ON THE PRIME DIVISORS OF THE CYCLOTOMIC FUNCTIONS*

BY

C. M. HUBER

Sylvester† gave the first theorem in which the prime divisors of the cyclotomic functions are distinguishable from the non-divisors by their linear character. T. Pepin‡ in a later paper proved this statement of Sylvester, namely that all prime divisors of the function $x^3-3x\pm 1$, if integral values are assigned to x, are 3, or primes of the form $18n\pm 1$ exclusively. In a footnote to the above paper, Sylvester states the conjecture that the period function which gives rise to the equation for the determination of the e periods of order f of the primitive qth roots of unity, q a prime, is divisible by any power of a prime which is an eth power residue modulo q.

In the following paper we shall establish the above conjecture by Sylvester, giving in the form of a general theorem a test as to whether a given prime is a divisor or non-divisor of the general cyclotomic functions. In the development we shall need a theorem stated by Kummer§ but not rigorously proved by him, as pointed out by H. J. S. Smith|| and Dirichlet¶, who both gave methods of correcting Kummer's error which are substantially the same as that given by Kummer himself in a later paper.** We shall give here an independent proof of the theorem to enable us to draw conclusion as to the ideal factors of the primes in the cyclotomic subfields.

Let q be an odd rational prime, and let ζ designate one of the primitive qth roots of unity. Let the domain of rationality defined by ζ be designated by $k(\zeta)$. Consider p a prime different from q and appertaining to the exponent f modulo q. Then f must be a divisor of $q-1$, so we write $q-1 = e\cdot f$. In $k(\zeta)$, p will be the product of e prime ideals each of degree f, hence we write $p = \mathfrak{p}_1\cdot\mathfrak{p}_2\cdots\mathfrak{p}_e$.

Let

$$\eta_h = \zeta^{g^h} + \zeta^{g^{e+h}} + \zeta^{g^{2e+h}} + \cdots + \zeta^{g^{(f-1)e+h}} \tag{1}$$

---

* Presented to the Society, October 25, 1924. The author wishes to acknowledge his indebtedness to Professor G. E. Wahlin for helpful criticisms and suggestions in the preparation of the manuscript.

† Comptes Rendus, vol. 90 (1880), pp. 287-9.

‡ Comptes Rendus, vol. 90 (1880), pp. 526-8.

§ Journal für Mathematik, vol. 30 (1846), pp. 107-116.

|| Report of British Association, 1860, p. 128, footnote.

¶ Bulletin des Sciences Mathématiques, ser. 2, vol. 33, p. 54.

** Journal für Mathematik, vol. 53 (1857), p. 143.

be a Gaussian period of f generators; η_h will be a root of an equation $P(x) = 0$ with rational integral coefficients of degree e. The pth power of η_h will satisfy the congruence

$$\eta_h^p \equiv \zeta^{pg^h} + \zeta^{pg^{e+h}} + \zeta^{pg^{2e+h}} + \cdots + \zeta^{pg^{(f-1)e+h}} \pmod{p}. \tag{2}$$

Now g is a primitive root of the congruence

$$g^{q-1} \equiv 1 \pmod{q} \tag{3}$$

and the integers $g^1, g^2, g^3, \cdots, g^{q-1}$ form a reduced residue system of incongruent integers, modulo q, where we mean by such a system all the integers of a complete residue system, modulo q, which are prime to q. Every integer that is not divisible by q is congruent to one and only one of these powers of g, mod q, and since p is not equal to q we have $p \equiv g^t$, mod q, where t is an integer of the set $1, 2, 3, \cdots, q-1$. Furthermore t must be a multiple of e, since p appertains to the exponent f and g to the exponent $q-1$, mod q, and raising both sides of the last congruence to the power f we get on comparison the two resulting relations $g^{t \cdot f} \equiv g^{e \cdot f}$, mod q, which is possible when and only when $t \cdot f \equiv e \cdot f$, mod $q-1$. Whence, since $q-1 = e \cdot f$, we conclude $t \equiv 0$, mod e. Therefore we can write $p \equiv g^{s \cdot e}$, mod q. Multiplying both sides of this congruence by $g^{k \cdot e+h}$, we have

$$p \cdot g^{k \cdot e+h} \equiv g^{(k+s)e+h} \pmod{q}. \tag{4}$$

Now $(k+s)e+h \equiv r \cdot e+h$, mod $q-1$, and since g is a primitive number,

$$g^{(k+s)e+h} \equiv g^{r \cdot e+h} \pmod{q}. \tag{5}$$

Here $r < f$ and $r \cdot e+h$ will appear somewhere among the integers $0, 1, 2, \cdots, q-2$. Then combining (4) and (5) we have

$$p \cdot g^{k \cdot e+h} \equiv g^{r \cdot e+h} \pmod{q}. \tag{6}$$

Let k run over the set of integers $0, 1, 2, \cdots, f-1$; then r will also run over the same set of integers, since r is less than f. As k varies over this set, r will vary over the same set in a different order and no two distinct values of k will give the same r; for suppose we could have, say,

$$p \cdot g^{k_1 \cdot e+h} \equiv g^{r_1 \cdot e+h} \pmod{q},$$

and

$$p \cdot g^{k_2 \cdot e+h} \equiv g^{r_1 \cdot e+h} \pmod{q}.$$

Then we must have

$$p \cdot g^{k_1 \cdot e+h} \equiv p \cdot g^{k_2 \cdot e+h} \pmod{q}.$$

We may divide out p, since p and q are by hypothesis relatively prime; hence we have $g^{k_1 \cdot e+h} \equiv g^{k_2 \cdot e+h}$, mod q. From this it follows that $k_1 \equiv k_2$, mod f, which since k_1 and k_2 are both less than f is possible only when $k_1 = k_2$. Then each power of the set $0 \cdot e+h$, $1 \cdot e+h$, $2 \cdot e+h$, $\cdots$, $(f-1)e+h$ will appear once and only once in the resulting system of exponents reduced mod $q-1$. Hence if we apply this reduction to each of the powers of the ζ's in (2) they will each go over into some one of the powers of the ζ's appearing in the period η_h and no two will be repeated. Hence we have exactly

$$\eta_h^p \equiv \zeta^{g^h} + \zeta^{g^{e+h}} + \zeta^{g^{2e+h}} + \cdots + \zeta^{g^{(f-1)e+h}} \pmod{p} \tag{7}$$

or

$$\eta_h^p \equiv \eta_h \pmod{p}. \tag{8}$$

Now $\mathfrak{p}_i$ is an ideal factor of p in $k(\zeta)$; hence in $k(\zeta)$ we have

$$\eta_h^p \equiv \eta_h \pmod{\mathfrak{p}_i}.$$

Also η_h is a generating number of $k(\eta)$; hence $\mathfrak{p}_i$ will be of the first degree in $k(\eta)$. Therefore p will be in $k(\eta)$ the product of e prime ideals each of the first degree, since the subscript i may run over the set of integers 1, 2, 3, $\cdots$, e. Hence we have the following

THEOREM I. *If p is a rational prime different from the rational prime q and appertaining to the exponent f, modulo q, and $q-1 = e \cdot f$, then in $k(\eta)$, the domain generated by η_h, a root of the Gauss period equation of degree e, p is the product of e prime ideals each of the first degree.*

We now take up the application of the preceding results to investigate some of the properties of the prime divisors of the general cyclotomic period function, ascertaining a means of distinguishing the divisors from the non-divisors.

Consider, as before, q any odd rational prime and let $\eta_0, \eta_1, \cdots, \eta_{e-1}$ be the e periods of order $f = (q-1)/e$ of the primitive qth roots of unity. The domain $k(\zeta)$ is an abelian domain and hence the sub-domain $k(\eta)$ is also an abelian domain, since every sub-domain of a cyclotomic domain is a cyclotomic domain and every cyclotomic domain is an abelian domain. Let x take on an integral value "a" and suppose $P(a)$ to be factored into its rational prime factors as follows: $P(a) = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$. Suppose p_i

is any one of these rational prime divisors of $P(a)$; then we have $P(a) \equiv 0$, $\mathrm{mod}\, p_i$. Hence $P(x) \equiv 0$, $\mathrm{mod}\, p_i$, has a solution in $k(1)$, and we write

$$P(x) \equiv (x-a)\cdot Q(x) \qquad (\mathrm{mod}\, p_i). \tag{9}$$

E. Netto* has shown that the essential divisor of the discriminant of the field defined by one of the e periods of the primitive qth roots of unity, q a prime, is q^{e-1}. Now we consider p_i as different from q and also not an unessential discriminantal divisor; therefore p_i cannot contain a power of a prime ideal in $k(\eta)$ as a factor. Now from (9) we see that p_i must have a prime ideal factor $\mathfrak{p}$ of the first degree in $k(\eta)$, since p_i is not an unessential discriminantal divisor. Then for every integer α of the domain, $\alpha^{p_i} \equiv \alpha$, $\mathrm{mod}\, \mathfrak{p}$. The domain $k(\eta)$ is an abelian domain; let G be the group of the domain. If we apply a substitution of G, $\mathfrak{p}$ will go over into $\mathfrak{p}'$, and α into α'. Hence we will have the relation $\alpha'^{p_i} \equiv \alpha'$, $\mathrm{mod}\, \mathfrak{p}'$, since if $\alpha^{p_i-1} - 1$ is a number of $\mathfrak{p}$, after the substitution is applied $\alpha'^{p_i-1} - 1$ will be a number of $\mathfrak{p}'$. This will be true for every integer of the domain, since α represented any integer of the domain; hence $\mathfrak{p}'$ is a prime ideal factor of p_i of the first degree. Now we can apply each of the e substitutions of G, and since p_i cannot contain a power of a prime ideal the resulting ideal factors will all be different from each other and each of the first degree. Then p_i will be the product of e prime ideals all of the first degree in $k(\eta)$.

Now in passing to the higher domain $k(\zeta)$, p_i will be the product of e or more ideals each of degree not greater than f, since some of the prime ideal factors of p_i in $k(\eta)$ may break up into further factors when we pass to $k(\zeta)$ or they may maintain their prime character and increase their degree. Such degree will not exceed f, since the sum of the degrees of the factors will not exceed the degree of the field. The necessary and sufficient condition that p_i resolve into factors of degree f in $k(\zeta)$ is that p_i appertain to f, modulo q. But the degree of no one of the ideal factors of p_i in $k(\zeta)$ can exceed f, hence p_i cannot appertain to an exponent greater than f. If p_i appertain to an exponent less than f, we shall show that such exponent must be a factor of f and hence of $(q-1)/e$. Let $\bar{e}$ be the number of factors into which p is decomposed when we pass to $k(\zeta)$ and $\bar{f}$ the degree of each factor. Then we have $\bar{e}\cdot\bar{f} = q-1 = e\cdot f$. Now since $\bar{e}$ is the number of factors, if we suppose that each $\mathfrak{p}$ is split up into σ factors when passing to $k(\zeta)$ we have $\bar{e} = e\sigma$, whence $e\sigma\bar{f} = e\cdot f$, or $\sigma\bar{f} = f$. That is, $\bar{f}$ is a factor of f. Hence it follows in any case that $p_i^{\bar{f}} \equiv 1$, $\mathrm{mod}\, q$. We now have

* Mathematische Annalen, vol. 24 (1884), p. 579.

THEOREM II. *Let* $P(x) = 0$ *be the equation which has as its roots the* e *periods* $\eta_0, \eta_1, \cdots, \eta_{e-1}$ *of order* f *of the primitive* q*th roots of unity, where* q *is a prime, and let "*a*" be an integral value of* x *such that* $P(a) = p_1^{e_1} \cdot p_2^{e_2} \cdots p_i^{e_i} \cdots p_k^{e_k}$, *where* $p_i (i = 1, 2, 3, \cdots, k)$ *is a rational prime which is not a divisor of the discriminant of* $P(x) = 0$; *then* p_i *must satisfy the congruence* $p_i^{(q-1)/e} \equiv 1, \bmod q$.

Conversely, we have, from Theorem I, if p_i appertains to an exponent $(q-1)/e$, then p_i will be in $k(\eta)$ the product of e prime ideals each of the first degree, and therefore the congruence $P(x) \equiv 0, \bmod p_i$, has e solutions in $k(1)$ so that there must exist at least e values of "a" such that p_i will be found somewhere among the divisors of $P(x)$.

If p_i appertains to an exponent which is a factor of f, say to $\bar{f}$, then $\bar{e}$ will be a multiple of e. Form the period

$$\bar{\eta}_h = \zeta^{g^h} + \zeta^{g^{\bar{e}+h}} + \zeta^{g^{2\bar{e}+h}} + \cdots + \zeta^{g^{(\bar{f}-1)e+h}}.$$

Let $\bar{e} = c \cdot e$; then c must be a factor of f. Then if we form the e periods, each one of these will be the sum of c $\bar{e}$ periods, hence the field $k(\eta)$ is a sub-field of $k(\bar{\eta})$. In the field $k(\bar{\eta})$ we have, from Theorem I, p_i the product of $\bar{e}$ prime ideals each of the first degree, so that, in passing to the sub-field $k(\eta)$, p_i will be the product of e prime ideals each of the first degree, because if the divisors of p_i are of the first degree in a field the divisors in a sub-field are necessarily of the first degree. In this case the congruence $P(x) \equiv 0$ will have e integral solutions and p_i will be found among the divisors of $P(x)$.

We may then classify all primes as to their character as divisors or non-divisors of the general cyclotomic function for the e periods of the primitive qth roots of unity. Those primes which belong to an exponent greater than $f = (q-1)/e$, except the primes that are divisors of the discriminant of the equation $P(x) = 0$, and all primes which belong to an exponent less than f but not a factor of f, will not be found as divisors of the function $P(x)$. But those primes which belong to an exponent $(q-1)/e$, or to an exponent which is a factor of $(q-1)/e$, will be found somewhere among the divisors of $P(x)$. We may state this result in the form of a general theorem.

THEOREM III. *A necessary and sufficient condition that* p *shall be a prime divisor of the cyclotomic function* $P(x)$ *is that it satisfy the congruence* $p^{(q-1)/e} \equiv 1, \bmod q$, *except for those primes which are divisors of the discriminant of* $P(x) = 0$.

It is evident from Theorem III that the conjecture of Sylvester is correct, since this is also a necessary and sufficient condition that p be an eth power residue modulo q.

There are certain forms which are associated with the period equations, and which are obtained from the period equations by linear transformation, which possess properties as the above with certain exceptions which are introduced by the transformation and which can be determined. These forms are important from the standpoint of their simplicity and applicability of the results found. Let p be a prime of the form $6 \cdot n + 1$. We can build three periods of the primitive pth roots of unity of order $(p-1)/3$ and the cubic equation having these periods as its roots is found to be*

$$x^3 + x^2 - \frac{p-1}{3} \cdot x - \frac{1}{9}\left(p \cdot a + \frac{p-1}{3}\right) = 0,$$

which by the transformation $y = 3x + 1$ takes the form

$$y^3 - 3py - pA = 0,$$

where $4 \cdot p = A^2 + 27B^2$ and $A \equiv 1, \bmod 3$; $B \equiv 0, \bmod 3$. The prime divisors of this function satisfy the congruence $p_i^{(p-1)/3} \equiv +1, \bmod p_i$, with certain exceptions which are brought in from the transformation that was made upon the period. The discriminant of the transformed cubic is $27(4p^3 + p^2A^2)$ which contains the unessential discriminantal divisor 3^3. The essential divisor of the discriminant is p^2, hence the prime divisors which may occur and yet not satisfy the relation as above given are the discriminantal divisors 3 and p.

If we consider primes of the form $4n + 1$, the quartic having the four periods of order $(p-1)/4$ as its roots is†

$$x^4 + x^3 - 3\left(\frac{p-1}{8}\right) \cdot x^2 - \frac{p(a+1) + \frac{p-1}{2}}{8} \cdot x - \frac{p(a+1)^2 - \left(\frac{p-1}{2}\right)^2}{64} = 0,$$

which by the transformation $y = 4x + 1$ becomes

$$(y^2 - p)^2 - 4p(y + a)^2 = 0.$$

Here we find the unessential discriminantal divisor 2 entering because of the transformation, hence with the exception of the divisors p and 2, all other primes which are not divisors of the discriminant of the field may be classed as divisors or non-divisors of the function $(y^2 - p)^2 - 4p(y + a)^2$ according as they satisfy the congruence $p_i^{(p-1)/4} \equiv 1, \bmod p$, or do not satisfy this relation.

* Gauss, *Disquisitiones Arithmeticae*, Art. 359.

† Bachmann, *Die Lehre von der Kreistheilung*, p. 228.

UNIVERSITY OF ILLINOIS
URBANA, ILL.