795.

NUMBERS, THEORY OF.

[From the *Encyclopædia Britannica, Ninth Edition*, vol. XVII. (1884), pp. 614—624.]

THE Theory of Numbers, or higher arithmetic, otherwise arithmology, is a subject which, originating with Euclid, has in modern times, in the hands of Legendre, Gauss, Lejeune-Dirichlet, Kummer, Kronecker, and others, been developed into a most extensive and interesting branch of mathematics. We distinguish between the ordinary (or say the simplex) theory and the various complex theories.

In the ordinary theory we have, in the first instance, positive integer numbers, the unit or unity 1, and the other numbers 2, 3, 4, 5, &c. We introduce the zero 0, which is a number *sui generis*, and the negative numbers $-1, -2, -3, -4$, &c., and we have thus the more general notion of integer numbers, $0, \pm 1, \pm 2, \pm 3$, &c.; $+1$ and -1 are units or unities. The sum of any two or more numbers is a number; conversely, any number is a sum of two or more parts; but even when the parts are positive a number cannot be, in a determinate manner, represented as a sum of parts. The product of two or more numbers is a number; but (disregarding the unities $+1$, -1, which may be introduced as factors at pleasure) it is not conversely true that every number is a product of numbers. A number such as 2, 3, 5, 7, 11, &c., which is not a product of numbers, is said to be a prime number; and a number which is not prime is said to be composite. A number other than zero is thus either prime or composite; and we have the theorem that every composite number is, in a determinate way, a product of prime factors.

We have complex theories in which all the foregoing notions (integer, unity, zero, prime, composite) occur; that which first presented itself was the theory with the unit i ($i^2 = -1$); we have here complex numbers, $a + bi$, where a and b are in the before-mentioned (ordinary) sense positive or negative integers, not excluding zero; we have the zero $0, = 0 + 0i$, and the four units $1, -1, i, -i$. A number other than zero is here either prime or else composite; for instance, 3, 7, 11, are prime numbers, and $5, = (2 + i)(2 - i)$, $9, = 3 . 3$, $13, = (3 + 2i)(3 - 2i)$, are composite numbers (generally any

positive real prime of the form $4n+3$ is prime, but any positive real prime of the form $4n+1$ is a sum of two squares, and is thus composite). And disregarding unit factors we have, as in the ordinary theory, the theorem that every composite number is, in a determinate way, a product of prime factors.

There is, in like manner, a complex theory involving the cube roots of unity—if α be an imaginary cube root of unity ($\alpha^2+\alpha+1=0$), then the integers of this theory are $a+b\alpha$ (a and b real positive or negative integers, including zero); a complex theory with the fifth roots of unity—if α be an imaginary fifth root of unity ($\alpha^4+\alpha^3+\alpha^2+\alpha+1=0$), then the integers of the theory are $a+b\alpha+c\alpha^2+d\alpha^3$ (a, b, c, d, real positive or negative integers, including zero); and so on for the roots of the orders 7, 11, 13, 17, 19. In all these theories, or at any rate for the orders 3, 5, 7 (see No. 37, *post*), we have the foregoing theorem: disregarding unit factors, a number other than zero is either prime or composite, and every composite number is, in a determinate way, a product of prime factors. But coming to the 23rd roots of unity the theorem ceases to be true. Observe that it is a particular case of the theorem that, if N be a prime number, any integer power of N has for factors only the lower powers of N,—for instance, $N^3=N.N^2$; there is no other decomposition $N^3=AB$. This is obviously true in the ordinary theory, and it is true in the complex theories preceding those for the 3rd, 5th, and 7th roots of unity, and probably in those for the other roots preceding the 23rd roots; but it is not true in the theory for the 23rd roots of unity. We have, for instance, 47, a number not decomposable into factors, but 47^3, $=AB$, is a product of two numbers each of the form $a+b\alpha+\ldots+kx^{21}$ (α a 23rd root). The theorem recovers its validity by the introduction into the theory of Kummer's notion of an ideal number.

The complex theories above referred to would be more accurately described as theories for the complex numbers involving the periods of the roots of unity: the units are the roots either of the equation $x^{p-1}+x^{p-2}+\ldots+x+1=0$ (p a prime number) or of any equation $x^{\frac{p-1}{e}}+\ldots\pm 1=0$ belonging to a factor of the function of the order $p-1$: in particular, this may be the quadric equation for the periods each of $\frac{1}{2}(p-1)$ roots; they are the theories which were first and have been most completely considered, and which led to the notion of an ideal number. But a yet higher generalization which has been made is to consider the complex theory, the units whereof are the roots of any given irreducible equation which has integer numbers for its coefficients.

There is another complex theory the relation of which to the foregoing is not very obvious, viz. Galois's theory of the numbers composed with the imaginary roots of an irreducible congruence, $F(x)\equiv 0$ (modulus a prime number p); the nature of this will be indicated in the sequel.

In any theory, ordinary or complex, we have a first part, which has been termed (but the name seems hardly wide enough) the theory of congruences; a second part, the theory of homogeneous forms: this includes in particular the theory of the binary quadratic forms $(a, b, c)(x, y)^2$; and a third part, comprising those miscellaneous investigations which do not come properly under either of the foregoing heads.

Ordinary Theory, First Part.

1. We are concerned with the integer numbers 0, ± 1, ± 2, ± 3, &c., or in the first place with the positive integer numbers 1, 2, 3, 4, 5, 6, &c. Some of these, 1, 2, 3, 5, 7, &c., are prime, others, $4 = 2^2$, $6 = 2.3$, &c., are composite; and we have the fundamental theorem that a composite number is expressible, and that in one way only, as a product of prime factors, $N = a^\alpha b^\beta c^\gamma \ldots$ (a, b, c, ... primes other than 1; α, β, γ, ... positive integers).

Gauss makes the proof to depend on the following steps: (i) the product of two numbers each smaller than a given prime number is not divisible by this number; (ii) if neither of two numbers is divisible by a given prime number the product is not so divisible; (iii) the like as regards three or more numbers; (iv) a composite number cannot be resolved into factors in more than one way.

2. Proofs will in general be only indicated or be altogether omitted, but, as a specimen of the reasoning in regard to whole numbers, the proofs of these fundamental propositions are given at length. (i) Let p be the prime number, a a number less than p, and if possible let there be a number b less than p, and such that ab is divisible by p; it is further assumed that b is the only number, or, if there is more than one, then that b is the least number having the property in question; b is greater than 1, for a being less than p is not divisible by p. Now p as a prime number is not divisible by b, but must lie between two consecutive multiples mb and $(m+1)b$ of b. Hence, ab being divisible by p, mab is also divisible by p; moreover, ap is divisible by p, and hence the difference of these numbers, $= a(p - mb)$, must also be divisible by p, or, writing $p - mb = b'$, we have ab' divisible by p, where b' is less than b; so that b is not the least number for which ab is divisible by p. (ii) If a and b are neither of them divisible by p, then a divided by p leaves a remainder α which is less than p, say we have $a = mp + \alpha$; and similarly b divided by p leaves a remainder β which is less than p, say we have $b = np + \beta$; then

$$ab = (mp + \alpha)(np + \beta), \quad = (mnp + n\alpha + m\beta)p + \alpha\beta,$$

and $\alpha\beta$ is not divisible by p, therefore ab is not divisible by p. (iii) The like proof applies to the product of three or more factors a, b, c, ... (iv) Suppose that the number $N = a^\alpha b^\beta c^\gamma \ldots$ (a, b, c, ... prime numbers other than 1), is decomposable in some other way into prime factors; we can have no prime factor p, other than a, b, c, ..., for no such number can divide $a^\alpha b^\beta c^\gamma \ldots$; and we must have each of the numbers a, b, c, ..., for if any one of them, suppose a, were wanting, the number N would not be divisible by a. Hence the new decomposition if it exists must be a decomposition $N = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$; and here, if any two corresponding indices, say α, α', are different from each other, then one of them, suppose α', is the greater, and we have $N \div p^\alpha = b^\beta c^\gamma \ldots = a^{\alpha' - \alpha} b^{\beta'} c^{\gamma'} \ldots$ That is, we have the number $N \div p^\alpha$ expressed in two different ways as a product, the number a being a factor in the one case, but not a factor in the other case. Thus the two exponents cannot be unequal, that is, we must have $\alpha = \alpha'$, and similarly we have $\beta = \beta'$, $\gamma = \gamma'$, ...; that is, there is *only* the original decomposition $N = a^\alpha b^\beta c^\gamma \ldots$

3. The only numbers divisible by a number $N = a^\alpha b^\beta c^\gamma \ldots$ are the numbers $a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$, where each exponent α' is equal to or greater than the corresponding exponent α. And conversely the only numbers which divide N are those of the form $a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$, where each index α' is at most equal to the corresponding index α; and in particular each or any of the indices α' may be $= 0$. Again, the least common multiple of two numbers $N = a^\alpha b^\beta c^\gamma \ldots$ and $N' = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$ is $a^{\alpha''} b^{\beta''} c^{\gamma''} \ldots$, where each index α'' is equal to the largest of the corresponding indices α, α';—observe that any one or more of the indices $\alpha, \beta, \gamma, \ldots, \alpha', \beta', \gamma', \ldots$, may be $= 0$, so that the theorem extends to the case where either of the numbers N, N', has prime factors which are not factors of the other number. And so the greatest common measure of two numbers $N = a^\alpha b^\beta c^\gamma \ldots$ and $N' = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$ is $a^{\alpha''} b^{\beta''} c^{\gamma''} \ldots$, where each index α'' is equal to the least of the corresponding indices α and α'.

4. The divisors of $N = a^\alpha b^\beta c^\gamma \ldots$ are the several terms of the product

$$(1 + a + \ldots + a^\alpha)(1 + b + \ldots + b^\beta)(1 + c + \ldots + c^\gamma),$$

where unity and the number N itself are reckoned each of them as a divisor. Hence the number of divisors is $= (\alpha+1)(\beta+1)(\gamma+1)\ldots$, and the sum of the divisors is

$$= \frac{(a^{\alpha+1} - 1)(b^{\beta+1} - 1)(c^{\gamma+1} - 1)\ldots}{(a-1)(b-1)(c-1)\ldots}.$$

5. In $N = a^\alpha b^\beta c^\gamma \ldots$ the number of integers less than N and prime to it is

$$\phi(N), = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\ldots$$

To find the numbers in question write down the series of numbers $1, 2, 3, \ldots, N$; strike out all the numbers divisible by a, then those divisible by b, then those divisible by c, and so on; there will remain only the numbers prime to N. For actually finding the numbers we may of course in striking out those divisible by b disregard the numbers already struck out as divisible by a, and in striking out with respect to c disregard the numbers already struck out as divisible by a or b, and so on; but in order to count the remaining numbers it is more convenient to ignore the previous strikings out. Suppose, for a moment, there are only two prime factors a and b, then the number of terms struck out as divisible by a is $= N.\frac{1}{a}$, and the number of terms struck out as divisible by b is $= N.\frac{1}{b}$; but then each term divisible by ab will have been twice struck out; the number of these is $= N.\frac{1}{ab}$, and thus the number of the remaining terms is $N\left(1 - \frac{1}{a} - \frac{1}{b} + \frac{1}{ab}\right)$, which is $= N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)$. By treating in like manner the case of three or more prime factors $a, b, c, \ldots$ we arrive at the general theorem. The formula gives $\phi(1) = 1$ viz. when $N = 1$, there is no factor $1 - \frac{1}{a}$; and it is necessary to consider $\phi(1)$ as being $= 1$. The explanation is that $\phi(N)$

properly denotes the number of integers not greater than N and prime to it; so that, when $N=1$, we have 1 an integer not greater than N and prime to it; but in every other case the two definitions agree.

6. If N, N', are numbers prime to each other, then $\phi(NN')=\phi(N)\,\phi(N')$, and so also for any number of numbers having no common divisor; in particular,

$$\phi(a^\alpha b^\beta c^\gamma \ldots)=\phi(a^\alpha)\,\phi(b^\beta)\,\phi(c^\gamma)\ldots;\quad \phi(a^\alpha)=a^\alpha\left(1-\frac{1}{a}\right),$$

and the theorem is at once verified. We have $N=\Sigma\phi(N')$, where the summation extends to all the divisors N' of N, unity and the number N itself being included; thus $15=\phi(15)+\phi(5)+\phi(3)+\phi(1),\ =8+4+2+1$.

7. The prime factor of the binomial function x^N-1 is

$$=\frac{(x^N-1)\,(x^{N/ab}-1)\ldots}{(x^{N/a}-1)\,(x^{N/b}-1)\ldots},$$

a rational and integral function of the degree $\phi(N)$; say this is called $[x^N-1]$, and we have $x^N-1=\Pi[x^{N'}-1]$, where the product extends to all the divisors N' of N, unity and the number N included. For instance

$$[x^{15}-1]=\frac{(x^{15}-1)\,(x-1)}{(x^5-1)\,(x^3-1)},\ =x^8-x^7+x^5-x^4+x^3-x+1;$$

and we have

$$x^{15}-1=[x^{15}-1]\,[x^5-1]\,[x^3-1]\,[x-1],$$
$$=(x^8-x^7+\ldots-x+1)\,(x^4+x^3+x^2+x+1)\,(x^2+x+1)\,(x-1).$$

8. Congruence to a given modulus. A number x is congruent to 0, to the modulus N, $x\equiv 0\,(\mathrm{mod.}\ N)$, when x is divisible by N; two numbers x, y are congruent to the modulus N, $x\equiv y\,(\mathrm{mod.}\ N)$, when their difference $x-y$ divides by N, or, what is the same thing, if $x-y\equiv 0\,(\mathrm{mod.}\ N)$. Observe that, if $xy\equiv 0\,(\mathrm{mod.}\ N)$, and x be prime to N, then $y\equiv 0\,(\mathrm{mod.}\ N)$.

9. Residues to a given modulus. For a given modulus N we can always find, and that in an infinity of ways, a set of N numbers, say N residues, such that every number whatever is, to the modulus N, congruent to one and only one of these residues. For instance, the residues may be $0, 1, 2, 3, \ldots, N-1$ (the residue of a given number is here simply the positive remainder of the number when divided by N); or, N being odd, the system may be

$$0,\ \pm 1,\ \pm 2,\ \ldots,\ \pm\tfrac{1}{2}(N-1),$$

and N even,

$$0,\ \pm 1,\ \pm 2,\ \ldots,\ \pm\tfrac{1}{2}(N-2),\ +\tfrac{1}{2}N.$$

10. Prime residues to a given modulus. Considering only the numbers which are prime to a given modulus N, we have here a set of $\phi(N)$ numbers, say $\phi(N)$ prime residues, such that every number prime to N is, to the modulus N, congruent to

one and only one of these prime residues. For instance, the prime residues may be the numbers less than N and prime to it. In particular, if N is a prime number p, then the residues may be the $p-1$ numbers, $1, 2, 3, \ldots, p-1$.

In all that follows, the letter p, in the absence of any statement to the contrary, will be used to denote an *odd* prime other than unity. A theorem for p may hold good for the even prime 2, but it is in general easy to see whether this is so or not.

11. Fermat's theorem, $x^{p-1}-1 \equiv 0 \pmod{p}$. The generalized theorem is $x^{\phi(N)}-1 \equiv 0 \pmod{N}$. The proof of the generalized theorem is as easy as that of the original theorem. Consider the series of the $\phi(N)$ numbers $a, b, c, \ldots$, each less than N and prime to it; let x be any number prime to N, then each of the numbers $xa, xb, xc, \ldots$, is prime to N, and no two of them are congruent to the modulus N, that is, we cannot have $x(a-b) \equiv 0 \pmod{N}$; in fact, x is prime to N, and the difference $a-b$ of two positive numbers each less than N will be less than N. Hence the numbers $xa, xb, xc, \ldots$, are in a different order congruent to the numbers $a, b, c, \ldots$; and multiplying together the numbers of each set we have $x^{\phi(N)}\, abc \ldots \equiv abc \ldots \pmod{N}$, or, since $a, b, c, \ldots$, are each prime to N, and therefore also the product $abc \ldots$ is prime to N, we have $x^{\phi(N)} \equiv 1$, or say $x^{\phi(N)} - 1 \equiv 0 \pmod{N}$.

In particular, if N be a prime number $= p$, then $\phi(N)$ is $= p-1$, and the theorem is $x^{p-1} - 1 \equiv 0 \pmod{p}$, x being now any number not divisible by p.

12. The general congruence $f(x) \equiv 0 \pmod{p}$. $f(x)$ is written to denote a rational and integral function with integer coefficients which may without loss of generality be taken to be each of them less than p; it is assumed that the coefficient A of the highest power of x is not $= 0$. If there is for x an integer value a such that $f(a) \equiv 0 \pmod{p}$, throughout), then a is said to be a root of the congruence $f(x) \equiv 0$; we may, it is clear, for a substitute any value whatever $a' = a + kp$, or say any value a' which is $\equiv a$, but such value a' is considered not as a different root but as the same root of the congruence. We have thus $f(a) \equiv 0$; and therefore $f(x) \equiv f(x) - f(a)$, $= (x-a) f_1(x)$, where $f_1(x)$ is a function of like form with $f(x)$, that is, with integer coefficients, but of the next inferior order $n-1$. Suppose there is another root b of the congruence, that is, an integer value b such that $f(b) \equiv 0$; we have then $(b-a) f_1(b) \equiv 0$, and $b-a$ is not $\equiv 0$ (for then b would be the same root as a). Hence $f_1(b) \equiv 0$, and $f(x) = (x-a)\{f_1(x) - f_1(b)\}$, $= (x-a)(x-b) f_2(x)$, where $f_2(x)$ is an integral function such as $f(x)$, but of the order $n-2$; and so on, that is, if there exist n different (non-congruent) roots of the congruence $f(x) \equiv 0$, then $f(x) = A(x-a)(x-b) \ldots (x-k)$, and the congruence may be written $A(x-a)(x-b) \ldots (x-k) \equiv 0$. And this cannot be satisfied by any other value l; for if so we should have $A(l-a)(l-b) \ldots (l-k) \equiv 0$, that is, some one of the congruences $(l-a) \equiv 0$, &c., would have to be satisfied, and l would be the same as one of the roots $a, b, c, \ldots, k$. That is, a congruence of the order n cannot have more than n roots, and if it have precisely n roots $a, b, c, \ldots, k$, then the form is $f(x) \equiv A(x-a)(x-b) \ldots (x-k)$, $\equiv 0$.

Observe that a congruence may have equal roots, viz. if the form be

$$f(x) \equiv A(x-a)^{\alpha}(x-b)^{\beta} \ldots, \equiv 0,$$

then the roots $a, b, \ldots$ are to be counted α times, β times, ... respectively; but clearly the whole number of roots $\alpha+\beta+\ldots$ is at most $=n$.

It is hardly necessary to remark that this theory of a congruence of the order n is precisely analogous to that of an equation of the order n, when only real roots are attended to. The theory of the imaginary roots of a congruence will be considered further on (see No. 41).

13. The linear congruence $ax \equiv c \pmod{b}$. This is equivalent to the indeterminate equation $ax+by=c$; if a and b are not prime to each other, but have a greatest common measure q, this must also divide c; supposing the division performed, the equation becomes $a'x+b'y=c'$, where a' and b' are prime to each other, or, what is the same thing, we have the congruence $a'x \equiv c' \pmod{b'}$. This can always be solved, for, if we consider the b' numbers $0, 1, 2, \ldots, b'-1$, one and only one of these will be $\equiv c' \pmod{b'}$. Multiplying these by any number a' prime to b', and taking the remainders in regard to b', we reproduce in a different order the same series of numbers $0, 1, 2, \ldots, b'-1$; that is, in the series $a', 2a', \ldots, (b'-1)a'$ there will be one and only one term $\equiv c' \pmod{b'}$, or, calling the term in question α, we have $x=\alpha$ as the solution of the congruence $a'x \equiv c' \pmod{b'}$; $a'\alpha - c'$ is then a multiple of b', say it is $=-b'\beta$, and the corresponding value of y is $y=\beta$. We may for α write $\alpha+mb'$, m being any positive or negative integer, not excluding zero (but, as already remarked, this is not considered as a distinct solution of the congruence); the corresponding value of y is clearly $=\beta-ma'$.

The value of x can be found by a process similar to that for finding the greatest common measure of the two numbers a' and c'; this is what is really done in the apparently tentative process which at once presents itself for small numbers, thus $6x \equiv 9 \pmod{35}$, we have $36x \equiv 54$, or, rejecting multiples of 35, $x \equiv 19$, or, if we please, $x=35m+19$.

In particular, we can always find a number ξ such that $a'\xi \equiv 1 \pmod{b'}$; and we have then $x=c'\xi$ as the solution of the congruence $a'x \equiv c'$. The value of ξ may be written $\xi \equiv \frac{1}{a'} \pmod{b'}$, where $\frac{1}{a'}$ stands for that integer value ξ which satisfies the original congruence $a'\xi \equiv 1 \pmod{b'}$; and the value of x may then be written $x \equiv \frac{c'}{a'} \pmod{b'}$. Another solution of the linear congruence is given in No. 21.

14. Wilson's theorem, $1.2.3\ldots\overline{p-1}+1 \equiv 0 \pmod{p}$. It has been seen that, for any prime number p, the congruence $x^{p-1}-1 \equiv 0 \pmod{p}$ of the order $p-1$ has the $p-1$ roots $1, 2, \ldots, p-1$; we have therefore

$$x^{p-1}-1 \equiv (x-1)(x-2)\ldots(x-\overline{p-1}),$$

or, comparing the terms independent of x, it appears that $1.2.3\ldots p-1 \equiv -1$, that is, $1.2.3\ldots\overline{p-1}+1 \equiv 0 \pmod{p}$,—the required theorem. For instance, where $p=5$, then $1.2.3.4+1 \equiv 0 \pmod{5}$, and where $p=7$, then $1.2.3.4.5.6+1 \equiv 0 \pmod{7}$.

15. A proof on wholly different principles may be given. Suppose, to fix the ideas, $p=7$; consider on a circle 7 points, the summits of a regular heptagon, and join

these in any manner so as to form a heptagon; the whole number of heptagons is $\frac{1}{2}.1.2.3.4.5.6$. Now of these we have $\frac{1}{7}(7-1), =3$, which are regular heptagons (convex or stellated); the number of remaining heptagons must be divisible by 7, for with any one such heptagon we connect the 6 heptagons which can be obtained from it by making it rotate through successive angles of $\frac{1}{7}360°$. That is, $\frac{1}{2}.1.2.3.4.5.6-\frac{1}{2}(7-1)\equiv 0$ (mod. 7), whence $1.2.3.4.5.6-7+1\equiv 0$, or finally $1.2.3.4.5.6+1\equiv 0$ (mod. 7). It is clear that the proof applies without alteration to the case of any prime number p.

If p is not a prime number, then $1.2.3\ldots\overline{p-1}\equiv 0$ (mod. p); hence the theorem shows directly whether a number p is or is not a prime number; but it is not of any practical utility for this purpose.

16. Prime roots of a prime number—application to the binomial equation $x^p-1=0$. Take, for instance, $p=7$. By what precedes, we have

$$x^6-1=[x^6-1][x^3-1][x^2-1][x-1], \quad =(x^2-x+1)(x^2+x+1)(x+1)(x-1);$$

and we have

$$x^6-1\equiv(x-1)(x-2)(x-3)(x-4)(x-5)(x-6) \text{ (mod. 7)};$$

whence also

$$(x^2-x+1)(x^2+x+1)(x+1)(x-1)\equiv(x-1)(x-2)(x-3)(x-4)(x-5)(x-6).$$

These two decompositions must agree together, and we in fact have

$$x^2-x+1\equiv(x-3)(x-5), \quad x^2+x+1\equiv(x-2)(x-3), \quad x+1\equiv x-6, \quad x-1\equiv x-1.$$

In particular, we thus have 3, 5, as the roots of the congruence $x^2-x+1\equiv 0$, that is, $[x^6-1]\equiv 0$, and these roots 3, 5, are not the roots of any other of the congruences $[x^3-1]\equiv 0$, $[x^2-1]\equiv 0$, $[x-1]\equiv 0$; that is, writing $a=3$ or 5 in the series of numbers $a, a^2, a^3, a^4, a^5, a^6$, we have a^6 as the first term which is $\equiv 1$ (mod. 7); the series in fact are

$$3, 9, 27, 81, 243, 729 \quad \equiv 3, 2, 6, 4, 5, 1,$$

$$5, 25, 125, 625, 3125, 15625 \equiv 5, 4, 6, 2, 3, 1.$$

And so, in general, the congruence $x^{p-1}-1\equiv 0$ (mod. p) has the $p-1$ real roots $1, 2, 3, \ldots, p-1$; hence the congruence $[x^{p-1}-1]\equiv 0$, which is of the order $\phi(p-1)$, has this number $\phi(p-1)$ of real roots; and, calling any one of these g, then in the series of powers $g, g^2, g^3, \ldots, g^{p-1}$, the first term which is $\equiv 1$ (mod. p) is g^{p-1}, that is, we have $g, g^2, g^3, \ldots, g^{p-1}=1, 2, 3, \ldots, p-1$ in a different order. Any such number g is said to be a prime root of p, and the number of prime roots is $\phi(p-1)$, the number of integers less than and prime to $p-1$.

The notion of a prime root was applied by Gauss to the solution of the binomial equation $x^p-1=0$, or, what is the same thing, to the question of the division of the circle (Kreistheilung), see Equation, Nos. 30 and 31, [786]; and, as remarked in the introduction to the present article, the roots or periods of roots of this equation present themselves as the units of a complex theory in the Theory of Numbers.

17. Any number x less than p is $\equiv g^m$, and, if m is not prime to $p-1$, but has with it a greatest common measure e, suppose $m = ke$, $p-1 = ef$, then

$$x \equiv g^{ke}, \quad x^f \equiv g^{kef} \equiv g^{k(p-1)} \equiv 1,$$

that is, $x^f \equiv 1$; and it is easily seen that in the series of powers $x, x^2, \ldots, x^f$, we have x^f as the first term which is $\equiv 1 \pmod{p}$. A number $\equiv g^m$, where m is not prime to $p-1$, is thus not a prime root; and it further appears that, g being any particular prime root, the $\phi(p-1)$ prime roots are $\equiv$ the numbers g^m, where m is any number less than $p-1$ and prime to it. Thus in the foregoing example $p=7$, where the prime roots were 3 and 5, the integers less than 6 and prime to it are 1, 5; and we, in fact, have $5 \equiv 3^5$ and $3 \equiv 5^5 \pmod{7}$.

18. Integers belonging to a given exponent; index of a number. If, as before, $p-1 = ef$, that is, if f be a submultiple of $p-1$, then any integer x such that x^f is the lowest power of x which is $\equiv 1 \pmod{p}$ is said to belong to the exponent f. The number of residues, or terms of the series $1, 2, 3, \ldots, p-1$, which belong to the exponent f is $\phi(f)$, the number of integers less than f and prime to it; these are the roots of the congruence $[x^f - 1] \equiv 0$ of the order $\phi(f)$. It is hardly necessary to remark that the prime roots belong to the exponent $p-1$.

A number $x \equiv g^m$ is said to have the index m; observe the distinction between the two terms exponent and index; and, further, that the index is dependent on the selected prime root g.

19. Special forms of composite modulus. If instead of a prime modulus p we have a modulus p^m which is the power of an odd prime, or a modulus $2p$ or $2p^m$ which is twice an odd prime or a power of an odd prime, then there is a theory analogous to that of prime roots, viz. the numbers less than the modulus and prime to it are congruent to successive powers of a prime root g; thus,

if $p^m = 3^2$, we have

$$2, 4, 8, 16, 32, 64 \equiv 2, 4, 8, 7, 5, 1 \pmod{9},$$

and if $2p^m = 2 \cdot 3^2$, we have

$$5, 25, 125, 625, 3125, 15625 \equiv 5, 7, 11, 13, 17, 1 \pmod{18}.$$

As regards the even prime 2 and its powers—for the modulus 2 or 4 the theory of prime roots does not come into existence, and for the higher powers it is not applicable; thus with modulus $=8$ the numbers less than 8 and prime to it are 1, 3, 5, 7; and we have $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.

20. Composite modulus $N = a^\alpha b^\beta c^\gamma \ldots$—no prime roots—irregularity. In the general case of a composite modulus it has been seen that, if x is any number less than N and prime to it, then $x^{\phi(N)} - 1 \equiv 0 \pmod{N}$. But, except in the above-mentioned cases p^m, $2p^m$, 2 or 4, there is not any number a such that $a^{\phi(N)}$ is the first power of a which is $\equiv 1$; there is always some submultiple $i = \frac{1}{\theta}\phi(N)$ such that a^i is the first

power which is $\equiv 1$. For instance, say $N = 24$, $\phi(N) = 8$, then the numbers less than 24 and prime to it are 1, 5, 7, 11, 13, 17, 19, 23; and we have

$$1^1 \equiv 1, \quad 5^2 \equiv 7^2 \equiv 13^2 \equiv 17^2 \equiv 19^2 \equiv 23^2 \equiv 1 \text{ (mod. 24)},$$

that is, 1 has the exponent 1, but all the other numbers have the exponent 2. So again where $N = 48$, the 16 numbers less than 48 and prime to it have, 1 the exponent 1, and 7, 13, 17, 23, 25, 31, 35, 41, 47 each the exponent 2, and the remaining numbers 5, 11, 19, 29, 37, 43 each the exponent 4. We cannot in this case by means of any single root or of any two roots express all the numbers, but we can by means of three roots, for instance, 5, 7, 13, express all the numbers less than 48 and prime to it; the numbers are in fact $\equiv 5^\alpha 7^\beta 13^\gamma$, where $\alpha = 0$, 1, 2, or 3, and β and γ each $= 0$ or 1.

Comparing with the theorem for a prime number p, where the several numbers $1, 2, 3, \ldots, p-1$, are expressed by means of a single prime root, $\equiv g^\alpha$, where $\alpha = 0, 1, 2, \ldots, p-1$, we have the analogue of a case presenting itself in the theory of quadratic forms,—the "irregularity" of a determinant (*post*, No. 31); the difference is that here (the law being known, $N =$ a composite number) the case is not regarded as an irregular one, while the irregular determinants do not present themselves according to any apparent law.

21. Maximum indicator—application to solution of a linear congruence. In the case $N = 48$ it was seen that the exponents were 1, 2, 4, the largest exponent 4 being divisible by each of the others, and this property is a general one, viz. if $N = a^\alpha b^\beta c^\gamma \ldots$ in the series of exponents (or, as Cauchy calls them, indicators) of the numbers less than N and prime to it, the largest exponent I is a multiple of each of the other exponents, and this largest exponent Cauchy calls the maximum indicator; the maximum indicator I is thus a submultiple of $\phi(N)$, and it is the smallest number such that for every number x less than N and prime to it we have $x^I - 1 \equiv 0$ (mod. N). The values of I have been tabulated from $N = 2$ to 1000.

Reverting to the linear congruence $ax \equiv c$ (mod. b), where a and b are prime to each other, then, if I is the maximum indicator for the modulus b, we have $a^I \equiv 1$, and hence it at once appears that the solution of the congruence is $x \equiv ca^{I-1}$.

22. Residues of powers for an odd prime modulus. For the modulus p, if g be a prime root, then every number not divisible by p is $\equiv$ one of the series of numbers $g, g^2, \ldots, g^{p-1}$; and, if k be any positive number prime to $p-1$, then raising each of these to the power k we reproduce in a different order the same series of numbers $g, g^2, \ldots, g^{p-1}$, which numbers are in a different order $\equiv 1, 2, \ldots, p-1$, that is, the residue of a kth power may be any number whatever of the series $1, 2, \ldots, p-1$.

But, if k is not prime to $p-1$, say their greatest common measure is e, and that we have $p - 1 = ef$, $k = me$, then for any number not divisible by p the kth power is $\equiv$ one of the series of f numbers $g^e, g^{2e}, \ldots, g^{fe}$; there are thus only f, $= \frac{1}{e}(p-1)$, out of the $p-1$ numbers $1, 2, 3, \ldots, p-1$, which are residues of a kth power.

23. Quadratic residues for an odd prime modulus. In particular, if $k=2$, then $e=2$, $f=\frac{1}{2}(p-1)$, and the square of every number not divisible by p is $\equiv$ one of the $\frac{1}{2}(p-1)$ numbers $g^2, g^4, \ldots, g^{p-1}$; that is, there are only $\frac{1}{2}(p-1)$ numbers out of the series $1, 2, 3, \ldots, p-1$ which are residues of a square number, or say quadratic residues, and the remaining $\frac{1}{2}(p-1)$ numbers are said to be quadratic non-residues of the modulus p,—we may say simply, residues and non-residues. But this result can be obtained more easily without the aid of the theory of prime roots. Every number not divisible by p is, to the modulus p, $\equiv$ one of the series of numbers $\pm 1, \pm 2, \pm 3, \ldots, \pm\frac{1}{2}(p-1)$; hence every square number is $\equiv$ one of the series of numbers $1^2, 2^2, 3^2, \ldots, \frac{1}{4}(p-1)^2$; and thus the $p-1$ numbers $1, 2, 3, \ldots, p-1$, are one-half of them residues and the other half non-residues of p. Thus, in the case $p=11$, every number not divisible by 11 is, to this modulus, $\equiv$ one of the series $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5$; whence the square of any such number is $\equiv$ one of the series 1, 4, 9, 16, 25, or say the series 1, 4, 9, 5, 3; that is, we have

residues	1, . 3, 4, 5, . . . 9, .
non-residues	. 2, . . . 6, 7, 8, . 10

Calling as usual the residues a and the non-residues b, we have in this case

$$\tfrac{1}{11}(\Sigma b - \Sigma a) = \tfrac{1}{11}(33-22), \ =1,$$

a positive integer; this is a property true for any prime number of the form $4n+3$, but for a prime number of the form $4n+1$ we have $\Sigma b - \Sigma a = 0$; the demonstration belongs to a higher part of the theory.

It is easily shown that the product of two residues or of two non-residues is a residue; but the product of a residue and a non-residue is a non-residue.

24. The law of reciprocity—Legendre's symbol. The question presents itself, given that P is a residue or a non-residue of Q, can we thence infer whether Q is a residue or a non-residue of P? In particular, if P, Q, are the odd primes p, q, for instance, given that $13 = R(17)$, can we thence infer that $17 = R(13)$, or that $17 = NR(13)$? The answer is contained in the following theorem: If p, q, are odd primes each or one of them of the form $4n+1$, then p, q, are each of them a residue or each of them a non-residue of the other; but, if p, q, are each of them of the form $4n+3$, then, according as p is a residue or a non-residue of q, we have q a non-residue or a residue of p.

The theorem is conveniently expressed by means of Legendre's symbol, viz. p being a positive odd prime, and Q any positive or negative number not divisible by p, then $\left(\frac{Q}{p}\right)$ denotes $+1$ or -1, according as Q is or is not a residue of p; if, as before, q is (as p) a positive odd prime, then the foregoing theorem is

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

The denominator symbol may be negative, say it is $-p$, we then have as a definition $\left(\frac{Q}{-p}\right) = \left(\frac{Q}{p}\right)$—observe that $\left(\frac{-Q}{p}\right)$ is not $= \left(\frac{Q}{-p}\right)$—and we have further the theorems

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

viz. -1 is a residue or a non-residue of p according as $p \equiv 1$ or $\equiv 3 \pmod 4$, and 2 is a residue or a non-residue of p according as $p \equiv 1$ or 7, or $\equiv 3$ or 5 (mod. 8). If, as definitions, $\left(\frac{p}{-1}\right) = +1$ and $\left(\frac{p}{2}\right) = +1$, these may be written

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

We have also, what is in fact a theorem given at the end of No. 23,

$$\left(\frac{QQ'}{p}\right) = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p}\right).$$

The further definition is sometimes convenient—

$$\left(\frac{Q}{p}\right) = 0, \text{ when } p \text{ divides } Q.$$

The law of reciprocity, as contained in the theorem

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

is a fundamental theorem in the whole theory; it was enunciated by Legendre, but first proved by Gauss, who gave no less than six demonstrations of it.

25. Jacobi's generalized symbol. Jacobi defined this as follows: The symbol $\left(\frac{Q}{\pm pp'p''\ldots}\right)$, where $p, p', p'', \ldots$ are positive odd primes equal or unequal, and Q is any positive or negative odd number prime to $pp'p''\ldots$, denotes $+1$ or -1 according to the definition

$$\left(\frac{Q}{\pm pp'p''\ldots}\right) = \left(\frac{Q}{p}\right)\left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\ldots,$$

the symbols on the right-hand side being Legendre's symbols. But the definition may be regarded as extending to the case where Q is not prime to $pp'p''\ldots$: then we have Q divisible by some factor p, and by the definition of Legendre's symbol in this case we have $\left(\frac{Q}{p}\right) = 0$; hence in the case in question of Q not being prime to $pp'p''\ldots$, the value of Jacobi's symbol is $= 0$.

We may further extend the definition of the symbol to the case where the numerator and the denominator of the symbol are both or one of them even, and present the definition in the most general form, as follows: suppose that $p, p', p'', \ldots$

being positive or negative even or odd primes, equal or unequal, and similarly $q, q', q'', \ldots$ being positive or negative even or odd primes, equal or unequal, we have $P = pp'p'' \ldots$ and $Q = qq'q'' \ldots$, then the symbol $\left(\frac{Q}{P}\right)$ will denote $+1$, -1, or 0, according to the definition

$$\left(\frac{Q}{P}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p'}\right)\left(\frac{q}{p''}\right)\cdots\left(\frac{q'}{p}\right)\left(\frac{q'}{p'}\right)\left(\frac{q'}{p''}\right)\cdots,$$

the symbols on the right-hand being Legendre's symbols. If P and Q are not prime to each other, then for some pair of factors p and q we have $p = \pm q$, and the corresponding Legendrian symbol $\left(\frac{q}{p}\right)$ is $= 0$, whence in this case $\left(\frac{Q}{P}\right) = 0$.

It is important to remark that $\left(\frac{Q}{P}\right) = +1$ is not a sufficient condition in order that Q may be a residue of P; if $P = 2^{\alpha}pp'p'' \ldots$, $p, p', p'', \ldots$ being positive odd primes, then, in order that Q may be a residue of P, it must be a residue of each of the prime factors $p, p', p'', \ldots$, that is, we must have

$$\left(\frac{Q}{p}\right) = +1, \quad \left(\frac{Q}{p'}\right) = +1, \quad \left(\frac{Q}{p''}\right) = +1, \ldots,$$

as many equations as there are unequal factors $p, p', p'', \ldots$ of the modulus P.

Ordinary Theory, Second Part,—Theory of Forms.

26. Binary quadratic (or quadric) forms—transformation and equivalence. We consider a form

$$ax^2 + 2bxy + cy^2, \quad = (a, b, c)(x, y)^2,$$

or when, as usual, only the coefficients are attended to, $= (a, b, c)$. The coefficients (a, b, c) and the variables (x, y) are taken to be positive or negative integers, not excluding zero. The discriminant $ac - b^2$ taken negatively, that is, $b^2 - ac$, is said to be the determinant of the form: and we thus distinguish between forms of a positive and of a negative determinant.

Considering new variables, $\alpha x + \beta y$, $\gamma x + \delta y$, where $\alpha, \beta, \gamma, \delta$, are positive or negative integers, not excluding zero, we have identically

$$(a, b, c)(\alpha x + \beta y, \gamma x + \delta y)^2 = (a', b', c')(x, y)^2,$$

where

$$a' = (a, b, c)(\alpha, \gamma)^2, \qquad = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

$$b' = (a, b, c)(\alpha, \gamma)(\beta, \delta), \quad = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$

$$c' = (a, b, c)(\beta, \delta)^2, \qquad = a\beta^2 + 2b\beta\delta + c\delta^2;$$

and thence

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

The form (a', b', c') is in this case said to be contained in the form (a, b, c); and a condition for this is obviously that the determinant D' of the contained form

shall be equal to the determinant D of the containing form multiplied by a square number; in particular, the determinants must be of the same sign. If the determinants are equal, then $(\alpha\delta - \beta\gamma)^2 = 1$, that is, $\alpha\delta - \beta\gamma = \pm 1$. Assuming in this case that the transformation exists, and writing $\alpha\delta - \beta\gamma = \epsilon$, and writing also

$$x' = \alpha x + \beta y,$$

$$y' = \gamma x + \delta y,$$

then conversely

$$x = \frac{1}{\epsilon}(\ \delta x' - \beta y'),\ = \alpha' x' + \beta' y',$$

$$y = \frac{1}{\epsilon}(-\gamma x' + \alpha y'),\ = \gamma' x' + \delta' y',$$

suppose, where α', β', γ', δ' are integers; and we have, moreover,

$$\alpha'\delta' - \beta'\gamma' = \frac{1}{\epsilon^2}(\alpha\delta - \beta\gamma),\ = \frac{1}{\epsilon},\ = \epsilon,$$

that is, $\alpha'\delta' - \beta'\gamma' = +1$ or -1, according as $\alpha\delta - \beta\gamma$ is $= +1$ or -1. The two forms (a, b, c), (a', b', c') are in this case said to be equivalent, and to be, in regard to the particular transformation, equivalent properly or improperly according as $\alpha\delta - \beta\gamma (= \alpha'\delta' - \beta'\gamma')$ is $= +1$ or $= -1$. We have, therefore, as a condition for the equivalence of two forms, that their determinants shall be equal; but this is not a sufficient condition. It is to be remarked also that two forms of the same determinant may be equivalent properly and also improperly; there may exist a transformation for which $\alpha\delta - \beta\gamma$ is $= +1$, and also a transformation for which $\alpha\delta - \beta\gamma$ is $= -1$. But this is only the case when each of the forms is improperly equivalent to itself; for instance, a form $x^2 - Dy^2$, which remains unaltered by the change x, y, into x, $-y$ (that is, α, β, γ, $\delta = 1$, 0, 0, -1, and therefore $\alpha\delta - \beta\gamma = -1$), is a form improperly equivalent to itself. A form improperly equivalent to itself is said to be an ambiguous form. In what follows, equivalent means always properly equivalent.

27. Forms for a given determinant—classes, &c. In the case where D, $= b^2 - ac$, is a square, the form $(a, b, c)(x, y)^2$ is a product of two rational factors; this case may be excluded from consideration, and we thus assume that the determinant D is either negative, or, being positive, that it is not a square. The forms (a, b, c) of a given positive or negative determinant are each of them equivalent to some one out of a finite number of non-equivalent forms which may be considered as representing so many distinct classes. For instance, every form of the determinant -1 is equivalent to $(1, 0, 1)$, that is, given any form (a, b, c) for which $b^2 - ac = -1$, it is possible to find integer values α, β, γ, δ, such that $\alpha\delta - \beta\gamma = +1$, and $(a, b, c)(\alpha x + \beta y, \gamma x + \delta y)^2 = (1, 0, 1)(x, y)^2$, that is, $= x^2 + y^2$. Or, to take a less simple example, every form of the determinant -35 is equivalent to one of the following forms: $(1, 0, 35)$, $(5, 0, 7)$, $(3, \pm 1, 12)$, $(4, \pm 1, 18)$,—$(2, 1, 8)$, $(6, 1, 6)$; for the first six forms, the numbers a, $2b$, c have no common factor, and these are said to be *properly primitive* forms, or to belong to the properly primitive order; for the last two forms, the numbers a, b, c have no common factor, but, a and c being each even, the numbers a, $2b$, c have a common factor 2,

and these are said to be *improperly primitive* forms, or to belong to the improperly primitive order. The properly primitive forms are thus the six forms (1, 0, 35), (5, 0, 7), (3, ±1, 12), (4, ±1, 18); or we may say that there are represented hereby six properly primitive classes. Derived forms, or forms which belong to a derived order, present themselves in the case of a determinant D having a square factor or factors, and it is not necessary to consider them here.

It is not proposed to give here the rules for the determination of the system of non-equivalent forms; it will be enough to state that this depends on the determination in the first instance of a system of *reduced* forms, that is, forms for which the coefficients a, b, c, taken positively satisfy certain numerical inequalities admitting only of a finite number of solutions. In the case of a negative determinant, the reduced forms are no two of them equivalent, and we thus have the required system of non-equivalent forms; in the case of a positive determinant, the reduced forms group themselves together in *periods* in such wise that the forms belonging to a period are equivalent to each other, and the required system of non-equivalent forms is obtained by selecting one form out of each such period. The principal difference in the theory of the two cases of a positive and a negative determinant consists in these periods; the system of non-equivalent forms once arrived at, the two theories are nearly identical.

28. Characters of a form or class—division into genera. Attending only to the properly primitive forms: for instance, those mentioned above for the determinant -35: the form (1, 0, 35) represents only numbers f which are residues of 5, and also residues of 7; we have, in fact, $f = x^2 + 35y^2$, $\equiv x^2 \pmod 5$, and also $\equiv x^2 \pmod 7$. Using the Legendrian symbols $\left(\frac{f}{5}\right)$ and $\left(\frac{f}{7}\right)$, we say that the form (1, 0, 35) has the characters $\left(\frac{f}{5}\right)$, $\left(\frac{f}{7}\right) = ++$. Each of the other forms has in like manner a determinate character $+$ or $-$ in regard to $\left(\frac{f}{5}\right)$ and also in regard to $\left(\frac{f}{7}\right)$; and it is found that for each of them the characters are $++$ or else $--$ (that is, they are never $+-$ or $-+$). We, in fact, have

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

and we thus arrange the six forms into genera, viz. we have three forms belonging to the genus $\left(\frac{f}{5}\right)$, $\left(\frac{f}{7}\right) = ++$, and three to the genus $\left(\frac{f}{5}\right)$, $\left(\frac{f}{7}\right) = --$, these characters $++$ and $--$ of genera being one-half of all the combinations $++$, $--$, $+-$, $-+$.

The like theory applies to any other negative or positive determinant; the several characters have reference in some cases not only to the odd prime factors of D but

also to the numbers 4 and 8, that is, there is occasion to consider also the Legendrian symbols $\left(\frac{-1}{f}\right)$, $=(-1)^{\frac{1}{2}(f-1)}$, and $\left(\frac{2}{f}\right)$, $=(-1)^{\frac{1}{8}(f^2-1)}$, and there are various cases to be considered according to the form of D in regard to its simple and squared factors respectively; but in every case there are certain combinations of characters (in number one-half of all the combinations) which correspond to genera, and the properly primitive forms belong to different genera accordingly, the number of forms being the same in each genus.

The form $(1, 0, -D)$ has the characters all +, and this is said to be the principal form, and the genus containing it the principal genus. For a given determinant, the characters of two genera may be compounded together according to the ordinary rule of signs, giving the characters of a new genus; in particular, if the characters of a genus are compounded with themselves, then we have the characters of the principal genus.

29. Composition of quadratic forms. Considering X, Y, as given lineo-linear functions of (x, y), (x', y'), defined by the equations

$$X = p_0xx' + p_1xy' + p_2yx' + p_3yy',$$
$$Y = q_0xx' + q_1xy' + q_2yx' + q_3yy',$$

the coefficients p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3, may be so connected with the coefficients (A, B, C), (a, b, c), (a', b', c'), of three quadratic forms as to give rise to the identity

$$(A, B, C)(X, Y)^2 = (a, b, c)(x, y)^2 . (a', b', c')(x', y')^2;$$

and, this being so, the form (A, B, C) is said to be compounded of the two forms (a, b, c) and (a', b', c'), the order of composition being indifferent.

The necessary and sufficient condition, in order that it may be possible to compound together two given forms (a, b, c), (a', b', c'), is that their determinants shall be to each other in the proportion of two square numbers; in particular, the two forms may have the same determinant D; and when this is so the compound form (A, B, C) will also have the same determinant D. The rules for this composition of two forms of the same determinant have been (as part of the general theory) investigated and established. The forms compounded of equivalent forms are equivalent to each other; we thus in effect compound *classes*, viz. considering any two classes, the composition of their representative forms gives a form which is the representative of a new class, and the composition of any two forms belonging to the two classes respectively gives a form belonging to the new class. But, this once understood, it is more simple to speak of the composition of forms, that is, of the forms belonging to the finite system of representative forms for a given determinant; and it will be enough to consider the properly primitive forms.

30. The principal form $(1, 0, D)$, compounded with any other form (a, b, c), gives rise to this same form (a, b, c); the principal form is on this account denoted by 1, viz. denoting the other form by ϕ, and expressing composition in like manner with

multiplication, we have $1 . \phi = \phi$. The form ϕ may be compounded with itself, giving a form denoted by ϕ^2; compounding this again with ϕ, we have a form denoted by ϕ^3; and so on. Since the whole number of forms is finite, we must in this manner arrive at the principal form, say we have $\phi^n = 1$, n being the least exponent for which this equation is satisfied. In particular, if the form ϕ belong to the principal genus, then the forms $\phi^2, \phi^3, \ldots, \phi^{n-1}$ will all belong to the principal genus, or the principal genus will include the forms $1, \phi, \phi^2, \ldots, \phi^{n-1}$, the powers of a form ϕ having the exponent n.

31. Regular and irregular determinants. The principal genus may consist of such a series of forms, and the determinant is then said to be *regular*; in particular, for a negative determinant D, $= -1$ to -1000, the determinant is always regular except in the thirteen cases $-D = 243, 307, 339, 459, 576, 580, 675, 755, 820, 884, 891, 900, 974$ (and, Perott, in *Crelle*, vol. XCV., 1883, except also for $-D = 468, 931$); the determinant is here said to be irregular. Thus for each of the values $-D = 576, 580, 820, 900$, the principal genus consists of four forms, not $1, \phi, \phi^2, \phi^3$, where $\phi^4 = 1$, but $1, \phi, \phi_1, \phi\phi_1$, where $\phi^2 = 1$, $\phi_1^2 = 1$, and therefore also $(\phi\phi_1)^2 = 1$.

Compounding together any two forms, we have a form with the characters compounded of the characters of the two forms; and in particular, combining a form with itself, we have a form with the characters of the principal form. Or, what is the same thing, any two genera compounded together give rise to a determinate genus, viz. the genus having the characters compounded of the characters of the two genera; and any genus compounded with itself gives rise to the principal genus.

Considering any regular determinant, suppose that there is more than one genus, and that the number of forms in each genus is $= n$; then, except in the case $n = 2$, it can be shown that there are always forms having the exponent $2n$. For instance, in the case $D = -35$, we have two genera each of three forms; there will be a form g having the exponent 6, or $g^6 = 1$; and the forms are $1, g, g^2, g^3, g^4, g^5$, where $1, g^2, g^4$, belong to the principal genus, and g, g^3, g^5, to the other genus. The characters refer to $\left(\frac{f}{5}\right)$, $\left(\frac{f}{7}\right)$, and the forms are

$++, (1, 0, 35)$ 1	$--, (3, -1, 12)$ g
$(4, 1, 9)$ g^2	$(5, 0, 7)$ g^3
$(4, -1, 9)$ g^4	$(3, 1, 12)$ g^5.

An instance of the case $n = 1$ is $D = -21$, there are here four genera each of a single form $1, c, c_1, cc_1$, where $c^2 = 1$, $c_1^2 = 1$; an instance of the case $n = 2$ is $D = -88$, there are here two genera each of two forms $1, c$, and c_1, cc_1, where $c^2 = 1$, $c_1^2 = 1$, thus there is here no form having the exponent $2n$. (See Cayley, *Tables, &c.*, in *Crelle*, t. LX., 1862, pp. 357—372, [335].) We may have 2^{k+1} genera, each of n forms, viz. such a system may be represented by $(1, \phi^2, \ldots, \phi^{2n-2}; \phi, \phi^3, \ldots, \phi^{2n-1})(1, c)(1, c_1)\ldots(1, c_{k-1})$, where $\phi^{2n} = 1$, $c^2 = 1$, $c_1^2 = 1, \ldots, c_{k-1}^2 = 1$; there is no peculiarity in the form ϕ: we may instead of it take any form such as $c\phi$, $cc_1\phi$, &c., for each of these is like ϕ, a form belonging to the exponent $2n$, and such that the even powers give the principal genus.

32. Ternary and higher quadratic forms—cubic forms, &c. The theory of the ternary quadratic forms

$$(a, b, c, a', b', c')(x, y, z)^2, = ax^2 + by^2 + cz^2 + 2a'yz + 2b'zx + 2c'xy,$$

or when only the coefficients are attended to, $\begin{pmatrix} a, & b, & c \\ a', & b', & c' \end{pmatrix}$, has been studied in a very complete manner; and those of the quaternary and higher quadratic forms have also been studied; in particular, the forms $x^2+y^2+z^2$, $x^2+y^2+z^2+w^2$ composed of three or four squares; and the like forms with five, six, seven, and eight squares. The binary cubic forms $(a, b, c, d)(x, y)^3$, $= ax^3 + 3bx^2y + 3cxy^2 + dy^3$, or when only the coefficients are attended to, (a, b, c, d), have also been considered, though the higher binary forms have been scarcely considered at all. The special ternary cubic forms $ax^3+by^3+cz^3+6lxyz$ have been considered. Special forms of the degree n with n variables, the products of linear factors, present themselves in the theory of the division of the circle (the Kreistheilung) and of the complex numbers connected therewith; but it can hardly be said that these have been studied as a part of the general theory of forms.

Complex Theories.

33. The complex theory which first presented itself is that of the numbers $a+bi$ composed with the imaginary i, $=\sqrt{-1}$; here if a and b are ordinary, or say simplex positive or negative integers, including zero, we regard $a+bi$ as an integer number, or say simply as a number in this complex theory. We have here a zero 0 ($a=0$, $b=0$) and the units 1, i, -1, $-i$, or as these may be written, 1, i, i^2, i^3 ($i^4=1$); the numbers $a+bi$, $a-bi$, are said to be conjugate numbers, and their product $(a+bi)(a-bi)$, $=a^2+b^2$, is the norm of each of them. And so the norm of the real number a is $=a^2$, and that of the pure imaginary number bi is $=b^2$. Denoting the norm by the letter N, $N(a \pm bi) = a^2+b^2$.

Any simplex prime number, $\equiv 1 \pmod 4$, is the sum of two squares a^2+b^2, for instance $13 = 9+4$, and it is thus a product $(a+bi)(a-bi)$, that is, it is not a prime number in the present theory, but each of these factors (or say any number $a+bi$, where a^2+b^2 is a prime number in the simplex theory) is a prime; and any simplex prime number, $\equiv 3 \pmod 4$, is also a prime in the present theory. The number $2, = (1+i)(1-i)$, is not a prime, but the factors $1+i$, $1-i$ are each of them prime; these last differ only by a unit factor i—$1 = i(1+i)$—so that $2, = -i(1+i)^2$, contains a square factor.

In the simplex theory we have numbers, for instance $5, -5$, differing from each other only by a unit factor, but we can out of these select one, say the positive number, and attend by preference to this number of the pair. It is in this way—viz. by restricting $a, b, c, \ldots$ to denote terms of the series 2, 3, 5, 7, ... of positive primes other than unity—that we are enabled to make the definite statement, a positive number N is, and that in one way only, $= a^\alpha b^\beta c^\gamma \ldots$; if N be a positive or negative number, then the theorem of course is, N is, and that in one way only, $= (-1)^m a^\alpha b^\beta c^\gamma \ldots$, where $m=0$, or 1, and $a, b, c, \ldots, \alpha, \beta, \gamma, \ldots$ are as before. To

obtain a like definite statement in the present theory, we require to distinguish between the four numbers $a+bi$, $-a-bi$, $-b+ai$, $b-ai$, which differ from each other only by a unit factor -1, $\pm i$. Consider a number $a+bi$ where a and b are the one of them odd and the other even (a and b may be either of them $=0$, the other is then odd), every prime number $a+bi$ other than $\pm 1 \pm i$ is necessarily of this form: for if a and b were both even, the number would be divisible by 2, or say by $(1+i)^2$, and if a and b were both odd, it would be divisible by $1+i$; then of the four associated numbers $a+bi$, $-a-bi$, $-b+ai$, $b-ai$, there is one and only one, $a+bi$, such that b is even and $a+b-1$ is evenly even; or say one and only one which is $\equiv 1 \pmod{2(1+i)}$. We distinguish such one of the four numbers from the other three and call it a *primary* number; the units ± 1, $\pm i$, and the numbers $\pm 1 \pm i$, are none of them primary numbers. We have then the theorem, a number N is in one way only $= i^m (1+i)^n A^\alpha B^\beta \ldots$, where $m = 0$, 1, 2, or 3, n is $=0$ or a positive integer, A, $B, \ldots$ are primary primes, α, $\beta, \ldots$ positive integers. Here i is a unit of the theory, $1+i$ is a special prime having reference to the number 2, but which might, by an extension of the definition, be called a primary prime, and so reckoned as one of the numbers A, $B, \ldots$; the theorem stated broadly still is that the number N is, and that in one way only, a product of prime factors, but the foregoing complete statement shows the precise sense in which this theorem must be understood. A like explanation is required in other complex theories; we have to select out of each set of primes differing only by unit factors some one number as a primary prime, and the general theorem then is that every number N is, and that in one way only, $= P . A^\alpha B^\beta C^\gamma \ldots$, where P is a product of unities, and A, B, $C, \ldots$ are primary primes.

34. We have in the simplex theory (*ante*, No. 10) the theorem that, p being an odd prime, there exists a system of $p-1$ residues, that is, that any number not divisible by p is, to the modulus p, congruent to one, and only one, of the $p-1$ numbers 1, 2, 3, ..., $p-1$. The analogous theorem in the complex theory is that, for any prime number p other than $\pm 1 \pm i$, there exists a system of $N(p)-1$ residues, that is, that every number not divisible by p is, to the modulus p, congruent to one of these $N(p)-1$ numbers.

But p may be a real prime such as 3, or a complex prime such as $3+2i$; and the system of residues presents itself naturally under very different forms in the two cases respectively. Thus in the case $p=3$, $N(3)=9$, the residues may be taken to be

$$\begin{array}{ccc} 1 & , 2 & , \\ i, & 1+i & , 2+i \\ 2i, & 1+2i, & 2+2i, \end{array}$$

being in number $N(3)-1=8$. And for $p=3+2i$, $N(3+2i)=13$, they may be taken to be the system of residues of 13 in the simplex theory, viz. the real numbers 1, 2, 3, ..., 12. We have in fact $5+i=(2+3i)(1-i)$, that is, $5+i \equiv 0 \pmod{2+3i}$, and consequently $a+bi \equiv a-5b$, a real number which, when $a+bi$ is not divisible by $3+2i$, may have any one of the foregoing values 1, 2, 3, ..., 12.

Taking then any number x not divisible by p, the $N(p)-1$ residues each multiplied by x are, to the modulus p, congruent to the series of residues in a different order; and we thus have,—say this is Fermat's theorem for the complex theory—$x^{N(p)-1}-1\equiv 0 \pmod{p}$, with all its consequences, in particular, the theory of prime roots.

In the case of a complex modulus such as $3+2i$, the theory is hardly to be distinguished from its analogue in the ordinary theorem; a prime root is $=2$, and the series of powers is 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, for the modulus $3+2i$ as for the modulus 13. But for a real prime such as 3 the prime root is a complex number; taking it to be $=2+i$, we have $(2+i)^3-1\equiv 0 \pmod{3}$, and the series of powers in fact is $2+i$, i, $2+2i$, 2, $1+2i$, $2i$, $1+i$, 1, viz. we thus have the system of residues (mod. 3).

We have in like manner a theory of quadratic residues; a Legendrian symbol $\left[\frac{p}{q}\right]$ (which, if p, q, are uneven primes not necessarily primary but subject to the condition that their imaginary parts are even, denotes $+1$ or -1 according as $p^{\frac{1}{2}(Nq-1)}$ is $\equiv 1$ or $\equiv -1 \pmod{q}$, so that $\left[\frac{p}{q}\right]=+1$ or -1 according as p is or is not a residue of q), a law of reciprocity expressed by the very simple form of equation $\left[\frac{p}{q}\right]=\left[\frac{q}{p}\right]$, and generally a system of properties such as that which exists in the simplex theory.

The theory of quadratic forms (a, b, c) has been studied in this complex theory; the results correspond to those of the simplex theory.

35. The complex theory with the imaginary cube root of unity has also been studied; the imaginary element is here γ, $=\frac{1}{2}(-1+\sqrt{-3})$, a root of the equation $\gamma^2+\gamma+1=0$; the form of the complex number is thus $a+b\gamma$, where a and b are any positive or negative integers, including zero. The conjugate number is $a+b\gamma^2$, $=a-b-b\gamma$, and the product $(a+b\gamma)(a+b\gamma^2)$, $=a^2-ab+b^2$, is the norm of each of the factors $a+b\gamma$, $a+b\gamma^2$. The whole theory corresponds very closely to, but is somewhat more simple than, that of the complex numbers $a+bi$.

36. The last-mentioned theory is a particular case of the complex theory for the imaginary λth roots of unity, λ being an odd prime. Here α is determined by the equation $\frac{\alpha^\lambda-1}{\alpha-1}=0$, that is, $\alpha^{\lambda-1}+\alpha^{\lambda-2}+\ldots+\alpha+1=0$, and the form of the complex number is $f(\alpha)$, $=a+b\alpha+c\alpha^2+\ldots+k\alpha^{\lambda-2}$, where $a, b, c, \ldots, k$, are any positive or negative integers, including zero. We have $\lambda-1$ conjugate forms, viz. $f(\alpha), f(\alpha^2), \ldots, f(\alpha^{\lambda-1})$, and the product of these is the norm of each of the factors $Nf(\alpha)$, $=Nf(\alpha^2)$, $=\ldots$, $=Nf(\alpha^{\lambda-1})$. Taking g any prime root of λ, $g^{\lambda-1}-1\equiv 0 \pmod{\lambda}$, the roots $\alpha, \alpha^2, \ldots, \alpha^{\lambda-1}$, may be arranged in the order $\alpha, \alpha^g, \alpha^{g^2}, \ldots, \alpha^{g^{\lambda-2}}$; and we have thence a grouping of the roots in periods, viz. if $\lambda-1$ be in any manner whatever expressed as a product of two factors, $\lambda-1=ef$, we may with the $\lambda-1$ roots form e periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$, each of

f roots. For instance, when $\lambda = 13$, a prime root is $g = 2$, and $\lambda - 1 = ef = 3 \cdot 4$; then the three periods each of four roots are

$$\eta_0 = \alpha + \alpha^8 + \alpha^{12} + \alpha^5,$$
$$\eta_1 = \alpha^2 + \alpha^3 + \alpha^{11} + \alpha^{10},$$
$$\eta_2 = \alpha^4 + \alpha^6 + \alpha^9 + \alpha^7.$$

So also, if $ef = 2 \cdot 6$, then the 2 periods each of 6 roots are

$$\eta_0 = \alpha + \alpha^4 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^{10},$$
$$\eta_1 = \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{11} + \alpha^5 + \alpha^7;$$

and so in other cases. In particular, if $f = 1$ and consequently $e = \lambda - 1$, the e periods each of f roots are, in fact, the single roots $\alpha, \alpha^g, \ldots, \alpha^{g^{\lambda-2}}$. We may, in place of the original form of the complex number

$$f(\alpha) = a + b\alpha + c\alpha^2 + \ldots + k\alpha^{\lambda-2},$$

consider the new form $f(\eta) = a\eta + b\eta_1 + \ldots + l\eta_{e-1}$, which when $f = 1$ is equivalent to the original form, but in any other case denotes a special form of complex number; instead of $\lambda - 1$ we have only e conjugate numbers, and the product of these e numbers may be regarded as the norm of $f(\eta)$.

37. The theory for the roots α includes as part of itself the theory for the periods corresponding to every decomposition whatever $\lambda - 1 = ef$ of $\lambda - 1$ into two factors, but each of these may be treated apart from the others as a theory complete in itself. In particular, a simple case is that of the half-periods $e = 2$, $f = \frac{1}{2}(\lambda - 1)$; and, inasmuch as the characteristic phenomenon of ideal numbers presents itself in this theory of the half-periods (first for the value $\lambda = 23$), it will be sufficient, by way of illustration of the general theory, to consider only this more special and far easier theory; we may even assume $\lambda = 23$.*

For the case in question, $\lambda - 1 = ef = 2 \cdot \frac{1}{2}(\lambda - 1)$, we have the two periods η_0, η_1, each of $\frac{1}{2}(\lambda - 1)$ roots; from the expressions for η_0, η_1, in terms of the roots we obtain at once $\eta_0 + \eta_1 = -1$, and with a little more difficulty $\eta_0\eta_1 = -\frac{1}{4}(\lambda - 1)$ or $\frac{1}{4}(\lambda + 1)$, according as λ is $\equiv 1$ or $3 \pmod 4$, that is, in the two cases respectively η_0, η_1, are the roots of the equation $\eta^2 + \eta - \frac{1}{4}(\lambda - 1) = 0$, and $\eta^2 + \eta + \frac{1}{4}(\lambda + 1) = 0$. And this equation once obtained, there is no longer any occasion to consider the original equation of the order $\lambda - 1$, but the theory is that of the complex numbers $a\eta_0 + b\eta_1$, or

* In the theory of the roots α, ideal numbers do not present themselves for the values $\lambda = 3$, 5, or 7; they do for the value $\lambda = 23$. It is stated in Smith's "Report on the Theory of Numbers," *Brit. Assoc. Report* for 1860, p. 136, [Collected Works, vol. 1. p. 114], that "for $\lambda = 11$, $\lambda = 13$, $\lambda = 17$, and $\lambda = 19$, it is not possible to say whether this is or is not the case for these values also." The writer is not aware whether this question has been settled; but in Reuschle's *Tafeln*, 1875, no ideal factors present themselves for these values of λ; and it is easy to see that, in the theory of the half-periods, the ideal factors first present themselves for the value $\lambda = 23$. It may be remarked that the solution of the question depends on the determination of a system of fundamental units for the values in question $\lambda = 11$, 13, 17, and 19; the theory of the units in the several complex theories is an important and difficult part of the theory, not presenting itself in the theory of the half-periods, which is alone attended to in the text.

if we please $a+b\eta$, composed with the roots of this quadric equation,—say the complex numbers $a+b\eta$, where a and b are any positive or negative integer numbers, including zero. In the case $\lambda=23$, the quadric equation is $\eta^2+\eta+6=0$. We have $N(a+b\eta)=(a+b\eta_0)(a+b\eta_1)=a^2-ab+\frac{1}{4}(\lambda+1)b^2$; and for $\lambda=23$, this is $N(a+b\eta)=a^2-ab+6b^2$. It may be remarked that there is a connexion with the theory of the quadratic forms of the determinant -23, viz. there are here the three improperly primitive forms (2, 1, 12), (4, 1, 6), (4, −1, 6), 23 being the smallest prime number for which there exists more than one improperly primitive form.

38. Considering then the case $\lambda=23$, we have η_0, η_1, the roots of the equation $\eta^2+\eta+6=0$; and a real number P is composite when it is $=(a+b\eta_0)(a+b\eta_1)$, $=a^2-ab+6b^2$, viz. if $4P=(2a-b)^2+23b^2$. Hence no number, and in particular no positive real prime P, can be composite unless it is a (quadratic) residue of 23; the residues of 23 are 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18; and we have thus, for instance, 5, 7, 11, as numbers which are *not* composite, while 2, 3, 13, are numbers which are not by the condition precluded from being composite: they are not, according to the foregoing signification of the word, composite (for 8, 12, 52, are none of them of the form x^2+23y^2), but *some* such numbers, residues that is of 23, are composite, for instance 59, $=(5-2\eta_0)(5-2\eta_1)$. And we have an indication, so to speak, of the composite nature of *all* such numbers; take for instance 13, we have $(\eta-4)(\eta+5)=-2.13$, where 13 does not divide either $\eta-4$ or $\eta+5$, and we are led to conceive it as the product of two ideal factors, one of them dividing $\eta-4$, the other dividing $\eta+5$. It appears, moreover, that a power 13^3 is in fact composite, viz. we have

$$13^3=(31-12\eta_0)(31-12\eta_1),\quad (2197=961+372+864);$$

and writing $13=\sqrt[3]{31-12\eta_0}.\sqrt[3]{31-12\eta_1}$ we have 13 as the product of two ideal numbers each represented as a cube root; it is to be observed that, 13 being in the simplex theory a prime number, these are regarded as prime ideal numbers. We have in like manner

$$2=\sqrt[3]{1-\eta_0}.\sqrt[3]{1-\eta_1},\quad 3=\sqrt[3]{1-2\eta_0}.\sqrt[3]{1-2\eta_1},\ \&c.;$$

every positive real prime which is a residue of 23 is thus a product of two factors ideal or actual. And, reverting to the equation $(\eta-4)(\eta+5)=-2.13$, or as this may be written

$$(\eta_1-4)(\eta_1+5)=-\sqrt[3]{1-\eta_0}\sqrt[3]{1-\eta_1}\sqrt[3]{31-12\eta_0}\sqrt[3]{31-12\eta_1},$$

we have $(\eta_1-4)^3$ and $(1-\eta_0)(31-12\eta_0)$ each $=14+55\eta_1$, or say

$$\eta_1-4=\sqrt[3]{1-\eta_0}\sqrt[3]{31-12\eta_0},$$

and similarly

$$\eta_1+5=-\sqrt[3]{1-\eta_1}\sqrt[3]{31-12\eta_1},$$

so that we verify that η_1-4, η_1+5, do thus in fact each of them contain an ideal factor of 13.

39. We have $2=\sqrt[3]{1-\eta_0}\sqrt[3]{1-\eta_1}$, viz. the ideal multiplier $\sqrt[3]{1-\eta_0}$ renders actual one of the ideal factors $\sqrt[3]{1-\eta_1}$ of 2, and it is found that this same ideal multiplier

$\sqrt[3]{1-\eta_0}$ renders actual one of the two ideal factors of any other decomposable number 3, 13, &c.,

$$\sqrt[3]{1-2\eta_0}\sqrt[3]{1-\eta_0} = 1+\eta_0, \quad \sqrt[3]{31-12\eta_0}\sqrt[3]{1-\eta_0} = -5-\eta_0, \text{ &c.}$$

Similarly the conjugate multiplier $\sqrt[3]{1-\eta_1}$ renders actual the other ideal factor of any number 2, 3, 13, &c. We have thus two classes, or, reckoning also actual numbers, three classes of prime numbers, viz. (i) ideal primes rendered actual by the multiplier $\sqrt[3]{1-\eta_0}$, (ii) ideal primes rendered actual by the multiplier $\sqrt[3]{1-\eta_1}$, (iii) actual primes. This is a general property in the several complex theories; there is always a finite number of classes of ideal numbers, distinguished according to the multipliers by which they are rendered actual; the actual numbers form a "principal" class.

40. General theory of congruences—irreducible functions. In the complex theory relating to the roots of the equation $\eta^2+\eta+6=0$, there has just been occasion to consider the equation $(\eta-4)(\eta+5)=-2.13$, or say the congruence $(\eta-4)(\eta+5)\equiv 0 \pmod{13}$; in this form the relation $\eta^2+\eta+6=0$ is presupposed, but if, dropping this equation, η be regarded as arbitrary, then there is the congruence $\eta^2+\eta+6\equiv(\eta-4)(\eta+5) \pmod{13}$. For a different modulus, for instance 11, there is not any such congruence exhibiting a decomposition of $\eta^2+\eta+6$ into factors. The function $\eta^2+\eta+6$ is irreducible, that is, it is not a product of factors with integer coefficients; in respect of the modulus 13 it becomes reducible, that is, it breaks up into factors having integer coefficients, while for the modulus 11 it continues irreducible. And there is a like general theory in regard to any rational and integral function $F(x)$ with integer coefficients; such function, assumed to be irreducible, may for a given prime modulus p continue irreducible, that is, it may not admit of any decomposition into factors with integer coefficients; or it may become reducible, that is, admit of a decomposition $F(x)\equiv\phi(x)\psi(x)\chi(x)\ldots \pmod{p}$. And, when this is so, it is thus a product, in one way only, of factors $\phi(x)$, $\psi(x)$, $\chi(x)$, ..., which are each of them irreducible in regard to the same modulus p; any such factor may be a linear function of x, and as such irreducible; or it may be an irreducible function of the second or any higher degree. It is hardly necessary to remark that, in this theory, functions which are congruent to the modulus p are regarded as identical, and that in the expression of $F(x)$ an irreducible function $\phi(x)$ may present itself either as a simple factor, or as a multiple factor, with any exponent. The decomposition is analogous to that of a number into its prime factors; and the whole theory of the rational and integral function $F(x)$ in regard to the modulus p is in many respects analogous to that of a prime number regarded as a modulus. The theory has also been studied where the modulus is a power p^ν.

41. The congruence-imaginaries of Galois. If $F(x)$ be an irreducible function to a given prime modulus p, this implies that there is no integer value of x satisfying the congruence $F(x)\equiv 0 \pmod{p}$; we assume such a value and call it i, that is, we assume $F(i)\equiv 0 \pmod{p}$; the step is exactly analogous to that by which, starting from the notion of a real root, we introduce into algebra the ordinary imaginary $i=\sqrt{-1}$. For instance, x^2-x+3 is an irreducible function to the modulus 7: there is no integer solution of the congruence $x^2-x+3\equiv 0 \pmod{7}$. Assuming a solution i such that

$i^2 - i + 3 \equiv 0 \pmod 7$, we have, always to this modulus, $i^2 = i - 3$, and thence i^3, i^4, &c., each of them equal to a linear function of i. We consider the numbers of the form $a + bi$, where a and b are ordinary integers which may be regarded as having each of them the values 0, 1, 2, 3, 4, 5, or 6; there are thus 7^2, $= 49$, such numbers, or, excluding zero, 48 numbers; and it is easy to verify that these are, in fact, the numbers $i, i^2, \ldots, i^{47}, i^{48}, = 1$, that is, we have i a prime root of the congruence $x^{48} - 1 \equiv 0 \pmod 7$. The irreducible function may be of the third or any higher degree; thus for the same modulus 7 there is the cubic function $x^3 - x + 2$, giving rise to a theory of the numbers of the form $a + bi + ci^2$, where i is a congruence-imaginary such that $i^3 - i + 2 \equiv 0 \pmod 7$; and instead of 7 the modulus may be any other odd prime p.

Ordinary Theory, Third Part.

42. In what precedes, no mention has been made of the so-called Pellian equation $x^2 - Dy^2 = 1$ (where D is a given positive number), and of the allied equations $x^2 - Dy^2 = -1$, or $= \pm 4$. The equations with the sign + have always a series of solutions, those with the sign − only for certain values of D; in every case where the solutions exist, a least solution is obtainable by a process depending on the expression of $\sqrt{D}$ as a continued fraction, and from this least solution the whole series of solutions can be obtained without difficulty. The equations are very interesting, as well for their own sake as in connexion with the theory of the binary quadratic forms of a positive non-square determinant.

43. The theory of the expression of a number as a sum of squares or polygonal numbers has been developed apart from the general theory of the binary, ternary, and other quadratic forms to which it might be considered as belonging. The theorem for two squares, that every prime number of the form $4n + 1$ is, and that in one way only, a sum of two squares, is a fundamental theorem in relation to the complex numbers $a + bi$. A sum of two squares multiplied by a sum of two squares is always a sum of two squares, and hence it appears that every number of the form $2^\alpha(4n + 1)$ is (in general, in a variety of ways) a sum of two squares.

Every number of the form $4n + 2$ or $8n + 3$ is a sum of three squares; even in the case of a prime number $8n + 3$ there is in general more than one decomposition, thus $59 = 25 + 25 + 9$ and $= 49 + 9 + 1$. Since a sum of three squares multiplied by a sum of three squares is not a sum of three squares, it is not enough to prove the theorem in regard to the primes of the form $8n + 3$.

Every prime number is (in general, in more than one way) a sum of four squares; and therefore every number is (in general, in more than one way) a sum of four squares, for a sum of four squares multiplied by a sum of four squares is always a sum of four squares.

Every number is (in general, in several ways) a sum of $m + 2$ $(m + 2)$gonal numbers, that is, of numbers of the form $\frac{1}{2}m(x^2 - x) + x$; and of these $m - 2$ may be at pleasure equal to 0 or 1; in particular, every number is a sum of three triangular numbers (a theorem of Fermat's).

The theorems in regard to three triangular numbers and to four square numbers are exhibited by certain remarkable identities in the Theory of Elliptic Functions; and generally there is in this subject a great mass of formulæ connected with the theory of the representation of numbers by quadratic forms. The various theorems in regard to the number of representations of a number as the sum of a definite number of squares cannot be here referred to.

44. The equation $x^\lambda + y^\lambda = z^\lambda$, where λ is any positive integer greater than 2, is not resoluble in whole numbers (a theorem of Fermat's). The general proof depends on the theory of the complex numbers composed of the λth roots of unity, and presents very great difficulty; in particular, distinctions arise according as the number λ does or does not divide certain of Bernoulli's numbers.

45. Lejeune-Dirichlet employs, for the determination of the number of quadratic forms of a given positive or negative determinant, a remarkable method depending on the summation of a series Σf^{-s}, where the index s is greater than but indefinitely near to unity.

46. Very remarkable formulæ have been given by Legendre, Tchebycheff, and Riemann for the approximate determination of the number of prime numbers less than a given large number x. Factor tables have been formed for the first nine million numbers, and the number of primes counted for successive intervals of 50,000; and these are found to agree very closely with the numbers calculated from the approximate formulæ. Legendre's expression is of the form $\frac{x}{\log x - A}$, where A is a constant not very different from unity; Tchebycheff's depends on the logarithm-integral $\mathrm{li}(x)$; and Riemann's, which is the most accurate, but is of a much more complicated form, contains a series of terms depending on the same integral.

The classical works on the Theory of Numbers are Legendre, *Théorie des Nombres*, 1st ed. 1798, 3rd ed. 1830; Gauss, *Disquisitiones Arithmeticæ*, Brunswick, 1801 (reprinted in the collected works, vol. I., Göttingen, 1863; French translation, under the title *Recherches Arithmétiques*, by Poullet-Delisle, Paris, 1807); and Lejeune-Dirichlet, *Vorlesungen über Zahlentheorie*, 3rd ed., with extensive and valuable additions by Dedekind, Brunswick, 1879—81. We have by the late Prof. H. J. S. Smith the extremely valuable series of "Reports on the Theory of Numbers," Parts I. to VI., *British Association Reports*, 1859—62, 1864—65, which, with his own original researches, [are] printed in the [first volume of the] collected works [published in 1894] by the Clarendon Press. See also Cayley, "Report of the Mathematical Tables Committee," *Brit. Assoc. Report*, 1875, pp. 305—336, [611], for a list of tables relating to the Theory of Numbers, and Mr J. W. L. Glaisher's introduction to the *Factor Table for the Sixth Million*, London, 1883, in regard to the approximate formulæ for the number of prime numbers.