 27564*. 29501. 34134. 58881. 64644. 89149. 131863. 231755. 273694. 415848
137	15. 122. 152. 289. 533. 1111. 2999. 3547. 4399. 5191*. 7276. 14811. 17247. 18099. 44677. 73721. 133149. 160168. 163609. 166851*. 1538221. 1686759. 40407039
149	10. 139. 159. 606. 1629. 1649. 2076. 2374. 4778. 4927*. 7440. 9546. 10291. 10887. 11185. 35303. 37836. 72851. 375967. 462953*
157	39. 118. 589. 667. 1374. 1609. 1766. 4749. 8753. 9616*. 15425. 16446. 19743. 20999. 27200. 41801. 48317. 55774. 67785. 69983*. 73672. 138199. 150681. 428021. 521044. 658576. 1055864. 2446492. 3643774. 5307581*. 8555207
173	41. 132. 214. 824. 906. 1252. 1689. 2381. 3501. 5841*. 9301. 9993. 12151. 15356. 26337. 27721. 37409. 64051. 154876. 178149*. 207814. 345094. 417317. 448976. 3297075. 118135085
181	48. 229. 314. 676. 2944. 3753. 4211. 4754. 10727. 11632*. 25931. 26016. 30179. 38601. 41859. 49099. 50632. 82307. 281226. 361409*. 3254151. 4515359. 7936717
193	12. 181. 205. 374. 591. 1556. 2521. 3100. 4065. 6381*. 6574. 14656. 16393. 22569. 35524. 88213. 88406. 92049. 139551*. 174074. 189538. 689601. 2001229
197	99. 295. 296. 2069. 2659. 3251. 4629. 4630. 5024. 5221*. 6008. 9161. 13101. 15661. 21768. 29254. 35361. 36149. 54274. 76534*. 83430. 87369. 102735. 148439. 150410. 179565. 187249. 288901. 788493. 979976*. 5456999. 12448726. 21432319. 41719774

Factorable $aa + 64$.

1	5 . 13
3	73
5	89
7	113
9	5 . 29
11	5 . 37
15	17 . 17
19	5 . 5 . 17
21	5 . 101
25	13 . 53
27	13 . 61
29	5 . 181
31	5 . 5 . 41
49	5 . 17 . 29
51	5 . 13 . 41
53	13 . 13 . 17
63	37 . 109
67	29 . 157
69	5, 5 . 193
79	5 . 13 . 97
81	5 . 5 . 5 . 53
85	37 . 197
95	61 . 149
115	97 . 137
121	5 . 17 . 173
131	5 . 5 . 13 . 53
149	5 . 61 . 73
155	13 . 17 . 109
159	5 . 37 . 137
181	5 . 5 . 13 . 101
183	13 . 29 . 89
219	5 . 5 . 17 . 113
223	17 . 29 . 101
233	5 . 37 . 113
281	5 . 5 . 29 . 109
309	5 . 97 . 197
339	5 . 13 . 29 . 61
359	5 . 17 . 37 . 41
381	5 . 5 . 37 . 157
389	5 . 13 . 17 . 137
391	5 . 13 . 13 . 181
393	17 . 61 . 149
433	37 . 37 . 137
441	5 . 13 . 41 . 73
455	29 . 37 . 193

461	5 . 17 . 41 . 61
467	13 . 97 . 173
529	5 . 17 . 37 . 89
571	5 . 13 . 29 . 173
581	5 . 5 . 5 . 37 . 73
661	5 . 17 . 53 . 97
703	13 . 193 . 197
707	41 . 89 . 137
717	53 . 89 . 109
729	5 . 13 . 13 . 17 . 37
831	5 . 5 . 5 . 5 . 5 . 13 . 17
873	53 . 73 . 197
879	5 . 29 . 73 . 73

911	5 . 13 . 113 . 113
937	13 . 17 . 29 . 137
989	5 . 13 . 101 . 149
1035	17 . 29 . 41 . 53
1097	41 . 149 . 197
1141	5 . 17 . 17 . 17 . 53
1169	5 . 5 . 5 . 13 . 29 . 29
1171	5 . 13 . 17 . 17 . 73
1191	5 . 53 . 53 . 101
1247	13 . 37 . 53 . 61
1343	29 . 37 . 41 . 41
1419	5 . 5 . 5 . 89 . 181
1491	5 . 37 . 61 . 197
1589	5 . 41 . 109 . 113
1609	5 . 41 . 73 . 173
1613	13 . 17 . 61 . 193
1637	13 13 . 101 . 157
1681	5 . 5 . 17 . 61 . 109
1691	5 . 13 . 29 . 37 . 41
1749	5 . 17 . 17 . 29 . 73
1839	5 . 37 . 101 . 181
1861	5 . 37 . 97 . 193
1999	5 . 41 . 101 . 193
2019	5 . 5 . 41 . 41 . 97
2041	5 . 73 . 101 . 113
2055	13 . 17 . 97 . 197
2081	5 . 5 . 5 . 5 . 13 . 13 41
2131	5 . 5 . 13 . 89 . 157
2201	5 . 53 . 101 . 181
2445	13 . 29 . 101 . 157
2479	5 . 73 . 113 . 149
2601	5 . 13 . 29 . 37 . 97
2625	5 . 13 . 53 . 73 . 137

2771	5 . 73 . 109 . 193
2989	5 . 13 . 13 . 97 . 109
3171	5 . 13 . 37 . 37 . 113
3199	5 . 13 . 29 . 61 . 89
3413	29 . 41 . 97 . 101
3721	5 . 17 . 29 . 41 . 137
4031	5 . 5 . 13 . 17 . 17 . 173
4061	5 . 17 . 17 . 101 . 113
4109	5 . 13 . 13 . 13 . 29 . 53
4315	13 41 . 181 . 193
4419	5 . 5 . 5 . 13 . 61 . 197
4541	5 . 17 . 41 . 61 . 97
4979	5 . 29 . 37 . 97 . 157
5097	13 . 61 . 181 . 181
5169	5 . 5 . 5 . 37 . 53 . 109
5381	5 . 5 . 13 . 41 . 41 . 53
5459	5 . 13 . 17 . 149 . 181
5761	5 . 17 . 37 . 61 . 173
5869	5 . 5 . 89 . 113 . 137
6081	5 . 5 . 5 . 29 . 101 . 101
7781	5 . 5 . 29 . 37 . 37 . 61
9039	5 . 29 . 37 . 97 . 157
9779	5 . 37 . 73 . 73 . 97
10519	5 . 37 . 37 . 53 . 61
10527	41 . 109 . 137 . 181
10831	5 . 5 . 5 . 5 . 17 . 61 . 181
11511	5 . 17 . 41 . 193 . 197
13331	5 . 5 . 5 . 5 . 5 . 29 . 37 . 53
13581	5 . 5 . 5 . 17 . 29 41 . 73
13889	5 . 41 . 89 . 97 . 109
13911	5 . 13 . 13 . 29 . 53 . 149
14451	5 . 29 . 73 . 109 . 181
16069	5 . 5 . 13 . 37 . 109 . 197
16985	17 . 29 . 53 . 61 . 181
17421	5 . 13 . 137 . 173 . 197
18511	5 . 13 . 17 . 17 . 17 . 29 . 37
18563	13 . 37 . 41 . 101 . 173
18685	17 . 29 . 73 . 89 . 109
24061	5 . 29 . 29 . 37 . 61 . 61
24261	5 . 17 . 17 . 37 . 101 . 109
27665	13 37 . 41 . 197 . 197
29019	5 . 5 . 37 . 53 . 89 . 193
29981	5 . 5 . 37 . 41 . 137 . 173
31669	5 . 5 . 5 . 5 . 13 . 17 . 53 . 137
58397	13 . 17 . 29 . 37 . 73 . 197
59279	5 . 13 . 53 . 73 . 89 . 157
88789	5 . 13 17 . 29 . 37 . 61 . 109
103481	5 . 5 . 13 . 13 . 17 . 29 . 53 . 97

132081	5 . 5 . 5 . 5 . 5 . 5 . 5 . 13 . 89 . 193
170529	5 . 17 . 29 . 41 . 53 . 61 . 89
213331	5 . 5 . 5 . 5 . 5 . 13 . 13 . 17 . 37 . 137
383229	5 . 17 . 17 . 61 . 89 . 97 . 193
728391	5 . 13 . 73 . 97 . 101 . 101 . 113
1934581	5 . 5 . 5 . 5 . 13 . 17 . 17 . 17 . 29 . 53 . 61
2446081	5 . 5 . 5 . 13 . 17 . 17 . 37 . 53 . 73 . 89
4056181	5 . 5 . 13 . 17 . 29 . 41 . 101 . 137 . 181
5106581	5 . 5 . 5 . 13 . 17 . 37 . 41 . 61 . 101 . 101
14836119	5 . 5 . 13 . 13 . 17 . 17 . 17 . 17 . 29 . 137 . 157

13	1
17	15. 19. 53. 831
29	9. 49. 1169
37	11. 729. 18511
41	31. 51. 359. 1343. 1691. 2081
53	25. 81. 131. 1035. 1141. 4109. 5381. 13331
61	27. 339. 461. 1247. 7781. 10519. 24061. 1934581
73	3. 149. 441. 581. 879. 1171. 1749. 13581
89	5. 183. 529. 3199. 170529. 2446081
97	79.661. 2019. 2601. 4541. 9779. 103481
101	21. 181. 223. 1191. 3413. 6081. 5106581
109	63. 155. 281. 717. 1681. 2989. 5169. 13889. 18685. 24261*. 88789
113	7. 219. 233. 911. 1589. 2041. 3171. 4061. 728391
137	115. 159. 389. 433. 707. 937. 2625. 3721. 5869. 31669*. 213331
149	95. 393. 989. 2479. 13911
157	67. 381. 1637. 2131. 2445. 4979. 9039. 59279. 1483619
173	121. 467. 571. 1609. 4031. 5761. 18563. 29981
181	29. 391. 1419. 1839. 2201. 5097. 5459. 10527. 10831. 14451*. 16985. 4056181
193	69. 455. 1613. 1861. 1999. 2771. 4315. 29019. 132081. 383229
197	85. 309. 703. 873. 1097. 1491. 2055. 4419. 11511. 16069*. 17421. 27665. 58397

Factorable $aa + 81$.

1	41
2	5 . 17
4	97
5	53
7	5 . 13
8	5 . 29
10	181
11	101

13	5 . 5 . 5
17	5 . 37
19	13 . 17
20	13 . 37
22	5 . 113
23	5 . 61
28	5 . 173
32	5 . 13 . 17
37	5 . 5 . 29
38	5 . 5 61
40	41 . 41
43	5 . 193
49	17 . 73
50	29 . 89
53	5 . 17 . 17
58	5 . 13 . 53
59	13 . 137
62	5 . 5 . 157
71	13 . 197
79	29 . 109
83	5 . 17 . 41
91	37 . 113
95	29 . 157
97	5 · 13 . 73
98	5 . 13 . 149
101	53 . 97
112	5 . 5 . 5 . 101
122	5 . 41 . 73
124	13 . 29 . 41
128	5 . 37 . 89
137	5 . 5 . 13 . 29
139	89 . 109
163	5 . 5 . 13 . 41
188	5 . 5 . 13 . 109
191	101 . 181
202	5 . 13 . 17 . 37
215	13 . 13 . 137
217	5 . 53 . 89
247	5 . 41 . 149
248	5 . 109 . 113
253	5 . 13 . 17 . 29
268	5 . 73 . 197
287	5 . 5 . 17 . 97
292	5 . 13 . 13 . 101
313	5 . 5 . 37 . 53
317	5 . 89 . 113
323	5 . 53 . 197
352	5 . 137 . 181

376	17 . 53 . 157
389	17 . 61 . 73
406	17 . 89 . 109
409	13 . 41 . 157
427	5 . 17 . 29 . 37
461	13 . 13 . 17 . 37
472	5 . 29 . 29 . 53
487	5 . 5 . 5 . 13 . 73
491	17 . 41 . 173
533	5 . 157 . 181
547	5 . 173 . 173
553	5 . 13 . 13 . 181
566	13 . 157 . 157
575	37 . 41 . 109
578	5 . 13 . 53 . 97
587	5 . 5 . 61 . 113
617	5 . 13 . 29 . 101
631	13 . 17 . 17 . 53
662	5 . 5 . 89 . 197
683	5 . 13 . 37 . 97
694	53 . 61 . 149
733	5 . 17 . 29 . 109
737	5 . 5 . 5 . 41 . 53
763	5 . 5 . 5 . 17 . 137
797	5 . 17 . 37 . 101
862	5 . 5 . 5 . 5 . 29 . 41
877	5 . 13 . 61 . 97
920	17 . 17 . 29 . 101
1018	5 . 17 . 89 . 137
1037	5 . 5 . 137 . 157
1060	13 . 13 . 61 . 109
1108	5 . 41 . 53 . 113
1118	5 . 53 . 53 . 89
1168	5 . 29 . 97 . 97
1201	37 . 101 . 193
1229	13 . 13 . 41 . 109
1243	5 . 17 . 61 . 149
1265	73 . 97 . 113
1277	5 . 17 . 53 . 181
1313	5 . 5 . 29 . 29 . 41
1436	13 . 41 . 53 . 73
1447	5 . 17 . 109 . 113
1463	5 . 5 . 13 . 37 . 89
1475	13 . 13 . 41 . 157
1487	5 . 5 . 5 . 5 . 29 . 61
1585	53 . 137 . 173
1639	41 . 181 . 181
1645	13 . 29 . 37 . 97

1685	17 . 37 . 37 . 61
1702	5 . 17 . 173 . 197
1703	5 . 29 . 73 . 137
1787	5 . 5 . 13 . 17 . 17 . 17
1807	5 . 53 . 61 . 101
2008	5 . 13 . 17 . 41 . 89
2009	13 . 29 . 53 . 101
2041	97 . 109 . 197
2051	29 . 29 . 41 . 61
2125	13 . 29 . 53 . 113
2138	5 . 5 . 5 . 13 . 29 . 97
2293	5 . 17 . 157 . 197
2312	5 . 5 . 29 . 73 . 101
2450	13 . 17 . 157 . 173
2531	17 . 29 . 73 . 89
2623	5 . 41 . 97 . 173
2705	17 . 29 . 41 . 181
2888	5 . 5 . 5 . 5 . 5 . 17 . 157
2906	13 . 37 . 97 . 181
3088	5 . 5 . 13 . 13 . 37 . 61
3238	5 . 5 . 41 . 53 . 193
3322	5 . 13 . 41 . 41 . 101
3347	5 . 13 . 17 . 37 . 137
3503	5 . 13 . 13 . 53 . 137
3517	5 . 13 . 17 . 29 . 193
3791	29 . 37 . 37 . 181
3988	5 . 5 . 29 . 97 . 173
4010	13 . 13 . 17 . 29 . 193
4112	5 . 5 . 5 . 17 . 73 . 109
4354	17 . 61 . 101 . 181
4388	5 . 5 . 5 . 13 . 17 . 17 . 41
4429	29 . 41 . 73 . 113
4648	5 . 13 . 29 . 73 . 157
4657	5 . 101 . 109 . 197
4837	5 . 5 . 41 . 101 . 113
5083	5 . 29 . 41 . 41 . 53
5162	5 . 5 . 61 . 101 . 173
5557	5 . 13 . 17 . 89 . 157
5747	5 . 109 . 157 . 193
5792	5 . 13 . 13 . 29 . 37 . 37
5833	5 . 17 . 17 . 61 . 193
6013	5 . 5 . 5 . 5 . 5 . 5 . 13 . 89
6233	5 . 13 . 37 . 41 . 197
6458	5 . 17 . 37 . 89 . 149
6532	5 . 5 . 37 . 113 . 157
6689	13 . 97 . 113 . 157
6883	5 . 13 . 13 . 17 . 17 . 97
7097	5 . 29 . 29 . 53 113

7160	53 . 61 . 101 . 157
7793	5 . 13 . 29 . 89 . 181
8158	5 . 13 . 13 . 17 . 41 . 113
8273	5 . 29 . 53 . 61 . 73
8638	5 . 5 . 5 . 13 . 17 . 37 . 73
9028	5 . 13 . 73 . 89 . 193
9101	41 . 73 . 101 . 137
9295	61 . 73 89 . 109
9562	5 . 5 . 13 . 29 . 89 . 109
9587	5 . 5 . 13 . 13 . 73 . 149
9607	5 . 17 . 29 . 97 . 193
10118	5 . 37 . 53 . 53 . 197
10577	5 . 29 . 41 . 97 . 97
11563	5 . 5 13 29 . 41 . 173
12143	5 . 29 . 29 . 89 . 197
12565	13 . 17 . 29 . 109 . 113
15233	5 . 29 . 73 . 97 . 113
16237	5 . 5 . 5 . 17 . 17 . 41 . 89
16522	5 . 17 . 29 . 37 . 41 . 73
16777	5 . 13 . 13 . 17 . 97 . 101
17888	5 . 5 . 5 5 . 37 . 101 . 137
17972	5 . 13 . 29 . 53 . 53 . 61
18887	5 . 5 . 29 . 37 . 61 . 109
18974	13 . 13 . 17 . 29 . 29 . 149
19558	5 . 13 . 13 . 41 . 61 . 181
20362	5 . 5 . 5 . 113 . 149 . 197
23368	5 . 13 . 13 . 53 . 89 . 137
24083	5 . 13 . 157 . 157 . 181
24499	13 . 17 . 61 . 113 . 197
24958	5 . 17 . 37 . 37 . 53 . 101
29153	5 . 13 . 17 . 29 . 89 . 149
29242	5 . 17 . 17 . 61 . 89 . 109
29765	17 . 37 . 41 . 89 . 193
30218	5 . 13 . 41 . 41 . 61 . 137
31487	5 . 5 . 5 . 5 . 5 . 41 . 53 . 73
31843	5 . 13 . 17 . 17 . 137 . 197
34763	5 . 5 . 5 . 5 . 17 . 29 . 37 . 53
35137	5 . 5 . 17 . 73 . 101 . 197
35783	5 . 13 . 17 . 17 . 173 . 197
37147	5 . 13 . 17 . 41 . 97 . 157
38201	13 . 17 . 17 . 29 . 37 . 181
44987	5 . 5 . 5 . 13 . 29 . 109 . 197
46963	5 . 5 . 13 . 29 . 29 . 53 . 73
56387	5 . 5 . 13 . 17 . 53 . 61 . 89
57037	5 . 5 . 13 . 17 . 37 . 73 . 109
60743	5 . 13 . 17 . 17 . 17 . 53 . 109
61337	5 . 5 . 41 . 109 . 113 . 149
69107	5 . 17 . 53 . 53 . 73 . 137

69244	13 . 13 . 29 . 37 . 137 . 193
79813	5 . 5 . 13 . 17 . 53 . 73 . 149
86528	5 . 17 . 29 . 97 . 173 . 181
87263	5 . 5 . 5 . 5 . 5 . 13 . 17 . 37 . 149
97577	5 . 29 . 61 . 73 . 73 . 101
98063	5 . 5 . 73 . 97 . 157 . 173
121933	5 . 13 41 . 97 . 149 . 193
132683	5 . 17 . 29 . 109 . 181 . 181
157723	5 . 13 . 13 . 29 . 53 . 61 . 157
168703	5 . 37 . 37 . 61 . 173 . 197
181508	5 . 41 . 41 . 101 . 197 . 197
195787	5 . 5 . 13 . 17 . 29 . 37 . 53 . 61
237322	5 . 13 . 13 . 13 . 17 . 17 . 113 . 157
269861	13 . 37 . 41 . 101 . 101 . 181
278297	5 . 5 . 13 . 37 . 97 . 113 . 113
297212	5 . 5 . 13 . 97 . 113 . 137 . 193
314387	5 . 5 . 41 . 41 . 73 . 89 . 181
327737	5 . 5 . 5 . 5 . 13 . 13 . 29 . 89 . 197

349487	5 . 5 . 5 . 29 . 29 . 53 . 97 . 113
474013	5 . 5 . 5 . 13 . 17 . 17 . 29 . 73 . 113.
609161	13 . 73 . 73 . 113 . 137 . 173
647665	29 . 37 . 53 . 97 . 193 . 197
934862	5 . 5 . 5 . 13 . 13 . 17 . 17 . 37 . 53 . 73
1125533	5 . 13 . 41 . 89 . 101 . 137 . 193
1158413	5 . 5 . 29 . 37 . 41 . 61 . 73 . 137
1880912	5 . 5 . 13 . 17 . 37 . 53 . 53 . 61 . 101
2023513	5 . 5 . 5 . 5 . 37 . 41 . 97 . 113 . 197
2092285	17 . 17 . 37 . 37 . 37 . 41 . 41 . 89
2898587	5 . 5 . 17 . 29 . 73 . 137 . 173 . 197
3559861	13 . 37 . 61 . 89 . 109 . 113 . 197
4034153	5 . 13 . 13 . 17 . 29 . 41 . 53 . 89 . 101
4676188	5 . 5 . 17 . 37 . 37 . 37 . 89 . 101 . 113
4802183	5 . 73 . 97 . 109 . 113 . 137 . 193
4947916	17 . 17 . 37 . 53 . 61 . 73 . 89 . 109
6678737	5 . 5 . 5 . 17 . 17 . 29 . 41 . 53 . 97 . 101
9578563	5 . 5 . 13 . 17 . 17 . 17 . 29 . 61 . 109 . 149
34928797	5 . 13 . 13 . 17 . 29 . 37 . 53 . 53 . 73 . 193
59554033	5 . 13 . 13 . 13 . 37 . 61 . 73 . 89 . 101 . 109

5	13
13	7
17	2. 19. 32. 53. 1787
29	8. 37. 137. 253
37	17. 20. 202. 427. 461. 5792

41	1. 40. 83. 124. 163. 862. 1313. 4388
53	5. 58. 313. 472. 631. 737. 5083. 34763
61	23. 38. 1487. 1685. 2051. 3088. 17972. 195787
73	49. 97. 122. 389. 487. 1436. 8273. 8638. 16522. 31487. 46963. 934862
89	50. 128. 217. 1118. 1463. 2008. 2531. 6013. 16237. 56387. 2092285
97	4. 101. 287. 578. 683. 877. 1168. 1645. 2138. 6883. 10577
101	11. 112. 292. 617. 797. 920.1807. 2009. 2312. 3322. 16777. 24958. 97577. 1880912. 4034153. 6678737
109	79. 139. 188. 406. 575. 733. 1060. 1229. 4112. 9295. 9562. 18887. 29242. 57037. 60743. 4947916. 59554033
113	22. 91. 248. 317. 587. 1108. 1265. 1447. 2125. 4429. 4837. 7097. 8158. 12565. 15233. 278297. 349487. 474013. 4676188
137	59. 215. 763. 1018. 1703. 3347. 3503. 9101. 17888. 23368. 30218. 69107. 1158413
149	98. 247. 694. 1243. 6458. 9587. 18974. 29153. 61337. 79813. 87263. 9578563
157	62. 95. 376. 409. 566. 1037. 1475. 2888. 4648. 5557. 6532. 6689. 7160. 37147. 157723. 237322
173	28. 491. 547. 1585. 2450. 2623. 3988. 5162. 11563. 98063. 609161
181	10. 191. 352. 533. 553. 1277. 1639. 2705. 2906. 3791. 4354. 7793. 19558. 24083. 38201. 86528. 132683. 269861. 314387
193	43. 1201. 3238. 3517. 4010. 5747. 5833. 9028. 9607. 29765. 69244. 121933. 297212. 1125533. 4802183. 34928797
197	71. 268. 323. 662. 1702. 2041. 2293. 4657. 6233. 10118. 12143. 20362. 24499. 31843. 35137. 35783. 44987. 168703. 181508. 327737. 647665. 2023513. 2898587. 3559861

A NEW QUADRATURE OF THE CIRCLE.

I. Acotg .5 = (2) − (13).

26684971	0210071265	7279572372	8848455203	4183360499	1499728341	833
	364	7220869565	2173913043	4782608695	6521739130	434
		4977954329	5694145758	6618876941	4575866188	769
		(43)	204560302	8420465116	2790697674	418
		(47)	299441	4645858042	5531914893	617
		(51)	441	5293752324	0156862745	098
		(55)	6550690367	0843578181	818	
		(59)	9770521	2254817540	338	
		(63)	14640	2730743726	600	
		(67)	22	0259630730	860	
		(71)	332561019	920		
		(75)	503719	091		
		(79)	765	142		
		(83)	1	165		
		(87)	1			
26684971	0210071630	9478396268	6921374192	0505397169	7498644659	104
0,2000640569	5190437336	8654456654	4566544566	5445665445	6654456654	456
	7710131	0688316235	2941176470	5882352941	1764705882	352
		185127900	6896551724	1379310344	8275862068	965
		266673	0412205651	4831745270	7696610135	634
			7830238	1276333963	9002267573	696
		(53)	16	9947155749	8300377358	490
		(57)	252833663	2909752140	350	
		(61)	378007	0506907695	003	
		(65)	567	5921253449	092	
		(69)	8555011744	329		
		(73)	12937990	364		
		(77)	19625	419		
		(81)	29	850		
		(85)	45			
0,2000640569	5198147467	9528161463	4824308667	9015775954	9600162348	045
26684971	0210071630	9478396268	6921374192	0505397169	7498644659	104
0,1973955598	4988075837	0049765194	7902934475	8510378785	2101517688	941

II. $\operatorname{Acotg} .70 = 2(2) - 2(13) - (29)$

0,0142857142	8571428571	4285714285	7142857142	8571428571	4285714285	714
3) 29154	5189504373	1778425655	9766763848	3965014577	2594752186	588
5) 5	9499018266	1986077229	7257095257	9282441839	7096447908	609
7) 12142656	7890201240	2509644305	1546792335	0693284989	369	
9) 2478	0932222490	0490308090	6745213631	0887896588	773	
11) 5057333106	6306222511	8552396982	3736915897	263		
13) 1032108	7972715555	6146643346	3229334064	468		
15) 210	6344484227	6644111559	8665965170	217		
17) 429866221	2709519206	4407891013	300			
19) 87727	8002593779	4298858753	268			
21) 17	9036327059	9549856909	949			
23) 36538025	9306030583	042				
25) 7456	7399858373	588				
27) 1	5217836705	790				
29) 3105680	960					
31) 633	812					
33) 128						
9718	1729834791	0592808551	9922254616	1321671525	7531584062	196
1734665	2555743034	3215663472	1649541762	1527612141	338	
459757555	1482383864	7141126998	3976083263	387		
14	0422965615	1776274103	9911064344	681		
4617	2526452304	1805203092	277			
1588609	8230696981	871				
563623581	695					
20	447					
9718	1731569456	3608309155	5043272185	4416655304	3545867487	890
0,0142857142	8571428571	4285714285	7142857142	8571428571	4285714285	714
1	1899803653	2397215445	9451419051	5856488367	9419289581	721
275	3436913610	0054478676	7416134847	8987544065	419	
79392	9844055042	7395895642	0248410312	651		
25286248	3100559953	3200464177	252			
8525539383	8073802709	997				
298	2695994334	943				
107092	446					
3						
0,0142857144	0471232500	0119922734	6518096163	0866047064	6911326560	146
9718	1731569456	3608309155	5043272185	4416655304	3545867487	890
0,0142847425	8739663043	6511613579	1474823977	6449391760	3365459072	256

III. $\operatorname{Acotg} .99 = -(2) + 2(13) - (29).$

0,0101010101	0101010101	0101010101	0101010101	0101010101	0101010101	010
3) 10306	1015212836	4555667892	0621375472	9212335579	0228548210	397
5) 1	0515357128	1335022514	8344109925	0559046254	0127571528	232
7) 1072886	1471414653	8633643925	1020361090	3228255032	295	
9) 109	4670081768	6617552662	3737477845	2290911973	781	
11) 111689631	8506950061	4898861083	3430495960	817		
13) 11395	7383788077	7534424942	4633550708	689		
15) 1	1627118027	5561425816	2373699984	767		
17) 1186319	5620402145	2725474308	742			
19) 121	0406654464	0491044329	589			
21) 123498281	2431434654	048				
23) 12600	5796595391	761				
25) 1	2856422466	625				
27) 1311745	991					
29) 133	837					
31) 13						
3435	3671737612	1518555964	0207125157	6404111859	6776182736	799
153269	4495916379	1233377703	5860051584	3318322147	470	
10153602	8955177278	3172623734	8493681450	983		
775141201	8370761721	0824913332	317			
6	3705613392	8446897069	978			
547	8512895451	815				
48583	184					
3435	3671890881	6024625946	1170821347	7513162840	6372940772	546
0,0101010101	0101010101	0101010101	0101010101	0101010101	0101010101	010
2103071425	6267004502	9668821985	0111809250	8025514305	646	
12	1630099085	4068616962	4859719760	5810101330	420	
876	5952599082	9041109610	9587196208	360		
69783	5036494243	8395616135	808			
5880870	5353877840	668				
514256898	665					
4	615					
0,0101010101	2204081538	7998024565	9791117914	9156023837	7787572825	192
3435	3671890881	6024625946	1170821347	7513162840	6372940772	546
0,0101006665	8532190657	1973398619	8620296567	1642860997	1414632052	646

IV. $\operatorname{Acotg} .307 = -3(2) + 3(5) + (13) + (29).$

	0,0032573289	9022801302	9315960912	0521172638	4364820846	9055374592	833
	3)	345 6088648397	3443000295	0769987174	1094169326	1556823471	597
	5)	36669764	6489336152	1087234559	3817877050	8899421286	416
	7)	389 0732490417	2580304164	8671007839	6274855960	501	
	9)	41281419	3298311709	4522474201	4009658191	131	
	11)	438 0037913381	6985798496	2620441698	672		
	13)	46473043	8878046300	7405517516	808		
	15)	493 0879254719	3742187243	551			
	17)	52317576	3638805103	367			
	19)	555	9995380734	067			
	21)	58897127	616				
	23)	624	909				
0,0032	115	2029549465	7814333365	0256662391	3698056442	0518941157	199
	55	5818927202	4654329166	4095858262	8039265137	214	
	39	8185264852	8816890772	3874585608	970		
	32	8725283647	9582812482	903			
	29	2157651617	582				
	27	169					
	115	2029549521	3633260607	3096256443	5336089154	4173256031	037
	0,0032573289	9022801302	9315960912	0521172638	4364820846	9055374592	833
	7333952	9297867230	4217446911	8763575410	1779884257	283	
	4586824	3699812412	1613608244	6001073132	347		
	3574849	5298311253	9031193655	139			
	3077504	4919929711	962				
	2804625	124					
	0,0032573289	9030135255	8618414966	8442006812	0043393260	0790259974	688
	115	2029549521	3633260607	3096256443	5336089154	4173256031	037
	0,0032573174	7000585734	4985154359	5345750368	4707304105	6617003943	651

TABLE OF ARCS CORRESPONDING TO GIVEN PRIME TANGENTS
IN UNITS OF THE RADIUS, TO 110 DIGITS.

2	0,7853981633	9744830961	5660845819	8757210492	9234984377	6455243736	1480769541	
5	0,4636476090	0080611621	4256231461	2144020285	3705428612	0263810933	0887201978	6
13	0,5880026035	4756755124	5611080625	0854276017	0724605592	4353726047	2072	
17	0,2449786631	2686415417	2082481211					
29	0,3805063771	1236486630	3587916810	4331044974	0571365810	0837576305	623	
37	0,1651486774	1462683827	9128289643	9435540983	8			

ON CALCULATING COMMON LOGARITHMS.

Calculate the logarithms of

$$\log \frac{1025}{*} = a$$
$$\log \frac{1024^2}{*} = b$$
$$\log \frac{81^2}{*} = c$$
$$\log \frac{125^2}{*} = d$$
$$\log \frac{99^2}{*} = e$$

($*$ denotes a denominator that is 1 less than the numerator) then, as is easily checked:

$$\log 2 = \frac{14\frac{3}{4} + \frac{5}{4}a + 2b - \frac{3}{4}c - 2d + e}{49} = f$$

It is also easy to derive

$$\log 41 = a + 12f - 2 = g$$
$$\log 3 = \frac{1 + c + 4f + g}{8}$$

$\log 11 \,.\, 31$ and $\log \frac{11}{7}$ and thus also $\log 7 \,.\, 31$

$\frac{17}{23 \,.\, 73}$	$\frac{7}{23 \,.\, 73}$	$\frac{1680^2}{*}$	from this 73
$\frac{7 \,.\, 73}{17}$	$\frac{136000}{*}$	from these $\frac{7}{23}$	$\left[\text{and } \frac{7}{23},\ \frac{7}{17}\right]$
	$\frac{511^2}{*}$		
$7 \,.\, 7 \,.\, 43$	$\frac{512001}{*}$	$\frac{7 \,.\, 7}{17}$ from this and $\frac{7}{17}$	$\left[\text{and } \frac{7}{23}\right]$
$17 \,.\, 43$	$\frac{730^2}{*}$		

gives 7, 17, 23, 43

---

a,	$\frac{81}{8}$	$\frac{81}{80}$	
b,	$\frac{41}{4}$	$\frac{6561}{6560}$	
c,	2	$\frac{1025}{1024}$	
d,	7	$\frac{2401}{2400}$	
e,	29	$\frac{1681^2}{1680.1682}$	
f,	43	$\frac{512001}{512000}$	
g,	23 . 73	$\frac{1680^2}{1679.1681}$	
h,	17	$\frac{136000}{135999}$	
i,	73	$\frac{511^2}{510.512}$	$\frac{730^2}{729.731}$
k,	13	$\frac{729^2}{728.730}$	
l,	19	$\frac{512^2}{511.513}$	
m,	47	$\frac{2116^2}{2115.2117}$	
n,	61	$\frac{2500^2}{2499.2501}$	
o,	31	$\frac{17081^2}{17080.17082}$	
p,	11	$\frac{1024^2}{1023.1025}$	$\frac{2001^2}{2000.2002}$
q,	71	$\frac{10935^2}{10934.10936}$	
r,	53	$\frac{788800}{788799}$	
s,	67	$\frac{274700}{274699}$	$\frac{3751^2}{*}$
t,	37	$\frac{1000000}{999999}$	$\frac{1331^2}{1330.1332}$

u,	59	$\frac{3481^2}{3480.3481}$	
v,	89	$\frac{4095^2}{4094.4096}$	
w,	83	$\frac{6889^2}{6888.6890}$	
x,	79	$\frac{3879^2}{3880.3882}$	
y,	97	$\frac{13871^2}{13870.13872}$	$\frac{46656^2}{46655.46657}$

[How these fractions can be used to calculate the logarithms of the small primes listed beside them, using the very rapidly convergent series in still increasing powers of $\frac{1}{x}$ for $\log \frac{x}{x-1}$, follows directly from the example at the beginning.

For calculating the logarithms of the smallest primes 2, 3, 7 one can, moreover, obtain still more advantageous series by suitably combining these numbers of Gauss with those given by Huyghens (Hugenii, Opera varia, Lugduni 1724 p. 457) as follows:

2	1000
	$1024 = 2^{10}$
3	$32805 = 3^8 \,.\, 5$
	$32768 = 2^{15}$
7	$2400 = 100 \,.\, 2^3 \,.\, 3$
	$2401 = 7^4$
11	$9800 = 100 \,.\, 2 \,.\, 7^2$
	$9801 = 3^4 \,.\, 11^2$
13	$123200 = 100 \,.\, 2^4 \,.\, 7 \,.\, 11$
	$123201 = 3^6 \,.\, 13$
17	$2600 = 100 \,.\, 2 \,.\, 13$
	$2601 = 3^2 \,.\, 17^2$
19	$28899 = 3^2 \,.\, 13^2 \,.\, 19$
	$28900 = 100 \,.\, 17^2$
23	$25920 = 10 \,.\, 2^5 \,.\, 3^4$
	$25921 = 7^2 \,.\, 23^2$
29	$613088 = 2^5 \,.\, 7^2 \,.\, 17 \,.\, 23$
	$613089 = 3^6 \,.\, 29^2$

31 $116280 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 17 \,.\, 19.$
$116281 = 11^2 \,.\, 31$
37 $165648 = 2^4 \,.\, 3 \,.\, 7 \,.\, 17 \,.\, 29$
$165649 = 11^2 \,.\, 37$
41 $1413720 = 10 \,.\, 2^2 \,.\, 3^3 \,.\, 7 \,.\, 11 \,.\, 17$
$1413721 = 29^2 \,.\, 41^2$
43 $978120 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 11 \,.\, 13 \,.\, 19$
$978121 = 23^2 \,.\, 43^2$
47 $664848 = 2^5 \,.\, 3^6 \,.\, 7 \,.\, 13$
$664849 = 31^2 \,.\, 47^2$
53 $3059000 = 100 \,.\, 7 \,.\, 19 \,.\, 23$
$3059001 = 3^2 \,.\, 11^2 \,.\, 53^2$
59 $5851560 = 10 \,.\, 2^2 \,.\, 3 \,.\, 11^2 \,.\, 13 \,.\, 31$
$5851561 = 41^2 \,.\, 59^2$
61 $3575880 = 10 \,.\, 2^2 \,.\, 3^3 \,.\, 7 \,.\, 11 \,.\, 43$
$3575881 = 31^2 \,.\, 61^2$
67 $1620528 = 2^4 \,.\, 3 \,.\, 7^2 \,.\, 13$
$1620529 = 19^2 \,.\, 67^2$
71 $2016399 = 3 \,.\, 7^2 \,.\, 11 \,.\, 29 \,.\, 43$
$2016400 = 100 \,.\, 2^2 \,.\, 71^2$
73 $5116644 = 2^2 \,.\, 3^2 \,.\, 13^2 \,.\, 29^2$
$5116645 = 7 \,.\, 17 \,.\, 19 \,.\, 31 \,.\, 73$
79 $5997600 = 100 \,.\, 2^3 \,.\, 3^2 \,.\, 7^2 \,.\, 17$
$5997601 = 31^2 \,.\, 79^2$
83 $1164240 = 10 \,.\, 2^3 \,.\, 3^3 \,.\, 7^2 \,.\, 11$
$1164241 = 13^2 \,.\, 83^2$
89 $2859480 = 10 \,.\, 2^2 \,.\, 3^2 \,.\, 13^2 \,.\, 47$
$2859481 = 19^2 \,.\, 89^2.$
97 $1138488 = 2^3 \,.\, 3 \,.\, 13 \,.\, 41 \,.\, 89$
$1138489 = 11^2 \,.\, 97^2$

To calculate the logarithms of all primes less than 200 one can use to advantage the decompositions of $aa + 1$, $a + 2$, $.. aa + 81$ found in the tables for circle division, provided one restricts attention to the numbers a that themselves have only primes less than 200 as divisors. The other a can then be used to calculate the logarithms of the larger prime divisors occurring in them.]

POSTHUMOUS PAPERS. FIRST TEN THOUSAND SQUARES.

	10	20	30	40	50	60	70	80	90	
00	1000	4000	9000	16000	25000	36000	49000	64000	81000	000
1	02	04	06	08	10	12	14	16	18	001
2	04	08	12	16	20	24	28	32	36	004
3	06	12	18	24	30	36	42	48	54	009
4	08	16	24	32	40	48	56	64	72	016
5	10	20	30	40	50	60	70	80	81090	025
6	12	24	36	48	60	72	84	64096	81108	036
7	14	28	42	56	70	84	49098	64112	26	049
8	16	32	48	64	80	36096	49112	28	44	064
09	18	36	54	72	25090	36108	26	44	62	081
10	20	40	60	80	25100	20	40	60	80	100
1	22	44	66	88	10	32	54	76	81198	121
2	24	48	72	16096	20	44	68	64192	81216	144
3	26	52	78	16104	30	56	82	64208	34	169
4	28	56	84	12	40	68	49196	24	52	196
5	30	60	90	20	50	80	49210	40	70	225
6	32	64	9096	28	60	36192	24	56	81288	256
7	34	68	9102	36	70	36204	38	72	81306	289
8	36	72	08	44	80	16	52	64288	24	324
19	38	76	14	52	25190	28	66	64304	42	361
20	40	80	20	60	25200	40	80	20	60	400
1	42	84	26	68	10	52	49294	36	78	441
2	44	88	32	76	20	64	49308	52	81396	484
3	46	92	38	84	30	76	22	68	81414	529
4	1048	4096	44	16192	40	36288	36	64384	32	576
5	50	4100	50	16200	50	36300	50	64400	50	625
6	52	04	56	08	60	12	64	16	68	676
7	54	08	62	16	70	24	78	32	81486	729
8	56	12	68	24	80	36	49392	48	81504	784
29	58	16	74	32	25290	48	49406	64	22	841
30	60	20	80	40	25300	60	20	80	40	900
1	62	24	86	48	10	72	34	64496	58	961
2	65	29	93	57	21	85	49	64513	77	024
3	67	33	9199	65	31	36397	63	29	81595	089
4	69	37	9205	73	41	36409	77	45	81613	156
5	71	41	11	81	51	21	49491	61	31	225
6	73	45	17	89	61	33	49505	77	49	296
7	75	49	23	16297	71	45	19	64593	67	369
8	77	53	29	16305	81	57	33	64609	81685	444
39	79	57	35	13	25391	69	47	25	81703	521
40	81	61	41	21	25401	81	61	41	21	600
1	83	65	47	29	11	36493	75	57	39	681
2	85	69	53	37	21	36505	49589	73	57	764
3	87	73	59	45	31	17	49603	64689	75	849
4	89	77	65	53	41	29	17	64705	81793	936
5	92	82	72	62	52	42	32	22	81812	025
6	94	86	78	70	62	54	46	38	30	116
7	96	90	84	78	72	66	60	54	48	209
8	1098	94	90	86	82	78	74	70	66	304
94	1100	4198	9296	16394	25492	36590	49688	64786	81884	401

11	21	31	41	51	61	71	81	91	
1210	4410	9610	16810	26010	37210	50410	65610	82810	000
12	14	16	18	20	22	24	26	28	201
14	18	22	26	30	34	38	42	46	404
16	22	28	34	40	46	52	58	64	609
18	26	34	42	50	58	66	74	82882	816
21	31	41	51	61	71	81	65691	82901	025
23	35	47	59	71	83	50495	65707	19	236
25	39	53	67	81	37295	50509	23	37	449
27	43	59	75	26091	37307	23	39	55	664
29	47	65	83	26101	19	37	55	73	881
32	52	72	16892	12	32	52	72	82992	100
34	56	78	16900	22	44	66	65788	83010	321
36	60	84	08	32	56	80	65804	28	544
38	64	90	16	42	68	50594	20	46	769
40	68	9696	24	52	80	50608	36	64	996
43	73	9703	33	63	37393	23	53	83083	225
45	77	09	41	73	37405	37	69	83101	456
47	81	15	49	83	17	51	65885	19	689
49	85	21	57	26193	29	65	65901	37	924
52	90	28	66	26204	42	80	18	56	161
1254	94	34	74	14	54	50694	34	74	400
56	4498	40	82	24	66	50708	50	83192	641
58	4502	46	90	34	78	22	66	83210	884
61	07	53	16999	45	37491	37	83	29	129
63	11	59	17007	55	37503	51	65999	47	376
65	15	65	15	65	15	65	66015	65	625
67	19	71	23	75	27	79	31	83283	876
70	24	78	32	86	40	50794	48	83302	129
72	28	84	40	26296	52	50808	64	20	384
74	32	90	48	26306	64	22	80	38	641
76	36	9796	56	16	76	36	66096	56	900
79	41	9803	65	27	37589	51	66113	75	161
81	45	09	73	37	37601	65	29	83393	424
83	49	15	81	47	13	79	45	83411	689
85	53	21	89	57	25	50893	61	29	956
88	58	28	17098	68	38	50908	78	48	225
90	62	34	17106	78	50	22	66194	66	496
93	66	40	14	88	62	36	66210	83484	769
95	71	47	23	26399	75	51	27	83503	044
1297	75	53	31	26409	87	65	43	21	321
1299	79	59	39	19	37699	79	59	39	600
1301	83	65	47	29	37711	50993	75	57	881
04	88	72	56	40	24	51008	66292	76	164
06	92	78	64	50	36	22	66308	83594	449
08	4596	84	72	60	48	36	24	83612	736
11	4601	91	81	71	61	51	41	31	025
13	05	9897	89	81	73	65	57	49	316
15	09	9903	17197	26491	85	79	73	67	609
17	13	09	17205	26501	37797	51093	66389	83685	904
1320	4618	9916	17214	26512	37810	51108	66406	83704	201

	10	20	30	40	50	60	70	80	90	
50	1102	4202	9302	16402	25502	36602	49702	64802	81902	500
1	04	06	08	10	12	14	16	18	20	601
2	06	10	14	18	22	26	30	34	38	704
3	08	14	20	26	32	38	44	50	56	809
4	10	18	26	34	42	50	58	66	74	916
5	13	23	33	43	53	63	73	83	81993	025
6	15	27	39	51	63	75	49787	64899	82011	136
7	17	31	45	59	73	87	49801	64915	29	249
8	19	35	51	67	83	36699	15	31	47	364
59	21	39	57	75	25593	36711	29	47	65	481
60	23	43	63	83	25603	23	43	63	82083	600
1	25	47	69	91	13	35	57	79	82101	721
2	27	51	75	16499	23	47	71	64995	19	844
3	29	55	81	16507	33	59	49885	65011	37	969
4	32	60	88	16	44	72	49900	28	56	096
5	34	64	9394	24	54	84	14	44	74	225
6	36	68	9400	32	64	36796	28	60	82192	356
7	38	72	06	40	74	36808	42	76	82210	489
8	40	76	12	48	84	20	56	65092	28	624
69	42	80	18	56	25694	32	70	65108	46	761
70	1144	84	24	64	25704	44	84	24	64	900
1	47	89	31	73	15	57	49999	41	82283	041
2	49	93	37	81	25	69	50013	57	82301	184
3	51	4297	43	89	35	81	27	73	19	329
4	53	4301	49	16597	45	36893	41	65189	37	476
5	55	05	55	16605	55	36905	55	65205	55	625
6	57	09	61	13	65	17	69	21	73	776
7	59	13	67	21	75	29	83	37	82391	929
8	62	18	74	30	86	42	50098	53	82409	084
79	64	22	80	38	25796	54	50112	70	28	241
80	66	26	86	46	25806	66	26	65286	46	400
1	68	30	92	54	16	78	40	65302	64	561
2	70	34	9498	62	26	36990	54	18	82482	724
3	72	38	9504	70	36	37002	68	34	82500	889
4	75	43	11	79	47	15	83	51	19	056
5	77	47	17	87	57	27	50197	67	37	225
6	79	51	23	16695	67	39	50211	83	55	396
7	81	55	29	16703	77	51	25	65399	73	569
8	83	59	35	11	87	63	39	65415	82591	744
89	85	63	41	19	25897	75	53	31	82609	921
90	88	68	48	28	25908	37088	68	48	28	100
1	90	72	54	36	18	37100	82	64	46	281
2	92	76	60	44	28	12	50296	80	64	464
3	94	80	66	52	38	24	50310	65496	82682	649
4	96	84	72	60	48	36	24	65512	82700	836
5	1199	89	79	69	59	49	39	29	19	025
6	1201	93	85	77	69	61	53	45	37	216
7	03	4397	91	85	79	73	67	61	55	409
8	05	4401	9597	16793	89	85	81	77	73	604
9	1207	4405	9603	16801	25999	37197	50395	65693	82791	801

11	21	31	41	51	61	71	81	91	
1322	4622	9922	17222	26522	37822	51122	66422	83722	500
24	26	28	30	32	34	36	38	40	801
27	31	35	39	43	47	51	55	59	104
29	35	41	47	53	59	65	71	77	409
31	39	47	55	63	71	79	66487	83795	716
34	44	54	64	74	84	51194	66504	83814	025
36	48	60	72	84	37896	51208	20	32	336
38	52	66	80	26594	37908	22	36	50	649
40	56	72	88	26604	20	36	52	68	964
43	61	79	17297	15	33	51	69	83887	281
45	65	85	17305	25	45	65	66585	83905	600
47	69	91	13	35	57	79	66601	23	921
50	74	9998	22	46	70	51294	18	42	244
52	78	10004	30	56	82	51308	34	60	569
54	82	10	38	66	37994	22	50	78	896
57	87	17	47	77	38007	37	67	83997	225
1359	91	23	55	87	19	51	83	84015	556
1361	4695	29	63	26697	31	65	66699		889
64	4700	36	72	26708	44	80	66716		224
66	04	42	80	18	56	51394	32		561
68	08	48	88	28	68	51408			900
71	13	55	17397	39	81	23			241
73	17	61	17405	49	38093	37			584
75	21	67	13	59	38105	51			929
78	26	74	22	70	18	66			276
80	30	80	30	80	30	80			625
82	34	86	38	26790	42	51494			976
85	39	93	47	26801	55	51509			329
87	43	10099	55	11	67	23			684
90	48	10106	64	22	80	38			041
92	52	12	72	32	38192	52			400
94	56	18	80	42	38204	66			761
97	61	25	89	53	17	81			124
1399	65	31	17497	63	29	51595			489
1401	69	37	17505	73	41	51609			856
04	74	44	14	84	54	24			225
06	78	50	22	26894	66	38			596
08	82	56	30	26904	78	52			969
11	87	63	39	15	38291	67			344
13	91	69	47	25	38303	81			721
16	4796	76	56	36	16	51696			100
18	4800	82	64	46	28	51710			481
20	04	88	72	56	40	24			864
23	09	10195	81	67	53	39			249
25	13	10201	89	77	65	53			636
28	18	08	17598	88	78	68			025
30	22	14	17606	26998	38390	82			416
32	26	20	14	27008	38402	51796			809
35	31	27	23	19	15	51811			204
1437	4835	10233	17631	27029	38427	51825			601

POSTHUMOUS PAPERS INDICES OF PRIMES IN THE HIGHER NUMBER DOMAIN.

	$-1+2i$	$-1-2i$	-3	$3+2i$	$3-2i$	$1+4i$	$1-4i$	$-5+2i$	$-5-2i$	$-1+6i$	$-1-6i$	$5+4i$	$5-4i$	-7	$7+2i$	$7-2i$	$-5+6i$	$-5-6i$	$-3+8i$	$-3-8i$	$5+8i$	$5-8i$	$9+4i$	$9-4i$
	i	i	$1-i$	$-1-i$	$+1-i$	$+1-2i$	$+1-2i$	$+1+i$	$-1+i$	$+1+i$	$-1+i$	$+2-i$	$+1-2i$	$+1-2i$	$-1+i$	$1+i$	$1-i$	$-1-i$	$1+i$	$-1-i$	$1-i$	$1-i$	$1+i$	$1+4i$
i	1	1	2	3	3	4	4	7	7	9	9	10	10	12	13	13	15	15	18	18	22	22	24	24
$1+i$	2	3	3	7	4	7	5	1	22	1	28	32	2	46	40	1	16	31	1	37	23	23	1	7
$1-i$	1	2	1	4	1	3	1	22	15	28	19	22	32	34	27	40	1	16	55	19	1	1	73	79
$-1+2i$	$*$	3	7	4	5	9	2	18	12	13	6	27	21	25	19	10	35	9	68	65	10	40	20	63
$-1-2i$	1	$*$	5	11	4	14	15	12	18	6	31	31	17	31	10	45	39	5	11	68	40	54	81	44
-3	3	1	$*$	2	2	3	5	17	3	16	16	25	35	16	21	47	12	12	6	42	51	29	14	50
$3+2i$	2	1	6	$*$	1	13	9	13	23	14	35	26	33	3	4	44	28	52	9	44	79	38	36	23
$3-2i$	3	2	2	7	$*$	15	11	9	27	17	14	3	6	21	44	4	52	28	44	27	82	57	89	60
$1+4i$	1	2	3	9	7	$*$	6	15	20	21	2	8	9	29	22	24	38	11	23	52	27	81	78	1
$1-4i$	2	3	1	1	3	10	$*$	20	1	2	3	19	8	11	24	22	41	38	52	5	15	5	79	18
$-5+2i$	0	2	1	3	11	11	12	$*$	25	5	28	29	24	30	51	41	19	36	71	66	8	75	91	58
$-5-2i$	2	0	3	5	9	4	13	11	$*$	28	23	24	39	18	15	25	36	49	30	53	53	8	70	85
$-1+6i$	3	0	4	8	3	5	10	19	22	$*$	29	33	5	22	27	33	34	59	39	67	65	12	39	32
$-1-6i$	0	1	4	9	8	6	3	22	5	11	$*$	15	3	10	7	1	29	34	49	21	12	87	32	9
$5+4i$	3	3	5	6	11	4	3	5	16	25	15	$*$	32	9	16	9	46	32	69	13	26	55	4	43
$5-4i$	1	1	7	5	6	5	12	16	19	33	7	32	$*$	15	35	16	32	46	31	15	33	70	37	28
-7	1	3	4	7	1	1	7	10	10	10	10	1	11	$*$	28	28	23	53	51	33	83	61	11	5
$7+2i$	1	0	1	10	12	2	8	21	9	1	25	36	7	44	$*$	43	55	26	37	10	87	85	27	89
$7-2i$	0	3	3	2	10	8	14	23	7	7	19	37	36	20	17	$*$	26	25	46	55	19	65	23	21
$-5+6i$	1	1	0	6	10	10	1	25	6	4	27	2	4	43	37	8	$*$	31	21	43	85	2	45	29
$-5-6i$	3	3	0	10	6	7	6	6	11	9	4	4	22	13	8	11	1	$*$	25	39	46	19	83	3
$-3+8i$	0	3	6	5	4	15	18	7	26	3	33	9	31	23	1	6	33	13	$*$	26	28	24	73	13
$-3-8i$	1	0	2	4	11	8	19	26	21	15	21	21	19	17	6	27	43	3	62	$*$	24	28	67	7
$5+8i$	2	0	7	7	10	11	15	4	5	9	8	38	13	19	39	7	25	2	24	56	$*$	30	77	79
$5-8i$	0	2	5	10	1	9	13	19	4	8	27	23	18	37	33	13	2	55	56	24	74	$*$	1	35
$9+4i$	0	1	2	8	5	14	7	11	14	35	4	28	25	39	3	39	21	7	1	11	49	1	$*$	90
$9\quad 4i$	3	0	6	11	8	1	2	14	25	4	17	35	28	33	13	29	37	51	65	19	23	71	6	$*$
$-1+10i$	2	2	5	2	0	7	7	16	17	31	17	21	10	5	46	35	50	45	39	34	57	42	10	54
$-1-10i$	2	2	7	0	2	1	1	3	16	35	13	30	31	35	9	46	15	50	70	21	86	79	42	22
$3+10i$	1	3	2	0	9	6	5	14	24	23	24	17	18	38	49	50	54	56	14	2	69	51	65	31
$3-10i$	1	3	6	3	0	3	10	24	14	24	5	38	27	26	50	23	56	54	38	50	29	3	49	47
$-7+8i$	3	2	7	1	9	14	9	22	9	7	22	7	15	12	5	23	48	6	4	47	11	68	58	82
$-7-8i$	2	1	5	3	7	15	2	23	22	22	25	5	37	36	49	31	6	48	29	4	68	77	46	70
-11	2	2	0	11	5	5	3	1	15	24	24	37	7	40	12	12	15	45	61	7	16	16	94	34
$-11+4i$	0	1	3	4	3	7	15	14	27	29	13	36	29	26	32	21	57	29	54	30	41	18	9	38
$-11-4i$	3	0	1	9	4	9	1	13	14	31	11	39	36	38	47	32	59	27	66	18	62	63	26	39
$7+10i$	3	1	3	3	4	12	0	3	1	26	10	23	20	4	6	12	44	22	29	31	47	14	12	75
$7-10i$	3	1	1	4	9	0	4	15	17	10	26	20	13	28	12	6	22	44	13	47	58	25	69	84
$11+6i$	2	3	4	11	7	0	12	17	4	20	12	7	14	17	18	49	8	29	43	18	13	11	75	20
$11-6i$	1	2	4	1	5	4	0	4	3	12	20	34	37	23	23	18	59	8	54	25	77	35	44	69
$-23+2i$	1	0	7	2	8	15	4	27	1	20	18	18	32	7	33	36	24	7	26	28	72	66	38	77
$-23-2i$	0	3	5	8	2	12	9	15	13	18	20	32	38	1	36	7	37	24	28	62	22	72	35	26
$-9+20i$	0	0	2	11	1	3	6	8	16	19	3	20	37	15	42	37	5	42	53	59	39	56	61	16
$-9-10i$	0	0	6	7	5	10	5	16	8	21	1	7	20	9	11	42	42	35	41	71	56	17	16	19
$-7+12i$	2	1	4	0	11	9	4	12	13	1	14	11	22	20	30	5	42	19	59	50	81	64	87	87

AUXILIARY TABLE

FOR SOLVING THE INDETERMINATE EQUATION

$$A = fxx + gyy$$

BY THE METHOD OF EXCLUSION.

It is assumed that a prime p has been chosen as the exclusion number, and that none of the numbers A, f, g is divisible by it. The table is also restricted to the two cases in which the value of the expression $\frac{A}{f}(\text{mod}.p)$ is either a fixed quadratic residue (always 1), or a fixed quadratic nonresidue modulo p. Finally, the table has been provided only for the case in which fg is a quadratic residue of p, and the opposite case has been omitted entirely. Section Six of the *Disquisitiones Arithmeticae* gives sufficient instruction on how to derive easily from the table what it does not contain directly.

Examples. Let the equation to be solved be $21680143 = xx + 78yy$

1) Exclusion number $= 5$ $\qquad fg = \text{N}, \quad \frac{A}{f} \equiv 3 \equiv 2 \,.\, 2^2$
From the table $1, 4$ for $fg = R$ and hence $0, 2, 3$ for $fg = \text{N}$, and for the above case $0, 1, 4$ or excluded $5n \pm 2$

2) Exclusion number $= 7$ $\qquad fg = R, \quad \frac{A}{f} \equiv 2 \equiv 1, 3^2$
From the table $0, 1, 2, 5, 6$ For the present case $0, 3, 6, 1, 4$ and excluded $7n \pm 2$

3) Exclusion number $= 11$ $\qquad fg = R, \quad \frac{A}{f} \equiv 1$
Thus we obtain $0, 1, 3, 5, 6, 8, 10$; excluded $11n \pm 2, 4$

4) Exclusion number $= 17$ $\qquad fg = \text{N}, \quad \frac{A}{f} \equiv 9 \equiv 1 \,.\, 3^1$

$$0 \,.\, 1 \,.\, 3 \,.\, 4 \,.\, 6$$
$$0 \,.\, 3 \,.\, 8 \,.\, 5 \,.\, 1$$
$$0, 2, 3, 4, 6, 7$$
$$\text{Exclusion number} \quad \pm 1, 5, 8$$

p	Value of $\frac{A}{f}(\text{mod}.p)$	Numbers, taken positively or negatively, to which x must be congruent modulo p.
3	1	0, 1
	2	1
5	1	0, 1
	2	1
7	1	0, 1, 2
	6	2, 3
11	1	0, 1, 3, 5
	10	1, 3, 4
13	1	0, 1, 2, 6
	2	1, 4, 5
17	1	0, 1, 3, 4, 6
	3	1, 2, 4, 6
19	1	0, 1, 2, 3, 4, 7
	18	1, 3, 6, 7, 8
23	1	0, 1, 4, 8, 9, 10, 11
	22	1, 2, 3, 4, 6, 8
29	1	0, 1, 5, 6, 8, 9, 11, 13
	2	1, 3, 5, 6, 8, 13, 14
31	1	0, 1, 2, 4, 5, 7, 10, 11, 13
	30	4, 5, 6, 8, 11, 12, 13, 14
37	1	0, 1, 2, 7, 8, 10, 11, 14, 16, 18
	2	1, 3, 6, 7, 8, 14, 15, 17, 18
41	1	0, 1 . 3, 9, 12, 13, 14, 16, 17, 18, 19
	3	1, 2, 6, 7, 8, 9, 11, 12, 13, 17
43	1	0, 1, 2, 3, 7, 8, 9, 11, 13, 17, 18, 20
	42	1, 2, 5, 6, 7, 8, 9, 16, 17, 19, 21
47	1	0, 1, 4, 6, 9, 10, 11, 16, 18, 19, 20, 22, 23
	46	2, 3, 5, 9, 13, 15, 16, 18, 19, 21, 22, 23
53	1	0, 1, 4, 5, 8, 10, 12, 13, 14, 16, 19, 20, 21, 22
	2	1, 3, 7, 8, 11, 12, 15, 16, 18, 21, 24, 25, 26
59	1	0, 1, 3, 5, 10, 11, 13, 14, 15, 17, 19, 22, 23, 24, 25, 29
	58	1, 3, 6

Exclusion number p	$\frac{A}{f}$	$\frac{f}{A}$	$fgRp$ Allowed		Excluded
3	1	1	0	1 . 2	
	2	2	1 . 2		0
5	1	1	0	1 . 4	2 . 3
	2	3	1 . 4		0 . 2 . 3
	3	2	2 . 3		0 . 1 . 4
	4	4	0	2 . 3	1 . 4
7	1	1	0 . 2 . 5	1 . 6	3 . 4
	2	4	0 . 1 . 6	3 . 4	2 . 5
	3	5	1 . 3 . 4 . 6		0 . 2 . 5
	4	2	0 . 3 . 4	2 . 5	1 . 6
	5	3	1 . 2 . 5 . 6		0 . 3 . 4
	6	6	2 . 3 . 4 . 5		0 . 1 . 6
11	1	1	0 . 3 . 5 . 6 . 8	1 . 10	2 . 4 . 7 . 9
	2	6	1 . 2 . 3 . 8 . 9 . 10		0 . 4 . 5 . 6 . 7
	3	4	0 . 3 . 4 . 7 . 8	5 . 6	1 . 2 . 9 . 10
	4	3	0 . 1 . 5 . 6 . 10	2 . 9	3 . 4 . 7 . 8
	5	9	0 . 1 . 2 . 9 . 10	4 . 7	3 . 5 . 6 . 8
	6	2	1 . 4 . 5 . 6 . 7 . 10		0 . 2 . 3 . 8 . 9
	7	8	2 . 3 . 5 . 6 . 8 . 9		0 . 1 . 4 . 7 . 10
	8	7	2 . 4 . 5 . 6 . 7 . 9		0 . 1 . 3 . 8 . 10
	9	5	0 . 2 . 4 . 7 . 9	3 . 8	1 . 5 . 6 . 10
	10	10	1 . 3 . 4 . 7 . 8 . 10		0 . 2 . 5 . 6 . 9
13	1	1	0 . 2 . 6 . 7 . 11	1 . 12	3 . 4 . 5 . 8 . 9 . 10
	2	7	1 . 4 . 5 . 8 . 9 . 12		0 . 2 . 3 . 6 . 7 . 10 . 11
	3	9	0 . 2 . 5 . 8 . 11	4 . 9	1 . 3 . 6 . 7 . 10 . 12
	4	10	0 . 1 . 4 . 9 . 12	2 . 11	3 . 5 . 6 . 7 . 8 . 10
	5	8	1 . 2 . 3 . 10 . 11 . 12		0 . 4 . 5 . 6 . 7 . 8 . 9
	6	11	3 . 4 . 6 . 7 . 9 . 10		0 . 1 . 2 . 5 . 8 . 11 . 12
	7	2	2 . 4 . 6 . 7 . 9 . 11		0 . 1 . 3 . 5 . 8 . 10 . 12
	8	5	2 . 3 . 5 . 8 . 10 . 11		0 . 1 . 4 . 6 . 7 . 9 . 12
	9	3	0 . 5 . 6 . 7 . 8	3 . 10	1 . 2 . 4 . 9 . 11 . 12
	10	4	0 . 1 . 3 . 10 . 12	6 . 7	2 . 4 . 5 . 8 . 9 . 11
	11	6	1 . 5 . 6 . 7 . 8 . 12		0 . 2 . 3 . 4 . 9 . 10 . 11
	12	12	0 . 3 . 4 . 9 . 10	5 . 8	1 . 2 . 6 . 7 . 11 . 12
17	1	1	0 . 3 . 4 . 6 . 11 . 13 . 14	1 . 16	2 . 5 . 7 . 8 . 9 . 10 . 12 . 15
	2	9	0 . 1 . 2 . 7 . 10 . 15 . 16	6 . 11	3 . 4 . 5 . 8 . 9 . 12 . 13 . 14
	3	6	1 . 2 . 4 . 6 . 11 . 13 . 15 . 16		0 . 3 . 5 . 7 . 8 . 9 . 10 . 12 . 14
	4	13	0 . 5 . 6 . 8 . 9 . 11 . 12	2 . 15	1 . 3 . 4 . 7 . 10 . 13 . 14 . 16
	5	7	1 . 2 . 3 . 8 . 9 . 14 15 . 16		0 . 4 . 5 . 6 . 7 . 10 . 11 . 12 . 13
	6.	3	2 . 5 . 6 . 7 . 10 . 11 . 12 . 15		0 . 1 . 3 . 4 . 8 . 9 . 13 . 14 . 16
	7	5	3 . 4 . 5 . 7 . 10 . 12 . 13 . 14		0 . 1 . 2 . 6 . 8 . 9 . 11 . 15 . 16
	8	15	0 . 2 . 3 . 4 . 13 . 14 . 15	5 . 12	1 . 6 . 7 . 8 . 9 . 10 . 11 . 16
	9	2	0 . 1 . 5 . 8 9 . 12 . 16	3 . 14	2 . 4 . 6 . 7 . 10 . 11 . 13 . 15
	10	12	1 . 3 . 5 . 6 . 11 . 12 . 14 . 16		0 . 2 . 4 . 7 . 8 . 9 . 10 . 13 . 15
	11	14	3 . 6 . 7 . 8 . 9 . 10 . 11 . 14		0 . 1 . 2 . 4 . 5 . 12 . 13 . 15 . 16
	12	10	2 . 4 . 5 . 8 . 9 . 12 . 13 . 15		0 . 1 . 3 . 6 . 7 . 10 . 11 . 14 . 16
	13	4	0 . 2 . 3 . 7 . 10 . 14 . 15	8 . 9	1 . 4 . 5 . 6 . 11 . 12 . 13 . 16
	14	11	1 . 4 . 7 . 8 . 9 . 10 . 13 . 16		0 . 2 . 3 . 5 . 6 . 11 . 12 . 14 . 15
	15	8	0 . 4 . 6 . 8 . 9 . 11 . 13	.7 . 10	1 . 2 . 3 . 5 . 12 . 14 . 15 . 16
	16	16	0 . 1 . 5 . 7 . 10 . 12 . 16	4 . 13	2 . 3 . 6 . 8 . 9 . 11 . 14 . 15
p	$\frac{A}{f}$	$\frac{f}{A}$	Excluded	$fgNp$	Allowed

POSTHUMOUS PAPERS. AUXILIARY TABLE FOR SOLVING THE EQUATION

$$A = fxx + gyy.$$

Exclusion number p	$\frac{A}{f}$	$\frac{f}{A}$	$fg\,R\,p$ Allowed		Excluded
19	1	1	0 2 . 3 . 4 . 7 . 12 . 15 . 16 . 17	1 . 18	5 . 6 . 8 9 . 10 . 11 . 13 . 14
	2	10	1 . 2 . 4 . 6 . 9 . 10 . 13 . 15 . 17 . 18		0 . 3 . 5 . 7 . 8 . 11 . 12 . 14 . 16
	3	13	4 . 5 . 6 . 7 . 9 . 10 . 12 . 13 . 14 . 15		0 . 1 . 2 . 3 . 8 . 11 . 16 . 17 . 18
	4	5	0 . 4 . 5 . 6 . 8 . 11 . 13 . 14 . 15	2 . 17	1 . 3 . 7 . 9 . 10 . 12 . 16 . 18
	5	4	0 . 1 . 2 . 6 . 8 . 11 . 13 . 17 . 18	9 . 10	3 4 . 5 . 7 . 12 . 14 . 15 . 16
	6	16	0 . 1 . 3 . 4 . 9 . 10 . 15 . 16 . 18	5 . 14	2 6 . 7 . 8 . 11 . 12 . 13 . 17
	7	11	0 . 1 . 3 . 5 . 6 . 13 . 14 . 16 . 18	8 . 11	2 . 4 . 7 . 9 . 10 . 12 . 13 . 15
	8	12	1 . 2 . 4 . 7 . 8 . 11 . 12 . 15 . 17 . 18		0 . 3 . 5 . 6 9 . 10 . 13 14 . 16
	9	17	0 . 2 . 6 . 7 . 9 . 10 . 12 . 13 . 17	3 . 16	1 . 4 . 5 . 8 . 11 . 14 . 15 . 18
	10	2	1 . 2 . 3 . 5 . 9 . 10 . 14 . 16 . 17 . 18		0 . 4 . 6 . 7 . 8 . 11 . 12 . 13 . 15
	11	7	0 . 2 5 . 8 . 9 . 10 . 11 . 14 . 17	7 . 12	1 . 3 . 4 6 . 13 . 15 . 16 . 18
	12	8	1 · 5 . 7 . 8 . 9 . 10 . 11 . 12 . 14 . 18		0 . 2 . 3 . 4 . 6 . 13 . 15 . 16 . 17
	13	3	2 . 3 . 4 . 5 . 8 . 11 . 14 . 15 . 16 . 17		0 . 1 . 6 . 7 . 9 . 10 . 12 . 13 . 18
	14	15	3 . 4 . 6 . 8 . 9 . 10 . 11 . 13 . 15 . 16		0 . 1 . 2 5 . 7 . 12 . 14 . 17 . 18
	15	14	2 . 3 . 5 . 6 . 7 . 12 . 13 . 14 . 16 . 17		0 . 1 . 4 . 8 . 9 . 10 . 11 . 15 . 18
	16	6	0 . 3 . 7 . 8 . 9 . 10 . 11 . 12 . 16	4 . 15	1 . 2 . 5 . 6 . 13 . 14 . 17 . 18
	17	9	0 . 1 . 4 . 5 . 6 . 13 . 14 . 15 . 18	6 . 13	2 . 3 . 8 . 9 . 10 . 11 . 16 . 17
	18	18	1 . 3 . 6 . 7 . 8 . 11 . 12 . 13 . 16 . 18		0 . 2 . 4 . 5 . 9 . 10 . 14 . 15 . 17
23	1	1	0.4.8.9.10.11.12.13.14.15.19	1 . 22	2 . 3 . 5 . 6 . 7 . 16 . 17 . 18 . 20 . 21
	2	12	0 . 1 . 3 . 4 . 6 9 . 14 . 17 . 19 . 20 . 22	5 . 18	2 . 7 . 8 . 10 . 11 . 12 . 13 . 15 . 16 . 21
	3	8	0 . 1 . 5 . 6 . 8 . 10 . 13 . 15 . 17 . 18 . 22	7 . 16	2 . 3 . 4 . 9 . 11 . 12 . 14 . 19 . 20 . 21
	4	6	0 . 1 . 3 . 5 . 7 . 8 . 15 . 16 . 18 . 20 . 22	2 . 21	4 . 6 . 9 . 10 . 11 . 12 . 13 . 14 . 17 . 19
	5	14	1 . 2 . 4 . 5 . 7 . 9 . 14 . 16 . 18 . 19 . 21 . 22		0 . 3 . 6 . 8 . 10 . 11 . 12 . 13 . 15 . 17 . 20
	6	4	0 . 2 . 4 . 5 . 6 . 7 . 16 . 17 . 18 . 19 . 21	11 . 12	1 . 3 . 8 . 9 . 10 . 13 . 14 . 15 . 20 . 22
	7	10	1 . 2 . 7 . 8 . 9 . 11 12 . 14 . 15 . 16 . 21 . 22		0 . 3 4 . 5 . 6 . 10 . 13 . 17 . 18 . 19 . 20
	8	3	0 . 2 . 5 . 6 . 8 . 11 . 12 . 15 17 . 18 . 21	10 . 13	1 . 3 . 4 . 7 . 9 . 14 . 16 . 19 . 20 . 22
	9	18	0 . 1 . 4 7 . 10 . 11 . 12 . 13 . 16 . 19 . 22	3 . 20	2 . 5 . 6 . 8 . 9 . 14 . 15 . 17 . 18 . 21
	10	7	1 . 2 . 3 . 5 . 10 . 11 . 12 . 13 . 18 . 20 . 21 . 22		0 . 4 . 6 . 7 . 8 . 9 . 14 . 15 . 16 . 17 . 19
	11	21	3 . 4 . 5 . 7 . 8 . 10 13 . 15 . 16 . 18 . 19 . 20		0 . 1 . 2 . 6 . 9 . 11 . 12 . 14 . 17 . 21 . 22
	12	2	0 . 2 . 3 . 7 . 10 . 11 . 12 . 13 . 16 . 20 . 21	9 . 14	1 . 4 . 5 . 6 . 8 . 15 . 17 . 18 . 19 . 22
	13	16	0 . 1 . 2 . 3 . 8 . 9 . 14 . 15 . 20 . 21 . 22	6 . 17	4 . 5 . 7 . 10 . 11 . 12 . 13 . 16 . 18 . 19
	14	5	1 . 5 . 6 . 9 . 10 11 . 12 . 13 14 . 17 . 18 . 22		0 . 2 . 3 . 4 . 7 . 8 . 15 . 16 . 19 . 20 . 21
	15	20	3 . 5 . 6 . 7 . 9 . 11 . 12 . 14 . 16 . 17 . 18 . 20		0 . 1 . 2 . 4 . 8 . 10 . 13 15 . 19 . 21 . 22
	16	13	0 . 2 . 6 . 7 . 9 . 10 . 13 . 14 . 16 . 17 21	4 . 19	1 . 3 . 5 . 8 . 11 . 12 . 15 . 18 . 20 . 22
	17	19	1 . 2 . 3 . 4 . 6 . 10 . 13 . 17 . 19 . 20 . 21 . 22		0 . 5 . 7 . 8 . 9 . 11 . 12 . 14 . 15 . 16 . 18
	18	9	0 . 3 . 4 . 5 . 9 . 11 . 12 . 14 . 18 . 19 . 20	8 . 15	1 . 2 . 6 . 7 . 10 . 13 . 16 . 17 . 21 . 22
	19	17	1 . 4 . 6 . 7 . 8 . 11 . 12 . 15 . 16 . 17 . 19 . 22		0 . 2 . 3 . 5 . 9 . 10 . 13 . 14 . 18 . 20 . 21
	20	15	2 . 4 . 5 . 8 . 9 . 10 . 13 . 14 . 15 . 18 19 . 21		0 . 1 . 3 . 6 . 7 . 11 . 12 . 16 . 17 . 20 . 22
	21	11	3 . 6 . 7 . 8 . 9 . 10 . 13 . 14 . 15 . 16 . 17 . 20		0 . 1 . 2 . 4 . 5 . 11 . 12 . 18 . 19 . 21 . 22
	22	22	2 . 3 . 4 . 6 8 . 11 . 12 . 15 . 17 . 19 . 20 . 21		0 . 1 . 5 . 7 . 9 . 10 . 13 . 14 . 16 . 18 . 22
p	$\frac{A}{f}$	$\frac{f}{A}$	Excluded	$fg\,N\,p$	Allowed

SECTION EIGHT.

A FULLER CONSIDERATION OF CERTAIN INVESTIGATIONS CONCERNING CIRCLE DIVISION.

367.

What we set out in the latter part of Section Seven, from Article 355 onward, certainly gives substantial examples of the great fertility of the theory of circle division, and of the remarkable connection linking this subject with various *arithmetic* investigations. There, however, the severe limits of space and time allowed us only to touch lightly on this field, which rewards our efforts with a richer harvest the further we advance into it. We therefore intend to take up here again one or another of the questions begun there and discuss them more fully: readers will certainly see with great wonder that the solution of several arithmetic problems, which anyone would have expected to be worlds apart from this subject, rests on this foundation.

368.

The investigation begun in Article 356 offers an especially fruitful subject. There we divided the collection of roots of the equation $x^n - 1 = 0$ (excluding unity) into two classes and showed how to determine the sum in each class. These sums were $= -\frac{1}{2} + \frac{1}{2}\sqrt{n}$ and $-\frac{1}{2} - \frac{1}{2}\sqrt{n}$ when n has the form $4n+1$, or $= -\frac{1}{2} + \frac{1}{2}\sqrt{-n}$ and $-\frac{1}{2} - \frac{1}{2}\sqrt{-n}$ when n has the form $4n+3$. Yet there we had not only restricted ourselves to the case where n is a *prime number*; we had also, what was of much greater importance still, left the *sign* of the radical quantity undetermined, or rather neglected to support this determination, indicated in a few words, with a solid proof. We must therefore make good these deficiencies before anything else.

.369.

Now let n be any positive integer, and R a root of the equation $x^n - 1. = 0$ none of whose powers preceding the power with exponent n equals unity (see Article 359, II.). As in Section VII, let us denote by $[\lambda]$ the power R^λ, so that $[0] = 1$, $[1]$, $[2]$, $[3] \ldots . [n-1]$ represent all the roots of the equation $x^n - 1 = 0$. Further, let us denote the sum

$$[0] + [1] + [4] + [9] + \ldots . + [(n-1)^2] \quad \text{by } \Sigma[\mathfrak{Q}]$$

and more generally

$$[0] + [\lambda] + [4\lambda] + [9\lambda] \ldots . + [\lambda(n-1)^2] \quad \text{by } \Sigma[\mathfrak{Q}\lambda]$$

so that $\mathfrak{Q}$ denotes, without further specification, the squares of the numbers $0, 1, 2, 3 \ldots . n-1$. Thus, just as in general $[\lambda] = [\mu]$ when λ, μ are any integers (positive or negative) congruent modulo n, we also have $\Sigma[\mathfrak{Q}\lambda] = \Sigma[\mathfrak{Q}\mu]$ when $\lambda \equiv \mu$. With these preparations we have the following.

370.

PROBLEM. *Determine the product of the two sums* $\Sigma[\mathfrak{Q}]$ *and* $\Sigma[-\mathfrak{Q}]$.

Solution. Since $nn \equiv 0$, $(n+1)^2 \equiv 1$, $(n+2)^2 \equiv 4$, etc. (mod.n), it is easy to see that $\Sigma[\mathfrak{Q}]$ becomes

$$\begin{aligned} &= [1] + [4] + [9] + [16] \ldots . + [nn] \\ &= [4] + [9] + [16] + [25] \ldots . + [(n+1)]^2 \\ &= [9] + [16] + [25] + [36] \ldots . + [(n+2)^2] \end{aligned}$$

etc. or in general

$$= [kk] + [(k+1)^2] + [(k+2)^2] + [(k+3)^2] \ldots . + [(n+k-1)^2]$$

Hence $[-kk] \times \Sigma[\mathfrak{Q}]$

$$= [0] + [2k+1] + [4k+4] + [6k+9] \ldots . + [(n-1)^2 + 2(n-1)k]$$

Hence $\Sigma[-\mathfrak{Q}] \times \Sigma[\mathfrak{Q}]$ expands into

$$\begin{aligned} &- [0] + [1] + [4] + [9] \ldots . + [(n-1)^2] \\ &+ [0] + [3] + [8] + [15] \ldots . + [nn-1] \\ &+ [0] + [5] + [12] + [21] \ldots . + [nn+2n-3] \\ &+ [0] + [7] + [16] + [27] \ldots . + [nn+4n-5] \\ &+ \text{etc.} \\ &+ [0] + [2n-1] + [4n] + [6n+3] \ldots . + [3nn-6n+3] \end{aligned}$$

Summing these parts *vertically* gives

$$\begin{aligned} n[0] + [1] \times \frac{1-[2n]}{1-[2]} + [4]\frac{1-[4n]}{1-[4]} + [9]\frac{1-[6n]}{1-[6]} \\ + \text{etc.} + [(n-1)^2] \times \frac{1-[2nn-2n]}{1-[2n-2]} \end{aligned}$$

In this expression all parts except the first vanish whenever n is odd; for then all of $1-[2n]$, $1-[4n]$, $1-[6n]$, etc. become $= 0$, whereas none of the denominators $1-[2]$, $1-[4]$, $1-[6]$, $1-[8]$, etc. up to $1-[2n-2]$ does. When n is even, however, one of the denominators is also $= 0$, namely $1-[n]$, to which the term $[\frac{1}{4}nn] \times \frac{1-[nn]}{1-[n]}$ corresponds; the sum of the parts from which

this term arose becomes $= n[\frac{1}{4}nn]$. Here again we must distinguish two cases. When n is divisible by four, $\frac{1}{4}nn \equiv 0\,(\mathrm{mod}.n)$ and therefore $[\frac{1}{4}nn] = 1$; but when n is twice an odd number, $\frac{1}{4}nn \equiv \frac{1}{2}n\,(\mathrm{mod}.n)$ and therefore necessarily $[\frac{1}{4}nn] = -1$. We finally conclude that
1) for an odd value of n, the required product is $= n$
2) for a value divisible by four, the product is $= 2n$
3) for a value that is twice an odd number, it is $= 0$. Q. E. I.

371.

It is now worth considering the nature of the sum $\Sigma[\mathfrak{Q}]$ more closely.

I. Since we may replace the squares 0, 1, 4, 9, 16, etc. by their least residues modulo n, it is evident that if M denotes, without further specification, the quadratic residues of the number n from 0 to $n-1$, and m the number of roots of the congruence $xx \equiv M(\mathrm{mod}.m)$, then $\Sigma[\mathfrak{Q}] = \Sigma m[M]$. We showed how to determine the number m in Articles 104, 105.

II. If n is an (odd) prime, then for $M = 0$ we have $m = 1$, whereas for every other value of M we have $m = 2$. If n is a power of an odd prime $= p^\nu$, then $m = 2$ for every value of M not divisible by p —

— — — — — — — — — — — — — — — — —

372.

If n is an (odd) prime, the residues m consist of zero, for which $M = 1$, and $\frac{1}{2}(n-1)$ other numbers, for which $M = 2$. Denoting these residues (excluding the residue 0), without further specification, by μ, our progression is $= 1 + 2\Sigma r^\mu$. Further, if ν denotes, without further specification, all remaining numbers below n, whose number is likewise $\frac{1}{2}(n-1)$ and which comprise all quadratic nonresidues of n below n, then evidently

$$1 + \Sigma r^\mu + \Sigma r^\nu = 1 + r + rr + r^3 \ldots + r^{n-1} = \frac{1 - r^n}{1 - r} = 0$$

Thus, setting the sum of our progression, that is $1 + 2\Sigma r^\mu = A$, we have $1 + 2\Sigma r^\nu = -A$, and also $\Sigma r^\mu - \Sigma r^\nu = A$.

By Article 356 we therefore have $A = \pm\sqrt{n}$ or $\pm\sqrt{-n}$, according as n is $\equiv 1$ or $\equiv 3\,(\mathrm{mod}.4)$. But this does not yet determine the sign of the root.

If, in our progression, which we shall denote by Π, we replace r by another similar root of the equation $x^n - 1 = 0$, say $r' = r^\lambda$, let Π' be the result.

373.

If n is the square or a higher power of a prime, say $= p^\pi$, some residues m consist of numbers not divisible by p; others are divisible by pp but not by a higher power of p; others can be divided by p^4 but not. by p^5; and so on to those divisible by $p^{\pi-2}$ but not by $p^{\pi-1}$, or by $p^{\pi-1}$ but not by p^π, according as π is even or odd. Finally there is the residue 0, the only one divisible by p^π (compare Article 102). Now denote, without further specification, by μ the quadratic residues of the number p below p, excluding zero (whose number is $= \frac{1}{2}(p-1)$). Those different classes of residues are then represented as follows. The first, which are not divisible by p, are represented by $\mu + kp$, where for k we must substitute all integers from 0 to $p^{\pi-1} - 1$, so that the number of all residues contained in this form is $= \frac{1}{2}(p-1)p^{\pi-1}$; for each of these, $M = 2$. The sum of all terms in Π corresponding to these residues is

$$= 2\Sigma r^{\mu+kp} = 2\Sigma r^\mu \,.\, \Sigma r^{kp}$$
$$= 2\Sigma r^\mu \,.\, \frac{r^{p^\pi} - 1}{r^p - 1} = 0$$

The second class of residues is represented by $\mu pp + kp^3$, where for k we must substitute all integers from 0 to $p^{\pi-3} - 1$, so that the number of all residues contained in this form is $= \frac{1}{2}(p-1)p^{\pi-3}$; for each of them, however, $M = 2p$. The sum of the terms in Π arising from these becomes

$$= 2p\Sigma r^{\mu pp+kp^3} = 2p\Sigma r^{\mu pp} \,.\, \Sigma r^{kp^3}$$
$$= 2p\Sigma r^{\mu pp} \,.\, \frac{r^{p^\pi} - 1}{r^{p^3} - 1} = 0$$

provided that $\pi > 3$. Similarly, the third, fourth, etc. class is represented by $\mu p^4 + kp^5$, $\mu p^6 + kp^7$, etc., where for k we must take all integers from 0 to $p^{\pi-5} - 1$, $p^{\pi-7} - 1$, etc.; for these, $M = 2pp$, $M = 2p^3$, etc. The sum of the terms in Π arising from the third, fourth, etc. class vanishes provided that $\pi > 5$, $\pi > 7$, etc.. respectively.

We conclude that when π is even, in Π only the terms corresponding to the residue 0 remain, and these are $= 1$; for these, however, $M = p^{\frac{1}{2}\pi}$, so that the sum of all terms in Π is $= p^{\frac{1}{2}\pi}$.

GAUSS TO DIRICHLET.

To Monsieur
Monsieur Lejeune Dirichlet in Paris.

I would have thanked you earlier for the memoir you so kindly sent me and for the great pleasure it gave me, had I not wished first to hear something of the outcome of my efforts in Berlin concerning your wishes and, I may add, my own. I am extremely pleased now to see, from a letter received from the Secretary of the Academy in Berlin, that we may hope that they will soon be willing to secure a suitable permanent position for you in your homeland.

The rarer this inclination is, the more pleased I am to find you so strongly drawn to the part of mathematics that has always been my favourite study. I sincerely wish you circumstances in which you remain as far as possible master of your time and of the choice of your work. Immediately after the appearance of my Disquisitiones, other kinds of work, and later my circumstances, greatly hindered me from following my inclination as much as I would have wished. Instead of a second part of that work, which I formerly intended, I shall in all probability have to confine myself to presenting a memoir on an individual subject from time to time. The three memoirs of this kind that have so far appeared in the 16th volume of the local Commentationes and in the first and fourth volumes of the Commentationes recentiores, however, contain (apart from a portion of the second) none of the subjects I already had in mind in 1801 for the continuation, but new ones. My later work of this kind likewise concerns a new subject, namely the theory of biquadratic residues, which I intend to present in about three memoirs; the first of these will shortly be printed for the sixth volume of the Comment. rec., and the main material for the remainder, as well as for the similar theory of cubic residues, may be regarded as essentially settled, although little of it has yet been properly put on paper.

Please give my regards to Herr von Humboldt, if he is still in Paris, and excuse my not writing to him directly now by my concern that the letter might not reach him, since, as I hear, he intended to leave Paris.

With sincere esteem

Yours most devotedly

Göttingen, 13 September 1826. C. F. Gauss.

I offer you, my highly esteemed friend, my most sincere thanks for your kind letter and for kindly sending your two memoirs. I am pleased to see the growing interest now beginning to be taken in investigations of higher arithmetic. I very much liked the successful way in which you derive the second, concerning the biquadratic residuacity of the number 2, from the first.

Presumably the 6th volume of our Commentationes has now reached Breslau, so you will probably be familiar by now with my Commentatio prima on biquadratic residues: if an opportunity arises, I would also gladly send you a separate copy. I could have chosen among several methods of proving the theorem in it; but you will see why I preferred the method used there, chiefly because the classification of 2 for those moduli for which it is a quadratic nonresidue (under B or D) must be regarded as an essential part of the theorem, to which most other methods of proof seem inapplicable.

I have had all the material for the entire investigation for 23 years, and the proofs of its main theorems (among which the theorem in the first memoir is *not* yet to be counted) for about 14 years — (although I wish and hope to be able to simplify something further in the latter, the proofs) —. I have planned the investigation for about 3 memoirs. I have already begun writing the second, and hope to finish it before long, unless the surveying duties recently assigned to me again cause some delay.

I had already also announced the concluding theorem $b \equiv \frac{1}{2}rr \,(\mathrm{mod}.p)$ in the local gel. Anzeigen three years ago and drawn attention to the remarkable knot still to be untied in connection with it; but I have not yet heard of anyone attempting it. A few days ago I did succeed with *one half*, and this discovery gave me all the more pleasure because it does not rest on induction at all — for I confess that I would not have expected precisely *this* connection — but a priori on combining other *very intricate* and interesting investigations, already 28 years old but still entirely unpublished, of which a faint indication is given in the closing note of the Disquis. Arithm. p. 668 [Gauss Werke vol. I. p. 466].

This is a sufficient criterion for the case where p has the form $8n + 5$.

Let the number of classes formed by the binary forms in each of the two kinds for the determinant $-p$ be $= k$. The beginning of a table I constructed up to the determinant -3000 is in Disquis. Arithm. p. 520. [Art. 303.] It should also be noted that for a p of the assumed form we always have $k = 2m+1$ when m denotes the number of decompositions of p into three positive squares (I say positive to exclude 0), as Legendre found by induction and

as was first proved in the Disquis. Arithm. from the theory of *ternary* forms. For example,

for $p =$	5,	13,	29,	37,	53,	61,	101,	109,	149,	157	etc.
$k =$	1,	1,	3,	1,	3,	3,	7,	3,	7,	3	
$m =$	0,	0,	1,	0,	1,	1,	3,	1,	3,	1	
			4	—	1	9	1 4 16	9	1 4 36	4	
			9		16	16	36 16 36	36	4 64 64	9	
			16		36	36	64 81 49	64	144 81 49	144	

With this assumption, the value of b that is $\equiv \frac{1}{2}rr \,(\text{mod.}p)$ is always

$$\equiv 2k + a - 1 \equiv 4m + a + 1 \;(\text{mod.}8)$$

which completely determines the sign of b. Here are 22 examples, doubling the extent of the table given at the end of the memoir.

p	k	a	b	p	k	a	b
5	1	+1	+2	181	5	+9	+10
13	1	−3	−2	197	5	+1	−14
29	3	+5	+2	229	5	−15	+2
37	1	+1	−6	269	11	+13	+10
53	3	−7	−2	277	3	+9	+14
61	3	+5	−6	293	9	+17	+2
101	7	+1	−10	317	5	−11	+14
109	3	−3	+10	349	7	+5	+18
149	7	−7	−10	373	5	−7	+18
157	3	−11	−6	389	11	+17	−10
173	7	+13	+2	397	3	−19	−6

The rule can therefore also be expressed as follows; (always assuming $p \equiv 5 \;(\text{mod.}8)$)

$$\begin{aligned} \text{We have } b &\equiv a + 1 \;(\text{mod.}8), && \text{if } m \text{ is even} \\ b &\equiv a + 5 && \text{if } m \text{ is odd.} \end{aligned}$$

I do not yet venture a conjecture as to whether a still simpler criterion is possible for distinguishing the case of even m from the odd case *in advance*, that is, without knowing the value of m itself, since, as I remarked above, this connection is still entirely new.

For the case $p \equiv 1 \pmod{8}$ the above congruence $b \equiv 2k + a - 1 \pmod{8}$ remains correct, but it no longer determines the sign of b, since both the positive and the negative values of b satisfy it. Here k is always even, $= 2m$ (with m understood just as above), or $= 2m + 2$ if m denotes the number of decompositions of p into 3 positive *unequal* squares, and $b \equiv 0 \pmod{4}$, or $b \equiv -b \pmod{8}$. I conjecture that the case $p \equiv 1 \pmod{8}$ or $b \equiv 0 \pmod{4}$ calls for deeper investigation, and perhaps again

$$\begin{aligned} b &\equiv 4 \pmod{8} \quad \text{easier than } b \equiv 0 \pmod{8} \\ b &\equiv 8 \pmod{16} \quad \text{easier than } b \equiv 0 \pmod{16} \end{aligned}$$

etc.

With the highest esteem I remain

Yours most devotedly in friendship

Göttingen, 30 May 1828. C. F. Gauss.

REMARKS.

In this second volume of GAUSS's works I have included all his memoirs, essays and tables on higher arithmetic, insofar as they are not already covered by the seven sections of the *Disqu. Arithm.*: the five memoirs published in the '*Commentationes societatis regiae scientiarum Gottingensis*' (in quarto), the reviews of these works of his own and of some works by others published in the '*Göttingischen Gelehrten Anzeigen*' (in octavo) (unsigned by GAUSS, but confirmed as his through the records of the Göttingen University Library), and a selection from his manuscript remains.

In the second printing I have also added the tables 'Circuli quadratura nova', 'On Calculating Logarithms', 'Quadratorum myrias prima', 'Indices of Primes in the Higher Number Domain', 'Auxiliary Table for Solving the Indeterminate Equation $A = fxx + gyy$ by the Method of Exclusion', as well as 'Sectio octava', as far as it was written down, and finally two letters from GAUSS to DIRICHLET, as essential parts of the history of higher arithmetic.

To make the subjects in so extensive a volume easier to survey, the theorems are distinguished typographically in the same way. To make both the earlier editions and the present one easier to use, references to the Disq. Arithm. give article numbers in place of page numbers, and references to memoirs give their own titles in place of their places of publication. The note originally attached to Article 2 of the memoir '*Theorematis arithmetici demonstratio nova*', which contained a correction to Article 139 of the Disqu. Arithm., has been inserted there at the relevant passage. The note on page 91 is taken from a handwritten note. Apart from this, the present edition differs from the earlier ones only in the correction of some printing errors. My additions are identified by square brackets [ ].

The *Table of the Quadratic Character of Primes* is printed in the manner of Tabula II of the Disqu. Arithm., described in Article 99 and especially used (in Article 331) for factoring numbers. The handwriting of the manuscript entitled '*Quadratorum numeris primis divisorum residua lateralia*' most closely resembles that of the second part of the table for converting common fractions into decimal fractions. In place of the horizontal strokes indicating a quadratic residue, it contains small circles; those in adjacent horizontal or vertical rows are always connected by lines. While proofreading I noticed several errors. I then found 190 discrepancies in the characters in a single comparison with JACOBI's *Canon Arithmeticus*, and by determining them directly found agreement with those printed tables. The edition here has been corrected accordingly.

The first part of the *Table for Converting Common Fractions into Decimal Fractions* is arranged here similarly to Tabula III of the Disqu. Arithm. For

the primes and their powers p^π between 3 and 463 it contains the mantissas (1), (2)..(0) of the decimal fractions of $\frac{10.r}{p^\pi}$, $\frac{10.rr}{p^\pi}$..$\frac{10}{p^\pi}$. Here r denotes unity, so that (1) = (2) = ..(0), when 10 is a primitive root of p^π; otherwise r denotes the smallest of those primitive roots of p^π for which, as base, the index of 10 takes its smallest value. To make the table easier to use, I have added the values other than 1 of r on page 420. The manuscript, which also does not yet give the distinguishing digits of the different periods, most closely resembles the Analysis residuorum in appearance and seems to precede in date the piece placed here as the second part of the whole table. This second part contains, for the primes and their power p^π between 467 and 997, the mantissas of the decimal fractions of $\frac{100}{p^\pi}$. The manuscript gives the divisors in decreasing order and ends with the words: *Explicitus October* 11. 1795. In print I have added, for the divisor 191 in period (1), the 71st digit, and omitted, for the divisor 829, a number between the 151st and 152nd digits.

The first part of the *Table of the Frequency of Primes*, discussed by Gauss himself in a letter (page 444), giving the number of primes in each of the first 1000 thousand groups, exists in a manuscript by Gauss. His manuscript remains, however, do not contain the counts mentioned in the letter of the hundred groups within the first million that contain a specified number of primes. The other part of the table, for the second and third million, comes from a manuscript by Goldschmidt alone. Herr Meissel, by counting and by his formula, has found the following corrections to pages 436 and 437:

Thousand	Gauss	True Value	Thousand	Gauss	True Value
20	102	104	546	68	69
159	87	77	601	75	76
199	96	86	625	68	78
206	85	83	668	73	74
245	78	88	675	69	73
289	85	77	784	74	75
290	84	85	800	81	71
334	80	81	879	68	78
352	80	81	985	74	70
501	78	79			

The formula of Encke mentioned in the letter from Gauss to Encke seems to be the following

$$\frac{n}{\log n} \sqrt[2\log n]{10}$$

which Encke gives in a letter to Gauss of 4 December 1849.

The *Table of the Number of Classes of Binary Quadratic Forms* gives the number of genera and classes and the index of irregularity for negative determinants in hundred groups 1 to 30, 43, 51, 61, 62, 63, 91 to 100, 117 to 120;

also, in a separate compilation, for those of the 1st, 3rd and 10th thousand groups, for the first 800 of the forms $-(15n+7)$ and $-(15n+13)$, and for some very large determinants; and for positive determinants in the 1st, 2nd, 3rd, 9th and 10th hundred groups and some others. The manuscript consists of separate slips with tables arranged in various ways. For instance, the older ones use the word Ordo in place of Genus, as in the individual hundred groups except the 9th and 10th for positive determinants, and also in some preliminary compilations in thousand groups. To make the arrangement easier to survey, the notation of the Disqu. Arithm. has been used throughout here. For lack of space, the greatest and least quotients obtained by dividing the number of classes by the determinant, and the numbers of determinants for which the quotient falls within certain bounds, are not placed below the individual hundred groups, but collected at the end of the table for negative determinants. Some surviving notes seem to indicate that Gauss first calculated the classes for determinants belonging to the same hundred group and the same remainder on division by 15. The determinants in these divisions were then arranged by the number of genera and classes, and finally all those in the same hundred group were ordered in the way reproduced here. Several later corrections have been inserted into the tables of individual hundred groups, but not into the compilations in thousand groups. Only the two tables with determinants of the forms $-(15n+7)$ and $-(15n+13)$ contain dates, respectively '*Expl. In. Febr. 1801*' and '*Expl. 27 Febr. 1807.*'

Among the errors I have noticed in these tables are the following. To make them easier to check, I give the period numbers of the fundamental classes, for example 4 . 4 . 2 for the determinant -11713, and the numbers represented by forms of the respective fundamental classes, for example 31 . 37 . 2. As in my memoir in volume 14 of the Memoirs of the Royal Society of Sciences at Göttingen, fundamental classes here mean classes which, together with the classes in their periods, produce by composition every properly primitive class of the determinant once and only once.

The following entries have already been omitted:

Hundred 9	G. IV ...	3.,	$-827[21 :: 3]$
26	IV	14	$-2587[24 :: 11]$
26	VIII	6	$-2564[56 :: 3]$
91	I	111	$-9059[117 :: 5]$
120	IV	32	$-11956^{*}2^{*}[36 . 2 :: 11 . 49]$
1	I	2	$+37[3 :: 3]$
2	I	2	$+101[3 :: 4]$

and added:

Hundred 9	G. IV . . .	3 . .	−828[6 . 2 :: 31 . 23]
26	IV	14	−2586[28 . 2 :: 7 . 2]
26	VIII	6	−2565[12 . 2 . 2 :: 7 . 2 . 5]
91	I	117	−9059[117 :: 5]
120	IV	32	−11966*2*[32 . 4 :: 5 . 83]
1	I	3	+37[3 :: 3]
2	I	3	+101[3 :: 4]

In the table for Hundred 3 and the last one on page 476, which in the manuscript occur together with a record of Hundreds 1 and 2 differing in appearance from the one printed here, the twelve divisions are designated, instead of I. Ordo unicus. 1; I. O. 2; I. O. 3; I. O. 4; II. Ordines duo. 1. 1; II. O. 1. 2; II. O. 2. 2; II. O. 3. 3; III. Ordines quatuor. 1. 1. 1. 1; III. O. 1. 1. 2. 2; III. O. 2. 2. 2. 2; IV. Ordines octo 1. 1. 1. 1. 1. 1. 1. 1, in the manner otherwise used here, as G. I. 1; G. I. 3; G. I. 5; G. I. 7; G. II. 1; G. II. 2; G. II. 3; G. II. 5; G. IV. 1; G. IV. 2; G. IV. 3; G. VIII. 1. Calculation gives, for example, 269. I. 3 [3 :: 4]; 235. IV. 3 [6 . 2 :: 3 . 5]; 401. I. 5 [5 :: 9]; 577. I. 7 [7 :: 3]; 727. II. 5 [10 :: 3]. (Genera I in place of Genus I on page 469 is a printing error).

Because of printing errors, omit:

Hundred 27.	G. IV	16 . . .	−2624*3*
93	IV	16	−9216
118	VIII	4	−11713*3*

and add:

Hundred 27.	G. IV	16 . . .	−2624*2*[16 . 4 :: 3 . 16]
93	IV	16	−9216*2*[16 . 4 :: 5 . 9]
118	VIII	4	−11713*2*[4 . 4 . 2 :: 31 . 37 . 2]

According to my calculation, also omit:

Hundred 10.	G. II	9 . . .	−972[6 . 3 :: 7 . 13]
17	IV	4	−1660[10 . 2 :: 11 . 5]
20	IV	12	−1982[24 :: 3]
21	IV	6	−2096[30 . 2 :: 3 . 4]
23	IV	9	−2221[18 :: 10]
24	IV	12	−2376[12 . 2 . 2 :: 5 . 8 . 8]
29	IV	9	−2887[25 :: 8]
61	IV	7	−6028[12 . 2 :: 13 . 4]

96	VIII	13	$-9594[20 \cdot 2 \cdot 2 :: 31 \cdot 2 \cdot 13]$
118	IV	25	$-11780[16 \cdot 4 \cdot 2 :: 3 \cdot 8 \cdot 19]$
118	VIII	16	$-11780[16 \cdot 4 \cdot 2 :: 3 \cdot 8 \cdot 19]$
119	VIII	16	$-11840[24 \cdot 2 \cdot 2 :: 5 \cdot 9 \cdot 7]$
Thousand I	G. II ...	3 ...	$-541[10 :: 11]$
I	II	4	$-415[10 :: 13]$
I	II	8	$-527[18 :: 3]$
I	II	8	$-722[18 :: 3]$
I	II	9	$-194[20 :: 5]$
I	II	9	$-459[6 \cdot 3 :: 5 \cdot 9]$
I	II	9	$-972[6 \cdot 3 :: 7 \cdot 13]$
I	II	11	$-842[26 :: 13]$
I	IV	3	$-784[8 \cdot 2 :: 5 \cdot 4]$
I	IV	4	$-532[4 \cdot 2 :: 13 \cdot 7]$
I	IV	5	$-425[12 \cdot 2 :: 3 \cdot 17]$
I	IV	5	$-608[12 \cdot 2 :: 13 \cdot 27]$
I	IV	5	$-629[18 \cdot 2 :: 5 \cdot 2]$
III	II	15	$-2578[16 :: 13]$
X	I	111	$-9059[117 :: 5]$
forms $-(15n+13)$	IV	4	$-2788^*2^*[8 \cdot 2 :: 19 \cdot 17]$

and add:

Hundred 10.	G. II	9	$-972^*3^*[6 \cdot 3 :: 7 \cdot 13]$
17	IV	12	$-1700[24 \cdot 2 :: 3 \cdot 17]$
20	IV	12	$-1937[24 \cdot 2 :: 7 \cdot 2]$
21	IV	6	$-2097[12 \cdot 2 :: 47 \cdot 2]$
23	IV	9	$-2224[18 \cdot 2 :: 5 \cdot 16]$
24	IV	12	$-2366[24 \cdot 2 :: 3 \cdot 2]$
29	IV	9	$-2885[18 \cdot 2 :: 3 \cdot 5]$
61	IV	6	$-6028[12 \cdot 2 :: 13 \cdot 4]$
96	VIII	13	$-9546[26 \cdot 2 \cdot 2 :: 5 \cdot 3 \cdot 37]$
118	IV	25	$-11750[50 \cdot 2 :: 3 \cdot 47]$
118	VIII	16	$-11780^*2^*[16 \cdot 4 \cdot 2 :: 3 \cdot 8 \cdot 19]$
119	VIII	16	$-11840^*2^*[16 \cdot 4 \cdot 2 :: 3 \cdot 16 \cdot 5]$
Thousand I.	G. II	5 ...	$-415[10 :: 13]$
I	II	5	$-541[10 :: 11]$
I	II	9	$-459^*3^*[6 \cdot 3 :: 5 \cdot 9]$
I	II	9	$-527[18 :: 3]$
I	II	9	$-722[18 :: 3]$
I	II	9	$-972^*3^*[6 \cdot 3 :: 7 \cdot 13]$
I	II	10	$-194[20 :: 5]$

I	II	13	$-842[26 :: 13]$
I	IV	2	$-532[4\,.\,2 :: 13\,.\,7]$
I	IV	4	$-784[8\,.\,2 :: 5\,.\,4]$
I	IV	6	$-425[12\,.\,2 :: 3\,.\,17]$
I	IV	6	$-608[12\,.\,2 :: 13\,.\,27]$
I	IV	9	$-629[18\,.\,2 :: 5\,.\,2]$
III	II	15	$-2518[30 :: 19]$
X	I	117	$-9059[117 :: 5]$
forms $-(15n+13)$	IV	4	$-2788[8\,.\,2 :: 19\,.\,17]$

The tables *for Circle Division* give, for 2452 numbers of the forms $aa+1$, $aa{+}4$, $aa{+}9$, $\ldots.\, aa{+}81$, all the odd prime divisors p beside the corresponding a, in those cases where all the prime divisors are less than 200; only then are $aa+1$ and so on called factorable.

To make the tables easier to use, Gauss has constructed, for each table from which the complete factorizations of numbers of one of the particular forms can be determined, an auxiliary table giving beside each prime p those numbers a whose square, increased by 1 or 4 . . ., has p as its greatest prime divisor.

The chief purpose of the tables is to facilitate the accurate calculation of arcs whose cotangents are given rational numbers. With their help, arcs for small cotangents can first be combined from arcs for large cotangents, reducing to a very small amount the calculations still needed for the series expressing arcs in terms of their cotangents. The developments towards this end in the manuscript remains are not extensive; the following is the one carried furthest. In it

$$\begin{array}{l}[2]\ [5]\ [13]\ [17]\ [29]\ [37]\ [41]\ [53]\ [61]\ldots[197]\\ (18)\ (57)\ (239)\ \left(\frac{79}{3}\right)\ldots\end{array}$$

denote the arcs with cotangents

$$1\quad 2\quad \frac{3}{2}\quad 4\quad \frac{5}{2}\quad 6\quad \frac{5}{4}\quad \frac{7}{2}\quad \frac{6}{5}\ldots 14\quad 18\quad 57\quad 239\quad \frac{79}{3}\ldots$$

Using the tables to factor $18+i$, $57+i$, $239+i$ into their complex prime factors gives

$$\begin{aligned}(18) &= 2[2]-2[5]-[13]\\ (57) &= -[2]+3[5]-[13]\\ (239) &= 3[2]\qquad -4[13]\end{aligned}$$

and from these

$$\begin{aligned}[2] &= 12(18)+8(57)-5(239)\\ [5] &= 7(18)+5(57)-3(239)\\ [13] &= 9(18)+6(57)-4(239)\end{aligned}$$

further, using the tables,

$$\begin{aligned}(268) &= -2[5] + 2[13] - [17] \quad \cdot \\ (38) &= -[5] \qquad\quad + 2[17]\end{aligned}$$

and from these, by eliminating [17] and substituting the values of [5], [13] obtained above,

$$(38) + 2(268) = (18) - (57) - (239)$$

Eliminating (18) then gives the new determination

$$\begin{aligned}[2] &= 12(38) + 20(57) + 7(239) + 24(268) \\ [5] &= 7(38) + 12(57) + 4(239) + 14(268) \\ [13] &= 9(38) + 15(57) + 5(239) + 18(268) \\ [17] &= 4(38) + 6(57) + 2(239) + 7(268)\end{aligned}$$

After successively using the cotangents 117, 327, 882, 18543, 307, 278, 378, 829, 993, 2943, 447, 606, 931, 1143, 1772, 6118, 34208, 44179, 85353, 485298, 17772, 9466, 330182, 5257, 114669, 12943, $[2][5]\ldots[61]$ are finally expressed in terms of (5257), (9466) ... (485298), and their coefficients are collected in the following columns:

	5257	9466	12943	34208	44179	85353	114669	330182	485298
2	+2805	−398	+1950	+1850	+2021	+2097	+1484	+1389	+808
5	+1656	−235	+1151	+1092	+1193	+1238	+876	+820	+477
13	+2100	−298	+1460	+1385	+1513	+1570	+1111	+1040	+605
17	+875	−124	+608	+577	+630	+654	+463	+433	+252
29	+1359	−193	+945	+896	+979	+1016	+719	+673	+391
37	+590	−84	+410	+389	+425	+441	+312	+292	+170
41	+2410	−342	+1675	+1589	+1736	+1802	+1275	+1193	+694
53	+994	−141	+691	+655	+716	+743	+526	+492	+286
61	+2481	−352	+1725	+1637	+1788	+1855	+1313	+1229	+715

The correctness of these equations, which can be used to determine $[2][5]\ldots[61]$, is seen directly from the factorizations supplied by the tables above:

(5257) =	[2]	+2[5]	−[13]	+[17]	.	.	−[41]	.	−[61]
(9466) =	2[2]	.	.	.	−[29]	−3[37]	.	.	−[61]
(12943) =	[2]	−4[5]	+3[13]	.	.	.	.	.	−[61]
(34208) =	2[2]	−[5]	−2[13]	+[17]	+[29]	.	.	−2[53]	.
(44179) =	3[2]	.	−3[13]	−2[17]	−[29]	.	.	+[53]	.
(85353) =	−[2]	−[5]	+[13]	−[17]	.	−[37]	+2[41]	−[53]	.
(114669) =	−3[2]	.	.	+[17]	.	+[37]	.	+2[53]	+2[61]
(330182) =	−4[2]	+5[5]	+[13]	.	+[29]	−[37]	−[41]	.	+[61]
(485298) =	−2[2]	−[5]	+4[13]	.	−2[29]	+[37]	.	+[53]	.

Gauss collects in the following overview the methods used so far by calculators to determine $\frac{\pi}{4} = (1)$

Machin	$(1) = 4(5) - (239)$
	also Clausen
Euler	$= (2) + (3)$
	(Euler to Goldbach 1746 May 28)
Vega	$= 5(7) + 2(\frac{79}{3})$
	(Vega Thesaurus logar. p. 633)
Vega	$= 2(3) + (7)$
	also Clausen (Astr. Nachr. vol. 25. p. 209)
Rutherford	$= 4(5) - (70) + (99)$
	(Philos. Trans. 1841. p. 283)
Dase	$= (2) + (5) + (8)$
	(Crelle Journal. vol. 27. p. 198)
Gauss. 1.	$= 12(18) + 8(57) - 5(239)$
Gauss. 2.	$= 12(38) + 20(57) + 7(239) + 24(268)$

The first calculations for the tables date from the preparation of the *Disquiss. Arr.*; they were advanced especially in 1846 and 47. By 21 July 1847, 2283 factorizations had been entered in tables in the order reproduced here. The remaining 169 were calculated later, and I have included them in this printing, whose arrangement differs from the original only in using repeated factors instead of powers to make typesetting easier.

The manuscripts containing these last calculations seem to give the results in the form in which they were first found. The order in which the numbers a appear suggests that the divisors of $aa + 1$ and so on were sought only for the smaller numbers, and that the larger ones were obtained from these by particular devices. Only the following rule is recorded, however: *From three numbers* a, $2a - n$, $2a + n$ *a fourth is found*

$$\frac{4a^3 - (nn-3)a}{nn+1}$$

This is always an integer for $n = 0$ *and* $n = 1$, *otherwise only*

$$\textit{for} \quad a \equiv 0 \quad \textit{and} \quad \equiv \pm\sqrt{-1} \quad \textit{mod}(nn+1) \quad \textit{when } n \textit{ is even}$$

$$\textit{and for} \quad a \equiv 0 \quad \textit{and} \quad \equiv \pm\sqrt{-1} \quad \textit{mod}\frac{nn+1}{2} \quad \textit{when } n \textit{ is odd}$$

Examples	$a = 253,$	$n = 6,$	1750507
	$a = 294,$	$n = 11,$	832902
	$a = 119,$	$n = 1,$	3370437
	$a = 57,$	$n = 3,$	74043
	$a = 123,$	$n = 9,$	90657

The fourth number has no prime divisors other than those of the first three, and of these only the odd prime divisors belonging to the number n are excluded.

The table '*Quadratorum myrias prima*' gives the thousands and hundreds in its heading row, the tens and units of the underlying number in its first vertical column, and, in the last vertical column of each individual table the three lowest digits of the square, and in the interior the four or five higher digits of the square.

The table '*Indices of Primes in the Higher Number Domain*' gives the modulus in each case in the top horizontal row, the base used in the second row, the residues in the first vertical column, and the indices in the interior. The stars $*$ denote zero residues.

The manuscript of the fragment '*Eighth Section. A Fuller Consideration of Certain Investigations Concerning Circle Division*' seems to date from the reworking of the 'Analysis residuorum' into the 'Disquisitiones arithmeticae'. The letters from Gauss to Dirichlet confirm the view that in higher arithmetic, too, Gauss discovered considerably more than is found in his manuscript remains.

Schering.

CONTENTS.

GAUSS'S WORKS, VOLUME II. HIGHER ARITHMETIC.

Papers.

A New Proof of an Arithmetical Theorem	1808 Jan. . .	Page 1
Summation of Certain Special Series	1808 Aug. . .	— 9
New Proofs and Extensions of the Fundamental Theorem in the Theory of Quadratic Residues	1817 Feb. .	— 47
Theory of Biquadratic Residues. First Paper	1825 Apr. .	— 65
Theory of Biquadratic Residues. Second Paper	1831 Apr. .	— 93

Reviews of His Own Writings.

A New Proof of an Arithmetical Theorem	1808 May . .	— 151
Summation of Certain Special Series	1808 Sept. .	— 155
Of the Fundamental Theorem in the Theory of Residues, etc.	1817 March .	— 159
Theory of Biquadratic Residues. Paper I.	1825 April .	— 165
Theory of Biquadratic Residues. Paper II.	1831 April .	— 169

Reviews of Other Writings.

[Dalberg] Investigations of the Arithmetical and Geometrical Irreducibility of Numbers and Their Powers	1809 March .	— 181
Chernac. Arithmetical Sieve	1812 March .	— 181
Burckhardt. Tables of Divisors	1814 Nov. 1816 Nov. 1817 Aug. .	— 183
Erchinger. Construction of the Seventeen-Sided Polygon	1825 Dec. .	— 186
Seeber. Investigations of the Properties of Positive Ternary Quadratic Forms	1831 July . .	— 188

Manuscript Remains.

Analysis of Residues:

Chapter Six. First Part. Solution of the Congruence $x^m - 1 \equiv 0$ Page 199
. . . . . .
Chapter Eight. General Investigations of Congruences . . . . . — 212
Further Development of the Investigations of Pure Equations — 243
. . . . . .
Proof of Some Theorems Concerning the Periods of Classes of Binary — 266
Quadratic Forms . . . . . .
On the Connection between the Number of Classes into Which Binary — 269
Quadratic Forms Are Distributed and Their Determinant. I. II . . X
. . . . . .
Geometrical Aspect of Ternary Forms . . . . . — 305
On the Theory of Biquadratic Residues. I. . . VI . . . . . — 313
On the Theory of Complex Numbers. I. . . VI . . . . . — 387
Table of the Quadratic Character of Primes . . . . . — 399
Table for Converting Common Fractions into Decimal Fractions — 411
. . . . . .
Table of the Frequency of Primes . . . . . — 435
Table of the Number of Classes of Binary Quadratic Forms . . . . . — 449
Table for Circle Division . . . . . — 477
A New Quadrature of the Circle . . . . . -. . . . . — . 497
On Calculating Logarithms . . . . . — 501
First Ten Thousand Squares . . . . . — 504
Indices of Primes in the Higher Number Domain . . . . . , ... — 506
Auxiliary Table for Solving the Equation $A = fxx + gyy$ . . . . . — 509
Eighth Section. A Fuller Consideration of Certain Investigations — 510
Concerning Circle Division.
Letters from Gauss to Dirichlet . . . . . — 514

Remarks . . . . . — 519

GÖTTINGEN,
PRINTED BY THE DIETRICH UNIVERSITY PRINTING HOUSE.
W. FR. KAESTNER.

Carl Friedrich Gauss

Collected Works

Volume III

A New Proof of the Theorem That Every Polynomial in One Variable Can Be Resolved into Real Factors of the First or Second Degree

Complete 1799 dissertation and complete second proof of 1815

Modern English translation

The historical title matter and the complete 1799 dissertation, Articles 1–24, follow, with Gauss's ten historical footnotes and all four figures. The complete second proof, Articles 1–20 with both historical footnotes, follows with its title matter. It was presented in 1815 and published in 1816. Later Volume-III works are outside this reader. Historical references retain the source numbering.

Historical source: Carl Friedrich Gauss, *Werke*, Volume III, Göttingen, 1866; dissertation first published at Helmstedt by C. G. Fleckeisen, 1799. Originally German title matter is rendered in modern German in the German reader; the historical original is retained separately.

AI-translated into English using OpenAI GPT-6.1 Sol; AI-produced typesetting.

Translation sources and terminology

Historical text: Carl Friedrich Gauss, *Werke*, Volume III, Göttingen, 1866. These English and German texts are AI-translated from the original-language edition. The following human translations and writings are consulted for the stated terminology and usage; their running text is not reproduced. Gauss's original mathematical formulations remain controlling.

Paul Taylor; Bernard Leak. Taylor's English translation of Gauss's second proof of the fundamental theorem of algebra, with corrections by Leak, 1983. The corresponding passages of the 1815 second proof were consulted for English polynomial, divisor, degree, symmetric-function and proof terminology. Related terminology was also consulted for the 1799 dissertation, for which this is not a parallel translation. No running text from this human translation is adopted. Its later use of complex quantities does not replace Gauss's definition of imaginary quantities here. The consulted online edition identifies the translation as December 1983, its LaTeX version as August 2003, and the underlying source as last modified on 8 June 2007. Its acknowledgements credit Mark Wainwright for returning Taylor's notes and Nikita Danilov for typo corrections.
`https://www.paultaylor.eu/misc/gauss.html`

H. Maser. German translator and editor, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Related German terminology for algebraic functions, roots, divisibility, quotients and degrees; not a parallel translation of this dissertation.
`https://archive.org/details/carlfriedrichga00gausgoog`

James Caddall Morehead and Adam Miller Hiltebeitel. Translators of Gauss's *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX edition. Related English geometrical, coordinate and infinitely small quantity terminology; not a parallel translation of the 1799 dissertation.
`https://www.gutenberg.org/ebooks/36856`

Ulrich Görtz. *Algebra*, Wintersemester 2021/22, section 3.1.1, Examples 3.1–3.2. Related contemporary German usage for polynomials, indeterminates, sums, numerators and denominators, and mathematical argument. This is a terminology reference, not a parallel translation of either proof. No running text or modern ring-theoretic argument is adopted.
`https://math.ug/a-ws2122/sect0006.html`

AI authorship and sources. AI-translated using OpenAI GPT-6.1 Sol, with AI-produced typesetting. Gauss is the author of the historical mathematical text. The named human translations are credited for their stated terminology and usage roles.

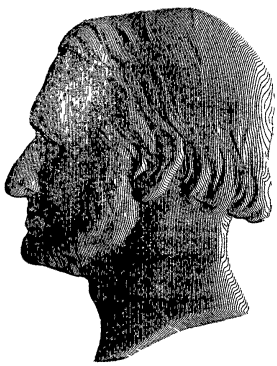
Scholarly citation metadata: `CITATIONS.bib`.

CARL FRIEDRICH GAUSS: WORKS

VOLUME III.

CARL FRIEDRICH GAUSS
WORKS

THIRD VOLUME



EDITED
BY THE
ROYAL SOCIETY OF SCIENCES
AT GÖTTINGEN

1866.

A NEW PROOF
OF THE THEOREM
THAT EVERY POLYNOMIAL

IN ONE VARIABLE
CAN BE RESOLVED INTO REAL FACTORS
OF THE FIRST OR SECOND DEGREE

SUBMITTED FOR
THE HIGHEST HONOURS IN PHILOSOPHY
TO THE ILLUSTRIOUS FACULTY OF PHILOSOPHY
OF THE ACADEMIA JULIA CAROLINA

BY

CARL FRIEDRICH GAUSS

HELMSTEDT
AT C. G. FLECKEISEN. MDCCLXXXXIX.

A NEW PROOF OF THE THEOREM
THAT EVERY POLYNOMIAL
IN ONE VARIABLE
CAN BE RESOLVED INTO REAL FACTORS OF THE FIRST OR SECOND DEGREE.

1.

Every determinate algebraic equation can be reduced to the form

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

where m is a positive integer. If we denote the left-hand side of this equation by X and suppose that the equation $X = 0$ is satisfied by several unequal values of x, say by setting $x = \alpha$, $x = \beta$, $x = \gamma$, etc., then the function X will be divisible by the product of the factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc. Conversely, if the product of several linear factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc. divides the function X, then the equation $X = 0$ will be satisfied by setting x equal to any of the quantities α, β, γ, etc. Finally, if X equals a product of m such linear factors (whether they are all different or some of them are identical), no linear factors other than these can divide the function X. An equation of degree m therefore cannot have more than m roots. At the same time, however, it is evident that an equation of degree m can have *fewer* roots even if X can be resolved into m linear factors: for if some of these factors are identical, the number of different ways of satisfying the equation will necessarily be smaller than m. Yet, for the sake of uniformity, mathematicians have preferred to say that the equation has m roots in this case too, with only some of them being equal to one another; which they may certainly allow themselves to do.

2.

What has been set out so far is adequately proved in books on algebra and nowhere offends geometric rigour. But analysts seem to have adopted too hastily, and without a prior sound proof, the theorem on which almost the entire theory of equations rests: *every function such as X can always be resolved into m linear factors*, or, what agrees with this completely, *every equation of degree m actually has m roots*. Since even quadratic equations very often lead to cases that contradict this theorem, algebraists, in order to bring these cases under it, were forced to invent an imaginary quantity whose square is -1. They then recognized that, if quantities of the form $a + b\sqrt{-1}$ are admitted in the same way as real quantities, the theorem holds not only for quadratic equations but also for cubic and biquadratic equations.

Yet this by no means justified concluding that, once quantities of the form $a + b\sqrt{-1}$ are admitted, every equation of the fifth or a higher degree can be satisfied, or, as it is usually expressed (though I would not favour this slippery wording), that the roots of every equation can be reduced to the form $a+b\sqrt{-1}$. In substance, this theorem differs in no respect from the one stated in the title of this work; giving a new rigorous proof of it is the aim of the present dissertation.

Moreover, ever since analysts discovered that there are infinitely many equations that would have no root at all unless quantities of the form $a+b\sqrt{-1}$ were admitted, such fictitious quantities have been regarded as a special kind of quantity, called *imaginary* to distinguish them from *real* quantities, and have been introduced throughout analysis. By what right? I do not discuss that here. — I shall complete my proof without any help from imaginary quantities, although I too would be entitled to use the same freedom that all recent analysts have used.

3.

Although what most elementary books offer as a proof of our theorem is so flimsy and so far removed from geometric rigour as scarcely to deserve mention, I shall nevertheless touch on it briefly so that nothing is left out. 'To show that every equation

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

or $X = 0$ actually has m roots, they undertake to prove that X can be resolved into m linear factors. For this purpose they assume m linear factors $x - \alpha$, $x - \beta$, $x - \gamma$, etc., where α, β, γ, etc. are still unknown, and set their product equal to the function X. Then, by comparing coefficients, they obtain m equations from which, they say, the unknowns α, β, γ, etc. can be determined, since their number is also m. Namely, $m - 1$ unknowns can be eliminated, leaving an equation containing only whichever unknown one wishes.' Passing over the other objections that could be made to such reasoning, I ask only: how can we be certain that this final equation actually has any root? Why could it not happen that no magnitude in the entire range of real and imaginary quantities satisfies either this final equation or the proposed one? — Experts will, moreover, readily see that this final equation must be *entirely identical* with the proposed one if the calculation has been carried out correctly: namely, eliminating the unknowns β, γ, etc. must give the equation

$$\alpha^m + A\alpha^{m-1} + B\alpha^{m-2} + \text{etc.} + M = 0$$

There is no need to say more about this reasoning.

Some authors who seem to have noticed the weakness of this method assume as an *axiom* that every equation actually has roots: if not possible roots, then impossible ones. They do not seem to have made sufficiently clear what they mean by possible and impossible quantities. If possible quantities are to mean the same as real quantities, and impossible quantities the same as imaginary ones, that axiom can by no means be admitted: it necessarily requires a proof. Yet the expressions do not seem intended in that sense; rather, the axiom seems to mean this: 'Although we are not yet certain that there must be m real or imaginary quantities satisfying a given equation of degree m, we shall nevertheless suppose this for a while; for if it should happen that so many real and imaginary quantities cannot be found, we shall certainly have a way out by saying that the remaining ones are impossible.' If someone prefers this wording to saying simply that the equation would not have so many roots in this case, I have no objection. But if he then uses these impossible roots as though they were something real, and says, for example, that the sum of all the roots of the equation $x^m + Ax^{m-1} + \text{etc.} = 0$ is $= -A$, even if there are impossible roots among them (an expression that properly means *even if some are missing*), I cannot approve of this at all. For impossible roots, understood in this sense, are still roots; that axiom therefore cannot possibly be admitted without proof, and would it be unreasonable to wonder whether there might be equations that do not even have impossible roots?[*)]

[*)] Here I always understand an imaginary quantity to mean a quantity of the form $a+b\sqrt{-1}$, as long as b is not $= 0$. All mathematicians of the first rank have always understood the expression in this sense. I do not think we should listen to those who have wished to call a quantity $a + b\sqrt{-1}$ imaginary only when $a = 0$, but impossible when $a = 0$ is not the case, since this distinction is neither necessary nor of any use. — If imaginary quantities are to be retained in analysis at all (which, for several reasons, seems more advisable than abolishing them, provided they are established on a sufficiently sound basis), they must necessarily be regarded as just as possible as real quantities. I would therefore prefer to include real and imaginary quantities under the common name *possible quantities*. In contrast, I would call a quantity *impossible* if it were required to satisfy conditions that cannot be satisfied even when imaginary quantities are admitted, but in such a way that this *wording* means the same as saying that no such quantity exists anywhere in the range of magnitudes. I would by no means allow a special kind of quantity to be formed from this. If someone says that a rectilinear equilateral right-angled triangle is impossible, no one will deny it. But if he wished to regard such an impossible triangle as a new kind of triangle and apply other properties of triangles to it, who could keep from laughing? This would be playing with words, or rather abusing them. — Even the greatest mathematicians have quite often applied truths that clearly presuppose the possibility of the quantities concerned to quantities whose possibility was still doubtful. Nor would I deny that such liberties generally concern only the form and, as it were, the covering of the reasoning, which a true mathematician's sharp eye can soon penetrate. Yet it seems more advisable, and more worthy of the eminence of a science rightly celebrated as the most perfect model of clarity and certainty, either to banish such freedoms altogether, or at least to use them more sparingly and only where even the less practised can see that the matter could have been completed without their help, perhaps less briefly, but just as rigorously. — I would not, moreover, deny that what I have said here against the misuse of

4.

Before reviewing other mathematicians' proofs of our theorem and setting out what seems objectionable to me in each, I note that it is enough to show only that every equation of any degree

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + M = 0$$

or $X = 0$ (where the coefficients A, B, etc. are supposed real) can be satisfied in at least one way by a value of x of the form $a + b\sqrt{-1}$. For it is known that X will then be divisible by the real quadratic factor $xx - 2ax + aa + bb$ if b is not $= 0$, and by the real linear factor $x - a$ if $b = 0$. In either case the quotient will be real and of lower degree than X; and since, by the same reasoning, this quotient must have a real factor of the first or second degree, it is evident that continuing this operation will ultimately resolve the function X into real linear or quadratic factors, or, if one prefers to use two imaginary linear factors in place of each real quadratic factor, into m linear factors.

5.

The first proof of the theorem is due to the distinguished mathematician D'Alembert, *Recherches sur le calcul intégral, Histoire de l'Acad. de Berlin, Année* 1746, p. 182 ff. It is also found in Bougainville, *Traité du calcul intégral, à Paris* 1754, p. 47 ff. The principal steps of this method are as follows.

First he shows that, if any function X of the variable x becomes $= 0$ either for $x = 0$ or for $x = \infty$, and can attain an infinitely small positive real value by assigning a real value to x, this function can also attain an infinitely small negative real value through a value of x that is either real or of the imaginary form $p + q\sqrt{-1}$. Namely, if Ω denotes an infinitely small value of X, and ω the corresponding value of x, he asserts that ω can be expressed by a rapidly convergent series $a\Omega^\alpha + b\Omega^\beta + c\Omega^\gamma$, etc., where the exponents α, β, γ, etc. are continually increasing rational quantities, which therefore, at least beyond some fixed distance from the beginning, become positive and make the terms in which they occur infinitely small. Now, if none of these exponents is a fraction with an even denominator, all the terms of the series become real for both positive and negative values of Ω. If, however, there are fractions with even denominators among these exponents, then for a negative value of Ω the corresponding terms are known to have the form $p + q\sqrt{-1}$. But because of the infinite convergence of the series, in the former case it is enough to retain only the first (that is, the largest) term; in the latter there is no need to proceed beyond the term that first produces an imaginary part.

impossible quantities could in a certain respect also be objected against imaginary quantities; but I reserve their defence, together with a fuller account of this entire matter, for another occasion.

By similar reasoning it can be shown that, if X can attain an infinitely small negative value from a real value of x, this function can attain an infinitely small positive real value from a real value of x or an imaginary one of the form $p + q\sqrt{-1}$.

From this he concludes, secondly, that there is also some finite real value of X, negative in the former case and positive in the latter, that can be produced by an imaginary value of x of the form $p + q\sqrt{-1}$.

It follows that, if X is a function of x that attains a real value V from a real value v of x, and also attains from a real value of x a real value greater or smaller by an infinitely small quantity, it can also take a real value smaller or greater, respectively, than V by an infinitely small and hence by a finite quantity, by assigning to x a value of the form $p + q\sqrt{-1}$. This is readily derived from what precedes by conceiving $V + Y$ substituted for X, and $v + y$ for x.

Finally, the distinguished D'ALEMBERT asserts that, if X is supposed capable of traversing an entire interval between two real values R, S (that is, of becoming equal both to R and to S, and to all intermediate real values), by assigning to x values always of the form $p + q\sqrt{-1}$, the function X can be increased or decreased still further by any finite real quantity (according as $S > R$ or $S < R$), while x always remains of the form $p + q\sqrt{-1}$. For if there were a real quantity U (with S supposed to lie between it and R) to which X could not become equal through such a value of x, there must be a *maximum* value of X (when $S > R$; a minimum when $S < R$), say T, attained from a value $p + q\sqrt{-1}$ of x, such that no value of the same form could be assigned to x that would bring the function X any closer to U, even by the smallest amount. Now, if in this equation between X and x we substitute $p + q\sqrt{-1}$ everywhere for x and then set equal to zero both the real part and the part containing the factor $\sqrt{-1}$, after omitting that factor, two other equations can be obtained by elimination from the two resulting equations (which contain p, q and X together with constants). One contains p, X and constants; the other, free of p, contains only q, X and constants. Thus, since X has traversed all values from R to T through real values of p, q, what precedes shows that X can approach U still more closely by assigning to p, q values of the forms $\alpha + \gamma\sqrt{-1}$, $\beta + \delta\sqrt{-1}$, respectively. But then $x = \alpha - \delta + (\gamma + \beta)\sqrt{-1}$, that is, it is still of the form $p + q\sqrt{-1}$, contrary to the hypothesis.

Now, if X is supposed to denote a function such as $x^m + Ax^{m-1} + Bx^{m-2} +$ etc. $+ M$, it is readily seen that real values can be assigned to x such that X traverses an entire interval between two real values. Hence x can attain some value of the form $p + q\sqrt{-1}$ from which X becomes $= 0$. Q. E. D.*)

*) It should be noted that, in his own account of this proof, the distinguished D'ALEMBERT used geometrical considerations, regarding X as the abscissa and x as the ordinate of a curve (following the practice of all mathematicians in the first part of this century, among whom

6.

The objections that seem possible against D'ALEMBERT's proof come down chiefly to the following.

1. The distinguished d'A. raises no doubt about the *existence* of values of x corresponding to given values of X, but assumes it and investigates only the *form* of those values.

Although this objection is in itself very serious, here it concerns only the form of expression, which can easily be corrected so as to remove it entirely.

2. The assertion that ω can always be expressed by a series of the kind he gives is certainly false if X is also to designate any transcendental function (as d'A. suggests in several places). This is evident, for example, if we put $X = e^{\frac{1}{x}}$, or $x = \frac{1}{\log X}$. Yet if we restrict the proof to the case in which X is an algebraic function of x (which suffices for the present purpose), the proposition is indeed true. — d'A., moreover, has offered nothing to support his supposition. The celebrated BOUGAINVILLE supposes X to be an algebraic function of x and recommends NEWTON's parallelogram for finding the series.

3. He uses infinitely small quantities more freely than is consistent with geometric rigour, or than a careful analyst would allow, at least in our own time (when they have a deservedly bad reputation). Nor does he make the leap from an infinitely small value of Ω to a finite one sufficiently clear. He seems to infer his proposition that Ω can also attain some finite value, less from the possibility of an infinitely small value of Ω than from this: if Ω denotes a very small quantity, then because of the rapid convergence of the series, the more terms of the series are taken, the closer one comes to the true value of ω; or, the more terms are included in the sum taken for ω, the more accurately the equation expressing the relation between ω and Ω, or x and X, will be satisfied. Apart from the fact that this entire argument seems too vague to yield any rigorous conclusion, I note that there are indeed series that, however small a value is assigned to the quantity in whose powers they proceed, nevertheless always diverge, so that, if only they are continued far enough, one can reach terms greater than any given quantity[*)]. This happens

the notion of functions was less familiar). Since, however, all his reasoning, considered only in its substance, rests on no geometrical principles but on purely analytical ones, and the expressions imaginary curves and imaginary ordinates seem rather harsh and more liable to offend the present-day reader, I have preferred a purely analytical presentation here. I added this note so that no one comparing D'ALEMBERT's own proof with this brief account should suspect that anything essential has been changed.

[*)] I note in passing on this occasion that many of these series seem at first sight extremely convergent: for example, most of those that the distinguished EULER uses in the latter part of the *Inst. Calc. Diff.*, Chapter VI, pp. 441–474, to assign as closely as possible the sums of other series (the remaining series on pp. 475–478 can indeed converge). As far as I know, no one has observed this before. It would therefore be very desirable to show clearly and rigorously why series of this kind, which at first converge very rapidly, then gradually more

when the coefficients of the series form a hypergeometric progression. It was therefore necessary to prove that such a hypergeometric series could not arise in the present case.

Moreover, it seems to me that the distinguished d'A. was wrong to resort to infinite series here, and that they are unsuitable for establishing this fundamental theorem of the theory of equations.

4. From the supposition that X can attain the value S, but not the value U, it does not yet follow that between S and U there must lie a value T that X can reach but cannot exceed. Another case still remains: there could be a limit between S and U that X can approach as closely as one wishes, yet never reach. From the arguments given by the distinguished d'A. it follows only that X can exceed every value it has reached by a further finite quantity. For instance, once it has become $= S$, it can be increased by some further finite quantity Ω; after this a new increment Ω' can be added, then another increment Ω'', etc., so that however many increments have already been added, none should be regarded as the last, but a new one can always be added. Yet although the *number* of possible increments is bounded by no limits, it could certainly happen that, if the increments $\Omega, \Omega', \Omega''$, etc. continually decreased, the sum $S + \Omega + \Omega' + \Omega''$, etc. would nevertheless never attain some limit, however many terms were considered.

Although this case cannot occur when X denotes a polynomial in x, without a proof that it cannot happen the method must nevertheless be regarded as incomplete. When, however, X is a transcendental function, or even an algebraic fractional function, that case can indeed occur: for example, whenever an infinitely large value of x corresponds to some value of X. Then D'ALEMBERT's method seems incapable of being reduced to unquestionable principles without many complications, and perhaps in some cases not at all.

For these reasons I cannot regard D'ALEMBERT's proof as satisfactory. Nevertheless, it seems to me that its real force is by no means broken by all these objections. I believe that on the same foundation (though in a very different way, and at least with greater circumspection) not only can a rigorous proof of our theorem be built, but everything one could wish for in the theory of *transcendental* equations can be obtained from it. I shall discuss this very important matter more fully on another occasion; meanwhile, compare Article 24 below.

and more slowly, and finally diverge more and more, nevertheless give a nearly true sum provided not too many terms are taken, and how far such a sum can safely be regarded as exact?

7.

After D'ALEMBERT, the distinguished EULER published his investigations on the same subject in *Recherches sur les racines imaginaires des équations, Hist. de l'Acad. de Berlin A.* 1749, p. 223 ff. He gave two methods there; the substance of the first is as follows.

First the distinguished Euler undertakes to prove that, if m denotes any power of the number 2, the function $x^{2m} + Bx^{2m-2} + Cx^{2m-3} + \text{etc.} + M = X$ (in which the coefficient of the second term is $= 0$) can always be resolved into two real factors in which x rises to degree m. For this purpose he assumes two factors,

$$x^m - ux^{m-1} + \alpha x^{m-2} + \beta x^{m-3} + \text{etc.}, \quad \text{and} \quad x^m + ux^{m-1} + \lambda x^{m-2} + \mu x^{m-3} \text{ etc.}$$

where the coefficients u, α, β, etc., λ, μ, etc. are still unknown, and sets their product equal to the function X. Comparing coefficients then gives $2m - 1$ equations, and evidently all that must be proved is that real values satisfying these equations can be assigned to the unknowns u, α, β, etc., λ, μ, etc. (whose number is also $2m-1$). Euler now asserts that, if u is first regarded as known, so that the number of unknowns is one less than the number of equations, then by suitably combining the equations according to known algebraic methods, all of α, β, etc., λ, μ, etc. can be determined rationally, without any extraction of roots, from u and the coefficients B, C, etc., and thus attain real values as soon as u becomes real. Moreover, all of α, β, etc., λ, μ, etc. can be eliminated to give an equation $U = 0$, where U is a polynomial in u alone and the known coefficients. Expanding this equation itself by the usual method of elimination would be an immense task when the proposed equation $X = 0$ is of a rather high degree, and completely impossible for an unspecified degree (according to Euler himself, p. 239). Yet here it is enough to know one property of this equation: the constant term in U (which does not involve the unknown u) is necessarily negative. From this it is known to follow that the equation has at least one real root, or that u, and therefore also α, β, etc., λ, μ, etc., can be determined as real quantities in at least one way. That property can be established by the following considerations. Since $x^m - ux^{m-1} + \alpha x^{m-2} + \text{etc.}$ is supposed to be a factor of the function X, u must be the sum of m roots of the equation $X = 0$, and must therefore have as many values as there are different ways of choosing m out of $2m$ roots; that is, by the principles of combinatorics, $\frac{2m.2m-1.2m-2.\ldots.m+1}{1.2.3\ldots m}$ values. This number is always twice an odd number (I omit the proof, which is not difficult); if it is put $= 2k$, its half k is therefore odd, while the equation $U = 0$ has degree $2k$. Now, since the second term is absent in the equation $X = 0$, the sum of all $2m$ roots is 0. Thus, if the sum of any m roots is $+p$, the sum of the remaining ones is $-p$: that is, if $+p$ is among the values of u, then $-p$ is among them too. From this Euler concludes that U is the product of k quadratic factors such

as $uu - pp$, $uu - qq$, $uu - rr$, etc., where $+p$, $-p$, $+q$, $-q$, etc. denote all $2k$ roots of the equation $U = 0$. Because the number of these factors is odd, the constant term in U is therefore the square of the product pqr, etc., with a negative sign. But the product pqr, etc. can always be determined rationally from the coefficients B, C, etc., and must therefore be a real quantity. Its square with a negative sign is thus certainly a negative quantity. Q. E. D.

Since these two real factors of X have degree m, and m is a power of the number 2, each can in the same way be resolved again into two real factors of degree $\frac{1}{2}m$. Repeated halving of the number m must eventually lead to two; hence continuing the operation evidently gives the function X resolved into real quadratic factors.

If, however, a function is proposed in which the second term is not absent, say $x^{2m} + Ax^{2m-1} + Bx^{2m-2} + \text{etc.} + M$, where $2m$ still denotes a power of two, the substitution $x = y - \frac{A}{2m}$ transforms it into a similar function without a second term. It readily follows that this function too can be resolved into real quadratic factors.

Finally, given a function of degree n, where n denotes a number that is not a power of two, let the next larger power of two than n be put $= 2m$, and multiply the proposed function by any $2m - n$ real linear factors. From the fact that the product can be resolved into real quadratic factors, it readily follows that the proposed function too must be resolvable into real factors of the second or first degree.

8.

The following objections can be made to this proof.

1. The rule by which Euler concludes that all $2m - 2$ unknowns α, β, etc., λ, μ, etc. can be determined rationally from $2m - 1$ equations is by no means general, but very often admits exceptions. If, for example, in Article 3 one regards one of the unknowns as known and tries to express the others rationally in terms of it and the given coefficients, one readily finds that this is impossible, and that no unknown quantity can be determined except by an equation of degree $m - 1$. Although here one can immediately see a priori that this must necessarily happen, one might nevertheless reasonably doubt whether, in the present case too, matters stand in the same way for some values of m, so that the unknowns α, β, etc., λ, μ, etc. cannot be determined from u, B, C, etc. except by an equation of degree perhaps higher than $2m$. For the case where the equation $X = 0$ is of the fourth degree, Euler derives rational values of the coefficients in terms of u and the given coefficients; but that this can also be done for all higher equations certainly needed a fuller explanation. — It seems worthwhile, moreover, to investigate more deeply and in the greatest generality those formulas that express α, β, etc. rationally in terms of u, B, C, etc. I shall undertake a fuller treatment of this

and other matters belonging to the theory of elimination (a subject by no means exhausted) on another occasion.

2. Even if it has been proved that, whatever the degree of the equation $X = 0$, formulas can always be found that express α, β, etc., λ, μ, etc. rationally in terms of u, B, C, etc., it is nevertheless certain that for some particular values of the coefficients B, C, etc. these formulas can become *indeterminate*, so that not only is it impossible to determine these unknowns rationally from u, B, C, etc., but in some cases there are actually no real values of α, β, etc., λ, μ, etc. corresponding to a real value of u. To confirm this, for brevity I refer the reader to Euler's paper itself, where the equation of the fourth degree is discussed more fully on p. 236. Everyone will immediately see that the formulas for the coefficients α, β become indeterminate if $C = 0$ and the value 0 is taken for u, and that their values not only cannot be assigned without extracting roots, but are not even real if $BB - 4D$ is a negative quantity. Although in this case one can readily see that u has other real values to which real values of α, β correspond, one might nevertheless fear that unraveling this difficulty (which Euler did not touch on at all) could require much greater effort in higher equations. Certainly this matter must by no means be passed over in silence in an exact proof.

3. The distinguished Euler tacitly supposes that the equation $X = 0$ has $2m$ roots, and puts their sum $= 0$ because the second term is absent in X. I have already stated above, in Article 3, what I think of this freedom (which all authors on this subject use). The proposition that the sum of all the roots of an equation equals its first coefficient with its sign changed seems applicable only to equations that have roots. Since this very proof is meant to establish that the equation $X = 0$ actually has roots, it seems inadmissible to suppose their existence. No doubt those who have not yet seen through the fallacy in this reasoning will reply that *what is proved here is not that the equation* $X = 0$ *can be satisfied* (for that is what the expression that it has roots means), *but only that it can be satisfied by values of* x *contained in the form* $a + b\sqrt{-1}$*; the former is supposed as an axiom.* But since no forms of quantities other than the real and the imaginary $a + b\sqrt{-1}$ can be conceived, it is not sufficiently clear how what is to be proved differs from what is supposed as an axiom. Indeed, even if it were possible to devise still other forms of quantities, say the form F, F', F'', etc., it should nevertheless not be admitted without proof that an equation can be satisfied by some value of x that is either real, or contained in the form $a + b\sqrt{-1}$, or in the form F, or in F', etc. That axiom can therefore have no other meaning than this: any equation can be satisfied *either* by a real value of the unknown, *or* by an imaginary value contained in the form $a+b\sqrt{-1}$, *or* perhaps by a value contained in some other form hitherto unknown, *or* by a value contained in no form at all. But how quantities of this kind, of which you cannot even

form an idea — a true shadow of a shadow — can be added or multiplied is certainly not understood with the clarity always required in mathematics*).

I do not, however, wish these objections to cast any doubt on the conclusions Euler drew from his supposition. On the contrary, I am certain that they can be established by a method neither difficult nor very different from Euler's, in such a way that not even the slightest doubt should remain for anyone. I criticize only the *form*, which, although it can be very useful in *discovering* new truths, nevertheless seems quite unacceptable in *proving* them before the public.

4. The distinguished Euler offered nothing at all to prove the assertion that the product pqr, etc. can be determined *rationally* from the coefficients in X. Everything he says about this for equations of the *fourth degree* is as follows (where a, b, c, d are the roots of the proposed equation $x^4+Bxx+Cx+D = 0$):

'No doubt it will be objected that I have supposed here that the quantity pqr was a real quantity and that its square $ppqqrr$ was positive; this was still doubtful, since, the roots a, b, c, d being imaginary, it could well happen that the square of the quantity pqr formed from them was negative. To this I reply that this case can never occur; for however imaginary the roots a, b, c, d may be, we nevertheless know that there must be $a + b + c + d = 0$: $ab + ac + ad + bc + bd + cd = B$; $abc + abd + acd + bcd = -C$*); $abcd = D$, these quantities B, C, D being real. But since $p = a + b$, $q = a + c$, $r = a + d$, their product $pqr = (a + b)(a + c)(a + d)$ can be determined, *as we know*, from the quantities B, C, D, and will consequently be real, just as we have seen that in fact $pqr = -C$ and $ppqqrr = CC$. It will readily be recognized in the same way that this same circumstance must occur in higher equations, and that no objections can be made to me on this ground.' Euler nowhere added the condition that the product pqr, etc. can be determined *rationally* in terms of B, C, etc.; nevertheless, he seems always to have understood it, since without it the proof can have no force. Now it is indeed true for equations of the fourth degree that expanding the product $(a + b)(a + c)(a + d)$ gives $aa(a+b+c+d)+abc+abd+acd+bcd = -C$; yet it does not seem sufficiently clear how in all higher equations the product can be determined rationally from the coefficients. The celebrated de Foncenex, who first observed this (*Miscell. phil. math. soc. Taurin.*, Vol. I, p. 117), rightly maintains that without a rigorous proof of this proposition the method loses all its

*)This whole matter will be greatly clarified by another investigation already in the press, where, on a subject very different but nevertheless analogous, I could have used a similar freedom with exactly the same right as all analysts have done here with equations. Although, with the help of such fictions, I could have completed in a few words the proofs of several truths that without them became very difficult and require the most subtle devices, I nevertheless preferred to refrain from them altogether, and I hope that few would have been satisfied had I imitated the analysts' method.

*)Euler has C in error, and hence also later wrongly puts $pqr = C$.

force; he confesses, however, that this proof seems rather difficult to him, and describes the path he tried in vain*). Nevertheless, the matter can be settled without much difficulty by the following method (whose substance I can only indicate here). Although in equations of the fourth degree it is not sufficiently clear that the product $(a+b)(a+c)(a+d)$ can be determined in terms of the coefficients B, C, D, one can readily see that the same product is also $= (b+a)(b+c)(b+d)$, as well as $= (c+a)(c+b)(c+d)$, and finally also $= (d+a)(d+b)(d+c)$. The product pqr will therefore be one quarter of the sum $(a+b)(a+c)(a+d)+(b+a)(b+c)(b+d)+(c+a)(c+b)(c+d)+(d+a)(d+b)(d+c)$, which, when expanded, can readily be foreseen a priori to be a polynomial in the roots a, b, c, d in which they all enter in the same way. Such functions can always be expressed rationally in terms of the coefficients of the equation whose roots are a, b, c, d. — The same thing is also evident if the product pqr is put into the form

$$\tfrac{1}{2}(a+b-c-d) \times \tfrac{1}{2}(a+c-b-d) \times \tfrac{1}{2}(a+d-b-c)$$

for one can readily foresee that this product, when expanded, will involve all of a, b, c, d in the same way. Those familiar with the subject will also readily gather from this how it must be applied to higher equations. — A complete account of the proof, which brevity does not allow me to include here, together with a fuller investigation of functions involving several variables in the same way, I reserve for another occasion.

I observe, moreover, that besides these four objections there are still some other points in Euler's proof that could be criticized; I pass over them in silence, however, lest I seem too severe a critic, especially since the foregoing seems sufficiently to show that the proof, at least in the form Euler proposed it, can by no means be regarded as complete.

After this proof Euler showed another way of reducing the theorem for equations whose degree is not a power of two to the solution of equations of that kind. But since this method teaches nothing for equations whose degree is a power of two, and is moreover open to all the preceding objections (except the fourth) just as the first general proof is, there is no need to discuss it more fully here.

*) An error seems to have crept into this account: namely, on p. 118, line 5, instead of the symbol p ("one chose only those in which p occurred", etc.), one must necessarily read *one and the same arbitrary root of the proposed equation*, or something similar, since the former makes no sense.

9.

In the same paper, on p. 263, the distinguished Euler tried to establish our theorem in yet another way, whose substance is as follows. Given an equation $x^n + Ax^{n-1} + Bx^{n-2}$ etc. $= 0$, no analytical expression representing its roots has yet been found if the exponent $n > 4$; nevertheless it seems certain (as Euler asserts) that it can contain nothing but arithmetical operations and extractions of roots, combined more intricately the greater n is. If this is granted, Euler shows very well that, however intricately the radical signs are combined, the value of the formula can always be represented in the form $M + N\sqrt{-1}$, where M, N are real quantities.

Against this reasoning one can object that, after the efforts of so many great mathematicians, very little hope remains of ever arriving at the general solution of algebraic equations, so that it becomes more and more probable that such a solution is altogether impossible and contradictory. This should seem all the less paradoxical *since what is commonly called the solution of an equation is, strictly speaking, nothing but its reduction to pure equations.* For the solution of pure equations is not taught by this, but supposed; and if you express a root of the equation $x^m = H$ by $\sqrt[m]{H}$, you have by no means solved it, nor have you done more than if you devised some sign to denote a root of the equation $x^n + Ax^{n-1} + \text{etc.} = 0$ and put the root equal to it. It is true that pure equations far surpass all others because of the ease of finding their roots by approximation and because of the elegant connection all their roots have with one another. It is therefore by no means to be criticized that analysts have denoted their roots by a special sign. Yet from the fact that they have included this sign, just like the arithmetical signs of addition, subtraction, multiplication, division and raising to a power, under the name of *analytical expressions*, it by no means follows that a root of any equation can be represented by them. Or, putting words aside, it is supposed without sufficient reason that the solution of any equation can be reduced to the solution of pure equations. Perhaps it would not be so difficult to prove this impossibility with full rigor already for the fifth degree; I shall present my investigations on this matter more fully elsewhere. Here it is enough that the general solvability of equations, understood in that sense, is still very doubtful, and that therefore a proof whose entire force depends on that supposition carries no weight in the present state of the subject.

10.

Later, the celebrated DE FONCENEX too, having noticed a defect in EULER'S first proof (above, Article 8, objection 4) that he could not remove, tried another path and presented it on p. 120 of the paper cited*). It consists in the following.

Let an equation $Z = 0$ be proposed, where Z denotes a function of degree m in the unknown z. If m is an odd number, it is already known that this equation has a real root; if m is even, however, the celebrated Foncenex tries in the following way to prove that the equation has at least one root of the form $p + q\sqrt{-1}$. Let $m = 2^n i$, where i denotes an odd number, and suppose that $zz + uz + M$ is a divisor of the function Z. Then the individual values of u will be the sums of pairs of roots of the equation $Z = 0$, with their sign changed; hence u will have $\frac{m.m-1}{1.2} = m'$ values. If u is supposed to be determined by an equation $U = 0$ (where U denotes a polynomial in u and the known coefficients in Z), this equation will have degree m'. One readily sees that m' will be a number of the form $2^{n-1}i'$, where i' denotes an odd number. Now, unless m' is odd, suppose again that $uu + u'u + M'$ is a divisor of U; similar reasoning will show that u' is determined by an equation $U' = 0$, where U' is a function of degree $\frac{m'.m'-1}{1.2}$ in u'. Putting $\frac{m'.m'-1}{1.2} = m''$, we have that m'' is a number of the form $2^{n-2}i''$, where i'' denotes an odd number. Now, unless m'' is odd, let $u'u' + u''u' + M''$ be a divisor of the function U'; then u'' will be determined by an equation $U'' = 0$, which, if it is supposed to have degree m''', gives m''' as a number of the form $2^{n-3}i'''$. It is evident that in the sequence of equations $U = 0$, $U' = 0$, $U'' = 0$, etc., the one in position n will have odd degree and therefore a real root. For brevity we shall put $n = 3$, so that the equation $U'' = 0$ has a real root u'', for one readily sees that the same reasoning holds for any other value of n. The celebrated de Foncenex then asserts that the coefficient M'' can be determined rationally from u'' and the coefficients in U' (which are readily understood to be polynomials in the coefficients in Z), or from u'' and the coefficients in Z, and is therefore real. It follows that the roots of the equation $u'u' + u''u' + M'' = 0$ will be contained in the form $p + q\sqrt{-1}$; but they will evidently satisfy the equation $U' = 0$ as well. There will therefore be some value of u' contained in the form $p + q\sqrt{-1}$. Now the coefficient M' can, in the same way as before, be determined rationally from u' and the coefficients in Z, and will therefore also be contained in the form $p + q\sqrt{-1}$. Hence the roots of the equation $uu + u'u + M'$ will be contained in the same form, and will at the same time satisfy the equation $U = 0$; that is, this equation will have a root contained in the form $p + q\sqrt{-1}$. Finally, it follows from this in a similar way that M too

*)The second volume of the same *Miscellanea*, p. 337, contains elucidations of this paper; these do not, however, concern the present investigation, but the logarithms of negative quantities, which had been discussed in the same paper.

is contained in the same form, as is a root of the equation $zz + uz + M = 0$, which will evidently also satisfy the proposed equation $Z = 0$. Thus any equation will have at least one root of the form $p + q\sqrt{-1}$.

11.

Objections 1, 2 and 3 that I made against EULER'S first proof (Article 8) have the same force against this method, with this difference, however: the second objection, to which EULER'S proof was open only in some special cases, must affect the present one in every case. Namely, one can prove a priori that, even if a formula is given that expresses the coefficient M' rationally in terms of u' and the coefficients in Z, this formula must necessarily become indeterminate for several values of u'; similarly, the formula that expresses the coefficient M'' in terms of u'' becomes indeterminate for some values of u'', etc. This is seen most clearly if we take an equation of the fourth degree as an example. Let us therefore put $m = 4$, and let the roots of the equation $Z = 0$ be α, β, γ, δ. Then it is evident that the equation $U = 0$ will be of the sixth degree and its roots $-(\alpha+\beta)$, $-(\alpha+\gamma)$, $-(\alpha+\delta)$, $-(\beta+\gamma)$, $-(\beta+\delta)$, $-(\gamma+\delta)$. The equation $U' = 0$, however, will be of the fifteenth degree, and the values of u' will be

$$\begin{array}{ccc}
2\alpha+\beta+\gamma, & 2\alpha+\beta+\delta, & 2\alpha+\gamma+\delta, \\
2\beta+\alpha+\gamma, & 2\beta+\alpha+\delta, & 2\beta+\gamma+\delta, \\
2\gamma+\alpha+\beta, & 2\gamma+\alpha+\delta, & 2\gamma+\beta+\delta, \\
2\delta+\alpha+\beta, & 2\delta+\alpha+\gamma, & 2\delta+\beta+\gamma, \\
\alpha+\beta+\gamma+\delta, & \alpha+\beta+\gamma+\delta, & \alpha+\beta+\gamma+\delta
\end{array}$$

Now we must stop at this equation, since its degree is odd, and it will in fact have the real root $\alpha+\beta+\gamma+\delta$ (which equals the first coefficient in Z with its sign changed and will therefore be not only real but also rational if the coefficients in Z are rational). But one can readily see that, if a formula is given that expresses the value of M' rationally in terms of the corresponding value of u', it necessarily becomes indeterminate for $u' = \alpha+\beta+\gamma+\delta$. For this value will be a root of the equation $U' = 0$ *three times*, and three values of M' will correspond to it, namely $(\alpha+\beta)(\gamma+\delta)$, $(\alpha+\gamma)(\beta+\delta)$ and $(\alpha+\delta)(\beta+\gamma)$, which can all be irrational. Evidently a rational formula could in this case produce neither an irrational value of M' nor three different values. From this example one can sufficiently gather that the celebrated DE FONCENEX'S method is by no means satisfactory; if it is to be made complete in every respect, the theory of elimination must be investigated much more deeply.

12.

Finally, the distinguished La Grange treated our theorem in the paper *Sur la forme des racines imaginaires des équations, Nouv. Mém. de l'Acad. de Berlin* 1772, p. 222 ff. This great mathematician took particular pains to supply the defects in Euler's first proof, and in fact investigated especially those matters that constitute the second and fourth objections above (Article 8) so deeply that nothing further remains to be desired, except perhaps that some doubts seem to remain in the earlier investigation concerning the theory of elimination, on which this whole investigation rests. — Yet he did not touch on the third objection at all; indeed, the whole investigation is built on the supposition that any equation of degree m actually has m roots.

Thus, after carefully weighing what has been set out so far, I hope that those familiar with the subject will welcome a new proof of this most important theorem drawn from entirely different principles. I now proceed to give it.

13.

Lemma. *If m denotes any positive integer, the function* $\sin\varphi \,.\, x^m - \sin m\varphi \,.\, r^{m-1}x + \sin(m-1)\varphi \,.\, r^m$ *will be divisible by* $xx - 2\cos\varphi \,.\, rx + rr$.

Proof. For $m = 1$ this function becomes $= 0$ and is therefore divisible by any factor; for $m = 2$ the quotient becomes $\sin\varphi$, and for any greater value the quotient will be $\sin\varphi \,.\, x^{m-2} + \sin 2\varphi \,.\, rx^{m-3} + \sin 3\varphi \,.\, rrx^{m-4} +$ etc. $+ \sin(m-1)\varphi \,.\, r^{m-2}$. For one readily verifies that, when this function is multiplied by $xx - 2\cos\varphi \,.\, rx + rr$, the product equals the proposed function.

14.

Lemma. *If the quantity r and the angle φ are determined so that the equations*

$$\begin{aligned} &r^m \cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + Br^{m-2}\cos(m-2)\varphi + \text{etc.} \\ &\qquad + Krr\cos 2\varphi + Lr\cos\varphi + M = 0 \quad . \quad . \quad [1] \\ &r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + Br^{m-2}\sin(m-2)\varphi + \text{etc.} \\ &\qquad + Krr\sin 2\varphi + Lr\sin\varphi = 0 \quad . \quad . \quad [2] \end{aligned}$$

hold, the polynomial $x^m + Ax^{m-1} + Bx^{m-2} + etc. + Kxx + Lx + M = X$ will be divisible by the quadratic factor $xx - 2\cos\varphi \,.\, rx + rr$, provided we do not have $r\sin\varphi = 0$; but if $r\sin\varphi = 0$, the same polynomial will be divisible by the linear factor $x - r\cos\varphi$.

Proof. I. By the preceding article, all the following quantities will be divisible by $xx - 2\cos\varphi \,.\, rx + rr$:

$$\begin{array}{rll}
\sin\varphi \,.\, rx^m & -\sin m\varphi \,.\, r^m x & +\sin(m-1)\varphi \,.\, r^{m+1} \\
A\sin\varphi \,.\, rx^{m-1} & -A\sin(m-1)\varphi \,.\, r^{m-1}x & +A\sin(m-2)\varphi \,.\, r^m \\
B\sin\varphi \,.\, rx^{m-2} & -B\sin(m-2)\varphi \,.\, r^{m-2}x & +B\sin(m-3)\varphi \,.\, r^{m-1} \\
 & \text{etc.} & \text{etc.} \\
K\sin\varphi \,.\, rxx & -K\sin 2\varphi \,.\, rrx & +K\sin\varphi \,.\, r^3 \\
L\sin\varphi \,.\, rx & -L\sin\varphi \,.\, rx & * \\
M\sin\varphi \,.\, r & * & +M\sin(-\varphi) \,.\, r
\end{array}$$

Their sum will therefore also be divisible by $xx - 2\cos\varphi \,.\, rx + rr$. Now the first parts of these quantities form the sum $\sin\varphi \,.\, rX$; the second parts, added together, give 0 by [2]; and it is easy to see that the sum of the third parts also vanishes if we multiply [1] by $\sin\varphi$ and [2] by $\cos\varphi$, and subtract the former product from the latter. It follows that the polynomial $\sin\varphi \,.\, rX$ is divisible by $xx - 2\cos\varphi \,.\, rx + rr$, and hence, unless $r\sin\varphi = 0$, so is the polynomial X. Q. E. P.

II. But if $r\sin\varphi = 0$, either $r = 0$ or $\sin\varphi = 0$. In the first case, $M = 0$ by [1], and thus X is divisible by x, or by $x - r\cos\varphi$; in the second case, $\cos\varphi = \pm 1$, $\cos 2\varphi = +1$, $\cos 3\varphi = \pm 1$, and in general $\cos n\varphi = \cos\varphi^n$. Thus, by [1], we obtain $X = 0$ on setting $x = r\cos\varphi$, and consequently the polynomial X will be divisible by $x - r\cos\varphi$. Q. E. S.

15.

The preceding theorem is usually proved with the aid of imaginary quantities; see EULER, *Introd. in Anal. Inf.*, Vol. I, p. 110. I thought it worth showing how it can be obtained just as easily without their aid. It is now clear that proving our theorem requires nothing more than showing the following: *Given any polynomial X of the form $x^m + Ax^{m-1} + Bx^{m-2} + etc. + Lx + M$, r and φ can be determined so that equations* [1] *and* [2] *hold.* For it follows that X has a real factor of the first or second degree; division will necessarily produce a real quotient of lower degree, which, for the same reason, will also have a factor of the first or second degree. By continuing this operation, X will eventually be resolved into real linear or quadratic factors. The purpose of the following investigations is therefore to prove that theorem.

16.

Imagine a fixed infinite plane (the plane of the plate, Fig. 1), and in it a fixed infinite straight line GC passing through a fixed point C. Take some length as the unit, so that all lengths of straight lines can be expressed by numbers. At any point P of the plane whose distance from the centre C is r and whose angle is $GCP = \varphi$, erect a perpendicular equal to the value of the expression

$$r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + \text{etc.} + Lr\sin\varphi$$

which, for brevity, I shall always denote by T in what follows. I always regard the distance r as positive; for points lying on the other side of the axis, the angle φ must be regarded either as greater than two right angles or as negative (which here amounts to the same thing). The endpoints of these perpendiculars (which must be taken above the plane for a positive value of T, below it for a negative value, and in the plane itself for a vanishing value) will lie on a continuous curved surface extending infinitely in every direction, which, for brevity, I shall call the *first surface* in what follows. In exactly the same way, refer another surface to the same plane and centre and the same axis, with its height above any point of the plane equal to

$$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + \text{etc.} + Lr \cos \varphi + M$$

an expression which, for brevity, I shall always denote by U. I shall distinguish this surface, which will likewise be continuous and extend infinitely in every direction, from the former by calling it the *second surface*. It is then clear that the whole task is to show that there is at least one point lying in the plane, in the first surface and in the second surface at the same time.

17.

It is easy to see that the first surface lies partly above and partly below the plane. For the distance r from the centre can clearly be taken so large that the remaining terms in T vanish in comparison with the first term $r^m \sin m\varphi$; and, by choosing the angle φ appropriately, this term can be made either positive or negative. The fixed plane will therefore necessarily be cut by the first surface. I shall call this intersection of the plane with the first surface the *first line*; it will thus be determined by the equation $T = 0$. For the same reason, the plane will be cut by the second surface; the intersection will form a curve determined by the equation $U = 0$, which I shall call the *second line*. Strictly speaking, each curve will consist of several branches, which may be entirely separate, though each will be a continuous line. Indeed, the first line will always be what is called a compound curve, and the axis GC must be regarded as part of this curve: whatever value is assigned to r, we always have $T = 0$ whenever $\varphi = 0$ or $= 180°$. But it is better to regard the collection of all branches passing through all points where $T = 0$ as a single curve (following the usage generally accepted in higher geometry), and likewise all branches passing through all points where $U = 0$. It is now clear that the task has been reduced to showing that there is at least one point in the plane where some branch of the first line is cut by a branch of the second line. For this purpose, we must examine the nature of these lines more closely.

18.

First of all, I observe that both curves are algebraic and, when referred to orthogonal coordinates, of degree m. For if the origin of abscissas is taken at C, the abscissas x towards G, and the ordinates y towards P, we have $x = r\cos\varphi$, $y = r\sin\varphi$, and thus in general, whatever n may be,

$$r^n \sin n\varphi = nx^{n-1}y - \frac{n\,.\,n-1\,.\,n-2}{1\,.\,2\,.\,3}x^{n-3}y^3 + \frac{n\,\ldots\,n-4}{1\,\ldots\,.5}x^{n-5}y^5 - \text{etc.},$$

$$r^n \cos n\varphi = x^n - \frac{n\,.\,n-1}{1\,.\,2}x^{n-2}yy + \frac{n\,.\,n-1\,.\,n-2\,.\,n-3}{1\,.\,2\,.\,3\,.\,4}x^{n-4}y^4 - \text{etc.}$$

Both T and U will therefore consist of several terms of the form $ax^\alpha y^\beta$, where α and β denote positive integers whose sum, at its greatest, is $= m$. It can also readily be foreseen that all terms of T contain the factor y, and thus that the first line is, strictly speaking, composed of a straight line (whose equation is $y = 0$) and a curve of degree $m - 1$; but we need not take this distinction into account here.

It will be more important to investigate whether the first and second lines have arms extending to infinity, and how many and of what kind. At an infinite distance from the point C, the first line, whose equation is $\sin m\varphi + \frac{A}{r}\sin(m-1)\varphi + \frac{B}{rr}\sin(m-2)\varphi$ etc. $= 0$, will coincide with the line whose equation is $\sin m\varphi = 0$. This represents m straight lines intersecting at the point C, the first of which is the axis GCG', while the others are inclined to it at angles of $\frac{1}{m}180$, $\frac{2}{m}180$, $\frac{3}{m}180$ etc. degrees. The first line therefore has $2m$ infinite branches, which divide the circumference of a circle drawn with infinite radius into $2m$ equal parts: the first branch cuts the circumference at the intersection of the circle and the axis, the second at a distance of $\frac{1}{m}180°$, the third at a distance of $\frac{2}{m}180°$, etc. In the same way, at an infinite distance from the centre the second line will have an asymptote expressed by the equation $\cos m\varphi = 0$. This is a collection of m straight lines likewise intersecting at the point C at equal angles, but in such a way that the first forms an angle of $\frac{1}{m}90°$ with the axis CG, the second an angle of $\frac{3}{m}90°$, the third an angle of $\frac{5}{m}90°$, etc. The second line will therefore also have $2m$ infinite branches, each occupying the middle position between two neighbouring branches of the first line, so that they cut the circumference of a circle drawn with an infinitely large radius at points whose angular distances from the axis are $\frac{1}{m}90°$, $\frac{3}{m}90°$, $\frac{5}{m}90°$, etc. It is also clear that the axis itself always forms two infinite branches of the first line, namely the first and the one in position $m + 1$. This arrangement of the branches is shown very clearly in Fig. 2,

drawn for the case $m = 4$; the branches of the second line are dotted to distinguish them from those of the first line, and the same applies to the fourth figure*). — Since these conclusions are of the greatest importance, however, and infinitely large quantities may trouble some readers, I shall also show in the next article how to obtain them without the aid of infinities.

19.

THEOREM. *With everything as above, a circle can be drawn with centre C, on whose circumference there are $2m$ points where $T = 0$ and as many where $U = 0$, arranged so that each of the latter lies between two of the former.*

Let the sum of all the coefficients A, B etc. K, L, M, taken positively, be $= S$, and take R to be both $> S\sqrt{2}$ and > 1*). I then say that what the theorem states necessarily holds for the circle drawn with radius R. For brevity, label the point of this circumference that is $\frac{1}{m}45$ degrees from its intersection with the left part of the axis, or for which $\varphi = \frac{1}{m}45°$, by (1); similarly, the point that is $\frac{3}{m}45°$ from that intersection, or for which $\varphi = \frac{3}{m}45°$, by (3); then the point where $\varphi = \frac{5}{m}45°$ by (5), and so on up to $(8m-1)$, which is $\frac{8m-1}{m}45$ degrees from that intersection if one always proceeds in the same direction (or $\frac{1}{m}45°$ in the opposite direction). Thus there are altogether $4m$ points on the circumference at equal intervals. Between $(8m-1)$ and (1) there will be one point where $T = 0$; likewise, one such point will lie between (3) and (5), between (7) and (9), between (11) and (13), etc., so that their number is $2m$. In the same way, one point where $U = 0$ will lie between (1) and (3), between (5) and (7), and between (9) and (11), so that their number is also $= 2m$. Finally, apart from these $4m$ points, there will be no others anywhere on the circumference where either T or U is $= 0$.

Proof. I. At the point (1), $m\varphi = 45°$, and thus

$$T = R^{m-1}(R\sqrt{\tfrac{1}{2}} + A\sin(m-1)\varphi + \tfrac{B}{R}\sin(m-2)\varphi + \text{etc.} + \tfrac{L}{R^{m-2}}\sin\varphi)$$

But the sum $A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi$ etc. certainly cannot be greater than S, and must therefore be less than $R\sqrt{\frac{1}{2}}$. It follows that at this point the value of T is certainly positive. All the more, then, T will have a positive value when $m\varphi$ lies between 45° and 135°; that is, the value of T will always be positive from the point (1) to (3). For the same reason, T will be positive everywhere from the point (9) to (11), and in general from any point $(8k+1)$ to $(8k+3)$, where k denotes any integer. Similarly, T will be negative everywhere between (5) and (7), between (13) and (15), etc., and in general between

*)The fourth figure was drawn on the assumption $X = x^4 - 2xx + 3x + 10$, so that readers less accustomed to general and abstract investigations can see in a concrete case the relative positions of the two curves. The length of the line CG was taken as $= 10$ ($CN = 1{,}26255$.)

*)When $S > \sqrt{\frac{1}{2}}$, the first condition implies the second; but when $S < \sqrt{\frac{1}{2}}$, the second implies the first.

$(8k+5)$ and $(8k+7)$; thus it cannot be $= 0$ anywhere in any of these intervals. But since its value is positive at (3) and negative at (5), it must be $= 0$ somewhere between (3) and (5); likewise somewhere between (7) and (9), between (11) and (13), etc., up to and including the interval between $(8m-1)$ and (1). Thus we have $T = 0$ at altogether $2m$ points. Q. E. P.

II. That there are no other points with this property apart from these $2m$ points is seen as follows. Since there are none between (1) and (3), between (5) and (7), etc., there could be more such points only if at least two lay in some interval between (3) and (5), or between (7) and (9), etc. Then, however, T would necessarily be a *maximum* or *minimum* somewhere in the same interval, and hence $\frac{\mathrm{d}T}{\mathrm{d}\varphi} = 0$. But $\frac{\mathrm{d}T}{\mathrm{d}\varphi} = mR^{m-2}(R\cos m\varphi + \frac{m-1}{m}A\cos(m-1)\varphi + \text{etc.})$, and between (3) and (5), $\cos m\varphi$ is always negative and $> \sqrt{\frac{1}{2}}$. It is therefore easy to see that $\frac{\mathrm{d}T}{\mathrm{d}\varphi}$ is negative throughout this interval; in the same way, it is positive everywhere between (7) and (9), negative between (11) and (13), etc. Thus it cannot be 0 in any of these intervals, and the supposition cannot stand. Therefore etc. Q. E. S.

III. In exactly the same way, it is proved that U has a negative value everywhere between (3) and (5), between (11) and (13), etc., and in general between $(8k+3)$ and $(8k+5)$; but a positive value between (7) and (9), between (15) and (17), etc., and in general between $(8k+7)$ and $(8k+9)$. It follows at once that $U = 0$ must hold somewhere between (1) and (3), between (5) and (7), etc., that is, at $2m$ points. But $\frac{\mathrm{d}U}{\mathrm{d}\varphi} = 0$ cannot hold in any of these intervals (which is easily proved in the same way as above). There will therefore be no more than those $2m$ points on the circumference of the circle where $U = 0$. Q. E. T. and Q.

The part of the theorem stating that there are no more than $2m$ points where $T = 0$, and no more than $2m$ where $U = 0$, can also be proved from the fact that equations $T = 0$, $U = 0$ represent curves of degree m. For it is known from higher geometry that such curves cannot be cut in more than $2m$ points by a circle, as a curve of the second degree.

20.

If another circle is drawn from the same centre with a radius greater than R and divided in the same way, then on this circle too there will be one point between (3) and (5) where $T = 0$, and likewise between (7) and (9), etc. It is easy to see that the less the radius of this circle differs from the radius R, the nearer such points lying between (3) and (5) on the two circumferences must be to each other. The same will hold if a circle is drawn with a radius somewhat smaller than R, but still greater than $S\sqrt{2}$ and 1. From this it is readily understood that the circumference of the circle drawn with radius R is actually *cut* by some branch of the first line at the point between (3) and (5) where $T = 0$; and the same holds for the remaining points where $T = 0$. In the

same way, it is clear that the circumference of this circle is cut by some branch of the second line at all $2m$ points where $U = 0$. These conclusions may also be expressed as follows: if a circle of the appropriate size is drawn with centre C, $2m$ branches of the first line and as many branches of the second line will enter it, in such a way that each pair of neighbouring branches of the first line is separated by some branch of the second line. See Fig. 2, where the circle will now be of finite rather than infinite size. The numbers attached to the individual branches must not be confused with the numbers by which, for brevity, I designated certain boundaries on the circumference in this and the preceding article.

21.

From this relative arrangement of the branches entering the circle, the necessary existence of an intersection of some branch of the first line with a branch of the second line inside the circle can now be deduced in so many different ways that I almost do not know which method to choose in preference to the others. The following seems the clearest. Let us label (Fig. 2) the point on the circumference where it is cut by the left part of the axis (which is itself one of the $2m$ branches of the first line) by 0; the next point, where a branch of the second line enters, by 1; the point next to this, where the second branch of the first line enters, by 2; and so on up to $4m - 1$. Thus a branch of the second line enters the circle at every point marked with an even number, while a branch of the second line enters at every point marked with an odd number. Now it is known from higher geometry that every algebraic curve (or each individual part of any algebraic curve, if it happens to consist of several parts) either returns into itself or extends to infinity in both directions. Hence, if a branch of an algebraic curve enters a bounded region, it must necessarily leave that region again somewhere[*)]. From this it is easily concluded that every point marked with an even number (or, for

[*)]It certainly seems to have been demonstrated well enough that an algebraic curve can neither suddenly break off anywhere (as happens, for example, with the transcendental curve whose equation is $y = \frac{1}{\log x}$), nor, after infinitely many windings, as it were lose itself at some point (like the logarithmic spiral); and, as far as I know, no one has raised a doubt on this matter. Nevertheless, if anyone demands it, I shall undertake to give a proof free from all doubt on another occasion. In the present case, however, it is clear that if some branch, for example 2, never left the circle anywhere (Fig. 3), you could enter the circle between 0 and 2, then go around the whole of this branch (which would have to lose itself in the region of the circle), and finally leave the circle again between 2 and 4, without encountering the first line anywhere along the entire path. That this is absurd is clear from the fact that, at the point where you entered the circle, the first surface was above you, and at your exit it was below you. You must therefore necessarily have encountered the first surface itself somewhere, or a point of the first line. — This reasoning, which rests on principles of the geometry of position that are no less valid than those of the geometry of magnitude, implies only that, if you enter the circle along some branch of the first line, you can leave it again at another place while always remaining on the first line; it does not imply that your path is a continuous line in the

brevity, *every even point*) must be joined within the circle to another even point by a branch of the first line; similarly, every point marked with an odd number must be joined to another such point by a branch of the second line. Although this connection of pairs of points may vary greatly with the nature of the polynomial X, so that it cannot be determined in general, it is nevertheless easy to prove that *whatever it may be, an intersection of the first line with the second line always results.*

22.

It seems that this necessity can most conveniently be proved by contradiction. Suppose, then, that each pair of even points and each pair of odd points can be joined in such a way that no intersection of a branch of the first line with a branch of the second line results. Since the axis is part of the first line, the point 0 will clearly be joined to the point $2m$. The point 1 therefore cannot be joined to any point lying beyond the axis, that is, to any point designated by a number greater than $2m$; for otherwise the joining line would necessarily cut the axis. Thus, if 1 is supposed to be joined to the point n, we shall have $n < 2m$. For a similar reason, if 2 is taken to be joined to n', we shall have $n' < n$; for otherwise the branch $2 \ldots n'$ would necessarily cut the branch $1 \ldots n$. For the same reason, the point 3 will be joined to one of the points lying between 4 and n'. It is clear that if 3, 4, 5, etc. are supposed to be joined to n'', n''', n'''', etc., then n''' lies between 5 and n'', n'''' between 6 and n''', etc. It is therefore evident that we shall eventually reach some point h joined to the point $h + 2$. Then the branch entering the circle at the point $h + 1$ will necessarily cut the branch joining the points h and $h + 2$. Since one of these two branches belongs to the first line and the other to the second, it is now clear that the supposition is contradictory, and hence that an intersection of the first line with the second line must occur somewhere. Combining this with what precedes, we conclude from all the investigations set out above that the theorem *that every polynomial in one variable can be resolved into real factors of the first or second degree* has been proved with full rigour.

23.

It is also not difficult to deduce from the same principles that there is not merely one intersection of the first line with the second, but at least m. It may, however, happen that the first line is cut by several branches of the second line at the same point, in which case the polynomial X will have several equal factors. But since it is enough here to have proved the necessity of one intersection, I shall not dwell on this further, for brevity. For the same reason, I shall not pursue other properties of these lines in more detail here:

sense accepted in higher geometry. But here it is enough for the path to be a continuous line in the ordinary sense, that is, nowhere interrupted but connected everywhere.

for example, that their intersections always occur at right angles; or that, if several arms of both curves meet at the same point, there will be as many arms of the first line as of the second, arranged alternately and intersecting at equal angles, etc.

Finally, I observe that it is by no means impossible to present the preceding proof, which I have here built on geometric principles, in a purely analytic form as well. But I thought that the presentation set out here would be less abstract, and that the true force of the proof is brought much more clearly before the eyes here than could be expected from an analytic proof.

To finish, I shall also indicate another method of proving our theorem. At first sight it will seem very different, not only from the preceding proof, but also from all the other proofs described above; yet, if one looks at its essence, it is in fact the same as D'ALEMBERT's. I leave it to the experts to compare it with his and to examine the parallel between the two; it is added solely for their sake.

24.

Above the plane of Fig. 4, I suppose the first and second surfaces to be drawn in the same way as above, relative to the axis CG and the fixed point C. Take any point on some branch of the first line, that is, where $T = 0$ (for example, any point M lying on the axis). Unless $U = 0$ holds there too, proceed from this point along the first line in the direction in which the absolute value of U decreases. If at the point M the absolute value of U happens to decrease in both directions, it is immaterial which way you proceed; I shall show at once what is to be done if U increases in both directions. It is therefore clear that, as you continue along the first line, you must eventually reach either a point where $U = 0$, or one where the value of U becomes a minimum, for example the point N. In the former case, what was sought has been found. In the latter, it can be proved that several branches of the first line intersect at this point (an even number of branches, in fact), half of which are such that, if you turn into one of them (in either direction), the value of U continues to decrease. (For brevity, I must omit the proof of this theorem, which is more lengthy than difficult.) You can therefore proceed again along this branch until U either becomes $= 0$ (as happens at P in Fig. 4) or again becomes a minimum. Then you will turn aside again, and must eventually reach a point where $U = 0$.

One might raise against this proof the doubt whether it is possible that, however far you proceed and although the value of U always decreases, these decreases nevertheless become continually slower, and that value never reaches some limit. This objection would correspond to the fourth in Article 6. But it would not be difficult to assign a boundary beyond which the value of U must not only change ever more rapidly, but can no longer *decrease*, so that the value 0 must necessarily already have occurred before you reach this boundary. I reserve for another occasion a fuller treatment of this and the remaining matters that I have only been able to indicate in this proof.

We discovered the principles on which this proof rests at the beginning of October 1797.

Fig 1.

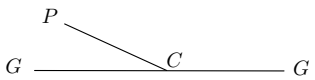


Fig.2.

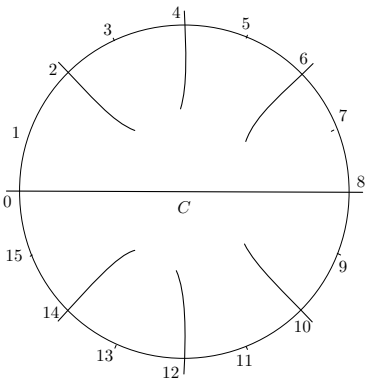


Fig 4

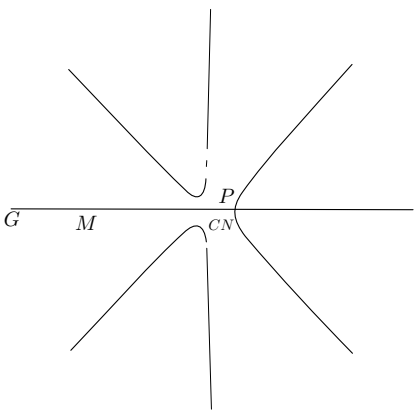
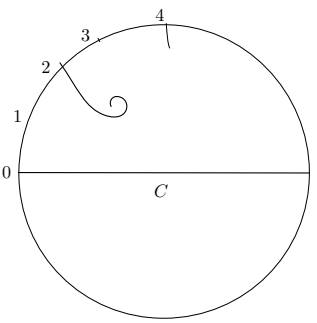


Fig 3



ANOTHER NEW PROOF

OF THE THEOREM

THAT EVERY POLYNOMIAL

IN ONE VARIABLE

CAN BE RESOLVED INTO REAL FACTORS

OF THE FIRST OR SECOND DEGREE

B Y

CARL FRIEDRICH GAUSS

SUBMITTED TO THE ROYAL SOCIETY OF SCIENCES, 1815,
DECEMBER 7.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. III.

Göttingen MDCCCXVI.

ANOTHER NEW PROOF OF THE THEOREM

THAT EVERY POLYNOMIAL

IN ONE VARIABLE

CAN BE RESOLVED INTO REAL FACTORS OF THE FIRST OR SECOND DEGREE.

1.

Although the proof of the theorem on resolving polynomials into factors that I gave in a paper published sixteen years ago seems to leave nothing to be desired either in rigour or in simplicity, I hope that mathematicians will not find it unwelcome if I return to this most important question and attempt to establish another proof, no less rigorous, from entirely different principles. That earlier proof depends, at least in part, on geometric considerations; the one I now undertake to set out, by contrast, will rest on purely analytic principles. In the work cited, I reviewed the more notable analytic methods by which other mathematicians had tried to prove our theorem up to that time, and gave a detailed account of the defects they suffer from. The most serious and truly fundamental of these is common to all those attempts, as well as to the more recent ones that have come to my attention; yet even then I declared that it seemed by no means unavoidable in an analytic proof. Let the experts now judge whether these further efforts have fully redeemed the pledge I gave at that time.

2.

Some preliminary investigations will precede the main discussion, both so that nothing may seem to be lacking and because their treatment may perhaps shed some fresh light even on matters that others have already touched upon. We shall first consider the greatest common divisor of two polynomials in one indeterminate. It should be stated at the outset that we are always speaking here only of polynomials: if a product is formed from two of them, each is called a *divisor* of that product. The *degree* of a divisor is determined by the exponent of the highest power of the indeterminate it contains, without any regard at all to the numerical coefficients. We can deal with the remaining matters concerning common divisors of polynomials more briefly, since they are entirely analogous to the corresponding properties of common divisors of numbers.

Given two polynomials Y, Y' in the indeterminate x, of which the former has a higher degree than the latter, or at least not a lower one, we shall form the following equations:

$$\begin{gathered} Y = qY' + Y'' \\ Y' = q'Y'' + Y''' \\ Y'' = q''Y''' + Y'''' \\ \text{etc., up to} \\ Y^{(\mu-1)} = q^{(\mu-1)}Y^{(\mu)} \end{gathered}$$

The rule is to divide Y first by Y' in the usual way; then Y' by the remainder Y'' of the first division, which has lower degree than Y'; then again the first remainder by the second, Y'''; and so on until a division without remainder is reached. That this must eventually happen follows from the continually decreasing degrees of the polynomials Y', Y'', Y''' etc. There is hardly any need to point out that these functions, as well as the quotients q, q', q'' etc., are *polynomials* in x. With this established, it is clear that:

I. Going backwards from the last of these equations to the first, the polynomial $Y^{(\mu)}$ is seen to divide each of the preceding ones, and is therefore certainly a common divisor of the given polynomials Y, Y'.

II. Going forwards from the first equation to the last, we see that every common divisor of the polynomials Y, Y' also divides each of the following ones, and hence the last, $Y^{(\mu)}$. Thus the polynomials Y, Y' cannot have any common divisor of higher degree than $Y^{(\mu)}$. Every common divisor of the same degree as $Y^{(\mu)}$ will stand to it in the ratio of a number to a number; hence it must itself be taken as the greatest common divisor.

III. If $Y^{(\mu)}$ has degree 0, that is, is a number, no function of the indeterminate x in the proper sense can divide Y, Y'. In this case, therefore, these polynomials are said to have no common divisor.

IV. Take the equation immediately before the last one; then eliminate $Y^{(\mu-1)}$ from it with the aid of the equation immediately before that; then again eliminate $Y^{(\mu-2)}$ with the aid of the preceding equation, and so on. In this way we obtain

$$\begin{aligned} Y^{(\mu)} &= +kY^{(\mu-2)} - k'Y^{(\mu-1)} \\ &= -k'Y^{(\mu-3)} + k''Y^{(\mu-2)} \\ &= +k''Y^{(\mu-4)} - k'''Y^{(\mu-3)} \\ &= -k'''Y^{(\mu-5)} + k''''Y^{(\mu-4)} \\ &\quad \text{etc.} \end{aligned}$$

if we suppose the polynomials k, k', k'' etc. to be formed by the following rule:

$$\begin{aligned} k &= 1 \\ k' &= q^{(\mu-2)} \\ k'' &= q^{(\mu-3)}k' + k \\ k''' &= q^{(\mu-4)}k'' + k' \\ k'''' &= q^{(\mu-5)}k''' + k'' \\ &\quad \text{etc.} \end{aligned}$$

We shall therefore have

$$\pm k^{(\mu-2)}Y \mp k^{(\mu-1)}Y' = Y^{(\mu)}$$

with the upper signs applying when μ is even and the lower when it is odd. Thus, when Y and Y' have no common divisor, we can in this way find two polynomials Z, Z' in the indeterminate x such that

$$ZY + Z'Y' = 1$$

V. The converse of this proposition clearly holds as well: if the equation

$$ZY + Z'Y' = 1$$

can be satisfied with Z, Z' polynomials in the indeterminate x, then Y and Y' certainly cannot have a common divisor.

3.

The second preliminary investigation will concern the transformation of symmetric functions. Let a, b, c etc. be indeterminate quantities, m in number. Denote their sum by λ', the sum of their products in pairs by λ'', the sum of their products in threes by λ''', etc., so that expanding the product

$$(x-a)(x-b)(x-c)\dots.$$

gives

$$x^m - \lambda' x^{m-1} + \lambda'' x^{m-2} - \lambda''' x^{m-3} + \text{etc.}$$

Thus $\lambda', \lambda'', \lambda'''$ etc. are symmetric functions of the indeterminates a, b, c etc.: that is, functions in which these indeterminates occur in the same way, or more explicitly, functions unchanged by any permutation of these indeterminates among themselves. More generally, every polynomial in $\lambda', \lambda'', \lambda'''$ etc. (whether it contains only these indeterminates or also others independent of a, b, c etc.) will clearly be a symmetric polynomial in the indeterminates a, b, c etc.

4.

The converse theorem is somewhat less evident. Let ρ be a symmetric function of the indeterminates a, b, c etc.; it will thus consist of a certain number of terms of the form

$$Ma^\alpha b^\beta c^\gamma \dots.$$

where α, β, γ etc. denote nonnegative integers, and M is a coefficient either fixed or at least independent of a, b, c etc. (if the function ρ happens to contain other indeterminates besides a, b, c etc.). First we shall establish a definite ordering of these individual terms. For this purpose, we first arrange the indeterminates a, b, c etc. in a definite order, which is itself entirely arbitrary: for example, with a in the first place, b in the second, c in the third, etc. Then, of the two terms

$$Ma^\alpha b^\beta c^\gamma \dots. \quad \text{and} \quad Ma^{\alpha'} b^{\beta'} c^{\gamma'} \dots.$$

we shall place the former higher in the ordering than the latter if

$$\begin{gathered} \text{or} \quad \alpha > \alpha', \quad \text{or} \quad \alpha = \alpha' \text{ and } \beta > \beta', \\ \text{or} \quad \alpha = \alpha', \ \beta = \beta' \text{ and } \gamma > \gamma', \quad \text{or etc.} \end{gathered}$$

that is, if the first nonvanishing one among the differences $\alpha - \alpha', \beta - \beta', \gamma - \gamma'$ etc. is positive. Terms in the same place in this ordering therefore differ only in their coefficient M, and can be combined into one term. We

shall accordingly suppose the individual terms of the function ρ to occupy different places in the ordering.

Now observe that, if $Ma^\alpha b^\beta c^\gamma \ldots\ldots$ is the highest of all the terms of the function ρ in this ordering, α must be greater than, or at least not less than, β. For if $\beta > \alpha$, the term $Ma^\beta b^\alpha c^\gamma \ldots\ldots$, which the function ρ must also contain since it is symmetric, would stand higher than $Ma^\alpha b^\beta c^\gamma \ldots\ldots$, contrary to the hypothesis. In the same way, β will be greater than, or at least not less than, γ; further, γ will not be less than the next exponent δ, etc. Hence each of the differences $\alpha - \beta$, $\beta - \gamma, \gamma - \delta$ etc. is a nonnegative integer.

Secondly, consider a product formed from any number of polynomials in the indeterminates a, b, c etc. Its highest term must be the product of the highest terms of those factors. It is equally clear that the highest terms of the functions $\lambda', \lambda'', \lambda'''$ etc. are respectively a, ab, abc etc. It follows that the highest term arising from the product

$$p = M\lambda'^{\alpha-\beta}\lambda''^{\beta-\gamma}\lambda'''^{\gamma-\delta}\ldots\ldots$$

is $Ma^\alpha b^\beta c^\gamma \ldots\ldots$. Thus, on setting $\rho - p = \rho'$, the highest term of the function ρ' will certainly stand lower in the ordering than the highest term of the function ρ. But p, and therefore also ρ', are clearly symmetric polynomials in a, b, c etc. Treating ρ' in the same way as ρ before it, we can therefore split it into $p' + \rho''$, where p' is a product of powers of $\lambda', \lambda'', \lambda'''$ etc. multiplied by a coefficient either fixed or at least independent of a, b, c etc., while ρ'' is a symmetric polynomial in a, b, c etc. whose highest term stands lower in the ordering than the highest term of ρ'. Continuing in the same way, ρ will clearly at last be reduced to the form $p + p' + p'' + p'''$ etc., that is, transformed into a polynomial in $\lambda', \lambda'', \lambda'''$ etc.

5.

We can also state the theorem proved in the preceding article as follows. Given any symmetric polynomial ρ in the indeterminates a, b, c etc., we can specify a polynomial in as many other indeterminates l', l'', l''' etc. which becomes ρ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. It is also easy to show that *this can be done in only one way.* For suppose that two different functions of the indeterminates l', l'', l''' etc., namely r and r', yield the same function of a, b, c etc. after the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. Then $r - r'$ will be a function of l', l'', l''' etc. which does not vanish in itself, but vanishes identically after those substitutions. We shall readily see that this is absurd if we consider that $r - r'$ must consist of a certain number of parts of the form

$$Ml'^\alpha l''^\beta l'''^\gamma \ldots\ldots$$

whose coefficients M do not vanish and which all differ from one another in their exponents.

The highest terms arising from these individual parts are therefore given by

$$Ma^{\alpha+\beta+\gamma+\text{etc.}}b^{\beta+\gamma+\text{etc.}}c^{\gamma+\text{etc.}}\ldots\ldots$$

and must consequently occupy different places in the ordering, so that the highest term of all cannot possibly cancel.

The actual calculation for transformations of this kind could, moreover, be greatly shortened by various shortcuts. We do not dwell on them here, since the mere possibility of the transformation already suffices for our purpose.

6.

Consider the product of $m(m-1)$ factors

$$\begin{aligned}&(a-b)(a-c)(a-d)\ldots\ldots\\ \times&(b-a)(b-c)(b-d)\ldots\ldots\\ \times&(c-a)(c-b)(c-d)\ldots\ldots\\ \times&(d-a)(d-b)(d-c)\ldots\ldots\\ &\text{etc.}\end{aligned}$$

which we shall denote by π. Since it involves the indeterminates a, b, c etc. symmetrically, we shall suppose it reduced to the form of a polynomial in $\lambda', \lambda'', \lambda'''$ etc. Let this polynomial become p when l', l'', l''' etc. are substituted respectively for $\lambda', \lambda'', \lambda'''$ etc. With this established, we shall call p the *determinant* of the polynomial

$$y = x^m - l'x^{m-1} + l''x^{m-2} - l'''x^{m-3} + \text{etc.}$$

Thus, for example, for $m = 2$ we have

$$p = -l'^2 + 4l''$$

Likewise, for $m = 3$ we find

$$p = -l'^2l''^2 + 4l'^3l''' + 4l''^3 - 18l'l''l''' + 27l'''^2$$

The determinant of the polynomial y is therefore a polynomial in the coefficients l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., becomes the product of all the differences between pairs of the quantities a, b, c etc. In the case $m = 1$, that is, when there is only one indeterminate a and hence no differences at all, it will be convenient to take the number 1 itself as the determinant of the polynomial y.

In establishing the notion of the determinant, we had to regard the coefficients of the polynomial y as indeterminate quantities. The determinant of a polynomial with fixed coefficients,

$$Y = x^m - L'x^{m-1} + L''x^{m-2} - L'''x^{m-3} + \text{etc.}$$

will be a fixed number P, namely the value of the polynomial p for $l' = L', l'' = L''$, $l''' = L'''$ etc. Thus, if we suppose that Y can be resolved into linear factors,

$$Y = (x - A)(x - B)(x - C)\ldots.$$

or that Y arises from

$$\upsilon = (x - a)(x - b)(x - c)\ldots.$$

by setting $a = A, b = B, c = C$ etc., so that the same substitutions turn $\lambda', \lambda'', \lambda'''$ etc. respectively into L', L'', L''' etc., then P will clearly equal the product of the factors

$$\begin{aligned}
&(A - B)(A - C)(A - D)\ldots. \\
\times&(B - A)(B - C)(B - D)\ldots. \\
\times&(C - A)(C - B)(C - D)\ldots. \\
\times&(D - A)(D - B)(D - C)\ldots. \\
&\text{etc.}
\end{aligned}$$

It follows that, if $P = 0$, at least two of the quantities A, B, C etc. must be equal; conversely, if it is not the case that $P = 0$, all the quantities A, B, C etc. must be unequal. We now observe that, on setting $\frac{\mathrm{d}Y}{\mathrm{d}x} = Y'$, or

$$\begin{aligned}
Y' = mx^{m-1} - (m-1)L'x^{m-2} + (m-2)L''x^{m-3} \\
-(m-3)L'''x^{m-4} + \text{etc.}
\end{aligned}$$

we have

$$\begin{aligned}
Y' = &(x - B)(x - C)(x - D)\ldots. \\
&+ (x - A)(x - C)(x - D)\ldots. \\
&+ (x - A)(x - B)(x - D)\ldots. \\
&+ (x - A)(x - B)(x - C)\ldots. \\
&+ \text{etc.}
\end{aligned}$$

Thus, if two of the quantities A, B, C etc. are equal, for example $A = B$, then Y' will be divisible by $x - A$; in other words, Y and Y' will have the common divisor $x - A$. Conversely, if Y' is supposed to have any common divisor with Y, then Y' must contain one of the linear factors $x-A, x-B, x-C$ etc., for example the first, $x - A$. This clearly cannot happen unless A equals one of the remaining quantities B, C, D etc. From all this we therefore obtain two THEOREMS:

I. *If the determinant of the polynomial Y is $= 0$, then Y certainly has a common divisor with Y'; hence, if Y and Y' have no common divisor, the determinant of the polynomial Y cannot be $= 0$.*

II. *If the determinant of the polynomial Y is not $= 0$, then Y and Y' certainly cannot have a common divisor; or, if Y and Y' have a common divisor, the determinant of the polynomial Y must necessarily be $= 0$.*

7.

But it must be carefully noted that the whole force of this very simple proof rests on the supposition that the polynomial Y can be resolved into linear factors. At this very point, where the general possibility of such a resolution is to be proved, that supposition would be nothing but begging the question. Yet not all those who have attempted analytic proofs of the main theorem have guarded against fallacies exactly like this. We have already pointed out the origin of this plausible illusion in the very statement of the inquiry: all of them investigated only the *form* of the roots of equations, whereas they ought to have proved their *existence*, which they rashly assumed. But enough has already been said in the paper cited above about this way of proceeding, which departs too far from rigour and clarity. We shall therefore now place the theorems of the preceding article, at least one of which we cannot do without for our purpose, on a firmer foundation. We shall begin with the second, as the easier one.

8.

Denote by ρ the function

$$\begin{aligned}
&\frac{\pi(x-b)(x-c)(x-d)\ldots.}{(a-b)^2(a-c)^2(a-d)^2\ldots.}\\
&+\frac{\pi(x-a)(x-c)(x-d)\ldots.}{(b-a)^2(b-c)^2(b-d)^2\ldots.}\\
&+\frac{\pi(x-a)(x-b)(x-d)\ldots.}{(c-a)^2(c-b)^2(c-d)^2\ldots.}\\
&+\frac{\pi(x-a)(x-b)(x-c)\ldots.}{(d-a)^2(d-b)^2(d-c)^2\ldots.}\\
&+\text{etc.}
\end{aligned}$$

which, since π is divisible by each denominator, is a polynomial in the indeterminates x, a, b, c etc. Further, set $\frac{\mathrm{d}\upsilon}{\mathrm{d}x} = \upsilon'$, so that we have

$$\begin{aligned}
\upsilon' = &(x-b)(x-c)(x-d)\ldots.\\
&+(x-a)(x-c)(x-d)\ldots.\\
&+(x-a)(x-b)(x-d)\ldots.\\
&+(x-a)(x-b)(x-c)\ldots.\\
&+\text{etc.}
\end{aligned}$$

For $x = a$ we clearly have $\rho\upsilon' = \pi$. Hence we conclude that the polynomial $\pi - \rho\upsilon'$ is identically divisible by $x - a$, and likewise by $x - b, x - c$ etc., as well as by their product υ. Thus, setting

$$\frac{\pi - \rho\upsilon'}{\upsilon} = \sigma$$

we obtain for σ a polynomial in the indeterminates x, a, b, c etc. which, like ρ, is symmetric with respect to the indeterminates a, b, c etc. We can therefore find two polynomials r, s in the indeterminates x, l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., become ρ, σ respectively. Following the analogy, let us denote the polynomial

$$\begin{aligned}
mx^{m-1} - (m-1)l'x^{m-2} + (m-2)l''x^{m-3}\\
-(m-3)l'''x^{m-4} + \text{etc.}
\end{aligned}$$

that is, the derivative $\frac{\mathrm{d}y}{\mathrm{d}x}$, by y', so that y' becomes υ' under those same substitutions. Then $p - sy - ry'$ clearly becomes $\pi - \sigma\upsilon - \rho\upsilon'$ under the same substitutions, that is, 0, and must therefore already vanish identically in itself (Article 5). We thus have the identity

$$p = sy + ry'$$

Hence, if we suppose that substituting $l' = L', l'' = L'', l''' = L'''$ etc. gives $r = R, s = S$, we also have identically

$$P = SY + RY'$$

Here S, R are polynomials in x, while P is a fixed quantity or number. It follows at once that Y and Y' cannot have a common divisor unless $P = 0$. This is precisely the second theorem of Article 6.

9.

We shall complete the proof of the first theorem by showing that, when Y and Y' have no common divisor, $P = 0$ certainly cannot hold. For this purpose, first suppose that two polynomials in the indeterminate x, namely fx and φx, have been found by the rules of Article 2, such that the identity

$$fx \,.\, Y + \varphi x \,.\, Y' = 1$$

holds. We write it here as

$$fx \,.\, \upsilon + \varphi x \,.\, \upsilon' = 1 + fx \,.\, (\upsilon - Y) + \varphi x \,.\, \frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x}$$

or, since we have

$$\begin{aligned} \upsilon' = {} & (x-b)(x-c)(x-d)\ldots. \\ & + (x-a) \,.\, \frac{\mathrm{d}[(x-b)(x-c)(x-d)\ldots.]}{\mathrm{d}x} \end{aligned}$$

in the following form:

$$\begin{aligned} & \varphi x \,.\, (x-b)(x-c)(x-d)\ldots. \\ & + \varphi x \,.\, (x-a) \,.\, \frac{\mathrm{d}[(x-b)(x-c)(x-d)\ldots.]}{\mathrm{d}x} \\ & + fx \,.\, (x-a)(x-b)(x-c)(x-d)\ldots. \\ & = 1 + fx \,.\, (\upsilon - Y) + \varphi x \,.\, \frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x} \end{aligned}$$

For brevity, we shall denote

$$fx \,.\, (y - Y) + \varphi x \,.\, \frac{\mathrm{d}(y - Y)}{\mathrm{d}x}$$

which is a polynomial in the indeterminates x, l', l'', l''' etc.,

$$\text{by} \quad F(x, l', l'', l''' \text{ etc.})$$

Thus we have identically

$$1 + fx\,.\,(\upsilon - Y) + \varphi x\,.\,\frac{\mathrm{d}(\upsilon - Y)}{\mathrm{d}x}$$
$$= 1 + F(x, \lambda', \lambda'', \lambda''' \text{ etc.})$$

We shall therefore have the identities [1]

$$\varphi a\,.\,(a-b)(a-c)(a-d)\ldots.$$
$$= 1 + F(a, \lambda', \lambda'', \lambda''' \text{ etc.})$$
$$\varphi b\,.\,(b-a)(b-c)(b-d)\ldots.$$
$$= 1 + F(b, \lambda', \lambda'', \lambda''' \text{ etc.})$$
$$\varphi c\,.\,(c-a)(c-b)(c-d)\ldots.$$
$$= 1 + F(c, \lambda', \lambda'', \lambda''' \text{ etc.})$$
$$\text{etc.}$$

Now suppose the product of all the expressions

$$1 + F(a, l', l'', l''' \text{ etc.})$$
$$1 + F(b, l', l'', l''' \text{ etc.})$$
$$1 + F(c, l', l'', l''' \text{ etc.})$$
$$\text{etc.}$$

which is a polynomial in the indeterminates a, b, c etc., l', l'', l''' etc., and is symmetric with respect to a, b, c etc., to be represented by

$$\psi(\lambda', \lambda'', \lambda''' \text{ etc.},\ l', l'', l''' \text{ etc.})$$

Multiplying all the equations [1] then gives the new identity [2]

$$\pi\varphi a\,.\,\varphi b\,.\,\varphi c\ldots. = \psi(\lambda', \lambda'', \lambda''' \text{ etc.},\ \lambda', \lambda'', \lambda''' \text{ etc.})$$

Further, since the product $\varphi a\,.\,\varphi b\,.\,\varphi c\ldots.$ involves the indeterminates a, b, c etc. symmetrically, we can clearly find a polynomial in the indeterminates l', l'', l''' etc. which, under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., becomes $\varphi a\,.\,\varphi b\,.\,\varphi c\ldots..$ Let t be this polynomial. We then also have identically [3]

$$pt = \psi(l', l'', l''' \text{ etc.},\ l', l'', l''')$$

since these same substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc. turn this equation into the identity [2].

Now the very definition of the function F gives the identity

$$F(x, L', L'', L''' \text{ etc.}) = 0$$

Hence we also have identically

$$1 + F(a, L', L'', L''' \text{ etc.}) = 1$$
$$1 + F(b, L', L'', L''' \text{ etc.}) = 1$$
$$1 + F(c, L', L'', L''' \text{ etc.}) = 1$$
$$\text{etc.}$$

and therefore also identically

$$\psi(\lambda', \lambda'', \lambda''' \text{ etc.},\ L', L'', L''' \text{ etc.}) = 1$$

and thus identically [4]

$$\psi(l', l'', l''' \text{ etc.},\ L'. L'', L''' \text{ etc.}) = 1$$

Combining equations [3] and [4], and substituting $l' = L'$, $l'' = L'', l''' = L'''$ etc., we shall therefore have [5]

$$PT = 1$$

where T denotes the value of the polynomial t corresponding to those substitutions. Since this value must be a finite quantity, P certainly cannot be $= 0$. Q. E. D.

10.

It is now clear from the preceding results that any polynomial Y in one indeterminate x whose determinant is $= 0$ can be decomposed into factors none of which has determinant 0. For, once the greatest common divisor of the polynomials Y and $\frac{\mathrm{d}Y}{\mathrm{d}x}$ has been found, the former is resolved into two factors. If one of these factors[*)] again has determinant 0, it will be resolved into two factors in the same way. We shall continue in this manner until Y is finally resolved into factors none of which has determinant 0.

It is also easy to see that among these factors into which Y is resolved, at least one must have the following property: among the factors of the number expressing its degree, the number two occurs no more often than among the factors of the number m expressing the degree of the polynomial Y. That is, if we set $m = k \,.\, 2^{\mu}$, with k denoting an odd number, then among the factors of the polynomial Y there is at least one of degree $k' \,.\, 2^{\nu}$, where k' is also odd, and either $\nu = \mu$ or $\nu < \mu$. This assertion follows at once from the fact that m is the sum of the numbers expressing the degrees of the individual factors of Y.

[*)] In fact, only the factor which is that common divisor can have determinant 0. But a proof of this proposition would lead us into some detours here; nor is it needed here, since the other factor, even if its determinant could also vanish, could be treated in the same way and resolved into factors.

11.

Before proceeding further, we shall explain an expression whose introduction is of great use in all investigations of symmetric functions, and which will also be very convenient for us. Suppose M is a function of some of the indeterminates a, b, c etc., and let μ be the number of them entering the expression M, without regard to any other indeterminates that M may also involve. Permuting those μ indeterminates in every possible way, both among themselves and with the remaining $m - \mu$ of a, b, c etc., produces from M other expressions similar to M. In all there are

$$m(m-1)(m-2)(m-3)\ldots.(m-\mu+1)$$

expressions, including M itself; we shall call their collection simply the *collection of all M.* It is then clear what is meant by the sum of all M, the product of all M, etc. Thus, for example, π is called the product of all $a - b$, υ the product of all $x - a$, and υ' the sum of all $\frac{\upsilon}{x-a}$, etc.

If M is symmetric with respect to some of the μ indeterminates it contains, permutations of these among themselves do not change the function M. Thus every term occurs several times in the collection of all M: namely, $1\,.\,2\,.\,3\ldots.\nu$ times, if ν is the number of indeterminates with respect to which M is symmetric. If M is symmetric not only with respect to ν indeterminates, but also with respect to ν' others, and again with respect to ν'' others, etc., then M remains unchanged whether two of the first ν indeterminates are interchanged, or two of the second ν', or two of the third ν'', etc. Thus

$$1\,.\,2\,.\,3\ldots.\nu\,.\quad 1\,.\,2\,.\,3\ldots.\nu'\,.\quad 1\,.\,2\,.\,3\ldots.\nu''\text{ etc.}$$

permutations always give identical terms. If we retain only one of these identical terms each time, we therefore obtain in all

$$\frac{m(m-1)(m-2)(m-3)\ldots.(m-\mu+1)}{1\,.\,2\,.\,3\ldots.\nu\,.\,1\,.\,2\,.\,3\ldots.\nu'\,.\,1\,.\,2\,.\,3\ldots.\nu''\text{ etc.}}$$

terms, whose collection we shall call the *collection of all M with repetitions excluded*, to distinguish it from the *collection of all M with repetitions included*. Unless an explicit qualification is given, we shall always understand repetitions to be included.

It is also easy to see that the sum of all M, or the product of all M, or more generally any symmetric function of all M, is always a symmetric function of the indeterminates a, b, c etc., whether repetitions are included or excluded.

12.

With u, x denoting indeterminates, consider now the product of all $u - (a+b)x + ab$, with repetitions excluded, and denote it by ζ. Thus ζ is the product of the following $\frac{1}{2}m(m-1)$ factors:

$$\begin{gathered} u-(a+b)x+ab \\ u-(a+c)x+ac \\ u-(a+d)x+ad \\ \text{etc.} \\ u-(b+c)x+bc \\ u-(b+d)x+bd \\ \text{etc.} \\ u-(c+d)x+cd \\ \text{etc. etc.} \end{gathered}$$

Since this function involves the indeterminates a, b, c etc. symmetrically, we can find a polynomial in the indeterminates u, x, l', l'', l''' etc., to be denoted by z, which becomes ζ when $\lambda', \lambda'', \lambda'''$ etc. are substituted for the indeterminates l', l'', l''' etc. Finally, denote by Z the function of the indeterminates u, x alone into which z passes when the indeterminates l', l'', l''' etc. are assigned the fixed values L', L'', L''' etc.

These three functions ζ, z, Z can be regarded as polynomials of degree $\frac{1}{2}m(m-1)$ in the indeterminate u with indeterminate coefficients. These coefficients are

for ζ, functions of the indeterminates x, a, b, c etc.
for z, functions of the indeterminates x, l', l'', l''' etc.
for Z, functions only of the indeterminate x.

The individual coefficients of z become those of ζ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., and those of Z under the substitutions $l' = L', l'' = L'', l''' = L'''$ etc. What we have just said about the coefficients also holds for the determinants of the functions ζ, z, Z. We shall now examine these more closely, with the aim of proving the following

THEOREM. *Whenever $P = 0$ does not hold, the determinant of the function Z certainly cannot be identically $= 0$.*

13.

The proof of this theorem would indeed be very easy if we were allowed to suppose that Y could be resolved into linear factors

$$(x-A)(x-B)(x-C)(x-D)\ldots.$$

For it would then also be certain that Z is the product of all $u-(A+B)x+AB$, and that the determinant of the function Z is the product of the differences between pairs of the quantities

$$\begin{gathered}(A+B)x-AB\\(A+C)x-AC\\(A+D)x-AD\\\text{etc.}\\(B+C)x-BC\\(B+D)x-BD\\\text{etc.}\\(C+D)x-CD\\\text{etc. etc}\end{gathered}$$

But this product cannot vanish identically unless one of its factors itself becomes identically $=0$. This would imply that two of the quantities A, B, C etc. are equal, and thus that the determinant P of the polynomial Y becomes $=0$, contrary to the hypothesis.

Setting aside this argument, which clearly starts by begging the question just as in Article 6, we now proceed directly to give a sound proof of the theorem of Article 12.

14.

The determinant of the function ζ will be the product of all the differences between pairs of $(a+b)x-ab$. The number of these differences is

$$\frac{1}{2}m(m-1)(\tfrac{1}{2}m(m-1)-1)=\frac{1}{4}(m+1)m(m-1)(m-2)$$

This number therefore gives the degree of the determinant of the function ζ with respect to the indeterminate x. The determinant of the function z will have the same degree. The determinant of the function Z, however, may have a lower degree, whenever some coefficients, starting from the highest power of x, vanish. Our task is now to prove that *all* the coefficients in the determinant of the function Z certainly cannot vanish.

On examining more closely the differences whose product is the determinant of the function ζ, we find that some of them—the differences between pairs of $(a+b)x-ab$ having an element in common—give

$$\text{the product of all}\quad (a-b)(x-c)$$

while the remaining ones—the differences between pairs of $(a+b)x-ab$ whose elements are distinct—give

the product of all $\quad (a+b-c-d)x-ab+cd, \quad$ with repetitions excluded.

The first product clearly contains each factor $a-b$ exactly $m-2$ times, and each factor $x-c$ exactly $(m-1)(m-2)$ times. We therefore readily conclude that this product is

$$= \pi^{m-2} \upsilon^{(m-1)(m-2)}$$

If we denote the second product by ρ, the determinant of the function ζ is thus

$$= \pi^{m-2} \upsilon^{(m-1)(m-2)} \rho$$

Further, let r denote the function of the indeterminates x, l', l'', l''' etc. which becomes ρ under the substitutions $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ etc., and let R denote the function of x alone into which r passes under the substitutions $l' = L', l'' = L''$, $l''' = L'''$ etc. It is then clear that the determinant of the function z is

$$= p^{m-2} y^{(m-1)(m-2)} r$$

and that the determinant of the function Z is

$$= P^{m-2} Y^{(m-1)(m-2)} R$$

Since, by hypothesis, P is not $= 0$, it now remains to prove that R certainly cannot vanish identically.

15.

For this purpose we shall introduce one more indeterminate w and consider the product of all

$$(a+b-c-d)w + (a-c)(a-d)$$

with repetitions excluded. Since it involves a, b, c etc. symmetrically, it can be represented as a polynomial in the indeterminates $w, \lambda', \lambda'', \lambda'''$ etc. We shall denote this function by $f(w, \lambda', \lambda'', \lambda'''$ etc.). The number of the factors $(a+b-c-d)w + (a-c)(a-d)$ is

$$= \frac{1}{2} m(m-1)(m-2)(m-3)$$

from which we readily conclude that

$$f(0, \lambda', \lambda'', \lambda''' \text{ etc.}) = \pi^{(m-2)(m-3)}$$

and hence also

$$f(0, l', l'', l''' \text{ etc.}) = p^{(m-2)(m-3)}$$

as well as

$$f(0, L', L'', L''' \text{ etc.}) = P^{(m-2)(m-3)}$$

In general, the polynomial $f(w, L', L'', L''' \text{ etc.})$ will have degree

$$\frac{1}{2}m(m-1)(m-2)(m-3)$$

but in special cases it may have a lower degree, if some coefficients, starting from the highest power of w, happen to vanish. It is impossible, however, for the entire function to be identically $= 0$, since the equation just found shows that at least its last term does not vanish. Suppose that the highest term of the polynomial $f(w, L', L'', L''' \text{ etc.})$ having a nonvanishing coefficient is Nw^ν. If we substitute $w = x - a$, then $f(x - a, L', L'', L''' \text{ etc.})$ is clearly a polynomial in the indeterminates x, a, or, equivalently, a polynomial in x with coefficients depending on the indeterminate a. Its highest term is nevertheless Nx^ν, and thus has a fixed coefficient, independent of a, which is not $= 0$. Likewise, $f(x - b, L', L'', L''' \text{ etc.}), f(x - c, L', L'', L''' \text{ etc.})$ are polynomials in the indeterminate x, each with highest term Nx^ν, while the coefficients of the following terms depend respectively on b, c etc. Hence the product of the m factors

$$\begin{gathered} f(x - a, L', L'', L''' \text{ etc.}) \\ f(x - b, L', L'', L''' \text{ etc.}) \\ f(x - c, L', L'', L''' \text{ etc.}) \\ \text{etc.} \end{gathered}$$

is a polynomial in x whose highest term is $N^m x^{m\nu}$, while the coefficients of the following terms depend on the indeterminates a, b, c etc.

Next consider the product of these m factors:

$$\begin{gathered} f(x - a, l', l'', l''' \text{ etc.}) \\ f(x - b, l', l'', l''' \text{ etc.}) \\ f(x - c, l', l'', l''' \text{ etc.}) \\ \text{etc.} \end{gathered}$$

As a function of the indeterminates x, a, b, c etc., l', l'', l''' etc., symmetric with respect to a, b, c etc., it can be represented as a function of the indeterminates $x, \lambda', \lambda'', \lambda'''$ etc., l', l'', l''' etc., which we shall denote by

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.},\ l', l'', l''' \text{ etc.})$$

Thus

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.},\ \lambda', \lambda'', \lambda''' \text{ etc.})$$

is the product of the factors

$$\begin{gathered} f(x-a, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ f(x-b, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ f(x-c, \lambda', \lambda'', \lambda''' \text{ etc.}) \\ \text{etc.} \end{gathered}$$

and is therefore identically divisible by ρ, since it is easy to see that every factor of ρ occurs in one of those factors. We therefore set

$$\begin{aligned} &\varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.},\ \lambda', \lambda'', \lambda''' \text{ etc.}) \\ &= \rho\psi(x, \lambda', \lambda'', \lambda''' \text{ etc.}) \end{aligned}$$

where the symbol ψ represents a polynomial. It follows readily that we also have identically

$$\begin{aligned} &\varphi(x, L', L'', L''' \text{ etc.},\ L', L'', L''' \text{ etc.}) \\ &= R\psi(x, L', L'', L''' \text{ etc.}) \end{aligned}$$

But we have proved above that the product of the factors

$$\begin{gathered} f(x-a, L', L'', L''' \text{ etc.}) \\ f(x-b, L', L'', L''' \text{ etc.}) \\ f(x-c, L', L'', L''' \text{ etc.}) \\ \text{etc.} \end{gathered}$$

which is $= \varphi(x, \lambda', \lambda'', \lambda''' \text{ etc.},\ L', L'', L''' \text{ etc.})$, has highest term $N^m x^{m\nu}$. The function $\varphi(x, L', L'', L''' \text{ etc.}, L', L'', L''' \text{ etc.})$ therefore has the same highest term, and is certainly not identically $= 0$. Hence R cannot be identically $= 0$ either, and neither can the determinant of the function Z. Q. E. D.

16.

THEOREM. *Let $\varphi(u,x)$*[*)] *denote a product of any number of factors in which the indeterminates u, x enter only linearly, that is, factors of the form*

$$\alpha+\beta u+\gamma x$$
$$\alpha'+\beta' u+\gamma' x$$
$$\alpha''+\beta'' u+\gamma'' x$$
$$\text{etc.}$$

and let w be another indeterminate. Then the function

$$\varphi(u+w\,.\,\tfrac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x},\ x-w\,.\,\tfrac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u})=\Omega$$

is identically divisible by $\varphi(u,x)$.

Proof. Setting

$$\begin{aligned}\varphi(u,x)&=(\alpha+\beta u+\gamma x)Q\\&=(\alpha'+\beta' u+\gamma' x)Q'\\&=(\alpha''+\beta'' u+\gamma'' x)Q''\\&\quad\text{etc.}\end{aligned}$$

we obtain for Q, Q', Q'' etc. polynomials in the indeterminates $u, x, \alpha, \beta, \gamma$, α', β', γ', $\alpha'', \beta'', \gamma''$ etc., and

$$\begin{aligned}\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x}&=\gamma Q+(\alpha+\beta u+\gamma x)\,.\,\frac{\mathrm{d}Q}{\mathrm{d}x}\\&=\gamma' Q'+(\alpha'+\beta' u+\gamma' x)\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}x}\\&=\gamma'' Q''+(\alpha''+\beta'' u+\gamma'' x)\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}x}\\&\quad\text{etc.}\end{aligned}$$

$$\begin{aligned}\frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}&=\beta Q+(\alpha+\beta u+\gamma x)\,.\,\frac{\mathrm{d}Q}{\mathrm{d}u}\\&=\beta' Q'+(\alpha'+\beta' u+\gamma' x)\,.\,\frac{\mathrm{d}Q'}{\mathrm{d}u}\\&=\beta'' Q''+(\alpha''+\beta'' u+\gamma'' x)\,.\,\frac{\mathrm{d}Q''}{\mathrm{d}u}\\&\quad\text{etc.}\end{aligned}$$

[*)] Every reader will see, even without our pointing it out, that the symbols introduced in the preceding article are confined to that article alone, and that the present meaning of the symbols φ, w must therefore not be confused with their former meaning.

When these values are substituted in the factors whose product is Ω, namely in

$$\alpha + \beta u + \gamma x + \beta w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x} - \gamma w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}$$
$$\alpha' + \beta' u + \gamma' x + \beta' w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x} - \gamma' w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}$$
$$\alpha'' + \beta'' u + \gamma'' x + \beta'' w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}x} - \gamma'' w \,.\, \frac{\mathrm{d}\varphi(u,x)}{\mathrm{d}u}$$
etc., respectively

these take the following values:

$$(\alpha + \beta u + \gamma x)(1 + \beta w \,.\, \tfrac{\mathrm{d}Q}{\mathrm{d}x} - \gamma w \,.\, \tfrac{\mathrm{d}Q}{\mathrm{d}u})$$
$$(\alpha' + \beta' u + \gamma' x)(1 + \beta' w \,.\, \tfrac{\mathrm{d}Q'}{\mathrm{d}x} - \gamma' w \,.\, \tfrac{\mathrm{d}Q'}{\mathrm{d}u})$$
$$(\alpha'' + \beta'' u + \gamma'' x)(1 + \beta'' w \,.\, \tfrac{\mathrm{d}Q''}{\mathrm{d}x} - \gamma'' w \,.\, \tfrac{\mathrm{d}Q''}{\mathrm{d}u})$$
etc.

Thus Ω is the product of $\varphi(u,x)$ and the factors

$$1 + \beta w \,.\, \frac{\mathrm{d}Q}{\mathrm{d}x} - \gamma w \,.\, \frac{\mathrm{d}Q}{\mathrm{d}u}$$
$$1 + \beta' w \,.\, \frac{\mathrm{d}Q'}{\mathrm{d}x} - \gamma' w \,.\, \frac{\mathrm{d}Q'}{\mathrm{d}u}$$
$$1 + \beta'' w \,.\, \frac{\mathrm{d}Q''}{\mathrm{d}x} - \gamma'' w \,.\, \frac{\mathrm{d}Q''}{\mathrm{d}u}$$

etc., that is, of $\varphi(u,x)$ and a polynomial in the indeterminates $u, x, w, \alpha, \beta, \gamma$, $\alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ etc. Q. E. D.

17.

The theorem of the preceding article clearly applies to the function ζ, which we shall now represent by

$$f(u, x, \lambda', \lambda'', \lambda''' \text{ etc.})$$

so that

$$f(u + w \,.\, \tfrac{\mathrm{d}\zeta}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}\zeta}{\mathrm{d}u},\ \lambda', \lambda'', \lambda''' \text{ etc.})$$

is identically divisible by ζ. The quotient is a polynomial in the indeterminates u, x, w, a, b, c etc., symmetric with respect to a, b, c etc.; we shall represent it by

$$\psi(u, x, w, \lambda', \lambda'', \lambda''' \text{ etc.})$$

We conclude that we also have identically

$$f(u + w \,.\, \tfrac{\mathrm{d}z}{\mathrm{d}x},\ x - w \,.\, \tfrac{\mathrm{d}z}{\mathrm{d}u},\ l', l'', l''' \text{ etc.})$$
$$= z\psi(u, x, w, l', l'', l''' \text{ etc.})$$

and likewise

$$f(u + w\,.\,\tfrac{\mathrm{d}Z}{\mathrm{d}x},\ x - w\,.\,\tfrac{\mathrm{d}Z}{\mathrm{d}u},\ L', L'', L''' \text{ etc.})$$
$$= Z\psi(u, x, w, L', L'', L''' \text{ etc.})$$

Thus, if we represent the function Z simply by $F(u, x)$, so that

$$f(u, x, L', L'', L''' \text{ etc.}) = F(u, x)$$

holds, we have identically

$$F(u + w\,.\,\tfrac{\mathrm{d}Z}{\mathrm{d}x},\ x - w\,.\,\tfrac{\mathrm{d}Z}{\mathrm{d}u})$$
$$= Z\psi(u, x, w, L', L'', L''' \text{ etc.})$$

18.

Suppose, then, that fixed values of u, x, namely $u = U, x = X$, give

$$\frac{\mathrm{d}Z}{\mathrm{d}x} = X', \quad \frac{\mathrm{d}Z}{\mathrm{d}u} = U'$$

We have identically

$$F(U + wX',\ X - wU')$$
$$= F(U, X)\,.\,\psi(U, X, w, L', L'', L''' \text{ etc.})$$

Whenever U' does not vanish, we may set

$$w = \frac{X - x}{U'}$$

which gives

$$F(U + \tfrac{XX'}{U'} - \tfrac{X'x}{U'},\ x)$$
$$= F(U, X)\,.\,\psi(U, X, \tfrac{X-x}{U'}, L', L'', L''' \text{ etc.})$$

This can also be stated as follows:

If in the function Z we set $u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$, it becomes

$$F(U, X)\,.\,\psi(U, X, \tfrac{X-x}{U'}, L', L'', L''' \text{ etc.})$$

19.

In the case where $P = 0$ does not hold, the determinant of the function Z is a function of the indeterminate x that does not vanish in itself. The number of fixed values of x for which this determinant can take the value 0 is therefore clearly finite. Thus infinitely many fixed values of x can be specified which give this determinant a value different from 0. Let X be such a value

of x, which we may also suppose to be *real*. The determinant of the function $F(u, X)$ is then not $= 0$. By Theorem II of Article 6, the functions

$$F(u, X) \quad \text{and} \quad \frac{\mathrm{d}F(u, X)}{\mathrm{d}u}$$

can therefore have no common divisor. Suppose further that there is a fixed value of u, namely U, either real or imaginary, that is, of the form $g + h\sqrt{-1}$, which makes $F(u, X) = 0$, so that $F(U, X) = 0$. Then $u - U$ is a factor of the polynomial $F(u, X)$, and the function $\frac{\mathrm{d}F(u,X)}{\mathrm{d}u}$ is consequently certainly not divisible by $u - U$. Suppose this function, $\frac{\mathrm{d}F(u,X)}{\mathrm{d}u}$, takes the value U' when $u = U$ is set. It certainly cannot be the case that $U' = 0$. Now U' is clearly the value of the partial derivative $\frac{\mathrm{d}Z}{\mathrm{d}u}$ for $u = U, x = X$. If we also denote by X' the value of the partial derivative $\frac{\mathrm{d}Z}{\mathrm{d}x}$ for the same values of u, x, the preceding article shows that the function Z vanishes identically under the substitution

$$u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$$

and is therefore identically divisible by the factor

$$u + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

Hence, on setting $u = xx$, we see that $F(xx, x)$ is divisible by

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

and thus takes the value 0 when x is taken to be a root of the equation

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'}) = 0$$

that is, when we set

$$x = \frac{-X' \pm \sqrt{(4UU'U' + 4XX'U' + X'X')}}{2U'}$$

These values are known to be either real or of the form $g + h\sqrt{-1}$.

It is now easy to prove that the function Y must also vanish for these same values of x. For $f(xx, x, \lambda', \lambda'', \lambda'''$ etc.) is clearly the product of all $(x - a)(x - b)$, with repetitions excluded, and thus is $= \upsilon^{m-1}$. It follows at once that

$$f(xx, x, l', l'', l''' \text{ etc.}) = y^{m-1}$$
$$f(xx, x, L', L'', L''' \text{ etc.}) = Y^{m-1}$$

or $F(xx, x) = Y^{m-1}$, whose fixed value therefore cannot vanish unless the value of Y vanishes at the same time.

20.

The preceding investigations have reduced the *solution* of the equation $Y = 0$, that is, the finding of a fixed value of x, either real or of the form $g + h\sqrt{-1}$, which satisfies it, to the solution of the equation $F(u, X) = 0$, provided that the determinant of the function Y is not $= 0$. It should be observed that, if all the coefficients in Y, that is, the numbers L', L'', L''' etc., are real quantities, all the coefficients in $F(u, X)$ are also real, provided that a real quantity is taken for X, as is allowed. The degree of the secondary equation $F(u, X) = 0$ is given by the number $\frac{1}{2}m(m-1)$. Whenever m is an even number of the form $2^\mu k$, with k denoting an undetermined odd number, the degree of the secondary equation is therefore given by a number of the form $2^{\mu-1}k$.

If the determinant of the function Y becomes $= 0$, Article 10 gives another polynomial $\mathfrak{Y}$ dividing it, whose determinant is not $= 0$ and whose degree is given by a number of the form $2^\nu k$, with either $\nu < \mu$ or $\nu = \mu$. Every solution of the equation $\mathfrak{Y} = 0$ also satisfies the equation $Y = 0$. The solution of the equation $\mathfrak{Y} = 0$ is again reduced to the solution of another equation whose degree is given by a number of the form $2^{\nu-1}k$.

We therefore conclude that, in general, the solution of any equation whose degree is an even number of the form $2^\mu k$ can be reduced to the solution of another equation whose degree is of the form $2^{\mu'}k$, with $\mu' < \mu$. Whenever this number is still even, that is, μ' is not $= 0$, the same method is applied again. We shall continue in this way until we reach an equation of odd degree. All its coefficients will be real if all the coefficients of the original equation were real. Such an equation of odd degree is known to have a solution, indeed a real root. Each of the preceding equations will therefore also have a solution, either through real roots or through roots of the form $g + h\sqrt{-1}$.

It has thus been established that any polynomial Y of the form $x^m - L'x^{m-1} + L''x^{m-2} -$ etc., where L', L'' etc. are fixed real quantities, contains a factor $x - A$, where A is a quantity either real or of the form $g + h\sqrt{-1}$. In the latter case it is easy to see that Y also takes the value 0 under the substitution $x = g - h\sqrt{-1}$, and is therefore divisible by $x - (g - h\sqrt{-1})$, hence also by the product $xx - 2gx + gg + hh$. Every polynomial Y therefore certainly contains a real factor of the first or second degree. Since the same holds again for the quotient, Y can clearly be resolved into real factors of the first or second degree. This was what the present paper set out to prove.
