FINITE FOURIER SERIES AND EQUATIONS IN FINITE FIELDS

BY

ALBERT LEON WHITEMAN

1. Introduction. Finite Fourier series were first employed for number theoretic purposes by Eisenstein [6] in 1844. Hurwitz [13], Rademacher [20], and Davenport [1] are among the later investigators who have given further applications of this method. In this paper we apply the method of multiple finite Fourier series to the theory of equations in finite fields.

We shall be concerned with the equation

$$c_1x_1^{a_1} + c_2x_2^{a_2} + \cdots + c_sx_s^{a_s} + c_{s+1} = 0, \tag{1.1}$$

where the coefficients $c_1, \cdots, c_s$ are given nonzero elements of a finite field $F(p^n)$ of order p^n, p is an odd prime, and the a_i are integers such that $0 < a_i < p^n - 1$. We assume that $s \geqq 2$ for $c_{s+1} \neq 0$ and $s > 2$ for $c_{s+1} = 0$, and seek the number of solutions of (1.1) in nonzero elements $x_1, \cdots, x_s$ of $F(p^n)$.

It should be noted that in the case $s = 1$, (1.1) reduces to the equation

$$c_1x_1^{a_1} + c_2 = 0, \tag{1.2}$$

with $c_1c_2 \neq 0$. Now any finite field may be represented by means of the residue classes with respect to some prime ideal in an algebraic field. Hence the theory of the equation (1.2) is included in the theory of the congruence

$$x^n \equiv \alpha \pmod{\mathfrak{p}} \tag{1.3}$$

where α is an integer in an algebraic field, $\mathfrak{p}$ is a prime ideal in that field, and $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$. The study of the congruence (1.3) has led to the theory of the class field and to the theory of the laws of reciprocity for nth powers [11].

In recent years the study of the equation (1.1) has played an increasingly important role in analytic number theory; in particular, the so-called "singular series" depend upon the number of solutions of equations over finite fields [15]. There are also applications to the Riemann hypothesis in function fields [2] and to Fermat's last theorem [3]. Other deep aspects of the problem have been revealed by the investigations of Mitchell [17; 18], of Davenport and Hasse [2], of Weil [24], and of Vandiver [23]. It does not seem too rash to predict that future developments of the theory will be comparable in interest to the classical laws of reciprocity.

Presented to the Society, April 28, 1951, under the title *Numbers of solutions of equations in finite fields*; received by the editors March 6, 1952.

As a preliminary to the explicit statement of the main problems of this paper it is convenient to introduce first the machinery of multiple finite Fourier series. Let $\mu_1, \mu_2, \cdots, \mu_s$ be a set of s non-negative integers and $m_1, m_2, \cdots, m_s$ a set of s positive integers. Let $\alpha_i = e^{2\pi i/m_i}$, $i=1, 2, \cdots, s$, be an m_ith root of unity. An arbitrary function $f(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$ is periodic in each μ_i with respect to the modulus m_i. It may therefore be expanded into a multiple finite Fourier series of the form

$$(1.4) \qquad f(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \sum_{j_1, j_2, \cdots, j_s} g(j_1, \cdots, j_s) \prod_{i=1}^{s} \alpha_i^{\mu_i j_i},$$

where the j_i range independently over $0, 1, \cdots, m_i - 1$. The system of linear equations (1.4) in the unknowns $g(j_1, \cdots, j_s)$ has a unique solution. Indeed the orthogonality relation

$$(1.5) \qquad \sum_{j_i=0}^{m_i-1} \alpha_i^{a j_i} \alpha_i^{-b j_i} = \begin{cases} m_i & (a \equiv b \pmod{m_i}), \\ 0 & (a \not\equiv b \pmod{m_i})) \end{cases}$$

enables us to determine the finite Fourier coefficients $g(k_1, \cdots, k_s)$ explicitly by means of the formula

$$(1.6) \qquad g(k_1, \cdots, k_s) \prod_{i=1}^{s} m_i = \sum_{\mu_1, \mu_2, \cdots, \mu_s} f(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \prod_{i=1}^{s} \alpha_i^{-\mu_i k_i},$$

where the μ_i range independently over $0, 1, \cdots, m_i - 1$. The finite Parseval relation is given by

$$(1.7) \qquad \prod_{i=1}^{s} m_i \sum_{j_1, j_2, \cdots, j_s} g(j_1, \cdots, j_s) \bar{g}(j_1 + k_1, \cdots, j_s + k_s)$$
$$= \sum_{\mu_1, \mu_2, \cdots, \mu_s} \left| f(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \right|^2 \prod_{i=1}^{s} \alpha_i^{\mu_i k_i},$$

where $\bar{g}(j_1, \cdots, j_s)$ denotes the complex conjugate of $g(j_1, \cdots, j_s)$. To prove (1.7) we introduce (1.6) into the left member of (1.7) and carry out the summation with respect to the j's. Applying the orthogonality relation (1.5) we obtain the right member of (1.7).

Let g be a generator of the cyclic group formed by the nonzero elements of $F(p^n)$ under multiplication. For a nonzero element a of $F(p^n)$ let ind a be defined by means of the equation $g^{\text{ind}\, a} = a$. In the theory of cyclotomy the generalized Jacobi-Cauchy sum of Vandiver [23, (11)] plays a fundamental role. This sum is defined for $s > 1$ by

$$(1.8) \qquad \psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \sum_{a_1, a_2, \cdots, a_{s-1}} \alpha_s^{\mu_s \,\text{ind}\, A} \prod_{i=1}^{s-1} \alpha_i^{\mu_i \,\text{ind}\, a_i},$$

and for $s = 1$ by $\psi(\alpha_1^{\mu_1}) = 1$. In this definition the integers m_i are restricted to be divisors of p^n-1, so that we may write $p^n-1=m_im_i'$, $i=1, 2, \cdots, s$. The elements a_i range independently over each element of $F(p^n)$, and the element A is defined by means of the equation

$$(1.9) \qquad A = 1 - a_1 - a_2 - \cdots - a_{s-1}.$$

The convention is also made that $\alpha^{\mu_i \text{ ind } (0)}=0$ for any μ_i.

We now return to the equation (1.1). For each u in $F(p^n)$ let $N_i(u)$, $1 \leqq i \leqq s$, be the number of solutions of the equation $x^{a_i}=u$. If the integers m_i are selected so that $(p^n-1, a_i)=m_i$, then $N_i(u)=1$ for $u=0$, and is otherwise equal to m_i or to 0 according as u is or is not an m_ith power in $F(p^n)$. It follows that the number of solutions of (1.1) is the same as the number of solutions of the equation

$$(1.10) \qquad c_1x_1^{m_1} + c_2x_2^{m_2} + \cdots + c_sx_s^{m_s} + c_{s+1} = 0.$$

In the case $c_{s+1}\neq 0$, we divide the terms of (1.10) by c_{s+1}, and put $c_i|c_{s+1}=g^{h_im_i+j_i}$, $0\leqq j_i\leqq m_i-1$. Equation (1.10) may then be put in the form

$$(1.11) \qquad g^{j_1+m_1\gamma_1} + g^{j_2+m_2\gamma_2} + \cdots + g^{j_s+m_s\gamma_s} + 1 = 0,$$

where $0\leqq \gamma_i \leqq m_i'-1$. The multiple cyclotomic number $(j_1, j_2, \cdots, j_s)$ is defined as the number of solutions in $\gamma_1, \gamma_2, \cdots, \gamma_s$ of the equation (1.11) for a fixed set of numbers $j_1, j_2, \cdots, j_s$ with the j_i in the range $0, 1, \cdots, m_i-1$ and the γ_i in the range $0, 1, \cdots, m_i'-1$. Hence the number of distinct sets of nonzero solutions of (1.1) is given by $m_1m_2\cdots m_s(j_1, j_2, \cdots, j_s)$.

In terms of the number $(j_1, j_2, \cdots, j_s)$, the ψ-function defined in (1.8) has the alternate representation [23, (15)]

$$(1.12) \qquad \psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \epsilon(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \sum_{j_1, j_2, \cdots, j_s} (j_1, j_2, \cdots, j_s) \prod_{i=1}^{s} \alpha_i^{\mu_i j_i},$$

where

$$(1.13) \qquad \epsilon = \epsilon(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \alpha_1^{\mu_1 \text{ ind } (-1)} \cdots \alpha_s^{\mu_s \text{ ind } (-1)}.$$

Since

$$g^{m_im_i'/2} = g^{(p^n-1)/2} = -1$$

in $F(p^n)$, we see that $\alpha^{\mu_i \text{ ind } (-1)} = \alpha_i^{\mu_i m_i m_i'/2} = \pm 1$, the sign depending on the value of μ_i. Hence $\epsilon = \pm 1$. We put

$$(1.14) \qquad \psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \epsilon(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})\Psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}),$$

and note that the sum in the right member of (1.12) may be regarded as the multiple finite Fourier series expansion of $\Psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$. The Parseval relation (1.7) now yields

$$(1.15)\quad \prod_{i=1}^{s} m_i \sum_{j_1,j_2,\cdots,j_s} (j_1, \cdots, j_s)(j_1 + k_1, \cdots, j_s + k_s) = \sum_{\mu_1,\mu_2,\cdots,\mu_s} \left| \Psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \right|^2 \prod_{i=1}^{s} \alpha_i^{-\mu_i k_i}.$$

We denote by $V(k_1, k_2, \cdots, k_s)$ the left member of (1.15). The first part of the present paper is concerned with the evaluation of the right member of (1.15) (see Theorem 1). This has been carried out by Vandiver [22] in the particular case $s=2$. Analogous sums have been studied by Dickson [4], Hurwitz [14], and Mordell [19]. The results have been employed to obtain inferior and superior limits for the number of solutions of the equation (1.1) (cf. [12]).

It will be seen in several instances that our methods differ from those employed by Vandiver [22]. A major difficulty is the evaluation of the complicated exponential sum $\rho(\alpha_1^{k_1}, \cdots, \alpha_s^{k_s})$ defined in (3.4) (see Theorem 2).

The remainder of the paper is taken up with the finite Fourier series expansion of the Ψ-function in the special case in which $\alpha_1 = \cdots = \alpha_s$ (see Theorem 3). The arithmetic sums studied by Dickson [3, (12)] and Hurwitz [14, (30)] thus appear in a natural manner as the finite Fourier coefficients in this expansion. In §7 we evaluate the Dickson-Hurwitz sum in the case $\mu_1 = \cdots = \mu_{s-1} = 0$. Finally we evaluate some quadratic relations of the Parseval type. It has been shown in another paper [25, (5.8)] that the Dickson-Hurwitz sums reduce to the so-called Jacobsthal sums in the particular case $n=1$, $\mu=1$, $s=2$. Thus Theorem 4 of the present paper may be regarded as a far-reaching generalization of the corresponding theorem [25, Theorem 1] in the theory of Jacobsthal sums.

The results of this paper may be compared with the results obtained by Faircloth [7] and by Faircloth and Vandiver [10]. These authors discuss the number of distinct sets of solutions of (1.1) in elements $x_1, \cdots, x_s$ of $F(p^n)$. Their methods and results for the case involving solutions in arbitrary elements are quite different from those involving solutions in nonzero elements. The formulas are in terms of a ψ-number [10, (8)] which is equivalent to (1.8).

It may be remarked that the formulas of Faircloth and Vandiver can be used to extend the main results of this paper to the cases in which (a) $c_{s+1}=0$ and the x's are arbitrary elements; (b) $c_{s+1}=0$ and the x's are nonzero elements; (c) $c_{s+1}\neq 0$ and the x's are arbitrary elements. It turns out that the problems involving solutions in nonzero elements are considerably more difficult than the problems involving solutions in arbitrary elements. However, we shall not go into these questions in the present paper.

2. **The ψ-functions.** Closely related to the generalized Jacobi-Cauchy sum (1.8) is the generalized Lagrange resolvent (cf. [23, p. 147]) defined by

$$(2.1)\qquad \tau(\alpha^{\mu}) = \sum_{a\in F(p^n)} \alpha^{\mu \operatorname{ind} a} \zeta^{\operatorname{tr}(a)},$$

where $\zeta = e^{2\pi i/p}$ and the numbers α and μ are defined as in (1.8). The symbol tr (a) denotes the trace of a and is defined as follows. If $n > 1$, let the $F(p^n)$ be defined by $f(\theta) = \theta^n + c_1\theta^{n-1} + \cdots + c_n = 0$, where $f(x)$ is an irreducible polynomial with coefficients in $F(p)$. Then let $a = d_1\theta^{n-1} + d_2\theta^{n-2} + \cdots + d_n$, $d_i \in F(p)$, and define

$$\text{tr }(a) = \sum_{i=1}^{n} (d_1\theta^{(n-1)(i)} + d_2\theta^{(n-2)(i)} + \cdots + d_n),$$

where $\theta^{(1)} = \theta, \theta^{(2)}, \cdots, \theta^{(n)}$ are the n conjugate roots of $f(x) = 0$ in $F(p^n)$. From the definition it follows immediately that

$$\text{tr }(a+b) = \text{tr }(a) + \text{tr }(b).$$

The following relation is also known [12, Lemma 1]:

$$(2.2) \qquad \sum_{a \in F(p^n)} \zeta^{\text{tr }(ab)} = \begin{cases} p^n & (b = 0), \\ 0 & (b \neq 0), \end{cases}$$

where b is an element of $F(p^n)$. The most important property of the function $\tau(\alpha^\mu)$ is given by

$$(2.3) \qquad \tau(\alpha^\mu)\tau(\alpha^{-\mu}) = \alpha^{\mu \text{ ind } (-1)} p^n,$$

provided that $\alpha^\mu \neq 1$. A broad extension of (2.3) has recently been obtained by Faircloth and Vandiver [9, (9)].

Returning to the ψ-function defined in (1.8), we now state two lemmas due to Faircloth and Vandiver [9] which will be useful in establishing our main results.

Lemma 1. *If* $\prod_{i=1}^{s} \alpha_i^{\mu_i} = 1$ *and* $\mu_i \not\equiv 0$ (*mod* m_i) *for at least one value of* i, *then*

$$\psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \frac{\prod_{i=1}^{s} \tau(\alpha_i^{\mu_i})}{-p^n}.$$

Lemma 2. *If* $\prod_{i=1}^{s} \alpha_i^{\mu_i} \neq 1$, *then*

$$\psi(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \frac{\prod_{i=1}^{s} \tau(\alpha_i^{\mu_i})}{\tau\left(\prod_{i=1}^{s} \alpha_i^{\mu_i}\right)}.$$

An important consequence of these two lemmas is the following result.

Lemma 3. *For an integer* r, $0 \leqq r \leqq s$, *define the function* $\psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$ *as a* ψ-*number for which* $\mu_i \not\equiv 0$ (mod m_i) *for* r *values of* i *and* $\mu_i \equiv 0$ (mod m_i) *for the remaining* $s-r$ *values of* i. *Then*

$$|\psi_r|^2 = p^{n(r-2)} \qquad \left(2 \leqq r \leqq s, \prod_{i=1}^{s} \alpha_i^{\mu_i} = 1\right), \tag{2.4a}$$

$$|\psi_r|^2 = p^{n(r-1)} \qquad \left(1 \leqq r \leqq s, \prod_{i=1}^{s} \alpha_i^{\mu_i} \neq 1\right). \tag{2.4b}$$

Note that r cannot equal 1 under the condition imposed in (2.4a). To prove Lemma 3 we first note that $\bar{\psi}_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{-\mu_s})$ is the complex conjugate of $\psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$ and that $\tau(1) = -1$. We then derive formulas (2.4a) and (2.4b) by applying Lemmas 1 and 2 in conjunction with (2.1) and (2.3).

We shall also make use of the function $\Psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$ whose definition is similar to the definition of the function $\psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s})$ of Lemma 3. From (1.13) and (1.14) it follows that $|\Psi_r|^2 = |\psi_r|^2$.

The case $r = 0$ is not covered in formulas (2.4a) and (2.4b). In this case, however, we may establish directly the following lemma.

LEMMA 4. *If* $r = 0$, *then*

$$\psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) = \frac{1}{p^n}((p^n - 1)^s + (-1)^{s+1}). \tag{2.5}$$

We have by (1.8)

$$\psi_0 = \psi(1, 1, \cdots, 1) = \sum_{a_1, a_2, \cdots, a_{s-1}} 1^{\operatorname{ind} A} 1^{\operatorname{ind} a_1} \cdots 1^{\operatorname{ind} a_{s-1}} \tag{2.6}$$

where A is defined by (1.9). Picking out those terms in (2.6) which contain no factor of the form $1^{\operatorname{ind}(0)}$, we see that $\psi_0 = (p^n - 1)^{s-1} - N_{s-1}$, where N_{s-1} denotes the number of solutions of the equation

$$a_1 + a_2 + \cdots + a_{s-1} = 1 \qquad (a_i \neq 0,\ i = 1, 2, \cdots, s-1). \tag{2.7}$$

Using (2.2) together with (2.7) we get

$$\begin{aligned} N_{s-1} &= \frac{1}{p^n} \sum_{a_1, a_2, \cdots, a_{s-1}; a_i \neq 0} \sum_a \zeta^{\operatorname{tr}(a(a_1 + a_2 + \cdots + a_{s-1} - 1))} \\ &= \frac{1}{p^n} \sum_a \zeta^{\operatorname{tr}(-a)} \sum_{a_1, a_2, \cdots, a_{s-1}; a_i \neq 0} \zeta^{\operatorname{tr}(aa_1)} \cdots \zeta^{\operatorname{tr}(aa_{s-1})} \\ &= \frac{1}{p^n}\left((p^n - 1)^{s-1} + (-1)^{s-1} \sum_{a \neq 0} \zeta^{\operatorname{tr}(-a)}\right) \\ &= \frac{1}{p^n}((p^n - 1)^{s-1} + (-1)^s). \end{aligned}$$

The result stated in (2.5) now follows immediately. A proof of Lemma 4 along completely different lines is given in the thesis of Faircloth [7].

An interesting application of Lemma 4 is obtained by putting $\mu_1 = \cdots = \mu_s = 0$ in (1.12) and (1.13). We get thus

$$(2.8) \qquad \sum_{j_1, j_2, \cdots, j_s} (j_1, j_2, \cdots, j_s) = \frac{1}{p^n}((p^n - 1)^s + (-1)^{s+1}).$$

For a generalization of (2.8) see Faircloth [8, Theorem 3].

In the sequel we shall also employ the following special result

$$(2.9) \qquad \psi(1, \cdots, 1, \alpha^\mu) = (-1)^{s-1} \qquad (\alpha^\mu \neq 1).$$

This formula follows at once from Lemma 2 and the fact that $\tau(1) = -1$. It may also be proved directly without much difficulty.

3. **The functions δ, λ, ρ, and ϕ.** To evaluate the right member of (1.15) we find it convenient to introduce certain auxiliary sums. For a fixed value of r let

$$(3.1) \qquad E = E_r = E(k_{i_1}, k_{i_2}, \cdots, k_{i_r}) \qquad (0 \leqq r \leqq s)$$

denote one of the $\binom{s}{r}$ sets of k's which may be selected from a set of s non-negative integers $k_1, k_2, \cdots, k_s$. There are 2^s sets (including the vacuous set) defined by (3.1). We first introduce the function $\delta(\alpha_i^{k_i})$ defined by

$$(3.2) \qquad \delta(\alpha_i^{k_i}) = \sum_{\mu_i=1}^{m_i-1} \alpha_i^{-\mu_i k_i} = \begin{cases} m_i - 1 & (k_i \equiv 0 \pmod{m_i}), \\ -1 & (k_i \not\equiv 0 \pmod{m_i}). \end{cases}$$

In terms of the δ-function we define for $1 \leqq r \leqq s$ the function

$$(3.3) \qquad \lambda_r(E_s) = \lambda_r(\alpha_1^{k_1}, \cdots, \alpha_s^{k_s}) = \sum_{E_r} \delta(\alpha_{i_1}^{k_{i_1}}) \cdots \delta(\alpha_{i_r}^{k_{i_r}}),$$

where the sum extends over the $\binom{s}{r}$ sets E_r. In other words, λ_r is the rth elementary symmetric function of the numbers $\delta(\alpha_1^{k_1}), \cdots, \delta(\alpha_s^{k_s})$. In particular, $\lambda_1(E_s) = \delta(\alpha_1^{k_1}) + \cdots + \delta(\alpha_s^{k_s})$ and $\lambda_s(E_s) = \delta(\alpha_1^{k_1}) \cdots \delta(\alpha_s^{k_s})$.

We next introduce the function

$$(3.4) \qquad \rho(E_s) = \rho(\alpha_1^{k_1}, \cdots, \alpha_s^{k_s}) = \sum \alpha_1^{-\mu_1 k_1} \cdots \alpha_s^{-\mu_s k_s},$$

where the sum extends over all the sets $\mu_1, \mu_2, \cdots, \mu_s$ for which $\prod_{i=1}^{s} \alpha_i^{\mu_i} = 1$ and $1 \leqq \mu_i \leqq m_i - 1$, $i = 1, 2, \cdots, s$. The function $\rho(E_r)$, $1 \leqq r \leqq s$, is similarly defined. Finally we define for $1 \leqq r \leqq s$ the function

$$(3.5) \qquad \phi_r(E_s) = \phi_r(\alpha_1^{k_1}, \cdots, \alpha_s^{k_s}) = \sum_{E_r} \rho(E_r),$$

where the sum extends over the $\binom{s}{r}$ sets E_r. Note in particular that each term of $\phi_1(E_s) = \rho(\alpha_1^{k_1}) + \cdots + \rho(\alpha_s^{k_s})$ is a vacuous sum.

Using the notation introduced in (3.3) and (3.5) we may write the right member of (1.15) in the form

$$\left| \Psi_0(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \right|^2 + \sum_{r=1}^{s} \left| \Psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \right|^2 (\lambda_r - \phi_r) + \sum_{r=2}^{s} \left| \Psi_r(\alpha_1^{\mu_1}, \cdots, \alpha_s^{\mu_s}) \right|^2 \phi_r.$$

Therefore by (2.4a), (2.4b), and (2.5) we get

THEOREM 1. *The sum* $V(k_1, \cdots, k_s)$ *defined in* (1.15) *is expressed by the formula*

$$V(k_1, k_2, \cdots, k_s) = \frac{1}{p^{2n}} ((p^n - 1)^s + (-1)^{s+1})^2 + \sum_{r=1}^{s} p^{n(r-1)} \lambda_r(E_s) - \sum_{r=2}^{s} (p^{n(r-1)} - p^{n(r-2)}) \phi_r(E_s), \tag{3.6}$$

where $\lambda_r(E_s)$ *and* $\phi_r(E_s)$ *are defined in* (3.3) *and* (3.5) *respectively.*

There remains the problem of evaluating $\phi_r(E_s)$. This is accomplished in the next section.

4. Evaluation of the ρ-function. Returning to the definition of the ρ-function in (3.4) we proceed to analyze the somewhat involved summation condition. Let m be the least common multiple of $m_1, m_2, \cdots, m_s$. Put $m = m_i t_i$, $i = 1, 2, \cdots, s$. Then we see that $\prod_{i=1}^{s} \alpha_i^{\mu_i} = 1$ if and only if

$$\mu_1 t_1 + \mu_2 t_2 + \cdots + \mu_s t_s \equiv 0 \pmod{m}. \tag{4.1}$$

In the case where $m_1, m_2, \cdots, m_s$ are prime each to each it follows that $\prod_{i=1}^{s} \alpha_i^{\mu_i} = 1$ if and only if $\mu_i \equiv 0 \pmod{m_i}$, $i = 1, 2, \cdots, s$. Therefore in this case the sum in (3.4) is vacuous. Consequently we have proved

$$\rho(E_s) = 0 \qquad (m_i \text{ prime each to each}). \tag{4.2}$$

Making use of (4.1) in conjunction with (3.2) we observe that (3.4) may be written in the form

$$\begin{aligned} \rho(E_s) &= \frac{1}{m} \sum_{\mu_1, \mu_2, \cdots, \mu_s; \mu_i \neq 0} \alpha_1^{-\mu_1 k_1} \cdots \alpha_s^{-\mu_s k_s} \sum_{h=0}^{m-1} e^{2\pi i h(\mu_1 t_1 + \cdots + \mu_s t_s)/m} \\ &= \frac{1}{m} \sum_{h=0}^{m-1} \delta(\alpha_1^{h-k_1}) \cdots \delta(\alpha_s^{h-k_s}). \end{aligned} \tag{4.3}$$

To evaluate the right member (4.3) we denote by $\theta(E_r)$ the number of values of h in the range $0 \leqq h \leqq m-1$ for which $h \equiv k_i \pmod{m_i}$ if $k_i \in E_r$ and $h \not\equiv k_i \pmod{m_i}$ if $k_i \notin E_r$. In terms of the function $\theta(E_r)$, (4.3) becomes

$$m\rho(E_s) = \sum_{r=0}^{s} \sum_{E_r} \theta(E_r)(m_{i_1} - 1)(m_{i_2} - 1) \cdots (m_{i_r} - 1)(-1)^{s-r}, \tag{4.4}$$

in view of (3.1) and (3.2).

Let $m(E_r)=[m_{i_1}, m_{i_2}, \cdots, m_{i_r}]$ be the least common multiple of a set of r m's. In particular, $m=m(E_s)=[m_1, m_2, \cdots, m_s]$. For the vacuous set E_0 put $m(E_0)=1$. Related to the function $\theta(E_r)$ is the function $t(E_r)$ which is defined as the number of values of h in the range $0\leqq h\leqq m-1$ such that $h\equiv k_i \pmod{m_i}$ for each k_i belonging to E_r. In particular, $t(E_s)=\theta(E_s)$. For the vacuous set E_0 put $t(E_0)=m$. For the set $E(k_i)$ consisting of a single k it is clear that

$$tE(k_i)=m/m_i.$$

To evaluate $t(E_r)$ in general we consider the system of linear congruences

$$(4.5)\qquad h\equiv k_{i_1} \pmod{m_{i_1}},\ h\equiv k_{i_2} \pmod{m_{i_2}},\ \cdots,\ h\equiv k_{i_r} \pmod{m_{i_r}},$$

where the numbers $k_{i_1}, k_{i_2}, \cdots, k_{i_r}$ belong to E_r and h is restricted to the range 0 to $m-1$. Let $d_{ij}=(m_i, m_j)$ denote the greatest common divisor of m_i and m_j. Then the Chinese remainder theorem (cf. [21, §5, chap. 7]) states that the system of simultaneous congruences (4.5) is soluble if and only if $k_i-k_j\equiv 0 \pmod{d_{ij}}$ for every pair k_i, k_j in E_r. Any solution h of this system satisfies the congruence $h\equiv h_0 \pmod{m(E_r)}$, where h_0 is uniquely determined $\pmod{m(E_r)}$. Thus for $2\leqq r\leqq s$ we get the formula

$$(4.6)\qquad t(E_r)=\begin{cases} m/m(E_r) & (k_i-k_j\equiv 0 \pmod{d_{ij}};\ k_i, k_j\in E_r),\\ 0 & \text{(otherwise)}.\end{cases}$$

In order to express the function $\theta(E_r)$ in terms of the function $t(E_r)$ we employ a standard combinatorial argument. Let E_{r+q}, $1\leqq q\leqq s-r$, be one of the $\binom{s-r}{q}$ sets which may be obtained by adjoining q additional k's to E_r. In accordance with this definition E_r is a subset of E_{r+q}. The problem of evaluating $\theta(E_r)$ is that of excluding from the h's counted in $t(E_r)$ those h's for which $h\equiv k_i \pmod{m_i}$ if $k_i\notin E_r$. According to a general combinatorial principle (cf. [21, theorem on p. 105]) the number of h's counted in $\theta(E_r)$ is given by the formula

$$(4.7\text{a})\qquad \begin{aligned}\theta(E_r) = t(E_r) - \sum_{E_{r+1}} t(E_{r+1}) + \sum_{E_{r+2}} t(E_{r+2}) - + \cdots\\ + (-1)^{s-r}\sum_{E_s} t(E_s)\end{aligned}$$

where the sum involving the sets E_{r+q} contains $\binom{s-r}{q}$ terms. In particular,

$$(4.7\text{b})\qquad \theta(E_0) = m - \sum_{E_1} t(E_1) + \sum_{E_2} t(E_2) - \sum_{E_3} t(E_3) + \cdots + (-1)^s t(E_s).$$

To complete the evaluation of $\rho(E_s)$ we substitute the right member of (4.7a) into (4.4). Our task is to pick out the coefficient of $(-1)^{s-r}t(E_r)$. It is not difficult to find that this coefficient is

$$\begin{aligned} 1 &+ [(m_{i_1} - 1) + (m_{i_2} - 1) + \cdots + (m_{i_r} - 1)] \\ &+ [(m_{i_1} - 1)(m_{i_2} - 1) + (m_{i_1} - 1)(m_{i_3} - 1) + \cdots] \\ &+ \cdots + [(m_{i_1} - 1)(m_{i_2} - 1) \cdots (m_{i_r} - 1)] \\ &= m_{i_1}m_{i_2} \cdots m_{i_r}. \end{aligned}$$

Hence (4.4) is transformed into

$$(4.8) \qquad m\rho(E_s) = \sum_{r=0}^{s} \sum_{E_r} (-1)^{s-r} t(E_r) m_{i_1}m_{i_2} \cdots m_{i_r}.$$

The final formula is expressed in terms of a function $d(E_r)$ which is defined by means of the equation

$$(4.9) \qquad d(E_r) = t(E_r)m_{i_1}m_{i_2} \cdots m_{i_r}/m.$$

Applying (4.6) to (4.9) we see that $d(E_r)$ may be defined alternatively as follows. For the vacuous set E_0 put $d(E_0)=1$. For the set $E(m_i)$ consisting of a single member put $dE(m_i)=1$. For $2 \leqq r \leqq s$ put $d(E_r)=m_{i_1}m_{i_2} \cdots m_{i_r}/m(E_r)$, provided that $k_i - k_j \equiv 0 \pmod{d_{ij}}$ for every pair k_i, k_j belonging to E_r. Otherwise put $d(E_r)=0$. In terms of the function $d(E_r)$, (4.8) may be expressed in a simple form. The result is stated in the following theorem:

THEOREM 2. *The formula*

$$(4.10) \qquad \rho(E_s) = \sum_{r=0}^{s} \sum_{E_r} (-1)^{s-r} d(E_r)$$

provides a solution of the problem of evaluating the sum $\rho(E_s)$ *defined in* (3.4).

Note that when the numbers $m_1, m_2, \cdots, m_s$ are prime each to each the value of each $d(E_r)$ is 1. In this case (4.10) becomes

$$\rho(E_s) = \sum_{r=0}^{s} (-1)^{s-r} \binom{s}{r} = (-1)^s (1-1)^s = 0,$$

in accordance with (4.2). We mention also that if $k_i - k_j \not\equiv 0 \pmod{d_{ij}}$ for every pair k_i, k_j belonging to E_s, then $d(E_r)=0$ for $2 \leqq r \leqq s$. We get in this case $\rho(E_s)=(-1)^{s-1}(s-1)$.

An interesting by-product of (3.4) and (4.10) is the following corollary of Theorem 2.

COROLLARY. *The number of sets of integers* $\mu_1, \mu_2, \cdots, \mu_s$, $1 \leqq \mu_i \leqq m_i - 1$, *for which* $\alpha_1^{\mu_1} \cdots \alpha_s^{\mu_s} = 1$ *is given by*

$$(4.11) \quad \rho(1, 1, \cdots, 1) = \sum_{r=0}^{s} \sum_{E_r} (-1)^{s-r} m_{i_1}m_{i_2} \cdots m_{i_r} / [m_{i_1}, m_{i_2}, \cdots, m_{i_r}].$$

The number $\rho(1, 1, \cdots, 1)$ is used by Faircloth [8, (9)] in his work on the number of distinct sets of solutions of equations of the type (1.1). Formula (4.11) is of importance in this connection.

As additional applications of formula (4.10) we deduce two special cases of interest. First in the case $s=2$ we note that $m_1m_2/[m_1, m_2]=d_{12}$ and thus obtain the formula

$$\rho(\alpha_1^{k_1}, \alpha_2^{k_2}) = \begin{cases} d_{12} - 1 & (k_1 \equiv k_2 \pmod{d_{12}}), \\ \phantom{d_{12}} - 1 & (k_1 \not\equiv k_2 \pmod{d_{12}}). \end{cases} \tag{4.12}$$

The case $s=3$ is more involved. We distinguish four essentially different cases. First case: $k_1-k_2\equiv 0 \pmod{d_{12}}$, $k_1-k_3\equiv 0 \pmod{d_{13}}$, $k_2-k_3\equiv 0 \pmod{d_{23}}$. Second case: $k_1-k_2\equiv 0 \pmod{d_{12}}$, $k_1-k_3\equiv 0 \pmod{d_{13}}$, $k_2-k_3\not\equiv 0 \pmod{d_{23}}$. Third case: $k_1-k_2\equiv 0 \pmod{d_{12}}$, $k_1-k_3\not\equiv 0 \pmod{d_{13}}$, $k_2-k_3\not\equiv 0 \pmod{d_{23}}$. Fourth case: $k_1-k_2\not\equiv 0 \pmod{d_{12}}$, $k_1-k_3\not\equiv 0 \pmod{d_{13}}$, $k_2-k_3\not\equiv 0 \pmod{d_{23}}$. Formula (4.10) now reduces to

$$\rho(\alpha_1^{k_1}, \alpha_2^{k_2}, \alpha_3^{k_3}) = \begin{cases} m_1m_2m_3/m + 2 - d_{12} - d_{13} - d_{23} & \text{(First case)}, \\ 2 - d_{12} - d_{13} & \text{(Second case)}, \\ 2 - d_{12} & \text{(Third case)}, \\ 2 & \text{(Fourth case)}. \end{cases} \tag{4.13}$$

Other results of this nature may be deduced in a similar fashion.

5. **Quadratic relations.** Formulas (3.3), (3.5), (3.6) and (4.10) provide a solution of the problem of evaluating $V(k_1, k_2, \cdots, k_s)$.

The case $s=2$ reduces to

$$\begin{aligned} V(k_1, k_2) = (p^n - 2)^2 + \delta(\alpha_1^{k_1}) + \delta(\alpha_2^{k_2}) + p^n\delta(\alpha_1^{k_1})\,\delta(\alpha_2^{k_2}) \\ - (p^n - 1)\rho(\alpha_1^{k_1}, \alpha_2^{k_2}), \end{aligned} \tag{5.1}$$

where the values of the δ- and ρ-functions are given by (3.2) and (4.12). Formula (5.1) leads immediately to the results of Vandiver [22, Theorem 1] mentioned in the introduction.

The case $s=3$ reduces to

$$\begin{aligned} V(k_1, k_2, k_3) = {} & ((p^n - 1)(p^n - 2) + 1)^2 + \delta(\alpha_1^{k_1}) + \delta(\alpha_2^{k_2}) + \delta(\alpha_3^{k_3}) \\ & + p^n(\delta(\alpha_1^{k_1})\delta(\alpha_2^{k_2}) + \delta(\alpha_1^{k_1})\delta(\alpha_3^{k_3}) + \delta(\alpha_2^{k_2})\delta(\alpha_3^{k_3})) \\ & + p^{2n}\delta(\alpha_1^{k_1})\delta(\alpha_2^{k_2})\delta(\alpha_3^{k_3}) \\ & - (p^n - 1)(\rho(\alpha_1^{k_1}, \alpha_2^{k_2}) + \rho(\alpha_1^{k_1}, \alpha_3^{k_3}) + \rho(\alpha_2^{k_2}, \alpha_3^{k_3})) \\ & - (p^{2n} - p^n)\rho(\alpha_1^{k_1}, \alpha_2^{k_2}, \alpha_3^{k_3}), \end{aligned} \tag{5.2}$$

where the values of the δ- and ρ-functions are given in (3.2), (4.12), and (4.13).

We confine ourselves to two special cases of (5.2). First, in the case $k_1=k_2=k_3=0$, we get after simplification

$$\begin{aligned} V(0, 0, 0) = {} & (p^n-1)^4 - 2(p^n-1)^3 \\ & + (p^n-1)^2(m_1-1)(m_2-1)(m_3-1) - m_1m_2m_3/m \\ & \qquad\qquad + d_{12} + d_{13} + d_{23} + 1) \\ & + (p^n-1)(2m_1m_2m_3 - m_1m_2 - m_1m_3 - m_2m_3 - m_1m_2m_3/m) \\ & + m_1m_2m_3. \end{aligned}$$

Second, we get in the case $k_1-k_2\not\equiv 0 \pmod{d_{12}}$, $k_1-k_3\not\equiv 0 \pmod{d_{13}}$, $k_2-k_3 \not\equiv 0 \pmod{d_{23}}$,

$$V(k_1, k_2, k_3) = (p^n-1)^4 - 2(p^n-1)^3,$$

provided that $k_1\not\equiv 0 \pmod{m_1}$, $k_2\not\equiv 0 \pmod{m_2}$, $k_3\not\equiv 0 \pmod{m_3}$.

For arbitrary s the right member of (3.6) is a complicated expression. However, a considerable simplification results when the numbers $m_1, m_2, \cdots, m_s$ are prime each to each. In this case we have, in view of (3.5) and (4.2), $\phi_r(\alpha_1^{k_1}, \cdots, \alpha_s^{k_s})=0$, $1\leqq r\leqq s$. Hence (3.6) becomes

$$(5.3)\quad V(k_1, k_2, \cdots, k_s) = \frac{1}{p^{2n}}((p^n-1)^s + (-1)^{s+1})^2 + \sum_{r=1}^{s} p^{n(r-1)}\lambda_r(E_s)$$

provided $m_1, m_2, \cdots, m_s$ are prime each to each.

There are two important particular cases of (5.3). In the first place, suppose that $k_i\equiv 0 \pmod{m_i}$, $i=1, 2, \cdots, s$. Then $\delta(\alpha_i^{k_i})=m_i-1$ and $\lambda_r(E_s)$ is the rth elementary symmetric function of the numbers m_1-1, $m_2-1, \cdots, m_s-1$. After transforming the right member of (5.3) we get the following corollary of Theorem 1.

COROLLARY 1. *If $m_1, m_2, \cdots, m_s$ are prime each to each then*

$$\begin{aligned} V(0, 0, \cdots, 0) = {} & \frac{1}{p^{2n}}((p^n-1)^s + (-1)^{s+1})^2 \\ & + \frac{1}{p^n}\left(-1 + \prod_{i=1}^{s}(1 + (m_i-1)p^n)\right). \end{aligned}$$

In the second place, suppose that $k_i\not\equiv 0 \pmod{m_i}$, $i=1, 2, \cdots, s$. Then we have $\delta(\alpha_i^{k_i}) = -1$ so that $\lambda_r(E_s) = (-1)^r\binom{s}{r}$. The sum in the right member of (5.3) now becomes

$$\sum_{r=1}^{s}(-1)^r\binom{s}{r}p^{n(r-1)} = \frac{(-1)^s}{p^n}((p^n-1)^s + (-1)^{s+1}).$$

Thus we have proved

COROLLARY 2. *If $m_1, m_2, \cdots, m_s$ are prime each to each and $k_i\not\equiv 0$* (mod

m_i), $i=1, 2, \cdots, s$, then

$$V(k_1, k_2, \cdots, k_s) = \frac{1}{p^{2n}}((p^n-1)^s+(-1)^{s+1})^2$$
$$+\frac{(-1)^s}{p^n}((p^n-1)^s+(-1)^{s+1}).$$

We conclude this section by remarking that it is not difficult to state theorems which express the left member of

$$2V(0, 0, \cdots, 0) - 2V(k_1, k_2, \cdots, k_s)$$
$$= \prod_{i=1}^{s} m_i \sum_{j_1, j_2, \cdots, j_s} ((j_1, \cdots, j_s) - (j_1+k_1, \cdots, j_s+k_s))^2$$

as the sum of squares (cf. [22, (17)]).

6. **Dickson-Hurwitz sums.** Let m be a divisor of p^n-1 so that we may write $p^n-1=mm'$. In this and later sections the symbol $(j_1, j_2, \cdots, j_s)$ denotes the number of distinct sets $\gamma_1, \gamma_2, \cdots, \gamma_s$, $0 \leqq \gamma_i \leqq m'-1$, which satisfy the equation $g^{j_1+m\gamma_1}+\cdots+g^{j_s+m\gamma_s}+1=0$, for a fixed set of numbers $j_1, j_2, \cdots, j_s$, $0 \leqq j_i \leqq m-1$. We shall expand the Ψ-function into a finite Fourier series in the particular case in which $\alpha_1=\alpha_2=\cdots=\alpha_s=\alpha=e^{2\pi i/m}$. As before we let $\mu_1, \mu_2, \cdots, \mu_s$ denote a set of s non-negative integers, but we now assume also that $\mu_s=1$. We first prove

THEOREM 3. *If μ denotes a non-negative integer, then the finite Fourier series expansion of $\Psi(\alpha^{\mu\mu_1}, \cdots, \alpha^{\mu\mu_{s-1}}, \alpha^\mu)$ is given by*

$$\Psi(\alpha^{\mu\mu_1}, \cdots, \alpha^{\mu\mu_{s-1}}, \alpha^\mu) = \sum_{i=0}^{m-1} D(i; \mu_1, \cdots, \mu_{s-1})\alpha^{\mu i}, \tag{6.1}$$

where the finite Fourier coefficient $D(i; \mu_1, \cdots, \mu_{s-1})$ is the Dickson-Hurwitz sum defined by

$$D(i; \mu_1, \cdots, \mu_{s-1}) = \sum_{j_1, j_2, \cdots, j_{s-1}} (j_1, \cdots, j_{s-1}, i-\mu_1 j_1 - \cdots - \mu_{s-1}j_{s-1}), \tag{6.2}$$

the numbers j_i ranging independently from 0 to $m-1$.

In the special case $n=1$, $s=2$, Theorem 3 reduces to a result due to Dickson [5, (16)]. To prove (6.1) we use the fact that to every nonzero element a in $F(p^n)$ there is an element h such that $g^h=a$. Thus we get from (1.8), (1.13), and (1.14)

$$\Psi(\alpha^{\mu\mu_1}, \cdots, \alpha^{\mu\mu_{s-1}}, \alpha^\mu) = \sum_{h_1, h_2, \cdots, h_{s-1}} \alpha^{\mu \text{ ind } H} \prod_{i=1}^{s-1} \alpha^{\mu\mu_i h_i},$$

where the number H is defined by $H=-1-g^{h_1}-g^{h_2}-\cdots-g^{h_{s-1}}$. Put $h_i=m\gamma_i+j_i$, $0\leqq j_i\leqq m-1$, $0\leqq\gamma_i\leqq m'-1$. Then the number of solutions of the congruence

$$\text{ind}\,(-1-g^{h_1}-g^{h_2}-\cdots-g^{h_{s-1}})+\mu_1h_1+\cdots+\mu_{s-1}h_{s-1}\equiv i \pmod{m}$$

is the same as the number of solutions of the equation

$$-1-g^{m\gamma_1+j_1}-\cdots-g^{m\gamma_{s-1}+j_{s-1}}=g^{m\gamma_s+(i-\mu_1j_1-\cdots-\mu_{s-1}j_{s-1})}.$$

The definition of the multiple cyclotomic symbol implies that the number of such solutions is precisely the Dickson-Hurwitz sum defined in (6.2). This completes the proof of Theorem 3.

Putting $\mu=0$ in (6.1) and applying Lemma 3, we obtain the result

$$(6.3)\qquad \sum_{i=0}^{m-1}D(i;\mu_1,\cdots,\mu_{s-1})=\frac{1}{p^n}((p^n-1)^s+(-1)^{s+1}).$$

This formula was derived by Hurwitz [14, (38)] in the case $n=1$, $s=2$. It is interesting to compare (2.8) with (6.3).

By (1.6) the finite Fourier coefficient in (6.1) is given by

$$(6.4)\qquad D(i;\mu_1,\cdots,\mu_{s-1})=\frac{1}{m}\sum_{\mu=0}^{m-1}\Psi(\alpha^{\mu\mu_1},\cdots,\alpha^{\mu\mu_{s-1}},\alpha^{\mu})\alpha^{-\mu i}.$$

By (1.7) the finite Parseval relation is given by

$$(6.5)\qquad \begin{aligned}&\sum_{i=0}^{m-1}D(i;\mu_1,\cdots,\mu_{s-1})D(i+k;\mu_1,\cdots,\mu_{s-1})\\&\qquad=\frac{1}{m}\sum_{\mu=0}^{m-1}\left|\Psi(\alpha^{\mu\mu_1},\cdots,\alpha^{\mu\mu_{s-1}},\alpha^{\mu})\right|^2\alpha^{-\mu k}.\end{aligned}$$

7. **The case $\mu_1=\cdots=\mu_{s-1}=0$.** In the special case of this section the Dickson-Hurwitz sum (6.2) becomes

$$(7.1)\qquad D_s(i)=D(i;0,\cdots,0)=\sum_{j_1,j_2,\cdots,j_{s-1}}(j_1,\cdots,j_{s-1},i).$$

We shall evaluate the sum in (7.1) explicitly. Putting $\mu_1=\cdots=\mu_{s-1}=0$ in (6.4) we obtain

$$(7.2)\qquad mD_s(i)=\Psi(1,1,\cdots,1)+\sum_{\mu=1}^{m-1}\Psi(1,\cdots,1,\alpha^{\mu})\alpha^{-\mu i}.$$

From (1.13), (1.14), and (2.9) we get $\Psi(1,\cdots,1,\alpha^{\mu})=(-1)^{s-1}\alpha^{\mu\,\text{ind}\,(-1)}$ for $\alpha^{\mu}\neq1$. Since ind $(-1)=(p^n-1)/2=mm'/2$ we infer easily that ind $(-1)\equiv0$ or $m/2$ (mod m) according as m' is even or odd. We distinguish two cases as follows. First case: $i=0$, m' even; $i=m/2$, m' odd. Second case: $i\neq0$, m' even, $i\neq m/2$, m' odd. For $0\leqq i\leqq m-1$, we deduce

$$(7.3)\qquad \sum_{\mu=1}^{m-1} \alpha^{\mu \operatorname{ind}(-1)}\alpha^{-\mu i} = \begin{cases} m-1 & \text{(First case)}, \\ -1 & \text{(Second case)}. \end{cases}$$

By Lemma 3 and (7.2), (7.3), we get after some simplification

$$D_s(i) = \begin{cases} \dfrac{m'}{p^n}((p^n-1)^{s-1}+(-1)^s)+(-1)^{s-1} & \text{(First case)}, \\ \dfrac{m'}{p^n}((p^n-1)^{s-1}+(-1)^s) & \text{(Second case)}. \end{cases}$$

The special case $s=2$ leads to the following well known formula due to Mitchell [17, (2)]

$$\sum_{j=0}^{m-1}(j,i) = \begin{cases} m'-1 & \text{(First case)}, \\ m' & \text{(Second case)}. \end{cases}$$

8. The Parseval relation.

The result (6.5) suggests the consideration of a sum $L(k;\mu_1,\cdots,\mu_{s-1})$ defined by

$$(8.1)\qquad L(k;\mu_1,\cdots,\mu_{s-1}) = \sum_{i=0}^{m-1} D(i;\mu_1,\cdots,\mu_{s-1})D(i+k;\mu_1,\cdots,\mu_{s-1}).$$

In the case $n=1$, $s=2$ a sum equivalent to (8.1) had already been studied by Lebesgue [16, p. 296] in 1854. The object of the present section is to evaluate the right member of (8.1). By (6.5) we have

$$(8.2)\qquad L(k;\mu_1,\cdots,\mu_{s-1}) = \frac{1}{m}\sum_{\mu=0}^{m-1} \left| \Psi(\alpha^{\mu\mu_1},\cdots,\alpha^{\mu\mu_{s-1}},\alpha^{\mu}) \right|^2 \alpha^{-\mu k}.$$

In order to compute the right member of (8.2) we require some additional notation. We put $\nu=\mu_1+\cdots+\mu_{s-1}+1$ and define integers t_i and m_i as follows:

$$(8.3)\qquad \begin{gathered} (\mu_1,m)=t_1,\cdots,(\mu_{s-1},m)=t_{s-1},\ (\nu,m)=t=t_s, \\ m=m_1t_1=\cdots=m_st_s. \end{gathered}$$

We emphasize that the m's thus defined are divisors of p^n-1, but are not arbitrary divisors as in §1–5. Here the m's depend on the choice of the μ's. It is still true, however, that $m=[m_1,\cdots,m_s]$. For m is a common multiple of the numbers $m_1,\cdots,m_s$ and is therefore a multiple of their least common multiple. If this least common multiple were not m itself, then the numbers $\mu_1,\cdots,\mu_{s-1},\nu$ would have a common prime factor. This is impossible.

We shall make use of the following lemma.

LEMMA 5. *Let μ be a number in the range $0\leqq\mu\leqq m-1$. If for $0\leqq r\leqq s-1$, r of the numbers $\mu\mu_1,\cdots,\mu\mu_{s-1},\mu\nu$ are divisible by m, and the remaining $s-r$ are not divisible by m, then*

$$|\Psi(\alpha^{\mu\mu_1}, \cdots, \alpha^{\mu\mu_{s-1}}, \alpha^{\mu})|^2 = p^{n(s-r-1)}. \tag{8.4}$$

The case $r=s$ is excluded from Lemma 5. We note, however, that all s of the numbers $\mu\mu_1, \cdots, \mu\mu_{s-1}, \mu\nu$ are divisible by m if and only if $\mu=0$. This case is covered by Lemma 4. Lemma 5 is a consequence of Lemma 3. If $\alpha^{\mu\nu}=1$, then exactly $s-r+1$ of the exponents in the left member of (8.4) are not divisible by m. This is the case covered by (2.4a). We get thus $|\Psi|^2 = p^{n(s-r-1)}$. If $\alpha^{\mu\nu}\neq 1$, then exactly $s-r$ of the exponents in the left member of (8.4) are not divisible by m. By (2.4b) we get again $|\Psi|^2 = p^{n(s-r-1)}$. In either event we deduce Lemma 5.

We next establish the following modified version of Lemma 5:

LEMMA 6. *Let the integers $m_1, \cdots, m_s$ be defined as in* (8.3). *For $0 \leqq r \leqq s-1$ let $E_r = E(m_{i_1}, m_{i_2}, \cdots, m_{i_r})$ be a set of r m's. If μ is a number in the range $0 \leqq \mu \leqq m-1$ for which $\mu \equiv 0$* (mod m_i) *if $m_i \in E_r$ and $\mu \not\equiv 0$ (mod m_i) if $m_i \notin E_r$, then formula* (8.4) *holds.*

Lemma 6 follows at once from the fact that $\mu\mu_i \equiv 0$ (mod m) if and only if $\mu \equiv 0$ (mod m_i). To prove this put $\mu_i = \mu_i' t_i$. Then $(\mu_i, m) = t_i$ if and only if $(\mu_i', m_i) = 1$, and $\mu\mu_i \equiv 0$ (mod m) if and only if $\mu\mu_i' \equiv 0$ (mod m_i). The proof is thus complete.

We now define for $0 \leqq r \leqq s$

$$\theta(E_r) = \sum_{\mu} \alpha^{-\mu k}, \tag{8.5}$$

where the sum extends over the values of μ in the range $0 \leqq \mu \leqq m-1$ for which $\mu \equiv 0$ (mod m_i) if $m_i \in E_r$, and $\mu \not\equiv 0$ (mod m_i) if $m_i \notin E_r$. To illustrate this definition we examine the particular case in which the μ's and ν are relatively prime to m. If E_0 is the vacuous set, then $\theta(E_0) = m-1$ or -1 according as k is or is not divisible by m; if $1 \leqq r \leqq s-1$, then the sum is empty and $\theta(E_r) = 0$; in the remaining case $\theta(E_s) = 1$. The number of values of μ over which the sum in (8.5) extends is, by the combinatorial principle employed in §4, given by

$$\frac{m}{m(E_r)} - \sum_{E_{r+1}} \frac{m}{m(E_{r+1})} + \sum_{E_{r+2}} \frac{m}{m(E_{r+2})} - + \cdots + (-1)^{s-r} \frac{m}{m(E_s)}, \tag{8.6}$$

where $m(E_r)$ denotes, as in §4, the least common multiple of the m's in E_r. It should be noted that the set E_r in (8.6) is a subset of each of the sets E_{r+q} (cf. discussion after (4.6)). We are now in the position to apply Lemmas 4 and 6 to the right member of (8.2). We get thus

$$\begin{aligned} mL(k; \mu_1, \cdots, \mu_{s-1}) = (1/p^{2n}) ((p^n - 1)^s + (-1)^{s+1})^2 \\ + \sum_{r=0}^{s-1} \sum_{E_r} p^{n(s-r-1)} \theta(E_r). \end{aligned} \tag{8.7}$$

The function $\theta(E_r)$ is, in many respects, analogous to the corresponding function which appears in formula (4.7a). In order to evaluate $\theta(E_r)$ we introduce the auxiliary sum

$$(8.8) \qquad t(E_r) = \sum_{\mu \equiv 0 (\mathrm{mod}\ m(E_r))} \alpha^{-\mu k},$$

where the sum extends over the $m/m(E_r)$ values of μ in the range $0 \leqq \mu \leqq m-1$ which are divisible by $m(E_r)$. By (8.6) we get for $0 \leqq r \leqq s$.

$$(8.9) \quad \theta(E_r) = t(E_r) - \sum_{E_{r+1}} t(E_{r+1}) + \sum_{E_{r+2}} t(E_{r+2}) - + \cdots + (-1)^{s-r} t(E_s).$$

Note in particular that (8.9) implies that $\theta(E_s) = t(E_s) = 1$. We proceed to evaluate $t(E_r)$. The values of μ in the range $0 \leqq \mu \leqq m-1$ for which $\mu \equiv 0$ (mod $m(E_r)$) may be put in the form

$$\mu = \lambda m(E_r), \ 0 \leqq \lambda \leqq m/m(E_r) - 1.$$

Thus (8.8) becomes

$$(8.10) \qquad t(E_r) = \sum_{\lambda} \exp\left(\frac{-2\pi i \lambda k}{m/m(E_r)}\right),$$

where λ runs over the integers in the range $0 \leqq \lambda \leqq m/m(E_r) - 1$. The sum in (8.10) equals zero unless λ is divisible by $m/m(E_r)$. Hence we have the result

$$(8.11) \qquad t(E_r) = \begin{cases} m/m(E_r) & (k \equiv 0 \ (\mathrm{mod}\ m/m(E_r))), \\ 0 & (k \not\equiv 0 \ (\mathrm{mod}\ m/m(E_r))). \end{cases}$$

We remark that $t(E_0) = m$ if $k \equiv 0$ (mod m) and equals 0 if $k \not\equiv 0$ (mod m). It is instructive to observe the analogy between (8.11) and (4.6).

There remains the problem of substituting the value of $\theta(E_r)$ in (8.9) into (8.7), and of picking out the coefficient of $(-1)^r t(E_r)$. For $0 \leqq r \leqq s-1$ this coefficient is

$$(8.12) \qquad \sum_{k=0}^{r} (-1)^k \binom{r}{k} p^{n(s-k-1)} = p^{n(s-r-1)}(p^n - 1)^r.$$

The coefficient of

$$(-1)^s t(E_s)$$

is

$$(8.13) \qquad \sum_{k=0}^{s-1} (-1)^k \binom{s}{k} p^{n(s-k-1)} = \frac{1}{p^n}((p^n - 1)^s + (-1)^{s+1}).$$

Introducing (8.12) and (8.13) into (8.7) we obtain the main result of this section:

THEOREM 4. *If* $L(k;\mu_1,\cdots,\mu_{s-1})$ *is the sum defined in* (8.1), *then*

$$\begin{aligned} &mL(k;\mu_1,\cdots,\mu_{s-1}) \\ (8.14)\qquad &= \frac{1}{p^{2n}}((p^n-1)^s+(-1)^{s+1})^2+\frac{(-1)^s}{p^n}((p^n-1)^s+(-1)^{s+1}) \\ &+\sum_{r=0}^{s-1}\sum_{E_r}(-1)^r t(E_r)p^{n(s-r-1)}(p^n-1)^r, \end{aligned}$$

where $t(E_r)$ *is defined by* (8.11).

9. **Special cases.** When $s=2$ the result given in Theorem 4 simplifies considerably. We put $p^n-1=mm'$, $\mu_1=\mu$, $\nu=\mu+1$, $(\mu,m)=t_1$, $(\nu,m)=t_2$, $m=m_1t_1=m_2t_2$. Then (8.14) becomes

$$\begin{aligned} (9.1)\qquad mL(k;\mu) &= (p^n-2)^2+(p^n-2)+p^nt(E_0) \\ &\quad - tE(m_1)(p^n-1)-tE(m_2)(p^n-1). \end{aligned}$$

Applying (8.11) with $k=0$ to (9.1) we get after a little manipulation

$$(9.2)\qquad L(0;\mu)=m'(p^n-2)+p^n-m'(t_1+t_2).$$

The case $k\not\equiv 0 \pmod m$ is more involved. The final formula may be expressed in the following form

$$(9.3)\qquad L(k;\mu)=\begin{cases} m'(p^n-2) & (t_1\nmid k,\ t_2\nmid k), \\ m'(p^n-2)-m't_1 & (t_1\mid k,\ t_2\nmid k), \\ m'(p^n-2)-m't_2 & (t_1\nmid k,\ t_2\mid k), \\ m'(p^n-2)-m'(t_1+t_2) & (t_1\mid k,\ t_2\mid k). \end{cases}$$

In the case $t_1=t_2=1$ the results in (9.2) and (9.3) reduce to certain formulas given by Hurwitz [14, (35), (36)] $(n=1)$, and Vandiver [22, (20), (21)].

When $s=3$ and $k=0$, we put $(\mu_1,m)=t_1$, $(\mu_2,m)=t_2$, $(\mu_1+\mu_2+1,m)=t_3$, $m=m_it_i$, $m/[m_i,m_j]=t_{ij}$, and obtain

$$\begin{aligned} (9.4)\qquad L(0;\mu_1,\mu_2) &= m'(p^n-2)((p^n-1)(p^n-2)+1)+p^{2n} \\ &\quad - m'p^n(t_1+t_2+t_3)+m'(p^n-1)(t_{12}+t_{13}+t_{23}). \end{aligned}$$

For s arbitrary the formulas which correspond to (9.2), (9.3), and (9.4) do not have a simple appearance. We confine our discussion to a formula which corresponds to the first case of (9.3). Suppose that $k\not\equiv 0 \pmod{m/m(E_r)}$ for each of the 2^s-1 sets E_r, $0\leqq r\leqq s-1$. Then (8.11) implies that $t(E_r)=0$, $0\leqq r\leqq s-1$, and (8.14) reduces in this case to

$$(9.5)\quad L(k;\mu_1,\cdots,\mu_{s-1})=\frac{m'}{p^{2n}}((p^n-1)^{s-1}+(-1)^s)((p^n-1)^s+(-1)^{s+1}).$$

To illustrate formula (9.5) we remark that it may be applied to the example $s=3$, $p=211$, $n=1$, $m=210$, $k=1$, $\mu_1=14$, $\mu_2=21$.

In general it does not seem possible to simplify the result in Theorem 4. However, in the particular case in which the μ's are relatively prime to m, simpler formulas can be obtained. We put, in this case, $t_1= \cdots =t_{s-1}=1$, $(\nu, m)=t=t_s$, $m=m_1= \cdots =m_{s-1}=m_s t_s$. Returning to the formula $t(E_r)$ in (8.11), we note that $t(E_r)=1$ for any set E_r other than the vacuous E_0 or the set $E(m_s)$ whose single member is m_s. The value of $t(E_0)$ is m if $m \mid k$ and is 0 if $m \nmid k$. The value of $tE(m_s)$ is t if $t \mid k$ and is 0 if $t \nmid k$.

Consider next the right member of (8.14) when $k \not\equiv 0 \pmod{m}$ and $t=1$. We have in this case

$$\sum_{r=0}^{s-1} \sum_{E_r} (-1)^r t(E_r) p^{n(s-r-1)}(p^n - 1)^r$$

$$(9.6) \qquad = \sum_{r=1}^{s-1} (-1)^r \binom{s}{r} p^{n(s-r-1)}(p^n - 1)^r$$

$$= - p^{n(s-1)} + \frac{(-1)^{s+1}}{p^n}((p^n - 1)^s + (-1)^{s+1}).$$

In general it is not difficult to modify the result in (9.6) appropriately to derive the following corollary of Theorem 4.

COROLLARY 1. *If $\mu_1, \cdots, \mu_{s-1}$ are non-negative integers relatively prime to m and if $(\mu_1 + \cdots + \mu_{s-1}+1, m)=t$, then the value of the function $mL(k; \mu_1, \cdots, \mu_{s-1})$ defined in* (8.1) *is given as follows*:

$$\frac{1}{p^{2n}}((p^n - 1)^s + (-1)^{s+1})^2 + (m - t)p^{n(s-1)} + (t - 1)p^{n(s-2)} \qquad (m \mid k),$$

$$\frac{1}{p^{2n}}((p^n - 1)^s + (-1)^{s+1})^2 - tp^{n(s-1)} + (t - 1)p^{n(s-2)} \qquad (t \mid k,\ m \nmid k),$$

$$\frac{1}{p^{2n}}((p^n - 1)^s + (-1)^{s+1})^2 - p^{n(s-2)} \qquad (t \nmid k).$$

We remark that an alternative proof of Corollary 1 may be deduced directly from (8.5) and (8.7). Another special case of interest is contained in the following corollary.

COROLLARY 2. *Under the hypotheses of Corollary* 1, *the value of the sum*

$$\sum_{i=0}^{m-1} (D(i; \mu_1, \cdots, \mu_{s-1}) - D(i + k; \mu_1, \cdots, \mu_{s-1}))^2 \qquad (k \not\equiv 0 \pmod{m})$$

is given by

$$2p^{n(s-1)} \qquad (k \equiv 0 \pmod{t}), \tag{9.7a}$$

$$2(p^{n(s-1)} - m'tp^{n(s-2)}) \qquad (k \not\equiv 0 \pmod{t}), \tag{9.7b}$$

where m' is defined by the equation $p^n - 1 = mm'$.

In the case $s=2$, $n=1$, $t=1$ the result in (9.7a) reduces to a formula due to Lebesgue [16, p. 298], rediscovered by Hurwitz [14, (37)], and later generalized by Vandiver [22, (22)] to $F(p^n)$. It should be noted that (9.7a) is a formula which gives representations of $2p^{n(s-1)}$ as the sum of m squares.

Bibliography

1. H. Davenport, *Note on linear fractional substitutions with large determinant*, Ann. of Math. (2) vol. 41 (1940) pp. 59–62.

2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. vol. 172 (1935) pp. 151–182.

3. L. E. Dickson, *Lower limit for the number of sets of solutions of $x^e+y^e+z^e \equiv 0$* (mod p), J. Reine Angew. Math. vol. 135 (1909) pp. 181–188.

4. ———, *Congruences involving only eth powers*, Acta Arithmetica vol. 1 (1935) pp. 161–167.

5. ———, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. vol. 37 (1935) pp. 363–380.

6. G. Eisenstein, *Aufgaben und Lehrsätze*, J. Reine Angew. Math. vol. 27 (1844) pp. 281–284.

7. O. B. Faircloth, *On the number of solutions of some general types of equations in a finite field*, Dissertation, University of Texas, May 1951, 36 pages. Published in Canadian Journal of Mathematics vol. 4 (1952) pp. 343–351.

8. ———, *Summary of new results concerning the solutions of equations in finite fields*, Proc. Nat. Acad. Sci. U. S. A. vol. 37 (1951) pp. 619–622.

9. O. B. Faircloth and H. S. Vandiver, *On multiplicative properties of a generalized Jacobi-Cauchy cyclotomic sum*, Proc. Nat. Acad. Sci. U. S. A. vol. 36 (1950) pp. 260–267. In Lemma 1 of this paper the condition "$\mu_i \not\equiv 0$ (mod m_i) for any i" may be replaced by the condition "$\mu_i \not\equiv 0$ (mod m_i) for at least one value of i."

10. ———, *On certain diophantine equations in rings and fields*, Proc. Nat. Acad. Sci. U. S. A. vol. 38 (1952) pp. 52–57.

11. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jber. Deutschen Math. Verein. vol. 35 (1926) pp. 1–55; vol. 36 (1927) pp. 233–311; Erganzungsband 6 (1930).

12. L. K. Hua and H. S. Vandiver, *On the existence of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U. S. A. vol. 34 (1948) pp. 258–263.

13. A. Hurwitz, *Sur quelques applications géométriques des séries de Fourier*, Ann. École Norm. (3) vol. 19 (1902) pp. 357–408 (=Mathematische Werke, vol. I, Basel, 1932, pp. 509–554). A simple introduction to the subject of finite Fourier series together with applications to geometry are also given by I. J. Schoenberg, Amer. Math. Monthly vol. 57 (1950) pp. 380–404.

14. ———, *Ueber die Kongruenz $ax^e+by^e+cz^e \equiv 0$* (mod p), J. Reine Angew. Math. vol. 136 (1909) pp. 272–292 (=Mathematische Werke, vol. II, Basel, 1933, pp. 430–445).

15. E. Landau, *Vorlesungen über Zahlentheorie*, vol. 1, Leipzig, 1927.

16. V. A. Lebesgue, *Demonstration de quelques formules d'un mémoire de M. Jacobi*, J. Math. Pures Appl. (1) vol. 19 (1854) pp. 289–300.

17. H. H. Mitchell, *On the generalized Jacobi-Kummer cyclotomic function*, Trans. Amer. Math. Soc. vol. 17 (1916) pp. 165–177.

18. ———, *On the congruence $cx^a+1=dy^a$ in a Galois field*, Ann. of Math. (2) vol. 18 (1917) pp. 120–131.

19. L. J. Mordell, *The number of solutions of some congruences in two variables*, Math. Zeit. vol. 37 (1933) pp. 193–209.

20. H. A. Rademacher, *The Fourier series and the functional equation of the absolute modular invariant $J(\tau)$*, Amer. J. Math. vol. 61 (1939) pp. 237–248.

21. J. V. Uspensky and M. A. Heaslett, *Elementary number theory*, New York and London, 1939.

22. H. S. Vandiver, *Quadratic relations involving the number of solutions of certain types of equations in a finite field*, Proc. Nat. Acad. Sci. U. S. A. vol. 35 (1949) pp. 681–685.

23. ———, *On a generalization of a Jacobi exponential sum associated with cyclotomy*, Proc. Nat. Acad. Sci. U. S. A. vol. 36 (1950) pp. 144–151.

24. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 497–508. For the connection with the results of Faircloth and Vandiver see [10; 23].

25. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. vol. 74 (1952) pp. 89–99.

University of Southern California,
Los Angeles, Calif.