which is seen to follow from Ceva's Theorem on considering the triangle ADE and the point G.

The corresponding theorem *in plano* is :—

If a transversal ABC meets three concurrent lines OA, OB, OC, and A′, B′, C′, are points in these lines such that OA′B′C′ is a parallelogram, then

$$OA'/OA - OB'/OB + OC'/OC = 0;$$

a theorem which is very easily proved.

If we invert the four points A, B, C, D, of the theorem proved above into the points P, Q, R, S, taking O as centre and k as radius of inversion, we have

$$OA.OP = k^2; \quad \therefore \ OA = k^2/OP.$$

Substituting in the relation

$$OA'/OA - OB'/OB + OC'/OC - OD'/OD = 0,$$

we get $$OA'.OP - OB'.OQ + OC'.OR - OD'.OS = 0.$$

Hence if four points P, Q, R, S, lie on the same sphere with the point O and a plane cuts OP, OQ, OR, OS, in A′, B′, C′, D′, so that A′B′C′D′ is a parallelogram, then the above relation holds.

The condition that the extremities of four vectors lie on a sphere passing through the origin, may be written

$$\frac{a}{a^2}.\alpha + \frac{b}{\beta^2}.\beta + \frac{c}{\gamma^2}.\gamma + \frac{d}{\delta^2}.\delta = 0, \text{ where } a + b + c + d = 0;$$

or, $$p\alpha + q\beta + r\gamma + s\delta = 0, \text{ where } pa^2 + q\beta^2 + c\gamma^2 + d\delta^2 = 0.$$

On the number of elements in space.

By Rev. Norman Fraser, M.A.

On the solution of the equation $x^p - 1 = 0$ (p being a prime number).

By J. Watt Butters.

[At the first meeting of this Session a paper was read on the value of $\cos 2\pi/17$, which evidently may be made to depend on the

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

solution of $x^{17}-1=0$.* The present paper is the outcome of a suggestion then made, that a sketch of Gauss's treatment of the general equation might prove interesting. To give completeness to the subject the necessary theorems on congruences have been prefixed. The convenient notation introduced by Gauss is here adopted; thus, when the difference between a and b is divisible by p, instead of writing $a=Mp+b$, we may write $a\equiv b \pmod p$, the value of M seldom being of importance. It is evident that if $a\equiv b$, then $na\equiv nb$, and $a^n\equiv b^n$, n being any positive integer, and the same modulus p being understood throughout. Also $a/n\equiv b/n$ provided n be prime to p. Other properties (similar to those of equations) are easily seen, but only the above are needed here.

Besides the *Disquisitiones Arithmeticæ* of Gauss, which was published in 1801, and of which there is a French translation, entitled, *Recherches Mathématiques*, the following, among others, have been consulted:—Legendre's *Théorie des Nombres*, Murphy's *Theory of Equations* (1839), two papers, by M. Realis, in *Nouvelles Annales de Mathématiques* (1843), Barlow's *Theory of Numbers* (1811). Other references will be found at the end.]

§ 1. If p be prime to a, then t can be found such that $a^t\equiv 1 \pmod p$, and $0<t<p$.

Consider the series

$$a,\ a^2,\ \ldots\ a^{p-1} \qquad (1);$$

$$1,\ 2,\ \ldots\ p-1 \qquad (2).$$

Since p is prime to a, and therefore to each power of a, if the terms in (1) be divided by p, there can be no zero remainder. Hence either (a) the remainders will be all different, and therefore the same as (2), or (b) two at least will be the same. If (a) be true, the theorem follows directly; if (b), let $a^m\equiv a^n \pmod p$ (where $p>m>n$), then $a^{m-n}\equiv 1$ where $0<m-n<p$.

Cor. 1. If $a^t\equiv 1$, $a^{t+1}\equiv a$, &c., *i.e.*, the remainders of the powers of a when divided by p will recur in groups of t terms. In symbols, $a^{rt+s}\equiv a^s$; or, if $m\equiv n \pmod t$ then $a^m\equiv a^n \pmod p$.

Cor. 2. If a^d be the lowest power of a which is $\equiv 1 \pmod p$, then the remainders got by dividing

$$1,\ a,\ a^2,\ \ldots\ a^{d-1} \qquad (3),$$

by p will be all different, and will be included in the series (2). In such a case a is said to *belong* to the exponent d.

* An elementary algebraic solution of this equation is given in *Knowledge*, vol. iii., p. 316 (1883).

§ 2. If p be a prime number which does not divide a, and a belong to the exponent d, then d is a factor of $p-1$.

Let the remainders got from the series (3) be

$$1,\ a,\ a',\ a'',\ \ldots\ (d \text{ terms}) \qquad (4).$$

If these (which by § 1. Cor. 2 are all different) include all the terms of the series (2), then $d=p-1$.

[a is then called a *primitive root* of p (Euler).]

If (4) is not the same as (2), let β be a term in (2) which is not in (4), and let the remainders of $\beta,\ a\beta,\ a'\beta,\ a''\beta,\ \ldots$ be

$$\beta,\ \beta',\ \beta'',\ \ldots\ (d \text{ terms}) \qquad (5).$$

(a) No two terms in (5) are congruent, and (b) no term in (5) is congruent with a term in (4).

(a) For if $\beta a^m \equiv \beta a^n \pmod{p}$, then $a^m \equiv a^n$, which is impossible by § 1, Cor. 2.

(b) If $\beta a^m \equiv a^n$, then, according as $m >$ or $< n$, $\beta a^d \equiv a^{n+d-m}$ or $\beta \equiv a^{n-m}$; *i.e.* (since $a^d \equiv 1$), $\beta \equiv a^{d-(n-m)}$ or $\equiv a^{n-m}$, which is contrary to the hypothesis that β is not in (4).

If series (4) and (5) exhaust (2), then $2d=p-1$; if not, we may proceed in the same manner, always getting another group of d terms (such that none of the terms in all the groups are congruent) until (2) is exhausted, which must take place as $p-1$ is finite. We see, therefore, that $(p-1)/d$ is an integer.

[Cor. By raising each side of the congruence $a^d \equiv 1 \pmod{p}$ to the integral power $(p-1)/d$, we get $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.]

§ 3. Lemma:—If $d,\ d',\ d'',\ \ldots$ be all the divisors of $p-1$ (including $p-1$ and unity) and if ϕd denote the number of integers not greater than d and prime to it*, then $\phi d + \phi d' + \ldots = p-1$.

If we multiply $(p-1)/d$ by each integer prime to d and not greater than it, we shall get ϕd integers, each not greater than $p-1$, and all unequal. Similarly, from d' we shall get $\phi d'$ integers, all unequal, and each $\not> p-1$. The integers in ϕd will also differ completely from those in $\phi d'$.

For if not we should have $m\frac{p-1}{d} = n\frac{p-1}{d'}$ where m is prime to d and n to d'. Consequently, $md' = nd$. We may suppose $m > n$, then since m is prime to d and divides nd it must divide n, which is impossible. Hence, from all the divisors $d,\ d'$, &c., we shall get

* Unity is considered as being prime to every number, itself included.

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

$\phi d + \phi d' + \ldots$ different integers, each not greater than $p-1$, and hence comprised in the series (2). Further, each term in (2) will be found included in the $\phi d + \phi d' + \ldots$ integers; for, let t be any term of that series and δ the G. C. M. of t and $p-1$, then $(p-1)/\delta$ will be a divisor to which t/δ is prime, and the product of $(p-1)/\{(p-1)/\delta\}$ by $t/\delta = t$. Hence $\phi d + \phi d' + \ldots = p-1$.

§ 4. Theorem: The number of integers less than p belonging to the exponent d is ϕd

If a be an integer belonging to d, then the terms in (3), or their remainders, are roots of $x^d \equiv 1 \pmod{p}$. Since this congruence cannot have more than d different roots and the above remainders are d in number and all different, it follows that the series (3) must contain all the integers belonging to d. Let ψd denote the number of them.

Let a^k be one of the series, then a^k does or does not belong to d, according as k is or is not prime to d.

1° Suppose k prime to d and let $km \equiv 1 \pmod{d}$, then (§ 1. Cor. 1.) $a^{km} \equiv a \pmod{p}$. If possible, let $(a^k)^e \equiv 1$, where $e < d$; $a^{kme} \equiv 1$ and $\therefore a^e \equiv 1$, which is contrary to the hypothesis that a belongs to d. Hence a^k belongs to d.

2°. Suppose k not prime to d and let δ be a common divisor. Since $kd/\delta \equiv 0 \pmod{d}$, $a^{kd/\delta} \equiv 1 \pmod{p}$, *i.e.*, $(a^k)^{d/\delta} \equiv 1$. Hence a^k does not belong to d.

Thus we have proved that if there be any integer belonging to d, there are as many as there are integers not greater than d and prime to it, *i.e.*, $\psi d = 0$ or $= \phi d$.

Now, evidently each term of the series (2) must belong to one of the divisors of $p-1$,

and hence $\psi d + \psi d' + \psi d'' + \ldots = p-1$ (A),

but $\phi d + \phi d' + \phi d'' + \ldots = p-1$ (B),

and since no term in (A) can exceed the corresponding term in (B), we must have $\psi d = \phi d$, &c.

Cor. This contains, as a particular case, the important theorem that every prime number has at least one primitive root. This amounts to saying that it is always possible to find an integer g, so that to each term of the series

$$1, g, g^2, \ldots g^{p-2} \qquad (6)$$

there will be congruent, to the modulus p, one of the series

$$1, 2, 3, \ldots p-1. \qquad (2)$$

Further: If λ be not divisible by p, then the series

$$\lambda, \lambda g, \lambda g^2, \ldots \lambda g^{p-2} \qquad (6')$$

is congruent with the series (2).

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

§ 5. Now, we know from the Theory of Equations that if r denote any imaginary root of the equation $x^p - 1 = 0$, then all the roots of $X \equiv (x^p - 1)/(x - 1) = 0$ are given by

$$r,\ r^2,\ r^3,\ \ldots\ r^{p-1} \tag{7}.$$

Moreover, since $r^p = 1$, $r^{p+1} = r$, &c., and generally $r^{mp+a} = r^a$, we see that if $a \equiv b \pmod p$ then $r^a = r^b$. Hence, by § 4, Cor., instead of the series (7) we may use

$$r\lambda,\ r\lambda g,\ r\lambda g^2,\ \ldots\ r\lambda g^{p-2}$$

to express the roots of $X = 0$.

To avoid the difficulty of printing the roots in this form, Gauss expresses them by the notation

$$[\lambda],\ [\lambda g],\ [\lambda g^2],\ \ldots\ [\lambda g^{p-2}] \tag{8}.$$

Evidently we have $[\lambda].[\mu] = [\lambda + \mu]$ and $[\lambda]^\mu = [\lambda\mu]$. Further, the roots $[\lambda g^m]$, $[\lambda g^n]$ will be identical or different according as m is congruent or is not congruent with $n \pmod{p-1}$.

§ 6. Since $p - 1$ is not a prime number, we may suppose $p - 1 = ef$. We may then write the roots as follows (putting $\lambda = 1$):—

$$\begin{array}{llll} [1], & [g^e], & [g^{2e}], & \ldots\ [g^{(f-1)e}] \\ [g], & [g^{e+1}], & [g^{2e+1}], & \ldots\ [g^{(f-1)e+1}] \\ [g^2], & [g^{e+2}], & [g^{2e+2}], & \ldots\ [g^{(f-1)e+2}] \\ \cdot & \cdot & \cdot & \cdots\ \cdot \\ [g^{e-1}], & [g^{2e-1}], & [g^{3e-1}], & \ldots\ [g^{ef-1}]. \end{array} \tag{9}$$

Where the first column contains the first e roots, the second column the second e roots, and so on.

If the series (8) be extended indefinitely, we know that any $p - 1$ consecutive terms will denote the roots given by (8) itself. Hence, considering the mode of formation of the above table, we see that if any row be extended indefinitely it also will reproduce the same roots as are given by the row itself. Hence if, for brevity, we put $g^e = h$, and denote the sum of the roots in any row by (f, λ), we may also denote it by $(f, \lambda h)$, $(f, \lambda h^2)$, $\ldots$ $(f, \lambda h^{f-1})$.

When we wish to speak of the roots in (f, λ) without expressing the idea of summation, we may speak of the *period* (f, λ). Periods containing the same number of roots are called *similar*.

Cor. 1. If (f, λ), (f, μ) denote similar periods, they will be identical, if they contain a common root. If μ is not divisible by p, then (f, μ) will be identical with one of the periods $(f, 1)$, (f, g), (f, g^2), $\ldots$ (f, g^{e-1}). If $\mu \equiv 0 \pmod p$, then (f, μ) will be equal to f units. These results follow directly from the above table.

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

Cor. 2. If f be not a prime number, say, $=ab$, then any period (f, λ) may be written thus:—

$$\begin{array}{llll} [\lambda], & [\lambda h^a], & \dots & [\lambda h^{(b-1)a}] \\ [\lambda h], & [\lambda h^{a+1}], & \dots & [\lambda h^{(b-1)a+1}] \\ \cdot & \cdot & \cdots & \cdot \\ [\lambda h^{a-1}], & [\lambda h^{2a-1}], & \dots & [\lambda h^{ab-1}]; \end{array}$$

i.e., we may break up any period (f, λ) or (ab, λ) into smaller periods (b, λ), $(b, \lambda h)$, ... $(b, \lambda h^{a-1})$. If b have factors, the process may be repeated, and so on.

§ 7. If (f, λ), (f, μ) be two similar periods, then

$$(f, \lambda).(f, \mu) = (f, \lambda+\mu) + (f, \lambda h+\mu) + (f, \lambda h^2+\mu) + \dots + (f, \lambda h^{f-1}+\mu).$$

By § 6. $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2) = \dots = (f, \lambda h^{f-1})$.

Hence $(f, \lambda).(f, \mu) = [\mu].(f, \lambda) + [\mu h].(f, \lambda h) + \dots + [\mu h^{f-1}].(f, \lambda h^{f-1})$

$$\begin{array}{llllll} = [\lambda+\mu] & +[\lambda h+\mu] & +[\lambda h^2+\mu] & & +\dots+[\lambda h^{f-1}+\mu] \\ +[\lambda h+\mu h] & +[\lambda h^2+\mu h] & +[\lambda h^3+\mu h] & & +\dots+[\lambda h^f+\mu h] \\ \dots & \dots & \dots & \dots & \dots \\ +[\lambda h^{f-1}+\mu h^{f-1}] & +[\lambda h^f+\mu h^{f-1}] & +[\lambda h^{f+1}+\mu h^{f-1}] & & +\dots+[\lambda h^{2f-2}+\mu h^{f-1}] \end{array}$$

= (by adding the terms in each column together)

$$(f, \lambda+\mu) + (f, \lambda h+\mu) + (f, \lambda h^2+\mu) + \dots + (f, \lambda h^{f-1}+\mu).$$

Cor. 1. From the results of § 6, Cor. 1, we see that the above product may be put in the form

$$(f, \lambda).(f, \mu) = af + b(f, 1) + c(f, g) + d(f, g^2) + \dots + k(f, g^{e-1}) \quad (10)$$

where the coefficients a, b, ... k are known integers.

Cor. 2. The product of any number of similar periods can be expressed in the form (10).

Cor. 3. Hence any rational integral function of similar periods can be expressed in the same form.

§ 8. If $(f, \lambda) = n$, then any similar period (f, μ) can be expressed in the form $(f, \mu) = a + bn + cn^2 + \dots$

where a, b, c, ... are rational coefficients.

Let n, n', n'', ... denote the periods (f, λ), $(f, \lambda g)$, $(f, \lambda g^2)$,... as far as $(f, \lambda g^{e-1})$, with one of which, say n', (f, μ) must coincide (unless $\mu \equiv 0 \pmod p$, when $(f, \mu) = f$).

Since the sum of the roots of $X = 0$ is -1 we have

$$0 = 1 + n + n' + n'' + \dots$$

and forming by § 7, Cor. 2, the valnes of n^2, n^3, ... n^{e-1} we get $e-2$ other equations

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

$$n^2 = af + bn + cn' + dn'' + \ldots$$
$$n^3 = a'f + b'n + c'n' + d'n'' + \ldots$$
$$n^4 = a''f + b''n + c''n' + d''n'' + \ldots$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

in which the coefficients are rational and independent of λ.

From these $e-1$ equations eliminate the $e-2$ quantities $n'', n''', \ldots$ and we will get an equation of the form $A + Bn + Cn^2 + \ldots + Mn^{e-1} + Nn' = 0$ (where A, B, ... N are integers and not all zero), which proves the theorem if N be not zero.

If we suppose that $N = 0$, then we get the equation

$$Mn^{e-1} + \ldots + Cn^2 + Bn + A = 0.$$

Now, since the $e-1$ equations from which this equation is deduced are all independent of λ, so will this equation be. It should therefore have the e roots $(f, 1)$, (f, g), (f, g^2), ... (f, g^{e-1}), but this is impossible since its degree is $e-1$; and therefore N cannot vanish.

[Gauss further considers the possibility of two of these roots being equal and there being therefore *apparently* only $e-1$ roots.]

Cor. If we form as above the values of $n^2, n^3, \ldots n^e$ in terms of $n, n', n'', \ldots$ and from the e equations eliminate the $e-1$ quantities $n', n'', \ldots$ we shall get an equation of the *eth* degree, the roots of which will be the e quantities $n, n', n'', \ldots$

We now require to form equations for the roots in each period. This is shown to be possible by the following theorem.

§ 9. If $F([\lambda], [\lambda'], [\lambda''], \ldots)$ be any rational integral *symmetric* function of the roots of any period (f, λ), it may be expressed in the form $a + b(f, 1) + c(f, g) + \ldots + k(f, g^{e-1})$. (10)

1°. It is evident that F may be expressed in the form $A + Br + Cr^2 + \ldots + Kr^{p-1}$, or $A + B[1] + C[2] + \ldots + K[p-1]$, for each term of F must be the product of certain powers of r, and therefore itself a power of r, and its exponent may be made less than p since $r^p = 1$.

2°. The roots belonging to the same period will have equal coefficients and therefore may be summed under the form $M(f, \mu)$, say. Let $[\alpha]$, $[\beta]$ be a pair of roots belonging to a given period; we may suppose $\beta = \alpha h^m$, where $g^{(p-1)/e} = h$. In the identity

$$F([\lambda], [\lambda'], [\lambda''], \ldots) = A + B[1] + C[2] + \ldots + K[p-1]$$

substitute λh^m for λ. This will not alter the value of F, since it is a symmetric function of the roots of (f, λ), and hence we get

$$F([\lambda], [\lambda'], [\lambda''], \ldots) = A + B[h^m] + C[2h^m] + \ldots + K[(p-1)h^m].$$

Comparing these two expressions for F, we see that $[1]$ and $[h^m]$ have equal coefficients, and similarly with $[2]$ and $[2h^m]$, ... with $[\alpha]$ and

$[ah^m]$; *i.e.*, with any two roots of the same period. Hence the theorem follows.

Cor. Since the coefficients of an equation are symmetric functions of its roots, we see that the coefficients of an equation determining the roots of a given period may be expressed in the form (10).

§ 10. The two last paragraphs show us that if $p-1=ef$, we can make the solution of $x^p-1=0$ depend upon the solution of equations of the degrees e and f. The following theorem shows us that if f is not prime, we may make the solution depend on equations of still lower degree.

Let as in § 6, Cor. 2, $f=ab$ and F be a symmetric function of the periods (b, λ), $(b, \lambda h)$, ... then F may be expressed in the form

$$a+b(f, 1)+c(f, g)+ \ \ldots \qquad (10)$$

By the last paragraph F may be put in the form $A+B(b, 1)+C(b, g)+ \ \ldots$

Now the periods (b, λ), $(b, \lambda h)$, ... of which (f, λ) is composed are unaltered when $\lambda h^{a.m}$ is put in place of λ, hence in $A+B(b, 1)+C(b, g)+ \ \ldots$ there ought to be a term (b, a) which has the same coefficient as $(b, ah^{a.m})$ where m may have the values 1, 2, 3, ... $a-1$; *i e.*, all the periods forming (f, λ) have the same coefficient. F may therefore be put in the required form.

§ 11. We may now describe the general method of making the solution of $x^p-1=0$ (where p is a prime number) depend on equations of as low degree as possible.

1°. Find a primitive root g of the prime number p.

2°. Find the remainders (mod p) of the series $1, g, g^2, \ldots g^{p-2}$.

3°. Resolve $p-1$ into its prime factors, say $p-1=abc \ldots k$.

4°. As in § 6, write the roots in a rectangular array, the first a in the first column, the second a in the second column, and so on, thus getting a periods of $bc \ldots k$ terms. Treat similarly the roots of each of these periods, getting b periods of $c \ldots k$ terms from each; and so on.

5°. Form an equation (A) (Cor. § 8), which has for its roots the a periods; any root of this may be taken as the value of $(bc \ldots k, 1)$, for *any* root of $X=0$ may be called r^1, and therefore any period may be considered as including [1]. The other periods $(bc \ldots k, g)$, $(bc \ldots k, g^2)$, ... may now be determined by § 8. Hence it is necessary to find only one root of (A).

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

We may distinguish the roots also by putting

$$[1] = \cos\frac{2m\pi}{p} + i\sin\frac{2m\pi}{p},$$

(where m is not divisible by p) and hence calculating from a table of sines and cosines the values of [2], [3],...with sufficient accuracy to determine their relative magnitude. We can thus distinguish the roots of (A) which should be denoted by $(bc \ldots k, 1)$, $(bc \ldots k, g)$, ... respectively.

6°. Now, form an equation (B) (§ 10), which has for its roots the b periods contained in $(bc \ldots k, 1)$. As before, we may arbitrarily assign any root of (B) as the value of $(c \ldots k, 1)$ and calculate the value of each similar period: or distinguish the roots by the help of a table of sines as above. Proceeding in this way we at last find the values of $(k, 1)$, (k, g), ...

7°. Now, form an equation (K) (Cor. § 9), which has for its roots the roots of $X = 0$ contained in $(k, 1)$. Any root of (K) being called [1], its successive powers will give all the other roots of $X = 0$.

§ 12. It is evident from the last paragragh that if $p - 1 = 2^a.3^b.5^c\ldots$ the solution of $X = 0$ may be made to depend on a equations of the 2nd degree, b equations of the 3rd degree, c of the 5th, &c.

That the solution may depend on quadratic equations only, we must have $p - 1 = 2^\alpha$, *i.e.*, p must be of the form $2^\alpha + 1$ and be a prime number. If a be odd then $2^a + 1$ is divisible by $2 + 1$ and hence p is not prime. Further if a contain an odd factor, say $a = bc$ where c is odd, then $2^{bc} + 1$ is divisible by $2^b + 1$ and again p is not prime. That the form $2^\alpha + 1$ may be prime it is therefore *necessary* that a should be of the form 2^m, *i.e.*, $p = 2^{2^m} + 1$. But this condition is not *sufficient* (as stated by Fermat) for Euler has shown that $2^{32} + 1$ (4,294,967,297) is divisible by 641.

When $m = 0, 1, 2, 3, 4$; p becomes 3, 5, 17, 257, 65537 which are all prime. Hence the corresponding roots of unity may be found by quadratic equations only. Further, we may inscribe in a circle regular polygons of 3, 5, 17, &c., sides by means of ruler and compasses. The case of a 17-gon is given later on.

[From other considerations we know that if an m-gon and an n-gon (m prime to n) can be inscribed in a circle, so also may an mn-gon. Further, we may inscribe a polygon having double the number of sides of any inscribed polygon. Hence an n-gon may be inscribed in a circle if n contains no *odd* factor except of the form $2^{2^m} + 1$, each such factor being prime and not repeated.]

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

§ 13. As illustrative of the above, let us consider the case where $p = 17$.

In the following table, each column (except the first) gives the numbers which are congruent (mod 17) to the successive powers of the first number in the column. The first column gives the corresponding exponent. For example, the column headed 6 gives the remainders when 6, 6^2, 6^3,... respectively are divided by 17.

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

This readily exemplifies the theorems in § 1 and Corollaries.

https://doi.org/10.1017/S0013091500030273 Published online by Cambridge University Press

The theorem of § 2 and Fermat's theorem are likewise illustrated; *e.g.*, the only exponents to which numbers *belong* in this table are 1, 2, 4, 8, and 16, all of which are factors of $17 - 1$.

§ 4 also finds illustration; *e.g.*, belonging to the exponent 8 are the numbers 2, 8, 9, 15; each of these numbers occurs as a remainder in the columns headed by these numbers; the corresponding exponents are always prime to 8 (unity being considered as prime to every number as in § 3); and the exponents corresponding to the other remainders are not prime to 8; lastly, 17 has a primitive root. (In fact there are $\phi 16 = 8$ primitive roots—viz., 3, 5, 6, 7, 10, 11, 12, and 14.)

§ 14. In general we need to find only one primitive root, and this may usually be done most simply by successive trial of the small numbers 2, 3,... Use should be made of the results in §§ 2 and 4. *E.g.* By trial we find the remainders of 2, 2^2, 2^3,... to be 2, 4, 8, 16, 15, 13, 9, 1. As a second trial we might take any of the numbers *not* contained in this series. In this case this is unnecessary, for, since 8 contains all the divisors of 16 (except 16 itself), we see that only the above numbers can belong to exponents less than 16, and hence the primitive roots of 17 are 3, 5, 6, 7, 10, 11, 12, 14, as above.

We may now arrange the roots in two periods as in § 6. We thus get:

(8, 1) containing [1], [9], [13], [15], [16], [8], [4], [2].
(8, 3) ,, [3], [10], [5], [11], [14], [7], [12], [6].

Calling these periods n and n' respectively, we have:

$$n + n' = (16, 1) = -1 \quad (a);$$

and § 7, $nn' = (8, 4) + (8, 11) + (8, 6) + (8, 12) + (8, 15) + (8, 8) + (8, 13) + (8, 7)$

$$= n + n' + n' + n' + n + n + n + n'$$
$$= 4(n + n') = -4 \quad (b),$$

and therefore n and n' are the roots of $n^2 + n - 4 = 0$.

We now break up the above periods into smaller periods, and get from the period (8, 1)

(4, 1) containing [1], [13], [16], [4] say m
(4, 9) ,, [9], [15], [8], [2] ,, m'.

Also from (8, 3) we get

(4, 3) containing [3], [5], [14], [12] say m''
(4, 10) ,, [10], [11], [7], [6] ,, m'''.

Here $m + m' = (8, 1) = n$, say (c)

and
$$mm' = (4, 10) + (4, 16) + (4, 9) + (4, 3)$$
$$= m''' + m + m' + m''$$
$$= n + n' = -1 \ (d)$$

and hence (4, 1) and (4, 9) are the roots of $m^2 - nm - 1 = 0$. Similarly (4, 3) and (4, 10) are the roots of $m^2 - n'm - 1 = 0$, for we have $m'' + m''' = n'$ (e) and $m''m''' = -1$ (f).

[To illustrate the application of § 9 Cor., we may find an equation for the roots contained in the period (4, 1). Let $x^4 - Ax^3 + Bx^2 - Cx + D = 0$ be the required equation. $A = \Sigma x' = m$

$$\Sigma x'x'' = [14] + [17] + [5] + [12] + [17] + [3] = 2 + m'' = B$$
$$\Sigma x'x''x''' = [16] + [4] + [1] + [13] = m = C$$

and $x'x''x'''x'''' = 1$. Therefore the equation for the roots r^1, r^{13}, r^{16}, r^4 of the original equation is $x^4 - mx^3 + (2 + m'')x^2 - mx + 1 = 0$ (A) where m and m' are known. Any root of this equation may be called r, the others being determined by their relationship to r.

By symmetry we have other 3 equations to determine the other 12 roots; or all the roots may be determined from the value of r, *any* root of (A) by forming the powers r^2, r^3, $\therefore$ r^{16}.]

Continuing, however, the process of separating the periods into lower periods we get:

(2, 1)	containing	[1], [16]	(2, 3)	containing	[3], [14]
(2, 13)	,,	[13], [4]	(2, 5)	,,	[5], [12]
(2, 9)	,,	[9], [8]	(2, 10)	,,	[10], [7]
(2, 15)	,,	[15], [2]	(2, 11)	,,	[11], [6]

Calling these periods $l_1, l_2, \ldots l_8$, we have

$$l_1 + l_2 = m \ (g), \text{ and } l_1 l_2 = l_5 + l_6 = m'' \ (h);$$
$$\therefore \ l^2 - ml + m'' = 0 \text{(B) has (2, 1) and (2, 13) for roots.}$$

Lastly $[1] + [16] = l_1$ and $[1].[16] = 1$ and therefore r is a root of $r^2 - l_1 r + 1$ (C).

It is easy to see that the reciprocal equation (A) is equivalent to the two quadratics (B) and (C).

§ 15. Inscription of a regular 17-gon in a given circle.

If AB be the side of a regular 34-gon then $AB = 2 \sin \frac{\pi}{34}$ (the radius being considered as unity), *i.e.* $AB = 2 \cos 4 \frac{2\pi}{17}$.

Now if we put $[1] = \cos \frac{2\pi}{17} + i \sin \frac{2\pi}{17}$

then $[16] = \cos \frac{2\pi}{17} - i \sin \frac{2\pi}{17}$

and $(2, 1) = 2 \cos \frac{2\pi}{17}$. Accordingly $AB = (2, 4)$.

From a table of cosines we get the following values to enable us to distinguish the roots:

$$l_1 = 1{\cdot}87\,;\ l_2 = {\cdot}18\,;\ l_3 = -1{\cdot}97\,;\ l_4 = 1{\cdot}48\,;$$
$$l_5 = {\cdot}89\,;\ l_6 = -{\cdot}55\,;\ l_7 = -1\,70\,;\ l_8 = -1{\cdot}21.$$

From these we get $m = 2{\cdot}05\,;\ m' = -{\cdot}49\,;\ m'' = {\cdot}34\,;\ m''' = -2{\cdot}91$. Lastly, $n = 1{\cdot}56$ and $n' = -2{\cdot}56$.

Construction :—Draw OX (fig. 3) a tangent and OY a diameter to the given circle with centre A and radius unity. Consider through out lengths to the right of O as positive and to the left as negative. In OX take $OB = -\frac{1}{4}$. With B as centre and radius BA describe a circle meeting OX in C and D, then 2OC, 2OD are the roots of (a) and (b). For $2OC.2OD = -4OA^2 = -4 = nn'$ and $2OC + 2OD = 4OB = -1 = n + n'$. By the above values we see that $2OC = n$ and $2OD = n'$.

With C as centre and CA as radius describe the circle EAF.

Then $OE.OF = -OA^2 = -1 = mm'$ (d)

and $OE + OF = 2OC = n$ (c)

Hence, considering the above values, we get $OE = m$.

With D as centre and DA as radius describe the circle GAH.

Then $OG.OH = -OA^2 = -1$ (f)

and $OG + OH = 2OD = n'$ (e)

Hence $OG = m''$

Make $OK = OA$ and on GK describe a semicircle meeting OY in L. Through M, the middle point of OE draw a parallel to OY and through L a parallel to OX. Let these meet in P. With P as centre and PL as radius describe a circle meeting OX in N and Q. Then $ON.OQ = OL^2 = OG.OK = OG = m''$ (h); and $ON + OQ = 2OM = OE = m$ (g). $ON = l_2 = (2, 4) =$ the length of the side of a regular 34-gon.

The above construction is based on that given in Serret's *Algébre Supérieure*. A geometrical analysis of the problem is given in Catalan's *Théorèmes et Problèmes de Géométrie Élémentaire*, 6ème éd. p. 267 (1879), and also (somewhat simplified) in the appendix to Casey's *Elements of Euclid*. Geometrical constructions are also given, by H. Schroeter, in *Crelle's Journal* (1872), translated in *Nouvelles Annales de Mathématiques* (1874), and by v. Staudt in *Crelle's Journal* (1842).