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`

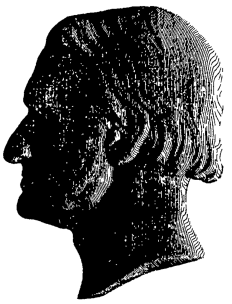
CARL FRIEDRICH GAUSS COLLECTED WORKS

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.