(1905–1910), who has traced the Celtiberian town, the lines of Scipio and several other Roman camps dating from the Numantine Wars. (F. J. H.)

NUMA POMPILIUS, second legendary king of Rome (715–672 B.C.), was a Sabine, a native of Cures, and his wife was the daughter of Titus Tatius, the Sabine colleague of Romulus. He was elected by the Roman people at the close of a year's interregnum, during which the sovereignty had been exercised by the members of the senate in rotation. Nearly all the early religious institutions of Rome were attributed to him. He set up the worhip of Terminus (the god of landmarks), appointed the festival of Fides (Faith), built the temple of Janus, reorganized the calendar and fixed days of business and holiday. He instituted the flamens (sacred priests) of Jupiter, Mars and Quirinus; the virgins of Vesta, to keep the sacred fire burning on the hearth of the city; the Salii, to guard the shield that fell from heaven; the pontifices and augurs, to arrange the rites and interpret the will of the gods; he also divided the handicraftsmen into nine gilds. He derived his inspiration from his wife, the nymph Egeria, whom he used to meet by night in her sacred grove. After a long and peaceful reign, during which the gates of Janus were closed, Numa died and was succeeded by the warlike Tullus Hostilius. Livy (xl. 29) tells a curious story of two stone chests, bearing inscriptions in Greek and Latin, which were found at the foot of the Janiculum (181 B.C.), one purporting to contain the body of Numa and the other his books. The first when opened was found to be empty, but the second contained fourteen books relating to philosophy and pontifical law, which were publicly burned as tending to undermine the established religion.

No single legislator can really be considered responsible for all the institutions ascribed to Numa; they are essentially Italian, and older than Rome itself. Even Roman tradition itself wavers; *e.g.* the fetiales are variously attributed to Tullus Hostilius and Ancus Marcius. The supposed law-books, which were to all appearance new when discovered, were clearly forgeries.

See Livy i. 18-21; Plutarch, *Numa*; Dion. Halic. ii. 58-76; Cicero, *De republica*, ii. 13-15. For criticism: Schwegler, *Römische Geschichte*, bk. xi.; Sir G. Cornewall Lewis, *Credibility of early Roman History*, ch. xi.; W. Ihne, *Hist. of Rome*, i.; E. Pais, *Storia di Roma*, i. (1898), where Numa is identified with Titus Tatius and made out to be a river god, Numicius, closely connected with Aeneas; J. B. Carter, *The Religion of Numa* (1906); O. Gilbert, *Geschichte und Topographie der Stadt Rom im Altertum* (1883–1885); and ROME: *Ancient History*.

NUMBER[1] (through Fr. *nombre*, from Lat. *numerus*; from a root seen in Gr. *νέμειν* to distribute), a word generally expressive of quantity, the fundamental meaning of which leads on analysis to some of the most difficult problems of higher mathematics.

1. The most elementary process of thought involves a distinction within an identity—the A and the not-A within the sphere throughout which these terms are intelligible. Again A may be a generic quality found in different modes Aa, Ab, Ac, &c.; for instance, colour in the modes, red, green, blue and so on. Thus the notions of "one," "two," and the vague "many" are fundamental, and must have impressed themselves on the human mind at a very early period: evidence of this is found in the grammatical distinction of singular, dual and plural which occurs in ancient languages of widely different races. A more definite idea of number seems to have been gradually acquired by realizing the equivalence, as regards plurality, of different concrete groups, such as the fingers of the right hand and those of the left. This led to the invention of a set of names which in the first instance did not suggest a numerical system, but denoted certain recognized forms of plurality, just as blue, red, green, &c., denote recognized forms of colour. Eventually the conception of the series of natural numbers became sufficiently clear to lead to a systematic terminology, and the science of arithmetic was thus rendered possible. But it is only in quite recent times that the notion of number has been submitted to a searching critical analysis: it is, in fact, one of the most characteristic results of modern mathematical research that the term *number* has been made at once more precise and more extensive.

2. *Aggregates* (also called *manifolds* or *sets*).—Let us assume the possibility of constructing or contemplating a permanent system of things such that (1) the system includes all objects to which a certain definite quality belongs; (2) no object without this quality belongs to the system; (3) each object of the system is permanently recognizable as the same thing, and as distinct from all other objects of the system. Such a collection is called an *aggregate*: the separate objects belonging to it are called its *elements*. An aggregate may consist of a single element.

It is further assumed that we can select, by a definite process, one or more elements of any aggregate A at pleasure: these form another aggregate B. If any element of A remains unselected, B is said to be a part of A (in symbols, $B<A$): if not, B is identical with A. Every element of A is a part of A. If $B<A$ and $C<B$, then $C<A$.

When a correspondence can be established between two aggregates A and B in such a way that to every element of A corresponds one and only one element of B, and conversely, A and B are said to be *equivalent*, or to have the same *power* (or *potency*); in symbols, $A \backsim B$. If $A \backsim B$ and $B \backsim C$, then $A \backsim C$. It is possible for an aggregate to be equivalent to a part of itself: the aggregate is then said to be *infinite*. As an example, the aggregates 2, 4, 6, . . . $2n$, &c., and 1, 2, 3, . . . n, &c., are equivalent, but the first is only a part of the second.

3. *Order*.—Suppose that when any two elements a, b of an aggregate A are taken there can be established, by a definite criterion, one or other of two alternative relations, symbolized by $a<b$ and $a>b$, subject to the following conditions:—(1) If $a>b$, then $b<a$, and if $a<b$, then $b>a$; (2) If $a>b$ and $b>c$, then $a>c$. In this case the criterion is said to arrange the aggregate in order. An aggregate which can be arranged in order may be called *ordinable*. An ordinable aggregate may, in general, by the application of different criteria, be arranged in order in a variety of ways. According as $a<b$ or $a>b$ we shall speak of a as anterior or posterior to b. These terms are chosen merely for convenience, and must not be taken to imply any meaning except what is involved in the definitions of the signs $>$ and $<$ for the particular criterion in question. The consideration of a succession of events in time will help to show that the assumptions made are not self-contradictory. An aggregate arranged in order by a definite criterion will be called an *ordered* aggregate. Let a, b be any two elements of an ordered aggregate, and suppose $a<b$. All the elements c (if any) such that $a<c<b$ are said to fall within the interval (a, b). If an element b, posterior to a, can be found so that no element falls within the interval (a, b), then a is said to be *isolated* from all subsequent elements, and b is said to be the element next after a. So if $b'<a$, and no element falls within the interval (b', a), then a is isolated from all preceding elements, and b' is the element next before a. As will be seen presently, for any assigned element a, either, neither, or both of these cases may occur.

An aggregate A is said to be *well-ordered* (or *normally ordered*) when, in addition to being ordered, it has the following properties: (1) A has a first or lowest element a which is anterior to all the rest; (2) if B is any part of A, then B has a first element. It follows from this that every part of a well-ordered aggregate is itself well-ordered. A well-ordered aggregate may or may not have a last element.

Two ordered aggregates A, B are said to be *similar* ($A \underline{\backsim} B$) when a one-one correspondence can be set up between their elements in such a way that if b, b' are the elements of B which correspond to any two elements a, a' of A, then $b>b'$ or $b<b'$ according as $a>a'$ or $a<a'$. For example, $(1, 3, 5, \ldots) \underline{\backsim} (2, 4, 6, \ldots)$, because we can make the even number $2n$ correspond to the odd number $(2n-1)$ and conversely.

Similar ordered aggregates are said to have the same *order-type*. Any definite order-type is said to be the *ordinal number* of every aggregate arranged according to that type. This somewhat vague definition will become clearer as we proceed.

[1] See also NUMERAL.

4. *The Natural Scale.*—Let a be any element of a well-ordered aggregate A. Then all the elements posterior to a form an aggregate A′, which is a part of A and, by definition, has a first element a'. This element a' is different from a, and immediately succeeds it in the order of A. (It may happen, of course, that a' does not exist; in this case a is the last element of A.) Thus in a well-ordered aggregate every element except the last (if there be a last element) is succeeded by a definite next element. The ingenuity of man has developed a symbolism by means of which *every* symbol is associated with a definite next succeeding symbol, and in this way we have a set of visible or audible signs 1, 2, 3, &c. (or their verbal equivalents), representing an aggregate in which (1) there is a definite order, (2) there is a first term, (3) each term has one next following, and consequently there is *no last term*. Counting a set of objects means associating them in order with the first and subsequent members of this conventional aggregate. The process of counting may lead to three diffeient results: (1) the set of objects may be finite in number, so that they are associated with a part of the conventional aggregate which has a last term; (2) the set of objects may have the same power as the conventional aggregate; (3) the set of objects may have a higher power than the conventional aggregate. Examples of (2) and (3) will be found further on. The order-type of 1, 2, 3, &c., and of similar aggregates will be denoted by ω; this is the first and simplest member of a set of transfinite ordinal numbers to be considered later on. Any finite number such as 3 is used ordinally as representing the order-type of 1, 2, 3 or any similar aggregate, and cardinally as representing the power of 1, 2, 3 or any equivalent aggregate. For reasons that will appear, ω is only used in an ordinal sense. The aggregate 1, 2, 3, &c., in any of its written or spoken forms, may be called the natural scale, and denoted by N. It has already been shown that N is infinite: this appears in a more elementary way from the fact that $(1, 2, 3, 4, \ldots) \simeq (2, 3, 4, 5, \ldots)$, where each element of N is made to correspond with the next following. Any aggregate which is equivalent to the natural scale or a part thereof is said to be *countable*.

5. *Arithmetical Operations.*—When the natural scale N has once been obtained it is comparatively easy, although it requires a long process of induction, to define the arithmetical operations of addition, multiplication and involution, as applied to natural numbers. It can be proved that these operations are free from ambiguity and obey certain formal laws of commutation, &c., which will not be discussed here. Each of the three direct operations leads to an inverse problem which cannot be solved except under certain implied conditions. Let a, b denote any two assigned natural numbers: then it is required to find natural numbers, x, y, z such that

$$a=b+x, \quad a=by, \quad a=z^b$$

respectively. The solutions, when they exist, are perfectly definite, and may be denoted by $a-b$, a/b and $\sqrt[b]{a}$; but they are only possible in the first case when $a>b$, in the second when a is a multiple of b, and in the third when a is a perfect bth power. It is found to be possible, by the construction of certain elements, called respectively *negative*, *fractional* and *irrational numbers*, and *zero*, to remove all these restrictions.

6. There are certain properties, common to the aggregates with which we have next to deal, analogous to those possessed by the natural scale, and consequently justifying us in applying the term *number* to any one of their elements. They are stated here, once for all, to avoid repetition; the verification, in each case, will be, for the most part, left to the reader. Each of the aggregates in question (A, suppose) is an ordered aggregate. If α, β are any two elements of A, they may be combined by two definite operations, represented by + and ×, so as to produce two definite elements of A represented by $\alpha+\beta$ and $\alpha\times\beta$ (or $\alpha\beta$); these operations obey the formal laws satisfied by those of addition and multiplication. The aggregate A contains one (and only one) element ι, such that if α is any element of A (ι included), then $\alpha+\iota>\alpha$, and $\alpha\iota=\alpha$. Thus A contains the elements ι, $\iota+\iota$, $\iota+\iota+\iota$, &c., or, as we may write them, ι, 2ι, 3ι, . . . $m\iota$ . . . such that $m\iota+n\iota=(m+n)\iota$ and $m\iota\times n\iota=mn\iota$; also $\iota<2\iota<3\iota$ . . . We may express this by saying that A contains an *image* of the natural scale. The element denoted by ι may be called the *ground element* of A.

7. *Negative Numbers.*—Let any two natural numbers a, b be selected in a definite order a, b (to be distinguished from b, a, in which the order is reversed). In this way we obtain from N an aggregate of symbols (a, b) which we shall call *couples*, or more precisely, if necessary, *polar couples*. This new aggregate may be arranged in order by means of the following rules:—

Two couples (a, b), (a', b') are said to be equal if $a+b'=a'+b$. In other words (a, b), (a', b') are then taken to be equivalent symbols for the same thing.

If $a+b'>a'+b$, we write $(a, b)>(a', b')$; and if $a+b'<a'+b$, we write $(a, b)<(a', b')$.

The rules for the addition and multiplication of couples are:

$$(a, b)+(a', b')=(a+a', b+b')$$
$$(a, b)\times(a', b')=(aa'+bb', ab'+a'b).$$

The aggregate thus defined will be denoted by $\bar{\text{N}}$; it may be called the scale of relative integers.

If ι denotes (2, 1) or any equivalent couple, $(a, b)+\iota=(a+2, b+1)>(a, b)$ and $(a, b)\times\iota=(2a+b, a+2b)=(a, b)$. Hence ι is the ground element of $\bar{\text{N}}$. By definition, $2\iota=\iota+\iota=(4, 2)=(3, 1)$: and hence by induction $m\iota=(m+1, 1)$, where m is any natural integer. Conversely every couple (a, b) in which $a>b$ can be expressed by the symbol $(a-b)\iota$. In the same way, every couple (a, b) in which $b>a$ can be expressed in the form $(b-a)\iota'$, where $\iota'=(1, 2)$.

8. It follows as a formal consequence of the definitions that $\iota+\iota'=(2, 1)+(1, 2)=(3, 3)=(1, 1)$. It is convenient to denote (1, 1) and its equivalent symbols by 0, because

$$(a, b)+(1, 1)=(a+1, b+1)=(a,b)$$
$$(a, b)\times(1, 1)=(a+b, a+b)=(1, 1);$$

hence $\iota+\iota'=0$, and we can represent $\bar{\text{N}}$ by the scheme—

$$\ldots\ 3\iota',\ 2\iota',\ \iota',\ 0,\ \iota,\ 2\iota,\ 3\iota\ \ldots$$

in which each element is obtained from the next before it by the addition of ι. With this notation the rules of operation may be written (m, n, denoting natural numbers)—

$$m\iota+n\iota\ =(m+n)\iota \quad m\iota'+n\iota'=(m+n)\iota'$$
$$m\iota+n\iota'=(m-n)\iota \text{ if } m>n$$
$$=(n-m)\iota' \quad m<n$$
$$m\iota\times n\iota=mn\iota, \quad m\iota'\times n\iota'=mn\iota, \quad m\iota\times n\iota'=mn\iota',$$

with the special rules for zero, that if α is any element of $\bar{\text{N}}$,

$$\alpha+0=\alpha, \quad \alpha\times 0=0.$$

To each element, α, of $\bar{\text{N}}$ corresponds a definite element α' such that $\alpha+\alpha'=0$; if $\alpha=0$, then $\alpha'=0$, but in every other case α, α' are different and may be denoted by $m\iota$, $m\iota'$. The natural number m is called the *absolute value* of $m\iota$ and $m\iota'$.

9. If α, β are any two elements of $\bar{\text{N}}$, the equation $\xi+\beta=\alpha$ is satisfied by putting $\xi=\alpha+\beta'$. Thus the symbol $\alpha-\beta$ is always interpretable as $\alpha+\beta'$, and we may say that within $\bar{\text{N}}$ subtraction is always possible; it is easily proved to be also free from ambiguity. On the other hand, α/β is intelligible only if the absolute value of α is a multiple of the absolute value of β.

The aggregate $\bar{\text{N}}$ has no first element and no last element. At the same time it is countable, as we see, for instance, by associating the elements 0, $a\iota$, $b\iota'$ with the natural numbers 1, $2a$, $2b+1$ respectively, thus—

$$(\text{N})\ 1, 2, 3, 4, 5, 6, \ldots$$
$$(\bar{\text{N}})\ 0, \iota, \iota', 2\iota, 2\iota', 3\iota \ldots$$

It is usual to write $+a$ (or simply a) for $a\iota$ and $-a$ for $a\iota'$; that this should be possible without leading to confusion or ambiguity is certainly remarkable.

10. *Fractional Numbers.*—We will now derive from N a different aggregate of couples $[a, b]$ subject to the following rules:

The symbols $[a, b]$, $[a', b']$, are equivalent if $ab'=a'b$. According as ab' is greater or less than $a'b$ we regard $[a, b]$ as being greater or less than $[a', b']$. The formulae for addition and multiplication are

$$[a, b]+[a', b']=[ab'+a'b, bb']$$
$$[a, b]\times[a', b']=[aa', bb'].$$

All the couples $[a, a]$ are equivalent to [1, 1], and if we denote this by v we have $[a, b]+v=[a+b, b]>[a, b]$, $[a, b]\times v=[a, b]$, so that v is the ground element of the new aggregate.

Again $2v=v+v=(2, 1)$, and by induction $mv=[m, 1]$. Moreover, if a is a multiple of b, say mb, we may denote $[a, b]$ by mv.

11. The new aggregate of couples will be denoted by R. It differs from N and $\overline{\mathrm{N}}$ in one very important respect, namely, that when its elements are arranged in order of magnitude (that is to say, by the rule above given) they are not isolated from each other. In fact if $[a, b]=\alpha$, and $[a', b']=\alpha'$, the element $[a+a', b+b']$ lies between α and α'; hence it follows that between any two different elements of R we can find as many other elements as we please. This property is expressed by saying that R is in *close order* when its elements are arranged in order of magnitude. Strange as it appears at first sight, R is a countable aggregate; a theorem first proved by G. Cantor. To see this, observe that every element of R may be represented by a "reduced" couple $[a, b]$, in which a, b are prime to each other. If $[a, b]$, $[c, d]$ are any two reduced couples, we will agree that $[a, b]$ is anterior to $[c, d]$ if either (1) $a+b<c+d$, or (2) $a+b=c+d$, but $a<c$. This gives a new criterion by which all the elements of R can be arranged in the succession

$$[1, 1], [1, 2], [2, 1], [1, 3], [3, 1,], [1, 4], [2, 3], [3, 2], [4, 1]. \ . \ .$$

which is similar to the natural scale.

The aggregate R, arranged in order of magnitude, agrees with $\overline{\mathrm{N}}$ in having no least and no greatest element; for if α denotes any element $[a, b]$, then $[2a-1, 2b]<\alpha$, while $[2a+1, 2b]>\alpha$.

12. The division of one element of R by another is always possible; for by definition

$$[c, d]\times[ad, bc]=[acd, bcd]=[a, b],$$

and consequently $[a, b]\div[c, d]$ is always interpretable as $[ad, bc]$. As a particular case $[m, 1]\div[n, 1]=[m, n]$, so that every element of R is expressible in one of the forms mv, mv/nv. It is usual to omit the symbol v altogether, and to represent the element $[m, n]$ by m/n, whether m is a multiple of n or not. Moreover, $m/1$ is written m, which may be done without confusion, because $m/1+n/1=(m+n)/1$, and $m/1\times n/1=mn/1$, by the rules given above.

13. Within the aggregate R subtraction is not always practicable; but this limitation may be removed by constructing an aggregate $\overline{\mathrm{R}}$ related to R in the same way as $\overline{\mathrm{N}}$ to N. This may be done in two ways which lead to equivalent results. We may either form symbols of the type (α, β), where α, β denote elements of R, and apply the rules of § 7; or else form symbols of the type $[\alpha, \beta]$, where α, β denote elements of $\overline{\mathrm{N}}$, and apply the rules of §10. The final result is that $\overline{\mathrm{R}}$ contains a zero element, 0, a ground element v, an element v' such that $v+v'=0$, and a set of elements representable by the symbols $(m/n)v$, $(m/n)v'$. In this notation the rules of operation are

$$\frac{m}{n}v+\frac{m'}{n'}v=\left(\frac{mn'+m'n}{nn'}\right)v, \quad \frac{m}{n}v'+\frac{m'}{n'}v'=\left(\frac{mn'+m'n}{nn'}\right)v';$$

$$\frac{m}{n}v+\frac{m'}{n'}v'=\frac{mn'-m'n}{nn'}v, \text{ or } \frac{m'n-mn'}{nn'}v', \text{ as } mn'>\text{or}<m'n;$$

$$\frac{m}{n}v\times\frac{m'}{n'}v=\frac{mm'}{nn'}v=\frac{m}{n}v'\times\frac{m'}{n'}v' \quad \frac{m}{n}v\times\frac{m'}{n'}v'=\frac{mm'}{nn'}v';$$

$$\frac{m}{n}v\div\frac{m'}{n'}v=\frac{mn'}{m'n}v=\frac{m}{n}v'\div\frac{m'}{n'}v', \quad \frac{m}{n}v\div\frac{m'}{n'}v'=\frac{mn'}{m'n}v'=\frac{m}{n}v'\div\frac{m'}{n'}v;$$

$$\alpha-\beta=\alpha+\beta', \text{ where } \beta+\beta'=0;$$
$$\alpha+0=\alpha, \ \alpha\times 0=0.$$

Here α and β denote any two elements of $\overline{\mathrm{R}}$. If $\beta=(m/n)v$, then $\beta'=(m/n)v'$, and if $\beta=(m/n)v'$, then $\beta'=(m/n)v$. If $\beta=0$, then $\beta'=0$.

14. When $\overline{\mathrm{R}}$ is constructed by means of couples taken from $\overline{\mathrm{N}}$, we must put $[m\iota, n\iota]=[m\iota', n\iota']=(m/n)v$, $[m\iota, n\iota']=[m\iota', n\iota]=(m/n)v'$, and $[0, \alpha]=0$, if α is any element of $\overline{\mathrm{N}}$ except 0. The symbols $[0, 0]$ and $[\alpha, 0]$ are inadmissible; the first because it satisfies the definition of equality (§ 10) with every symbol $[\alpha, \beta]$, and is therefore indeterminate; the second because, according to the rule of addition,

$$[\alpha, 0]+[\iota, \iota]=[\alpha\iota, 0]=[\alpha, 0],$$

which is inconsistent with $\xi+v>\xi$.

In the same way, if 0 denotes the zero element of $\overline{\mathrm{R}}$, and ξ any other element, the symbol $0/0$ is indeterminate, and $\xi/0$ inadmissible, because, by the formal rules of operation, $\xi/0+v=\xi/0$, which conflicts with the definition of the ground element v. It is usual to write $+\frac{m}{n}$ $\left(\text{or simply } \frac{m}{n}\right)$ for $\frac{m}{n}v$, and $-\frac{m}{n}$ for $\frac{m}{n}v'$. Each of these elements is said to have the absolute value m/n. The criterion for arranging the elements of $\overline{\mathrm{R}}$ in order of magnitude is that, if ξ, η are any two elements of it, $\xi>\eta$ when $\xi-\eta$ is positive; that is to say, when it can be expressed in the form $(m/n)v$.

15. The aggregate $\overline{\mathrm{R}}$ is very important, because it is the simplest type of a *field of rationality*, or *corpus*. An algebraic corpus is an aggregate, such that its elements are representable by symbols α, β, &c., which can be combined according to the laws of ordinary algebra; every algebraic expression obtained by combining a finite number of symbols, by means of a finite chain of rational operations, being capable of interpretation as representing a definite element of the aggregate, with the single exception that division by zero is inadmissible. Since, by the laws of algebra, $\alpha-\alpha=0$, and $\alpha/\alpha=1$, every algebraic field contains $\overline{\mathrm{R}}$, or, more properly, an aggregate which is an image of $\overline{\mathrm{R}}$.

16. *Irrational Numbers.*—Let α denote any element of $\overline{\mathrm{R}}$; then α and all lesser elements form an aggregate, A say; the remaining elements form another aggregate A', which we shall call complementary to A, and we may write $\overline{\mathrm{R}}=\mathrm{A}+\mathrm{A}'$. Now the essence of this separation of $\overline{\mathrm{R}}$ into the parts A and A' may be expressed without any reference to α as follows:—

I. The aggregates A, A' are complementary; that is, their elements, taken together, make up the whole of $\overline{\mathrm{R}}$.

II. Every element of A is less than every element of A'.

III. The aggregate A' has no least element. (This condition is artificial, but saves a distinction of cases in what follows.)

Every separation $\overline{\mathrm{R}}=\mathrm{A}+\mathrm{A}'$ which satisfies these conditions is called a *cut* (or *section*), and will be denoted by (A, A'). We have seen that every rational number α can be associated with a cut. Conversely, every cut (A, A) in which A has a last element α is perfectly definite, and specifies α without ambiguity. But there are other cuts in which A has no last element. For instance, all the elements (α) of $\overline{\mathrm{R}}$ such that either $\alpha\leqq 0$, or else $\alpha>0$ and $\alpha^2<2$, form an aggregate A, while those for which $\alpha>0$ and $\alpha^2>2$, form the complementary aggregate A'. This separation is a cut in which A has no last element; because if p/q is any positive element of A, the element $(3p+4q)/(2p+3q)$ exceeds p/q, and also belongs to A. *Every cut of this kind is said to define an irrational number.* The justification of this is contained in the following propositions:—

(1) A cut is a definite concept, and the assemblage of cuts is an aggregate according to definition; the generic quality of the aggregate being the separation of $\overline{\mathrm{R}}$ into two complementary parts, without altering the order of its elements.

(2) The aggregate of cuts may be arranged in order by the rule that (A, A') < (B, B') if A is a part of B.

(3) This criterion of arrangement preserves the order of magnitude of all rational numbers.

(4) Cuts may be combined according to the laws of algebra, and, when the cuts so combined are all rational, the results are in agreement with those derived from the rational theory.

As a partial illustration of proposition (4) let (A, A'), (B, B') be any two cuts; and let C' be the aggregate whose elements are obtained by forming all the values of $\alpha'+\beta'$, where α' is *any* element of A' and β' is any element of B'. Then if C is the complement of C', it can be proved that (C, C') is a cut; this is said to be the sum of (A, A') and (B, B'). The difference, product and quotient of two cuts may be defined in a similar way. If $\mathfrak{n}$ denotes the irrational cut chosen above for purposes of illustration, we shall have $\mathfrak{n}^2=(\mathrm{C}, \mathrm{C}')$ where C' comprises all the numbers $\alpha'\beta'$ obtained by multiplying *any* two elements, α', β' which are rational and positive, and such that $\alpha'^2>2$, $\beta'^2>2$. Since $\alpha'^2\beta'^2>4$ it follows that $\alpha'\beta'$ is positive and greater than 2; it can be proved conversely that every rational number which is greater than 2 can be expressed in the form $\alpha'\beta'$. Hence $\mathfrak{n}^2=2$, so that the cut $\mathfrak{n}$ actually gives a real arithmetical meaning to the positive root of the equation $x^2=2$; in other words we may say that n defines the irrational number $\sqrt{2}$. The theory of cuts, in fact, provides a logical basis for the treatment of all finite numerical irrationalities, and enables us to justify all arithmetical operations involving the use of such quantities.

17. Since the aggregate of cuts ($\mathfrak{N}$ say) has an order of magnitude, we may construct cuts in this aggregate. Thus if a is any element of $\mathfrak{N}$, and $\mathfrak{A}$ is the aggregate which consists of a and all anterior elements of $\mathfrak{N}$, we may write $\mathfrak{N}=\mathfrak{A}+\mathfrak{A}'$, and $(\mathfrak{A}, \mathfrak{A}')$ is a cut in which $\mathfrak{A}$ has a last element a. It is a remarkable fact that no other kind of cut in $\mathfrak{N}$ is possible; in other words, *every conceivable cut* in $\mathfrak{N}$ *is defined by one of its own elements.* This is expressed by saying that $\mathfrak{N}$ is a *continuous* aggregate, and $\mathfrak{N}$ itself is referred to *as the numerical continuum* of *real numbers.* The property of continuity must be carefully distinguished from that of close order (§ 11); a continuous aggregate is necessarily in close order, but the converse is not always true. The aggregate $\mathfrak{N}$ is not countable.

18. Another way of treating irrationals is by means of *sequences.* A sequence is an unlimited succession of rational numbers

$$a_1, a_2, a_3 \ . \ . \ . \ a_m, a_{m+1} \ . \ . \ .$$

(in order-type ω) the elements of which can be assigned by a definite rule, such that when any rational number ϵ, however small, has been fixed, it is possible to find an integer m, so that for *all* positive integral values of n the absolute value of $(a_{m+n}-a_m)$ is less than ϵ. Under these conditions the sequence may be taken to represent a definite number, which is, in fact, the limit of a_m when m increases without limit. Every rational number a can be expressed as a sequence in the form $(a, a, a, \ldots)$, but this is only one of an infinite variety of such representations, for instance—

$$1=(\cdot 9, \cdot 99, \cdot 999, \ . \ . \ . \ )=\left(\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \ . \ . \ . \ \frac{2^n-1}{2^n} \ . \ . \ . \right)$$

and so on. The essential thing is that we have a mode of representation which can be applied to rational and irrational numbers alike, and provides a very convenient symbolism to express the results of arithmetical operations. Thus the rules for the sum and product of two sequences are given by the formulae

$$(a_1, a_2, a_3, \ . \ . \ . \ )+(b_1, b_2, b_3, \ . \ . \ . \ )=(a_1+b_1, a_2+b_2, a_3+b_3 \ . \ . \ . \ )$$
$$(a_1, a_2, a_3, \ . \ . \ . \ )\times(b_1, b_2, b_3, \ . \ . \ . \ )=(a_1b_1, a_2b_2, a_3b_3 \ . \ . \ . \ )$$

from which the rules for subtraction and division may be at once inferred. It has been proved that the method of sequences is ultimately equivalent to that of cuts. The advantage of the former lies in its convenient notation, that of the latter in giving a clear definition of an irrational number without having recourse to the notion of a limit.

19. *Complex Numbers.*—If a is an assigned number, rational or irrational, and n a natural number, it can be proved that there is a real number satisfying the equation $x^n=a$, except when n is even and a is negative: in this case the equation is not satisfied by any real number whatever. To remove the difficulty we construct an aggregate of polar couples $\{x, y\}$, where x, y are any two real numbers, and define the addition and multiplication of such couples by the rules

$$\{x, y\}+\{x', y'\}=\{x+x', y+y\};$$
$$\{x, y\}\times\{x', y'\}=\{xx'-yy', xy'+x'y\}.$$

We also agree that $\{x, y\}<\{x', y'\}$, if $x<x'$ or if $x=x'$ and $y<y'$. It follows that the aggregate has the ground element $\{1, 0\}$, which we may denote by σ; and that, if we write τ for the element $\{0, 1\}$,

$$\tau^2=\{-1, 0\}=-\sigma.$$

Whenever m, n are rational, $\{m, n\}=m\sigma+n\tau$, and we are thus justified in writing, if we like, $x\sigma+y\tau$ for $\{x, y\}$ in all circumstances. A further simplification is gained by writing x instead of $x\sigma$, and regarding τ as a symbol which is such that $\tau^2=-1$, but in other respects obeys the ordinary laws of operation. It is usual to write i instead of τ; we thus have an aggregate $\mathfrak{J}$ of complex numbers $x+yi$. In this aggregate, which includes the real continuum as part of itself, not only the four rational operations (excluding division by $\{0, 0\}$, the zero element), but also the extraction of roots, may be effected without any restriction. Moreover (as first proved by Gauss and Cauchy), if $a_0, a_1, \ldots a_n$ are any assigned real or complex numbers, the equation

$$a_0z^n+a_1z^{n-1}+\ldots+a_{n-1}z+a_n=0,$$

is always satisfied by precisely n real or complex values of z, with a proper convention as to multiple roots. Thus any algebraic function of any finite number of elements of $\mathfrak{J}$ is also contained in $\mathfrak{J}$, which is, in this sense, a closed arithmetical field, just as $\mathfrak{N}$ is when we restrict ourselves to rational operations. The power of $\mathfrak{J}$ is the same as that of $\mathfrak{N}$.

20. *Transfinite Numbers.*—The theory of these numbers is quite recent, and mainly due to G. Cantor. The simplest of them, ω, has been already defined (§ 4) as the order-type of the natural scale. Now there is no logical difficulty in constructing a scheme

$$u_1, u_2, u_3 \ . \ . \ . \ | \ v_1,$$

indicating a well-ordered aggregate of type ω immediately followed by a distinct element v_1: for example, we may think of all positive odd integers arranged in ascending order of magnitude and then think of the even number 2. A scheme of this kind is said to be of order-type $(\omega+1)$; and it will be convenient to speak of $(\omega+1)$ as the *index* of the scheme. Similarly we may form arrangements corresponding to the indices

$$\omega+2, \omega+3 \ . \ . \ . \ \omega+n,$$

where n is any positive integer. The scheme

$$u_1, u_2, u_3 \ . \ . \ . \ | \ v_1, v_2, v_3 \ . \ .$$

is associated with $\omega+\omega=2\omega$;

$$u_{11}, u_{12}, u_{13} \ . \ . \ . \ | \ u_{21}, u_{22}, u_{23} \ . \ . \ . \ | \ . \ . \ . \ | \ u_{n1}, u_{n2} \ . \ . \ . \ | \ . \ . \ .$$

with $\omega.\omega$ or ω^2; and so on. Thus we may construct arrangements of aggregates corresponding to any index of the form

$$\phi(\omega)=a\omega^n+b\omega^{n-1}+ \ . \ . \ . \ +k\omega+l,$$

where $n, a, b, \ldots l$ are all positive integers.

We are thus led to the construction of a scheme of symbols—

$$\begin{array}{ll}
\text{I.} & 1, 2, 3, \ . \ . \ . \ n \ . \ . \ . \\
\text{II.} & \left\{\begin{array}{l}
\omega, \omega+1, \ . \ . \ . \ \omega+n, \ . \ . \ . \\
2\omega, 2\omega+1, \ . \ . \ . \ 2\omega+n, \ . \ . \ . \\
\vdots \\
\omega^2, \omega^2+1, \omega^2+2 \ . \ . \ . \ \omega^2+n, \ . \ . \ . \\
\vdots \\
\phi(\omega), \phi(\omega)+1, \ . \ . \ . \ \phi(\omega)+n, \ . \ . \ . \\
\vdots
\end{array}\right. \\
\text{III.} & \left\{\begin{array}{l}
\omega^\omega, \omega^\omega+1, \ . \ . \ . \ \omega^\omega+n, \ . \ . \ . \\
\vdots \\
\omega^{\phi(\omega)}, \omega^{\phi(\omega)}+1, \ . \ . \ . \ \omega^{\phi(\omega)}+n, \ . \ . \ . \\
\vdots
\end{array}\right.
\end{array}$$

The symbols $\phi(\omega)$ form a countable aggregate: so that we may, if we like (and in various ways), arrange the rows of block (II.) in a scheme of type ω: we thus have each element a succeeded in its row by $(a+1)$, and the row containing $\phi(\omega)$ succeeded by a definite next row. The same process may be applied to (III.), and we can form additional blocks (IV.), (V.), &c., with first elements $\omega_4=\omega^{\omega^\omega}$, $\omega_5=\omega^{\omega_4}$, &c. All the symbols in which ω occurs are called *transfinite ordinal numbers.*

21. The index of a finite set is a definite integer however the set may be arranged; we may take this index as also denoting the power of the set, and call it the *number* of things in the set. But the index of an infinite ordinable set depends upon the way in which its elements are arranged; for instance, ind. $(1, 2, 3, \ . \ . \ . \ )=\omega$, but ind. $(1, 3, 5, \ . \ . \ . \ | \ 2, 4, 6, \ . \ . \ . \ )=2\omega$. Or, to take another example, the scheme—

$$\begin{array}{l}
1, 3, 5, \ . \ . \ . \ (2n-1) \ . \ . \ . \\
2, 6, 10, \ . \ . \ . \ 2\,(2n-1) \ . \ . \ . \\
\vdots \quad \vdots \quad \vdots \\
2^m, 2^m.\,3, 2^m.\,5, \ . \ . \ . \ 2^m\,(2n-1) \ . \ . \ . \\
\vdots
\end{array}$$

where each row is supposed to follow the one above it, gives a permutation of $(1, 2, 3, \ . \ . \ . \ )$, by which its index is changed from ω to ω^2. It has been proved that there is a permutation of the natural scale, of which the index is $\phi(\omega)$, any assigned element of (II.); and that, if the index of any ordered aggregate is $\phi(\omega)$, the aggregate is countable. Thus the power of all aggregates which can be associated with indices of the class (II.) is the same as that of the natural scale; this power may be denoted by a. Since a is associated with all aggregates of a particular power, independently of the arrangement of their elements, it is analogous to the integers, 1, 2, 3, &c., when used to denote powers of finite aggregates; for this reason it is called the *least transfinite cardinal number*.

22. There are aggregates which have a power greater than a: for instance, the arithmetical continuum of positive real numbers, the power of which is denoted by c. Another one is the aggregate of all those order-types which (like those in II. above) are the indices of aggregates of power a. The power of this aggregate is denoted by $\aleph_1$. According to Cantor's theory it is the transfinite cardinal number next superior to a, which for the sake of uniformity is also denoted by $\aleph_0$. It has been conjectured that $\aleph_1=c$, but this has neither been verified nor disproved. The discussion of the aleph-numbers is still in a controversial stage (November 1907) and the points in debate cannot be entered upon here.

23. Transfinite numbers, both ordinal and cardinal, may be combined by operations which are so far analogous to those of ordinary arithmetic that it is convenient to denote them by the same symbols. But the laws of operation are not entirely the same; for instance, 2ω and $\omega 2$ have different meanings: the first has been explained, the second is the index of the scheme $(a_1 b_1 \mid a_2 b_2 \mid a_3 b_3 \mid \ldots \mid a_n b_n \mid \ldots)$ or any similar arrangement. Again if n is any positive integer, $na=a^n=a$. It should also be observed that according to Cantor's principles of construction every ordinal number is succeeded by a definite next one; but that there are definite ordinal numbers (*e.g.* ω, ω^2) which have no ordinal immediately preceding them.

24. *Theory of Numbers.*—The theory of numbers is that branch of mathematics which deals with the properties of the natural numbers. As Dirichlet observed long ago, the whole of the subject would be coextensive with mathematical analysis in general; but it is convenient to restrict it to certain fields where the appropriateness of the above definition is fairly obvious. Even so, the domain of the subject is becoming more and more comprehensive, as the methods of analysis become more systematic and more exact.

The first noteworthy classification of the natural numbers is into those which are prime and those which are composite. A prime number is one which is not exactly divisible by any number except itself and 1; all others are composite. The number of primes is infinite (Eucl. *Elem.* ix. 20), and consequently, if n is an assigned number, however large, there is an infinite number (a) of primes greater than n.

If m, n are any two numbers, and $m>n$, we can always find a definite chain of positive integers (q_1, r_1), (q_2, r_2), &c., such that

$$m=q_1 n+r_1,\ \ n=q_2 r_1+r_2,\ \ r_1=q_3 r_2+r_3,\ \ \text{\&c.}$$

with $n>r_1>r_2>r_3\ldots$; the process by which they are calculated will be called *residuation*. Since there is only a finite number of positive integers less than n, the process must terminate with two equalities of the form

$$r_{h-2}=q_h r_{h-1}+r_h,\quad r_{h-1}=q_{h+1}r_h.$$

Hence we infer successively that r_h is a divisor of $r_{h-1}, r_{h-2},\ldots r_1$, and finally of m and n. Also r_h is the greatest common factor of m, n: because any common factor must divide r_1, r_2, and so on down to r_h; and the highest factor of r_h is r_h itself. It will be convenient to write $r_h=\mathrm{dv}\,(m, n)$. If $r_h=1$, the numbers m, n are said to be *prime to each other*, or *co-primes*.

25. The foregoing theorem of residuation is of the greatest importance; with the help of it we can prove three other fundamental propositions, namely:—

(1) If m, n are any two natural numbers, we can always find two other natural numbers x, y such that

$$\mathrm{dv}(m,n)=xm-yn.$$

(2) If m, n are prime to each other, and p is a prime factor of mn, then p must be a factor of either m or n.

(3) Every number may be uniquely expressed as a product of prime factors.

Hence if $n=p^\alpha q^\beta r^\gamma\ldots$ is the representation of any number n as the product of powers of different primes, the divisors of n are the terms of the product
$(1+p+p^2+\ldots+p^\alpha)\quad(1+q+\ldots+q^\beta)\quad(1+r+\ldots+r^\gamma)\ldots$
their number is $(\alpha+1)\ (\beta+1)\ (\gamma+1)\ldots$; and their sum is $\Pi(p^{\alpha+1}-1)\div\Pi(p-1)$. This includes 1 and n among the divisors of n.

26. *Totients.*—By the totient of n, which is denoted, after Euler, by $\phi(n)$, we mean the number of integers prime to n, and not exceeding n. If $n=p^a$, the numbers not exceeding n and *not* prime to it are $p, 2p, \ldots (p^a-p), p^a$ of which the number is p^{a-1}: hence $\phi(p^a)=p^a-p^{a-1}$. If m, n are prime to each other, $\phi(mn)=\phi(m)\phi(n)$; and hence for the general case, if $n=p^a q^\beta r^\gamma\ldots, \phi(n)=\Pi p^{a-1}(p-1)$, where the product applies to all the different prime factors of n. If d_1, d_2, &c., are the different divisors of n,

$$\phi(d_1)+\phi(d_2)+\ldots=n.$$

For example, $15=\phi(15)+\phi(5)+\phi(3)+\phi(1)=8+4+2+1$.

27. *Residues and congruences.*—It will now be convenient to include in the term "number" both zero and negative integers. Two numbers a, b are said to be *congruent with respect to the modulus* m, when $(a-b)$ is divisible by m. This is expressed by the notation $a\equiv b \pmod{m}$, which was invented by Gauss. The fundamental theorems relating to congruences are

If $\quad a\equiv b$ and $c\equiv d \pmod{m}$, then $a\pm c\equiv b\pm d$, and $ab\equiv cd$.
If $\quad ha\equiv hb \pmod{m}$ then $a\equiv b \pmod{m/d}$, where $d=\mathrm{dv}(h, m)$.

Thus the theory of congruences is very nearly, but not quite, similar to that of algebraic equations. With respect to a given modulus m the scale of relative integers may be distributed into m classes, any two elements of each class being congruent with respect to m. Among these will be $\phi(m)$ classes containing numbers prime to m. By taking any one number from each class we obtain a *complete system of residues* to the modulus m. Supposing (as we shall always do) that m is positive, the numbers $0, 1, 2, \ldots (m-1)$ form a system of least positive residues; according as m is odd or even, $0, \pm1, \pm2, \ldots \pm\frac{1}{2}(m-1)$, or $0, \pm1, \pm2, \ldots \pm\frac{1}{2}(m-2), \frac{1}{2}m$ form a system of absolutely least residues.

28. *The Theorems of Fermat and Wilson.*—Let $r_1, r_2, \ldots r_t$ where $t=\phi(m)$, be a complete set of residues prime to the modulus m. Then if x is any number prime to m, the residues $xr_1, xr_2, \ldots xr_t$ also form a complete set prime to m (§ 27). Consequently $xr_1 \cdot xr_2 \ldots xr_t\equiv r_1 r_2 \ldots r_t$, and dividing by $r_1 r_2\ldots r_t$, which is prime to the modulus, we infer that

$$x^{\phi(m)}\equiv 1 \pmod{m}.$$

which is the general statement of Fermat's theorem. If m is a prime p, it becomes $x^{p-1}\equiv 1 \pmod{p}$.

For a prime modulus p there will be among the set $x, 2x, 3x, \ldots (p-1)x$ just one and no more that is congruent to 1: let this be xy. If $y\equiv x$, we must have $x^2-1=(x-1)\ (x+1)\equiv 0$, and hence $x\equiv\pm 1$: consequently the residues $2, 3, 4, \ldots (p-2)$ can be arranged in $\frac{1}{2}(p-3)$ pairs (x, y) such that $xy\equiv 1$. Multiplying them all together, we conclude that $2.3.4\ldots(p-2)\equiv 1$ and hence, since $1.(p-1)\equiv -1$,

$$(p-1)!\equiv -1 \pmod{p},$$

which is Wilson's theorem. It may be generalized, like that of Fermat, but the result is not very interesting. If m is composite $(m-1)!+1$ cannot be a multiple of m: because m will have a prime factor p which is less than m, so that $(m-1)!\equiv 0 \pmod{p}$. Hence Wilson's theorem is invertible: but it does not supply any practical test to decide whether a given number is prime.

29. *Exponents, Primitive Roots, Indices.*—Let p denote an odd prime, and x any number prime to p. Among the powers $x, x^2, x^3, \ldots x^{p-1}$ there is certainly one, namely x^{p-1}, which $\equiv 1 \pmod{p}$; let x^e be the lowest power of x such that $x^e\equiv 1$. Then e is said to be the exponent to which x appertains $(\bmod\ p)$: it is always a factor of $(p-1)$ and can only be 1 when $x\equiv 1$. The residues x for which $e=p-1$ are said to be *primitive roots of* p. They always exist, their number is $\phi(p-1)$, and they can be found by a methodical, though tedious, process of exhaustion. If g is any one of them, the complete set may be represented by $g, g^a, g^b, \ldots$ &c. where a, b, &c., are the numbers less than $(p-1)$ and prime to it, other than 1. Every number x which is prime to p is congruent, mod p, to g^i, where i is one of the numbers $1, 2, 3, \ldots (p-1)$; this number i is called *the index of x to the base* g. Indices are analogous to logarithms: thus

$$\mathrm{ind}_g(xy)\equiv\mathrm{ind}_g x+\mathrm{ind}_g y.\ \mathrm{ind}_g(x^h)\equiv h\ \mathrm{ind}_g x\ (\bmod\ \overline{p-1}).$$

Consequently tables of primitive roots and indices for different primes are of great value for arithmetical purposes. Jacobi's *Canon Arithmeticus* gives a primitive root, and a table of numbers and indices for all primes less than 1000.

For moduli of the forms $2p$, p^m, $2p^m$ there is an analogous theory (and also for 2 and 4); but for a composite modulus of other forms there are no primitive roots, and the nearest analogy is the representation of prime residues in the form $\alpha^x \beta^y \chi^z \ldots$, where $\alpha, \beta, \gamma, \ldots$ are selected prime residues, and $x, y, z, \ldots$ are indices of restricted range. For instance, all residues prime to 48 can be exhibited in the form $5^x\, 7^y\, 13^z$, where $x=0, 1, 2, 3$; $y=0, 1$; $z=0, 1$; the total number of distinct residues being $4.2.2=16=\phi(48)$, as it should be.

30. *Linear Congruences.*—The congruence $a'x\equiv b' \pmod{m'}$ has no solution unless $\mathrm{dv}(a', m')$ is a factor of b'. If this condition is satisfied, we may replace the given congruence by the equivalent one $ax\equiv b \pmod{m}$, where a is prime to b as well as to m. By residuation (§§ 24, 25) we can find integers h, k such that $ah-mk=1$, and thence obtain $x\equiv bh \pmod{m}$ as the complete solution of the given congruence. To the modulus m' there are m'/m incongruent solutions. For example, $12x\equiv 30 \pmod{21}$ reduces to $2x\equiv 5 \pmod{7}$ whence $x\equiv 6 \pmod{7}\equiv 6, 13, 20 \pmod{21}$. There is a theory of simultaneous

linear congruences in any number of variables, first developed with precision by Smith. In any particular case, it is best to replace as many as possible of the given congruences by an equivalent set obtained by successively eliminating the variables $x, y, z, \ldots$ in order. An important problem is to find a number which has given residues with respect to a given set of moduli. When possible, the solution is of the form $x \equiv a \pmod{m}$, where m is the least common multiple of the moduli. Supposing that p is a prime, and that we have a corresponding table of indices, the solution of $ax \equiv b \pmod{p}$ can be found by observing that ind $x \equiv$ ind b–ind a (mod $\overline{p-1}$).

31. *Quadratic Residues. Law of Reciprocity.*—To an odd prime modulus p, the numbers $1, 4, 9, \ldots (p-1)^2$ are congruent to $\frac{1}{2}(p-1)$ residues only, because $(p-x)^2 = x^2$. Thus for $p=5$, we have $1, 4, 9, 16 \equiv 1, 4, 4, 1$ respectively. There are therefore $\frac{1}{2}(p-1)$ quadratic residues and $\frac{1}{2}(p-1)$ quadratic non-residues prime to p; and there is a corresponding division of incongruent classes of integers with respect to p. The product of two residues or of two non-residues is a residue; that of a residue and a non-residue is a non-residue; and taking any primitive root as base the index of any number is even or odd according as the number is a residue or a non-residue. Gauss writes $a\mathrm{R}p$, $a\mathrm{N}p$ to denote that a is a residue or non-residue of p respectively.

Given a table of indices, the solution of $x^2 \equiv a \pmod{p}$ when possible, is found from 2ind $x \equiv$ ind a (mod $\overline{p-1}$), and the result may be written in the form $x \equiv \pm r \pmod{p}$. But it is important to discuss the congruence $x^2 \equiv a$ without assuming that we have a table of indices. It is sufficient to consider the case $x^2 \equiv q \pmod{p}$, where q is a positive prime less than p; and the question arises whether the quadratic character of q with respect to p can be deduced from that of p with respect to q. The answer is contained in the following theorem, which is called *the law of quadratic reciprocity* (for real positive odd primes): if p, q are each or one of them of the form $4n+1$, then p, q are each of them a residue, or each a non-residue of the other; but if p, q are each of the form $4n+3$, then according as p is a residue or non-residue of q we have q a non-residue or a residue of p.

Legendre introduced a symbol $\left(\frac{m}{q}\right)$ which denotes $+1$ or -1 according as $m\mathrm{R}q$ or $m\mathrm{N}q$ (q being a positive odd prime and m any number prime to q); with its help we may express the law of reciprocity in the form

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

This theorem was first stated by Legendre, who only partly proved it; the first complete proof, by induction, was published by Gauss, who also discovered five (or six) other more or less independent proofs of it. Many others have since been invented.

There are two supplementary theorems relating to -1 and 2 respectively, which may be expressed in the form

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}. \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)},$$

where p is any positive odd prime.

It follows from the definition that

$$\left(\frac{p_1{}^{\alpha} p_2{}^{\beta} p_3{}^{\gamma} \ldots}{q}\right) = \left(\frac{p_1}{q}\right)^{\alpha} \left(\frac{p_2}{q}\right)^{\beta} \left(\frac{p_3}{q}\right)^{\gamma} \ldots$$

and that $\left(\frac{m}{q}\right) = \left(\frac{m'}{q}\right)$, if $m = m' \pmod{q}$. As a simple application of the law of reciprocity, let it be required to find the quadratic character of 11 with respect to 1907. We have

$$\left(\frac{11}{1907}\right) = -\left(\frac{1907}{11}\right) = -\left(\frac{6}{11}\right) = 1$$

because 6N11. Hence 11R1907.

Legendre's symbol was extended by Jacobi in the following manner. Let P be any positive odd number, and let p, p', p'', &c. be its (equal or unequal) prime factors, so that $\mathrm{P} = pp'p'' \ldots$. Then if Q is any number prime to P, we have a generalized symbol defined by

$$\left(\frac{\mathrm{Q}}{\mathrm{P}}\right) = \left(\frac{\mathrm{Q}}{p}\right)\left(\frac{\mathrm{Q}}{p'}\right)\left(\frac{\mathrm{Q}}{p''}\right) \ldots$$

This symbol obeys the law that, if Q is odd and positive,

$$\left(\frac{\mathrm{P}}{\mathrm{Q}}\right)\left(\frac{\mathrm{Q}}{\mathrm{P}}\right) = (-1)^{\frac{1}{4}(\mathrm{P}-1)(\mathrm{Q}-1)},$$

with the supplementary laws

$$\left(\frac{-1}{\mathrm{P}}\right) = (-1)^{\frac{1}{2}(\mathrm{P}-1)}, \quad \left(\frac{2}{\mathrm{P}}\right) = (-1)^{\frac{1}{8}(\mathrm{P}^2-1)}.$$

It is found convenient to add the conventions that

$$\left(\frac{\mathrm{Q}}{-\mathrm{P}}\right) = \left(\frac{\mathrm{Q}}{\mathrm{P}}\right)$$

when Q and P are both odd; and that the value of the symbol is 0 when P, Q are not co-primes.

In order that the congruence $x^2 \equiv a \pmod{m}$ may have a solution it is necessary and sufficient that a be a residue of each distinct prime factor of m If these conditions are all satisfied, and $m = 2^{\kappa} p^{\lambda} q^{\mu} \ldots$, where p, q, &c., are the distinct odd prime factors of m, being t in all, the number of incongruent solutions of the given congruence is 2^t, 2^{t+1} or 2^{t+2}, according as $\kappa < 2$, $\kappa = 2$, or $\kappa > 2$ respectively. The actual solutions are best found by a process of exhaustion. It should be observed that $\left(\frac{a}{m}\right) = 1$ is a necessary but not a sufficient condition for the possibility of the congruence.

32. *Quadratic forms.*—It will be observed that the solution of the linear congruence $ax \equiv b \pmod{m}$ leads to all the representations of b in the form $ax+my$, where x, y are integers. Many of the earliest researches in the theory of numbers deal with particular cases of the problem: given four numbers m, a, b, c, it is required to find all the integers x, y (if there be any) which satisfy the equation $ax^2+bxy+cy^2=m$. Fermat, for instance, discovered that every positive prime of the form $4n+1$ is uniquely expressible as the sum of two squares. There is a corresponding arithmetical theory for forms of any degree and any number of variables; only those of linear forms and binary quadratics are in any sense complete, as the difficulty of the problem increases very rapidly with the increase of the degree of the form considered or of the number of variables contained in it.

The form $ax^2+bxy+cy^2$ will be denoted by $(a, b, c)(x, y)^2$ or more simply by (a, b, c) when there is no need of specifying the variables. If k is the greatest common factor of a, b, c, we may write $(a, b, c) = k(a', b', c')$ where (a', b', c') is a *primitive* form, that is, one for which dv $(a', b', c') = 1$. The other form is then said to be derived from (a', b', c') and to have a divisor k. For the present we shall concern ourselves only with primitive forms. Writing $\mathrm{D} = b^2-4ac$, the invariant D is called the *determinant* of (a, b, c), and there is a first classification of forms into *definite* forms for which D is negative, and *indefinite* forms for which D is positive. The case $\mathrm{D}=0$ or a positive square is rejected, because in that case the form breaks up into the product of two linear factors. It will be observed that $\mathrm{D} \equiv 0, 1 \pmod{4}$ according as b is even or odd; and that if k^2 is any odd square factor of D there will be forms of determinant D and divisor k.

If we write $x' = \alpha x + \beta y$, $y' = \gamma x + \delta y$, we have identically

$$(a, b, c)(x', y')^2 = (a', b', c')(x, y)^2$$

where

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

Hence also

$$\mathrm{D}' = b'^2 - 4a'c' = (\alpha\delta-\beta\gamma)^2(b^2-4ac) = (\alpha\delta-\beta\gamma)^2\,\mathrm{D}.$$

Supposing that $\alpha, \beta, \gamma, \delta$ are integers such that $\alpha\delta - \beta\gamma = n$, a number different from zero, (a, b, c) is said to be transformed into (a', b', c') by the substitution $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ of the nth order. If $n^2=1$, the two forms are said to be *equivalent*, and the equivalence is said to be *proper* or *improper* according as $n=1$ or $n=-1$. In the case of equivalence, not only are x', y' integers wherever x, y are so, but conversely; hence every number representable by (a, b, c) is representable by (a', b', c') and conversely. For the present we shall deal with proper equivalence only and write $f \sim f'$ to indicate that the forms f, f' are properly equivalent. Equivalent forms have the same divisor. A complete set of equivalent forms is said to form a *class*; classes of the same divisor are said to form an *order*, and of these the most important is the *principal* order, which consists of the primitive classes. It is a fundamental theorem that for a given determinant the number of classes is finite; this is proved by showing that every class must contain one at least of a certain finite number of so-called *reduced* forms, which can be found by definite rules of calculation.

33. *Method of Reduction.*—This differs according as D is positive or negative, and will require some preliminary lemmas. Suppose that any complex quantity $z = x+yi$ is represented in the usual way by a point (x, y) referred to rectangular axes. Then by plotting off all the points corresponding to $(\alpha z+\beta) / (\gamma z+\delta)$, we obtain a complete set of properly equivalent points. These all lie on the same side of the axis of x, and there is precisely one of them and no more which satisfies the conditions: (i.) that it is not outside the area which is bounded by the lines $2x = \pm 1$; (ii.) that it is not inside the circle $x^2+y^2=1$; (iii.) that it is not on the line $2x=1$, or on the arcs of the circle $x^2+y^2=1$ intercepted by $2x=1$ and $x=0$. This point will be called the *reduced* point equivalent to z. In the positive half-plane $(y>0)$ the aggregate of all reduced points occupies the interior and half the boundary of an area which will be called the *fundamental triangle*, because the areas equivalent to it, and finite, are all triangles bounded by circular arcs, and having angles $\frac{1}{3}\pi$, $\frac{1}{3}\pi$, 0 and the fundamental triangle may be considered as a special case when one vertex goes to infinity. The aggregate of equivalent triangles forms a kind of mosaic which fills up the whole of the positive half-plane. It will be convenient to denote the fundamental triangle (with its half-boundary, for which $x<0$) by ∇; for a reason which will appear later, the set of equivalent triangles will be said to make up the *modular dissection* of the positive half-plane.

Now let $f' = (a', b', c')$ be any definite form with a' positive and determinant $-\Delta$. The root of $a'z^2+b'z+c'=0$ which is represented by a point in the positive half-plane is

$$\omega = \frac{-b'+i\sqrt{\Delta}}{2a'},$$

and this is a reduced point if either

$$\begin{aligned} &\text{(i.)} \quad b' < a' < c' \\ &\text{(ii.)} \quad b' = a', \ a' \overline{\overline{<}} c' \\ &\text{(iii.)} \ a' = c', \ 0 < b' \overline{\overline{<}} a'. \end{aligned}$$

Cases (ii.) and (iii.) only occur when the representative point is on the boundary of ∇. A form whose representative point is reduced is said to be a reduced form. It follows from the geometrical theory that every form is equivalent to a reduced form, and that there are as many distinct classes of positive forms of determinant $-\Delta$ as there are reduced forms. The total number of reduced forms is limited, because in case (i.) we have $\Delta = 4ac - b^2 > 3b^2$, so that $b < \sqrt{\tfrac{1}{3}\Delta}$, while $4a^2 < 4ac < \Delta + b^2 < \tfrac{4}{3}\Delta$; in case (ii.) $\Delta = 4ac - a^2 > 3a^2$, or else $a = b = c = \sqrt{\tfrac{1}{3}\Delta}$; in case (iii.) $\Delta = 4a^2 - b^2 > 3b^2, 4a^2 = \Delta + b^2 < \tfrac{4}{3}\Delta$, or else $a = b = c = \sqrt{\tfrac{1}{3}\Delta}$. With the help of these inequalities a complete set of reduced forms can be found by trial, and the number of classes determined. The latter cannot exceed $\tfrac{1}{3}\Delta$; it is in general much less.

With an indefinite form (a, b, c) we may associate the representative circle

$$a(x^2+y^2)+bx+c=0,$$

which cuts the axis of x in two real points. The form is said to be reduced if this circle cuts ∇; the condition for this is $a(a \pm \tfrac{1}{2}b + c) < 0$, which can be expressed in the form $3a^2 + (a \pm b)^2 < \text{D}$, and it is hence clear that the absolute values of a, b, and therefore of c, are limited. As before, there are a limited number of reduced forms, but they are not all non-equivalent. In fact they arrange themselves, according to a law which is not very difficult to discover, in cycles or *periods*, each of which is associated with a particular class. The main result is the same as before: that the number of classes is finite, and that for each class we can find a representative form by a finite process of calculation.

34. *Problem of Representation.*—It is required to find out whether a given number m' can be represented by the given form (a', b', c'). One condition is clearly that the divisor of the form must be a factor of m'. Suppose this is the case; and let m, (a, b, c) be the quotients of m' and (a', b', c') be the divisor in question. Then we have now to discover whether m can be represented by the primitive form (a, b, c). First of all we will consider proper representations

$$m = (a, b, c)\ (\alpha, \gamma)^2$$

where α, γ are co-primes. Determine integers β, δ such that $\alpha\delta - \beta\gamma = 1$, and apply to (a, b, c) the substitution $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$; the new form will be (m, n, l), where

$$n^2 - 4ml = \text{D} = b^2 - 4ac.$$

Consequently $n^2 = \text{D} \pmod{4m}$, and D must be a quadratic residue of m. Unless this condition is satisfied, there is no proper representation of m by any form of determinant D. Suppose, however, that $n^2 = \text{D} \pmod{4m}$ is soluble and that n_1, n_2, &c. are its roots. Taking any one of these, say n_i, we can find out whether (m, n_i, l_i) and (a, b, c) are equivalent; if they are, there is a substitution $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ which converts the latter into the former, and then $m = a\alpha^2 + b\alpha\gamma + c\gamma^2$. As to derived representations, if $m = (a, b, c)\ (tx, ty)^2$, then m must have the square factor t^2, and $m/t^2 = (a, b, c)\ (x, y)^2$; hence everything may be made to depend on proper representation by primitive forms.

35. *Automorphs. The Pellian Equation.*—A primitive form (a, b, c) is, by definition, equivalent to itself; but it may be so in more ways than one. In order that (a, b, c) may be transformed into itself by the substitution $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$, it is necessary and sufficient that

$$\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} = \begin{pmatrix} \tfrac{1}{2}(t+bu), & -cu \\ au, & \tfrac{1}{2}(t-bu) \end{pmatrix}$$

where (t, u) is an integral solution of

$$t^2 - \text{D}u^2 = 4.$$

If D is negative and $-\text{D} > 4$, the only solutions are $t = \pm 2, u = 0$; $\text{D} = -3$ gives $(\pm 2, 0)$, $(\pm 1, \pm 1)$; $\text{D} = -4$ gives $(\pm 2, 0)$, $(0, \pm 1)$. On the other hand, if $\text{D} > 0$ the number of solutions is infinite, and if (t_1, u_1) is the solution for which t, u have their least positive values, all the other positive solutions may be found from

$$\frac{t_n + u_n\sqrt{\text{D}}}{2} = \left(\frac{t_1 + u_1\sqrt{\text{D}}}{2}\right)^n (n = 2, 3, 4 \ldots).$$

The substitutions by which (a, b, c) is transformed into itself are called its *automorphs*. In the case when $\text{D} = 0 \pmod 4$ we have $t = 2\text{T}$, $u = 2\text{U}$, $\text{D} = 4\text{N}$, and (T, U) any solution of

$$\text{T}^2 - \text{NU}^2 = 1.$$

This is usually called the Pellian equation, though it should properly be associated with Fermat, who first perceived its importance. The minimum solution can be found by converting $\sqrt{\text{N}}$ into a periodic continued fraction.

The form (a, b, c) may be improperly equivalent to itself; in this case all its improper automorphs can be expressed in the form

$$\begin{pmatrix} \lambda & , (\kappa + b\lambda)/2a \\ (\kappa - b\lambda)/2c, & -\lambda \end{pmatrix}$$

where $\kappa^2 - \text{D}\lambda^2 = 4ac$. In particular, if $b \equiv 0 \pmod a$ the form (a, b, c) is improperly equivalent to itself. A form improperly equivalent to itself is said to be *ambiguous*.

36. *Characters of a form or class. Genera.*—Let (a, b, c) be any primitive form; we have seen above (§ 32) that if $\alpha, \beta, \gamma, \delta$ are any integers

$$4(a\alpha^2 + b\alpha\gamma + c\gamma^2)(a\beta^2 + b\beta\delta + c\delta^2) = b'^2 - (\alpha\delta - \beta\gamma)^2\text{D}$$

where $b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$. Now the expressions in brackets on the left hand may denote any two numbers m, n representable by the form (a, b, c); the formula shows that $4mn$ is a residue of D, and hence mn is a residue of every odd prime factor of D, and if p is any such factor the symbols $\left(\frac{m}{p}\right)$ and $\left(\frac{n}{p}\right)$ will have the same value. Putting $(a, b, c) = f$, this common value is denoted by $\left(\frac{f}{p}\right)$ and called a *quadratic character* (or simply character) of f with respect to p. Since a is representable by f $(x = 1, y = 0)$ the value $\left(\frac{f}{p}\right)$ is the same as $\left(\frac{a}{p}\right)$. For example, if $\text{D} = -140$, the scheme of characters for the six reduced primitive forms, and therefore for the classes they represent, is

	$\left(\frac{f}{5}\right)$	$\left(\frac{f}{7}\right)$
(1, 0, 35)	+	+
(4, ±2, 9)		
(5, 0, 7)	−	−
(3, ±2, 12)		

In certain cases there are supplementary characters of the type $\left(\frac{-1}{f}\right)$ and $\left(\frac{2}{f}\right)$, and the characters $\left(\frac{f}{p}\right)$ are discriminated according as an odd or even power of p is contained in D; but in every case there are certain combinations of characters (in number one-half of all possible combinations) which form the *total characters* of actually existing classes. Classes which have the same total character are said to belong to the same *genus*. Each genus of the same order contains the same number of classes.

For any determinant D we have a principal primitive class for which all the characters are +; this is represented by the principal form $(1, 0, -n)$ or $(1, 1, -n)$ according as D is of the form $4n$ or $4n+1$. The corresponding genus is called the principal genus. Thus, whea $\text{D} = -140$, it appears from the table above that in the primitive order there are two genera, each containing three classes; and the non-existent total characters are + − and − +.

37. *Composition.*—Considering X, Y as given lineo-linear functions of (x, y), (x', y') defined by the equations

$$\begin{aligned} \text{X} &= p_0xx' + p_1xy' + p_2x'y + p_3yy' \\ \text{Y} &= q_0xx' + q_1xy' + q_2x'y + q_3yy' \end{aligned}$$

we may have identically, in x, y, x', y',

$$(\text{A, B, C})\ (\text{X, Y})^2 = (a, b, c)\ (x, y)^2 \times (a', b', c')\ (x', y')^2$$

and, this being so, the form (A, B, C) is said to be compounded of the two forms (a, b, c), (a', b', c'), the order of composition being indifferent. In order that two forms may admit of composition into a third, it is necessary and sufficient that their determinants be in the ratio of two squares. The most important case is that of two primitive forms ϕ, χ of the same determinant; these can be compounded into a form denoted by $\phi\chi$ or $\chi\phi$ which is also primitive and of the same determinant as ϕ or χ. If A, B, C are the classes to which ϕ, χ, $\phi\chi$ respectively belong, then any form of A compounded with any form of B gives rise to a form belonging to C. For this reason we write $\text{C} = \text{AB} = \text{BA}$, and speak of the multiplication or composition of classes. The principal class is usually denoted by 1, because when compounded with any other class A it gives this same class A.

The total number of primitive classes being finite, h, say, the series A, A^2, A^3, &c., must be recurring, and there will be a least exponent e such that $\text{A}^e = 1$. This exponent is a factor of h, so that every class satisfies $\text{A}^h = 1$. Composition is associative as well as commutative, that is to say, $(\text{AB})\text{C} = \text{A}(\text{BC})$; hence the symbols $\text{A}_1, \text{A}_2, \ldots \text{A}_h$ for the h different classes define an Abelian group (see GROUPS) of order h, which is representable by one or more base-classes $\text{B}_1, \text{B}_2, \ldots \text{B}_i$ in such a way that each class A is enumerated once and only once by putting

$$\text{A} = \text{B}_1{}^x\text{B}_2{}^y \ldots \text{B}_i{}^z \qquad (x \leq m, y \leq n, \ldots z \leq p)$$

with $mn \ldots p = h$, and $\text{B}_1{}^m = \text{B}_2{}^n = \ldots = \text{B}_i{}^p = 1$. Moreover, the bases may be so chosen that m is a multiple of n, n of the next corresponding index, and so on. The same thing may be said with regard to the symbols for the classes contained in the principal genus, because two forms of that genus compound into one of the same kind. If this latter group is cyclical, that is, if all the classes of the principal genus can be represented in the form 1, A, $A^2, \dots A^{\nu-1}$, the determinant D is said to be *regular*; if not, the determinant is irregular. It has been proved that certain specified classes of determinants are always irregular; but no complete criterion has been found, other than working out the whole set of primitive classes, and determining the group of the principal genus, for deciding whether a given determinant is irregular or not.

If A, B are any two classes, the total character of AB is found by compounding the characters of A and B. In particular, the class A^2, which is called the duplicate of A, always belongs to the principal genus. Gauss proved, conversely, that every class in the principal genus may be expressed as the duplicate of a class. An ambiguous class satisfies $A^2=1$, that is, its duplicate is the principal class; and the converse of this is true. Hence if $B_1, B_2, \dots B_i$ are the base-classes for the whole composition-group, and $A=B_1^x B_2^y \dots B_i^s$ (as above) $A^2=1$, if $2x=0$ or m, $2y=0$ or n, &c.; hence the number of ambiguous classes is 2^i. As an example, when $D=-1460$, there are four ambiguous classes, represented by

$$(1, 0, 365), (2, 2, 183), (5, 0, 73), (10, 10, 39);$$

hence the composition-group must be dibasic, and in fact, if we put B_1, B_2 for the classes represented by (11, 6, 34) and (2, 2, 183), we have $B_1^{10}=B_2^2=1$ and the 20 primitive classes are given by $B_1^x B_2^y (x \leqq 10,\ y \leqq 2)$. In this case the determinant is regular and the classes in the principal genus are 1, B_1^2, B_1^4, B_1^6, B_1^8.

38. On account of its historical interest, we may briefly consider the form x^2+y^2, for which $D=-4$. If p is an odd prime of the form $4n+1$, the congruence $m^2 \equiv -4 \pmod{4p}$ is soluble (§ 31); let one of its roots be m, and $m^2+4=4lp$. Then (p, m, l) is of determinant -4, and, since there is only one primitive class for this determinant, we must have $(p, m. l) \sim (1, 0, 1)$. By known rules we can actually find a substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ which converts the first form into the second; this being so, $\begin{pmatrix}\delta, & -\beta \\ -\gamma, & \alpha\end{pmatrix}$ will transform the second into the first, and we shall have $p=\gamma^2+\delta^2$, a representation of p as the sum of two squares. This is unique, except that we may put $p=(\pm\gamma)^2+(\pm\delta)^2$. We also have $2=1^2+1^2$ while no prime $4n+3$ admits of such a representation.

The theory of composition for this determinant is expressed by the identity $(x^2+y^2)(x'^2+y'^2)=(xx' \pm yy')^2+(xy' \mp yx')^2$; and by repeated application of this, and the previous theorem, we can show that if $N=2^a p^b q^c \dots$, where $p, q, \dots$ are odd primes of the form $4n+1$, we can find solutions of $N=x^2+y^2$, and indeed *distinct* solutions. For instance $65=1^2+8^2=4^2+7^2$, and conversely two distinct representations $N=x^2+y^2=u^2+v^2$ lead to the conclusion that N is composite. This is a simple example of the application of the theory of forms to the difficult problem of deciding whether a given large number is prime or composite; an application first indicated by Gauss, though, in the present simple case, probably known to Fermat.

39. *Number of classes. Class-number Relations.*—It appears from Gauss's posthumous papers that he solved the very difficult problem of finding a formula for $h(D)$, the number of properly primitive classes for the determinant D. The first published solution, however, was that of P. G. L. Dirichlet; it depends on the consideration of series of the form $\Sigma(ax^2+bxy+cy^2)^{-1-s}$ where s is a positive quantity, ultimately made very small. L. Kronecker has shown the connexion of Dirichlet's results with the theory of elliptic functions, and obtained more comprehensive formulae by taking (a, b, c) as the standard type of a quadratic form, whereas Gauss, Dirichlet, and most of their successors, took $(a, 2b, c)$ as the standard, calling (b^2-ac) its determinant. As a sample of the kind of formulae that are obtained, let p be a prime of the form $4n+3$; then

$$h(-4p)=\Sigma\alpha-\Sigma\beta, \quad h(4p)\log(t+u\sqrt{p})=\log\Pi\left(\tan\frac{b\pi}{4p}\right)$$

where in the first formula $\Sigma\alpha$ means the sum of all quadratic residues of p contained in the series $1, 2, 3, \dots \frac{1}{2}(p\sim 1)$ and $\Sigma\beta$ is the sum of the remaining non-residues; while in the second formula (t, u) is the least positive solution of $t^2-pu^2=1$, and the product extends to all values of b in the set $1, 3, 5, \dots (4p-1)$ of which p is a non-residue. The remarkable fact will be noticed that the second formula gives a solution of the Pellian equation in a trigonometrical form.

Kronecker was the first to discover, in connexion with the complex multiplication of elliptic functions, the simplest instances of a very curious group of arithmetical formulae involving sums of class-numbers and other arithmetical functions; the theory of these relations has been greatly extended by A. Hurwitz. The simplest of all these theorems may be stated as follows. Let H (Δ) represent the number of classes for the determinant $-\Delta$, with the convention that $\frac{1}{2}$ and not 1 is to be reckoned for each class containing a reduced form of the type $(a, 0, a)$ and $\frac{1}{3}$ for each class containing a reduced form (a, a, a); then if n is any positive integer,

$$\sum_{\kappa=0,\pm1,\dots} H(4n-\kappa^2)=\Phi(n)+\Psi(n) \qquad (-2\sqrt{n} \leqq \kappa \leqq 2\sqrt{n})$$

where $\Phi(n)$ means the sum of the divisors of n, and $\Psi(n)$ means the excess of the sum of those divisors of n which are greater than $\sqrt{n}$ over the sum of those divisors which are less than $\sqrt{n}$. The formula is obtained by calculating in two different ways the number of reduced values of z which satisfy the modular equation $J(nz)=J(z)$, where $J(z)$ is the absolute invariant which, for the elliptic function $\wp(u;\ g_2, g_3)$ is $g_2^3 \div (g_2^3-27g_3^2)$, and z is the ratio of any two primitive periods taken so that the real part of iz is negative (see below, § 68). It should be added that there is a series of scattered papers by J. Liouville, which implicitly contain Kronecker's class-number relations, obtained by a purely arithmetical process without any use of transcendents.

40. *Bilinear Forms.*—A bilinear form means an expression of the type $\Sigma a_{ik}x_i y_k$ $(i=1, 2, \dots m;\ \ k=1, 2, \dots n)$; the most important case is when $m=n$, and only this will be considered here. The invariants of a form are its determinant $[a_{nn}]$ and the elementary factors thereof. Two bilinear forms are equivalent when each can be transformed into the other by linear integral substitutions $x'=\Sigma\alpha x$, $y'=\Sigma\beta y$. Every bilinear form is equivalent to a *reduced* form $\sum_1^r e_i x_i y_i$, and $r=n$, unless $[a_{nn}]=0$. In order that two forms may be equivalent it is necessary and sufficient that their invariants should be the same. Moreover, if $a\sim b$ and $c\sim d$, and if the invariants of the forms $a+\lambda c$, $b+\lambda d$ are the same for all values of λ, we shall have $a+\lambda c \sim b+\lambda d$, and the transformation of one form to the other may be effected by a substitution which does not involve λ. The theory of bilinear forms practically includes that of quadratic forms, if we suppose x_i, y_i to be cogredient variables. Kronecker has developed the case when $n=2$, and deduced various class-relations for quadratic forms in a manner resembling that of Liouville. So far as the bilinear forms are concerned, the main result is that the number of classes for the positive determinant $a_{11}a_{22}-a_{12}a_{21}=\Delta$ is $12\{\Phi(\Delta)+\Psi(\Delta)\}+2\epsilon$, where ϵ is 1 or 0 according as Δ is or is not a square, and the symbols Φ, Ψ have the meaning previously assigned to them (§ 39).

41. *Higher Quadratic Forms.*—The algebraic theory of quadratics is so complete that considerable advance has been made in the much more complicated arithmetical theory. Among the most important results relating to the general case of n variables are the proof that the class-number is finite; the enumeration of the arithmetical invariants of a form; classification according to orders and genera, and proof that genera with specified characters exist; also the determination of all the rational transformations of a given form into itself. In connexion with a definite form there is the important conception of its *weight*; this is defined as the reciprocal of the number of its proper automorphs. Equivalent forms are of the same weight; this is defined to be the weight of their class. The weight of a genus or order is the sum of the weights of the classes contained in it; and expressions for the weight of a given genus have actually been obtained. For binary forms the sum of the weights of all the genera coincides with the expression denoted by H(Δ) in § 39. The complete discussion of a form requires the consideration of $(n-2)$ associated quadratics; one of these is the contravariant of the given form, each of the others contains more than n variables. For certain quaternary and senary classes there are formulae analogous to the class-relations for binary forms referred to in § 39 (see Smith, *Proc. R.S.* xvi., or *Collected Papers*, i. 510).

Among the most interesting special applications of the theory are certain propositions relating to the representation of numbers as the sum of squares. In order that a number may be expressible as the sum of two squares it is necessary and sufficient for it to be of the form PQ^2, where P has no square factor and no prime factor of the form $4n+3$. A number is expressible as the sum of three squares if, and only if, it is of the form m^2n with $n \equiv 1, \pm2 \pm3 \pmod 8$; when $m=1$ and $n \equiv 3 \pmod 8$, all the squares are odd, and hence follows Fermat's theorem that every number can be expressed as the sum of three triangular numbers (one or two of which may be 0). Another famous theorem of Fermat's is that every number can be expressed as the sum of four squares; this was first proved by Jacobi, who also proved that the number of solutions of $n=x^2+y^2+z^2+t^2$ is $8\Phi(n)$, if n is odd, while if n is even it is 24 times the sum of the odd factors of n. Explicit and finite, though more complicated, formulae have been obtained for the number of representations of n as the sum of five, six, seven and eight squares respectively. As an example of the outstanding difficulties of this part of the subject may be mentioned the problem of finding all the integral (not merely rational) automorphs of a given form f. When f is ternary, C. Hermite has shown that the solution depends on finding all the integral solutions of $F(x, y, z)+t^2=1$, where F is the contravariant of f.

Thanks to the researches of Gauss, Eisenstein, Smith, Hermite and others, the theory of ternary quadratics is much less incomplete than that of quadratics with four or more variables. Thus methods of reduction have been found both for definite and for indefinite forms; so that it would be possible to draw up a table of representative forms, if the result were worth the labour. One specially important theorem is the solution of $ax^2+by^2+cz^2=0$; this is always possible if $-bc$, $-ca$, $-ab$ are quadratic residues of a, b, c respectively, and a formula can then be obtained which furnishes all the solutions.

42. *Complex Numbers.*—One of Gauss's most important and far-reaching contributions to arithmetic was his introduction of complex

integers $a+bi$, where a, b are ordinary integers, and, as usual, $i^2=-1$. In this theory there are four units ± 1, $\pm i$; the numbers $i^h(a+bi)$ are said to be *associated*; $a-bi$ is the conjugate of $a+bi$ and we write $N(a\pm bi)=a^2+b^2$, the *norm* of $a+bi$, its conjugate, and associates. The most fundamental proposition in the theory is that the process of residuation (§ 24) is applicable; namely, if m, n are any two complex integers and $N(m)>N(n)$, we can always find integers q, r such that $m=qn+r$ with $N(r)\leq\frac{1}{2}N(n)$. This may be proved analytically, but is obvious if we mark complex integers by points in a plane. Hence immediately follow propositions about resolutions into prime factors, greatest common measure, &c., analogous to those in the ordinary theory; it will only be necessary to indicate special points of difference.

We have $2=-i(1+i)^2$, so that 2 is associated with a square: a real prime of the form $4n+3$ is still a prime, but one of the form $4n+1$ breaks up into two conjugate prime factors, for example, $5=(1-2i)(1+2i)$ An integer is even, semi-even, or odd according as it is divisible by $(1+i)^2$, $(1+i)$ or is prime to $(1+i)$. Among four associated odd integers there is one and only one which $\equiv 1$ (mod $2+2i$); this is said to be *primary*; the conjugate of a primary number is primary, and the product of any number of primaries is primary. The conditions that $a+bi$ may be primary are $b\equiv 0$ (mod 2) $a+b-1\equiv 0$ (mod 4). Every complex integer can be uniquely expressed in the form $i^m(1+i)^n a^\alpha b^\beta c^\gamma\ldots$, where $0\leq m<4$, and a, b, c, ... are primary primes.

With respect to a complex modulus m, all complex integers may be distributed into $N(m)$ incongruous classes. If $m=h(a+bi)$ where a, b are co-primes, we may take as representatives of these classes the residues $x+yi$ where $x=0, 1, 2,\ldots\{(a^2+b^2)h-1\}$; $y=0, 1, 2, \ldots(h-1)$. Thus when $b=0$ we may take $x=0, 1, 2,\ldots(h-1)$; $y=0, 1, 2,\ldots(h-1)$, giving the h^2 residues of the real number h; while if $a+bi$ is prime, $1, 2, 3,\ldots(a^2+b^2-1)$ form a complete set of residues.

The number of residues of m that are prime to m is given by

$$\phi(m)=N(m)\Pi\left(1-\frac{1}{N(p)}\right)$$

where the product extends to all prime factors of m. As an analogue to Fermat's theorem we have, for any integer prime to the modulus,

$$x^{\phi(m)}\equiv 1 \,(\text{mod } m), x^{N(p)-1}\equiv 1 \,(\text{mod } p)$$

according as m is composite or prime. There are $\phi\{N(p)-1\}$ primitive roots of the prime p; a primitive root in the real theory for a real prime $4n+1$ is also a primitive root in the new theory for each prime factor of $(4n+1)$, but if $p=4n+3$ be a prime its primitive roots are necessarily complex.

43. If p, q are any two odd primes, we shall define the symbols $\left(\frac{p}{q}\right)_2$ and $\left(\frac{p}{q}\right)_4$ by the congruences

$$p^{\frac{1}{2}\{N(q)-1\}}\equiv\left(\frac{p}{q}\right)_2,\ p^{\frac{1}{4}\{N(q)-1\}}\equiv\left(\frac{p}{q}\right)_4 (\text{mod } q),$$

it being understood that the symbols stand for absolutely least residues. It follows that $\left(\frac{p}{q}\right)_2=1$ or -1 according as p is a quadratic residue of q or not; and that $\left(\frac{p}{q}\right)_4=1$ only if p is a biquadratic residue of q. If p, q are primary primes, we have two laws of reciprocity, expressed by the equations

$$\left(\frac{p}{q}\right)_2=\left(\frac{q}{p}\right)_2,\ \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=(-1)^{\frac{1}{4}\{N(p)-1\}.\frac{1}{4}\{.N(q)-1\}}.$$

To these must be added the supplementary formulae

$$\left(\frac{i}{p}\right)_2=(-1)^{\frac{1}{4}\{N(p)-1\}},\ \left(\frac{1+i}{a+bi}\right)_2=(-1)^{\frac{1}{8}\{(a+b)^2-1\}},$$

$$\left(\frac{i}{a+bi}\right)_4=i^{\frac{1}{2}(a-1)}\qquad\left(\frac{1+i}{a+bi}\right)_4=i^{\frac{1}{4}\{a+b-(1+b)^2\}},$$

$a+bi$ being a primary odd prime. In words, the law of biquadratic reciprocity for two primary odd primes may be expressed by saying that the biquadratic characters of each prime with respect to the other are identical, unless $p\equiv q\equiv 3+2i$ (mod 4), in which case they are opposite. The law of biquadratic reciprocity was discovered by Gauss, who does not seem, however, to have obtained a complete proof of it. The first published proof is that of Eisenstein, which is very beautiful and simple, but involves the theory of lemniscate functions. A proof on the lines indicated in Gauss's posthumous papers has been developed by Busche; this probably admits of simplification. Other demonstrations, for instance Jacobi's, depend on cyclotomy (see below).

44. *Algebraic Numbers.*—The first extension of Gauss's complex theory was made by E. E. Kummer, who considered complex numbers represented by rational integral functions of any roots of unity, thus including the ordinary theory and Gauss's as special cases. He was soon faced by the difficulty that, in some cases, the law that an integer can be uniquely expressed as the product of prime factors appeared to break down. To see how this happens take the equation $\eta^2+\eta+6=0$, the roots of which are expressible as rational integral functions of 23rd roots of unity, and let η be either of the roots. If we define $a\eta+b$ to be an integer, when a, b are natural numbers, the product of any number of such integers is uniquely expressible in the form $l\eta+m$. Conversely every integer can be expressed as the product of a finite number of indecomposable integers $a+b\eta$, that is, integers which cannot be further resolved into factors of the same type. But this resolution is not necessarily unique: for instance $6=2.3=-\eta(\eta+1)$, where $2, 3, \eta, \eta+1$ are all indecomposable and essentially distinct. To see the way in which Kummer surmounted the difficulty consider the congruence

$$u^2+u+6\equiv 0 (\text{mod } p)$$

where p is any prime, except 23. If $-23Rp$ this has two distinct roots u_1, u_2; and we say that $a\eta+b$ is divisible by the ideal prime factor of p corresponding to u_1, if $au_1+b\equiv 0$ (mod p). For instance, if $p=2$ we may put $u_1=0$, $u_2=1$ and there will be two ideal factors of 2, say p_1 and p_2 such that $a\eta+b\equiv 0$ (mod p_1) if $b\equiv 0$ (mod 2) and $a\eta+b\equiv 0$ (mod p_2) if $a+b\equiv 0$ (mod 2). If both these congruences are satisfied, $a\equiv b\equiv 0$ (mod 2) and $a\eta+b$ is divisible by 2 in the ordinary sense. Moreover $(a\eta+b)(c\eta+d)=(bc+ad-ac)\eta+(bd-6ac)$ and if this product is divisible by p_1, $bd\equiv 0$ (mod 2), whence either $a\eta+b$ or $c\eta+d$ is divisible by p_1; while if the product is divisible by p_2 we have $bc+ad+bd-7ac\equiv 0$ (mod 2) which is equivalent to $(a+b)(c+d)\equiv 0$ (mod 2), so that again either $a\eta+b$ or $c\eta+d$ is divisible by p_2. Hence we may properly speak of p_1 and p_2 as *prime* divisors. Similarly the congruence $u^2+u+6\equiv 0$ (mod 3) defines two ideal prime factors of 3, and $a\eta+b$ is divisible by one or the other of these according as $b\equiv 0$ (mod 3) or $2a+b\equiv 0$ (mod 3); we will call these prime factors p_3, p_4. With this notation we have (neglecting unit factors)

$$2=p_1p_2,\ 3=p_3p_4,\ \eta=p_1p_3,\ 1+\eta=p_2p_4.$$

Real primes of which -23 is a non-quadratic residue are also primes in the field (η); and the prime factors of any number $a\eta+b$, as well as the degree of their multiplicity, may be found by factorizing $(6a^2-ab+b^2)$, the norm of $(a\eta+b)$. Finally *every* integer divisible by p_2 is expressible in the form $\pm 2m\pm(1+\eta)n$ where m, n are natural numbers (or zero); it is convenient to denote this fact by writing $p_2=[2, 1+\eta]$, and calling the aggregate $2m+(1+\eta)n$ a compound modulus with the base $2, 1+\eta$. This generalized idea of a modulus is very important and far-reaching; an aggregate is a modulus when, if α, β are any two of its elements, $\alpha+\beta$ and $\alpha-\beta$ also belong to it. For arithmetical purposes those moduli are most useful which can be put into the form $[\alpha_1, \alpha_2,\ldots\alpha_n]$ which means the aggregate of all the quantities $x_1\alpha_1+x_2\alpha_2+\ldots+x_n\alpha_n$ obtained by assigning to $(x_1,x_2,\ldots x_n)$, independently, the values $0_1\pm 1$, ± 2, &c. Compound moduli may be multiplied together, or raised to powers, by rules which will be plain from the following example. We have

$$p_2^2=[4, 2(1+\eta), (1+\eta)^2]=[4, 2+2\eta, -5+\eta]=[4, 12, -5+\eta]$$
$$=[4, -5+\eta]=[4, 3+\eta]$$

hence

$$p_2^3=p_2^2.p_2=[4, 3+\eta]\times[2, 1+\eta]=[8, 4+4\eta, 6+2\eta, 3+4\eta+\eta^2]$$
$$=[8, 4+4\eta, 6+2\eta, -3+3\eta]=(\eta-1)[\eta+2, \eta-6, 3]=(\eta-1)[1, \eta].$$

Hence every integer divisible by p_2^3 is divisible by the actual integer $(\eta-1)$ and conversely; so that in a certain sense we may regard p_2 as a cube root. Similarly the cube of any other ideal prime is of the form $(a\eta+b)[1, \eta]$. According to a principle which will be explained further on, all primes here considered may be arranged in three classes; one is that of the real primes, the others each contain ideal primes only. As we shall see presently all these results are intimately connected with the fact that for the determinant -23 there are three primitive classes, represented by $(1, 1, 6)$ $(2, 1, 3)$, $(2, -1, 3)$ respectively.

45. Kummer's definition of ideal primes sufficed for his particular purpose, and completely restored the validity of the fundamental theorems about factors and divisibility. His complex integers were more general than any previously considered and suggested a definition of an algebraic integer in general, which is as follows: if $a_1, a_2,\ldots a_n$ are ordinary integers (*i.e.* elements of $\overline{N}$, § 7), and θ satisfies an equation of the form

$$\theta^n+a_1\theta^{n-1}+a_2\theta^{n-2}+\ldots+a_{n-1}\theta+a_n=0,$$

θ is said to be an algebraic integer. We may suppose this equation irreducible; θ is then said to be of the nth order. The n roots θ, θ', θ'', ...$\theta^{(n-1)}$ are all different, and are said to be conjugate. If the equation began with $a_0\theta^n$ instead of θ^n, θ would still be an algebraic number; every algebraic number can be put into the form θ/m, where m is a natural number and θ an algebraic integer.

Associated with θ we have a *field* (or *corpus*) $\Omega=R(\theta)$ consisting of all rational functions of θ with real rational coefficients; and in like manner we have the conjugate fields $\Omega'=R(\theta')$, &c. The aggregate of integers contained in Ω is denoted by $\mathfrak{o}$.

Every element of Ω can be put into the form

$$\omega=c_0+c_1\theta+\ldots+c_{n-1}\theta^{n-1}$$

where c_0, c_1, ...c_{n-1} are real and rational. If these coefficients are all integral, ω is an integer; but the converse is not necessarily true. It is possible, however, to find a set of integers ω_1, ω_2, ...ω_n belonging to Ω, such that every integer in Ω can be uniquely expressed in the form

$$\omega=h_1\omega_1+h_2\omega_2+\ldots+h_n\omega_n$$

where $h_1, h_2, \dots h_n$ are elements of N which may be called the *co-ordinates* of ω with respect to the *base* $\omega_1, \omega_2, \dots \omega_n$. Thus $\mathfrak{o}$ is a modulus (§ 44), and we may write $\mathfrak{o}=[\omega_1, \omega_2, \dots \omega_n]$. Having found one base, we can construct any number of equivalent bases by means of equations such as $\omega_i' = \sum_j c_{ij}\omega^j$, where the rational integral coefficients c_i^j are such that the determinant $|c_{nn}| = \pm 1$.

If we write

$$\sqrt{\Delta} = \begin{vmatrix} \omega_1, & \omega_2, & \dots & \omega_n \\ \omega'_1, & \omega'_2, & \dots & \omega'_n \\ \omega''_1, & \omega''_2, & \dots & \omega''_n \\ \vdots & & & \\ \omega_1^{(n-1)}, & \omega_2^{(n-1)}, & \dots & \omega_n^{(n-1)} \end{vmatrix}$$

Δ is a rational integer called the *discriminant* of the field. Its value is the same whatever base is chosen.

If α is any integer in Ω, the product of α and its conjugates is a rational integer called the *norm* of α, and written $N(\alpha)$. By considering the equation satisfied by α we see that $N(\alpha)=\alpha\alpha_1$ where α_1 is an integer in Ω. It follows from the definition that if α, β are any two integers in Ω, then $N(\alpha\beta)=N(\alpha)N(\beta)$; and that for an ordinary real integer m, we have $N(m)=m^n$.

46. *Ideals.*—The extension of Kummer's results to algebraic numbers in general was independently made by J. W. R. Dedekind and Kronecker; their methods differ mainly in matters of notation and machinery, each having special advantages of its own for particular purposes. Dedekind's method is based upon the notion of an *ideal*, which is defined by the following properties:—

(i.) An ideal $\mathfrak{m}$ is an aggregate of integers in Ω.

(ii.) This aggregate is a modulus; that is to say, if μ, μ' are any two elements of $\mathfrak{m}$ (the same or different) $\mu-\mu'$ is contained in $\mathfrak{m}$. Hence also $\mathfrak{m}$ contains a zero element, and $\mu+\mu'$ is an element of $\mathfrak{m}$.

(iii.) If μ is any element of $\mathfrak{m}$, and ω any element of $\mathfrak{o}$, then $\omega\mu$ is an element of $\mathfrak{m}$. It is this property that makes the notion of an ideal more specific than that of a modulus.

It is clear that ideals exist; for instance, $\mathfrak{o}$ itself is an ideal. Again, all integers in Ω which are divisible by a given integer α (in $\mathfrak{o}$) form an ideal; this is called a *principal ideal*, and is denoted by $\mathfrak{o}\alpha$. Every ideal can be represented by a base (§§ 44, 45), so that we may write $\mathfrak{m}=[\mu_1, \mu_2, \dots \mu_n]$, meaning that every element of $\mathfrak{m}$ can be uniquely expressed in the form $\Sigma h_i\mu_i$, where h_i is a rational integer. In other words, every ideal has a base (and therefore, of course, an infinite number of bases). If $\mathfrak{a}$, $\mathfrak{b}$ are any two ideals, and if we form the aggregate of all products $\alpha\beta$ obtained by multiplying each element of the first ideal by each element of the second, then this aggregate, together with all sums of such products, is an ideal which is called the product of $\mathfrak{a}$ and $\mathfrak{b}$ and written $\mathfrak{ab}$ or $\mathfrak{ba}$. In particular $\mathfrak{oa}=\mathfrak{a}$, $\mathfrak{o}^2=\mathfrak{o}$,$\mathfrak{o}\alpha$. $\mathfrak{o}\beta=\mathfrak{o}\alpha\beta$. This law of multiplication is associative as well as commutative. It is clear that every element of $\mathfrak{ab}$ is contained in $\mathfrak{a}$: it can be proved that, conversely, if every element of $\mathfrak{c}$ is contained in $\mathfrak{a}$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}=\mathfrak{c}$. In particular, if α is any element of $\mathfrak{a}$, there is an ideal $\mathfrak{a}'$ such that $\mathfrak{o}\alpha=\mathfrak{aa}'$. A *prime ideal* is one which has no divisors except itself and $\mathfrak{o}$. It is a fundamental theorem that every ideal can be resolved into the product of a finite number of prime ideals, and that this resolution is unique. It is the decomposition of a principal ideal into the product of prime ideals that takes the place of the resolution of an integer into its prime factors in the ordinary theory. It may happen that all the ideals in Ω are principal ideals; in this case every resolution of an ideal into factors corresponds to the resolution of an integer into actual integral factors, and the introduction of ideals is unnecessary. But in every other case the introduction of ideals or some equivalent notion, is indispensable. When two ideals have been resolved into their prime factors, their greatest common measure and least common multiple are determined by the ordinary rules. Every ideal may be expressed (in an infinite number of ways) as the greatest common measure of two principal ideals.

47. There is a theory of congruences with respect to an ideal modulus. Thus $\alpha\equiv\beta \pmod{\mathfrak{m}}$ means that $\alpha-\beta$ is an element of $\mathfrak{m}$. With respect to $\mathfrak{m}$, all the integers in Ω may be arranged in a finite number of incongruent classes. The number of these classes is called the *norm* of $\mathfrak{m}$, and written $N(\mathfrak{m})$. The norm of a prime ideal $\mathfrak{p}$ is some power of a real prime p; if $N(\mathfrak{p})=p^f$, $\mathfrak{p}$ is said to be a prime ideal of degree f. If $\mathfrak{m}$, $\mathfrak{n}$ are any two ideals, then $N(\mathfrak{mn})=N(\mathfrak{m})N(\mathfrak{n})$. If $N(\mathfrak{m})=m$, then $m\equiv 0 \pmod{\mathfrak{m}}$, and there is an ideal $\mathfrak{m}'$ such that $\mathfrak{o}m=\mathfrak{mm}'$. The norm of a principal ideal $\mathfrak{o}\alpha$ is equal to the absolute value of $N(\alpha)$ as defined in § 45.

The number of incongruent residues prime to $\mathfrak{m}$ is—

$$\phi(\mathfrak{m})=N(\mathfrak{m})\Pi\left(1-\frac{1}{N(\mathfrak{p})}\right),$$

where the product extends to all prime factors of $\mathfrak{m}$. If ω is any element of $\mathfrak{o}$ prime to $\mathfrak{m}$,

$$\omega^{\phi(\mathfrak{m})}\equiv 1 \pmod{\mathfrak{m}}.$$

Associated with a prime modulus $\mathfrak{p}$ for which $N(\mathfrak{p})=p^f$ we have $\phi(p^f-1)$ primitive roots, where ϕ has the meaning given to it in the ordinary theory. Hence follow the usual results about exponents, indices, solutions of linear congruences, and so on. For any modulus $\mathfrak{m}$ we have $N(\mathfrak{m})=\Sigma\phi(\mathfrak{d})$, where the sum extends to all the divisors of $\mathfrak{m}$.

48. Every element of $\mathfrak{o}$ which is not contained in any other ideal is an *algebraic unit*. If the conjugate fields $\Omega, \Omega', \dots \Omega^{(n-1)}$ consist of r_1 real and $2r_2$ imaginary fields, there is a system of units $\epsilon_1, \epsilon_2, \dots \epsilon_r$, where $r=r_1+r_2-1$, such that every unit in Ω is expressible in the form $\epsilon=\rho\epsilon_1^a\epsilon_2^b\dots\epsilon_r^l$ where ρ is a root of unity contained in Ω and $a, b, \dots l$ are natural numbers. This theorem is due to Dirichlet.

The norm of a unit is $+1$ or -1; and the determination of all the units contained in a given field is in fact the same as the solution of a Diophantine equation

$$F(h_1, h_2, \dots h_n)=\pm 1.$$

For a quadratic field the equation is of the form $h_1^2-nh_2^2=\pm 1$, and the theory of this is complete; but except for certain special cubic corpora little has been done towards solving the important problem of assigning a definite process by which, for a given field, a system of fundamental units may be calculated. The researches of Jacobi, Hermite, and Minkowsky seem to show that a proper extension of the method of continued fractions is necessary.

49. *Ideal Classes.*—If $\mathfrak{m}$ is any ideal, another ideal $\mathfrak{n}$ can always be found such that $\mathfrak{mn}$ is a principal ideal; for instance, one such multiplier is $\mathfrak{m}^{-1}N(\mathfrak{m})$. Two ideals $\mathfrak{m}$, $\mathfrak{m}'$ are said to be equivalent ($\mathfrak{m}\sim\mathfrak{m}'$) or to belong to the same *class*, if there is an ideal $\mathfrak{n}$ such that $\mathfrak{mn}$, $\mathfrak{m}'\mathfrak{n}$ are both principal ideals. It can be proved that two ideals each equivalent to a third are equivalent to each other and that all ideals in Ω may be distributed into a finite number, h, of ideal classes. The class which contains all principal ideals is called the principal class and denoted by O.

If $\mathfrak{m}$, $\mathfrak{n}$ are any two ideals belonging to the classes A, B respectively, then $\mathfrak{mn}$ belongs to a definite class which depends only upon A, B and may be denoted by AB or BA indifferently. Thus the class-symbols form an Abelian group of order h, of which O is the unit element; and, *mutatis mutandis*, the theorems of § 37 about composition of classes still hold good.

The principal theorem with regard to the determination of h is the following, which is Dedekind's generalization of the corresponding one for quadratic fields, first obtained by Dirichlet. Let

$$\zeta(s)=\sum_{(\mathfrak{m})} N(\mathfrak{m})^{-s}$$

where the sum extends to all ideals $\mathfrak{m}$ contained in Ω; this converges so long as the real quantity s is positive and greater than 1. Then κ being a certain quantity which can be calculated ***when a fundamental system of units is known***, we shall have

$$\kappa h = \underset{s=1}{Lt}\{(s-1)\zeta(s)\}.$$

The expression for κ is rather complicated, and very peculiar; it may be written in the form

$$\kappa=\frac{2^{r1+r2}\pi^{r2}}{w}\cdot\frac{R}{|\sqrt{\Delta}|}$$

where $|\sqrt{\Delta}|$ means the absolute value of the square root of the discriminant of the field, r_1, r_2 have the same meaning as in § 48, w is the number of roots of unity in Ω, and R is a determinant of the form $|l_i(\epsilon^j)|$, of order (r_1+r_2-1), with elements which are, in a certain special sense, "logarithms" of the fundamental units $\epsilon_1, \epsilon_2, \dots \epsilon_r$.

50. The discriminant Δ enjoys some very remarkable properties. Its value is always different from ± 1; there can be only a finite number of fields which have a given discriminant; and the rational prime factors of $\Delta(\Omega)$ are precisely those rational primes which, in Ω, are divisible by the square (or some higher power) of a prime ideal. Consequently, every rational prime not contained in Δ is resolvable, in Ω, into the product of distinct primes, each of which occurs only once. The presence of multiple prime factors in the discriminant was the principal difficulty in the way of extending Kummer's method to all fields, and was overcome by the introduction of compound moduli—for this is the common characteristic of Dedekind's and Kronecker's procedure.

51. *Normal Fields.*—The special properties of a particular field Ω are closely connected with its relations to the conjugate fields $\Omega', \Omega'', \dots \Omega^{(n-1)}$. The most important case is when each of the conjugate fields is identical with Ω: the field is then said to be *Galoisian* or *normal*. The aggregate $R(\theta, \theta', \dots \theta^{(n-1)})$ of all rational functions of θ and its conjugates is a normal field: hence every arithmetical field of order n is either normal, or contained in a normal field of a higher order. The roots of an equation $f(\theta)=0$ which defines a normal field are associated with a group of substitutions: if this is Abelian, the field is called Abelian; if it is cyclic, the field is called cyclic. A cyclotomic field is one the elements of which are all expressible as rational functions of roots of unity; in particular the complete cyclotomic field C_m, of order $\phi(m)$, is the aggregate of all rational functions of a primitive mth root of unity. To Kronecker is due the very remarkable theorem that all Abelian (including cyclic) fields are cyclotomic: the first published proof of this was given by Weber, and another is due to D. Hilbert.

Many important theorems concerning a normal field have been established by Hilbert. He shows that if Ω is a given normal field of order m, and $\mathfrak{p}$ any of its prime ideals, there is a finite series of associated fields Ω_1, Ω_2, &c., of orders m_1, m_2, &c., such that $m_i\equiv 0$ (mod. $m^i{}_{+1}$), and that if $r^i=m/m^i$, $\mathfrak{p}^{r^i}=\mathfrak{p}_i$, a prime ideal in Ω^i. If Ω_i is the last of this series, it is called the *field of inertia*

(*Trägheitskörper*) for $\mathfrak{p}$: next after this comes another field of still lower order called the *resolving field* (*Zerlegungskörper*) for $\mathfrak{p}$, and in this field there is a prime *of the first degree*, $\mathfrak{p}_{l+1}$, such that $p_{l+1}=\mathfrak{p}^k$, where $k=m/m_l$. In the field of inertia $\mathfrak{p}_{l+1}$ remains a prime, but becomes of higher degree; in Ω_{l-1}, which is called the *branch-field* (*Verzweigungskörper*) it becomes a power of a prime, and by going on in this way from the resolving field to Ω, we obtain $(l+2)$ representations for any prime ideal of the resolving field. By means of these theorems, Hilbert finds an expression for the exact power to which a rational prime p occurs in the discriminant of Ω, and in other ways the structure of Ω becomes more evident. It may be observed that whem m is prime the whole series reduces to Ω and the rational field, and we conclude that every prime ideal in Ω is of the first or mth degree: this is the case, for instance, when $m=2$, and is one of the reasons why quadratic fields are comparatively so simple in character.

52. *Quadratic Fields.*—Let m be an ordinary integer different from $+1$, and not divisible by any square: then if x, y assume all ordinary rational values the expressions $x+y\sqrt{m}$ are the elements of a field which may be called $\Omega(\sqrt{m})$. It should be observed that $\sqrt{m}$ means one definite root of $x^2-m=0$, it does not matter which: it is convenient, however, to agree that $\sqrt{m}$ is positive when m is positive, and $i\sqrt{m}$ is negative when m is negative. The principal results relating to Ω will now be stated, and will serve as illustrations of §§ 44-51.

In the notation previously used

$$\mathfrak{n}=[1,\ \tfrac{1}{2}(1+\sqrt{m})] \text{ or } [1,\ \sqrt{m}]$$

according as $m\equiv 1 \pmod 4$ or not. In the first case $\Delta=m$, in the second $\Delta=4m$. The field Ω is normal, and every ideal prime in it is of the first degree.

Let q be any odd prime factor of m; then $q=\mathfrak{q}^2$, where $\mathfrak{q}$ is the prime ideal $[q,\ \tfrac{1}{2}(q+\sqrt{m})]$ when $m\equiv 1 \pmod 4$ and in other cases $[q, \sqrt{m}]$. An odd prime p of which m is a quadratic residue is the product of two prime ideals $\mathfrak{p}$, $\mathfrak{p}'$, which may be written in the form $[p,\ \tfrac{1}{2}(a+\sqrt{m})]$, $[p, \tfrac{1}{2}(a-\sqrt{m})]$ or $[p,\ a+\sqrt{m}]$, $[p, a-\sqrt{m}]$, according as $m\equiv 1 \pmod 4$ or not: here a is a root of $x^2\equiv m \pmod p$, taken so as to be odd in the first of the two cases. All other rational odd primes are primes in Ω. For the exceptional prime 2 there are four cases to consider: (i.) if $m\equiv 1 \pmod 8$, then $2=[2,\tfrac{1}{2}(1+\sqrt{m})]\times[2,\tfrac{1}{2}(1-\sqrt{m})]$. (ii.) If $m\equiv 5 \pmod 8$, then 2 is prime: (iii.) if $m\equiv 2 \pmod 4$, $2=[2,\sqrt{m}]^2$: (iv.) if $m=3$ (mod$\equiv 4$), $2=[2,1+\sqrt{m})^2$. Illustrations will be found in § 44 for the case $m=23$.

53. *Normal Residues. Genera.*—Hilbert has introduced a very convenient definition, and a corresponding symbol, which is a generalization of Legendre's quadratic character. Let n, m be rational integers, m not a square, w any rational prime; we write $\left(\frac{n,\ m}{w}\right)=+1$ if, to the modulus w, n is congruent to the norm of an integer contained in $\Omega(\sqrt{m})$; in all other cases we put $\left(\frac{n,\ m}{w}\right)=-1$. This new symbol obeys a set of laws, among which may be especially noted $\left(\frac{n,\ w}{w}\right)=\left(\frac{w,\ n}{w}\right)=\left(\frac{n}{w}\right)$ and $\left(\frac{n,\ m}{w}\right)=+1$, whenever n, m are prime to p.

Now let $q_1, q_2, \ldots q_t$ be the different rational prime factors of the discriminant of $\Omega(\sqrt{m})$; then with any rational integer a we may associate the t symbols

$$\left(\frac{a,\ m}{q_1}\right),\ \left(\frac{a,\ m}{q_2}\right), \ldots \left(\frac{a\ \ m}{q_t}\right)$$

and call them the total character of a with respect to Ω. This definition may be extended so as to give a total character for every ideal $\mathfrak{a}$ in Ω, as follows. First let Ω be an imaginary field $(m<0)$; we put $r=t$, $\bar{n}=\mathrm{N}(\mathfrak{a})$, and call

$$\left(\frac{\bar{n},\ m}{q_1}\right), \ldots \left(\frac{\bar{n},\ m}{q_r}\right)$$

the total character of $\mathfrak{a}$. Secondly, let Ω be a real field; we first determine the t separate characters of -1, and if they are all positive we put $\bar{n}=+\mathrm{N}(\mathfrak{a})$, $r=t$, and adopt the r characters just written above as those of $\mathfrak{a}$. Suppose, however, that one of the characters of -1 is negative; without loss of generality we may take it to be that with reference to q_t. We then put $r=t-1$, $\bar{n}=\pm\mathrm{N}(\mathfrak{a})$ taken with such a sign that $\left(\frac{\bar{n},\ m}{q_t}\right)=+1$, and take as the total character of $\mathfrak{a}$ the symbols $\left(\frac{\bar{n},\ m}{q_i}\right)$ for $i=1, 2, \ldots (t-1)$.

With these definitions it can be proved that all ideals of the same class have the same total character, and hence there is a distribution of classes into genera, each genus containing those classes for which the total character is the same (cf. § 36).

Moreover, we have the fundamental theorem that an assigned set of r units ± 1 corresponds to an actually existing genus if, and only if, their product is $+1$, so that the number of actually existing genera is 2^{r-1}. This is really equivalent to a theorem about quadratic forms first stated and proved by Gauss; the same may be said about the next proposition, which, in its natural order, is easily proved by the method of ideals, whereas Gauss had to employ the theory of ternary quadratics.

Every class of the principal genus is the square of a class.

An ambiguous ideal in Ω is defined as one which is unaltered by the change of $\sqrt{m}$ to $-\sqrt{m}$ (that is, it is the same as its conjugate) and not divisible by any rational integer except ± 1. The only ambiguous prime ideals in Ω are those which are factors of its discriminant. Putting $\Delta=\mathfrak{q}_1^2\,\mathfrak{q}_2^2\ldots\mathfrak{q}_t^2$, there are in Ω exactly 2^t ambiguous ideals: namely, those factors of Δ, including $\mathfrak{n}$, which are not divisible by any square. It is a fundamental theorem, first proved by Gauss, that the number of ambiguous classes is equal to the number of genera.

54. *Class-Number.*—The number of ideal classes in the field $\Omega(\sqrt{m})$ may be expressed in the following forms:—

(i.) $m<0$:

$$h=\frac{\tau}{2\Delta}\sum_{n}\left(\frac{\Delta}{n}\right)n \qquad (n=1,\ 2, \ldots, -\Delta);$$

(ii.) $m>0$:

$$h=\frac{1}{2\log\epsilon}\log\frac{\Pi\sin\frac{b\pi}{\Delta}}{\Pi\sin\frac{a\pi}{\Delta}}.$$

In the first of these formulae τ is the number of units contained in Ω; thus $\tau=6$ for $\Delta=-3$, $\tau=4$ for $\Delta=-4$, $\tau=2$ in other cases. In the second formula, ϵ is the fundamental unit, and the products are taken for all the numbers of the set $(1, 2, \ldots \Delta)$ for which $\left(\frac{\Delta}{a}\right)=+1$, $\left(\frac{\Delta}{b}\right)=-1$ respectively. In the ideal theory the only way in which these formulae have been obtained is by a modification of Dirichlet's method; to prove them without the use of transcendental analysis would be a substantial advance in the theory.

55. Suppose that any ideal in Ω is expressed in the form $[\omega_1, \omega_2]$; then any element of it is expressible as $x\omega_1+y\omega_2$, where x, y are rational integers, and we shall have $\mathrm{N}\ (x\omega_1+y\omega_2)=ax^2+bxy+cy^2$, where a, b, c are rational numbers contained in the ideal. If we put $x=\alpha x'+\beta y', y=\gamma x'+\delta y'$, where α, β, γ, δ are rational numbers such that $\alpha\delta-\beta\gamma=\pm 1$, we shall have simultaneously $(a,\ b,\ c)\ (x,\ y)^2=(a',\ b',\ c')\ (x',\ y')^2$ as in § 32 and also

$$(a', b', c')\ (x', y')^2=\mathrm{N}\{x'(\alpha\omega_1+\gamma\omega_2)+y'(\beta\omega_1+\delta\omega_2)\}=\mathrm{N}(x'\omega'_1+y'\omega'_2),$$

where $[\omega'_1, \omega'_2]$ is the same ideal as before. Thus all equivalent forms are associated with the same ideal, and the numbers representable by forms of a particular class are precisely those which are norms of numbers belonging to the associated ideal. Hence the class-number for ideals in Ω is also the class-number for a set of quadratic forms; and it can be shown that all these forms have the same determinant Δ. Conversely, every class of forms of determinant Δ can be associated with a definite class of ideals in $\Omega(\sqrt{m})$, where $m=\Delta$ or $\tfrac{1}{4}\Delta$ as the case may be. Composition of form-classes exactly corresponds to the multiplication of ideals: hence the complete analogy between the two theories, so long as they are really in contact. There is a corresponding theory of forms in connexion with a field of order n: the forms are of the order n, but are only very special forms of that order, because they are algebraically resolvable into the product of linear factors.

56. *Complex Quadratic Forms.*—Dirichlet, Smith and others, have discussed forms (a, b, c) in which the coefficients are complex integers of the form $m+ni$; and Hermite has considered bilinear forms $axx'+bxy'+b'x'y+cyy'$, where x', y', b' are the conjugates of x, y, b and a, c, are real. Ultimately these theories are connected with fields of the fourth order; and of course in the same way we might consider forms (a, b, c) with integral coefficients belonging to any given field of order n: the theory would then be ultimately connected with a field of order $2n$.

57. *Kronecker's Method.*—In practice it is found convenient to combine the method of Dedekind with that of Kronecker, the main principles of which are as follows. Let $\mathrm{F}(x, y, z, \ldots)$ be a polynomial in any number of indeterminates (*umbrae*, as Sylvester calls them) with ordinary integral coefficients; if n is the greatest common measure of the coefficients, we have $\mathrm{F}=n\mathrm{E}$, where E is a primary or unit form. The positive integer n is called the divisor of F; and the divisor of the product of two forms is equal to the product of the divisors of the factors. Next suppose that the coefficients of F are integers in a field Ω of order n. Denoting the conjugate forms by $\mathrm{F}', \mathrm{F}'', \ldots \mathrm{F}^{(n-1)}$, the product $\mathrm{FF'F''}\ldots\mathrm{F}^{(n-1)}=f\mathrm{E}$, where f is a real positive integer, and E a unit form with real integral coefficients. The natural number f is called the norm of F. If F, G are any two forms (in Ω) we have $\mathrm{N(FG)}=\mathrm{N(F)N(G)}$. Let the coefficients of F be α_1, α_2, &c., those of G β_1, β_2, &c., and those of FG γ_1, γ_2, &c.; and let $\mathfrak{p}$ be any prime ideal in Ω. Then if $\mathfrak{p}^m$ is the highest power of $\mathfrak{p}$ contained in each of the coefficients α_i, and $\mathfrak{p}^n$ the highest power of $\mathfrak{p}$ contained in each of the coefficients β_i, $\mathfrak{p}^{m+n}$ is the highest power of $\mathfrak{p}$ contained by the whole set of coefficients γ_i. Writing $\mathrm{dv}(\alpha_1, \alpha_2, \ldots)$ for the highest ideal divisor of α_1, α_2, &c., this is called the *content* of F; and we have the theorem that the

product of the contents of two forms is equal to the content of the product of the forms. Every form is associated with a definite ideal $\mathfrak{m}$, and we have $N(F)=N(\mathfrak{m})$ if $\mathfrak{m}$ is the content of F, and $N(\mathfrak{m})$ has the meaning already assigned to it. On the other hand, to a given ideal correspond an indefinite number of forms of which it is the content; for instance (§ 46, end) we can find forms $\alpha x+\beta y$ of which any given ideal is the content.

58. Now let $\omega_1, \omega_2, \dots \omega_n$ be a basis of $\mathfrak{o}$; $u_1, u_2, \dots u_n$ a set of indeterminates; and

$$\xi=\omega_1u_1+\omega_2u_2+\dots+\omega_nu_n:$$

ξ is called the *fundamental form* of Ω. It satisfies the equation $N(x-\xi)=0$, or

$$F(x)=x^n+U_1x^{n-1}+\dots+U_n=0$$

where $U_1, U_2, \dots U_n$ are rational polynomials in $u_1, u_2, \dots u_n$ with rational integral coefficients. This is called the fundamental equation.

Suppose now that p is a rational prime, and that $p=\mathfrak{p}^a\mathfrak{q}^b\mathfrak{r}^c\dots$ where $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \dots$ &c., are the different ideal prime factors of p, then if $F(x)$ is the left-hand side of the fundamental equation there is an identical congruence

$$F(x)\equiv\{P(x)\}^a\{Q(x)\}^b\{R(x)\}^c\dots(\text{mod } p)$$

where $P(x)$, $Q(x)$, &c., are prime functions with respect to p. The meaning of this is that if we expand the expression on the right-hand side of the congruence, the coefficient of every term $x^lu_1^m\dots u_n^t$ will be congruent, mod p, to the corresponding coefficient in $F(x)$. If f, g, h, &c., are the degrees of $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$, &c. (§ 47), then $f, g, h, \dots$ are the dimensions in $x, u_1, u_2, \dots u_n$ of the forms of P, Q, R, respectively. For every prime p, which is not a factor of Δ, $a=b=c=\dots=1$ and $F(x)$ is congruent to the product of a set of different prime factors, as many in number as there are different ideal prime factors of p. In particular, if p is a prime in Ω, $F(x)$ is a prime function (mod p) and conversely.

It generally happens that rational integral values $a_1, a_2, \dots a_n$ can be assigned to $u_1, u_2, \dots u_n$ such that U_n, the last term in the fundamental equation, then has a value which is prime to p. Supposing that this condition is satisfied, let $a_1\omega_1+a_2\omega_2+\dots+a_n\omega_n=\alpha$; and let $P_1(\alpha)$ be the result of putting $x=\alpha$, $u_i=a_i$ in $P(x)$. Then the ideal $\mathfrak{p}$ is completely determined as the greatest common divisor of p and $P_1(\alpha)$; and similarly for the other prime factors of p. There are, however, exceptional cases when the condition above stated is not satisfied.

59. *Cyclotomy.*—It follows from de Moivre's theorem that the arithmetical solution of the equation $x^m-1=0$ corresponds to the division of the circumference of a circle into m equal parts. The case when m is composite is easily made to depend on that where m is a power of a prime; if m is a power of 2, the solution is effected by a chain of quadratic equations, and it only remains to consider the case when $m=q^\kappa$, a power of an odd prime. It will be convenient to write $\mu=\phi(m)=q^{\kappa-1}(q-1)$; if we also put $r=e^{2\pi i/m}$, the *primitive* roots of $x^m=1$ will be μ in number, and represented by r, r^a, r^b, &c. where $1, a, b$, &c., form a complete set of prime residues to the modulus m. These will be the roots of an irreducible equation $f(x)=0$ of degree μ; the symbol $f(x)$ denoting $(x^m-1)\div(x^{m/q}-1)$. There are primitive roots of the congruence $x^\mu\equiv1$ (mod m); let g be any one of these. Then if we put $r^{g^h}=r_h$, we obtain all the roots of $f(x)=0$ in a definite cyclical order $(r_1, r_2\dots r_\mu)$; and the change of r into r^g produces a cyclical permutation of the roots. It follows from this that every cyclic polynomial in $r_1, r_2, \dots r_\mu$ with rational coefficients is equal to a rational number. Thus if we write $l+ag+bg^2+.+kg^{\mu-1}=n$, we have, in virtue of $r_h=r^{g^k}$, $r_1{}^ar_2{}^b\dots r_{\mu-1}{}^kr_\mu{}^l=r^n$, and, if we use S to denote cyclical summation, $S(r_1{}^ar_2{}^b\dots r_\mu{}^l)=r^n+r^{ng}+\dots+r^{ng^{\mu-1}}$, the sum of the nth powers of all the roots of $f(x)=0$, and this is a rational integer or zero. Since every cyclic polynomial is the sum of parts similar to $S(r_1{}^ar_2{}^b\dots r_\mu{}^l)$, the theorem is proved. Now let e, f be any two conjugate factors of μ, so that $ef=\mu$, and let

$$\eta_i=r_i+r_{i+e}+r_{i+2e}+\dots+r_{i+(f-1)e}\qquad(i=1, 2, \dots e)$$

then the elementary symmetric functions $\Sigma\eta_i$, $\Sigma\eta_i\eta^j$, &c., are cyclical functions of the roots of $f(x)=0$ and therefore have rational values which can be calculated: consequently $\eta_1, \eta_2, \dots\eta_e$, which are called the f-nomial periods, are the roots of an equation

$$F(\eta)=\eta^e+c_1\eta^{e-1}+\dots+c_e=0$$

with rational integral coefficients. This is irreducible, and defines a field of order e contained in the field defined by $f(x)=0$. Moreover, the change of r into r^g alters n_i into η_{i+1}, and we have the theorem that any cyclical function of $\eta_1, \eta_2, \dots n_e$ is rational. Now let h, k be any conjugate factors of f and put

$$z_i=r_i+r_{i+he}+r^i{}_{+2he}+\dots r^i{}_{+(f-h)e}\qquad(i=1, 2, 3,)$$

then $\zeta_1, \zeta_{1+e}, \zeta_{1+2e}\dots\zeta_{1+(h-1)e}$ will be the roots of an equation

$$G(\zeta)=\zeta^h-\eta_1\zeta^{h-1}+c_2\zeta^{h-2}+\dots+c_h=0,$$

the coefficients of which are expressible as rational polynomials in η_1. Dividing h into two conjugate factors, we can deduce from $G(\zeta)=0$ another period equation, the coefficients of which are rational polynomials in η_2, ζ_1, and so on. By choosing for e, h, &c., the successive prime factors of μ, ending up with 2, we obtain a set of equations of prime degree, each rational in the roots of the preceding equations, and the last having r_1 and r_1^{-1} for its roots. Thus to take a very interesting historical case, let $m=17$, so that $\mu=16=2^4$, the equations are all quadratics, and if we take 3 as the primitive roct of 17, they are

$$\eta^2+\eta-4=0,\qquad \zeta^2-\eta\zeta-1=0$$
$$2\lambda^2-2\zeta\lambda+(\eta\zeta-\eta+\zeta-3)=0,\quad \rho^2-\lambda\rho+1=0.$$

If two quantities (real or complex) a and b are represented in the usual way by points in a plane, the roots of $x^2+ax+b=0$ will be represented by two points which can be found by a Euclidean construction, that is to say, one requiring only the use of rule and compass. Hence a regular polygon of seventeen sides can be inscribed in a given circle by means of a Euclidean construction; a fact first discovered by Gauss, who also found the general law, which is that a regular polygon of m sides can be inscribed in a circle by Euclidean construction if and only if $\phi(m)$ is a power of 2; in other words $m=2^\kappa P$ where P is a product of different odd primes, each of which is of the form 2^n+1.

Returning to the case $m=q^k$, we shall call the chain of equations $F(\eta)=0$, &c., when each is of prime degree, a set of Galoisian auxiliaries. We can find different sets, because in forming them we can take the prime factors of μ in any order we like; but their number is always the same, and their degrees always form the same aggregate, namely, the prime factors of μ. No other chain of auxiliaries having similar properties can be formed containing fewer equations of a given prime degree p; a fact first stated by Gauss, to whom this theory is mainly due. Thus if $m=q^\kappa$ we must have at least $(\kappa-1)$ auxiliaries of order q, and if $q-1=2^\alpha p^\beta\dots$, we must also have α quadratics, β equations of order p, and so on. For this reason a set of Galoisian auxiliaries may be regarded as providing the simplest solution of the equation $f(x)=0$.

60. When m is an odd prime p, there is another very interesting way of solving the equation $(x^p-1)\div(x-1)=0$. As before let $(r_1, r_2, \dots r_{p-1})$ be its roots arranged in a cycle by means of a primitive root of $x^{p-1}\equiv1$ (mod p); and let ϵ be a primitive root of $\epsilon^{p-1}=1$. Also let

$$\theta_1=r_1+\epsilon r_2+\epsilon^2r_3+\dots+\epsilon^{p-2}r_{p-1}$$
$$\theta_k=r_1+\epsilon^kr_2+\epsilon^{2k}r_3+\dots+\epsilon^{-k}r_{p-1}\qquad(k=2, 3, \dots p-2)$$

so that θ_k is derived from θ_1 by changing ϵ into ϵ^k.

The cyclical permutation $(r_1, r_2, \dots r_{p-1})$ applied to θ_k converts it into $\epsilon^{-k}\theta_k$; hence $\theta_1\theta_k/\theta_{k+1}$ is unaltered, and may be expressed as a rational, and therefore as an integral function of ϵ. It is found by calculation that we may put

$$\psi_k(\epsilon)=\frac{\theta_1\theta_k}{\theta_{k+1}}=\sum_{m=2}^{m=p+1}\epsilon^{\text{ind}\,m+k\,\text{ind}(p+1-m)}\qquad[k=1, 2, \dots(p-3)]$$

while

$$\theta_1\theta_{p-2}=-p.$$

In the exponents of $\psi_k(\epsilon)$ the indices are taken to the base g used to establish the cyclical order $(r_1, r_2\dots r_{p-1})$. Multiplying together the $(p-2)$ preceding equalities, the result is

$$\theta_1{}^{p-1}=-p\psi_1(\epsilon)\psi_2(\epsilon)\dots\psi_{p-3}(\epsilon)=R(\epsilon)$$

where $R(\epsilon)$ is a rational integral function of ϵ the degree of which, in its reduced form, is less than $\phi(p-1)$. Let ρ be any one definite root of $x^{p-1}=R(\epsilon)$, and put $\theta_1=\rho$: then since

$$\frac{\theta_1{}^k}{\theta_k}=\psi_1\psi_2\dots\psi_{k-1}$$

we must take $\theta_k=\rho^k/\psi_1\psi_2\dots\psi_{k-1}=R_k(\epsilon)\rho^k$, where $R_k(\epsilon)$ is a rational function of ϵ, which we may suppose put into its reduced integral form; and finally, by addition of the equations which define θ_1, θ_2, &c.,

$$(p-1)r_1=\rho+R_2(\epsilon)\rho^2+R_3(\epsilon)\rho^3+\dots+R_{p-2}(\epsilon)\rho^{p-2}.$$

If in this formula we change ρ into $\epsilon^{-k}\rho$, and r_1 into r_{k+1}, it still remains true.

It will be observed that this second mode of solution employs a Lagrangian resolvent θ_1; considered merely as a solution it is neither so direct nor so fundamental as that of Gauss. But the form of the solution is very interesting; and the auxiliary numbers $\psi(\epsilon)$ have many curious properties, which have been investigated by Jacobi, Cauchy and Kronecker.

61. When $m=q^\kappa$, the discriminant of the corresponding cyclotomic field is $\pm q^\lambda$, where $\lambda=q^{\kappa-1}(\kappa q-\kappa-1)$. The prime q is equal to $\mathfrak{q}^\mu$, where $\mu=\phi(m)=q^{\kappa-1}(q-1)$, and $\mathfrak{q}$ is a prime ideal of the first degree. If p is any rational prime distinct from g, and f the least exponent such that $p^f\equiv1$ (mod. m), f will be a factor of μ, and putting $\mu/f=e$, we have $p=\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_e$, where $\mathfrak{p}_1, \mathfrak{p}_2\dots\mathfrak{p}_e$ are different prime ideals each of the fth degree. There are similar theorems for the case when m is divisible by more than one rational prime.

Kummer has stated and proved laws of reciprocity for quadratic and higher residues in what are called regular fields, the definition of which is as follows. Let the field be $R(e^{2\pi i/p})$, where p is an odd prime; then this field is regular, and p is said to be a regular prime, when h, the number of ideal classes in the field, is not divisible by p. Kummer proved the very curious fact that p is regular if, and only if, it is not a factor of the denominators of the first $\frac{1}{2}(p-3)$ Bernoullian numbers. He also succeeded in showing that in the field $R(e^{2\pi i/p})$ the equation $\alpha^p+\beta^p+\gamma^p=0$ has no integral solutions whenever h is not divisible by p^2. What is known as the "last" theorem of Fermat is his assertion that if m is any natural number exceeding 2, the equation $x^m+y^m=z^m$ has no rational solutions, except the obvious ones for which $xyz=0$. It would be sufficient to prove Fermat's theorem for all prime values of m; and whenever Kummer's theorem last quoted applies, Fermat's theorem will hold. Fermat's theorem is true for all values of m such that $2<m<101$, but no complete proof of it has yet been obtained.

Hilbert has studied in considerable detail what he calls Kummer fields, which are obtained by taking x, a primitive pth root of unity, and y any root of $y^p-a=0$, where a is any number in the field $R(x)$ which is not a perfect pth power in that field. The Kummer field is then $R(x, y)$, consisting of all rational functions of x and y. Other fields that have been discussed more or less are general cubic fields, some special biquadratic and a few Abelian fields not cyclic.

Among the applications of cyclotomy may be mentioned the proof which it affords of the theorem, first proved by Dirichlet, that if m, n are any two rational integers prime to each other, the linear form $mx+n$ is capable of representing an infinite number of primes.

62. *Gauss's Sums.*—Let m be any positive real integer; then

$$\sum_{s=0}^{s=m-1} e^{2s^2\pi i/m}=\frac{i+i^{1-m}}{1+i}\sqrt{m}.$$

This remarkable formula, when m is prime, contains results which were first obtained by Gauss, and thence known as Gauss's sums. The easiest method of proof is Kronecker's, which consists in finding the value of $\int\{e^{2\pi iz^2/m}dz/(1-e^{2\pi iz})\}$, taken round an appropriate contour. It will be noticed that one result of the formula is that the square root of any integer can be expressed as a rational function of roots of unity.

The most important application of the formula is the deduction from it of the law of quadratic reciprocity for real primes: this was done by Gauss.

63. One example may be given of some remarkable formulae giving explicit solutions of representations of numbers by certain quadratic forms. Let p be any odd prime of the form $7n+2$; then we shall have $p=7n+2=x^2+7y^2$, where x is determined by the congruences

$$2x\equiv\frac{(3n)!}{(n)!\,(2n)!}\pmod{p};\quad x\equiv 3\pmod{7}.$$

This formula was obtained by Eisenstein, who proved it by investigating properties of integers in the field generated by $\eta^2-21\eta-7=0$, which is a component of the field generated by seventh roots of unity. The first formula of this kind was given by Gauss, and relates to the case $p=4n+1=x^2+y^2$; he conceals its connexion with complex numbers. Probably there are many others which have not yet been stated.

64. *Higher Congruences. Functional Moduli.*—Suppose that p is a real prime, and that $f(x)$, $\phi(x)$ are polynomials in x with rational integral coefficients. The congruence $f(x)\equiv\phi(x)\pmod{p}$ is identical when each coefficient of f is congruent, mod p, to the corresponding coefficient of ϕ. It will be convenient to write, under these circumstances, $f\sim\phi\pmod{p}$ and to say that f, ϕ are equivalent, mod p. Every polynomial of degree h is equivalent to another of equal or lower degree, which has none of its coefficients negative, and each of them less than p. Such a polynomial, with unity for the coefficient of the highest power of x contained in it, may be called a reduced polynomial with respect to p. There are, in all, p^h reduced polynomials of degree h. A polynomial may or may not be equivalent to the product of two others of lower degree than itself; in the latter case it is said to be prime. In every case, F being any polynomial, there is an equivalence $F\sim cf_1f_2\dots f_l$ where c is an integer and $f_1, f_2,\dots f_l$ are prime functions; this resolution is unique. Moreover, it follows from Fermat's theorem that $\{F(x)\}^p\sim F(x^p)$, $\{F(x)\}^{p^2}\sim F(x^{p^2})$, and so on.

As in the case of equations, it may be proved that, ***when the modulus is prime***, a congruence $f(x)\equiv 0\pmod{p}$ cannot have more incongruent roots than the index of the highest power of x in $f(x)$, and that if $x\equiv\xi$ is a solution, $f(x)\sim(x-\xi)f_1(x)$, where $f_1(x)$ is another polynomial. The solutions of $x^p\equiv x$ are all the residues of p; hence $x^p-x\sim x(x+1)(x+2)\dots(x+p-1)$, where the right-hand expression is the product of all the linear functions which are prime to p. A generalization of this is contained in the formula

$$x(x^{p^{m}-1}-1)\sim\Pi f(x)\pmod{p}$$

where the product includes every prime function $f(x)$ of which the degree is a factor of m. By a process similar to that employed in finding the equation satisfied by primitive mth roots of unity, we can find an expression for the product of all prime functions of a given degree m, and prove that their number is $(m>1)$

$$\frac{1}{m}(p^m-\Sigma p^{m/a}+\Sigma p^{m/ab}-\dots)$$

where $a, b, c\dots$ are the different prime factors of m. Moreover, if F is any given function, we can find a resolution

$$F\sim cF_1F_2\dots F_m\pmod{p}$$

where c is numerical, F_1 is the product of all prime linear functions which divide F, F_2 is the product of all the prime quadratic factors, and so on.

65. By the functional congruence $\phi(x)\equiv\psi(x)\pmod{p, f(x)}$ is meant that polynomials U, V can be found such that $\phi(x)=\psi(x)+pU+Vf(x)$ identically. We might also write $\phi(x)\sim\psi(x)\pmod{p, f(x)}$; but this is not so necessary here as in the preceding case of a simple modulus. Let m be the degree of $f(x)$; without loss of generality we may suppose that the coefficient of x^m is unity, and it will be further assumed that $f(x)$ is a prime function, mod p. Whatever the dimensions of $\phi(x)$, there will be definite functions $\chi(x)$, $\phi_1(x)$ such that $\phi(x)=f(x)\chi(x)+\phi_1(x)$ where $\phi_1(x)$ is of lower dimension than $f(x)$; moreover, we may suppose $\phi_1(x)$ replaced by the equivalent reduced function $\phi_2(x)$ mod p. Finally then, $\phi\equiv\phi_2\pmod{p, f(x)}$ where ϕ_2 is a reduced function, mod p, of order not greater than $(m-1)$. If we put $p^m=n$, there will be in all (including zero) n residues to the compound modulus (p, f): let us denote these by $R_1, R_2,\dots R_n$. Then (cf. § 28) if we reject the one zero residue (R_n, suppose) and take any function ϕ of which the residue is not zero, the residues of $\phi R_1, \phi R_2,\dots\phi R_{n-1}$ will all be different, and we conclude that $\phi^{n-1}\equiv 1\pmod{p, f}$. Every function therefore satisfies $\phi^n\sim\phi\pmod{p, f}$; by putting $\phi=x$ we obtain the principal theorem stated in § 64.

A still more comprehensive theory of compound moduli is due to Kronecker; it will be sufficiently illustrated by a particular case. Let m be a fixed natural number; X, Y, Z, T assigned polynomials, with rational integral coefficients, in the independent variables x, y, z; and let U be any polynomial of the same nature as X, Y, Z, T. We may write $U\sim 0\pmod{m, X, Y, Z, T}$ to express the fact that there are integral polynomials M, X′, Y′, Z′, T′ such that

$$U=mM+X'X+Y'Y+Z'Z+T'T$$

identically. In this notation $U\sim V$ means that $U-V\sim 0$. The number of independent variables and the number of functions in the modulus are unrestricted; there may be no number m in the modulus, and there need not be more than one. This theory of Kronecker's is admirably adapted for the discussion of all algebraic problems of an arithmetical character, and is certain to attain a high degree of development.

It is worth mentioning that one of Gauss's proofs of the law of quadratic reciprocity (*Gött. Nachr.* 1818) involves the principle of a compound modulus.

66. *Forms of Higher Degree.*—Except for the case alluded to at the end of § 55, the theory of forms of the third and higher degree is still quite fragmentary. C. Jordan has proved that the class number is finite. H. Poincaré has discussed the classification of ternary and quaternary cubics. With regard to the ternary cubic it is known that from any rational solution of $f=0$ we can deduce another by a process which is equivalent to finding the tangential of a point (x_1, y_1, z_1) on the curve, that is, the point where the tangent at (x_1, y_1, z_1) meets the curve again. We thus obtain a series of solutions (x_1, y_1, z_1), (x_2, y_2, z_2), &c., which may or may not be periodic. E. Lucas and J. J. Sylvester have proved that for certain cubics $f=0$ has no rational solutions; for instance $x^3+y^3-Az^3=0$ has rational solutions only if $A=ab(a+b)/c^3$, where a, b, c are rational integers. Waring asserted that every natural number can be expressed as the sum of not more than 9 cubes, and also as the sum of not more than 19 fourth powers; these propositions have been neither proved nor disproved.

67.. *Results derived from Elliptic and Theta Functions.*—For the sake of reference it will be convenient to give the expressions for the four Jacobian theta functions. Let ω be any complex quantity such that the real part of $i\omega$ is negative; and let $q=e^{\pi i\omega}$. Then

$$\theta_{00}(v)=\sum_{-\infty}^{+\infty}q^{n^2}e^{2n\pi iv}=1+2q\cos 2\pi v+2q^4\cos 4\pi v+2q^9\cos 6\pi v+\dots$$

$$=\prod_{1}^{\infty}(1-q^{2n})(1+2q^{2n-1}\cos 2\pi v+q^{4n-2}),$$

$$\theta_{01}(v)=1-2q\cos 2\pi v+2q^4\cos 4\pi v-2q^9\cos 6\pi v+\dots$$

$$=\prod_{1}^{\infty}(1-q^{2n})(1-2q^{2n-1}\cos 2\pi v+q^{4n-2}),$$

$$\theta_{10}(v)=2q^{\frac{1}{4}}\cos\pi v+2q^{\frac{9}{4}}\cos 3\pi v+2q^{\frac{25}{4}}\cos 5\pi v+\dots$$

$$=2q^{\frac{1}{4}}\cos\pi v\prod_{1}^{\infty}(1-q^{2n})(1+2q^{2n}\cos 2\pi v+q^{4n}),$$

$$\theta_{11}(v)=2q^{\frac{1}{4}}\sin\pi v-2q^{\frac{9}{4}}\sin 3\pi v+2q^{\frac{25}{4}}\sin 5\pi v-\dots$$

$$=2q^{\frac{1}{4}}\sin\pi v\prod_{1}^{\infty}(1-q^{2n})\,(1-2q^{2n}\cos 2\pi v+q^{4n}).$$

Instead of $\theta_{00}(0)$, &c., we write θ_{00}, &c. Clearly $\theta_{11}=0$; we have the important identities

$$\theta_{11}'=\pi\theta_{00}\theta_{10}\theta_{01}\qquad\theta_{00}^4=\theta_{01}^4+\theta_{10}^4$$

where θ_{11}' means the value of $d\theta_{11}(v)/dv$ for $v=0$. If, now, we put

$$\sqrt{\kappa}=\frac{\theta_{10}}{\theta_{00}},\quad\sqrt{\kappa'}=\frac{\theta_{01}}{\theta_{00}},\quad u=\pi\theta_{00}^2v,$$

so that $\kappa^2+\kappa'^2=1$, we shall have

$$\frac{\theta_{11}(v)}{\theta_{01}(v)}=\sqrt{\kappa}\cdot\operatorname{sn} u,\ \frac{\theta_{10}(v)}{\theta_{01}(v)}=\sqrt{\frac{\kappa}{\kappa'}}\cdot\operatorname{cn} u,\frac{\theta_{00}(v)}{\theta_{01}(v)}=\frac{1}{\sqrt{\kappa'}}\cdot\operatorname{dn} u,$$

and, supposing for simplicity that $i\omega$ is a real negative quantity,

$$\pi\theta_{00}{}^2=2\mathrm{K},\quad \omega\pi\theta_{00}{}^2=2i\mathrm{K}',\quad \omega=i\mathrm{K}'/\mathrm{K},$$

the notation being that which is now usual for the elliptic functions. It is found that

$$\frac{\kappa\mathrm{K}}{\pi}\operatorname{sn}2\mathrm{K}u=2\sum_{1}^{\infty}\frac{q^{s-\frac{1}{2}}}{1-q^{2s-1}}\sin(2s-1)\pi u,$$

$$\frac{\kappa\mathrm{K}}{\pi}\operatorname{cn}2\mathrm{K}u=2\sum_{1}^{\infty}\frac{q^{s-\frac{1}{2}}}{1-q^{2s-1}}\cos(2s-1)\pi u,$$

$$\frac{\mathrm{K}}{\pi}\operatorname{dn}2\mathrm{K}u=\tfrac{1}{2}+2\sum_{1}^{\infty}\frac{q^{s}}{1+q^{2s}}\cos 2s\pi u.$$

From the last formula, by putting $u=0$, we obtain

$$1+4\sum_{1}^{\infty}\frac{q^{s}}{1+q^{2s}}=\frac{2\mathrm{K}}{\pi}=\theta_{00}{}^2(1+2q+2q^4+2q^{\rho}+\ldots)^2,$$

and hence, by expanding both sides in ascending powers of q, and equating the coefficients of q^n, we arrive at a formula for the number of ways of expressing n as the sum of two squares. If δ is any odd divisor of n, including 1 and n itself if n is odd, we find as the coefficient of q^n in the expansion of the left-hand side $4\Sigma(-1)^{\frac{1}{2}(\delta-1)}$; on the right-hand side the coefficient enumerates all the solutions $n=(\pm x)^2+(\pm y)^2$, taking account of the different signs (except for 0^2) and of the order in which the terms are written (except when $x^2=y^2$). Thus if n is an odd prime of the form $4k+1$, $\Sigma(-1)^{\frac{1}{2}(\delta-1)}=2$, and the coefficient of q^n is 8, which is right, because the one possible composition $n=a^2+b^2$ may be written $n=(\pm a)^2+(\pm b)^2=(\pm b)^2+(\pm a)^2$, giving eight representations.

By methods of a similar character formulae can be found for the number of representations of a number as the sum of 4, 6, 8 squares respectively. The four-square theorem has been stated in § 41; the eight-square theorem is that the number of representations of a number as the sum of eight squares is sixteen times the sum of the cubes of its factors, if the given number is odd, while for an even number it is sixteen times the excess of the cubes of the even factors above the cubes of the odd factors. The five-square and seven-square theorems have not been derived from q-series, but from the general theory of quadratic forms.

68. Still more remarkable results are deducible from the theory of the transformation of the theta functions. The elementary formulae are

$$\theta_{11}(u,\omega+1)=e^{\pi i/4}\theta_{11}(u,\omega),\quad \theta_{10}(u,\omega+1)=e^{\pi i/4}\theta_{10}(u,\omega),$$
$$\theta_{01}(u,\omega+1)=\theta_{00}(u,\omega),\qquad \theta_{00}(u,\omega+1)=\theta_{01}(u,\omega),$$

$$e^{-\pi iu^2/\omega}\theta_{11}\left(\frac{u}{\omega},\ -\frac{1}{\omega}\right)=-i\sqrt{-i\omega}\,\theta_{11}(u,\omega),$$

$$e^{-\pi iu^2/\omega}\theta_{10}\left(\frac{u}{\omega},\ -\frac{1}{\omega}\right)=\sqrt{-i\omega}\,\theta_{10}(u,\omega),$$

$$e^{-\pi iu^2/\omega}\theta_{10}\left(\frac{u}{\omega},\ -\frac{1}{\omega}\right)=\sqrt{-i\omega}\,\theta_{01}(u,\omega),$$

$$e^{-\pi iu^2/\omega}\theta_{00}\left(\frac{u}{\omega},\ -\frac{1}{\omega}\right)=\sqrt{-i\omega}\,\theta_{00}(u,\omega),$$

where $\sqrt{-i\omega}$ is to be taken in such a way that its real part is positive. Taking the definition of κ given in § 67, and considering κ as a function of ω, we find

$$\kappa(\omega+1)=i\theta_{10}{}^2/\theta_{01}{}^2=i\kappa(\omega)/\kappa'(\omega),$$
$$\kappa\left(-\frac{1}{\omega}\right)=\theta_{01}{}^2/\theta_{00}{}^2=\kappa'(\omega).$$

For convenience let $\kappa^2(\omega)=\sigma$: then the substitutions $(\omega,\omega+1)$ and $(\omega,-\omega^{-1})$ convert σ into $\sigma/(\sigma-1)$ and $(1-\sigma)$ respectively. Now if $\alpha,\beta,\gamma,\delta$ are any real integers such that $\alpha\delta-\beta\gamma=1$, the substitution $[\omega,(\alpha\omega+\beta)/(\gamma\omega+\delta)]$ can be compounded of $(\omega,\omega+1)$ and $(\omega,-\omega^{-1})$; the effect on σ will be the same as if we apply a corresponding substitution compounded of $[\sigma,\ \sigma/(\sigma-1)]$ and $[\sigma,\ 1-\sigma]$. But these are periodic and of order 3, 2 respectively]; therefore we cannot get more than six values of σ, namely

$$\sigma,\ 1-\sigma,\ \frac{\sigma}{\sigma-1},\ \frac{1}{1-\sigma},\ \frac{\sigma-1}{\sigma},\ \frac{1}{\sigma},$$

and any symmetrical function of these will have the same value at any two equivalent places in the modular dissection (§ 33). Their sum is constant, but the sum of their squares may be put into the form

$$\frac{2(\sigma^2-\sigma+1)^3}{\sigma^2(\sigma-1)^2}-3;$$

hence $(\sigma^2-\sigma+1)^3\div\sigma^2(\sigma-1)^2$ has the same value at equivalent places. F. Klein writes

$$\mathrm{J}=\frac{4(\tau^2-\sigma+1)^3}{27\sigma^2(\sigma-1)^2};$$

this is a transcendental function of ω, which is a special case of a Fuchsian or automorphic function. It is an analytical function of q^2, and may be expanded in the form

$$\mathrm{J}=\frac{1}{1728}\{q^{-2}+744+c_1q^2+c_2q^4+\ldots\}$$

where c_1, c_2, &c., are rational integers.

69. Suppose, now, that a, b, c, d are rational integers, such that $\mathrm{dv}(a,b,c,d)=1$ and $ad-bc=n$, a positive integer. Let $(a\omega+b)/(c\omega+d)=\omega'$; then the equation $\mathrm{J}(\omega')=\mathrm{J}(\omega)$ is satisfied if and only if $\omega'\sim\omega$, that is, if there are integers $\alpha,\beta,\gamma,\delta$ such that $\alpha\delta-\beta\gamma=1$, and

$$(a\omega+b)(\gamma\omega+\delta)-(c\omega+d)(\alpha\omega+\beta)=0.$$

If we write $\psi(n)=n\Pi(1+p^{-1})$, where the product extends to all prime factors (p) of n, it is found that the values of ω fall into $\psi(n)$ equivalent sets, so that when ω is given there are not more than $\psi(n)$ different values of $\mathrm{J}(\omega')$. Putting $\mathrm{J}(\omega')=\mathrm{J}'$, $\mathrm{J}(\omega)=\mathrm{J}$, we have a modular equation

$$f_1(\mathrm{J}',\mathrm{J})=0$$

symmetrical in J, J′, with integral coefficients and of degree $\psi(n)$. Similarly when $\mathrm{dv}(a,b,c,d)=\tau$ we have an equation $f_\tau(\mathrm{J}',\mathrm{J})=0$ of order $\psi(n/\tau^2)$; hence the complete modular equation for transformations of the nth order is

$$\mathrm{F}(\mathrm{J}',\mathrm{J})=\Pi f_\tau(\mathrm{J}',\mathrm{J})=0,$$

the degree of which is $\Phi(n)$, the sum of the divisors of n.

Now if in F(J′, J) we put J′ = J, the result is a polynomial in J alone, which we may call G(J). To every linear factor of G corresponds a class of quadratic forms of determinant (κ^2-4n) where $\kappa^2<4n$ and κ is an integer or zero: conversely from every such form we can derive a linear factor $(\mathrm{J}-a)$ of G. Moreover, if with each form we associate its weight (§ 41) we find that with the notation of § 39 the degree of G is precisely $\Sigma\mathrm{H}(4n-\kappa^2)-\epsilon_n$, where $\epsilon_n=1$ when n is a square, and is zero in other cases. But this degree may be found in another way as follows. A complete representative set of transformations of order n is given by $\omega'=(a\omega+b)/d$, with $ad=n$, $0\leqq b<d$; hence

$$\mathrm{G}(\mathrm{J})=\Pi\left\{\mathrm{J}(\omega)-\mathrm{J}\left(\frac{a\omega+b}{d}\right)\right\},$$

and by substituting for $\mathrm{J}(\omega)$ and $\mathrm{J}\left(\frac{a\omega+b}{d}\right)$ their values in terms of q, we find that the lowest term in the factor expressed above is either $q^{-2}/1728$ or $q^{-2a/d}/1728$, or a constant, according as $a<d$, $a>d$ or $a=d$. Hence if ν is the order of G(J), so that its expansion in q begins with a term in $q^{-2\nu}$ we must have

$$\nu=\sum_{d>\sqrt{n}}(1\cdot d)+\sum_{d>\sqrt{n}}\left(\frac{a}{d}\cdot d\right)=\sum_{d>\sqrt{n}}d+\sum_{a>\sqrt{n}}a$$
$$=2\Sigma d$$

extending to all divisors of n which exceed $\sqrt{n}$. Comparing this with the other value, we have

$$\sum_{\kappa}\mathrm{H}(4n-\kappa^2)=2\sum_{d>\sqrt{n}}d+\epsilon_n=\Phi(n)+\Psi(n),$$

as stated in § 39.

70. Each of the singular moduli which are the roots of G(J) = 0 corresponds to exactly one primitive class of definite quadratic forms, and conversely.

Corresponding to every given negative determinant $-\Delta$ there is an irreducible equation $\psi(j)=0$, where $j=1728\mathrm{J}$, the coefficients of which are rational integers, and the degree of which is $h(-\Delta)$. The coefficient of the highest power of j is unity, so that j is an arithmetical integer, and its conjugate values belong one to each primitive class of determinant $-\Delta$. By adjoining the square roots of the prime factors of Δ the function $\psi(j)$ may be resolved into the product of as many factors as there are genera of primitive classes, and the degree of each factor is equal to the number of classes in each genus. In particular, if $\{1,\ 1,\ \frac{1}{4}(\Delta+1)\}$ is the only reduced form for the determinant $-\Delta$, the value of j is a real negative rational cube. At the same time its approximate value is $\exp\left[-2\pi i\cdot\frac{1+i\sqrt{\Delta}}{2}\right]+744=744-e^{\pi\sqrt{\Delta}}$, so that, approximately, $e^{\pi\sqrt{\Delta}}=m^3+744$ where m is a rational integer. For instance $e^{\pi\sqrt{43}}=884736743\cdot9997775\ldots=960^3+744$ very nearly, and for the class (1, 1, 11) the exact value of j is -960^3. Four and only four other similar determinants are known to exist, namely −11, −19, −67, −163, although thousands have been classified. According to Hermite the decimal part of $e^{\pi\sqrt{163}}$ begins with twelve nines; in this case Weber has shown that the exact value of j is $-2^{18}\cdot3^3\cdot5^3\cdot23^3\cdot29^3$.

71. The function $j(\omega)$ is the most fundamental of a set of quantities called *class-invariants*. Let (a, b, c) be the representative of any class of definite quadratic forms, and let ω be the root of $ax^2+bx+c=0$ which has a positive imaginary part; then $\mathrm{F}(\omega)$ is said to be a class-invariant for (a, b, c) if $\mathrm{F}\left(\frac{\alpha\omega+\beta}{\gamma\omega+\delta}\right)=\mathrm{F}(\omega)$ for all real integers α β,γ,δ such that $\alpha\delta-\beta\gamma=1$. This is true for $j(\omega)$ whatever ω may be, and it is for this reason that j is so fundamental. But, as will be seen from the above examples, the value of j soon becomes so large that its calculation is impracticable. Moreover, there is the difficulty of constructing the modular equation $f_1(\mathrm{J},\mathrm{J}')=0$ (§69), which

has only been done in the cases when $n=2, 3$ (the latter by Smith in *Proc. Lond. Math. Soc.* ix. p. 242).

For moderate values of Δ the difficulty can generally be removed by constructing algebraic functions of j. Suppose we have an irreducible equation

$$x^m+c_1x^{m-1}+\ldots+c_m=0,$$

the coefficients of which are rational functions of $j(\omega)$. If we apply any modular substitution $\omega'=S(\omega)$, this leaves the equation unaltered, and consequently only permutates the roots among themselves: thus if $x_1(\omega)$ is any definite root we shall have $x_1(\omega')=x_i(\omega)$, where i may or may not be equal to 1. The group of unitary substitutions which leave all the roots unaltered is a factor of the complete modular group. If we put $y=x(n\omega)$, y will satisfy an equation similar to that which defines x, with j' written for j; hence, since j, j' are connected by the equation $f_1(j, j')=0$, there will be an equation $\psi(x, y)=0$ satisfied by x and y. By suitably choosing x we can in many cases find $\psi(x, y)$ without knowing $f_1(j, j')$; and then the equation $\psi(x, x)=0$ defines a set of singular moduli, each one of which belongs to a certain value of ω and all the quantities derived from it by the substitutions which leave $x(\omega)$ unaltered.

As one of the simplest examples, let $n=2$, $x^3-j(\omega)=y^3-j(\omega')=0$. Then the equation connecting x, y in its complete form is of the ninth degree in each variable; but it can be proved that it has a rational factor, namely

$$y^3-x^2y^2+495xy+x^3-2^4\cdot 3^3\cdot 5^3=0,$$

and if in this we put $x=y=u$, the result is

$$u^4-2u^3-495u^2+2^4.3^3.5^3=0,$$

the roots of which are 12, 20, −15, −15. It remains to find the values of ω, to which they belong. Writing $\gamma_2(\omega)=\sqrt[3]{j}$, it is found that we may define γ_2 in such a way that $\gamma_2(\omega+1)=e^{-2\pi i/3}\gamma_2(\omega)$, $\gamma_2(-\omega^{-1})=\gamma_2(\omega)$, whence it is found that

$$\gamma_2\left(\frac{a\omega+\beta}{\gamma\omega+\delta}\right)=e^{-\frac{2\pi i}{3}(\gamma\delta+\gamma a+\beta\delta-\beta\delta\gamma^2)}\gamma_2(\omega).$$

We shall therefore have $\gamma_2(2\omega)=\gamma_2(\omega)$ for all values of such that

$$2\omega=\frac{a\omega+\beta}{\gamma\omega+\delta}, a\delta-\beta\gamma=1,\ \gamma\delta+\gamma a+\beta\delta-\beta\delta\gamma^2\equiv 0 \pmod 3.$$

Putting $(a, \beta, \gamma, \delta)=(0, -1, 1, 0)$ the conditions are satisfied, and $2\omega=i\sqrt{2}$. Now $j(i)=1728$, so that $\gamma_2(i)=12$; and since $j(\omega)$ is positive for a pure imaginary, $\gamma_2(i\sqrt{2})=20$. The remaining case is settled by putting

$$\frac{\omega}{2}=\frac{a\omega+\beta}{\gamma\omega+\delta},$$

with a, β, γ, δ satisfying the same conditions as before. One solution is $(-1, 2, 1, 1)$ and hence $\omega^2+3\omega+4=0$, so that $\gamma_2\left(\frac{-3+i\sqrt{7}}{2}\right)=-15$.

Besides γ_2, other irrational invariants which have been used with effect are $\gamma_3=\sqrt{(j-1728)}$, the moduli κ, κ', their square and fourth roots, the functions f, f_1, f_2 defined by

$$f=2^{\frac{1}{6}}(\kappa\kappa')^{-\frac{1}{12}},\ f_1=\sqrt[4]{\kappa'}\,.f,\ f_2=\sqrt[4]{\kappa}.f,$$

and the function $\eta(n\omega)/\eta(\omega)$ where $\eta(\omega)$ is defined by

$$\eta(\omega)=q^{\frac{1}{12}}\sum_{-\infty}^{+\infty}(-1)^s q^{3s^2+s}=\frac{1}{\sqrt{3}}\theta_{11}\left(\frac{2}{3},\frac{\omega}{3}\right)=q^{\frac{1}{12}}\prod_{1}^{\infty}(1-q^{2s}).$$

72. Another powerful method, developed by C. F. Klein and K. E. R. Fricke, proceeds by discussing the deficiency of $f_1(j, j')=0$ considered as representing a curve. If this deficiency is zero, j and j' may be expressed as rational functions of the same parameter, and this replaces the modular equation in the most convenient manner. For instance, when $n=7$, we may put

$$j=\frac{(\tau^2+13\tau+49)(\tau^2+5\tau+1)^3}{\tau}=\phi(\tau),\ j'=\phi(\tau'),$$

$$\tau\tau'=49.$$

The corresponding singular moduli are found by solving $\phi(\tau)=\phi(\tau')$. For deficiency 1 we may find in a similar way two auxiliary functions x, y connected by some simple equation $\psi(x, y)=0$ not exceeding the fourth degree, and such that j, j' are each rational functions of x and y.

Hurwitz has extended this field of research almost indefinitely, not only by generalising the formulae for class-number sums, such as that in § 69, but also by bringing the modular-function theory into connexion with that of algebraic correspondence and Abelian integrals. A comparatively simple example may help to indicate the nature of these researches. From the formulae given at the beginning of § 67, we can deduce, by actual multiplication of the corresponding series,

$$\frac{1}{\pi}\theta'_{11}\theta_{00}=\theta^2_{00}\theta_{01}\theta_{10}=\sum_{-\infty}^{+\infty}\left(\frac{-1}{\xi}\right)|\xi|q^{\xi^2/4}\times\sum_{-\infty}^{+\infty}q^{\eta^2}\quad\left[\begin{matrix}\xi=\pm 1, \pm 3, \ldots\ ;\\ \eta=0,\ \pm 1,\ \pm 2, \ldots\end{matrix}\right.$$

$$=\Sigma\chi(m)q^{m/4}\qquad [m=1, 5, 9, \ldots$$

where

$$\chi(m)=\Sigma\left(\frac{-1}{\xi}\right)|\xi|$$

extended over all the representations $m=\xi^2+4\eta^2$. In a similar way

$$\frac{1}{\pi}\theta'_{11}\theta_{10}=\theta_{00}\theta_{10}^2\theta_{01}=2\Sigma(-1)^{\frac{1}{4}(m-1)}\chi(m)q^{m/2}$$

$$\frac{1}{\pi}\theta'_{11}\theta_{01}=\theta_{00}\theta_{10}\theta_{01}^2=\Sigma(-1)^{\frac{1}{4}(m-1)}\chi(m)q^{m/4}$$

If, now, we write

$$j_1(\omega)=\Sigma\frac{(-1)^{\frac{1}{4}(m-1)}\chi(m)}{m}q^{m/2},\quad j_2(\omega)=2\Sigma\frac{(-1)^{\frac{1}{4}(m-1)}\chi(m)}{m}q^{m/4},$$

$$j_3(\omega)=2\Sigma\frac{\chi(m)}{m}q^{m/4}$$

we shall have

$$dj_1:dj_2:dj_3=\theta_{10}:\theta_{01}:\theta_{00}$$

where $\theta_{10}, \theta_{01}, \theta_{00}$, are connected by the relation (§ 67)

$$\theta_{10}^4+\theta_{01}^4-\theta_{00}^4=0$$

which represents, in homogeneous co-ordinates, a quartic curve of deficiency 3. For this curve, or any equivalent algebraic figure, $j_1(\omega)$, $j_2(\omega)$ and $j_3(\omega)$ supply an independent set of Abelian integrals of the first kind. If we put $x=\sqrt{\kappa}$, $y=\sqrt{\kappa'}$, it is found that

$$\int\frac{dx}{y^3}=\tfrac{1}{2}j_3(\omega),\quad \int\frac{dx}{y^3}=\tfrac{1}{2}j_2(\omega),\quad \int\frac{xdx}{y^3}=\tfrac{1}{2}j_1(\omega),$$

so that the integrals which the algebraic theory gives in connexion with $x^4+y^4-1=0$ are directly identified with $j_1(\omega)$, $j_2(\omega)$, $j_3(\omega)$, provided that we put $x=\sqrt{\kappa(\omega)}$.

Other functions occur in this theory analogous to $j_1(\omega)$, but such that in the q-series which are the expansions of them the coefficients and exponents depend on representations of numbers by quaternary quadratic forms.

73. In the *Berliner Sitzungsberichte* for the period 1883–1890, L. Kronecker published a very important series of articles on elliptic functions, which contain many arithmetical results of extreme elegance; some of these Kronecker had announced without proof many years before. A few will be quoted here, without any attempt at demonstration; but in order to understand them, it will be necessary to bear in mind two definitions. The first relates to the Legendre-Jacobi symbol $\left(\frac{a}{b}\right)$. If a, b have a common factor we put $\left(\frac{a}{b}\right)=0$; while if a is odd and $b=2^hc$, where c is odd, we put $\left(\frac{a}{b}\right)=\left(\frac{2^h}{a}\right)\left(\frac{a}{c}\right)$. The other definition relates to the classification of discriminants of quadratic forms. If D is any number that can be such a discriminant, we must have $D\equiv 0$ or $1 \pmod 4$, and in every case we can write $D=D_0Q^2$, where Q^2 is a square factor of D, and D_0 satisfies one of the following conditions, in which P denotes a product of different odd primes:—

$D_0=P$, with $P\equiv 1 \pmod 4$
$D_0=4P$, $\qquad P\equiv -1 \pmod 4$
$D_0=8P$, $\qquad P\equiv \pm 1 \pmod 4$.

Numbers such as D_0 are called *fundamental discriminants*; every discriminant is uniquely expressible as the product of a fundamental discriminant and a positive integral square.

Now let D_1, D_2 be any two discriminants, then D_1D_2 is also a discriminant, and we may put $D_1D_2=D=D_0Q^2$, where D_0 is fundamental: this being done, we shall have

$$\tau\sum_{h=1}^{h=\infty}\sum_{k=1}^{k=\infty}\left(\frac{D_1Q^2}{h}\right)\left(\frac{D_2Q^2}{k}\right)F(hk)$$

$$=\tfrac{1}{2}\sum_{a,b,c}\left[\left(\frac{D_1}{A}\right)+\left(\frac{D_2}{A}\right)\right]\sum_{m,n}\left(\frac{Q^2}{m}\right)F(am^2+bmn+cn^2)$$

where we are to take $h, k=1, 2, 3, \ldots+\infty$; $m, n=0, \pm 1, \pm 2, \ldots \pm\infty$ except that, if $D<0$, the case $m=n=0$ is excluded, and that, if $D>0$, $(2am+bn)T \gtrless nU$ where (T, U) is the least positive solution of $T^2-DU^2=4$. The sum $\sum\limits_{a,b,c}$ applies to a system of representative primitive forms (a, b, c) for the determinant D, chosen so that a is prime to Q, and b, c are each divisible by all the prime factors of Q. A is any number prime to 2D and representable by (a, b, c); and finally $\tau=2, 4, 6, 1$ according as $D<-4$, $D=-4$, $D=-3$ or $D>0$. The function F is quite arbitrary, subject only to the conditions that $F(xy)=F(x)F(y)$, and that the sums on both sides are convergent. By putting $F(x)=x^{-1-\rho}$, where ρ is a real positive quantity, it can be deduced from the foregoing that, if D_2 is not a square, and if D_1 is different from 1,

$$\tau H(D_1Q^2)H(D_2Q^2)=\operatorname*{Lt}_{\rho=0}\sum_{a,b,c}\left(\frac{D_1}{A}\right)\sum_{m,n}\left(\frac{Q^2}{m}\right)(am^2+bmn+cn^2)^{-1-\rho}$$

where the function $H(d)$ is defined as follows for any discriminant d:—

$$d=-\Delta<0\qquad \tau H(d)=\frac{2\pi}{\sqrt{\Delta}}h(-\Delta)$$

$$d>0\qquad H(d)=\frac{h(d)}{2\sqrt{d}}\log\frac{T+U\sqrt{d}}{T-U\sqrt{d}}$$

$h(d)$ meaning the number of primitive forms for the determinant d. This is a generalisation of a theorem due to Dirichlet.

Thert is another formula which, in a certain sense, is the generalisation of Gauss's sums (§ 62) in cyclotomy. Let $\psi(u, v)$ denote the function $\theta_{11}(u+v) \div \theta_{01}(u)\theta_{01}(v)$ and let D_1, D_2 be any two fundamental discriminants such that D_1D_2 is also fundamental and negative: then

$$\frac{\tau\theta'_{11}}{2\pi\,|\sqrt{D_1D_2}|}\sum_{s_1,s_2}\left(\frac{D_1}{s_1}\right)\left(\frac{D_2}{s_2}\right)\psi\left(\frac{2s_1}{|D_1|},\frac{2s_2}{|D_2|}\right)$$

$$=\sum_{a,\,b,\,c}\left[\left(\frac{D_1}{A}\right)+\left(\frac{D_2}{A}\right)\right]\sum_{m,\,n} q^{\frac{1}{2}(am^2+bmn+cn^2)}$$

where, on the left-hand side, we are to sum for $s_i = 1, 2, 3 \ldots |D_i|$; and on the right we are to take a complete set of iepresentative piimitive forms (a, b, c) for the determinant D_1D_2, and give to m, n all positive and negative integral values such that $am^2+bmn+cn^2$ is odd. The quantity τ is 2, if $D_1D_2 < -4$, $\tau=4$ if $D_1D_2=-4$, $\tau=6$ if $D_1D_2=-3$. By putting $D_2=1$, we obtain, after some easy transformations,

$$\sum_{s=1}^{s=\Delta}\left(\frac{-\Delta}{s}\right)\operatorname{sn}\frac{4sK}{\Delta}=\frac{4\sqrt{\Delta}}{\tau\theta_{10}{}^2}\Sigma\Sigma q^{\frac{1}{2}(am^2+bmn+cn^2)},$$

which holds for any fundamental discriminant $-\Delta$. For instance, taking $\omega=iK'/K$, and $\Delta=3$, we have $\theta_{10}{}^2=2\kappa K/\pi$, and $\Sigma q^{\frac{1}{2}(m^2+mn+n^2)}=\frac{2\kappa K\sqrt{3}}{\pi}\operatorname{sn}\frac{4K}{3}$; a verification is afforded by making 2K approach the value π, in which case q, κ vanish, while the limit of $q^{\frac{1}{2}}/\kappa$ is $\frac{1}{4}$, whence the limiting value of $\operatorname{sn}\frac{4K}{3}$ is that of $6q^{\frac{1}{2}}/\kappa\sqrt{3}$, which $=6/4\sqrt{3}=\sqrt{3}/2$, as it should be.

Several of Kronecker's formulae connect the solution of the Pellian equation with elliptic modular functions: one example may be given here. Let D be a positive discriminant of the form $8n+5$, let (T, U) be the least solution of $T^2-DU^2=1$: then, if $h(D)$ is the number of primitive classes for the determinant D,

$$(T-U\sqrt{D})^{h(D)}=\Pi(2\kappa\kappa')^2$$

where the product on the right extends to a certain sixth part of those values of $2\kappa\kappa'$ which are singular, and correspond to the field $\Omega(\sqrt{-D})$, or in other words are connected with the class invariant $j(\sqrt{-D})$. For instance, if $D=5$, the equation to find $(\kappa\kappa')^2$ is

$$4.\delta\{(\kappa\kappa')^2-1\}^3+(25+13\sqrt{5})^3(\kappa\kappa')^4=0$$

one root of which is given by $(2\kappa\kappa')^2=9-4\sqrt{5}=T-U\sqrt{5}$ which is right, because in this case $h(D)=1$.

74. *Frequency of Primes.*—The distribution of primes in a finite interval $(a, a+b)$ is very irregular, if we change a and keep b constant. Thus if we put $n!=\mu$, the numbers $\mu+2$, $\mu+3, \ldots (\mu+n-1)$ are all composite, so that we can form a run of consecutive composite numbers as extensive as we please; on the other hand, there is possibly no limit to the number of cases in which p and $p+2$ are both primes. Legendre was the first to find an approximate formula for $F(x)$, the number of primes not exceeding x. He found by induction

$$F(x)=x\div(\log_e x-1{\cdot}08366)$$

which answers fairly well when x lies between 100 and 1,000,000, but becomes more and more inaccurate as x increases. Gauss found, by theoretical considerations (which, however, he does not explain), the approximate formula

$$F(x)=L(x)=\int_2^x\frac{dx}{\log x}$$

(where, as in all that follows, log x is taken to the base e). This value is ultimately too large, but when x exceeds a million it is nearer the truth than the value given by Legendre's formula.

By a singularly profound and original analysis, Riemann succeeded in finding a formula, of the same type as Gauss's, but more exact for very large values of x. In its complete form it is very complicated; but, by omitting terms which ultimately vanish (for sufficiently large values of x) in comparison with those retained, the formula reduces to

$$F(x)=A+\sum_m(-1)^\mu\frac{1}{m}L(x^{1/m})\quad(m=1, 2, 3, 5, 6, 7, 11, \ldots)$$

where the summation extends to all positive integral values of m which have no square factor, and μ is the number of different prime factors of m, with the convention that when $m=1$, $(-1)^\mu=1$. The symbol A denotes a constant, namely

$$A=\Sigma\frac{(-1)^\mu}{m}\times\left\{\frac{1}{2}-\int_2^\infty\frac{dx}{x(x^2-1)\log x}\right\}$$

and L is used in the sense given above.

P. L. Tchébichev obtained some remarkable results on the frequency of primes by an ingenious application of Stirling's theorem. One of these is that there will certainly be $(k+1)$ primes between a and b, provided that

$$a<\frac{5b}{6}-2\sqrt{b}-\frac{16}{25}R\log 6\,(\log b)^2-\frac{5}{24R}(4k+25)-\frac{25}{6R}$$

where $R=\frac{1}{2}\log 2+\frac{1}{3}\log 3+\frac{1}{5}\log 5-\frac{1}{30}\log 30=0{\cdot}921292\ldots$. From this may be inferred the truth of Bertrand's conjecture that there is always at least one prime between a and $(2a-2)$ if $2a>7$. Tchébichev's results were generalized and made more precise by Sylvester.

The actual calculation of the number of primes in a given interval may be effected by a formula constructed and used by D. F. E Meissel. The following table gives the values of $F(n)$ for various values of n, according to Meissel's determinations:—

n	$F(n)$
20,000	2,262
100,000	9,592
500,000	41,538
1,000,000	78,498

Riemann's analysis mainly depends upon the properties of the function

$$\zeta(s)=\sum_n n^{-s}\qquad(n=1, 2, 3, \ldots),$$

considered as a function of the complex variable s. The above definition is only valid when the real part of s exceeds 1; but it can be generalized by writing

$$2\sin\pi z\Gamma(z)\zeta(z)=i\int_\infty^\infty\frac{(-x)^{z-1}dx}{e^x-1}$$

where the integral is taken from $x=+\infty$ along the axis of real quantities to $x=\epsilon$, where ϵ is a very small positive quantity, then round a circle of radius ϵ and centre at the origin, and finally from $x=\epsilon$ to $x=+\infty$ along the axis of real quantities. This function $\zeta(z)$ is of great importance, and has been recently studied by von Mangoldt Landau and others.

Reference has already been made to the fact that if l, m are coprimes the linear form $lx+m$ includes an infinite number of primes. Now let (a, b, c) be any primitive quadratic form with a total generic character C; and let $lx+m$ be a primitive linear form chosen so that all its values have the character C. Then it has been proved by Weber and Meyer that (a, b, c) is capable of representing an infinity of primes all of the linear form $lx+m$.

75. *Arithmetical Functions.*—This term is applied to symbols such as $\phi(n)$, $\Phi(n)$, &c., which are associated with n by an intrinsic arithmetical definition. The function $\Phi(n)$ was written $\int n$ by Euler, who investigated its properties, and by proving the formula $\prod_1^\infty(1-q^s)=\sum_{-\infty}^{+\infty}q^{\frac{1}{2}(3s^2+s)}$ deduced the result that

$$\int n=\int(n-1)+\int(n-2)-\int(n-5)-\ldots=\Sigma(-1)^{s-1}\int\left(n-\frac{3s^2\pm s}{2}\right)$$

where on the right hand we are to take all positive values of s such that $n-\frac{1}{2}(3s^2\pm s)$ is not negative, and to interpret $\int o$ as n, if this term occurs. J. Liouville makes frequent use of this function in his papers, but denotes it by $\zeta(n)$.

If the quantity x is positive and not integral, the symbol $E(x)$ or $[x]$ is used to denote the integer (including zero) which is obtained by omitting the fractional part of x; thus $E(\sqrt{2})=1$, $E(0{\cdot}7)=0$, and so on. For some purposes it is convenient to extend the definition by putting $E(-x)=-E(x)$, and agreeing that when x is a positive integer, $E(x)=x-\frac{1}{2}$; it is then possible to find a Fourier sine-series representing $x-E(x)$ for all real values of x. The function $E(x)$ has many curious and important properties, which have been investigated by Gauss, Hermite, Hacks, Pringsheim, Stern and others. What is perhaps the simplest proof of the law of quadratic reciprocity depends upon the fact that if p, q are two odd primes, and we put $p=2h+1$, $q=2k+1$

$$\sum_{r=1}^{r=h}E\left(\frac{rp}{q}\right)+\sum_{s=1}^{s=k}E\left(\frac{sp}{q}\right)=hk=\tfrac{1}{4}(p-1)(q-1)$$

the truth of which is obvious, if we rule a rectangle $p''\times q''$ into unit squares, and draw its diagonal. This formula is Gauss's, but the geometrical proof is due to Eisenstein. Another useful formula is

$$\sum_{r=1}^{r=m-1}E\left(x+\frac{r}{m}\right)=E(mx)-E(x),\text{ which is due to Hermite.}$$

Various other arithmetical functions have been devised for particular purposes; two that deserve mention (both due to Kronecker) are δ_{hk}, which means 0 or 1 according as h, k are unequal or equal, and sgn x, which means $x\div|x|$.

76. *Transcendental Numbers.*—It has been proved by Cantor that the aggregate of all algebraic numbers is countable. Hence immediately follows the proposition (first proved by Liouville) that there are numbers, both real and complex, which cannot be defined by any combination of a finite number of equations with rational integral coefficients. Such numbers are said to be transcendental. Hermite first completely proved the transcendent character of e; and Lindemann, by a similar method, proved the transcendence of π. Thus it is now finally established that the quadrature of the circle is impossible, not only by rule and compass, but even with the help of any number of algebraic curves of any order when the coefficients in their equations are rational (see Hermite, *C.R.* lxxvii., 1873, and Lindemann, *Math. Ann.* xx., 1882). Another number which is almost certainly transcendent is Euler's constant C. It may be convenient to give here the following numerical values:—

$$\begin{array}{lllll} \pi = 3{\cdot}14159 & 26535 & 89793 & 23846\ldots & \\ e = 2{\cdot}71828 & 18284 & 59045 & 23536\ldots & \\ C = 0{\cdot}57721 & 56649 & 01532 & 8606065\ldots & \text{(Gauss-Nicolai)} \end{array}$$

$$\log_{10} = (\pi \log_{10} e) = 0{\cdot}13493 \quad 41840\ldots \text{(Weber)},$$

the last of which is useful in calculating class-invariants.

77. *Miscellaneous Investigations.*—The foregoing articles (§§ 24-76) give an outline of what may be called the analytical theory of numbers, which is mainly the work of the 19th century, though many of the researches of Lagrange, Legendre and Gauss, as well as all those of Euler, fall within the 18th. But after all, the germ of this remarkable development is contained in what is only a part of the original Diophantine analysis, of which, beyond question, Fermat was the greatest master. The spirit of this method is still vigorous in Euler; but the appearance of Gauss's *Disquisitiones arithmeticae* in 1801 transformed the whole subject, and gave it a new tendency which was strengthened by the discoveries of Cauchy, Jacobi, Eisenstein and Dirichlet. In recent times Edouard Lucas revived something of the old doctrine, and it can hardly be denied that the Diophantine method is the one that is really germane to the subject. Even the strange results obtained from elliptic and modular functions must somehow be capable of purely arithmetical proof without the use of infinite series. Besides this, the older arithmeticians have announced various theorems which have not been proved or disproved, and made a beginning of theories which are still in a more or less rudimentary stage. As examples of the latter may be mentioned the partition of numbers (see NUMBERS, PARTITION OF, below), and the resolution of large numbers into their prime factors.

The general problem of partitions is to find all the integral solutions of a set of linear equations $\Sigma c_i x_i = m_i$ with integral coefficients, and fewer equations than there are variables. The solutions may be further restricted by other conditions—for instance, that all the variables are to be positive. This theory was begun by Euler: Sylvester gave lectures on the subject, of which some portions have been preserved; and various results of great generality have been discovered by P. A. MacMahon. The author last named has also considered Diophantine inequalities, a simple problem in which is "to enumerate all the solutions of $7x \geqslant 13y$ in positive integers."

The resolution of a given large number into its prime factors is still a problem of great difficulty, and tentative methods have to be applied. But a good deal has been done by Seelhoff, Lucas, Landry, A. J. C. Cunningham and Lawrence to shorten the calculation, especially when the number is given in, or can be reduced to, some particular form.

It is well known that Fermat was led to the erroneous conjecture (he did *not* affirm it) that 2^m+1 is a prime whenever m is a power of 2. The first case of failure is when $m=32$; in fact $2^{32}+1 \equiv 0$ (mod 641). Other known cases of failure are $m=2^n$, with $n=6$, 12, 23, 26 respectively; at the same time, Eisenstein asserted that he had proved that the formula 2^m+1 included an infinite number of primes. His proof is not extant; and no other has yet been supplied. Similar difficulties are encountered when we examine Mersenne's numbers, which are those of the form 2^p-1, with p a prime; the known cases for which a Mersenne number is prime correspond to $p=2$, 3, 5, 7, 13, 17, 19, 31, 61.

A perfect number is one which, like 6 or 28, is the sum of its aliquot parts. Euclid proved that $2^{p-1}(2^p-1)$ is perfect when (2^p-1) is a prime: and it has been shown that this formula includes all perfect numbers which are even. It is not known whether any odd perfect numbers exist or not.

Friendly numbers (*numeri amicabiles*) are pairs such as 220, 284, each of which is the sum of the aliquot parts of the other. No general rules for constructing them appear to be known, but several have been found, in a more or less methodical way.

78. In conclusion it may be remarked that the science of arithmetic (*q.v.*) has now reached a stage when all its definitions, processes and results are demonstrably independent of any theory of variable or measurable quantities such as those postulated in geometry and mathematical physics; even the notion of a limit may be dispensed with, although this idea, as well as that of a variable, is often convenient. For the application of arithmetic to geometry and analysis, see FUNCTION.

AUTHORITIES.—W. H. and G. E. Young, *The Theory of Sets of Points* (Cambridge, 1906; contains bibliography of theory of aggregates); P. Bachmann, *Zahlentheorie* (Leipzig, 1892; the most complete treatise extant); Dirichlet-Dedekind, *Vorlesungen über Zahlentheorie* (Braunschweig, 3rd and 4th ed., 1879, 1894); K. Hensel, *Theorie der algebraischen Zahlen* (Leipzig, 1908); H. J. S. Smith, *Report on the Theory of Numbers* (*Brit. Ass. Rep.*, 1859–1863, 1865, or *Coll. Math. Papers*, vol. i.); D. Hilbert, "Bericht über die Theorie der algebraischen Zahlkörper" (in *Jahresber. d. deutschen Math.-Vereinig.*, vol. iv., Berlin, 1897); Klein-Fricke, *Elliptische Modulfunctionen* (Leipzig, 1890–1892); H. Weber, *Elliptische Functionen u. algebraische Zahlen* (Braunschweig, 1891). Extensive bibliographies will be found in the Royal Society's *Subject Index*, vol. i. (Cambridge, 1908) and *Encycl. d. math. Wissenschaften*, vol. i. (Leipzig, 1898). (G. B. M.)

NUMBERS, BOOK OF, the fourth book of thc Bible, which takes its title from the Latin equivalent of the Septuagint Ἀριθμοί. While the English version follows the Septuagint directly in speaking of Genesis, Exodus, Leviticus and Deuteronomy, it follows the Vulgate in speaking of Numbers. Since this book describes the way in which an elaborate census of Israel was taken on two separate occasions, the first at Sinai at the beginning of the desert wanderings and the second just before their close on the plains of Moab, the title is quite appropriate. The name given to it in modern Hebrew Bibles from its fourth word *Bemidhbar* ("In the desert") is at least equally appropriate. The other title in use among the Jews, *Vayyidhabber* ("And he said"), is simply the first word of the book and has no reference to its contents.

Numbers is the first part of the second great division of the Hexateuch. In the first three books we are shown how God raised up for Himself a chosen people and how the descendants of Israel on entering at Sinai into a solemn league and covenant with Yahweh (Jehovah) became a separate nation, a peculiar people. In the last three books we are told what happened to Israel between the time it entered into this solemn covenant and its settlement in the Promised Land under the successor of Moses. Yet, though thus part of a larger whole, the book of Numbers has been so constructed by the Redactor as to form a self-contained division of that whole.

The truth of this statement is seen by comparing the first verse of the book with the last. The first is as evidently meant to serve as an introduction to the book as the last is to serve as its conclusion. This is not to say, however, that the book is all of a piece, or written on a systematic plan. On the contrary, no book in the Hexateuch gives such an impression of incoherence, and in none are the different strata which compose the Hexateuch more distinctly discernible.

It is noteworthy that the problems of Hexateuchal criticism are gradually changing their character, as one after another of the main contentions of Biblical scholars regarding the date and authorship of the Hexateuch passes out of the list of debatable questions into that of acknowledged facts. No competent scholars now question the existence, hardly any one the relative dates, of J, E, and P. In Numbers one can tell almost at a glance which parts belong to P, the Priestly Code, and which to JE, the narrative resulting from the combination of the Judaic work of the Yahwist with the Ephraimitic work of the Elohist. The main difficulty in Numbers is to determine to which stratum of P certain sections should be assigned.

The first large section (i.—x. 10) is wholly P, and the last eleven chapters are also P with the exception of two or three paragraphs in chap. xxxii., while the intervening portion is mainly P with the exception of three important episodes and two or three others of less importance. The three main episodes are those of the twelve spies, the rebellion of Korah, Dathan and Abiram, and Balaam's mission to Balak. The last is the only one even of these three in which there is nothing belonging to P. Another passage which we may here mention is one where the elements of JE can be readily separated and assigned to their respective authors, viz. chaps. xi. and xii. It is generally agreed that to E belongs the passage describing the outpouring of the Spirit on Eldad and Medad and the remarkable prayer of Moses in xi. 29, "Would God that all the Lord's people were prophets that the Lord