SECTION VII

EQUATIONS DEFINING SECTIONS OF A CIRCLE

▶ 335. Among the splendid developments contributed by modern mathematicians, the theory of circular functions without doubt holds a most important place. We often have occasion in a variety of contexts to refer to this remarkable type of quantity, and there is no part of general mathematics that does not depend on it in some fashion. Since the most brilliant modern mathematicians by their industry and shrewdness have built it into an extensive discipline, one would hardly expect any part of the theory, let alone an elementary part, could be significantly expanded. I refer to the theory of trigonometric functions corresponding to arcs that are commensurable with the circumference, i.e., the theory of regular polygons. Only a small part of this theory has been developed so far, as the present section will make clear. The reader might be surprised to find a discussion of this subject in the present work which deals with a discipline apparently so unrelated; but the treatment itself will make abundantly clear that there is an intimate connection between this subject and higher Arithmetic.

The principles of the theory which we are going to explain actually extend much farther than we will indicate. For they can be applied not only to circular functions but just as well to other transcendental functions, e.g. to those which depend on the integral $\int [1/\sqrt{(1 - x^4)}]dx$ and also to various types of congruences. Since, however, we are preparing a large work on those transcendental functions and since we will treat congruences at length in the continuation of these *Disquisitiones*, we have decided to consider only circular functions here. And although we could discuss them in all their generality, we reduce them to the simplest case in the following article, both for the sake of brevity and in order that the new principles of this theory may be more easily understood.

Gauss initiated the study of elliptic curves over finite fields

The discussion is reduced to the simplest case in which the number of parts into which the circle is cut is a prime number

▶ 336. If we designate the circumference of the circle or four right angles by P, and if m, n are integers and n a product of relatively prime factors a, b, c, etc.: the angle $A = mP/n$ can be reduced by the methods of article 310 to the form $A = [(\alpha/a) + (\beta/b) + (\gamma/c) + \text{etc.}]P$, and the trigonometric functions corresponding to it can be found by known methods from those for the parts $\alpha P/a$, $\beta P/b$, etc. Therefore, since we can take a, b, c, etc. to be prime numbers or powers of prime numbers, it is sufficient to consider the division of the circle into parts whose number is a prime or the power of a prime, and we can immediately get a polygon of n sides from the polygons of a, b, c, etc. sides. However, we will restrict our discussion to the case where the circle is divided into an (odd) prime number of parts, especially for the following reason. It is clear that circular functions corresponding to the angle mP/p^2 are derived from functions belonging to mP/p by the solution of an equation of degree p. And from these by an equation of the same degree we can derive functions belonging to mP/p^3 etc. Therefore if we already have a polygon of p sides, to determine a polygon of p^λ sides we necessarily require the solution of $\lambda - 1$ equations of degree p. Even though the following theory could be extended to this case also, nevertheless we could not avoid so many equations of degree p, and there is no way of reducing their degree if p is prime. Thus, e.g., it will be shown below that a polygon of 17 sides can be constructed geometrically; but to get a polygon of 289 sides there is no way to avoid solving an equation of degree 17.

Equations for trigonometric functions of arcs which are a part or parts of the whole circumference: reduction of trigonometric functions to the roots of the equation $x^n - 1 = 0$

▶ 337. It is well known that the trigonometric functions of all the angles kP/n where k denotes in general all the numbers $0, 1, 2, \ldots n - 1$, are expressed by the roots of equations of degree n. The *sines* are the roots of equation (I):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx = 0$$

the *cosines* are the roots of equation (II):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx \mp \frac{1}{2^{n-1}} = 0$$

and the *tangents* are the roots of equation (III):

$$x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \text{etc.} \pm nx = 0$$

These equations are all true for any odd value of n, and equation II is true for even values also. If we set $n = 2m + 1$ they can be easily reduced to degree m; for I and III this just requires dividing on the left by x and substituting y for x^2. Equation II however includes the root $x = 1\,(= \cos 0)$ and all the others are equal in pairs ($\cos P/n = \cos(n-1)P/n$, $\cos 2P/n = \cos(n-2)P/n$, etc.); thus the left side is divisible by $x - 1$ and the quotient will be a square. If we extract the square root, equation II is reduced to the following:

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3}$$

$$+ \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - \text{etc.} = 0$$

Its roots will be the cosines of the angles $P/n, 2P/n, 3P/n, \ldots mP/n$. Up to now there have not been any further reductions of these equations for the case where n is a prime number.

Nevertheless none of these equations is so tractable and so suitable for our purposes as $x^n - 1 = 0$. Its roots are intimately connected with the roots of the above. That is, if for brevity we write i for the imaginary quantity $\sqrt{-1}$, the roots of the equation $x^n - 1 = 0$ will be

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r$$

where for k we should take all the numbers $0, 1, 2, \ldots n-1$. Therefore since $1/r = \cos kP/n - i\sin kP/n$ the roots of equation I will be $[r - (1/r)]/2i$ or $i(1 - r^2)/2r$; the roots of equation II, $[r + (1/r)]/2 = (1 + r^2)/2r$; finally the roots of equation III, $i(1 - r^2)/(1 + r^2)$. For this reason we build our investigation on a consideration of the equation $x^n - 1 = 0$, and presume that n is an odd prime number. In order not to interrupt the order of the investigation we will first consider the following lemma.

▶ 338. PROBLEM. *Given the equation*

$$(W) \ldots z^m + Az^{m-1} + \text{etc.} = 0$$

to find the equation (W') *whose roots are the* λ*th power of the roots of equation* (W)*, where* λ *is a given positive integral exponent.*

Solution. If we designate the roots of the equation W by a, b, c, etc., the roots of the equation W' will be $a^\lambda, b^\lambda, c^\lambda$, etc. By a well-known theorem of Newton, from the coefficients of equation W we can find the sum of any powers of the roots a, b, c, etc. Therefore, we find the sums

$$a^\lambda + b^\lambda + c^\lambda + \text{etc.}, \qquad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} + \text{etc.},$$

$$\text{up to } a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{etc.}$$

and by an inverse procedure according to the same theorem, the coefficients of the equation W' can be deduced. Q.E.F. At the same time it is clear that if all the coefficients of W are rational, all those in W' will also be rational. And by another method it can be proven that if all the former are integers, the latter will be integers also. We will not spend more time on this theorem here, since it is not necessary for our purpose.

▶ 339. The equation $x^n - 1 = 0$ (we will always presume that n is an odd prime number) has only one real root, $x = 1$; the remaining $n - 1$ roots which are given by the equation

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$$

are all imaginary; we will denote their complex by Ω and the function

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 \text{ by } X.$$

If therefore r is any root in Ω, we will have $1 = r^n = r^{2n}$ etc. and in general $r^{en} = 1$ for any positive or negative integral value of e. Thus if λ, μ are integers which are congruent relative to n, we will have $r^\lambda = r^\mu$. But if λ, μ are noncongruent relative to n, then r^λ and r^μ will be unequal; for in this case we can find an integer ν such that $(\lambda - \mu)\nu \equiv 1 \pmod{n}$ so $r^{(\lambda-\mu)\nu} = r$ and certainly $r^{\lambda-\mu}$ does not $= 1$. It is also clear that any power of r is also a root of the equation $x^n - 1 = 0$. Therefore, since the quantities $1 (= r^0)$,

$r, r^2, \ldots r^{n-1}$ are all different, they will give us all the roots of the equation $x^n - 1 = 0$ and so the numbers $r, r^2, r^3, \ldots r^{n-1}$ will coincide with Ω. More generally, then, Ω will coincide with $r^e, r^{2e}, r^{3e}, \ldots r^{(n-1)e}$ if e is any positive or negative integer not divisible by n. We have therefore

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$$

and from this

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1$$

and

$$1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

If we have two roots such as r and $1/r$ $(= r^{n-1})$ or in general r^e and r^{-e}, we will call them *reciprocal* roots. Manifestly the product of two simple factors $x - r$ and $x - (1/r)$ is real and $= x^2 - 2x \cos \omega + 1$ where the angle ω is equal either to the angle P/n or some multiple of it.

► 340. Since by designating one root in Ω by r we can express all roots of the equation $x^n - 1 = 0$ by powers of r, the product of several roots of this equation can be expressed by r^λ in such a way that λ is either 0 or positive and $< n$. Therefore if we let $\phi(t, u, v, \ldots)$ be a rational integral algebraic function of the unknowns t, u, v, etc. which is the sum of terms of the form $ht^\alpha u^\beta v^\gamma \ldots$: manifestly if we substitute roots of the equation $x^n - 1 = 0$ for t, u, v, etc., say $t = a, u = b, v = c$, etc. then $\phi(a, b, c, \ldots)$ can be reduced to the form

$$A + A'r + A''r^2 + A'''r^3 + \ldots + A^\nu r^{n-1}$$

in such a way that the coefficients A, A', etc. (some of them can be missing and so $= 0$) are determined quantities. And all of these coefficients will be integers if all the coefficients in $\phi(t, u, v, \ldots)$, i.e. all the h, are integers. And if after this we substitute $a^2, b^2, c^2, \ldots$ for $t, u, v, \ldots$ respectively, each term $ht^\alpha u^\beta v^\gamma, \ldots$ which had been reduced to r^σ will now become $r^{2\sigma}$ and thus

$$\phi(a^2, b^2, c^2, \ldots) = A + A'r^2 + A''r^4 + A'''r^6 + \ldots + A^\nu r^{2n-2}$$

And in general for any integral value of λ,

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

This proposition is very important and is fundamental to the following discussion. It also follows from this that

$$\phi(1, 1, 1, \ldots) = \phi(a^n, b^n, c^n, \ldots) = A + A' + A'' + \ldots + A^\nu$$

and

$$\phi(a, b, c, \ldots) + \phi(a^2, b^2, c^2, \ldots) + \phi(a^3, b^3, c^3, \ldots) + \phi(a^n, b^n, c^n, \ldots) = nA$$

Hence this sum is integral and divisible by n when all the coefficients in $\phi(t, u, v, \ldots)$ are integers.

Theory of the roots of the equation $x^n - 1 = 0$ (where n is assumed to be prime)

▶ 341. THEOREM. *If the function X is divisible by the function of lower degree*

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L$$

the coefficients $A, B, \ldots L$ cannot all be integers.

Except for the root 1, the remaining roots contained in (Ω) are included in the equation $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$; the function X cannot be decomposed into factors in which all the coefficients are rational

Demonstration. Let $X = PQ$ and $\mathfrak{P}$ the complex of the roots of the equation $P = 0$, $\mathfrak{Q}$ the complex of the roots of the equation $Q = 0$, so that Ω consists of $\mathfrak{P}$ and $\mathfrak{Q}$ taken together. Further let $\mathfrak{R}$ be the complex of reciprocal roots of $\mathfrak{P}$, $\mathfrak{S}$ the complex of reciprocal roots of $\mathfrak{Q}$ and let the roots which are contained in $\mathfrak{R}$ be roots of the equation $R = 0$ (this becomes $x^\lambda + (Kx^{\lambda-1}/L) + \text{etc.} + (Ax/L) + (1/L) = 0$) and let those that are contained in $\mathfrak{S}$ be roots of the equation $S = 0$. Manifestly if we take the roots $\mathfrak{R}$ and $\mathfrak{S}$ together we will get the complex Ω and $RS = X$. Now we must distinguish four cases.

I. When $\mathfrak{P}$ coincides with $\mathfrak{R}$ and consequently $P = R$. In this case obviously pairs of roots in $\mathfrak{P}$ will always be reciprocal and so P will be the product of $\lambda/2$ paired factors $x^2 - 2x\cos\omega + 1$; since such a factor $= (x - \cos\omega)^2 + \sin\omega^2$, it is clear that for any real value of x, P necessarily has a real positive value. Let the equations whose roots are the square, cubic, biquadratic, ... $n - 1$st powers of the roots in $\mathfrak{P}$ be respectively $P' = 0$, $P'' = 0$, $P''' = 0$, ... $P^\nu = 0$ and let the values of the functions $P, P', P'', \ldots P^\nu$ which are obtained by letting $x = 1$ be respectively $p, p', p'', \ldots p^\nu$. Then by what we have said before, p will be a positive quantity, and for a similar reason p', p'', etc. will also be positive. Since therefore p is the value of the function $(1 - t)(1 - u)(1 - v)$ etc. which is obtained by substituting for t, u, v, etc. the roots contained

in $\mathfrak{P}$; p' the value of the same function obtained by substituting for t, u, v, etc. the squares of those roots etc.; and 0 its value when $t = 1$, $u = 1$, $v = 1$ etc.: the sum $p + p' + p'' \ldots p^{\lambda}$ will be an integer divisible by n. Further the product $PP'P'' \ldots$ will be $= X^{\lambda}$ and so $pp'p'' \ldots = n^{\lambda}$.

Now if all the coefficients in P were rational, all of those in P', P'', etc. would also be rational by article 338. However by article 42 all these coefficients would have to be integers. Thus p, p', p'', etc. would also be integers. And since their product is n^{λ} and their number is $n - 1 > \lambda$, some of them (at least $n - 1 - \lambda$) must $= 1$, and the others equal either to n or to a power of n. And if g of them $= 1$, the sum $p + p' +$ etc. will be $\equiv g \pmod{n}$ and so certainly not divisible by n. Thus our supposition is inconsistent.

II. When $\mathfrak{P}$ and $\mathfrak{R}$ do not coincide but contain some common roots, let $\mathfrak{T}$ be this complex and $T = 0$, the equation of which they are the roots. Then T will be the greatest common divisor of the functions P, R (as is clear from the theory of equations). However, pairs of roots in $\mathfrak{T}$ will be reciprocal and as we saw before not all the coefficients in T can be rational. But this would certainly happen if all those of P and thus also of R were rational, as one can see from the nature of the operation by which we find the greatest common divisor. Thus our supposition is absurd.

III. When $\mathfrak{Q}$ and $\mathfrak{S}$ either coincide or have common roots, we can show in exactly the same way that not all the coefficients in Q are rational; but they would be rational if all those in P were rational, so this is impossible.

IV. If $\mathfrak{P}$ has no root in common with $\mathfrak{R}$, and $\mathfrak{Q}$ none in common with $\mathfrak{S}$, all the roots $\mathfrak{P}$ would necessarily be found in $\mathfrak{S}$, and all the roots $\mathfrak{Q}$ in $\mathfrak{R}$. Therefore $P = S$ and $Q = R$, and so $X = PQ$ will be the product of P times R; i.e.

$$\text{of } x^{\lambda} + Ax^{\lambda-1} \ldots + Kx + L \text{ times } x^{\lambda} + \frac{K}{L}x^{\lambda-1} \ldots + \frac{A}{L}x + \frac{1}{L}$$

So letting $x = 1$, we have

$$nL = (1 + A \ldots + K + L)^2$$

Now if all coefficients in P were rational, and so by article 42

also integers, L, which must divide the last coefficient in X, i.e. unity, will necessarily $= \pm 1$ and so $\pm n$ would be a square. But since this is contrary to the hypothesis, the supposition is inconsistent.

By this theorem therefore it is clear that no matter how X is decomposed into factors, some of the coefficients at least will be irrational, and so cannot be determined except by an equation of a degree higher than unity.

Declaration of the purpose of the following discussions

▶ 342. It is not without some value to declare in a few words the purpose of the following discussions. We intend to resolve X *gradually* into more and more factors, and in such a way that their coefficients are determined by equations of as low an order as possible. In so doing we will finally come to simple factors or to the roots Ω. We will show that if the number $n - 1$ is resolved in any way into integral factors α, β, γ, etc. (we can assume each of them is prime), X can be resolved into α factors of degree $(n-1)/\alpha$ with coefficients determined by an equation of degree α; each of these will be resolved into β others of degree $(n-1)/\alpha\beta$ with the aid of an equation of degree β etc. Thus if we designate by ν the number of factors α, β, γ, etc. the determination of the roots Ω is reduced to the solution of ν equations of degree α, β, γ, etc. For example, for $n = 17$ where $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, there will be four quadratic equations to solve; for $n = 73$ three quadratic and two cubic equations.

In what follows we will often have to consider powers of the root r whose exponents are again powers, and expressions of this sort are very hard to set up in type. Therefore to simplify the printing we will use the following abbreviation. For r, r^2, r^3, etc. we will write $[1], [2], [3]$, etc. and in general for r^λ where λ is any integer, we will write $[\lambda]$. Such expressions are not completely determined, but they will become so as soon as we take a specific root from Ω for r or $[1]$. In general $[\lambda], [\mu]$ will be equal or unequal according as λ, μ are congruent or noncongruent relative to the modulus n. Further $[0] = 1$; $[\lambda] \cdot [\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$; the sum $[0] + [\lambda] + [2\lambda] \ldots + [(n-1)\lambda]$ is either 0 or n according as λ is not divisible or divisible by n.

▶ 343. If, for the modulus n, g is the sort of number we called a primitive root in Section III, the $n - 1$ numbers $1, g, g^2, \ldots g^{n-2}$ will be congruent to the numbers $1, 2, 3, \ldots n - 1$ relative to the

modulus n. The order will be different, but every number in one series will be congruent to one in the other. From this it follows immediately that the roots $[1], [g], [g^2], \ldots [g^{n-2}]$ coincide with Ω. By a similar argument the roots

All the roots in (Ω) are distributed into certain classes (periods)

$$[\lambda], [\lambda g], [\lambda g^2], \ldots [\lambda g^{n-2}]$$

will coincide with Ω when λ is any integer not divisible by n. Further since $g^{n-1} \equiv 1 \pmod{n}$ it is easy to see that the two roots $[\lambda g^\mu], [\lambda g^\nu]$ will be identical or different according as μ, ν are congruent or noncongruent relative to $n - 1$.

If therefore G is another primitive root, the roots $[1], [g] \ldots [g^{n-2}]$ will also coincide with $[1], [G], \ldots [G^{n-2}]$ except for order. Further, if e is a divisor of $n - 1$, and we set $n - 1 = ef$, $g^e = h$, $G^e = H$, then the f numbers $1, h, h^2, \ldots h^{f-1}$ will be congruent to $1, H, H^2, \ldots H^{f-1}$ relative to n (without respect to order). For suppose that $G \equiv g^\omega \pmod{n}$ and that μ is an arbitrary positive number $< f$ and that ν is the least residue of $\mu\omega \pmod{f}$: then we will have $\nu e \equiv \mu\omega e \pmod{n-1}$ and so $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$ or $H^\mu \equiv h^\nu$; i.e. any number in the second series $1, H, H^2$, etc. will be congruent to a number in the series $1, h, h^2, \ldots$ and vice versa. Thus the f roots $[1], [h], [h^2], \ldots [h^{f-1}]$ will be identical with $[1], [H], [H^2], \ldots [H^{f-1}]$. In the same way it is easy to see that the more general series

The cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ has a unique subgroup of each size $d \mid (p-1)$.

$$[\lambda], [\lambda h], [\lambda h^2], \ldots [\lambda h^{f-1}] \quad \text{and} \quad [\lambda], [\lambda H], [\lambda H^2], \ldots [\lambda H^{f-1}]$$

coincide. We will designate the *sum* of f such roots, $[\lambda] + [\lambda h] + \text{etc.} + [\lambda h^{f-1}]$ by (f, λ). Since it is not changed by taking a different primitive root g, it must be considered as independent of g. And we will call the *complex* of the same roots the *period* (f, λ) and we disregard the order of the roots.[a] To display such a period it will be convenient to reduce each root to its simplest expression, that is, to substitute for the numbers $\lambda, \lambda h, \lambda h^2$, etc. their least residues relative to the modulus n. And we might order the terms according to the sizes of these residues.

orbit method to make candidates for primitive elements of intermediate fields.

For example, for $n = 19$, 2 is a primitive root and the period (6, 1) consists of the roots $[1], [8], [64], [512], [4096], [32768]$ or

[a] In what follows we can also call the sum the numerical value of the period, or simply the period, when there is no fear of ambiguity.

[1], [7], [8], [11], [12], [18]. Similarly, the period (6, 2) consists of the roots [2], [3], [5], [14], [16], [17]. The period (6, 3) is identical with the preceding. The period (6, 4) contains the roots [4], [6], [9], [10], [13], [15].

Various theorems concerning these periods

▶ 344. We present immediately the following observations concerning periods of this type:

I. Since $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. (mod. n), it is clear that $(f, \lambda), (f, \lambda h), (f, \lambda h^2)$, etc. are composed of the same roots. In general therefore if we designate by $[\lambda']$ any root in (f, λ), this period will be completely identical with (f, λ'). If therefore two periods which have the same number of roots (we will call them *similar*) have one root in common, they will be identical. Therefore it cannot happen that two roots are contained together in a period and only one of them is found in another similar period. Further, if two roots $[\lambda]$, $[\lambda']$ belong to the same period of f terms, the value of the expression λ'/λ (mod. n) is congruent to some power of h; that is, we can presume that $\lambda' \equiv \lambda g^{ve}$ (mod. n).

II. If $f = n - 1$, $e = 1$ the period $(f, 1)$ will coincide with Ω. In the remaining cases Ω will be composed of the periods $(f, 1), (f, g), (f, g^2), \ldots (f, g^{e-1})$. Therefore these periods will be completely different from one another and it is clear that any other similar period (f, λ) will coincide with one of these if $[\lambda]$ belongs to Ω; i.e. if λ is not divisible by n. The period $(f, 0)$ or (f, kn) is manifestly composed of f unities. It is also clear that if λ is any number nondivisible by n, the complex of e periods $(f, \lambda), (f, \lambda g), (f, \lambda g^2) \ldots (f, \lambda g^{e-1})$ will also coincide with Ω. Thus, e.g., for $n = 19$, $f = 6$, Ω will consist of the three periods (6, 1), (6, 2), (6, 4). Any other similar period, except (6, 0) can be reduced to one of these.

III. If $n - 1$ is the product of three positive numbers a, b, c, it is manifest that any period of bc terms is composed of b periods of c terms; for example (bc, λ) is composed of $(c, \lambda), (c, \lambda g^a), (c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$. Thus these latter are said to be contained in the former. So for $n = 19$ the period (6, 1) consists of the three periods (2, 1), (2, 8), (2, 7). The first contains the roots r, r^{18}; the second r^8, r^{11}; the third r^7, r^{12}.

▶ 345. THEOREM. *Let (f, λ), (f, μ) be two similar periods, not necessarily different, and let (f, λ) consist of the roots $[\lambda]$, $[\lambda']$, $[\lambda'']$,*

etc. Then the product of (f, λ) *times* (f, μ) *will be the sum of* f *similar periods, namely*

$$. = (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \text{etc.} = W$$

Demonstration. Let as above $n - 1 = ef$; g a primitive root for the modulus n and $h = g^e$. From what we have said above, we have $(f, \lambda) = (f, \lambda h)$ etc., and the product we want will be

$$= [\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] \cdot (f, \lambda h^2) + \text{etc.}$$

and so

$$\begin{aligned} &= [\lambda + \mu] \quad + [\lambda h + \mu] \ldots \quad + [\lambda h^{f-1} + \mu] \\ &+ [\lambda h + \mu h] \quad + [\lambda h^2 + \mu h] \ldots \quad + [\lambda h^f + \mu h] \\ &+ [\lambda h^2 + \mu h^2] + [\lambda h^3 + \mu h^2] \ldots + [\lambda h^{f+1} + \mu h^2] \text{ etc.} \end{aligned}$$

This expression will contain altogether f^2 roots. And if we add the vertical columns together we will have

$$(f, \lambda + \mu) + (f, \lambda h + \mu) + \ldots + (f, \lambda h^{f-1} + \mu)$$

This expression coincides with W because by hypothesis the numbers $\lambda, \lambda', \lambda''$, etc. are congruent to $\lambda, \lambda h, \lambda h^2, \ldots \lambda h^{f-1}$ relative to the modulus n (we are not concerned with order here) and so also

$$\lambda + \mu, \quad \lambda' + \mu, \quad \lambda'' + \mu, \text{ etc.}$$

will be congruent to

$$\lambda + \mu, \quad \lambda h + \mu, \quad \lambda h^2 + \mu, \ldots \lambda h^{f-1} + \mu \qquad \text{Q.E.D.}$$

We add the following corollaries to this theorem:

I. If k is any integer, the product of $(f, k\lambda)$ times $(f, k\mu)$ will be

$$= (f, k(\lambda + \mu)) + (f, k(\lambda' + \mu)) + (f, k(\lambda'' + \mu)) + \text{etc.}$$

II. Since the single terms of W coincide either with the sum $(f, 0)$ which $= f$, or with one of the sums $(f, 1), (f, g), (f, g^2) \ldots (f, g^{e-1})$, W can be reduced to the following form

$$W = af + b(f, 1) + b'(f, g) + b''(f, g^2) + \ldots + b^{e}(f, g^{e-1})$$

where the coefficients a, b, b', etc. are positive integers (or some may even $= 0$). It is further clear that the product of $(f, k\lambda)$ times

$(f, k\mu)$ will then become

$$= af + b(f, k) + b'(f, kg) + \ldots + b^e(f, kg^{e-1})$$

Thus, e.g., for $n = 19$ the product of the sum (6, 1) times itself or the square of this sum will be $=(6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = 6 + 2(6, 1) + (6, 2) + 2(6, 4)$.

III. Since the product of the individual terms of W times a similar period (f, ν) can be reduced to an analogous form, it is manifest that the product of three periods $(f, \lambda) \cdot (f, \mu) \cdot (f, \nu)$ can be represented by $cf + d(f, 1) \ldots + d^e(f, g^{e-1})$ and the coefficients c, d, etc. will be integers and positive (or $=0$) and for any integral value of k we have

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = cf + d(f, k) + d'(f, kg) + \text{etc.}$$

This theorem can be extended to the product of any number of similar periods, and it does not matter whether these periods are all different or partly or all identical.

IV. It follows from this that if in any rational integral algebraic function $F = \phi(t, u, v, \ldots)$ we substitute for the unknowns t, u, v, etc. respectively the similar periods (f, λ), (f, μ), (f, ν), etc., its value will be reducible to the form

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) \ldots + B^e(f, g^{e-1})$$

and the coefficients A, B, B', etc. will all be integers if all the coefficients in F are integers. But if afterward we substitute $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$, etc. for t, u, v, etc. respectively, the value of F will be reduced to $A + B(f, k) + B'(f, kg) + \text{etc.}$

▶ 346. THEOREM. *If we suppose that λ is a number not divisible by n, and if for brevity we write p for (f, λ), any other similar period (f, μ) which has μ not divisible by n can be reduced to a form*

$$\alpha + \beta p + \gamma p^2 + \ldots + \theta p^{e-1}$$

where the coefficients α, β, etc. are determined rational quantities.

Demonstration. Let us designate by p', p'', p''', etc. the periods $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3)$, etc. on up to $(f, \lambda g^{e-1})$. Their number will be $e - 1$ and one of them will necessarily coincide with (f, μ). We

For subfields of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, the orbit method on ζ_p works to give explicit primitive elements

immediately have the equation

$$0 = 1 + p + p' + p'' + p''' + \text{etc.} \ldots \text{(I)}$$

Now if according to the rules of the preceding article we form the powers of p up to p^{e-1}, we will have $e - 2$ other equations

$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \text{etc.} \ldots \text{(II)}$$

$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc.} \ldots \text{(III)}$$

$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{etc.} \ldots \text{(IV) etc.}$$

All the coefficients A, a, a', etc.; B, b, b', etc.; etc. will be integers and as follows immediately from the preceding article, completely independent of λ; that is, the same equations will hold no matter what value we give to λ. This remark can also be extended to equation I as long as λ is not divisible by n. Let us suppose that $(f, \mu) = p'$; for it is easy to see that if (f, μ) coincides with any of the other periods p'', p''', etc. the following line of argument can be used in a completely analogous way. Since the number of equations I, II, III, etc. is $e - 1$, the quantities p'', p''', etc. whose number is $= e - 2$ can be eliminated from them by known methods. The resulting equation (Z) will be free from them:

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \text{etc.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

This can be done in such a way that all the coefficients $\mathfrak{A}, \mathfrak{B}, \ldots \mathfrak{N}$ are integers and certainly not all $= 0$. Now if we do not have $\mathfrak{N} = 0$, it follows that p' can be determined as the theorem demands. It remains therefore to show that we cannot have $\mathfrak{N} = 0$.

Suppose that $\mathfrak{N} = 0$. The equation Z becomes $\mathfrak{M}p^{e-1} + \text{etc.} + \mathfrak{B}p + \mathfrak{A} = 0$. Since this cannot have degree higher than $e - 1$, it is not satisfied by more than $e - 1$ different values of p. But since the equations from which Z is deduced are independent of λ, it follows that Z does not depend on λ and so it will hold, no matter what integer not divisible by n is taken for λ. Therefore this equation will be satisfied by any of the sums $(f, 1), (f, g), (f, g^2), \ldots (f, g^{e-1})$, and it follows immediately that not all these sums can be unequal but at least two of them must be equal. Let one of these two equal sums contain the roots $[\zeta], [\zeta'], [\zeta'']$, etc. and the other the roots $[\eta], [\eta'], [\eta'']$, etc. We will suppose (this is legitimate) that all the numbers ζ, ζ', ζ'', etc., η, η', η'', etc. are positive and $< n$. Manifestly all

will be different and none of them $=0$. We will designate by Y the function

$$x^{\cdot} + x^{\cdot\cdot} + x^{\cdot\cdot\cdot} + \text{etc.} - x^{\eta} - x^{\eta\cdot} - x^{\eta\cdot\cdot} - \text{etc.}$$

Its highest term cannot exceed x^{n-1} and $Y = 0$ if we set $x = [1]$. Thus Y will have a factor $x - [1]$ in *common* with the function denoted by X in the preceding. It is easy to show that this would be absurd. For if Y and X have a common factor, the greatest common divisor of the functions X, Y (it cannot have degree $n - 1$ because Y is divisible by x) would have all of its coefficients rational. This would follow from the nature of the operation involved in finding the greatest common divisor of two functions whose coefficients are all rational. But in article 341 we showed that X cannot have a factor with rational coefficients of degree less than $n - 1$. Therefore the supposition that $\mathfrak{N} = 0$ cannot be consistent.

Example. For $n = 19$, $f = 6$ we have $p^2 = 6 + 2p + p' + 2p''$. Since $0 = 1 + p + p' + p''$ we deduce that $p' = 4 - p^2$, $p'' = -5 - p + p^2$. Therefore

$$(6,2) = 4 - (6,1)^2, \qquad (6,4) = -5 - (6,1) + (6,1)^2$$

$$(6,4) = 4 - (6,2)^2, \qquad (6,1) = -5 - (6,2) + (6,2)^2$$

$$(6,1) = 4 - (6,4)^2, \qquad (6,2) = -5 - (6,4) + (6,4)^2$$

▶347. THEOREM. *If $F = \phi(t, u, v, \ldots)$ is an invariable[b] rational integral algebraic function in f unknowns t, u, v, etc. and if we substitute for these the f roots contained in the period (f, λ), and by the rules of article 340 the value of F is reduced to the form*

$$A + A'[1] + A''[2] + \text{etc.} = W$$

then the roots in this expression which belong to the same period of f terms will have equal coefficients.

Demonstration. Let $[p]$, $[q]$ be two roots belonging to the same

[b] Invariable functions are those in which all the unknowns are contained in the same way or, more clearly, functions which are not changed no matter how the unknowns are permuted; such are, e.g., the sum of the unknowns, their product, the sum of the products of pairs of them, etc.

period and suppose that p, q are positive and less than n. We must show that $[p]$ and $[q]$ have the same coefficient in W. Let $q \equiv pg^{\nu e}$ (mod. n); and let the roots contained in (f, λ) be $[\lambda], [\lambda'], [\lambda'']$, etc. where we suppose that $\lambda, \lambda', \lambda''$, etc. are positive and less than n; finally, let the least positive residues of the numbers $\lambda g^{\nu e}, \lambda' g^{\nu e}, \lambda'' g^{\nu e}$, etc. relative to the modulus n be μ, μ', μ'', etc. Manifestly they will be identical with the numbers $\lambda, \lambda', \lambda''$, etc., although the order may be transposed. From article 340 it is clear that

$$\phi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots) = (\mathrm{I})$$

is reduced to

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{etc.} \qquad \text{or to}$$

$$A + A'[\theta] + A''[\theta'] + \text{etc.} = (W')$$

Here θ, θ', etc. are the least residues of the numbers $g^{\nu e}, 2g^{\nu e}$, etc. relative to the modulus n and so we see that $[q]$ has the same coefficient in (W') as $[p]$ has in (W). If we expand the expression (I) we will get the same thing we get from expanding the expression $\phi([\mu], [\mu'], [\mu'']$, etc.) because $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$, etc. (mod. n). Now this last expression produces the same result as $\phi([\lambda], [\lambda'], [\lambda'']$, etc.) since the numbers μ, μ', μ'', etc. differ only in order from the numbers $\lambda, \lambda', \lambda''$, etc. and this does not matter in an invariable function. Thus W' is completely identical with W and so the root $[q]$ will have the same coefficient in W as $[p]$. Q.E.D.

We see therefore that W can be reduced to the form

$$A + a(f, 1) + a'(f, g) + a''(f, g^2) \ldots + a^{\varepsilon}(f, g^{\varepsilon - 1})$$

and the coefficients $A, a, \ldots a^{\varepsilon}$ will be determined quantities and integers if all the rational coefficients in F are integers. Thus, e.g., if $n = 19$, $f = 6$, $\lambda = 1$ and the function ϕ designates the sum of products of the unknowns taken two by two, its value is reduced to $3 + (6, 1) + (6, 4)$.

If after this the roots of another period $(f, k\lambda)$ are substituted for t, u, v, etc., the value of F will become

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \text{etc.}$$

▶ 348. In any equation

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \ldots = 0$$

the coefficients α, β, γ, etc. are invariable functions of the roots; that is, α is the sum of all of them, β is the sum of their products taken two at a time, γ the sum of their products taken three at a time, etc. Therefore in the equation whose roots are the ones contained in the period (f, λ), the first coefficient will $=(f, \lambda)$ and each of the others can be reduced to the form

$$A + a(f, 1) + a'(f, g) \ldots + a^{e}(f, g^{e-1})$$

with all the A, a, a', etc. integers. It is further evident that the equation whose roots are the roots contained in any other period $(f, k\lambda)$ can be derived from the one above by substituting (f, k) for $(f, 1)$ in each of the coefficients, (f, kg) for (f, g), and in general (f, kp) for (f, p). In this way therefore we can specify e equations $z = 0$, $z' = 0$, $z'' = 0$, etc. whose roots will be the roots contained in $(f, 1), (f, g), (f, g^2)$, etc. as soon as we know the e sums $(f, 1)$, (f, g), (f, g^2), etc. or rather as soon as we find any *one* of them. This is true because, by article 346, all the rest can be deduced rationally from one of them. This done, the function X will be resolved into e factors of degree f, for manifestly the product of the functions z, z', z'', etc. will $= X$.

Example. For $n = 19$ the sum of all the roots in the period $(6, 1) = (6, 1) = \alpha$; the sum of their products taken two at a time $= 3 + (6, 1) + (6, 4) = \beta$; similarly, the sum of the products taken three at a time $= 2 + 2(6, 1) + (6, 2) = \gamma$; the sum of the products taken four at a time $= 3 + (6, 1) + (6, 4) = \delta$; the sum of products taken five at a time $= (6, 1) = \varepsilon$; the product of all of them $= 1$. Thus the equation

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0$$

will contain all the roots included in $(6, 1)$. And if we substitute $(6, 2), (6, 4), (6, 1)$ for $(6, 1), (6, 2), (6, 4)$ respectively in the coefficients α, β, γ, etc. we will get the equation $z' = 0$ which will contain the roots of $(6, 2)$. And if the same permutation is applied again we will have the equation $z'' = 0$ containing the roots of $(6, 4)$, and the product $zz'z'' = X$.

▶ 349. It is often more convenient, especially when f is a large number, to deduce the coefficients β, γ, etc. from the sums of the powers of the roots by Newton's theorem. Thus the sum of the squares of roots contained in (f, λ) is $= (f, 2\lambda)$, the sum of the

cubes is $=(f, 3\lambda)$, etc. If we write q, q', q'', etc. for (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc. we will have

$$\alpha = q, \qquad 2\beta = \alpha q - q', \qquad 3\gamma = \beta q - \alpha q' + q'', \text{ etc.}$$

Here by article 345 the product of two periods is to be converted immediately into a sum of periods. Thus in our example, if we write p, p', p'' respectively for (6, 1), (6, 2), (6, 4) we will have $q, q', q'', q''', q'''', q''''$ respectively $= p, p', p', p'', p', p''$; thus

$$\alpha = p, \qquad 2\beta = p^2 - pp' = 6 + 2p + 2p''$$

$$3\gamma = (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'$$

$$4\delta = (2 + 2p + p')p - (3 + p + p'')p' + pp' - p''$$

$$= 12 + 4p + 4p'', \text{ etc.}$$

However, it is sufficient to compute half the coefficients in this way, for it is not difficult to prove that the last are equal to the first in inverse order; that is, the last $= 1$, the second last $= \alpha$, the third last $= \beta$, etc.; or, another way, the last can be derived from the first by substituting for $(f, 1)$, (f, g), etc. the periods $(f, -1)$, $(f, -g)$, etc. or $(f, n-1)$, $(f, n-g)$, etc. The former case holds when f is even, the latter when f is odd. The last coefficient, however, will always $= 1$. The basis for this is established by the theorem of article 79, but for the sake of brevity we will not dwell on the argument.

▶ 350. THEOREM. *Let $n - 1$ be the product of the three positive integers α, β, γ and let the period $(\beta\gamma, \lambda)$ which has $\beta\gamma$ terms be composed of β lesser periods of γ terms, (γ, λ), (γ, λ'), (γ, λ''), etc. Let us suppose further that in a function of β unknowns just as in article 347, that is in $F = \phi(t, u, v, \ldots)$, we substitute the sums (γ, λ), (γ, λ'), (γ, λ''), etc. for the unknowns t, u, v, etc. respectively and that according to the rules of the article 345.IV its value is reduced to*

$$A + a(\gamma, 1) + a'(\gamma, g) \ldots + a^{\varepsilon}(\gamma, g^{\alpha\beta - \alpha}) \ldots + a^{\theta}(\gamma, g^{\alpha\beta - 1}) = W$$

then I say that if F is an invariable function, the periods in W which are contained in the same period of $\beta\gamma$ terms (i.e. in general the periods (γ, g^{μ}) and $(\gamma, g^{\alpha\nu + \mu})$ where ν is any integer) will have the same coefficients.

For $\mathbb{Q}(\zeta_p) \supseteq K' \supseteq K \supseteq \mathbb{Q}$, computing min. poly over K for primitive element built above for $K'/\mathbb{Q}$

Demonstration. Since the period $(\beta\gamma, \lambda g^\alpha)$ is identical with $(\beta\gamma, \lambda)$, the lesser periods $(\gamma, \lambda g^\alpha)$, $(\gamma, \lambda' g^\alpha)$, $(\gamma, \lambda'' g^\alpha)$, etc. which comprise the former, necessarily coincide with those that comprise the latter, although in a different order. And if we suppose that F will be transformed into W' by substituting the former quantities for t, u, v, etc., respectively, W' will coincide with W. But by article 347 we have

$$W' = A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \ldots + a^\varepsilon(\gamma, g^{\alpha\beta}) \ldots + a^\theta(\gamma, g^{\alpha\beta+\alpha-1})$$
$$= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \ldots + a^\varepsilon(\gamma, 1) \ldots + a^\theta(\gamma, g^{\alpha-1})$$

so this expression must coincide with W and the first, second, third, etc. coefficients in W (beginning with a) must coincide with the $(\alpha + 1)$st, the $(\alpha + 2)$nd, the $(\alpha + 3)$rd, etc. And we conclude in general that the coefficients of the periods (γ, g^μ), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu})$ $\ldots (\gamma, g^{\nu\alpha+\mu})$, which are the $\mu + 1$st, the $\alpha + \mu + 1$st, the $2\alpha + \mu + 1$st $\ldots \nu\alpha + \mu + 1$st, must coincide with one another. Q.E.D.

Thus it is clear that W can be reduced to the form

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

with all the coefficients A, a, etc. integers when all the coefficients in F are integers. Suppose after this we substitute in F in place of the unknowns, β periods of γ terms which constitute another period of $\beta\gamma$ terms, for example those contained in $(\beta\gamma, \lambda k)$ which are $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, etc. Then the resulting value will be $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \ldots + a^\varepsilon(\beta\gamma, g^{\alpha-1}k)$.

It is obvious that the theorem can also be extended to the case where $\alpha = 1$ or $\beta\gamma = n - 1$. In this case *all* the coefficients in W will be equal, and W will be reduced to the form $A + a(\beta\gamma, 1)$.

▶ 351. Now keeping the terminology of the preceding article, it is clear that the individual coefficients of the equation whose roots are the β sums (γ, λ), (γ, λ'), (γ, λ''), etc. can be reduced to a form like

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \ldots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

and the numbers A, a, etc. will all be integers. And we can derive from this the equation whose roots are the β periods of γ terms contained in another period $(\beta\gamma, k\lambda)$ if in every coefficient we substitute $(\beta\gamma, k\mu)$ for every period $(\beta\gamma, \mu)$. If therefore $\alpha = 1$ all β

periods of γ terms will be determined by an equation of degree β, and each of the coefficients will be of the form $A + a(\beta\gamma, 1)$. As a result, *they will all be known quantities* because $(\beta\gamma, 1) = (n - 1, 1) = -1$. If $\alpha > 1$, the coefficients of the equation whose roots are all the periods of γ terms contained in a given period of $\beta\gamma$ terms will be known quantities as long as all the numerical values of all α periods of $\beta\gamma$ terms are known. The calculation of the coefficients of these equations will often be much easier, especially when β is not very small, if first we calculate the sums of the powers of the roots and deduce from these the coefficients by the theorem of Newton, just as we did above in article 349.

Example 1. For $n = 19$ we want the equation whose roots are the sum (6, 1), (6, 2), (6, 4). If we designate these roots by p, p', p'', etc. respectively and the equation we want by

$$x^3 - Ax^2 + Bx - C = 0$$

we get

$$A = p + p' + p'', \qquad B = pp' + pp'' + p'p'', \qquad C = pp'p''$$

and then

$$A = (18, 1) = -1$$

and

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'', \quad p'p'' = 3p + p' + 2p''$$

so

$$B = 6(p + p' + p'') = 6(18, 1) = -6$$

and finally

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$$

therefore the equation we want is

$$x^3 + x^2 - 6x - 7 = 0$$

Using the other method, we have

$$p + p' + p'' = -1$$

$$p^2 = 6 + 2p + p' + 2p'', \qquad p'p' = 6 + 2p' + p'' + 2p,$$

$$p''p'' = 6 + 2p'' + p + 2p'$$

therefore

$$p^2 + p'p' + p''p'' = 18 + 5(p + p' + p'') = 13$$

and similarly

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2$$

From this and Newton's theorem we derive the same equation as before.

II. For $n = 19$ we want the equation whose roots are the sums (2, 1), (2, 7), (2, 8). If we designate them by q, q', q'' we find

$$q + q' + q'' = (6, 1), \qquad qq' + qq'' + q'q'' = (6, 1) + (6, 4),$$
$$qq'q'' = 2 + (6, 2)$$

and so, keeping the same notation as in the preceding, the equation we want will be

$$x^3 - px^2 + (p + p'')x - 2 - p' = 0$$

The equation whose roots are the sums (2, 2), (2, 3), (2, 5) contained in (6, 2) can be deduced from the preceding by substituting p', p'', p for p, p', p'', respectively, and if we make the same substitution once again we will get the equation whose roots are the sums (2, 4), (2, 6), (2, 9) contained in (6, 4).

The solution of the equation $X = 0$ as evolved from the preceding discussion

▶ 352. The preceding theorems contain along with their corollaries the basic principles of the whole theory, and the method of finding the values of the roots Ω can now be treated in a few words.

First we must take a number g which is a primitive root for the modulus n and find the least residues of the powers of g up to g^{n-2} relative to the modulus n. Resolve $n - 1$ into factors, and indeed into prime factors if we want to reduce the problem to equations of the lowest possible degree. Let these (the order is arbitrary) be $\alpha, \beta, \gamma, \ldots \zeta$ and set

$$\frac{n-1}{\alpha} = \beta\gamma \ldots \zeta = a, \qquad \frac{n-1}{\alpha\beta} = \gamma \ldots \zeta = b, \text{ etc.}$$

Distribute all the roots Ω into α periods of a terms, each of these again into β periods of b terms, and each of these again into γ periods, etc. Determine as in the preceding article the equation (A) of degree α, whose roots are the α sums of a terms; their values can be determined by solving this equation.

But here a difficulty arises because it seems to be uncertain which sum should be made equal to which root of the equation (A); that is, which root should be denoted by $(a, 1)$, which by (a, g), etc. We can solve this difficulty in the following way. We can designate by $(a, 1)$ any root at all of the equation (A); for since any root of this equation is the sum of a roots of Ω, and it is completely arbitrary which root of Ω is denoted by $[1]$, we will be free to assume that $[1]$ expresses one of the roots which constitute a given root of equation (A), and hence this root of equation (A) will be $(a, 1)$. The root $[1]$ will not yet be completely determined; it still remains entirely arbitrary (i.e., indefinite) which of the roots that make up $(a, 1)$ we choose to adopt as $[1]$. As soon as $(a, 1)$ is determined, all the remaining sums of a terms can be deduced from it (art. 346). Thus it is clear that we need solve for only one root of the equation. We can also use the following less direct method for the same purpose. Take for $[1]$ a definite root; i.e. let $[1] = \cos kP/n + i \sin kP/n$ with the integer k taken arbitrarily but in such a way that it is not divisible by n. When this is done $[2], [3]$, etc. will also determine definite roots, and the sums $(a, 1), (a, g)$, etc. will designate definite quantities. Now if these quantities are calculated from a table of sines with just enough precision so that one can decide which are the larger and which the smaller, there will be no doubt left as to how to distinguish the individual roots of the equation (A).

When in this way we have found all α sums of a terms, we will determine by the methods of the preceding article the equation (B) of degree β, whose roots are the β sums of b terms contained in $(a, 1)$. The coefficients of this equation will all be known quantities. Since at this stage it is arbitrary which of the $a = \beta b$ roots contained in $(a, 1)$ is denoted by $[1]$, any given root of equation (B) can be expressed by $(b, 1)$ because it is licit to suppose that one of the b roots of which it is composed is denoted by $[1]$. We just determine therefore any one root of the equation (B) by solving it. Let it $= (b, 1)$ and derive from it by article 346 all the remaining sums of b terms. In this way we have at the same time a method of confirming the calculation, since the total of all sums of b terms forming any one period of a terms is known. In some cases it is just as easy to form $\alpha - 1$ other equations of degree β, whose roots are respectively the individual β sums of b terms contained in the remaining

periods of a terms (a, g), (a, g^2), etc. and to determine *all* roots by the solution of these equations and of the equation B. Then in the same way as above with the help of a table of sines we can decide which are the periods of b terms to which the individual roots found in this way are equal. But to help in this judgment various other devices can be used which cannot be fully explained here. One of them, however, for the case where $\beta = 2$ is especially useful and can be explained more briefly by illustration than by rule. We will use it in the following examples.

After we have found the values of all the $\alpha\beta$ sums of b terms in this way, we can use a similar method to determine by equations of degree γ all the $\alpha\beta\gamma$ sums of c terms. That is, we can *either* get *one* equation of degree γ according to article 350, whose roots are the γ sums of c terms contained in $(b, 1)$, and by solving this find a root and let it $=(c, 1)$ and finally from this by the methods of article 346 deduce all the remaining sums; *or* in a similar way find the $\alpha\beta$ equations of degree γ whose roots are respectively the γ sums of c terms contained in the individual periods of b terms. We can solve all these equations for all their roots and determine the order of the roots with the help of the table of sines as we did above. However, for $\gamma = 2$ we can use the device we will demonstrate below.

If we continue in this way we will finally have all the $(n - 1)/\zeta$ sums of ζ terms; and if we find by the methods of article 348 the equation of degree ζ whose roots are the ζ roots of Ω contained in $(\zeta, 1)$, all its coefficients will be known quantities. And if we solve for any one of its roots, we can let it $=[1]$, and its powers will give us all the other roots Ω. If we prefer, we could solve for *all* the roots of this equation. Then by the solution of the other $[(n - 1)/\zeta] - 1$ equations of degree ζ, which contain respectively all the ζ roots in each of the remaining periods of ζ terms, we can find all the remaining roots Ω.

It is clear, however, that as soon as the first equation (A) is solved, or as soon as we have the values of all the α sums of a terms, we will also have the resolution of the function X into α factors of degree a, by article 348. Further, after solving equation (B) or after finding the values of all the $\alpha\beta$ sums of b terms, each of those factors will be resolved again into β factors, and so X will be resolved into $\alpha\beta$ factors of b dimensions etc.

Example for n = 19 where the operation is reduced to the solution of two cubic and one quadratic equation

▶ 353. *First example for* $n = 19$. Since here we have $n - 1 = 3 \cdot 3 \cdot 2$ finding the roots Ω is reduced to the solution of two cubic and one quadratic equation. This example is more easily understood because for the most part the necessary operations have already been discussed above. If we take the number 2 as the primitive root g, the least residues of its powers will produce the following (the exponents of the powers are written in the first line and the residues in the second):

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

From this, by articles 344, 345, we can easily find the following distribution of all the roots Ω into three periods of six terms and of each of these into three periods of two terms:

$$\Omega = (18, 1)\begin{cases}(6, 1)\begin{cases}(2, 1) \ldots [1], [18]\\(2, 8) \ldots [8], [11]\\(2, 7) \ldots [7], [12]\end{cases}\\(6, 2)\begin{cases}(2, 2) \ldots [2], [17]\\(2, 16) \ldots [3], [16]\\(2, 14) \ldots [5], [14]\end{cases}\\(6, 4)\begin{cases}(2, 4) \ldots [4], [15]\\(2, 13) \ldots [6], [13]\\(2, 9) \ldots [9], [10]\end{cases}\end{cases}$$

The equation (A) whose roots are the sums $(6, 1), (6, 2), (6, 4)$ is found to be $x^3 + x^2 - 6x - 7 = 0$ and one of the roots is -1.2218761623. If we call this root $(6, 1)$ we have

$$(6, 2) = \quad 4 - (6, 1)^2 \qquad = 2.5070186441$$
$$(6, 4) = -5 - (6, 1) + (6, 1)^2 = -2.2851424818$$

Thus X is resolved into three factors of degree 6, if these values are substituted in article 348.

Equation for $Q(\sqrt[3]{q})^+/K$

The equation (B) whose roots are the sums $(2,1),(2,7),(2,8)$ comes out to be

$$x^3 - (6,1)x^2 + [(6,1) + (6,4)]x - 2 - (6,2) = 0$$

or

$$x^3 + 1.2218761623x^2 - 3.5070186441x - 4.5070186441 = 0$$

One root is -1.3545631433 which we will call $(2,1)$. By the method of article 346 we find the following equations (for brevity we will write q for $(2,1)$).

$$(2,2) = q^2 - 2, \quad (2,3) = q^3 - 3q, \quad (2,4) = q^4 - 4q^2 + 2,$$

$$(2,5) = q^5 - 5q^3 + 5q, \qquad (2,6) = q^6 - 6q^4 + 9q^2 - 2,$$

$$(2,7) = q^7 - 7q^5 + 14q^3 - 7q$$

$$(2,8) = q^8 - 8q^6 + 20q^4 - 16q^2 + 2$$

$$(2,9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q$$

In the present case these equations can be found more easily as follows than by the methods of article 346. If we suppose that

$$[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$$

we have

$$[18] = \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} = \cos\frac{kP}{19} - i\sin\frac{kP}{19}$$

and so

$$(2,1) = 2\cos\frac{kP}{19}$$

and in general

$$[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19} \quad \text{and} \quad \text{so}$$

$$(2,\lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$$

Therefore if $q/2 = \cos\omega$, we will have $(2,2) = 2\cos 2\omega$, $(2,3) = 2\cos 3\omega$ etc., and the same formulae as above will be derived from known equations for the cosines of multiple angles. Now from

these formulae we derive the following numerical values:

$(2, 2) = -0.1651586909$	$(2, 6) = 0.4909709743$
$(2, 3) = 1.5782810188$	$(2, 7) = -1.7589475024$
$(2, 4) = -1.9727226068$	$(2, 8) = 1.8916344834$
$(2, 5) = 1.0938963162$	$(2, 9) = -0.8033908493$

The values of (2, 7), (2, 8) can also be found from equation (*B*) of which they are the two remaining roots. And the doubt as to *which* of these roots is (2, 7) and which (2, 8) can be removed either by an approximate calculation according to the formulae given above or by means of sine tables. A cursory reference shows us that $(2, 1) = 2\cos\omega$ by letting $\omega = 7P/19$ and so we have

$$(2, 7) = 2\cos\tfrac{49}{19}P = 2\cos\tfrac{8}{19}P, \quad \text{and}$$
$$(2, 8) = 2\cos\tfrac{56}{19}P = 2\cos\tfrac{1}{19}P.$$

Similarly we can find the sums (2, 2), (2, 3), (2, 5) also by the equation

$$x^3 - (6, 2)x^2 + [(6, 1) + (6, 2)]x - 2 - (6, 4) = 0$$

whose roots they are, and the uncertainty as to which roots correspond to which sums can be removed in exactly the same way as before. Finally the sums (2, 4), (2, 6), (2, 9) can be found by the equation

$$x^3 - (6, 4)x^2 + [(6, 2) + (6, 4)]x - 2 - (6, 1) = 0$$

[1] and [18] are the roots of the equation $x^2 - (2, 1)x + 1 = 0$. One of them

$$= \tfrac{1}{2}(2, 1) + i\sqrt{[1 - \tfrac{1}{4}(2, 1)^2]} = \tfrac{1}{2}(2, 1) + i\sqrt{[\tfrac{1}{2} - \tfrac{1}{4}(2, 2)]}$$

and the other

$$= \tfrac{1}{2}(2, 1) - i\sqrt{[\tfrac{1}{2} - \tfrac{1}{4}(2, 2)]}$$

and the numerical values will be

$$= -0.6772815716 \pm 0.7357239107\, i$$

The sixteen remaining roots can be found either from the powers of one or the other of these roots or by solving the eight other similar equations. To decide which root has the positive sign for its imaginary part and which the negative in the second method,

we can use sine tables or the device that will be explained in the following example. In this way we will find the following values with the upper sign corresponding to the first root and the lower sign to the second root:

$$\begin{aligned}
[1] \text{ and } [18] &= -0.6772815716 \pm 0.7357239107\,i \\
[2] \text{ and } [17] &= -0.0825793455 \mp 0.9965844930\,i \\
[3] \text{ and } [16] &= 0.7891405094 \pm 0.6142127127\,i \\
[4] \text{ and } [15] &= -0.9863613034 \pm 0.1645945903\,i \\
[5] \text{ and } [14] &= 0.5469481581 \mp 0.8371664783\,i \\
[6] \text{ and } [13] &= 0.2454854871 \pm 0.9694002659\,i \\
[7] \text{ and } [12] &= -0.8794737512 \mp 0.4759473930\,i \\
[8] \text{ and } [11] &= 0.9458172417 \mp 0.3246994692\,i \\
[9] \text{ and } [10] &= -0.4016954247 \pm 0.9157733267\,i
\end{aligned}$$

Example for n = 17 where the operation is reduced to the solution of four quadratic equations

▶ 354. *Second example for* $n = 17$. Here $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ so the calculation will be reduced to four quadratic equations. For the primitive root we will take the number 3. The least residues of its powers relative to the modulus 17 are the following:

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

From this we derive the following distributions of the complex Ω into two periods of eight terms, four of four terms, eight of two terms:

$$\Omega = (16,1)\begin{cases}(8,1)\begin{cases}(4,1)\begin{cases}(2,1)\ldots[1],[16]\\(2,13)\ldots[4],[13]\end{cases}\\(4,9)\begin{cases}(2,9)\ldots[8],[9]\\(2,15)\ldots[2],[15]\end{cases}\end{cases}\\(8,3)\begin{cases}(4,3)\begin{cases}(2,3)\ldots[3],[14]\\(2,5)\ldots[5],[12]\end{cases}\\(4,10)\begin{cases}(2,10)\ldots[7],[10]\\(2,11)\ldots[6],[11]\end{cases}\end{cases}\end{cases}$$

The equation (A) whose roots are the sums $(8, 1), (8, 3)$ is found by the rules of article 351 to be $x^2 + x - 4 = 0$. Its roots are

$$-(1/2) + (\sqrt{17})/2 = 1.5615528128$$

and

$$-(1/2) - (\sqrt{17})/2 = -2.5615528128$$

We will set the former $= (8, 1)$ so the latter necessarily $= (8, 3)$.

The equation (B) whose roots are the sums $(4, 1)$ and $(4, 9)$ is $x^2 - (8, 1)x - 1 = 0$. Its roots are

$$\tfrac{1}{2}(8, 1) \pm \tfrac{1}{2}\sqrt{[4 + (8, 1)^2]} = \tfrac{1}{2}(8, 1) \pm \tfrac{1}{2}\sqrt{[12 + 3(8, 1) + 4(8, 3)]}$$

We will set $(4, 1)$ equal to the quantity which has the positive radical sign and whose numerical value is 2.0494811777. Thus the quantity with the negative radical sign whose numerical value is -0.4879283649 will be expressed by $(4, 9)$. The remaining sums of four terms $(4, 3)$ and $(4, 10)$, can be calculated in two ways. *First*, by the method of article 346 which gives the following formulae when we abbreviate $(4, 1)$ by the letter p:

$$(4, 3) = -\tfrac{3}{2} + 3p - \tfrac{1}{2}p^3 = 0.3441507314$$

$$(4, 10) = \tfrac{3}{2} + 2p - p^2 - \tfrac{1}{2}p^3 = -2.9057035442$$

The same method gives the formula $(4, 9) = -1 - 6p + p^2 + p^3$ and from it we get the same value as above.

The *second* method allows us to determine the sums $(4, 3)$, $(4, 10)$ by solving the equation of which they are the roots. The equation is $x^2 - (8, 3)x - 1 = 0$. Its roots are

$$\tfrac{1}{2}(8, 3) \pm \tfrac{1}{2}\sqrt{[4 + (8, 3)^2]} \quad \text{or} \quad \tfrac{1}{2}(8, 3) + \tfrac{1}{2}\sqrt{[12 + 4(8, 1) + 3(8, 3)]}$$

$$\text{and} \quad \tfrac{1}{2}(8, 3) - \tfrac{1}{2}\sqrt{[12 + 4(8, 1) + 3(8, 3)]}$$

And we can remove the doubt as to *which* root should be expressed by $(4, 3)$ and which by $(4, 10)$ by the following device which we mentioned in article 352. Calculate the product of $(4, 1) - (4, 9)$ times $(4, 3) - (4, 10)$. It $= 2(8, 1) - 2(8, 3)$.[c] Manifestly the value of this expression is positive $= +2\sqrt{17}$ and, since the first factor of

[c] The real basis of this device is the fact that we can foresee in advance that the product does not contain sums of four terms but only sums of eight terms. The trained mathematician can easily grasp the reason for this. For the sake of brevity we shall omit it.

pp 433-4 computes explicit quadratic equations for a tower of subfields of $\mathbb{Q}(\zeta_{17})^+/\mathbb{Q}$ via group theory $\mathrm{Gal}(\mathbb{Z}/17\mathbb{Z})^\times$ (and R-stuff to find correct sign of $\sqrt{\ }$'s in "quadratic formula")

the product, $(4, 1) - (4, 9) = +\sqrt{[12 + 3(8, 1) + 4(8, 3)]}$, is positive, the other factor, $(4, 3) - (4, 10)$, must also be positive. Therefore $(4, 3)$ is equal to the first root which has the positive sign in front of the radical, and $(4, 10)$ is equal to the second root. From these will result the same numerical values as above.

Having found all the sums of four terms, we proceed to the sums of two terms. Equation (C) whose roots are $(2, 1), (2, 13)$ and contained in $(4, 1)$ will be $x^2 - (4, 1)x + (4, 3) = 0$. Its roots are

$$\tfrac{1}{2}(4, 1) \pm \tfrac{1}{2}\sqrt{[-4(4, 3) + (4, 1)^2]}$$

or

$$\tfrac{1}{2}(4, 1) \pm \tfrac{1}{2}\sqrt{[4 + (4, 9) - 2(4, 3)]}$$

When we take the positive radical quantity, we get the value 1.8649444588, which we set $=(2, 1)$ and so $(2, 13)$ will be equal to the other whose value is $=0.1845367189$. If the remaining sums of two terms are to be found by the method of article 346, we can use the same formulae for $(2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8)$ as we did in the preceding example for similar quantities, that is to say, $(2, 2)$ [or $(2, 15)$] $= (2, 1)^2 - 2$ etc. But if it seems preferable to find them in pairs by solving a quadratic equation, for $(2, 9), (2, 15)$ we get the equation $x^2 - (4, 9)x + (4, 10) = 0$ whose roots are

$$\tfrac{1}{2}(4, 9) \pm \tfrac{1}{2}\sqrt{[4 + (4, 1) - 2(4, 10)]}$$

We can determine which sign to use in the same way as above. Calculating the product of $(2, 1) - (2, 13)$ times $(2, 9) - (2, 15)$ we get $-(4, 1) + (4, 9) - (4, 3) + (4, 10)$. Since this is negative and the factor $(2, 1) - (2, 13)$ is positive, $(2, 9) - (2, 15)$ must be negative and we should use the upper positive sign for $(2, 15)$ and the lower negative sign for $(2, 9)$. From this we find that $(2, 9) = -1.9659461994$, $(2, 15) = 1.4780178344$. Then, since in calculating the product of $(2, 1) - (2, 13)$ times $(2, 3) - (2, 5)$ we get the positive quantity $(4, 9) - (4, 10)$, the factor $(2, 3) - (2, 5)$ must be positive. And by a calculation like the one above we find

$$(2, 3) = \tfrac{1}{2}(4, 3) + \tfrac{1}{2}\sqrt{(4 + (4, 10) - 2(4, 9))} = \quad 0.8914767116$$

$$(2, 5) = \tfrac{1}{2}(4, 3) - \tfrac{1}{2}\sqrt{(4 + (4, 10) - 2(4, 9))} = -0.5473259801$$

Finally by completely analogous operations we have

$$(2, 10) = \tfrac{1}{2}(4, 10) - \tfrac{1}{2}\sqrt{(4 + (4, 3) - 2(4, 1))} = -1.7004342715$$

$$(2, 11) = \tfrac{1}{2}(4, 10) + \tfrac{1}{2}\sqrt{(4 + (4, 3) - 2(4, 1))} = -1.2052692728$$

It remains now to get down to the roots Ω themselves. Equation (D) whose roots are [1] and [16] gives us $x^2 - (2, 1)x + 1 = 0$. The roots of this are

$$\tfrac{1}{2}(2, 1) \pm \tfrac{1}{2}\sqrt{[(2, 1)^2 - 4]} \quad \text{or rather} \quad \tfrac{1}{2}(2, 1) \pm \tfrac{1}{2}i\sqrt{[4 - (2, 1)^2]}$$

or

$$\tfrac{1}{2}(2, 1) \pm \tfrac{1}{2}i\sqrt{[2 - (2, 15)]}$$

We will take the upper sign for [1], the lower for [16]. We can get the fourteen remaining roots either from the powers of [1] or by solving seven quadratic equations, each of which will give us two roots, and the uncertainty about the signs of the radical quantities can be removed by the same device we used above. Thus [4] and [13] are the roots of the equation $x^2 - (2, 13)x + 1 = 0$ and so equal to

$$\tfrac{1}{2}(2, 13) \pm \tfrac{1}{2}i\sqrt{[2 - (2, 9)]}$$

By calculating the product of [1] − [16] times [4] − [13] however we get (2, 5) − (2, 3), a real negative quantity. Therefore, since [1] − [16] is $+i\sqrt{(2 - (2, 15))}$, i.e. the product of the imaginary i times a real *positive* quantity, [4] − [13] must also be the product of i times a real *positive* quantity because $i^2 = -1$. As a result we will take the upper sign for [4] and the lower sign for [13]. Similarly for the roots [8] and [9] we find

$$\tfrac{1}{2}(2, 9) \pm \tfrac{1}{2}i\sqrt{[2 - (2, 1)]}$$

so, since the product of [1] − [16] times [8] − [9] is (2, 9) − (2, 10) and negative, we must take the upper sign for [8], the lower sign for [9]. If we then compute the remaining roots we will obtain the following numerical values, where the upper sign is to be taken for the first root, the lower sign for the second:

$$[1], [16] \ldots \quad 0.9324722294 \pm 0.3612416662\, i$$

$$[2], [15] \ldots \quad 0.7390089172 \pm 0.6736956436\, i$$

$$[3], [14] \ldots \quad 0.4457383558 \pm 0.8951632914\, i$$

[4], [13]... $0.0922683595 \pm 0.9957341763\, i$

[5], [12]... $-0.2736629901 \pm 0.9618256432\, i$

[6], [11]... $-0.6026346364 \pm 0.7980172273\, i$

[7], [10]... $-0.8502171357 \pm 0.5264321629\, i$

[8], [9]... $-0.9829730997 \pm 0.1837495178\, i$

What precedes can suffice for solving the equation $x^n - 1 = 0$ and so also for finding the trigonometric functions corresponding to the arcs that are commensurable with the circumference. But this subject is so important that we cannot conclude without indicating some of the observations that throw light on the subject, as well as examples that are related to it or depend on it. Among such we will especially select those that can be solved without a lot of apparatus that depends on other investigations and we will consider them only as *examples* of this vast theory which must be consider in great detail at a later time.

Further discussions concerning periods of roots

▶ 355. Since n is always presumed to be odd, 2 will appear among the factors of $n - 1$, and the complex Ω will be composed of $(n - 1)/2$ periods of two terms. Such a period $(2, \lambda)$ will consist of the roots $[\lambda]$ and $[\lambda g^{(n-1)/2}]$ where as above g represents any primitive root for the modulus n. But $g^{(n-1)/2} \equiv -1 \pmod{n}$ and so $\lambda g^{(n-1)/2} \equiv -\lambda$ (see art. 62) and $[\lambda g^{(n-1)/2}] = [-\lambda]$. Therefore if we suppose that $[\lambda] = \cos kP/n + i \sin kP/n$, and $[-\lambda] = \cos kP/n - i \sin kP/n$, we will have the sum $(2, \lambda) = 2 \cos kP/n$. At this point we only draw the conclusion that the value of any sum of two terms is a real quantity. Since any period which has an even number of terms $= 2a$ can be decomposed into a periods of two terms, it is clear in general that the value of any sum which has an even number of terms is always a real quantity. Therefore if in article 352 among the factors α, β, γ, etc. we save two until the end, all the operations will be done on real quantities until we come to a sum of two terms, and the imaginaries will be introduced when we pass from these sums to the roots themselves.

Sums having an even number of terms are real quantities

The equation defining the distribution of the roots (Ω) into two periods

▶ 356. We should give special attention to the auxiliary equations by which we determine for any value of n the sums that form the complex Ω. They are connected in a surprising way with the most recondite properties of the number n. Here we will restrict

ourselves to the two following cases. *First*, the quadratic equation whose roots are sums of $(n-1)/2$ terms, *second*, in the case where $n-1$ has the factor 3, we will consider the cubic equation whose roots are sums of $(n-1)/3$ terms.

If for brevity we write m for $(n-1)/2$ and designate by g some primitive root for the modulus n, the complex Ω will consist of two periods $(m, 1)$ and (m, g). The former will contain the roots $[1], [g^2], [g^4], \ldots [g^{n-3}]$, the latter the roots $[g], [g^3], [g^5], \ldots [g^{n-2}]$. Let us suppose that the least positive residues of the numbers $g^2, g^4, \ldots g^{n-3}$ relative to the modulus n are, disregarding order, R, R', R'', etc. and that the residues of $g, g^3, g^5, \ldots g^{n-2}$ are N, N', N'', etc. Then the roots of which $(m, 1)$ consists, coincide with $[1], [R], [R'], [R'']$, etc. and the roots of the period (m, g) with $[N], [N'], [N'']$, etc. It is clear that all the numbers $1, R, R', R''$, etc. are *quadratic residues* of the number n. Since they are all different and less than n, and since their number is $=(n-1)/2$ and so equal to the number of all positive residues of n that are less than n, these residues will coincide completely with those numbers. All the numbers N, N', N'', etc. are different from each other and from the numbers $1, R, R'$, etc. and together with these exhaust all the numbers $1, 2, 3, \ldots n-1$. It follows that the numbers N, N', N'', etc. must coincide with all the positive *quadratic non-residues* of n that are less than n. Now if we suppose that the equation whose roots are the sums $(m, 1), (m, g)$ is

$$x^2 - Ax + B = 0$$

we have

$$A = (m, 1) + (m, g) = -1, \qquad B = (m, 1) \cdot (m, g)$$

The product of $(m, 1)$ times (m, g) by article 345

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{etc.} = W$$

and so will be reduced to a form $\alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$. To determine the coefficients α, β, γ we observe *first* that $\alpha + \beta + \gamma = m$ (because the number of sums in $W = m$); *second*, that $\beta = \gamma$ (this follows from article 350 since the product $(m, 1) \cdot (m, g)$ is an invariable function of the sums $(m, 1), (m, g)$ of which the larger sum $(n-1, 1)$ is composed); *third*, since all the numbers $N+1$, $N'+1$, $N''+1$, etc. are strictly contained within the bounds 2 and

$n + 1$, it is clear that *either* no sum in W can be reduced to $(m, 0)$ and so $\alpha = 0$ when the number $n - 1$ does not occur among the numbers N, N', N'', etc. *or* that one sum, say (m, n) can be reduced to $(m, 0)$ and so $\alpha = 1$ when $n - 1$ does occur among the numbers N, N', N'', etc. In the former case therefore we will have $\alpha = 0$, $\beta = \gamma = m/2$, in the latter $\alpha = 1$, $\beta = \gamma = (m - 1)/2$. And it follows that since the numbers β and γ must be integers, the former case will hold, that is, $n - 1$ (or, what is the same thing, -1) will not be found among the nonresidues of n when m is even or n is of the form $4k + 1$. The latter case will hold, that is, $n - 1$ or -1 will be a nonresidue of n whenever m is odd or n of the form $4k + 3$.[4] Now since $(m, 0) = m$, $(m, 1) + (m, g) = -1$ the product we see will be $= -m/2$ in the former case and $= (m + 1)/2$ in the latter. Thus the equation in the former case will be $x^2 + x - (n - 1)/4 = 0$ with roots $-(1/2) \pm (\sqrt{n})/2$, in the latter $x^2 + x + [(n + 1)/4]$ with roots $-(1/2) \pm i(\sqrt{n})/2$.

Let $\mathfrak{R}$ stand for all the positive quadratic residues of n that are less than n and $\mathfrak{N}$ for all the nonresidues. Then no matter which root of Ω is chosen for $[1]$, the difference between the sums $\Sigma[\mathfrak{R}]$ and $\Sigma[\mathfrak{N}]$ will be $= \pm\sqrt{n}$ for $n \equiv 1$ and $= \pm i\sqrt{n}$ for $n \equiv 3 \pmod 4$. And it follows that if k is any integer not divisible by n we will have

$$\sum \cos \frac{k\mathfrak{R}P}{n} - \sum \frac{k\mathfrak{R}P}{n} = \pm\sqrt{n}$$

and

$$\sum \sin \frac{k\mathfrak{R}P}{n} - \sum \sin \frac{k\mathfrak{R}P}{n} = 0$$

for $n \equiv 1 \pmod 4$. On the other hand for $n \equiv 3 \pmod 4$ the first difference will $= 0$ and the second $= \pm\sqrt{n}$. These theorems are so elegant that they deserve special note. We observe that the upper signs always hold when for k we take unity or a quadratic residue of n and the lower when k is a nonresidue. These theorems retain

[4] In this way we have given a new demonstration of the theorem which says that -1 is a residue of all prime numbers of the form $4k + 1$ and a nonresidue of all those of the form $4k + 3$. Above (art. 108, 109, 262) we proved it in several different ways. If it is preferable to presuppose this theorem, there will be no need for the distinction between the two cases because β and γ will already be integers.

the same or even greater elegance when they are extended to composite values of n. But these matters are on a higher level of investigation, and we will reserve their consideration for another occasion.

Demonstration of a theorem mentioned in Section IV

▶ 357. Let the equation of degree m whose roots are the m roots contained in the period $(m, 1)$ be the following:

$$x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$$

or $z = 0$. Here $a = (m, 1)$ and each of the remaining coefficients b etc. will be of the form $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ with $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ integers (art. 348). If we denote by z' the function into which z is transformed when for $(m, 1)$ we everywhere substitute (m, g) and for (m, g) we substitute (m, g^2) or what is the same thing $(m, 1)$, then the roots of the equation $z' = 0$ will be the roots contained in (m, g) and the product

$$zz' = \frac{x^n - 1}{x - 1} = X$$

Therefore z can be reduced to a form $R + S(m, 1) + T(m, g)$ where R, S, T will be integral functions of x with all their coefficients integers. Having done this we will have

$$z' = R + S(m, g) + T(m, 1)$$

And if for brevity we write p and q for $(m, 1)$ and (m, g) respectively

$$2z = 2R + (S + T)(p + q) - (T - S)(p - q)$$
$$= 2R - S - T - (T - S)(p - q)$$

and similarly

$$2z' = 2R - S - T + (T - S)(p - q)$$

so if we set

$$2R - S - T = Y, \qquad T - S = Z$$

we will have $4X = Y^2 - (p - q)^2 Z^2$ and since $(p - q)^2 = \pm n$

$$4X = Y^2 \mp nZ^2$$

The upper sign will hold when n is of the form $4k + 1$, the lower when it is of the form $4k + 3$. This is the theorem we promised (art. 124) to prove. It is easy to see that the two terms of highest degree in the function Y will always be $2x^m + x^{m-1}$ and the

highest in the function Z, x^{m-1}. The remaining coefficients, all of which will be integers, will vary according to the nature of the number n and cannot be given a general analytic formula.

Example. For $n = 17$, by the rules of article 348 the equation whose roots are the eight roots contained in (8, 1) will be

$$x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 - (4p + 3q)x^3 + (4 + p + 2q)x^2 - px + 1 = 0$$

therefore

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1$$

$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x$$

$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2$$

and

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2$$

$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + x$$

Here are some other examples:

n	Y	Z
3	$2x + 1$	1
5	$2x^2 + x + 2$	x
7	$2x^3 + x^2 - x - 2$	$x^2 + x$
11	$2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$	$x^4 + x$
13	$2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4x^2 - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5x^2 - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + x^2 + x$

The equation for distributing the roots (Ω) into three periods

▶ 358. We proceed now to a consideration of the cubic equations which for the case where n is of the form $3k + 1$ determine the three sums of $(n - 1)/3$ terms which compose the complex Ω. Let g be any primitive root for the modulus n and $(n - 1)/3 = m$ which will be an even integer. Then the three sums that compose

Ω will be $(m, 1), (m, g), (m, g^2)$ for which we will write p, p', p'' respectively. It is clear that the first contains the roots $[1], [g^3], [g^6], \ldots [g^{n-4}]$, the second the roots $[g], [g^4], \ldots [g^{n-3}]$, and the third the roots $[g^2], [g^5], \ldots [g^{n-2}]$. Let us suppose that the equation we want is

$$x^3 - Ax^2 + Bx - C = 0$$

We will have

$$A = p + p' + p'', \qquad B = pp' + p'p'' + pp'', \qquad C = pp'p''$$

and $A = -1$. Let the least positive residues of the numbers $g^3, g^6, \ldots g^{n-4}$ relative to the modulus n and disregarding order, be $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, etc., and $\mathfrak{R}$ the complex of them and the number 1. Similarly let $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$, etc. be the least residues of the numbers $g, g^4, g^7, \ldots g^{n-3}$ and $\mathfrak{R}'$ their complex; finally let $\mathfrak{A}'', \mathfrak{B}'', \mathfrak{C}''$, etc. be the least residues of $g^2, g^5, g^8, \ldots g^{n-2}$ and $\mathfrak{R}''$ their complex. Thus all the numbers in $\mathfrak{R}, \mathfrak{R}', \mathfrak{R}''$ will be different and will coincide with $1, 2, 3, \ldots n-1$. First of all we must observe here that the number $n-1$ must be in $\mathfrak{R}$, since it is easy to see that it is a residue of $g^{3m/2}$. It also follows from this that the two numbers $h, n-h$ will always be found in the *same* one of the three complexes $\mathfrak{R}, \mathfrak{R}', \mathfrak{R}''$, for if one of them is a residue of the power g^λ, the other will be a residue of the power $g^{\lambda+(3m/2)}$ or of $g^{\lambda-(3m/2)}$ if $\lambda > 3m/2$. We will denote by $(\mathfrak{R}\mathfrak{R})$ the numbers of numbers in the series $1, 2, 3, \ldots n-1$ which belong to $\mathfrak{R}$ by themselves and when increased by unity; $(\mathfrak{R}\mathfrak{R}')$ will be the number of numbers in the same series, which are contained in $\mathfrak{R}$ themselves but are in $\mathfrak{R}'$ when increased by unity. It will be immediately obvious what is the meaning of the notation $(\mathfrak{R}\mathfrak{R}''), (\mathfrak{R}'\mathfrak{R}), (\mathfrak{R}'\mathfrak{R}'), (\mathfrak{R}'\mathfrak{R}''), (\mathfrak{R}''\mathfrak{R}), (\mathfrak{R}''\mathfrak{R}'), (\mathfrak{R}''\mathfrak{R}'')$. Having done this, I say *first* that $(\mathfrak{R}\mathfrak{R}') = (\mathfrak{R}'\mathfrak{R})$. For if we suppose that h, h', h'', etc. are all the numbers of the series $1, 2, 3, \ldots n-1$ which are themselves in $\mathfrak{R}$ but with $h+1, h'+1, h''+1$, etc. in $\mathfrak{R}'$ so that by definition the number of them is $(\mathfrak{R}\mathfrak{R}')$, then it is clear that all the numbers $n-h-1$, $n-h'-1, n-h''-1$, etc. are contained in $\mathfrak{R}'$ and the next larger numbers $n-h, n-h'$, etc. in $\mathfrak{R}$; and since there are $(\mathfrak{R}'\mathfrak{R})$ such numbers in all, we certainly cannot have $(\mathfrak{R}'\mathfrak{R}) < (\mathfrak{R}\mathfrak{R}')$. We show similarly that it is not possible to have $(\mathfrak{R}\mathfrak{R}') < (\mathfrak{R}'\mathfrak{R})$ so these numbers are necessarily equal. In exactly the same way we

can show that $(\mathfrak{RR}'') = (\mathfrak{R}''\mathfrak{R})$, $(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}')$. *Second*, since any number in $\mathfrak{R}$ with the exception of the largest one $n-1$ must be followed by the next larger one in $\mathfrak{R}$ or in $\mathfrak{R}'$ or in $\mathfrak{R}''$, the sum $(\mathfrak{RR}) + (\mathfrak{RR}') + (\mathfrak{RR}'')$ must be equal to the number of all numbers in $\mathfrak{R}$ diminished by unity, that is $= m - 1$. For a similar reason

$$(\mathfrak{R}'\mathfrak{R}) + (\mathfrak{R}'\mathfrak{R}') + (\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}) + (\mathfrak{R}''\mathfrak{R}') + (\mathfrak{R}''\mathfrak{R}'') = m$$

With these preliminaries, by the rules of article 345 we evolve the product pp' into $(m, \mathfrak{A}' + 1) + (m, \mathfrak{B}' + 1) + (m, \mathfrak{C}' + 1) +$ etc. This expression is easily reduced to $(\mathfrak{R}'\mathfrak{R})p + (\mathfrak{R}'\mathfrak{R}')p' + (\mathfrak{R}'\mathfrak{R}'')p''$. By article 345.I we can get from this the product $p'p''$ by substituting for $(m, 1), (m, g), (m, g^2)$ respectively the quantities (m, g), $(m, g^2), (m, g^3)$, i.e. p', p'', p respectively for p, p', p''. Thus we have $p'p'' = (\mathfrak{R}'\mathfrak{R})p' + (\mathfrak{R}'\mathfrak{R}')p'' + (\mathfrak{R}'\mathfrak{R}'')p$. Similarly $p''p = (\mathfrak{R}'\mathfrak{R})p'' + (\mathfrak{R}'\mathfrak{R}')p + (\mathfrak{R}'\mathfrak{R}'')p'$. From this we get immediately

$$B = m(p + p' + p'') = -m$$

In a manner similar to that by which pp' was developed, we can also reduce pp'' to $(\mathfrak{R}''\mathfrak{R})p + (\mathfrak{R}''\mathfrak{R}')p' + (\mathfrak{R}''\mathfrak{R}'')p''$. And since this expression must be identical with the preceding, we will necessarily have $(\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}'\mathfrak{R}')$ and $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R})$. Now if we let

$$(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a, \qquad (\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R}) = (\mathfrak{RR}') = b$$

$$(\mathfrak{R}'\mathfrak{R}') = (\mathfrak{R}''\mathfrak{R}) = (\mathfrak{RR}'') = c$$

we will have $m - 1 = (\mathfrak{RR}) + (\mathfrak{RR}') + (\mathfrak{RR}'') = (\mathfrak{RR}) + b + c$. And since $a + b + c = m$, $(\mathfrak{RR}) = a - 1$. Thus the nine unknown quantities are reduced to three a, b, c or rather, since $a + b + c = m$, to two. Finally it is clear that the square p^2 becomes $(m, 1 + 1) + (m, \mathfrak{A} + 1) + (m, \mathfrak{B} + 1) + (m, \mathfrak{C} + 1) +$ etc. Among the terms of this expression we have (m, n) which reduces to $(m, 0)$ or to m and the remaining terms reduce to $(\mathfrak{RR})p + (\mathfrak{RR}')p' + (\mathfrak{RR}'')p''$ so we have $p^2 = m + (a - 1)p + bp' + cp''$.

As a result of all this we have the following reductions:

$$\begin{aligned} p^2 &= m + (a-1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'' \end{aligned}$$

along with the conditional equation

$$a + b + c = m \qquad \text{(I}$$

and we know besides that these numbers are integers. As a resul we have

$$C = p \cdot p'p'' = ap^2 + bpp' + cpp''$$
$$= am + (a^2 + b^2 + c^2 - a)p + (ab + bc + ac)p'$$
$$+ (ab + bc + ac)p''$$

But since $pp'p''$ is an invariable function of p, p', p'', the coefficient by which they are multiplied in the preceding expression are neces sarily equal (art. 350) and we have the new equation

$$a^2 + b^2 + c^2 - a = ab + bc + ac \qquad \text{(II)}$$

and from this we get $C = am + (ab + bc + ac)(p + p' + p'')$ or (on account of (I) and the fact that $p + p' + p'' = -1$)

$$C = a^2 - bc \qquad \text{(III)}$$

Now even though C depends on three unknowns and there are only two equations, nevertheless with the help of the condition that a, b, c be integers, they will suffice to completely determine C. To show this we express equation (II) as

$$12a + 12b + 12c + 4 = 36a^2 + 36b^2 + 36c^2 - 36ab - 36ac$$
$$- 36bc - 24a + 12b + 12c + 4$$

By (I), the left-hand side becomes $= 12m + 4 = 4n$. The right-hand side reduces to

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2$$

or if we write k for $2a - b - c$, to $(3k - 2)^2 + 27(b - c)^2$. Thus the number $4n$ (i.e. the quadruple of any prime of the form $3m + 1$) can be represented by the form $x^2 + 27y^2$. This can, of course, be deduced without any difficulty from the general theory of binary forms, but it is remarkable that such a decomposition is related to the values of a, b, c. Now the number $4n$ can always be decomposed in only one way into the sum of a square and 27

times another square. We show this as follows.[e] If we suppose that

$$4n = t^2 + 27u^2 = t't' + 27u'u'$$

we have *first*

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16n^2$$

second

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16n^2$$

third

$$(tu' + t'u)(tu' - t'u) = 4n(u'u' - u^2)$$

From the third equation it follows that n, since it is a prime number, divides one of the numbers $tu' + t'u, tu' - t'u$. From the first and the second, however, it is clear that each of these numbers is less than n, so the one which n divides is necessarily $=0$. Therefore $u'u - u^2 = 0$ and $u'u' = u^2$ and $t't' = t^2$; i.e. the two decompositions are the same. Now suppose that the decomposition of $4n$ into a square and 27 times a square is known (this can be done by the direct method of Section V or the indirect method of art. 323, 324). We will then have $4n = M^2 + 27N^2$ and the squares $(3k - 2)^2, (b - c)^2$ will be determined, and we will have two equations in place of equation (II). But clearly not only the square $(3k - 2)^2$ but its root $3k - 2$ will be determined. Because it must either $= +M$ or $= -M$ the ambiguity is removed easily. For since k must be an integer, we will have $3k - 2 = +M$ or $= -M$ according as M is of the form $3z + 1$ or $3z + 2$.[f] Now since $k = 2a - b - c = 3a - m$ we will have $a = (m + k)/3$, $b + c = m - a = (2m - k)/3$ and so

$$C = a^2 - bc = a^2 - \tfrac{1}{4}(b + c)^2 + \tfrac{1}{4}(b - c)^2$$
$$= \tfrac{1}{9}(m + k)^2 - \tfrac{1}{36}(2m - k)^2 + \tfrac{1}{4}N^2 = \tfrac{1}{12}k^2 + \tfrac{1}{3}km + \tfrac{1}{4}N^2$$

and thus we have found all the coefficients of the equation.

[e] This proposition can be proved much more directly from the principles of Section V.

[f] Manifestly M cannot be of the form $3z$ because otherwise $4n$ would be divisible by 3. With regard to the ambiguity as to whether $b - c$ must $= N$ or $= -N$ it is unnecessary to consider the question here, and by the nature of the case it cannot be determined because it depends on the selection of the primitive root g. For some primitive roots the difference $b - c$ will be positive, for others negative.

Q.E.F. This formula will be much simpler if we substitute for N^2 its value from the equation $(3k-2)^2 + 27N^2 = 4n = 12m + 4$. After calculation we get

$$C = \tfrac{1}{9}(m + k + 3km) = \tfrac{1}{9}(m + kn)$$

The same value can be reduced to $(3k-2)N^2 + k^3 - 2k^2 + k - km + m$. And although this expression is less useful, it shows immediately that C comes out to be an integer, as it should.

Example. For $n = 19$ we have $4n = 49 + 27$, so $3k - 2 = +7$, $k = 3$, $C = (6 + 57)/9 = 7$ and the equation we want is $x^3 + x^2 - 6x - 7 = 0$ as we saw above (art. 351). Similarly, for $n = 7, 13, 31, 37, 43, 61, 67$ the value of k is respectively $1, -1, 2, -3, -2, 1, -1$ and $C = 1, -1, 8, -11, -8, 9, -5$.

Although the problem we have solved in this article is rather intricate, we did not wish to omit it because of the elegance of the solution and because it gave occasion for using various devices that are fruitful also in other discussions.[8]

Reduction to pure equations of the equations by which the roots (Ω) are found

▶ 359. The preceding discussion had to do with the *discovery* of auxiliary equations. Now we will explain a very remarkable property concerning their *solution*. Everyone knows that the most eminent geometers have been unsuccessful in the search for a general solution of equations higher than the fourth degree, or (to define the search more accurately) for the REDUCTION OF MIXED EQUATIONS TO PURE EQUATIONS. And there is little doubt that this problem is not merely beyond the powers of contemporary analysis but proposes the impossible (cf. what we said on this subject in *Demonstratio nova*, art. 9[1]). Nevertheless it is certain that there are innumerable mixed equations of every degree which admit a reduction to pure equations, and we trust that geometers will find it gratifying if we show that our equations are always of this kind. But because of the length of this discussion we will

[8] *Corollary.* Let ε be the root of the equation $x^3 - 1 = 0$ and we will have $(p + \varepsilon p' + \varepsilon^2 p'')^3 = n(M + N\sqrt{-27})/2$. Let $M/\sqrt{4n} = \cos\phi$, $N\sqrt{27}/\sqrt{4n} = \sin\phi$ and as a result

$$p = -\tfrac{1}{3} + \tfrac{2}{3}\cos\tfrac{1}{3}\phi\sqrt{n}; \qquad M \equiv +1 \pmod 3; \qquad 1 \equiv M(1\cdot 2\cdot 3\ldots m)^3 \pmod n$$

Setzt man $3x + 1 = y$, *so wird die Gleichung* $y^3 - 3ny - Mn = 0$ (If we let $3x + 1 = y$, we then have $y^3 - 3ny - Mn = 0$).

[1] This is Gauss' doctoral dissertation. Its full title is *Demonstratio nova theorematis Omnem Functionem Algebraicam Rationalem Integram unis variabilis in Factores Reales primi vel secundi gradus resolvi posse*, Helmstedt, 1799.

present here only the most important principles necessary to show the reduction is possible; we reserve for another time a more complete consideration, which the topic deserves. We will first present some general observations about the roots of the equation $x^e - 1 = 0$ which also embrace the case where e is a composite number.

I. These roots are given (as is known from elementary textbooks) by $\cos kP/e + i \sin kP/e$ where for k we take the e numbers $0, 1, 2, 3, \ldots e-1$ or any others that are congruent to these relative to the modulus e. One root, for $k = 0$ or for any k divisible by e will $= 1$. For any other value of k there will be a root that is different from 1.

II. Since $(\cos kP/e + i \sin kP/e)^\lambda = \cos \lambda kP/e + i \sin \lambda kP/e$, it is clear that if R is such a root corresponding to a value of k which is relatively prime to e, then in the series R, R^2, R^3, etc. the eth term $= 1$, and all the antecedent values are different from 1. It follows immediately that all e of the quantities $1, R, R^2, R^3, \ldots R^{e-1}$ are unequal and, since they all satisfy the equation $x^e - 1 = 0$, they will give all the roots of this equation.

III. Under the same assumption the sum

$$1 + R^\lambda + R^{2\lambda} \ldots + R^{\lambda(e-1)} = 0$$

for any value of the integer λ not divisible by e. For it is $= (1 - R^{\lambda e})/(1 - R^\lambda)$ and the numerator of this fraction $= 0$, but the denominator is not $= 0$. When λ is divisible by e, the sum obviously $= e$.

▶ 360. Let n, as always, be a prime number, g a primitive root for the modulus n, and $n - 1$ the product of three positive integers α, β, γ. For brevity we will include in this the cases where α or $\gamma = 1$. When $\gamma = 1$, we just replace the sums $(\gamma, 1)$, (γ, g), etc. by the roots $[1]$, $[g]$, etc. Suppose therefore that all the α sums of $\beta\gamma$ terms $(\beta\gamma, 1), (\beta\gamma, g), (\beta\gamma, g^2), \ldots (\beta\gamma, g^{\alpha-1})$ are known and that we want to find the sums of γ terms. We have reduced the operation above to a mixed equation of degree β. Now we will show how to solve it by a pure equation of the same degree. For brevity for the sums

$$(\gamma, 1), (\gamma, g^\alpha), (\gamma, g^{2\alpha}), \ldots (\gamma, g^{\alpha\beta-\alpha})$$

To give "radical" expression for K'/K inside $\Omega(\zeta_\beta)/\Omega$ with $[K' : K] = \beta$, shows that $K'(\zeta_\beta) = K(\zeta_\beta)(t)$ where $t^\beta = T \in K(\zeta_\beta)$

which are contained in $(\beta\gamma, 1)$, we will write $a, b, c, \ldots m$ respectively. And for the sums

$$(\gamma, g), (\gamma, g^{\alpha+1}), \ldots (\gamma, g^{\alpha\beta-\alpha+1})$$

contained in $(\beta\gamma, g)$ we will write $a', b', \ldots m'$. And for

$$(\gamma, g^2), (\gamma, g^{\alpha+2}), \ldots (\gamma, g^{\alpha\beta-\alpha+2})$$

we will write $a'', b'', \ldots m''$, etc. until we come to those that are contained in $(\beta\gamma, g^{\alpha-1})$.

I. Let R be an arbitrary root of the equation $x^\beta - 1 = 0$ and let us suppose that the power of β degree of the function

$$t = a + Rb + R^2c + \ldots + R^{\beta-1}m$$

is, according to the rules of article 345,

$$\begin{aligned} N &+ Aa + Bb + Cc \ldots + Mm \\ &+ A'a' + B'b' + C'c' \ldots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ &+ \text{etc.} \qquad\qquad = T \end{aligned}$$

where all the coefficients N, A, B, A', etc. are rational integral functions of R. Let us also suppose that the β power of two other functions

$$u = R^\beta a + Rb + R^2c \ldots + R^{\beta-1}m$$

$$u' = b + Rc + R^2d \ldots + R^{\beta-2}m + R^{\beta-1}a$$

become respectively U and U'. It is easy to see from article 350 that since u' results from replacing the sums $a, b, c, \ldots m$ with $b, c, d, \ldots a$, we have

$$\begin{aligned} U' = N &+ Ab + Bc + Cd \ldots + Ma \\ &+ A'b' + B'c' + C'd' \ldots + M'a' \\ &+ A''b'' + B''c'' + C''d'' \ldots + M''a'' \\ &+ \text{etc.} \end{aligned}$$

It is also clear that, since $u = Ru'$, we will have $U = R^\beta U'$. And since $R^\beta = 1$ the corresponding coefficients in U and U' will be equal. Finally, since t and u differ only in so far as a is

multiplied by unity in t and by R^β in u, all the corresponding coefficients (i.e. those that multiply the same sums) in T and U will be equal, and so also the corresponding coefficients in T and U'. Therefore $A = B = C$ etc. $= M$; $A' = B' = C'$ etc.; $A'' = B''$ $= C''$ etc.; etc. so T is reduced to a form like

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \text{etc.}$$

where the individual coefficients N, A, A', etc. are of the form

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{etc.}$$

in such a way that p, p', p'', etc. are given integers.

II. If we take for R a determined root of the equation $x^\beta - 1 = 0$ (we suppose that we already have its solution) and in such a way that no power less than the β power is equal to unity, T will also be a determined quantity, and from it we can derive t by the pure equation $t^\beta - T = 0$. But since this equation has β roots which are $t, Rt, R^2t, \ldots R^{\beta-1}t$, there can be a doubt as to which root should be chosen. This is arbitrary, however, because we must remember that after all the sums of $\beta\gamma$ terms are determined, the root [1] is defined only in that one of the $\beta\gamma$ roots contained in $(\beta\gamma, 1)$ must be denoted by this symbol. So it is entirely arbitrary which of the β sums making up $(\beta\gamma, 1)$ is designated by a. And if after one of these sums is expressed by a we suppose that $t = \mathfrak{T}$, it is easy to see that the sum we now designate by b can be changed to a, and what was formerly $c, d, \ldots a, b$ now becomes $b, c, \ldots m, a$, and the value of t is now $= \mathfrak{T}/R = \mathfrak{T}R^{\beta-1}$. Similarly, if we now decide to let a equal the sum which in the beginning was c, the value of t becomes $\mathfrak{T}R^{\beta-2}$ and so on. Thus t can be considered equal to any of the quantities $\mathfrak{T}, \mathfrak{T}R^{\beta-1}, \mathfrak{T}R^{\beta-2}$, etc., i.e. to any root of the equation $x^\beta - T = 0$ according as we let one or another of the sums in $(\beta\gamma, 1)$ be expressed by $(\gamma, 1)$. Q.E.D.

III. After the quantity t has been determined in this way, we must determine the $\beta - 1$ others which result from t by substituting for R successively $R^2, R^3, R^4, \ldots R^\beta$, that is, by finding

$$t' = a + R^2b + R^4c \ldots + R^{2\beta-2}m$$

$$t'' = a + R^3b + R^6c \ldots + R^{3\beta-3}m, \quad \text{etc.}$$

We have the last of these already because it manifestly $= a +$

$b + c \ldots + m = (\beta\gamma, 1)$. The others can be found in the following way. We use the methods of article 345 to find the product $t^{\beta-2}t'$ just as we found t^{β} in I. Then we use a method just like the preceding to show that from this we get a form

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, g^2) \text{ etc.} = T'$$

Here $\mathfrak{N}, \mathfrak{A}, \mathfrak{A}'$, etc. are rational integral functions of R and so T' is a known quantity and $t' = T't^2/T$. In exactly the same way we find some T'' by calculating the product $t^{\beta-3}t''$. This expression will have a similar form and because its value is known we can derive the equation $t'' = T''t^3/T$. Then t''' can be found from the equation $t''' = T'''t^4/T$ where again T''' is a known quantity, etc.

This method would not be applicable if we had $t = 0$ for then $T = T' = T''$ etc. $= 0$. But it can be shown that this is impossible, although the demonstration is so long that we must omit it here. There are also some special artifices for converting the fractions T'/T, T''/T, etc. into rational *integral* functions of R and some shorter methods in the case where $\alpha = 1$ for finding the values of t', t'', etc. but we cannot consider them here.

IV. Finally, as soon as we have found t, t', t'', etc. by observation III of the preceding article we have immediately that $t + t' + t''$ + etc. $= \beta a$. This gives us the value of a and from this, by article 346, we can derive the values of all the remaining sums of γ terms. The values of b, c, d, etc. can also be found from the following equations, as a little investigation will show:

$$\beta b = R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{etc.}$$

$$\beta c = R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{etc.}$$

$$\beta d = R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \text{etc.}, \quad \text{etc.}$$

Among the great number of observations that we could make concerning the preceding discussion we will emphasize only one. With regard to the solution of the pure equation $x^{\beta} - T = 0$, it is clear that in many cases T has the imaginary value $P + iQ$ so the solution depends partly on the division of an angle (whose tangent $= Q/P$), partly on the division of a ratio [unity to $\sqrt{(P^2 + Q^2)}$] into β parts. And it is remarkable (we will not pursue this subject here) that the value of $\sqrt[\beta]{(P^2 + Q^2)}$ can always be expressed *rationally* by already known quantities. Thus, except for the

extraction of a square root, the *only* thing required for a solution is the division of the angle, e.g. for $\beta = 3$ only the trisection of an angle.

Finally, since nothing prevents us from setting $\alpha = 1$, $\gamma = 1$ and so $\beta = n - 1$, it is evident that the solution of the equation $x^n - 1 = 0$ can immediately be reduced to the solution of a pure equation $x^{n-1} - T = 0$ of degree $n - 1$. Here T is determined by the roots of the equation $x^{n-1} - 1 = 0$. As a result the division of the whole circle into n parts requires, *first*, the division of the whole circle into $n - 1$ parts; *second*, the division into $n - 1$ parts of another arc which can be constructed as soon as the first division is accomplished; *third*, the extraction of one square root, and it can be shown that this is always $\sqrt{n}$.

Method of finding the angles corresponding to the individual roots of (Ω)

▶ 361. It remains to examine more closely the connection between the roots Ω and the trigonometric functions of the angles $P/n, 2P/n, 3P/n \ldots (n-1)P/n$. The method we used for finding the roots of Ω (unless we consult sine tables, but this would be less direct) leaves uncertain *which* roots correspond to the *individual* angles; i.e. which root $= \cos P/n + i \sin P/n$, which $= \cos 2P/n + i \sin 2P/n$, etc. But this uncertainty can be easily removed by reflecting that the cosines of the angles $P/n, 2P/n, 3P/n, \ldots (n-1)P/2n$ are continually decreasing (provided we pay attention to signs) and that the sines are positive. On the other hand the angles $(n-1)P/n, (n-2)P/n, (n-3)P/n, \ldots (n+1)P/n$ have the same cosines as the above, but the sines are negative although they have the same absolute value. Therefore of the roots Ω the two that have the largest real parts (they are equal to each other) correspond to the angles P/n, $(n-1)P/n$. The former has the coefficient of i positive, the latter negative. Of the remaining $n - 3$ roots, those that have the largest real part correspond to the angles $2P/n$, $(n-2)P/n$, and so forth. As soon as the root to which the angle P/n corresponds is known, those that correspond to the remaining angles can be determined from this one because, if we suppose that it $= [\lambda]$, the roots $[2\lambda]$, $[3\lambda]$, $[4\lambda]$, etc. will correspond to the angles $2P/n$, $3P/n$, $4P/n$, etc. Thus in the example in article 353 we see that the root corresponding to the angle $P/19$ must be [11], and [8] to the angle $18P/19$. Similarly the roots [3], [16], [14], [5], etc. will correspond to the angles $2P/19$, $17P/19$, $3P/19$, $16P/19$, etc. In the example of article

Application of the preceding to trigonometric functions

354 the root [1] will correspond to the angle $P/17$, [2] to the angle $2P/17$, etc. In this way the cosines and sines of the angles P/n, $2P/n$, etc. will be completely determined.

▶ 362. With regard to the remaining trigonometric functions of these angles, they could of course all be derived from the corresponding sines and cosines by ordinary well-known methods. Thus secants and tangents can be found by dividing unity and the sine, respectively, by the cosine; cosecants, and cotangents by dividing unity and the cosine by the sine. But it will often be much more useful to obtain the same quantities with the help of the following formulae by addition alone and no divisions. Let ω be any one of the angles P/n, $2P/n, \ldots (n-1)P/n$ and let $\cos\omega + i\sin\omega = R$ so that R will be one of the roots Ω, then

Derivation of tangents, cotangents, secants, and cosecants from sines and cosines without division

$$\cos\omega = \frac{1}{2}\left(R + \frac{1}{R}\right) = \frac{1+R^2}{2R},$$

$$\sin\omega = \frac{1}{2i}\left(R - \frac{1}{R}\right) = \frac{i(1-R^2)}{2R}$$

And from this

$$\sec\omega = \frac{2R}{1+R^2} \qquad \tan\omega = \frac{i(1-R^2)}{1+R^2},$$

$$\operatorname{cosec} = \frac{2Ri}{R^2-1}, \qquad \operatorname{cotan}\omega = \frac{i(R^2+1)}{R^2-1}$$

Now we will show how to transform the numerators of these four fractions so that they will be divisible by the denominators.

I. Since $R = R^{n+1} = R^{2n+1}$ we have $2R = R + R^{2n+1}$. This expression is divisible by $1 + R^2$ since n is an odd number. So we have

$$\sec\omega = R - R^3 + R^5 - R^7 \ldots + R^{2n-1}$$

and so (since $\sin\omega = -\sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega$ etc. we have $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega$$

or finally (since $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$, etc.)

$$= 2(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega) \pm \cos n\omega$$

the upper or lower sign to be taken according as n is of the form $4k + 1$ or $4k + 3$. Obviously this formula can also be expressed as

$$\sec\omega = \pm[1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega]$$

II. Similarly by substituting $1 - R^{2n+2}$ for $1 - R^2$ we have

$$\tan\omega = i(1 - R^2 + R^4 - R^6 \ldots - R^{2n})$$

or (since $1 - R^{2n} = 0$, $R^2 - R^{2n-2} = 2i\sin 2\omega$, $R^4 - R^{2n-4} = 2i\sin 4\omega$, etc.)

$$\tan\omega = 2[\sin 2\omega - \sin 4\omega + \sin 6\omega \ldots \mp \sin(n-1)\omega]$$

III. Since $1 + R^2 + R^4 \ldots + R^{2n-2} = 0$, we have

$$n = n - 1 - R^2 - R^4 \ldots R^{2n-2}$$
$$= (1 - 1) + (1 - R^2) + (1 - R^4) \ldots + (1 - R^{2n-2})$$

and each of its terms is divisible by $1 - R^2$. So

$$\frac{n}{1 - R^2} = 1 + (1 + R^2) + (1 + R^2 + R^4) \ldots + (1 + R^2 + R^4 \ldots + R^{2n-4})$$
$$= (n-1) + (n-2)R^2 + (n-3)R^4 \ldots + R^{2n-4}$$

Multiplying by 2, and subtracting the quantity

$$0 = (n-1)(1 + R^2 + R^4 \ldots + R^{2n-2})$$

and again multiplying by R we have

$$\frac{2nR}{1 - R^2} = (n-1)R + (n-3)R^3 + (n-5)R^5 \ldots - (n-3)R^{2n-3} - (n-1)R^{2n-1}$$

and from this we get immediately

$$\operatorname{cosec}\omega = \frac{1}{n}[(n-1)\sin\omega + (n-3)\sin 3\omega \ldots - (n-1)\sin(2n-1)\omega]$$
$$= \frac{2}{n}[(n-1)\sin\omega + (n-3)\sin 3\omega + \text{etc.} + 2\sin(n-2)\omega]$$

This formula can also be expressed as

$$\operatorname{cosec}\omega = -\frac{2}{n}[2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega]$$

IV. If we multiply the value of $n/(1 - R^2)$ given above by $1 + R^2$ and subtract the quantity

$$0 = (n - 1)(1 + R^2 + R^4 \ldots + R^{2n-2})$$

we have

$$\frac{n(1 + R^2)}{1 - R^2} = (n - 2)R^2 + (n - 4)R^4 + (n - 6)R^6 \ldots - (n - 2)R^{2n-2}$$

and from this it immediately follows that

$$\operatorname{cotan}\omega = \frac{1}{n}[(n - 2)\sin 2\omega + (n - 4)\sin 4\omega + (n - 6)\sin 6\omega \ldots - (n - 2)\sin(n - 2)\omega]$$

$$= \frac{2}{n}[(n - 2)\sin 2\omega + (n - 4)\sin 4\omega \ldots + 3\sin(n - 3)\omega + \sin(n - 1)\omega]$$

and this formula can also be expressed as

$$\operatorname{cotan}\omega = -\frac{2}{n}[\sin\omega + 3\sin 3\omega \ldots + (n - 2)\sin(n - 2)\omega]$$

Method of successively reducing the equations for trigonometric functions

▶ 363. When $n - 1 = ef$, the function X can be resolved into e factors of degree f as soon as we know the values of all the e sums of f terms (art. 348). In the same way, if we suppose that $Z = 0$ is an equation of degree $n - 1$ whose roots are the sines or any other trigonometric functions of the angles $P/n, 2P/n \ldots (n - 1)P/n$, the function Z can be resolved into e factors of degree f in the following way.

Let Ω consist of the e periods of f terms, $(f, 1) = P, P', P''$, etc.; the period P of the roots $[1], [a], [b], [c]$, etc.; P' of the roots $[a'], [b'], [c']$, etc.; P'' of the roots $[a''], [b''], [c'']$, etc., etc. Let the angle ω correspond to the root $[1]$, and thus the angles $a\omega, b\omega$, etc. to the roots $[a], [b]$, etc., the angles $a'\omega, b'\omega$, etc. to the roots $[a'], [b']$, etc., the angles $a''\omega, b''\omega$, etc. to the roots $[a''], [b'']$, etc. It is easy to see that all these angles taken together coincide with respect to the trigonometric functions[h] with the angles $P/n, 2P/n, 3P/n, \ldots (n - 1)P/n$. Now if we denote the function we are considering by the character ϕ prefixed to the angle, and if we

[h] Two angles coincide in this respect if their difference is equal to the circumference or to a multiple of it. We can say that they are *congruent relative to the circumference* if we want to use the term congruence in an extended sense.

let Y be the product of the e factors

$$x - \phi\omega, \qquad x - \phi a\omega, \qquad x - \phi b\omega, \text{ etc.}$$

and the product of the factors $x - \phi a'\omega, x - \phi b'\omega$, etc. $= Y'$, the product of $x - \phi a''\omega, x - \phi b''\omega$, etc. $= Y''$ etc.: then necessarily the product $YY'Y'' \ldots = Z$. It remains now to show that all the coefficients in the functions Y, Y', Y'', etc. can be reduced to the form

$$A + B(f, 1) + C(f, g) + D(f, g^2) \ldots + L(f, g^{e-1})$$

When we have done this, manifestly all of them will be known as soon as we know the values of all the sums of f terms. We show this in the following way.

Just as $\cos\omega = ([1]/2) + ([1]^{n-1}/2)$, $\sin\omega = -(i[1]/2) + (i[1]^{n-1}/2)$ so by the preceding article all the remaining trigonometric functions of the angle ω can be reduced to the form $\mathfrak{A} + \mathfrak{B}[1] + \mathfrak{C}[1]^2 + \mathfrak{D}[1]^3 +$ etc., and it is not difficult to see that the function of the angle $k\omega$ then becomes $= \mathfrak{A} + \mathfrak{B}[k] + \mathfrak{C}[k]^2 + \mathfrak{D}[k]^3 +$ etc. where k is any integer. Now since the individual coefficients in Y are invariable rational integral functions of $\phi\omega, \phi a\omega, \phi b\omega$, etc., if we substitute their values for these quantities, the individual coefficients will become invariable rational integral functions of $[1], [a], [b]$, etc. Therefore by article 347 they are reduced to the form $A + B(f, 1) + C(f, g) +$ etc. The coefficients in Y', Y'', etc. can also be reduced to similar forms. Q.E.D.

▶ 364. We add a few observations concerning the problem of the preceding article.

I. The individual coefficients in Y' are functions of roots contained in the period P' [we can let it $= (f, a')$] just like the functions of the roots in P giving the corresponding coefficients in Y. It is clear from article 347 therefore that we can derive Y' from Y by substituting everywhere in Y the quantities (f, a'), $(f, a'g)$, $(f, a'g^2)$, etc. for $(f, 1), (f, g), (f, g^2)$, etc. respectively. And Y'' can be derived from Y by substituting everywhere in Y (f, a''), $(f, a''g)$, $(f, a''g^2)$, etc. for $(f, 1), (f, g), (f, g^2)$, etc. respectively etc. Therefore as soon as we have the function Y, the remaining Y', Y'', etc. follow easily.

II. Let us suppose that

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{etc.}$$

Then the coefficients α, β, etc. are respectively the sum of the roots of the equation $Y = 0$, i.e. of the quantities $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc., the sum of their products taken two by two, etc. But often these coefficients will be found much more easily by a method similar to that of article 349, that is by calculating the sum of the roots $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc., the sum of their squares, cubes, etc. and deducing from this by Newton's theorem the coefficients we want. Whenever ϕ designates the tangent, secant, cotangent, or cosecant we have still other methods of abbreviating the process, but we cannot consider them here.

III. The case where f is an even number merits special consideration for then each of the periods P, P', P'', etc. will be composed of $f/2$ periods of two terms. Let P consist of the periods $(2, 1)$, $(2, a)$, $(2, b)$, $(2, c)$, etc. The numbers $1, a, b, c$, etc. and $n - 1$, $n - a$, $n - b$, $n - c$, etc. taken together will coincide with the numbers $1, a, b, c$, etc. or at least (this comes to the same thing) will be congruent to them relative to the modulus n. But $\phi(n - 1)\omega = \pm\phi\omega$, $\phi(n - a)\omega = \pm\phi a\omega$ etc. the upper signs to be taken when ϕ designates the cosine or secant, the lower when ϕ designates the sine, tangent, cotangent, or cosecant. It follows from this that in the first two cases the factors of which Y is composed will be equal two by two, and thus Y is a square and will $= y^2$ if we suppose that y is equal to the product of

$$x - \phi\omega, \qquad x - \phi a\omega, \qquad x - \phi b\omega, \text{ etc.}$$

In the same cases the remaining function Y', Y'', etc. will be squares, and if we suppose that P' is composed of $(2, a')$, $(2, b')$, $(2, c')$, etc.; P'' of $(2, a'')$, $(2, b'')$, $(2, c'')$, etc., etc., the product of $x - \phi a'\omega$, $x - \phi b'\omega$, $x - \phi c'\omega$, etc. $= y'$, the product of $x - \phi a''\omega$, $x - \phi b''\omega$, etc. $= y''$, etc., then $Y' = y'y'$, $Y'' = y''y''$, etc.; and the function Z will also be a square (cf. above, art. 337) and its root will be equal to the product of y, y', y'', etc. But clearly y', y'', etc. can be derived from y just as we said that Y, Y'' are derived from Y (cf. I). Further, the individual coefficients in y can also be reduced to the form

$$A + B(f, 1) + C(f, g) + \text{etc.}$$

because the sums of the individual powers of the roots of the

If $\mathbb{Q}(\zeta_p) \supset K \supset \mathbb{Q}$ (even) then $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_p)^+/K^+)$, so subfields of $\mathbb{Q}(\zeta_p)^+/K^+$ correspond to those of $\mathbb{Q}(\zeta_p)/K$ via $F^+ \rightsquigarrow K \cdot F^+$

equation $y = 0$ are equal to one half the sums for the equation $Y = 0$ and thus are reducible to such a form. In the four latter cases however Y will be the product of the factors

$$x^2 - (\phi\omega)^2, \qquad x^2 - (\phi a\omega)^2, \qquad x^2 - (\phi b\omega)^2, \text{ etc.}$$

and thus of the form

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{etc.}$$

It is clear that the coefficients λ, μ, etc. can be deduced from the sums of squares, biquadrates, etc. of the roots, $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc. And the same thing is true for the functions Y', Y'', etc.

Example I. Let $n = 17$, $f = 8$ and let ϕ designate the cosine. Then we will have

$$Z = (x^8 + \tfrac{1}{2}x^7 - \tfrac{7}{4}x^6 - \tfrac{3}{4}x^5 + \tfrac{15}{16}x^4 + \tfrac{5}{16}x^3 - \tfrac{5}{32}x^2 - \tfrac{1}{32}x + \tfrac{1}{256})^2$$

and thus $\sqrt{Z}$ will be resolved into two factors y, y' of degree four. The period $P = (8, 1)$ consists of $(2, 1), (2, 9), (2, 13), (2, 15)$ so y will be a product of the factors

$$x - \phi\omega, \qquad x - \phi 9\omega, \qquad x - \phi 13\omega, \qquad x - \phi 15\omega$$

Substituting $([k]/2) + ([n - k]/2)$ for $\phi k\omega$ we find that

$$\phi\omega + \phi 9\omega + \phi 13\omega + \phi 15\omega = (8, 1)/2$$

$$(\phi\omega)^2 + (\phi 9\omega)^2 + (\phi 13\omega)^2 + (\phi 15\omega)^2 = 2 + [(8, 1)/4]$$

Likewise the sum of the cubes is $= [3(8, 1)/8] + [(8, 3)/8]$ and the sum of the biquadrates is $= [3/2] + [5(8, 1)/16]$. So by Newton's theorem the coefficients in y will be

$$y = x^4 - \tfrac{1}{2}(8, 1)x^3 + \tfrac{1}{4}[(8, 1) + 2(8, 3)]x^2 - \tfrac{1}{8}[(8, 1) + 3(8, 3)]x + \tfrac{1}{16}[(8, 1) + (8, 3)]$$

and y' is derived from y by interchanging $(8, 1)$ and $(8, 3)$. Therefore if we substitute for $(8, 1), (8, 3)$ the values $-(1/2) + (\sqrt{17})/2$, $-(1/2) - (\sqrt{17})/2$ we get

$$y = x^4 + (\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} + \tfrac{1}{8}\sqrt{17})x^2 + (\tfrac{1}{4} + \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$

$$y' = x^4 + (\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} - \tfrac{1}{8}\sqrt{17})x^2 + (\tfrac{1}{4} - \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$

Similarly $\sqrt{Z}$ can be resolved into four factors of degree two. The first will be $(x - \phi\omega)(x - \phi 13\omega)$, the second $(x - \phi 9\omega)(x - \phi 15\omega)$, the third $(x - \phi 3\omega)(x - \phi 5\omega)$, the fourth $(x - \phi 10\omega)(x - \phi 11\omega)$, and all the coefficients in these factors can be expressed by the four sums (4, 1), (4, 9), (4, 3), (4, 10). Manifestly the product of the first factor times the second will be y, the product of the third times the fourth y'.

Example II. If with everything else the same, we suppose that ϕ stands for the sine so that

$$Z = x^{16} - \tfrac{17}{4}x^{14} + \tfrac{119}{16}x^{12} - \tfrac{221}{32}x^{10} + \tfrac{935}{256}x^{8} - \tfrac{561}{512}x^{6} + \tfrac{357}{2048}x^{4} - \tfrac{51}{4096}x^{2} + \tfrac{17}{65536}$$

is to be resolved into two factors of degree 8 which we designate y, y', then y will be a product of four double factors

$$x^2 - (\phi\omega)^2, \qquad x^2 - (\phi 9\omega)^2, \qquad x^2 - (\phi 13\omega)^2, \qquad x^2 - (\phi 15\omega)^2$$

Now since

$$\phi k\omega = -\tfrac{1}{2}i[k] + \tfrac{1}{2}i[n - k]$$

we have

$$(\phi k\omega)^2 = -\tfrac{1}{4}[2k] + \tfrac{1}{2}[n] - \tfrac{1}{4}[2n - 2k] = \tfrac{1}{2} - \tfrac{1}{4}[2k] - \tfrac{1}{4}[2n - 2k]$$

Thus the sum of the squares of the roots $\phi\omega, \phi 9\omega, \phi 13\omega, \phi 15\omega$ will be $2 - ((8, 1)/4)$, the sum of their fourth powers $= (3/2) - (3(8, 1)/16)$, the sum of their sixth powers $= (5/4) - (9(8, 1)/64) - ((8, 3)/64)$, the sum of their eighth powers $(35/32) - (27(8, 1)/256) - ((8, 3)/32)$. As a result we have

$$y = x^8 - (2 - \tfrac{1}{4}(8, 1))x^6 + (\tfrac{3}{2} - \tfrac{5}{16}(8, 1) + \tfrac{1}{8}(8, 3))x^4 - (\tfrac{1}{2} - \tfrac{9}{64}(8, 1) + \tfrac{5}{64}(8, 3))x^2 + \tfrac{1}{16} - \tfrac{5}{256}(8, 1) + \tfrac{3}{256}(8, 3)$$

and y' is determined from y by interchanging $(8, 1), (8, 3)$, so by substituting the values of these sums we get

$$y = x^8 - (\tfrac{17}{8} - \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} - \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{17}{32} - \tfrac{7}{64}\sqrt{17})x^2 + \tfrac{17}{256} - \tfrac{1}{64}\sqrt{17}$$

$$y' = x^8 - (\tfrac{17}{8} + \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} + \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{17}{32} + \tfrac{7}{64}\sqrt{17})x^2 + \tfrac{17}{256} + \tfrac{1}{64}\sqrt{17}$$

Thus Z can be resolved into four factors whose coefficients can be expressed by the sums of four terms. The product of two of them will be y, the product of the other two y'.

Sections of the circle which can be effected by means of quadratic equations or by geometric constructions

▶ 365. Thus by the preceding discussions we have reduced the division of the circle into n parts, if n is a prime number, to the solution of as many equations as there are factors in the number $n - 1$. The degree of the equations is determined by the size of the factors. Whenever therefore $n - 1$ is a power of the number 2, which happens when the value of n is 3, 5, 17, 257, 65537, etc. the division of the circle is reduced to quadratic equations only, and the trigonometric functions of the angles P/n, $2P/n$, etc. can be expressed by square roots which are more or less complicated (according to the size of n). Thus in these cases the division of the circle into n parts or the inscription of a regular polygon of n sides can be accomplished by geometric constructions. Thus, e.g., for $n = 17$, by articles 354, 361 we get the following expression for the cosine of the angle $P/17$:

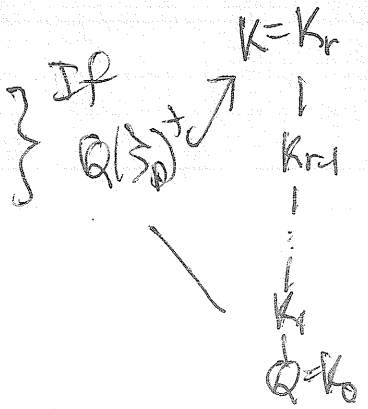
$$-\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{[34 - 2\sqrt{17}]} + \tfrac{1}{8}\sqrt{[17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17}) - 2\sqrt{(34 + 2\sqrt{17})}]}}$$

The cosine of multiples of this angle will have a similar form, but the sine will have one more radical sign. It is certainly astonishing that although the geometric divisibility of the circle into three and five parts was already known in Euclid's time, nothing was added to this discovery for 2000 years. And all geometers had asserted that, except for those sections and the ones that derive directly from them (that is, division into 15, $3 \cdot 2^n$, $5 \cdot 2^n$, and 2^n parts), there are no others that can be effected by geometric constructions.

It is easy to show that if the prime number $n = 2^m + 1$, the exponent m can have no other prime factors except 2, and so it is equal to 1 or 2 or a higher power of the number 2. For if m were divisible by any odd number ζ (greater than unity) so that $m = \zeta\eta$, then $2^m + 1$ would be divisible by $2^\eta + 1$ and so necessarily composite. All values of n, therefore, that can be reduced to quadratic equations, are contained in the form $2^{2^\nu} + 1$. Thus the five numbers 3, 5, 17, 257, 65537 result from letting $\nu = 0, 1, 2, 3, 4$ or $m = 1, 2, 4, 8, 16$. But the geometric division of the circle cannot be accomplished for *all* numbers contained in the formula but

only for those that are prime. Fermat was misled by his induction and affirmed that all numbers contained in this form are necessarily prime, but the distinguished Euler first noticed that this rule is erroneous for $v = 5$ or $m = 32$, since the number $2^{32} + 1 = 4294967297$ involves the factor 641.

Whenever $n - 1$ involves prime factors other than 2, we are always led to equations of higher degree, namely, to one or more cubic equations when 3 appears once or several times among the prime factors of $n - 1$, to equations of the fifth degree when $n - 1$ is divisible by 5, etc. WE CAN SHOW WITH ALL RIGOR THAT THESE HIGHER-DEGREE EQUATIONS CANNOT BE AVOIDED IN ANY WAY NOR CAN THEY BE REDUCED TO LOWER-DEGREE EQUATIONS. The limits of the present work exclude this demonstration here, but we issue this warning lest anyone attempt to achieve geometric constructions for sections other than the ones suggested by our theory (e.g. sections into 7, 11, 13, 19, etc. parts) and so spend his time uselessly.



then every prime $\ell \mid \frac{p-1}{2}$ divides $[K_i : K_{i-1}]$ for some i.

▶ 366. If a circle is to be cut into a^α parts where a is a prime number, manifestly this can be done geometrically when $a = 2$ but not for any other value of a if $\alpha > 1$, for then besides the equations required for the division into a parts, there will necessarily be $\alpha - 1$ others of degree a to be solved, and these cannot be avoided in any way or reduced. Therefore in general the degree of the necessary equations can be known from the prime factors of the number $(a - 1)a^{\alpha - 1}$ (including also the case where $\alpha = 1$).

Finally if the circle is to be cut into $N = a^\alpha b^\beta c^\gamma \ldots$ parts where a, b, c, etc. are unequal prime numbers, it suffices to effect divisions into a^α, b^β, c^γ, etc. parts (art. 336). So in order to know the degree of the equations necessary for this purpose, we must consider the prime factors of the numbers

$$(a - 1)a^{\alpha - 1}, \qquad (b - 1)b^{\beta - 1}, \qquad (c - 1)c^{\gamma - 1}, \text{ etc.}$$

or, what comes to the same thing, the factors of their product. We remark that this product indicates the number of numbers relatively prime to N and less than it (art. 38). Geometrically therefore this division can be accomplished only when this number is a power of 2. But when the factors include primes other than 2, say p, p', etc. then equations of degree p, p', etc. cannot be avoided.

$[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N)$
(i.e. irreducibility of Φ_N over $\mathbb{Q}$)
for all N.

In general therefore in order to be able to divide the circle geometrically into N parts, N must be 2 or a higher power of 2, *or* a prime number of the form $2^m + 1$, *or* the product of several prime numbers of this form, *or* the product of one or several such primes times 2 or a higher power of 2. In brief, it is required that N involve no odd prime factor that is not of the form $2^m + 1$ nor any prime factor of the form $2^m + 1$ more than once. The following are the 38 values of N below 300:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.