ON THE GENERALIZED JACOBI-KUMMER CYCLOTOMIC FUNCTION*

BY

HOWARD H. MITCHELL

1. Introduction

A number of writers have been interested in the properties of the trinomial congruences

$$cx^\lambda + 1 \equiv dy^\lambda, \qquad \text{mod. } q,$$

where q is a prime of the form $\lambda\nu + 1$, and c, d are integers prime to q. The pioneer work in this field was done by Gauss,† who showed that for $\lambda = 3$ the determination of the number of solutions could be made to depend on the representation of $4q$ by the form $A^2 + 27B^2$, and for $\lambda = 4$ on the representation of q by the form $A^2 + B^2$.

For the general value of λ the congruence is intimately related to Jacobi's cyclotomic function,‡

$$\psi_{-a,\,-b}(\alpha) = \sum_h \alpha^{-bh+(a+b)\,\text{ind.}\,(g^h+1)},$$

where α is a primitive λth root of unity, a, b integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod. λ, g a primitive root, mod. q, and where h ranges over the values $0, 1, 2, \cdots, q-2$ with the exception of $(q-1)/2$. This relation has been used by a number of authors in the investigation of the congruences.§

The present writer considers the similar congruences in the Galois field of order q^t, where q is any prime not contained in λ, and t any exponent such that $q^t \equiv 1$, mod. λ. By means of certain relations between the number of solutions of these congruences similar to those used by Gauss in the special cases mentioned above, a more general function than Jacobi's is derived. We obtain this more general function if in Jacobi's function we consider g to be a primitive root in the Galois field of order q^t, and let h range over the values $0, 1, 2, \cdots, q^t - 2$ with the exception of $(q^t - 1)/2$ if q is odd and 0 if $q = 2$.

* Presented to the Society, December 28, 1915.

† *Disquisitiones Arithmeticæ*, § 358; *Theoria Residuorum Biquadraticorum*, §§ 15–20.

‡ Cf. for example H. Weber, *Algebra* (1898), Bd. I, §§ 177, 178; Bd. II, § 203.

§ Cf. for example Carey, Quarterly Journal of Mathematics, vol. 26 (1893), pp. 322–371; Dickson, Journal für Mathematik, vol. 135 (1908), pp. 181–188; Cornacchia, Giornale di Mathematiche di Battaglini, vol. 47 [(2) 16] (1909), pp. 219–268.

This function is also more general than that considered by Kummer.[*] The latter used the set of residues with respect to a prime ideal factor of q in the algebraic realm $k(\alpha)$. This is a Galois field of order q^{t_1}, where t_1 is the exponent to which q belongs, mod. λ. He also restricted λ to be prime. For this case he determined the prime ideal factors of the function.[§] In a later paper he determined the ideal factors of the Jacobi function for λ composite.[†] The references given later will be exclusively to the first of these two papers.

By an extension of Kummer's work, this determination is obtained in the present paper for the case where λ is composite and where the exponent t has the more general meaning given above. In going over this work of Kummer's in the first paper referred to an error was discovered. The author found it necessary to construct a different argument at this point.

As a result of the determination of the ideal factors of the function a relation between the functions for different Galois fields is found. It is shown that if the primitive roots in the two fields are properly related,

$$\Psi_{-a,\,-b}(\alpha) = (-1)^{s-1}\psi^{s}_{-a,\,-b}(\alpha),$$

where ψ denotes the function for the field of order q^{t_1}, and Ψ the function for the field of order q^t, and where $s = t/t_1$.

A result of Kummer's is extended by showing that if q belongs to an even exponent, $2t_1$, mod. λ, and if $q^{t_1} \equiv -1$, mod. λ, then

$$\Psi_{-a,\,-b}(\alpha) = (-1)^{s-1} q^{t},$$

where, as before, $s = t/t_1$.

The writing of this paper was undertaken at the suggestion of Mr. H. S. Vandiver, and his interest and advice have been of great value to the author.

2. Derivation of the function $\Psi(\alpha)$

We consider the Galois field of order q^t, where q is any prime, and where $q^t - 1 = \lambda\nu$. We suppose the marks of the field other than 0 represented as powers of a primitive root and denote by σ_i any mark whose index is congruent to i, mod. λ. We denote with Kummer the number of solutions of the congruence $1 + \sigma_i \equiv \sigma_j$ by

$$\overset{j}{m}_{i}$$

[*] *Ueber die Ergänzungsätze den allgemeinen Reciprocitätsgesetzen,* Journal für Mathematik, vol. 44 (1851).

[§] For a corresponding generalization of the Lagrange resolvent function cf. Stickelberger, Mathematische Annalen, vol. 37 (1890), pp. 321–367. He assumes λ to be composite.

[†] *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist,* Abhandlungen der Koeniglichen Academie der Wissenschaften zu Berlin, 1856.

in formulas, but by m_i^j in the text. We represent also the residue ind. (-1), mod. λ, by ϵ, so that if q is odd, $\epsilon \equiv 0, \lambda/2$ according as ν is even or odd, whereas if $q = 2$, $\epsilon \equiv 0$.

Proceeding by the method used by Gauss and also by a number of other authors, we obtain the following relations connecting the quantities m_i^j:

$$(1)\qquad \overset{j}{m}_i = \overset{i+\epsilon}{m}_{j+\epsilon} = \overset{i-j}{m}_{-j+\epsilon} = \overset{-j}{m}_{i-j+\epsilon} = \overset{j-i}{m}_{-i} = \overset{-i+\epsilon}{m}_{j-i+\epsilon};$$

$$(2)\qquad \sum_i \overset{0}{m}_i = \nu - 1; \qquad \sum_i \overset{j}{m}_i = \nu;$$

where $i \equiv 0, 1, 2, \cdots, \lambda - 1$; $j \equiv 1, 2, \cdots, \lambda - 1$, mod. λ.

By a method also due to Gauss we may obtain certain quadratic relations connecting the quantities m_i^j. This method consists in equating two expressions for the number of solutions of the congruence $\sigma_j + \sigma_k \equiv \sigma_l + 1$. There are m_i^j marks σ_j for which $\sigma_j \equiv 1 + \sigma_i$, and for each of these there are m_{k-i}^{l-i} pairs of marks σ_k, σ_l for which $\sigma_i + \sigma_k \equiv \sigma_l$. If $j \equiv 0$, $l \equiv k$, mod. λ, there are ν additional solutions, $\sigma_j \equiv 1$, $\sigma_l \equiv \sigma_k$. Hence we have in general

$$\sum_i \overset{j}{m}_i \overset{l-i}{m}_{k-i} = \sum_i \overset{k}{m}_i \overset{l-i}{m}_{j-i},$$

where $i \equiv 0, 1, 2, \cdots, \lambda - 1$, whereas if $j \equiv 0$, $l \equiv k$, mod. λ, we must add ν to the left-hand side of the equation, and if $k \equiv 0$, $l \equiv j$, mod. λ, we must add ν to the right-hand side.

If we multiply this equation by $\alpha^{aj+bk+cl}$, where α is a primitive λth root of unity, and then form the sum for $j, k, l \equiv 0, 1, 2, \cdots, \lambda - 1$, we obtain

$$\sum_{i,j,k,l} \overset{j}{m}_i \overset{l-i}{m}_{k-i} \alpha^{aj+bk+cl} + \nu \sum_k \alpha^{bk+ck} = \sum_{i,j,k,l} \overset{k}{m}_i \overset{l-i}{m}_{j-i} \alpha^{aj+bk+cl} + \nu \sum_j \alpha^{aj+cj}.$$

By replacing on the left $l - i$, $k - i$ by l, k, and on the right $l - i$, $j - i$ by l, j, the resulting equation may be written as follows:

$$(3)\qquad \begin{aligned} &\sum_{i,j} \overset{j}{m}_i \alpha^{aj+(b+c)i} \times \sum_{k,l} \overset{l}{m}_k \alpha^{bk+cl} + \nu \sum_k \alpha^{(b+c)k} \\ &\qquad = \sum_{i,k} \overset{k}{m}_i \alpha^{bk+(a+c)i} \times \sum_{j,l} \overset{l}{m}_j \alpha^{aj+cl} + \nu \sum_j \alpha^{(a+c)j}. \end{aligned}$$

If now we suppose $a + c \equiv 0$, $b + c \not\equiv 0$, mod. λ, the second term on the left vanishes, whereas the second term on the right has the value $\lambda\nu$. If we write, following the notation for the Jacobi function,

$$(4)\qquad \Psi_{-a,\,-b}(\alpha) = \sum_{i,j} \overset{j}{m}_i \alpha^{-bi+(a+b)j},$$

equation (3) takes the form

$$\Psi_{-b,\,b-a}(\alpha)\Psi_{a-b,\,b}(\alpha) = \Psi_{-b,\,0}(\alpha)\Psi_{0,\,a}(\alpha) + \lambda\nu.$$

By use of equations (1) and (2) we find if $a \not\equiv 0$, $b \not\equiv 0$, $a - b \not\equiv 0$, mod. λ,

$$\Psi_{a-b,\, b}(\alpha) = \Psi_{b,\, a-b}(\alpha) = \Psi_{-b,\, b-a}(\alpha^{-1});$$

$$\Psi_{-b,\, 0}(\alpha) = \Psi_{0,\, a}(\alpha) = -1 .$$

Hence by a slight change in notation we have finally

$$\Psi_{-a,\, -b}(\alpha)\Psi_{-a,\, -b}(\alpha^{-1}) = q^t, \tag{5}$$

where now $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod. λ. Another proof of this relation may be given by using Kummer's argument.

The function defined by (4) may also be written

$$\Psi_{-a,\, -b}(\alpha) = \sum_h \alpha^{-bh+(a+b)\,\text{ind.}\,(g^h+1)}, \tag{6}$$

where g is the primitive root referred to above, and $h = 0, 1, 2, \cdots, q^t - 2$ with the exception of $(q^t - 1)/2$ if q is odd and 0 if $q = 2$. For there are m_i^j numbers h which satisfy the two conditions $h \equiv i$, ind. $(g^h + 1) \equiv j$, mod. λ. This is the form in which the function is written by Kummer,* though as pointed out above the function we consider here is more general than his.

The function satisfies essentially the same relations as the Jacobi function. For example, we find from (4) by use of (1)

$$\begin{aligned}(7)\quad \Psi_{--a,\, -b}(\alpha) = \Psi_{-b,\, -a}(\alpha) &= (-1)^{q\nu a}\,\Psi_{-a,\, a+b}(\alpha) \\ &= (-1)^{q\nu a}\,\Psi_{a+b,\, -a}(\alpha) = (-1)^{q\nu b}\,\Psi_{-b,\, a+b}(\alpha) \\ &= (-1)^{q\nu b}\,\Psi_{a+b,\, --b}(\alpha),\end{aligned}$$

where we have put $\alpha_{,}^{e} = (-1)^{q\nu}$, since it has the value $+1$ unless q and ν are both odd.

Also if in equation (3) we assume that $b + c \not\equiv 0$, $a + c \not\equiv 0$, mod. λ, we have

$$\Psi_{-a-b-c,\, b+c}(\alpha)\Psi_{-b-c,\, b}(\alpha) = \Psi_{-a-b-c,\, a+c}(\alpha)\Psi_{-a-c,\, a}(\alpha),$$

or by using one of the equations (7),

$$\Psi_{\acute{a},\, b+c}(\alpha)\Psi_{c,\, b}(\alpha) = \Psi_{b,\, a+c}(\alpha)\Psi_{c,\, a}(\alpha). \tag{8}$$

The function also satisfies the relation:

$$\Psi(\alpha^{q^h}) = \Psi(\alpha),\dagger \tag{9}$$

where h is an arbitrary exponent. In particular if t is even and if there exist values of h for which $q^h \equiv -1$, mod. λ, we have

$$\Psi(\alpha^{-1}) = \Psi(\alpha),$$

* L. c.

† Cf. Kummer, l. c. The subscripts will be omitted from now on.

and hence

$$\Psi(\alpha) = \pm q^{t/2}.$$

If λ is the power of a prime ($\lambda > 3$) it may also be shown that

$$(10) \qquad \Psi(\alpha) \equiv -1, \qquad \text{mod. } (1-\alpha)^3.\text{*}$$

3. Determination of the ideal factors of $\Psi(\alpha)$

Kummer has determined the ideal factors of $\Psi(\alpha)$ tor the case where λ is prime and where the field of residues is that determined by a prime ideal factor of q in the realm $k(\alpha)$. By an extension of his metbod we will determine the ideal factors in the case where λ is composite and the field of residues is the Galois field of order q^t, t being any exponent for which $q^t \equiv 1$, mod. λ.

In $k(\alpha)$, q is the product of $\phi(\lambda)/t_1$ different ideal prime factors, where t_1 is the exponent to which q belongs, mod. λ. We will construct an algebraic field of degree $\phi(\lambda)s$, where $s = t/t_1$, which contains $k(\alpha)$ as a subfield and in which the prime ideal factors of q are the same as in the field $k(\alpha)$. The λth roots of unity with q as modulus determine a Galois field of order q^{t_1}. There exist congruences of degree s with coefficients in this field and which are irreducible in the field. Such a congruence determines a Galois field of order q^t.

There must therefore exist equations of degree s with coefficients in $k(\alpha)$, which are irreducible both as equations and when regarded as congruences, mod. q. We consider a particular equation of this sort and let β denote one of its roots. The realm $k(\alpha, \beta)$ is then of degree $\phi(\lambda)s$ and a residue system with respect to a prime ideal factor of q in this realm is the Galois field of order q^t. The number of ideal factors of q in this realm is thus $\phi(\lambda)s/t = \phi(\lambda)/t_1$, i. e., the same as in the realm $k(\alpha)$.

We now suppose that g represents an integer in the realm $k(\alpha, \beta)$ which is a primitive root with respect to $\mathfrak{q}(\alpha)$, a prime ideal factor of q, and which satisfies the congruence

$$g^{\nu} \equiv \alpha, \qquad \text{mod. } \mathfrak{q}(\alpha),$$

where $\nu = (q^t - 1)/\lambda$. It follows then by Kummer's† method that

$$g^{\nu q^t} \equiv \alpha, \qquad \text{mod. } \mathfrak{q}(\alpha)^{t+1}.$$

A change in Kummer's work is necessary here, since for λ composite we cannot assume the existence of a primitive root γ with respect to λ. Instead it will be found sufficient to employ the least positive residue $|m|$ of m, mod. λ. If then in the expression (6) for $\Psi(\alpha)$ we replace α by α^i, where i is any residue prime to λ, we obtain

* Cf. Schwering, Journal für Mathematik, vol. 93 (1882), pp. 334–337; Kronecker, ibid., vol. 93 (1882), pp. 338–364.

† L. c. We put $n = 1$ in Kummer's work.

$$\Psi(\alpha^i) = \sum_h \alpha^{-|bi|h + |(a+b)i| \operatorname{ind.}(g^h+1)},$$

where we have replaced his γ_{-i} by $|(a+b)i|$, $\gamma_{\rho-i}$ by $|bi|$.

Proceeding then by his method we finally obtain the congruence

$$(11) \quad \Psi(\alpha) \equiv \sum_z \frac{(q^t-1)\prod(|(a+b)i|\nu q^t)}{\prod(|ai|\nu q^t + \lambda\nu z)\prod(|bi|\nu q^t - \lambda\nu z)}, \qquad \text{mod. } \mathfrak{q}_i^{t+1},$$

where we have put $\mathfrak{q}_i = \mathfrak{q}(\alpha^{i'})$, $ii' \equiv 1$, mod. λ, $\prod(m) = 1 \cdot 2 \cdots m$, where the summation is to be taken over all rational integral values of z for which neither $|ai|q^t + \lambda z$ nor $|bi|q^t - \lambda z$ is negative, and where it is assumed that $|ai| + |bi| = |(a+b)i|$. This restriction will be removed later.

Since $\Psi(\alpha)$ cannot be divisible by a higher power of $\mathfrak{q}_i$ than the tth, the problem is now reduced to finding how many times the sum of binomial coefficients on the right side of this congruence contains the factor q. Kummer next attempts to show that the term in the sum corresponding to the value $z = 0$ is divisible by a lower power of q than any other, and hence that $\Psi(\alpha)$ contains the factor $\mathfrak{q}_i$ just as often as this term contains the factor q. An error occurs in this portion of the proof, although the result is correct.

He first observes that if A is any positive integer such that

$$A = a_0 + a_1 q + a_2 q^2 + \cdots + a_{k-1} q^{k-1},$$

where each $a_i = 0, 1, 2, \cdots, q-1$, then the number of factors q contained in $\prod(A)$ is

$$(12) \qquad \frac{A - (a_0 + a_1 + \cdots + a_{k-1})}{q-1}.$$

If similarly

$$B = b_0 + b_1 q + b_2 q^2 + \cdots + b_{k-1} q^{k-1},$$

$$A + B = c_0 + c_1 q + c_2 q^2 + \cdots + c_{k-1} q^{k-1} + \epsilon_{k-1} q^k,$$

where $0 \leqq b_i < q$, $0 \leqq c_i < q$, and where

$$(13) \qquad \begin{aligned} a_0 + b_0 &= \epsilon_0 q + c_0, \\ \epsilon_0 + a_1 + b_1 &= \epsilon_1 q + c_1, \\ \epsilon_1 + a_2 + b_2 &= \epsilon_2 q + c_2, \\ &\cdots\cdots\cdots \\ \epsilon_{k-2} + a_{k-1} + b_{k-1} &= \epsilon_{k-1} q + c_{k-1}, \end{aligned}$$

he shows that the number N of factors q contained in the binomial coefficient

$$\frac{\prod(A+B)}{\prod(A)\prod(B)}$$

is given by the formula

$$N = \epsilon_0 + \epsilon_1 + \epsilon_2 + \cdots + \epsilon_{k-1}. \tag{14}$$

Applying this result to the coefficients in the congruence (11), he observes that for any value of z he has $c_0 = c_1 = c_2 = \cdots = c_{t-1} = 0$. For $z = 0$ he has also $a_0 = a_1 = a_2 = \cdots = a_{t-1} = 0$, $b_0 = b_1 = b_2 = \cdots = b_{t-1} = 0$, and hence $\epsilon_0 = \epsilon_1 = \epsilon_2 = \cdots = \epsilon_{t-1} = 0$. In order that neither A nor B shall be negative he concludes that z is numerically less than q^t, and hence that the term for $z = 0$ is the only one in which A and B are divisible by q^t. Consequently for any other value of z one or more of these ϵ's must have the value 1.

Kummer argues erroneously that the values of the remaining ϵ's, ϵ_t, ϵ_{t+1}, $\cdots$, ϵ_{k-1} cannot be diminished if instead of $z = 0$ we substitute some other value of z, in fact that only ϵ_t is in any way affected by the values of the preceding ϵ's. The point at which the error occurs is where he says (p. 117, l. 5): "Auch werden durch diese Bestimmungen die Werthe der übrigen Zahlen ϵ_{nt}, ϵ_{nt+1}, $\cdots$, ϵ_{k-1} im allgemeinen gar nicht verändert, etc."

That this is not the case may be seen from the particular example in which $q = 11$, $t = 3$, $\lambda = 7$, $|ai| = 3$, $|bi| = 3$. For $z = 0$ we obtain ϵ_0, ϵ_1, $\epsilon_2 = 0, 0, 0$ and ϵ_3, ϵ_4, $\epsilon_5 = 1, 1, 0$, whereas for $z = 55$ the first set of ϵ's are $0, 1, 1$ and the second set $1, 0, 0$.

We can however show that the sum of all the ϵ's is increased when z is replaced by a value different from 0. Let $z = \pm q^e z'$, where z' is positive and prime to q. Then if we suppose that B is the number which is *decreased* when we take a value ot z different from 0, we may write, since $\lambda\nu = q^t - 1$,

$$A(z) \equiv -q^e z' + a_t q^t + a_{t+1} q^{t+1} + \cdots + a_{t+e-1} q^{t+e-1}, \qquad \text{mod. } q^{t+e},$$

$$B(z) \equiv q^e z' + b_t q^t + b_{t+1} q^{t+1} + \cdots + b_{t+e-1} q^{t+e-1}, \qquad \text{mod. } q^{t+e},$$

where the a's and the b's denote the coefficients of the corresponding powers of q for $z = 0$.

Since $q^e z' < q^t$, by writing z' in terms of powers ot q we may give $B(z)$ the desired form and the coefficients of q^t, q^{t+1}, $\cdots$, q^{t+e-1} will still be b_t, b_{t+1}, $\cdots$, b_{t+e-1}. We may write $A(z)$ in the desired form by expressing $q^t - q^e z'$ in terms of powers of q and changing one or more of the a's as follows. If $a_t \mp 0$, we replace a_t by $a_t - 1$. If $a_{t+\mu}$ is the first a which is not 0, we may, if $0 < \mu < e$, replace $a_{t+\mu}$ by $a_{t+\mu} - 1$, and write the coefficients of q^t, q^{t+1}, $\cdots$, $q^{t+\mu-1}$ each as $q - 1$. If $\mu \geqq e$, we may write the coefficients of q^t, q^{t+1}, $\cdots$, q^{t+e-1} each as $q - 1$.

From equations (13) it follows that ϵ_e, ϵ_{e+1}, $\cdots$, ϵ_{t-1} must now each have the value 1. If $a_t \mp 0$, we conclude that ϵ_t, ϵ_{t+1}, $\cdots$, ϵ_{t+e-1} are unaltered. If $0 < \mu < e$, each of the ϵ's, ϵ_t, ϵ_{t+1}, $\cdots$, $\epsilon_{t+\mu-1}$ will be changed from 0 to 1, and $\epsilon_{t+\mu}$, $\epsilon_{t+\mu+1}$, $\cdots$, ϵ_{t+e-1} will be unaltered. If $\mu \geqq e$, each of the ϵ's, ϵ_t,

$\epsilon_{t+1}, \cdots, \epsilon_{t+e-1}$ will be changed from 0 to 1. Hence in any case none of the ϵ's which precede ϵ_{t+e} can be diminished, whereas at least $t - e$ of them must be increased.

Since $A + B < q^{2t}$, ϵ_{2t-1} must be 0 for all values of z, and hence the only ϵ's which may be diminished are $\epsilon_{t+e}, \epsilon_{t+e+1}, \cdots, \epsilon_{2t-2}$. Since there are but $t - e - 1$ of these we conclude that the sum of all the ϵ's must be increased by at least one. Hence the binomial coefficient for $z = 0$ is divisible by a lower power of q than any other, and hence $\Psi(\alpha)$ contains the ideal $\mathfrak{q}_i$ to exactly the same power as this particular term contains the factor q.

To obtain an expression for the number of times this coefficient contains the factor q, we write

$$|ai|\nu q^t = a_t q^t + a_{t+1} q^{t+1} + \cdots + a_{2t-1} q^{2t-1},$$

where $0 \leqq a_i < q$. By Kummer's method we obtain the following set of equations:

$$|aiq^{t-j}| + \lambda a_{t+j} = |aiq^{t-j-1}|q \quad (j = 0, 1, 2, \cdots, t-1),$$

or

$$|aiq^{t-j}| + \lambda a_{t+j} \equiv 0, \qquad \text{mod. } q. \tag{15}$$

Similarly we have

$$|biq^{t-j}| + \lambda b_{t+j} \equiv 0, \qquad \text{mod. } q,$$

$$|(a+b)iq^{t-j}| + \lambda c_{t+j} \equiv 0,$$

from which we obtain, by use of (13),

$$|aiq^{t-j}| + |biq^{t-j}| - |(a+b)iq^{t-j}| \equiv \epsilon_{t+j-1}\lambda, \qquad \text{mod. } q. \tag{16}$$

From this we conclude that $\epsilon_{t+j-1} = 1, 0$ according as $|aiq^{t-j}| + |biq^{t-j}| \gtrless \lambda$.

We therefore conclude that the number of times the factor q is contained in the binomial coefficient for $z = 0$, and hence the number of times the ideal $\mathfrak{q}_i$ is contained in $\Psi(\alpha)$, is equal to the number of the expressions $|aiq^{t-j}| + |biq^{t-j}|$ $(j = 0, 1, 2, \cdots, t-1)$, whose values exceed λ. Kummer gives the criterion in a somewhat different form.

The above argument is restricted to values of i for wbich

$$|ai| + |bi| = |(a+b)i|,$$

i. e., $|ai| + |bi| < \lambda$. By Kummer's method this restriction may be removed. If $|ai| + |bi| > \lambda$, then $|a(-i)| + |b(-i)| < \lambda$, and hence the ideal $\mathfrak{q}_{-i}$ is one tor which the criterion is true. If we denote by m_i the number of times $\mathfrak{q}_i$ is contained in $\Psi(\alpha)$, it follows that $\mathfrak{q}_i$ will be contained m_{-i} times in $\Psi(\alpha^{-1})$. Since $\Psi(\alpha)\Psi(\alpha^{-1}) = q^t$, we have $m_i + m_{-i} = t$. Since m_{-i} is equal to the number of the t sums $|a(-i)q^{t-j}| + |b(-i)q^{t-j}|$, whose values exceed λ, m_i must then be equal to the number of these sums whose values are less than λ, or what is the same thing, the number of the sums $|aiq^{t-j}| + |biq^{t-j}|$, whose values exceed λ. The criterion is therefore valid for every ideal factor of q.

In applying the criterion it should be noticed that

$$\mathfrak{q}_i(\alpha) = \mathfrak{q}_i(\alpha^q) = \mathfrak{q}_i(\alpha^{q^2}) = \cdots,$$

so that i need only be assigned $\phi(\lambda)/t_1$ values, such that the quotient of no two of them is congruent, mod. λ, to a power of q, where as above t_1 denotes the exponent to which q belongs, mod. λ. We may therefore state the

THEOREM. *If $g^\nu \equiv \alpha$, mod. $\mathfrak{q}$, then the number of times the ideal $\mathfrak{q}_i$ is contained in $\Psi(\alpha)$ is equal to the number of the expressions $|aiq^{t-j}| + |biq^{t-j}|$ $(j = 0, 1, 2, \cdots, t-1)$, whose values exceed λ, where i assumes $\phi(\lambda)/t_1$ values prime to λ such that the quotient of no two of them is congruent, mod. λ, to a power of q.*[*]

For example, if $q = 11$, $\lambda = 15$, $t = 2$, there are four different prime ideal factors of 11, which may be written $\mathfrak{q}(\alpha)$, $\mathfrak{q}(\alpha^2)$, $\mathfrak{q}(\alpha^4)$, $\mathfrak{q}(\alpha^8)$. These may be taken to be the principal ideals $(2 + \alpha^3)$, $(2 + \alpha^6)$, $(2 + \alpha^{12})$, $(2 + \alpha^9)$. If $a \equiv 3$, $b \equiv 5$, mod. 15, and if the primitive root g satisfies the condition $g^8 \equiv \alpha$, mod. $(2 + \alpha^3)$, we have

$$\begin{array}{rl}
|3| + |5| < 15, & |3 \cdot 11| + |5 \cdot 11| < 15, \\
|3 \cdot 8| + |5 \cdot 8| > 15, & |3 \cdot 8 \cdot 11| + |5 \cdot 8 \cdot 11| < 15, \\
|3 \cdot 4| + |5 \cdot 4| > 15, & |3 \cdot 4 \cdot 11| + |5 \cdot 4 \cdot 11| > 15, \\
|3 \cdot 2| + |5 \cdot 2| > 15, & |3 \cdot 2 \cdot 11| + |5 \cdot 2 \cdot 11| < 15,
\end{array}$$

from which we conclude that the ideal defined by $\Psi_{-3,-5}(\alpha)$ must be

$$(2 + \alpha^6)(2 + \alpha^{12})^2(2 + \alpha^9).$$

We find that a primitive root satisfying the above condition is $g = 5\alpha + 6$, and by use of this we find that $\Psi_{-3,-5}(\alpha) = -4 - 6\alpha^3 + 6\alpha^6 + 3\alpha^{12}$. We then find directly that the two ideals coincide, in fact that

$$\Psi_{-3,-5}(\alpha) = -\alpha^3(2 + \alpha^6)(2 + \alpha^{12})^2(2 + \alpha^9),$$

where the expressions on the right are now regarded as actual numbers.

As a consequence of the above theorem we may state at once tbe following

THEOREM. *If $\mathfrak{q}$ is any prime ideal factor of q, and m_i denotes the number of the sums $|aiq^{t-j}| + |biq^{t-j}|$ $(j = 0, 1, 2, \cdots, t-1)$, whose value exceeds λ, where a, b are any two integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod. λ, and where i assumes $\phi(\lambda)/t_1$ values prime to λ such that the quotient of no two of them is congruent, mod. λ, to a power of q, then the product, $\prod_i \mathfrak{q}_i^{m_i}$, is a principal ideal.*

[*] Cf. the criterion for the Jacobi function; for example, H. Weber, *Algebra* (1899), Bd. II, § 203 (14). For the generalized Lagrange resolvent see Stickelberger (l. c.), p. 355.

4. A relation between the Ψ-functions

It is clear from the form in which the above criterion is given that the value of m_i for the general value of t is s times what it is for $t = t_1$, where $t = st_1$. Hence if we denote by $\Psi(\alpha)$ the function for the general value of t, and by $\psi(\alpha)$ the function for $t = t_1$, and for the same pair of values of a and b, it follows that

$$\Psi(\alpha) = E(\alpha)\psi^s(\alpha),$$

where $E(\alpha)$ is a unit and where the primitive roots in the two fields satisfy the congruence

$$g^\nu \equiv g_1^{\nu_1}, \qquad \text{mod. } \mathfrak{q}.$$

We have also

$$\Psi(\alpha^{-1}) = E(\alpha^{-1})\psi^s(\alpha^{-1}),$$

and hence by forming tbe product $E(\alpha)E(\alpha^{-1}) = 1$. It follows from this that $E(\alpha) = \pm\alpha^e$.*

We will show that $E(\alpha) = (-1)^{s-1}$, and to do this we will first show that

$$\Psi(\alpha) \equiv (-1)^{s-1}\psi^s(\alpha), \qquad \text{mod. } \mathfrak{q}_i^{sm_i+1},$$

provided i has any value for which $|ai| + |bi| < \lambda$, and where m_i denotes the number of times $\mathfrak{q}_i$ is contained in $\psi(\alpha)$.

In the case of the function $\Psi(\alpha)$ the binomial coefficient in the congruence (11) which corresponds to the value $z = 0$ is divisible by q^{sm_i}, and every other coefficient is divisible by a higher power of q. Since

$$t + 1 = st_1 + 1 \geqq sm_i + 1,$$

we conclude that

$$\Psi(\alpha) \equiv \frac{-\prod(|(a+b)i|\nu q^t)}{\prod(|ai|\nu q^t)\prod(|bi|\nu q^t)}, \qquad \text{mod. } \mathfrak{q}_i^{sm_i+1}. \tag{17}$$

In the case of $\psi(\alpha)$ we find

$$\psi^s(\alpha) \equiv \frac{(-1)^s\prod^s(|(a+b)i|\nu_1 q^{t_1})}{\prod^s(|ai|\nu_1 q^{t_1})\prod^s(|bi|\nu_1 q^{t_1})}, \qquad \text{mod. } \mathfrak{q}_i^{sm_i+1}.$$

Since each of these two expressions is divisible by q^{sm_i}, we need only consider their residues, mod. q, after the powers of q have been removed.

If, as above, we write

$$A = a_0 + a_1 q + a_2 q^2 + \cdots + a_{k-1} q^{k-1},$$

where $0 \leqq a_i < q$, we find that the product of all the numbers in the set $1, 2, \cdots, A$, which are prime to q, is congruent, mod. q, to

$$\prod(a_0)(-1)^{a_1 + a_2 q + a_3 q^2 + \cdots + a_{k-1} q^{k-2}},$$

* Kronecker, Journal für Mathematik, vol. 53 (1857), p. 176.

where we have used Wilson's Theorem. The product of all the numbers in the set $1, 2, \cdots, A$, which are each divisible by exactly one factor q, divided by the power of q which this product contains, is congruent, mod. q, to

$$\prod(a_1)(-1)^{a_2+a_3q+\dots+a_{k-1}q^{k-3}}.$$

Proceeding in this way we find that after all the factors q have been removed from $\prod(A)$, the result is congruent, mod. q, to

$$\prod(a_0)\prod(a_1)\cdots\prod(a_{k-1})(-1)^N,\text{*}$$

where

$$N = \frac{A-(a_0+a_1+\cdots+a_{k-1})}{q-1},$$

i. e., the number of times q is originally contained in $\prod(A)$.

From this we conclude that

$$\Psi(\alpha) \equiv \frac{\prod(c_t)\prod(c_{t+1})\cdots\prod(c_{2t-1})}{\prod(a_t)\cdots\prod(a_{2t-1})\prod(b_t)\cdots(b_{2t-1})}(-1)^{sm_i+1}q^{sm_i}, \tag{18}$$
$$\text{mod. } \mathfrak{q}_i^{sm_i+1},$$

where, as previously, the a's, b's, and c's represent the coefficients of $|ai|\nu q^t$, $|bi|\nu q^t$, and $|(a+b)i|\nu q^t$, when expressed in terms of powers of q. A similar congruence is obtained for $\psi^s(\alpha)$, where t is to be replaced by t_1, each factorial is to be raised to the power s, and the exponent of -1 is to be replaced by $sm_i + s$.

If we write

$$|ai|\nu_1 q^{t_1} = a_{t_1}q^{t_1} + a_{t_1+1}q^{t_1+1} + \cdots + a_{2t_1-1}q^{2t_1-1},$$

then by means of the expressions for ν and ν_1 we obtain

$$|ai|\nu q^t = (a_{t_1}q^t + a_{t_1+1}q^{t+1} + \cdots$$
$$+ a_{2t_1-1}q^{t+t_1-1})(1 + q^{t_1} + q^{2t_1} + \cdots + q^{(s-1)t_1}),$$

from which it is clear that in the expression for $|ai|\nu q^t$ each a_i will appear s times as often as in that for $|ai|\nu_1 q^{t_1}$. A similar relation holds for the other numbers. We therefore conclude that

$$\Psi(\alpha) \equiv (-1)^{s-1}\psi^s(\alpha), \qquad \text{mod. } \mathfrak{q}_i^{sm_i+1}.$$

Since we have found that

$$\Psi(\alpha) = \pm\alpha^e\psi^s(\alpha),$$

we obtain

$$\pm\alpha^e \equiv (-1)^{s-1}, \qquad \text{mod. } \mathfrak{q}_i.$$

* Cf. Stickelberger, l. c., p. 343.

If $\alpha^e \neq \pm 1$, $1 \pm \alpha^e$ is either a unit or a factor of λ, and hence prime to $\mathfrak{q}_i$. We therefore conclude that, if q is odd,

$$\Psi(\alpha) = (-1)^{s-1} \psi^s(\alpha), \tag{19}$$

whereas, if $q = 2$,

$$\Psi(\alpha) = \pm \psi^s(\alpha).$$

By a special method we may show that the sign is the same for $q = 2$. If λ is the power of a prime,

$$\Psi(\alpha) \equiv \psi(\alpha) \equiv -1, \qquad \text{mod. } (1 - \alpha),$$

so that the sign must be $(-1)^{s-1}$ in this case.

We now proceed by induction and assume that (19) holds in all cases where λ is the product of n primes (not necessarily all different). If then the equation

$$\Psi(\alpha) = (-1)^s \psi^s(\alpha)$$

holds in case λ is the product of $n + 1$ primes, and if μ is any prime factor of λ (and therefore odd), we have

$$\Psi^\mu(\alpha) = (-1)^s \psi^{s\mu}(\alpha),$$

whence

$$\Psi(\alpha^\mu) \equiv (-1)^s \psi^s(\alpha^\mu), \qquad \text{mod. } \mu.$$

This is however impossible* in view of our assumption, since α^μ is a λ/μth root of unity, and λ/μ is the product of only n primes. Hence equation (19) must hold for any λ and is therefore true for $q = 2$ as well as when q is odd.

We have therefore the

THEOREM. *If $\Psi(\alpha)$ and $\psi(\alpha)$ are two functions for the same values of a and b in the Galois fields of order q^t and q^{t_1} respectively, and if the primitive roots in those two fields are so chosen that $g^\nu \equiv g_1^{\nu_1}$ in the field, then*

$$\Psi(\alpha) = (-1)^{s-1} \psi^s(\alpha),$$

where $s = t/t_1$.

5. Determination of $\Psi(\alpha)$ for a special type of field

If q belongs to an even exponent, say $2t$, mod. λ, and if $q^t \equiv -1$, mod. λ, then, as we have seen (from (9)),

$$\psi(\alpha) = \pm q^t.$$

By methods similar to those employed above we may determine the ambiguous sign. If i has a value for which $|ai| + |bi| < \lambda$, we conclude from (18) that

$$\psi(\alpha) \equiv \frac{\prod(c_{2t}) \prod(c_{2t+1}) \cdots \prod(c_{4t-1})}{\prod(a_{2t}) \cdots \prod(a_{4t-1}) \prod(b_{2t}) \cdots \prod(b_{4t-1})} (-1)^{t+1} q^t, \quad \text{mod: } \mathfrak{q}_i^{t+1}.$$

* The same is true if one of the three congruences $\mu a \equiv 0$, $\mu b \equiv 0$, $\mu(a + b) \equiv 0$, mod. λ, is satisfied, since in that case both functions have the value -1.

From (15)

$$|aiq^{2t-j}| + \lambda a_{2t+j} \equiv 0, \qquad \text{mod. } q,$$

where $j = 0, 1, 2, \cdots, 2t - 1$. If we replace j by j', where $j' = j \pm t$, and make use of our assumption that $q^t \equiv -1$, mod. λ, we obtain

$$\lambda + \lambda(a_{2t+j} + a_{2t+j'}) \equiv 0, \qquad \text{mod. } q,$$

whence it follows that

$$a_{2t+j} + a_{2t+j'} = q - 1.$$

By use of Wilson's Theorem we have, if q is odd,

$$\prod(a_{2t+j}) \prod(a_{2t+j'}) \equiv (-1)^{a_{2t+j}+1}, \qquad \text{mod. } q.$$

By use of this relation together with the similar ones in the b's and c's, we obtain the congruence,

$$\psi(\alpha) \equiv q^t(-1)^{1+\Sigma(c_{2t+j}-a_{2t+j}-b_{2t+j})}, \qquad \text{mod. } \mathfrak{q}_i^{t+1},$$

where the summation is to be taken over the values $j = 0, 1, 2, \cdots, t - 1$.

From (13) we have, since we have assumed q to be odd,

$$c_{2t+j} - a_{2t+j} - b_{2t+j} \equiv \epsilon_{2t+j-1} - \epsilon_{2t+j}, \qquad \text{mod. } 2,$$

and hence, since $\epsilon_{2t-1} = 0$,

$$\sum(c_{2t+j} - a_{2t+j} - b_{2t+j}) \equiv -\epsilon_{3t-1}, \qquad \text{mod. } 2.$$

By assumption $|ai| + |bi| < \lambda$, and hence $|aiq^t| + |biq^t| > \lambda$. Hence from (16) we conclude that $\epsilon_{3t-1} = 1$, and consequently

$$\psi(\alpha) \equiv q^t, \qquad \text{mod. } \mathfrak{q}_i^{t+1}.$$

Hence if q is odd, we must have

$$\psi(\alpha) = q^t.\text{*}$$

More generally, if $q^{t_1} \equiv -1$, mod. λ, and t_1 is the smallest exponent which has that property, and if $t = st_1$, then for the Galois field of order q^{2t} we have by the previous theorem

$$\Psi(\alpha) = (-1)^{s-1} q^t. \tag{20}$$

Equation (20) may be shown to hold for $q = 2$ by the same method that was used in the case of equation (19) for $q = 2$. We have therefore the

THEOREM. *If q belongs to the exponent $2t_1$, mod. λ, and if $q^{t_1} \equiv -1$, mod. λ, then for the Galois field of order q^{2t}*

$$\Psi(\alpha) = (-1)^{s-1} q^t,$$

where $t = st_1$.

* Stickelberger (l. c., p. 341) has obtained a similar result for the Lagrange function, from which this may be deduced.

UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA.