Mathematics. — "*The primitive divisor of* $x^m—1$". By Prof. J. C. KLUYVER.

(Communicated in the meeting of November 25, 1916).

The binomial equation $x^m-1=0$ has $M=\varphi(m)$ special roots, which do not belong to any binomial equation of lower degree. Denoting by ν the integers less than m and prime to m these special roots are of the form $x_\nu = e^{\frac{2\pi i\nu}{m}}$ and the product

$$F_m(x) = \underset{\nu}{\Pi}(x—x_\nu)$$

is called by KRONECKER the primitive divisor of $x^n—1$.

It is shewn that $F_m(x)$ cannot be resolved into rational factors and that the decomposition of $x^m—1$ into rational prime factors is given by the equation

$$x^m-1 = \underset{d/m}{\Pi} F_d(x),$$

where d is successively equal to the different divisors of m, unity and m itself included.

By inverting this formula in the usual manner, we infer that

$$F_m(x) = x^M F_m\left(\frac{1}{x}\right) = \underset{d/m}{\Pi}(x^d—1)^{\mu(d)} = \underset{d/m}{\Pi}(1-x^d)^{\mu(d')}.$$

$$(dd'=m)$$

In this fundamental equation $\mu(d')$ stands for zero, if d' has a square divisor and otherwise $\mu(d')$ equals $+1$ or -1, according as d' is a product of an even or of an odd number of prime numbers.

From this expression of $F_m(x)$ the following properties of the primitive divisor may be deduced.

I. If $m=n_1n_2$ and n_1 and n_2 are relatively prime, then

$$F_m(x) = \underset{d/n_1}{\Pi} F_{n_2}(x^d)^{\mu\left(\frac{n_1}{d}\right)}.$$

II. The greatest common measure of $F_{n_1}(x^{n_2})$ and $F_{n_2}(x^{n_1})$ is $F_{n_1n_2}(x)$, n_1 and n_2 being prime to each other.

III. If m has at least two different prime divisors, then $F_m(1)=1$, but $F_m(1)=p$, when m is a prime number p or equal to a power of p.

IV. If m resolved into prime factors is of the form $m=$ $=p_1^{\nu_1}p_2^{\nu_2}\ldots p_k^{\nu_k}$ and m_0 denotes the product $p_1p_2\ldots p_k$, then

$$F_m(x) = F_{m_0}\left(x^{\frac{m}{m_0}}\right).$$

From this proposition it follows that in order to find a definite expression for the polynomial $F_m(x)$, we need only consider the case that m has no square divisors, and a further limitation is still possible. In fact, when m having a single factor 2 is equal to $2n$ we have

$$F_{2n}(x) = \frac{F_n(x^2)}{F_n(x)} = F_n\,(-x),$$

and thus the construction of the primitive divisor in general is made to depend on the case that m is a product of unequal odd prime numbers.

V. Let p be a prime number not dividing the integer n and $m = pn$, then

$$F_m(x) - 1 \text{ is divisible by } x^{p-1} - 1,$$

when n is not a factor of $p-1$.

On the contrary. when $p - 1 = kn$

$$F_m(x) - 1 \text{ is divisible by } \frac{x^{p-1}-1}{F_n(x)}$$

and

$$F_m(x) + p \text{ is divisible by } F_n(x).$$

VI. Let p be a prime number not dividing the integer n and $m = pn$, then

$$F_m(x) - x^{p\varphi(n)} \text{ is divisible by } x^{p+1} - 1,$$

when n is not a factor of $p + 1$.

On the contrary, when $p + 1 = kn$

$$F_m(x) - x^{p\varphi(n)} \text{ is divisible by } \frac{x^{p+1}-1}{F_n(x)}$$

and

$$F_m(x) + px^{p\varphi(n)} \text{ is divisible by } F_n(x).$$

VII. The sum of the roots x_j of the primitive divisor $F_m(x)$ is equal to $\mu(m)$.

VIII. Denoting by D the greatest common measure of the integers k and m and supposing m to have no square divisors the sum of the k^{th} powers of the roots x_j is equal to

$$\mu(m)\,\mu(D)\,\varphi(D).$$

From the known values of the sums $\sum x_j^k$, $k = 1, 2, 3 \ldots.$ the coefficients A_h of the polynomial

$$F_m(x) = A_0 + A_1 x + A_2 x^2 + \ldots + A_M x^M$$

might be calculated, but we may proceed in a slightly different way.

Supposing m to be a product of unequal odd prime numbers the integers r less than m and prime to m may be arranged into two groups according as the Legendre symbol $\left(\frac{v}{m}\right)$ has the value $+1$ or -1. This implies an arrangement of the roots of $F_m(x)$. We have the roots $u = e^{\frac{2\pi ic}{m}}$, where $\left(\frac{c}{m}\right) = +1$ and an equal number of roots $u' = e^{\frac{2\pi i c'}{m}}$, where $\left(\frac{c'}{m}\right) = -1$.

Now by proposition VIII we have

$$\sum_u u^k + \sum_{u'} u'^k = \mu(m)\,\mu(D)\,\varphi(D),$$

but at the same time we infer from Gauss's theorem

$$\sum_u u^k - \sum_{u'} u'^k = \left(\frac{k}{m}\right) i^{\frac{1}{4}(m-1)^2} \sqrt{m}.$$

Hence the sums $\sum\limits_u u^k$ and $\sum\limits_{u'} u'^k$ may be calculated separately and if we introduce the conjugate (real or complex) irrationalities

$$\eta = \tfrac{1}{2} \left\{ \mu(m) + i^{\frac{1}{4}(m-1)^2} \sqrt{m} \right\},$$

$$\eta' = \tfrac{1}{2} \left\{ \mu(m) - i^{\frac{1}{4}(m-1)^2} \sqrt{m} \right\},$$

it will be found that there exists a polynomial $f^m(x, \eta) = \prod\limits_u (x-u)$, linear in η with real integer coefficients, having the roots u and also a quite similar conjugate polynomial $f_m(x, \eta') = \prod\limits_u (x - u')$, having the roots u'.

As obviously

$$F_m(x) = f_m(x,\eta) \times f_m(x,\eta')$$

it appears that by adjoining the irrationality η to the set of real integers the polynomial $F_m(x)$ has become decomposable.

The values of $\sum\limits_u u^k$ and $\sum\limits_u u'^k$ for $k = 1, 2, 3, \ldots, \frac{M}{2}$ being calculated, it would be possible to find the coefficients of either of the polynomials $f_m(x, \eta)$ and $f_m(x, \eta')$, but I will only apply Gauss's theorem to deduce a tolerably regular expression for their product $F_m(x)$.

If we substitute for x successively the roots u and u' in the identity

$$x^n F_m(x) = \sum_{h=0}^{h=M} A_h x^{h+n},$$

the application of the theorem gives at once

$$0 = \sum_{u} u^n F_m(u) - \sum_{u'} u'^n F_m(u') = i^{\frac{1}{4}(m-1)^2} \sqrt{m} \sum_{h=0}^{h=M} A_k \left(\frac{k+n}{m}\right),$$

and hence

$$\sum_{h=0}^{h=M} A_k \left(\frac{h+n}{m}\right) = 0.$$

From this relation we obtain taking n equal to $0, -1, -2, \ldots, -M+1$ a set of M equations from which the ratios of the coefficients A_h can be solved. In fact, these M equations must be mutually independent, because they are equivalent to the ordinary NEWTON and WARING relations between the coefficients of an algebraic equation and the sums of similar powers of roots.

Joining to the M equations the equation

$$F_m(x) = \sum_{h=0}^{h=M} A_h x^h,$$

we may eliminate the coefficient A_h and introducing a determinate constant C we shall find

$$C \times F_m(x) = \begin{vmatrix} 1 & x & x^2 & x^3 & \ldots & x^{M-1} & x^M \\ 0 & \left(\frac{1}{m}\right) & \left(\frac{2}{m}\right) & \left(\frac{3}{m}\right) & \ldots & \left(\frac{M-1}{m}\right) & \left(\frac{M}{m}\right) \\ \left(\frac{-1}{m}\right) & 0 & \left(\frac{1}{m}\right) & \left(\frac{2}{m}\right) & \ldots & \left(\frac{M-2}{m}\right) & \left(\frac{M-1}{m}\right) \\ \left(\frac{-2}{m}\right) & \left(\frac{-1}{m}\right) & 0 & \left(\frac{1}{m}\right) & \ldots & \left(\frac{M-3}{m}\right) & \left(\frac{M-4}{m}\right) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \left(\frac{-M+1}{m}\right) & \left(\frac{-M+2}{m}\right) & \left(\frac{-M+3}{m}\right) & \left(\frac{-M+4}{m}\right) & \ldots & 0 & \left(\frac{1}{m}\right) \end{vmatrix}.$$

Observing that the term x^M in $F_m(x)$ has the coefficient $+1$, the constant C is readily determined as a symmetric or as a skew symmetric determinant.

As we already remarked proposition VIII in itself suffices to calculate the coefficients A_h and it is evident that in this way there might be deduced a second determinant also representing $F_m(x)$. To obtain this second determinant we have only to replace everywhere in the first the symbols $\left(\frac{k}{m}\right)$ and $\left(\frac{-k}{m}\right)$ by $\mu(D)\,\varphi(D)$, when D is the greatest common measure of k and m, taking $D=m$ for $k=0$, and it is rather remarkable that notwithstanding the dissimilar character of the elements of these determinants both represent one and the same polynomial.

If m is prime, we have $M = m - 1$ and the determinant representing $F_m(x)$ by adding to the first column all the other ones is immediately reduced to the polynomial $1 + x + x^2 + \ldots + x^{m-1}$. In the general case the coefficients of $F_m(x)$ are not of so simple a character as perhaps might be presumed. Only two of them, the coefficients A_1 and A_{M-1}, take the simple value $-\mu(m)$ and therefore I may end with the proposition

IX. If m is the product of unequal odd prime factors, then

$$\mu(m) \times \begin{vmatrix} 0 & \left(\frac{1}{m}\right) & \left(\frac{2}{m}\right) & \ldots & \left(\frac{M-1}{m}\right) \\ \left(\frac{-1}{m}\right) & 0 & \left(\frac{1}{m}\right) & \ldots & \left(\frac{M-2}{m}\right) \\ \left(\frac{-2}{m}\right) & \left(\frac{-1}{m}\right) & 0 & \ldots & \left(\frac{M-3}{m}\right) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \left(\frac{-M+1}{m}\right) & \left(\frac{-M+2}{m}\right) & \left(\frac{-M+3}{m}\right) & \ldots & 0 \end{vmatrix} =$$

$$= \begin{vmatrix} 0 & \left(\frac{1}{m}\right) & \left(\frac{2}{m}\right) & \ldots & \left(\frac{M-2}{m}\right) & \left(\frac{M}{m}\right) \\ \left(\frac{-1}{m}\right) & 0 & \left(\frac{1}{m}\right) & \ldots & \left(\frac{M-3}{m}\right) & \left(\frac{M-1}{m}\right) \\ \left(\frac{-2}{m}\right) & \left(\frac{-1}{m}\right) & 0 & \ldots & \left(\frac{M-4}{m}\right) & \left(\frac{M-2}{m}\right) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \left(\frac{-M+1}{m}\right) & \left(\frac{-M+2}{m}\right) & \left(\frac{-M+3}{m}\right) & \ldots & \left(\frac{-1}{m}\right) & \left(\frac{1}{m}\right) \end{vmatrix}.$$

Thus it is shewn that the symbol $\mu(m)$ is expressible by LEGENDRE symbols only.

Pathology. — "*On passive immunisation against tetanus.*" By Prof. Dr. C. H. H. SPRONCK and WILHELMINA HAMBURGER, Arts.

(Communicated in the meeting of November 25, 1916).

As known, the injection of a heterologous serum not seldom causes symptoms of disease, and experience teaches us, that the injection of a large quantity of serum oftener causes the so-called serum disease than the injection of a smaller quantity. Hence the endeavours of the serum institutes to produce an immune serum with high titre, so that the injection of a small quantity of serum