TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 171, September 1972

ON THE EVALUATION OF BREWER'S CHARACTER SUMS

BY

REINALDO E. GIUDICI, JOSEPH B. MUSKAT AND STANLEY F. ROBINSON[1]

ABSTRACT. A decade ago in this journal B. W. Brewer defined a sequence of polynomials $V_n(x, 1)$ and for $n = 4$ and 5 evaluated

$$\sum_{x=1}^{p} \chi(V_n(x, 1)),$$

χ the nonprincipal quadratic character of the prime p, in closed form. A. L Whiteman derived these results by means of cyclotomy.

Brewer subsequently defined $V_n(x, Q)$. This paper applies cyclotomy to the more general polynomials and provides evaluations for several more values of n. Relevant quadratic decompositions of primes are studied.

1. **Introduction.** Let $f_m(x) = \sum_{j=0}^{m} a_j x^j$ denote a polynomial of degree m with integral coefficients. Let p be a fixed odd prime, and assume $p \nmid a_m$. Let χ denote the nonprincipal quadratic character (mod p) and define the character sum

$$S(f_m) = \sum_{x=0}^{p-1} \chi(f_m(x)).$$

$$S(f_0) = p\chi(a_0).$$

$$S(f_1) = 0. \tag{1.1}$$

$$S(f_2) = \begin{cases} -\chi(a_2) & \text{if } p \nmid (a_1^2 - 4a_2a_0), \\ (p-1)\chi(a_2) & \text{otherwise.} \end{cases} \qquad [11] \tag{1.2}$$

If $m \geq 3$, however, formulas for evaluating $S(f_m)$ in closed form have been found only in special cases. Bounds on $|S(f_m)|$ can be derived, however, for larger classes of polynomials. André Weil proved that if m is odd, unless $f(x) \equiv g^2(x)h(x)$ (mod p), where $g(x)$ is a nonconstant polynomial with integral coefficients,

Received by the editors July 10, 1970.

AMS 1970 *subject classifications*. Primary 10G05, 12C20, 10C05.

[1] This research was partially supported by the Agency for International Development contract 1a–221 and National Science Foundation grants GP-3464, GP-5308, and GP-8973.

$$|S(f_m)| < (m-1)\sqrt{p}. \quad [20]$$

The form of the bound suggests that given appropriate quadratic decompositions of p in the form

$$p = c_1y_1^2 + c_2y_2^2 + \cdots + c_ky_k^2, \qquad c_j > 0,\ 1 \le j \le k,$$

it is plausible that a closed form expression for $S(f_m)$ might consist of a linear combination of some of the y's and a constant. One such expression was given by Ernst Jacobsthal, who proved that for $f_3(x) = x(x^2 + a)$, if $p = X^2 + 4Y^2 \equiv X \equiv 1 \pmod 4$,

$$(1.3) \qquad S(f_3) = \begin{cases} -2(a|p)_4X & \text{if } \chi(a) = +1, \\ \pm 4Y & \text{if } \chi(a) = -1. \end{cases}$$

(The biquadratic residue symbol $(a|p)_4$ will be used throughout only for primes $p \equiv 1 \pmod 4$ and values of a such that $\chi(a) = +1$, so that the symbol will ·assume only the values ± 1.) If $p \equiv 3 \pmod 4$, $S(f_3) = 0$. [11]

The evaluations of Jacobsthal and similar results of Lothar von Schrutka [17] and Sarvadaman Chowla [4], [5] were generalized by Albert L. Whiteman, who considered the *Jacobsthal sum*

$$(1.4) \qquad \Phi_n(a) = \sum_{x=1}^{p-1} \chi(x(x^n + a)),$$

and the related sum

$$(1.5) \qquad \Psi_n(a) = \sum_{x=1}^{p-1} \chi(x^n + a).$$

He expressed both sums in terms of Dickson-Hurwitz sums. These sums appear as coefficients of Jacobi sums, which are character sums defined in the theory of cyclotomy. (See §3.) Certain of the Jacobi sums, in turn, can be transformed into diagonal quadratic decompositions of p. For example, if both n and $(p-1)/n$ are even numbers and g is a primitive root of p,

$$\sum_{j=0}^{n-1} \Phi_n(g^j)^2 = n^2p. \quad [21, (4.3)]$$

Recently Burns W. Brewer considered an interesting sequence of polynomials $V_n(x, Q)$. Let

$$(1.6) \qquad \begin{aligned} &V_n(x, Q) = xV_{n-1}(x, Q) - QV_{n-2}(x, Q), \qquad n > 2, \\ &V_1(x, Q) = x, \qquad V_2(x, Q) = x^2 - 2Q. \end{aligned}$$

He defined

$$(1.7) \qquad \Lambda_n(Q) = S(V_n(x, Q)) = \sum_{x=0}^{p-1} \chi(V_n(x, Q)).$$

He evaluated $\Lambda_n(1)$, $n = 1, 2, 3, 4$, and 5 [1], and $\Lambda_5(Q)$ [2] by means of certain binomial coefficient congruences.

Whiteman obtained some of Brewer's evaluations by means of Jacobi sums and the related Eisenstein sums ([25], [26], [27]). Whiteman's methods were extended to evaluate $\Lambda_6(Q)$ and $\Lambda_{10}(Q)$ and to relate $\Lambda_{2n}(Q)$ to $\Lambda_n(Q)$ if n is odd. [16]

This paper presents several contributions to the evaluation of $\Lambda_n(Q)$. Some new classes of quadratic decompositions of p are developed. As applications, $\Lambda_n(Q)$, $n = 7, 8, 9, 12, 14$, and 18, are derived, and a new expression for $\Lambda_{10}(Q)$ is obtained.

2. **Reduction formulas.** Let $\Lambda_n(Q)$ be defined by (1.7). Let λ be a generator of $\mathrm{GF}(p^2)$. Then $g = \lambda^{p+1}$ is a primitive root of p.

Brewer proved that if $Q' \equiv g^{2k}Q \pmod{p}$, then

$$\Lambda_n(Q') = \chi(g)^{kn}\Lambda_n(Q). \qquad [2, \text{Theorem } 1]$$

Two immediate consequences are that it suffices to determine $\Lambda_n(1)$ and $\Lambda_n(g)$ and that

$$\Lambda_n(Q) = -\Lambda_n(Q) = 0, \qquad p \equiv 3 \pmod{4},\ n \text{ odd}. \tag{2.1}$$

He also showed that if

$$\Omega_n(Q) = \sum_{s=0}^{p-2} \chi(g^{ns} + Q^n g^{-ns}),$$

$$\Theta_n(Q) = \sum_{t=0}^{p} \chi(\lambda^{n[t(p-1)+r]} + Q^n\lambda^{-n[t(p-1)+r]}), \tag{2.2}$$

where $Q \equiv g^r \pmod{p}$, then

$$2\Lambda_n(Q) = \Omega_n(Q) + \Theta_n(Q). \qquad [2, \text{Lemma } 2] \tag{2.3}$$

In order to evaluate a Brewer sum $\Lambda_n(Q) = \Lambda_n(g^r)$ of order n in closed form, one first decomposes the sum by means of (2.3). Then one seeks to reduce $\Omega_n(g^r)$ and $\Theta_n(g^r)$, where possible, to sums of lower orders, or in some cases to constants. This section is devoted to reduction procedures.

$\Omega_n(g^r)$ can be replaced by the sums Φ and Ψ defined by equations (1.4) and (1.5):

$$\Omega_n(g^r) = \begin{cases} \Phi_{2n}(g^{nr}), & n \text{ odd}, \qquad [16, (3.4)] \\ \Psi_{2n}(g^{nr}), & n \text{ even}. \qquad [16, (3.3)] \end{cases} \tag{2.4}$$

Whiteman proved that

(2.5) $$\Phi_n(g^{tn+k}) = (-1)^{t(n+1)}\,\Phi_n(g^k),$$ [21, (2.1)]

(2.6) $$\Psi_n(g^{tn+k}) = (-1)^{tn}\,\Psi_n(g^k),$$ [21, (3.5)]

(2.7) $$\Phi_n(g^k) = \begin{cases} (-1)^{k+1}\Phi_n(g^{n-k}), & n \text{ even}, \\ (-1)^{k+1}\Psi_n(g^{n-k}), & n \text{ odd}, \end{cases}$$ [21, (3.7)]

(2.8) $$\Psi_{2n}(g^k) = \Psi_n(g^k) + \Phi_n(g^k).$$ [21, (3.9)]

Combining (2.6) with (2.7) gives

(2.9) $$\Phi_n(1) = \Psi_n(1) \quad \text{if } n \text{ is odd.}$$

Lemma 1. *If $(n, b) = d$, then there exist integers y and z, $(z, b) = 1$, such that*

(2.10) $$nz + by = d.$$

Proof. (2.10) has an integer solution (z_0, y_0), and the general solution is

$$z = z_0 + tb/d, \qquad y = y_0 - tn/d, \qquad t \text{ any integer.}$$ [13, Theorem 2–6]

Since this is also the general solution of $zn/d + yb/d = 1$, $(z_0, b/d) = 1$. Then Dirichlet's theorem guarantees that there are infinitely many primes in the arithmetic progression $z_0 + tb/d$.

Theorem 1. *If $(n, p-1) = d$, then $\Phi_n(a) = \Phi_d(a)$ and $\Psi_n(a) = \Psi_d(a)$.*

Proof. In Lemma 1 let $b = p - 1$. Since $(z, p-1) = 1$, h and h^z run together over reduced residue systems (mod p). Since z is odd,

$$\Phi_n(a) = \sum_{h=1}^{p-1} \chi(h^z)\chi(h^{nz} + a) = \sum_{h=1}^{p-1} \chi(h)\chi(h^d + a) = \Phi_d(a).$$

Similarly,

$$\Psi_n(a) = \sum_{h=1}^{p-1} \chi(h^{nz} + a) = \sum_{h=1}^{p-1} \chi(h^d + a) = \Psi_d(a).$$

The reduction of $\Omega_n(Q)$ is summarized by the following: (Brackets denote the greatest integer function.)

Corollary 1. *Let $u = (2n, p-1)$. If n is odd, let $t = [nr/u]$.*

$$\Omega_n(g^r) = \begin{cases} (-1)^t\Phi_u(1), & r \text{ even}, \\ (-1)^t\Phi_u(g^{u/2}), & r \text{ odd}. \end{cases}$$

If n is even,

$$\Omega_n(g^r) = \Psi_{u/2}(1) + (-1)^{2nr/u}\Phi_{u/2}(1).$$

Proof. Let n be odd. By (2.4) and Theorem 1,

$$\Omega_n(g^r) = \Phi_{2n}(g^{nr}) = \Phi_u(g^{nr}).$$

If r is even, $t = nr/u$. Apply (2.5):

$$\Phi_u(g^{nr}) = \Phi_u(g^{tu}) = (-1)^{t(u+1)}\Phi_u(1) = (-1)^t\Phi_u(1).$$

If r is odd, $t = nr/u - 1/2$.

$$\Phi_u(g^{nr}) = \Phi_u(g^{tu+u/2}) = (-1)^t\Phi_u(g^{u/2}).$$

If n is even, by (2.4) and Theorem 1,

$$\Omega_n(g^r) = \Psi_{2n}(g^{nr}) = \Psi_u(g^{nr}) = \Psi_{u/2}(g^{nr}) + \Phi_{u/2}(g^{nr}),$$

by (2.8). Apply (2.6) and (2.5) with $s = 2nr/u$:

$$\Omega_n(g^r) = \Psi_{u/2}(g^{us/2}) + \Phi_{u/2}(g^{us/2}) = \Psi_{u/2}(1) + (-1)^s\Phi_{u/2}(1).$$

The reduction of $\Theta_n(Q)$ was studied in [16], where the following were proved:
(2.11) If $d = (n, p+1)$, $\Theta_n(Q) = \Theta_d(Q^{n/d})$ [16, Theorem 5.1].
(2.12) If n is odd, $\Theta_{2n}(Q) = \Theta_n(Q^2)$ [16, Theorem 5.4].
If $\xi \in \mathrm{GF}(p^2)$, define the trace $T(\xi) = \xi + \xi^p$. Then (2.2) becomes

$$\Theta_n(Q) = \Theta_n(g^r) = \sum_{t=0}^{p} \chi(\lambda^{n[t(p-1)+r]} + \lambda^{n[r(p+1)-t(p-1)-r]})$$

$$= \sum_{t=0}^{p} \chi(\lambda^{n[t(p-1)+r]} + \lambda^{n[pr+pt(p-1)]}) = \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+r]})).$$

Lemma 2. $\chi(T(\lambda^{c+k(p+1)})) = (-1)^k\chi(T(\lambda^c))$.

Proof.

$$T(\lambda^{c+k(p+1)}) = \lambda^{c+k(p+1)} + \lambda^{p[c+k(p+1)]} = \lambda^{c+k(p+1)} + \lambda^{pc+k(p+1)}$$

$$= \lambda^{k(p+1)}(\lambda^c + \lambda^{pc}) = g^kT(\lambda^c).$$

Lemma 2 shows that although λ is of order $p^2 - 1$, certain exponents of λ in $\Theta_n(Q)$ need be examined only modulo $2(p+1)$.

The next two theorems, which generalize Theorems 5.2 and 5.3 of [16], show that in order to obtain $\Theta_n(Q)$ it suffices to compute $\Theta_n(1)$ and, if n is odd and $p \equiv 1 \pmod 4$, also $\Theta_n(g)$. The latter also indicates conditions when $\Theta_n(Q) = 0$.

Theorem 2. $\Theta_n(g^{r+2k}) = (-1)^{nk}\Theta_n(g^r)$.

Proof.

$$\Theta_n(g^{r+2k}) = \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+r+2k]}))$$

$$= \sum_{u=-k}^{p-k} \chi(T(\lambda^{n[(u+k)(p-1)+r+2k]})) = \sum_{u=-k}^{p-k} \chi(T(\lambda^{n[u(p-1)+r+k(p+1)]}))$$

$$= (-1)^{nk} \sum_{u=-k}^{p-k} \chi(T(\lambda^{n[u(p-1)+r]})),$$

by Lemma 2,

$$= (-1)^{nk} \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+r]})) = (-1)^{nk}\Theta_n(g^r),$$

since t and u both run over complete residue systems (mod $(p+1)$).

Corollary 2. *If n is odd and $p \equiv 3 \pmod 4$, then $\Theta_n(g^r) = 0$.*

Proof. $\Theta_n(g^r) = \Theta_n(g^{r+p-1}) = (-1)^{n(p-1)/2}\,\Theta_n(g^r) = -\Theta_n(g^r)$.

The notation $q^{\nu} \| N$, where q is a prime, means that $q^{\nu} \mid N$ but $q^{\nu+1} \nmid N$.

Theorem 3. *If n is even, $2^{\eta} \| n$, and $2^{\rho} \| (p+1)$, then*

$$\Theta_n(g) = \begin{cases} \Theta_n(1), & \rho < \eta, \\ -\Theta_n(1), & \rho = \eta, \\ \Theta_n(1) = 0, & \rho > \eta. \end{cases}$$

Proof. First assume $\rho \leq \eta$. Let $k = (p+1)/2^{\rho+1} - 1/2$; k is an integer.

$$\Theta_n(g) = \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+1]}))$$

$$= \sum_{u=k}^{p+k} \chi(T(\lambda^{n[(u-k)(p-1)+1]})) = \sum_{u=k}^{p+k} \chi(T(\lambda^{n[u(p-1)-k(p-1)+1]}))$$

$$= \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)-k(p-1)+1]})).$$

$n[-k(p-1)+1] = -(1/2)(p-1) \cdot n(p+1)/2^{\rho} + (1/2)n(p-1) + n = (p+1)b$, where $b = -(1/2)(p-1) \cdot n/2^{\rho} + n/2$. By Lemma 2, $\Theta_n(g) = (-1)^b\Theta_n(1)$.

If $\rho = \eta = 1$, $(1/2)(p-1)$ is even and $n/2$ is odd. If $\rho = \eta > 1$, $(1/2)(p-1)$ is odd and $n/2$ is even. In either case, b is odd, so if $\rho = \eta$, $\Theta_n(g) = -\Theta_n(1)$.

If $\rho < \eta$, $n/2^{\rho}$ and $n/2$ are both even, so $\Theta_n(g) = \Theta_n(1)$.

Now assume $\rho > \eta$. Let $k = (p+1)/2^{\eta+1}$.

$$\Theta_n(Q) = \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+r]}))$$

$$= \sum_{u=-k}^{p-k} \chi(T(\lambda^{n[(u+k)(p-1)+r]})) = \sum_{u=-k}^{p-k} \chi(T(\lambda^{n[u(p-1)+k(p-1)+r]}))$$

$$= \sum_{t=0}^{p} \chi(T(\lambda^{n[t(p-1)+r]+b(p+1)})) = (-1)^k \Theta_n(Q),$$

where $b = (1/2)(p-1) \cdot n/2^{\eta}$. Since $\rho \geq 2$, b is odd, so $\Theta_n(Q) = -\Theta_n(Q) = 0$.

According to (2.11), $\Theta_n(Q)$ can be reduced to a Θ sum of lower order unless $p \equiv -1 \pmod{n}$. If n is even and $p \equiv -1 \pmod{2n}$, $\Theta_n(Q) = 0$, by Theorem 3. If n is odd and $p \equiv -1 \pmod{4n}$, $\Theta_n(Q) = 0$, by Corollary 2. The cyclotomy over $\mathrm{GF}(p^2)$ required to evaluate $\Theta_n(1)$, where n is even and $p \equiv n-1 \pmod{2n}$, and $\Theta_n(1)$ and $\Theta_n(g)$, where n is odd and $p \equiv 2n-1 \pmod{4n}$, is developed in §4.

Similarly, reduction may be applied in the evaluation of $\Omega_n(Q)$ unless $p \equiv 1 \pmod{2n}$, according to Corollary 1. §3 presents the cyclotomy over $\mathrm{GF}(p)$ required for evaluation where $p \equiv 1 \pmod{2n}$.

3. **Cyclotomy over GF(p).** Let $p \equiv 1 \pmod{e}$. Set $f = (p-1)/e$. Let $\beta = \exp(2\pi i/e)$. If e is even, let $e = 2E$.

Let g be a fixed primitive root modulo p. If $p \nmid a$, define the index of a, (mod $p-1$), by the congruence $g^{\mathrm{Ind}\ a} \equiv a \pmod{p}$.

The Jacobi sum $R(u, v) = R_e(u, v)$ of order e is defined by

$$R_e(u, v) = \sum_{a=2}^{p-1} \beta^{v\ \mathrm{Ind}\ a + u\ \mathrm{Ind}(1-a)} \tag{3.1}$$

$$= (-1)^{uf} \sum_{a=1}^{p-2} \beta^{u\ \mathrm{Ind}\ a + v\ \mathrm{Ind}(a+1)}.$$

$$R_e(u, 0) = \begin{cases} p-2, & e \mid u, \\ -1, & \text{otherwise}. \end{cases} \qquad [24, (2.5)] \tag{3.2}$$

$$R_e(u, v) = R_e(v, u) = (-1)^{vf} R_e(-u-v, v). \qquad [7, (83)] \tag{3.3}$$

If e does not divide u, v, or $u+v$,

$$R_e(u, v)\, R_e(-u, -v) = p. \qquad [7, (28)] \tag{3.4}$$

If the exponents of β in (3.1) which are congruent (mod e) are grouped, one may write

$$R_e(u, v) = (-1)^{vf} \sum_{j=0}^{e-1} C_j \beta^j. \tag{3.5}$$

The coefficients C_j will be called *Jacobi coefficients*. Clearly,

$$R_e(ku, kv) = (-1)^{kvf} \sum_{j=0}^{e-1} C_j \beta^{kj}. \tag{3.6}$$

The inverted form of the finite Fourier series (3.5) is

$$C_m = \frac{1}{e} \sum_{k=0}^{e-1} (-1)^{kvf} R_e(ku, kv)\, \beta^{-km}. \tag{3.7}$$

The cyclotomic number $(h, k) = (h, k)_e$ *of order* e is defined to be the number of solutions of

$$\begin{aligned} &g^s + 1 \equiv g^t \pmod{p}, \qquad 0 \le s,\ t \le p-2, \\ &s \equiv h \pmod{e}, \qquad t \equiv k \pmod{e}. \end{aligned} \tag{3.8}$$

The following identities are well known [7, (14), (15)]:

$$(h, k) = (-h, k-h), \tag{3.9}$$

$$(h, k) = \begin{cases} (k, h), & f \text{ even}, \\ (k+E, h+E), & f \text{ odd}. \end{cases} \tag{3.10}$$

A Jacobi sum can be expressed in terms of the cyclotomic numbers as a double finite Fourier series:

$$R_e(u, v) = (-1)^{uf} \sum_{h=0}^{e-1} \sum_{k=0}^{e-1} (h, k)_e \beta^{hu+kv}. \qquad [23, (2.6)]$$

The inverted form is

$$e^2(h, k)_e = \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} (-1)^{uf} R_e(u, v)\, \beta^{-hu-kv}. \qquad [23, (2.7)] \tag{3.11}$$

For Jacobi sums which can be expressed in the form $R_e(vn, n)$, one may write

$$R_e(vn, n) = (-1)^{vnf} \sum_{j=0}^{e-1} B(j, v) \beta^{nj}, \tag{3.12}$$

where the coefficients $B(j, v) = B_e(j, v)$ are Dickson-Hurwitz sums [22, (2.7)] defined by

$$B_e(j, v) = \sum_{h=0}^{e-1} (h, j - vh)_e. \tag{3.13}$$

If $e = xy$,

$$(h,\ k)_x = \sum_{m=0}^{y-1} \sum_{q=0}^{y-1} (h + mx,\ k + qx)_e. \qquad [9, (2)]$$

Hence

$$B_x(j,\ v) = \sum_{m=0}^{y-1} B_e(j + mx,\ v). \tag{3.14}$$

$$B_e(j,\ 0) = \begin{cases} f - 1, & e \mid j, \\ f, & e \nmid j. \end{cases} \qquad [7, (17)] \tag{3.15}$$

If e is even, by (3.14) and (3.15),

$$B_e(j,\ E) + B_e(j + E,\ E) = B_E(j,\ 0) = \begin{cases} 2f - 1, & E \mid j, \\ 2f, & E \nmid j. \end{cases} \qquad [26, \text{Lemma } 3] \tag{3.16}$$

If e is even, define

$$D(j,\ v) = D_e(j,\ v) = B_e(j,\ v) - B_e(j + E,\ v). \tag{3.17}$$

Whiteman proved that if v and e are relatively prime,

$$B(j,\ v) = B(jv',\ v'), \quad \text{where } vv' \equiv 1 \pmod{e}. \qquad [23, \text{Lemma } 1]$$

An immediate consequence is

$$D_e(j,\ v) = D_e(jv',\ v'), \quad \text{where } vv' \equiv 1 \pmod{e}. \tag{3.18}$$

From (3.9) and (3.13), $B(j,\ v) = B(j,\ e - v - 1)$. Hence

$$D_e(j,\ v) = D_e(j,\ e - v - 1). \tag{3.19}$$

If E is even, $E - 1$ and e are relatively prime, so that, by (3.18) and (3.19),

$$D_e(j,\ E) = D_e(j,\ E - 1) = D_e(j(E - 1),\ E - 1) = D_e(j(E - 1),\ E). \tag{3.20}$$

Whiteman related Dickson-Hurwitz sums to the Jacobsthal sum $\Phi_n(a)$ and the related sum $\Psi_n(a)$:

$$eB_e(j,\ 1) = p - 1 + \begin{cases} \Phi_e(4g^j), & e \text{ odd}, \\ \Psi_e(4g^j), & e \text{ even}. \end{cases} \qquad [21, (5.8)] \tag{3.21}$$

$$\Phi_E(1) = (-1)^{(E-1)f} ED_e(0,\ E). \qquad [26, \text{Lemma } 4] \tag{3.22}$$

The latter can be generalized as follows:

Theorem 4. $\Phi_E(g^r) = (-1)^{r+(E-1)f} ED_e(-r,\ E)$.

Proof.

$$\Phi_E(g^r) = \sum_{h=1}^{p-1} \chi(h)\chi(h^E + g^r) = \chi(g^r)\sum_{j=0}^{p-2} \chi(g^j)\chi(g^{jE-r} + 1)$$

$$= (-1)^r \sum_{s=0}^{(p-3)/2} [\chi(g^{2sE-r} + 1) - \chi(g^{(2s+1)E-r} + 1)].$$

From the definition of cyclotomic number in (3.8), the number of values of s for which $g^{2sE-r} + 1$ is a quadratic residue of p is $E\sum_{t=0}^{E-1} (-r, 2t)_e$, while $E\sum_{t=0}^{E-1} (-r, 2t+1)_e$ is the number of values of s for which $g^{2sE-r} + 1$ is a quadratic nonresidue. Thus

$$\sum_{s=0}^{(p-3)/2} \chi(g^{2sE-r} + 1) = E\sum_{t=0}^{E-1} [(-r, 2t)_e - (-r, 2t+1)_e].$$

Similarly,

$$\sum_{s=0}^{(p-3)/2} \chi(g^{(2s+1)E-r} + 1) = E\sum_{t=0}^{E-1} [(E-r, 2t)_e - (E-r, 2t+1)_e].$$

Thus

$$\Phi_E(g^r) = (-1)^r E\sum_{t=0}^{E-1} [(-r, 2t)_e + (E-r, 2t+1)_e - (E-r, 2t)_e - (-r, 2t+1)_e]$$

$$= (-1)^r E\sum_{s=0}^{e-1} [(sE-r, s)_e - (sE+E-r, s)_e] = (-1)^r(-1)^{(E-1)f} E D_e(-r, E),$$

by (3.10), (3.13), and (3.17).

In connection with applying Theorem 4, note that

$$D_e(0, E) \equiv -\chi(2) \pmod 4. \tag{3.23}$$

This follows from [14, Theorem 2 and the preceding Lemma].

For the evaluation of $\Omega_n(Q)$, Theorem 4 is sufficient, for any Ψ sum may be transformed into a sum of Jacobsthal sums by repeated use of (2.8) and finally (2.7). One can, however, evaluate a Ψ sum directly; this approach, which generalizes [16, (4.1)], will be used in evaluating $\Lambda_8(Q)$.

Theorem 5. *If* $p = 2Ef + 1$ *and* E *is even,*

$$\Omega_E(g^r) = \sum_{m=0}^{e-1} (-1)^{m(f+r)} R_e(m, E).$$

Proof. By (2.4),

$$\Omega_E(g^r) = \Psi_e(g^{Er}) = \sum_{h=1}^{p-1} \chi(h^e + g^{Er}) = \sum_{s=0}^{p-2} \chi(g^{es} + g^{Er}) = \sum_{s=0}^{p-2} \chi(g^{es-Er} + 1).$$

By the definition of cyclotomic number,

$$\Omega_E(g^r) = e \sum_{t=0}^{E-1} [(-Er,\ 2t)_e - (-Er,\ 2t+1)_e]$$

$$= e \sum_{t=0}^{E-1} e^{-2} \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} (-1)^{uf} R_e(u,\ v)[\beta^{Eru-2tv} - \beta^{Eru-(2t+1)v}],$$

by (3.11),

$$= e^{-1} \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} (-1)^{uf} R_e(u,\ v)\beta^{Eru}(1 - \beta^{-v}) \sum_{t=0}^{E-1} \beta^{-2tv}.$$

The inner sum vanishes unless $v = 0$ or E; if $v = 0$, $1 - \beta^{-v} = 0$. Hence

$$\Omega_E(g^r) = \sum_{u=0}^{e-1} (-1)^{uf} R_e(u,\ E)\beta^{Eru} = \sum_{u=0}^{e-1} (-1)^{u(f+r)} R_e(u,\ E).$$

This section concludes with the derivation of several quadratic decompositions of p used in expressing values of certain Brewer sums. The method was suggested by work of Herbert Walum [19].

Theorem 6. *Let* $e = xy$. *If for every integer* t *none of* $u(xt+1)$, $v(xt+1)$, *and* $(u+v)(xt+1)$ *is divisible by* e, *then*

$$\sum_{j=0}^{y-1} \left| \sum_{m=0}^{x-1} \beta^{ym} C_{j+ym} \right|^2 = p,$$

where the C's are defined in (3.5).

Proof. By (3.7),

$$\sum_{m=0}^{x-1} \beta^{ym} C_{j+ym} = \sum_{m=0}^{x-1} \beta^{ym} e^{-1} \sum_{s=0}^{e-1} (-1)^{svf} R_e(su,\ sv)\beta^{-s(j+ym)}$$

$$= e^{-1} \sum_{s=0}^{e-1} (-1)^{svf} R_e(su,\ sv)\beta^{-sj} \sum_{m=0}^{x-1} \beta^{ym(1-s)}$$

$$= \frac{x}{e} \sum_{t=0}^{y-1} (-1)^{(tx+1)vf} R_e((tx+1)u,\ (tx+1)v)\beta^{-(tx+1)j},$$

since the inner sum vanishes unless $s \equiv 1 \pmod{x}$. Thus

$$\sum_{j=0}^{y-1}\left|\sum_{m=0}^{x-1}\beta^{ym}C_{j+ym}\right|^2$$

$$=\frac{x^2}{e^2}\sum_{j=0}^{y-1}\sum_{t=0}^{y-1}(-1)^{(tx+1)v/f}R_e((tx+1)u,\ (tx+1)v)\,\beta^{-(tx+1)j}$$

$$\cdot\sum_{z=0}^{y-1}(-1)^{(zx+1)v/f}R_e(-(zx+1)u,\ -(zx+1)v)\,\beta^{(zx+1)j}$$

$$=\frac{1}{y^2}\sum_{t=0}^{y-1}\sum_{z=0}^{y-1}(-1)^{(t-z)xv/f}R_e((tx+1)u,\ (tx+1)v)$$

$$\cdot\,R_e(-(zx+1)u,\ -(zx+1)v)\sum_{j=0}^{y-1}\beta^{(z-t)xj}$$

$$=\frac{1}{y}\sum_{t=0}^{y-1}R_e((tx+1)u,\ (tx+1)v)\,R_e(-(tx+1)u,\ -(tx+1)v), \tag{3.24}$$

since the innermost sum vanishes unless $z = t$. The hypotheses of the theorem insure that (3.4) can be applied to every term in (3.24), so that (3.24) becomes $(1/y)\ \Sigma_{t=0}^{y-1}\ p = p$.

Let $2^{\nu}\|u$, $2^{\mathbf{v}}\|v$, $2^{\omega}\|u+v$, and $2^{\delta}\|e$. If $x = 4$, $tx + 1$ is odd, so the hypotheses of Theorem 6 are satisfied if

(3.25) δ is greater than $\mathbf{v}$, v, and ω.

$$|C_j+\beta^yC_{j+y}+\beta^{2y}C_{j+2y}+\beta^{3y}C_{j+3y}|^2=(C_j-C_{j+2y})^2+(C_{j+y}-C_{j+3y})^2.$$

Since $E = 2y$,

$$p=\sum_{j=0}^{y-1}[(C_j-C_{j+2y})^2+(C_{j+y}-C_{j+3y})^2]=\sum_{j=0}^{E-1}(C_j-C_{j+E})^2. \tag{3.26}$$

((3.25) is satisfied if $u \equiv 1 \pmod 4$ and $v \equiv 1, 2 \pmod 4$ or $u \equiv 2 \pmod 4$ and $v \equiv 1 \pmod 4$.) Of particular interest in the case $u = E$, $v = 1$. $R_e(E, 1)$ can be expressed in the form (3.12). Then (3.26) becomes

$$p=\sum_{j=0}^{E-1}D_e(j,\ E)^2. \tag{3.27}$$

For further simplification, apply (3.20) to obtain $D_e(j, E) = \pm D_e(E-j, E)$. If, furthermore, $4 \mid E$, then

$$D(E/2,\ E)=D(3E/2,\ E)=-D(E/2,\ E)=0. \tag{3.28}$$

Hence (3.27) becomes

$$(3.29) \qquad p = D_e(0, E)^2 + 2 \sum_{j=1}^{E/2-1} D_e(j, E)^2, \qquad e \equiv 0 \pmod 8),$$

$$(3.30)\ p = D_e(0, E)^2 + D_e(E/2, E)^2 + 2 \sum_{j=1}^{E/2-1} D_e(j, E)^2, \qquad e \equiv 4 \pmod 8).$$

Consider now $x = 3$. If the hypotheses of Theorem 6 are satisfied, then

$$|C_j + \beta^y C_{j+y} + \beta^{2y} C_{j+2y}|^2 = C_j^2 + C_{j+y}^2 + C_{j+2y}^2 - C_jC_{j+y} - C_jC_{j+2y} - C_{j+y}C_{j+2y}$$
$$= (1/4)(2C_j - C_{j+y} - C_{j+2y})^2 + (3/4)(C_{j+y} - C_{j+2y})^2.$$

Thus

$$(3.31) \qquad 4p = \sum_{j=0}^{y-1} [(2C_j - C_{j+y} - C_{j+2y})^2 + 3(C_{j+y} - C_{j+2y})^2].$$

Now let $x = 6$. If the hypotheses of Theorem 6 are satisfied, and $D_j = C_j - C_{j+E}$,

$$\begin{aligned} &|C_j + \beta^y C_{j+y} + \beta^{2y} C_{j+2y} + \beta^{3y} C_{j+3y} + \beta^{4y} C_{j+4y} + \beta^{5y} C_{j+5y}|^2 \\ &= |D_j + \beta^y D_{j+y} + \beta^{2y} D_{j+2y}|^2 \\ (3.32) \qquad &= D_j^2 + D_{j+y}^2 + D_{j+2y}^2 + D_jD_{j+y} - D_jD_{j+2y} + D_{j+y}D_{j+2y} \\ &= (1/4)(2D_j + D_{j+y} - D_{j+2y})^2 + (3/4)(D_{j+y} + D_{j+2y})^2. \end{aligned}$$

Hence

$$(3.33) \qquad 4p = \sum_{j=0}^{y-1} [(2D_j + D_{j+y} - D_{j+2y})^2 + 3(D_{j+y} + D_{j+2y})^2].$$

Further simplification can be achieved for the coefficients of $R_e(E, 1)$, E even. Here $E = 3y$. By (3.20)

$$(3.34) \qquad D_e(k, E) = -(-1)^k D_e(E - k, E),$$

so that the expression (3.32) takes on the same value for $j = k$ and $j = E - 2y - k = y - k$. This permits pairing of terms in (3.33). Only the terms corresponding to $j = 0$ and $j = y/2$ are unpaired. They can be simplified. Set $k = y$ in (3.34); the $j = 0$ term in (3.33) becomes $4[D_e(0, E) + D_e(y, E)]^2$. For $j = y/2$ there are two cases. When $y/2$ is odd, $D_e(y/2, E) = D_e(5y/2, E)$, so the $j = y/2$ term in (3.33) becomes $4[D_e(y/2, E) + D_e(E/2, E)]^2$. If, however, $y/2$ is even, $D_e(5y/2, E) = - D_e(y/2, E)$ and $D_e(3y/2, E) = D_e(E/2, E) = 0$, by (3.28). The $j = y/2$ term in (3.33) becomes $12D_e(y/2, E)^2$. Hence if

$$Z = \sum_{j=1}^{y/2-1} [(2D_e(j, E) + D_e(j + y,\ E) - D_e(j + 2y,\ E))^2$$
$$+ 3(D_e(j + y,\ E) + D_e(j + 2y,\ E))^2],$$

$$p = [D_e(0,\ E) + D_e(y,\ E)]^2 + 3D_e(y/2,\ E)^2 + Z/2, \qquad e \equiv 0 \pmod{24},$$

(3.35) $$p = [D_e(0,\ E) + D_e(y,\ E)]^2 + [D_e(y/2,\ E) + D_e(E/2,\ E)]^2 + Z/2,$$
$$e \equiv 12 \pmod{24}.$$

To show that all the squares in the sum Z are even, one notes that all the relevant $D_e(i,\ E)$ are even:

$$D_e(i,\ E) = B_e(i,\ E) - B_e(i + E,\ E) = 2f - 2B_e(i + E,\ E),$$

by (3.16).

4. Cyclotomy over $\mathrm{GF}(p^2)$. Let $p = E(2f + 1) - 1$. λ has been defined as a generator of $\mathrm{GF}(p^2)$. If $\xi \in \mathrm{GF}(p^2)$, let ind ξ be defined, modulo $p^2 - 1$, by the equation $\lambda^{\mathrm{ind}\ \xi} = \xi$. Set $e = 2E$; $e|(p^2 - 1)$. Let $\beta = \exp(2\pi i/e)$.

Let ψ denote the primitive eth power character of $\mathrm{GF}(p^2)$ defined by

$$\psi(\xi) = \begin{cases} \beta^{\mathrm{ind}\ \xi}, & \xi \neq 0, \\ 0, & \xi = 0. \end{cases}$$

Note that if $a \in \mathrm{GF}(p)$ and $a \equiv g^r \pmod{p}$,

$$\psi(a) = \beta^{\mathrm{ind}\ a} = \beta^{(p+1)r} = \beta^{E(2f+1)r} = (-1)^r = \chi(a),$$

so that ψ is an extension of the character χ to $\mathrm{GF}(p^2)$.

The generalized Gaussian sum $\tau(\beta^s)$ over $\mathrm{GF}(p^2)$ is defined by

$$\tau(\beta^s) = \sum_{\xi \in \mathrm{GF}(p^2);\ \xi \neq 0} \beta^{s\ \mathrm{ind}\xi} \zeta^{T(\xi)}, \qquad \zeta = \exp(2\pi i/p).$$

(4.1) $$\tau(\beta^s)\tau(\beta^{-s}) = \beta^{s\,\mathrm{ind}(-1)} p^2. \qquad [18,\ \text{p. } 335]$$

Let N be a fixed quadratic nonresidue of p. $P(x) = x^2 - N$ is an irreducible quadratic polynomial in $\mathrm{GF}(p)[x]$. Hence the residues $a + bx$, modulo $P(x)$, a, $b \in \mathrm{GF}(p)$, $x^2 = N$, form a representation of $\mathrm{GF}(p^2)$.

The Eisenstein sum $\epsilon(\beta^s)$ is defined by

(4.2) $$\epsilon(\beta^s) = \sum_{b=0}^{p-1} \beta^{s\ \mathrm{ind}(1+bx)} = \sum_{b=0}^{p-1} \psi^s(1 + bx). \qquad [10]$$

If s is odd,

(4.3) $$\tau(\beta^s) = \chi(2)G\epsilon(\beta^s), \qquad [27,\ (3.8)]$$

where $G = \sum_{a=0}^{p-1} \chi(a)\zeta^a$ is the ordinary Gaussian sum. Whiteman combined (4.1) with (4.3) to show that

$$\epsilon(\beta^s)\epsilon(\beta^{-s}) = p \quad \text{if } s \text{ is odd.} \qquad [27,\ (3.5)] \tag{4.4}$$

Further relationships between Eisenstein sums will be derived by combining (4.3) with the Davenport-Hasse identity [6, (0.9)]

$$\prod_{k=0}^{y-1} \tau(\beta^{kx+t}) = \psi^{-yt}(y)\tau(\beta^{yt}) \prod_{k=1}^{y-1} \tau(\beta^{kx}), \qquad e = xy. \tag{4.5}$$

Let a_i be the number of values of b, $0 \leq b \leq p - 1$, for which $\operatorname{ind}(1 + bx) \equiv i \pmod{e}$. Then the Eisenstein sum (4.2) can be expressed as $\epsilon(\beta^s) = \sum_{i=0}^{e-1} a_i\beta^{si}$. The Fourier transform is

$$ea_i = \sum_{s=0}^{e-1} \epsilon(\beta^s)\beta^{-si}. \tag{4.6}$$

$$a_i + a_{i+E} = \begin{cases} 2f, & i = E/2, \\ 2f + 1, & 0 \leq i \leq E - 1, \quad i \neq E/2. \end{cases} \qquad [27,\ \text{Lemma } 3] \tag{4.7}$$

If $\psi(1 + bx) = \beta^i$, $\psi(1 - bx) = \psi(1 + bx)^p = \beta^{pi} = \beta^{(E-1)i}$. This shows a 1-1 correspondence between numbers of the form $1 + bx$ whose index is $\equiv i \pmod{e}$ and numbers of this form whose index is $\equiv (E - 1)i \pmod{e}$. Hence

$$a_i = a_{i(E-1)}; \tag{4.8}$$

$$\epsilon(\beta^s) = \epsilon(\beta^{(E-1)s}) \qquad [27,\ (3.9)] \tag{4.9}$$

is an immediate consequence. Furthermore, $\operatorname{ind}(1 + bx) \equiv 0 \pmod{e}$ if and only if $\operatorname{ind}(1 - bx) \equiv 0 \pmod{e}$, so that the numbers of the form $1 + bx$, $1 \leq b \leq p - 1$, whose indices are $\equiv 0 \pmod{e}$ may be paired. In addition, however, $\operatorname{ind} 1 \equiv 0 \pmod{e}$, so that by (4.7)

$$a_0 \text{ is odd}, \qquad a_E \text{ is even}. \tag{4.10}$$

Whiteman established (4.8) and (4.10) for $e = 20$ [27, (4.6) and p. 78].

Define the difference $d_i = a_i - a_{i+E}$. $d_0 = a_0 - a_E = 2f + 1 - 2a_E$, by (4.7). Apply (4.10):

$$d_0 \equiv 2f + 1 \pmod{4}. \tag{4.11}$$

Whiteman showed that ([27, (3.25), (3.26)] and (2.12))

$$\Theta_E(1) = \begin{cases} Ed_0, & E \equiv 0 \pmod{8}, \\ (-1)^f Ed_0, & E \equiv 2 \pmod{8}, \\ -Ed_0, & E \equiv 4 \pmod{8}, \\ -(-1)^f Ed_0, & E \equiv 6 \pmod{8}. \end{cases} \tag{4.12}$$

If n is even, set $n = E$ and use (4.12). If n is odd, $\Theta_n(1) = \Theta_{2n}(1)$, by

(2.12). Set $2n = E$ and apply (4.12). The only remaining case in the discussion at the end of §2 is the evaluation of $\Theta_{E/2}(g)$, $E/2$ odd, $p \equiv E - 1 \pmod{2E}$.

In proving (4.12), Whiteman defined

$$\Upsilon_n(j) = \sum_{k=0}^{p} \psi(\lambda^{(p-1)(j+kn)} + 1)$$

and showed that

$$\Upsilon_E(j) = \chi(2) E d_j \beta^{-j}. \qquad [27, (3.22)]$$

$$\Theta_n(g) = \sum_{t=0}^{p} \chi(\lambda^{n[(p-1)t+1]} + \lambda^{pn[(p-1)t+1]})$$

$$= \sum_{t=0}^{p} \psi(\lambda^{pn[(p-1)t+1]}) \psi(\lambda^{(-1p)n[(p-1)t+1]} + 1)$$

$$= \beta^{pn} \sum_{t=0}^{p} \beta^{(1-p)nt} \psi(\lambda^{(p-1)n(2t-1)} + 1).$$

Now set $n = E/2$. Since $p \equiv 1 \pmod 4$,

$$\Theta_{E/2}(g) = \beta^{E/2} \sum_{t=0}^{p} \psi(\lambda^{(p-1)n(2t-1)}) = \beta^{E/2} \Upsilon_E(-E/2)$$

$$= \beta^{E/2} \chi(2)\, E d_{-E/2} \beta^{E/2}.$$

$$\text{(4.13)} \qquad \Theta_{E/2}(g) = \chi(2)\, E d_{E/2}.$$

The following is analogous to Theorem 6.

Theorem 7. *If* $p = E(2f + 1) - 1$, *let* $e = xy$, x *even. Then*

$$\sum_{j=0}^{y-1} \left| \sum_{m=0}^{x-1} \beta^{ym} a_{j+ym} \right|^2 = p.$$

Proof. By (4.6),

$$\sum_{m=0}^{x-1} \beta^{ym} a_{j+ym} = \frac{1}{e} \sum_{m=0}^{x-1} \beta^{ym} \sum_{s=0}^{e-1} \epsilon(\beta^s) \beta^{-s(j+ym)}$$

$$= \frac{1}{e} \sum_{s=0}^{e-1} \epsilon(\beta^s) \beta^{-sj} \sum_{m=0}^{x-1} \beta^{ym(1-s)} = \frac{x}{e} \sum_{t=0}^{y-1} \epsilon(\beta^{tx+1}) \beta^{-(tx+1)j}.$$

Thus

$$\sum_{j=0}^{y-1}\left|\sum_{m=0}^{x-1}\beta^{ym}a_{j+ym}\right|^2$$

$$=\frac{x^2}{e^2}\sum_{j=0}^{y-1}\sum_{t=0}^{y-1}\epsilon(\beta^{tx+1})\beta^{-(tx+1)j}\sum_{z=0}^{y-1}\epsilon(\beta^{-zx}-1)\,\beta^{(zx+1)j}$$

$$=\frac{1}{y^2}\sum_{t=0}^{y-1}\epsilon(\beta^{tx+1})\sum_{z=0}^{y-1}\epsilon(\beta^{-zx}-1)\sum_{j=0}^{y-1}\beta^{jx(z-t)}$$

$$=\frac{1}{y}\sum_{t=0}^{y-1}\epsilon(\beta^{tx+1})\,\epsilon(\beta^{-tx}-1)=\frac{1}{y}\sum_{t=0}^{y-1}p=p,$$

by (4.4).

Set $x=4$ in Theorem 7. Then $E=2y$.

$$|a_j+\beta^y a_{j+y}+\beta^{2y}a_{j+2y}+\beta^{3y}a_{j+3y}|^2=|d_j+\beta^y d_{j+y}|^2=d_j^2+d_{j+y}^2.$$

(4.14) $$p=\sum_{j=0}^{y-1}(d_j^2+d_{j+y}^2)=\sum_{j=0}^{E-1}d_j^2.$$

It follows from (4.8) that $d_j=\pm d_{E-j}$. Then (4.14) becomes

(4.15) $$p=d_0^2+d_{E/2}^2+2\sum_{j=1}^{E/2-1}d_j^2,\qquad e\equiv 0 \pmod 4).$$

If $E/2$ is even, $a_{E/2}=a_{3E/2}$, so $d_{E/2}=0$. Hence

(4.16) $$p=d_0^2+2\sum_{j=1}^{E/2-1}d_j^2,\qquad e\equiv 0 \pmod 8).$$

If $x=6$ in Theorem 7,

$$|a_j+\beta^y a_{j+y}+\beta^{2y}a_{j+2y}+\beta^{3y}a_{j+3y}+\beta^{4y}a_{j+4y}+\beta^{5y}a_{j+5y}|^2$$
$$=|d_j+d_{j+y}/2-d_{j+2y}/2+(d_{j+y}+d_{j+2y})\sqrt{-3}/2|^2.$$
$$=(1/4)[(2d_j+d_{j+y}-d_{j+2y})^2+3(d_{j+y}+d_{j+2y})^2].$$

Hence

(4.17) $$4p=\sum_{j=0}^{y-1}[(2d_j+d_{j+y}-d_{j+2y})^2+3(d_{j+y}+d_{j+2y})^2].$$

The reader has doubtless noted by now the striking parallel between the Eisenstein sum coefficients a_i and the Jacobi coefficients $B_e(i,E)$. This is now exploited to obtain from (4.17)

$$p = (d_0 + d_y)^2 + 3d_{y/2}^2 + \frac{1}{2}\sum_{j=1}^{y/2-1} [(2d_j + d_{j+y} - d_{j+2y})^2 + 3(d_{j+y} + d_{j+2y})^2], \qquad e \equiv 0 \pmod{24},$$

(4.18)
$$p = (d_0 + d_y)^2 + (d_{y/2} + d_{E/2})^2 + \frac{1}{2}\sum_{j=1}^{y/2-1} [(2d_j + d_{j+y} - d_{j+2y})^2 + 3(d_{j+y} + d_{j+2y})^2], \qquad e \equiv 12 \pmod{24}.$$

The argument is the same as that at the end of §3, but with (4.8) playing the role of (3.20). Showing that $d_{j+y} \pm d_{j+2y}$ is even is slightly different: (4.7) implies that each d term in the summation is odd; the sum of two odd terms is even.

5. **Brewer sums of orders** 1, 2, 3, 4, **and** 6. This section contains the evaluations of several character sums. These evaluations, drawn mostly from earlier papers, are needed in the next sections.

$\Phi_2(a)$, evaluated by Jacobsthal, was given in §1. (See (1.3).) By (1.5) and (1.2),

(5.1)
$$\Psi_2(a) = \sum_{x=0}^{p-1} \chi(x^2 + a) - \chi(a) = \begin{cases} -2, & \chi(a) = 1, \\ 0, & \chi(a) = -1. \end{cases}$$

(5.2)
$$\Psi_1(1) = \Phi_1(1) = -1. \qquad (2.8), (2.9), (5.1)$$

$$\Lambda_1(Q) = \sum_{x=0}^{p-1} \chi(x) = 0. \qquad (1.7), (1.1)$$

Thus by (2.3) and (2.4), $\Phi_2(Q) + \Theta_1(Q) = 0$;

(5.3) $\Theta_1(Q) = -\Phi_2(Q)$.

(5.4) $\Psi_4(Q^2) = \Psi_2(Q^2) + \Phi_2(Q^2) = -2 + \chi(Q)\Phi_2(1)$. (2.8), (5.1), (2.5)

$\Lambda_2(Q) = -1$, by (1.2). Hence by (2.3), (2.4), and (5.4), $-2 = \Psi_4(Q^2) + \Theta_2(Q) = -2 + \chi(Q)\Phi_2(1) + \Theta_2(Q)$.

(5.5)
$$\Theta_2(Q) = -\chi(Q)\Phi_2(1)$$

$$\Lambda_3(Q) = \Phi_2(-3Q). \qquad (1.7), (1.4)$$

$$\Lambda_3(Q) = 0, \quad p \equiv 3 \pmod 4. \qquad (2.1)$$

Now assume $p \equiv 1 \pmod 4$. Set

(5.6)
$$R_4(1, 1) = (-1)^f[D_4(0, 1) + D_4(1, 1)\sqrt{-1}] = -X + 2Y\sqrt{-1}.$$

From (3.19) and (3.23), $X \equiv 1 \pmod 4$.

By (2.5), (3.22), and (3.19), if $p \equiv 1 \pmod 4$,

$$\Phi_2(Q^2) = \chi(Q)\Phi_2(1) = 2\chi(Q)(-1)^f D_4(0, 2) = -2\chi(Q)X. \tag{5.7}$$

Similarly, by Theorem 4, if $p \equiv 1 \pmod 4$,

$$\begin{aligned}\Phi_2(g) &= -2(-1)^f D_4(3, 2) = 2(-1)^f D_4(1, 1) = 4Y,\\ \Phi_2(g^3) &= -4Y.\end{aligned} \tag{5.8}$$

Note the agreement with (1.3).

(5.9) $\Theta_2(Q) = 2\chi(Q)X$, $p \equiv 1 \pmod 4$. (5.5), (5.7)

(5.10) $\Psi_4(Q^2) = -2 - 2\chi(Q)X$, $p \equiv 1 \pmod 4$. (5.4), (5.7)

$$\Lambda_3(1) = \Phi_2(-3) = \begin{cases} 4Y, & \text{if } X \equiv -Y \pmod 3, \quad [1, \text{Theorem } 1] \\ -2(-3|p)_4 X, & p \equiv 1 \pmod{12}. \quad [26, \text{p. } 46] \end{cases} \tag{5.11}$$

In the former case in (5.11), obviously $p \equiv 5 \pmod{12}$. The latter result can be obtained from (5.7).

For $p \equiv 5 \pmod{12}$, if $\operatorname{Ind}(-3) \equiv 1 \pmod 4$, $\operatorname{Ind}(-3g) \equiv 2 \pmod 4$, while if $\operatorname{Ind}(-3) \equiv 3 \pmod 4$, $\operatorname{Ind}(-3g) \equiv 0 \pmod 4$. Then by (5.7)

$$\Lambda_3(g) = \begin{cases} 2X, & \operatorname{Ind}(-3) \equiv 1 \pmod 4, \\ -2X, & \operatorname{Ind}(-3) \equiv 3 \pmod 4. \end{cases} \tag{5.12}$$

Consider now $p \equiv 1 \pmod{12}$. If -3 is a biquadratic residue of p, by (5.8), $\Phi_2(-3g) = \Phi_2(g) = 4Y$, while if $\operatorname{Ind}(-3) \equiv 2 \pmod 4$, $\Phi_2(-3g) = -4Y$. Thus-

$$\Lambda_3(g) = 4(-3|p)_4 Y. \tag{5.13}$$

The choice of g affects the sign of Y. If $p \equiv 5 \pmod 8$, the sign of Y can be related to the index of 2:

$$Y \equiv -\operatorname{Ind} 2 \pmod 4. \quad [12, \text{Theorem } 2]$$

If $p \equiv 1 \pmod 4$, $\Theta_4(Q) = \Theta_2(Q^2) = \Theta_2(1)$, by (2.11) and Theorem 2. If $p \equiv 5 \pmod 8$, by Corollary 1, $\Omega_4(Q) = \Psi_2(1) + \Phi_2(1)$. Hence by (2.3), (5.1), and (5.5),

$$2\Lambda_4(Q) = -2 + \Phi_2(1) - \Phi_2(1) = -2.$$

If $p \equiv 1 \pmod 8$, by Corollary 1 and (3.22),

$$\Omega_4(Q) = \Psi_4(1) + \chi(Q)\Phi_4(1) = \Psi_4(1) + 4\chi(Q)(-1)^f D_8(0, 4).$$

Hence by (2.3), (5.9), and (5.10),

$$2\Lambda_4(Q) = -2 + 4(-1)^f \chi(Q) D_8(0, 4).$$

Applying (3.20) to (3.12), one may set

$$R_8(1,\ 3) = (-1)^f[D_8(0,\ 3) + D_8(1,\ 3)\sqrt{-2}] = C + D\sqrt{-2}. \tag{5.14}$$

Thus by (3.19),

$$\Lambda_4(Q) = -1 + 2\chi(Q)C,$$

$$\Psi_8(Q^4) = -2 - 2X + 4\chi(Q)C. \tag{5.15}$$

Note that by (3.23), $C \equiv -(-1)^f \pmod 4$.

If $p \equiv 3 \pmod 4$, by Corollary 1 and (5.2),

$$\Omega_4(Q) = \Psi_1(1) + \Phi_1(1) = -2.$$

$$\Theta_4(Q) = \begin{cases} \chi(Q)\Theta_4(1), & p \equiv 3 \pmod 8, \\ 0, & p \equiv 7 \pmod 8). \end{cases} \qquad \text{(Theorem 3)} \tag{5.16}$$

If $p \equiv 3 \pmod 8$, by (4.12), $\Theta_4(1) = -4d_0$. Now by (4.16), $d_0^2 + 2d_1^2 = p$. Set $C = -d_0$. Thus

$$\Theta_4(1) = 4C, \qquad C \equiv 2f - 1 \pmod 4. \qquad (4.11) \tag{5.17}$$

In summary,

$$\Lambda_4(Q) = \begin{cases} -1 + 2\chi(Q)C, & p \equiv 1,\ 3 \pmod 8, \\ -1, & \text{otherwise}, \end{cases}$$

where $C \equiv 2f - 1 \pmod 4$, $f = [p/8]$, $C^2 + 2D^2 = p$.

$\Lambda_4(1)$ was evaluated in [1] and [25].

If $p \equiv 5 \pmod 6$,

$$\Lambda_6(Q) = \begin{cases} 4\chi(Q)Y - 1, & p \equiv 5 \pmod{12}, \\ -1, & p \equiv 11 \pmod{12}. \end{cases} \qquad [16,\ (6.2)]$$

If $p \equiv 1 \pmod 6$, one may set

$$R_6(1,\ 2) = -A + B\sqrt{-3}, \qquad A \equiv 1 \pmod 3. \qquad [7,\ \text{pp. } 408\text{–}410] \tag{5.18}$$

Then

$$\Lambda_6(Q) = \begin{cases} -1 - 2A, & p \equiv 7 \pmod{12}, \\ -1 - 2A - 2(-3\,|\,p)_4\,\chi(Q)X, & p \equiv 1 \pmod{12}. \end{cases} \qquad [16,\ (6.11)] \tag{5.19}$$

A, C, and X will retain their meanings through the next three sections.

6. Evaluation of $\Lambda_8(Q)$ and $\Lambda_{12}(Q)$.

By (2.3) and (2.4),

$$2\Lambda_8(Q) = \Omega_8(Q) + \Theta_8(Q) = \Psi_{16}(Q^8) + \Theta_8(Q).$$

From Theorem 1 and (2.6),

$$\Psi_{16}(Q^8) = \begin{cases} \Psi_2(1) = -2, & p \equiv 3 \text{ (mod 4)}, \qquad (5.1)\\ \Psi_4(1) = -2 - 2X, & p \equiv 5 \text{ (mod 8)}, \qquad (5.10)\\ \Psi_8(1) = -2 - 2X + 4C, & p \equiv 9 \text{ (mod 16)}. \qquad (5.15)\end{cases}$$

By means of (2.11) and Theorems 2 and 3,

$$\Theta_8(Q) = \begin{cases} \Theta_2(1) = 2X, & p \equiv 1 \text{ (mod 4)}, \qquad (5.9)\\ \Theta_4(1) = 4C, & p \equiv 3 \text{ (mod 8)}, \qquad (5.17)\\ 0, & p \equiv 15 \text{ (mod 16)}.\end{cases}$$

It remains to evaluate the two cases where the reduction procedures of §2 do not help, namely $\Omega_8(Q)$, $p \equiv 1$ (mod 16), and $\Theta_8(Q)$, $p \equiv 7$ (mod 16).

According to Theorem 5, if $p \equiv 1$ (mod 16) and $Q \equiv g^r$ (mod p),

$$\Omega_8(Q) = \sum_{m=0}^{15} (-1)^{m(f+r)} R_{16}(m, 8) = (-1)^{f+r} \sum_{k=0}^{7} R_{16}(2k+1, 8) + \sum_{k=0}^{7} R_{16}(2k, 8).$$

The first sum, by (3.12) and (3.6), can be written as

$$\sum_{k=0}^{7} \sum_{j=0}^{15} B_{16}(j, 8)\beta^{(2k+1)j} = \sum_{j=0}^{15} B_{16}(j, 8)\beta^j \sum_{k=0}^{7} \beta^{2kj}$$
$$= 8[B_{16}(0, 8) - B_{16}(8, 8)] = 8D_{16}(0, 8).$$

The terms of the second sum are evaluated individually. By (5.14) and (3.3),

$$R_{16}(2, 8) = R_{16}(6, 8) = C + D\sqrt{-2}.$$

Their complex conjugates are $R_{16}(14, 8)$ and $R_{16}(10, 8)$; they are equal to $C - D\sqrt{-2}$. By (5.6), $R_{16}(4, 8) = -X + 2Y\sqrt{-1}$; $R_{16}(12, 8) = -X - 2Y\sqrt{-1}$. $R_{16}(0, 8) = R_{16}(8, 8) = -1$, by (3.2) and (3.3). Hence

$$\Omega_8(Q) = -2 - 2X + 4C + 8(-1)^f \chi(Q) D_{16}(0, 8).$$

If $p \equiv 7$ (mod 16), by Theorems 2 and 3 and (4.12), $\Theta_8(Q) = \chi(Q)\Theta_8(1) = 8\chi(Q)d_0$.

The evaluation of $\Lambda_8(Q)$ can now be summarized as follows:

p (mod 16)	$\Lambda_8(Q)$
1	$-1 + 2C + 4(-1)^f\chi(Q)D_{16}(0, 8)$
3, 9, 11	$-1 + 2C$
5, 13, 15	-1
7	$-1 + 4\chi(Q)d_0$

By (3.29) and (4.16) both $D_{16}(0, 8)$ and d_0 correspond to x_0 in the quaternary quadratic form

$$p = x_0^2 + 2x_1^2 + 2x_2^2 + 2x_3^2; \tag{6.1}$$

by (3.4) and (4.4), furthermore,

$$2x_0x_2 = x_1^2 - x_3^2 - 2x_1x_3. \tag{6.2}$$

Given the decomposition (6.1), one can determine the sign of x_0 as follows:

$$(6.3)\quad \begin{aligned} x_0 &= D_{16}(0, 8) \equiv 3 \pmod 4, && (3.23)\\ x_0 &= d_0 \equiv 2f + 1 \equiv (-1)^f \pmod 4. && (4.11)\end{aligned}$$

Rewrite (6.2) as $2x_0x_2 = (x_1 - x_3)^2 - 2x_3^2$. If q is an odd prime divisor of x_0 or x_2,

$$2x_3^2 \equiv (x_1 - x_3)^2 \pmod q. \tag{6.4}$$

Consequently, if $q \equiv \pm 3 \pmod 8$, 2 is a quadratic nonresidue of q, so q divides x_3, and also x_1. Then q^2 divides either x_0 or x_2. Factor q^2 out of both sides of (6.4) and repeat the procedure if possible. The conclusion is that if $q \equiv \pm 3 \pmod 8$, q^{2j} exactly divides either x_0 or x_2, for some integer j, and then $q^j \mid x_1$, $q^j \mid x_3$. It follows that x_0 and x_2 are both $\equiv \pm 1 \pmod 8$. Combine with (6.3): $D_{16}(0, 8) \equiv 7 \pmod 8$, $d_0 \equiv (-1)^f \pmod 8$.

In evaluating $\Lambda_{12}(Q)$, eight residue classes, modulo 24, must be examined. Curiously, no two residue classes have the same formulas.

$$2\Lambda_{12}(Q) = \Omega_{12}(Q) + \Theta_{12}(Q) = \Psi_{24}(Q^{12}) + \Theta_{12}(Q).$$

Theorems 2 and 3, Corollary 1, (2.6), (2.11), and (2.12) are used for reduction. Then (2.8) and (2.9) are applied to eliminate all Ψ sums. The results are shown in the following table. Other relations used in a specific case are cited in the right margin.

$p \pmod{24}$	$\Psi_u(Q^{12})$	$\Theta_v(Q)$	
1	$\Psi_{24}(Q^{12}) = \chi(Q)\,\Phi_{12}(1) + \Phi_6(1) + 2\,\Phi_3(1)$	$\Theta_2(1) = 2X$	(5.9)
5	$\Psi_4(1) = -2 - 2X$	$\Theta_6(1) = \Theta_3(1)$	(5.10)
7	$\Psi_6(1) = 2\Phi_3(1)$	$\Theta_4(Q^3) = 0$	
11	$\Psi_2(1) = -2$	$\Theta_{12}(Q) = \chi(Q)\Theta_{12}(1)$	(5.1)
13	$\Psi_{12}(1) = \Phi_6(1) + 2\Phi_3(1)$	$\Theta_2(1) = 2X$	(5.9)
17	$\Psi_8(Q^{12}) = 4\chi(Q)C - 2X - 2$	$\Theta_6(1) = \Theta_3(1)$	(5.15)
19	$\Psi_6(1) = 2\Phi_3(1)$	$\Theta_4(Q^3) = 4\chi(Q)C$	(5.16), (5.17)
23	$\Psi_2(1) = -2$	$\Theta_{12}(1) = 0$	(5.1)

$$(6.5) \qquad \Phi_3(1) = -2A - 1, \quad p \equiv 1 \pmod 6). \quad [5, \text{Theorem } 2]$$

When $p \equiv 5 \pmod{12}$, $\Theta_3(1) = 2\Lambda_3(1) - \Omega_3(1)$; $\Omega_3(1) = \Phi_6(1) = \Phi_2(1) = -2X$, by (2.3), (2.4), Theorem 1, and (5.7). Apply (5.11):

$$(6.6) \qquad \Theta_3(1) = 8Y + 2X, \quad X \equiv -Y \pmod 3, \quad p \equiv 5 \pmod{12}.$$

When $p \equiv 1 \pmod{12}$, $\Phi_6(1) = 2\Lambda_3(1) - \Theta_3(1)$. Apply (5.11), (2.11), (5.3), and (5.7):

$$(6.7) \qquad \Phi_6(1) = -X[2 + 4(-3 \mid p)_4], \quad p \equiv 1 \pmod{12}.$$

$$\begin{aligned} \Phi_{12}(1) &= 12(-1)^f D_{24}(0, 12), \quad p \equiv 1 \pmod{24}, && (3.22) \\ &= (-1)^f\{8D_{24}(0, 12) + 8D_{24}(4, 12) \\ &\qquad + 4[D_{24}(0, 12) + D_{24}(8, 12) + D_{24}(16, 12)]\}, && (3.20) \\ &= 8(-1)^f U + 4(-1)^f D_8(0, 4) = 8(-1)^f U + 4C, \end{aligned}$$

by [14, (81), (92)], (3.14), and (5.14), where $p = U^2 + 24V^2$, $U \equiv \operatorname{Ind} 3 - 1 \pmod 4$.

Next it will be shown that

$$(6.8) \qquad \Theta_{12}(1) = \Theta_4(1) = 4C, \quad p \equiv 11 \pmod{24},$$

so that the evaluation of $\Lambda_{12}(Q)$ may be summarized as follows. Note that if $p \equiv 5$ or $7 \pmod 8$, $\Lambda_{12}(g) = \Lambda_{12}(1)$.

$p \pmod{24}$	$\Lambda_{12}(Q)$
1	$\chi(Q)[4(-1)^f U + 2C] - 2A - 1 - 2(-3 \mid p)_4 X$
5	$4Y - 1$
7	$-2A - 1$
11	$2\chi(Q)C - 1$
13	$-2A - 1 - 2(-3 \mid p)_4 X$
17	$2\chi(Q)C + 4Y - 1$
19	$2\chi(Q)C - 2A - 1$
23	-1

To establish (6.8), consider for $e = 24$ the Eisenstein sum $\epsilon(\beta) = \Sigma_{i=0}^{23} a_i\beta^i = \Sigma_{i=0}^{11} d_i\beta^i$.

$$\epsilon(\beta^3) = \sum_{i=0}^{7} (a_i + a_{i+8} + a_{i+16})\beta^{3i} = \sum_{i=0}^{3} (d_i + d_{i+8} + d_{i+16})\beta^{3i}$$

is an Eisenstein sum of order 8.

According to (4.12),

$$\Theta_{12}(1) = -12d_0, \tag{6.9}$$

$$\Theta_4(1) = -4(d_0 + d_8 + d_{16}) = -4(d_0 - d_4 + d_8). \tag{6.10}$$

Let $y = 3,\ t = 1$ in (4.5):

$$\tau(\beta)\tau(\beta^9)\tau(\beta^{17}) = \psi^{-3}(3)\tau(\beta^3)\tau(\beta^8)\tau(\beta^{16}).$$

$$\tau(\beta^8)\tau(\beta^{16}) = -\tau(\beta^7)\tau(\beta^{17}). \qquad (4.1)$$

Since $p \equiv 11 \pmod{24}$, $\psi^{-3}(3) = \chi(3) = 1$. Thus

$$\tau(\beta)\tau(\beta^9)\tau(\beta^{17}) = -\tau(\beta^3)\tau(\beta^7)\tau(\beta^{17}).$$

$$\epsilon(\beta)\epsilon(\beta^9) = -\epsilon(\beta^3)\epsilon(\beta^7). \qquad (4.3)$$

Apply (4.9) with $s = 3$: $\epsilon(\beta) = -\epsilon(\beta^7)$.

If the Eisenstein sums of order 24 are expressed in terms of the basis $\{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7\}$ and the relationships

$$d_1 = d_{11},\ d_2 = -d_{10},\ d_3 = d_9,\ d_4 = -d_8,\ d_5 = d_7,\ d_6 = 0 \qquad (4.8) \tag{6.11}$$

are used, then

$$\epsilon(\beta) = (d_0 + d_4) + (d_1 - d_3)\beta + 2d_2\beta^2 + (d_3 - d_1)\beta^3$$
$$+ (d_5 + d_3)\beta^5 - d_2\beta^6 + (d_5 + d_1)\beta^7,$$
$$-\epsilon(\beta^7) = (-d_0 - d_4) + (-d_3 - d_5)\beta + 2d_2\beta^2 + (d_3 + d_5)\beta^3$$
$$+ (-d_1 + d_3)\beta^5 - d_2\beta^6 + (-d_1 - d_5)\beta^7.$$

Equate coefficients of 1: $d_0 + d_4 = -d_0 - d_4$. Hence $d_0 = -d_4$. Also, $d_8 = -d_4$, by (6.11). Substitute into (6.10): $\Theta_4(1) = -12d_0 = \Theta_{12}(1)$, by (6.9). This establishes (6.8).

Equating coefficients of β shows that $d_1 = -d_5$, so that

$$\epsilon(\beta) = (d_1 - d_3)(\beta - \beta^3 - \beta^5) + d_2(2\beta^2 - \beta^6) = -(d_1 - d_3)\sqrt{-2} + d_2\sqrt{3}.$$

Let $W = d_1 - d_3$, $V = d_2$. (4.4) implies that $\epsilon(\beta)\epsilon(\beta^{-1}) = p = 2W^2 + 3V^2$. Since an odd square is $\equiv 1 \pmod 8$ and $p \equiv 11 \pmod{24}$, $8 | 2W^2$, so W is even. Thus if $2U = W$, $p = 8U^2 + 3V^2$.

7. **Evaluations of $\Lambda_9(Q)$ and $\Lambda_{18}(Q)$.** For $p \equiv 3 \pmod 4$, $\Lambda_9(Q) = 0$, by (2.1).

$$2\Lambda_9(Q) = \Omega_9(Q) + \Theta_9(Q) = \Phi_{18}(Q^9) + \Theta_9(Q).$$

Applying the reduction formulas of §2 produces the following:

p (mod 36)	$\Phi_u(Q^9)$	$\Theta_v(Q)$
1	$\Phi_{18}(Q^9)$	$\Theta_1(Q^9)$
5, 29	$\Phi_2(Q^9)$	$\Theta_3(Q^3)$
13, 25	$\Phi_6(Q^9)$	$\Theta_1(Q^9)$
17	$\Phi_2(Q^9)$	$\Theta_9(Q)$

First consider $Q = 1$. The evaluations of $\Phi_2(1)$, $\Phi_6(1)$, $\Theta_1(1)$, and $\Theta_3(1)$ are given in (5.7), (6.7), (5.3), and (6.6), respectively. According to (3.22), $\Phi_{18}(1) = 18(-1)^f D_{36}(0, 18)$; this can be expressed in terms of a coordinate in a quadratic form of ten variables given by (3.30). There is also a more complicated expression for $\Phi_{18}(1)$ in terms of a coordinate of a form in six variables given by (3.35). The latter is developed here.

Let $H_0 = D_{36}(0, 18) + D_{36}(6, 18)$ denote the first coordinate of (3.35) with $e = 36$. Then

$$\begin{aligned}\Phi_{18}(1) &= (-1)^f[12D_{36}(0, 18) + 12D_{36}(6, 18)\\ &\qquad + 6D_{36}(0, 18) + 6D_{36}(12, 18) + 6D_{36}(24, 18)]\\ &= 12(-1)^f H_0 + \Phi_6(1),\end{aligned}$$

by (3.20), (3.14), and (3.22). Apply (6.7):

$$\Phi_{18}(1) = 12(-1)^f H_0 - 2X[1 + 2(-3|p)_4].$$

$$\Theta_9(1) = \Theta_{18}(1) = 18(-1)^f d_0, \quad \text{by (2.12) and (4.12).}$$

Although d_0 can be expressed in terms of a quadratic form in ten variables given by (4.15), a form in six variables given by (4.18) will be used.

Set $h_0 = d_0 + d_6$. h_0 is the first variable in (4.18) with $e = 36$.

$$\begin{aligned}\Theta_9(1) &= (-1)^f[12(d_0 + d_6) + 6(d_0 + d_{12} + d_{24})]\\ &= 12(-1)^f h_0 - (-1)^{f+(p+1-6)/12}\Theta_6(1)\end{aligned}$$

by (4.12). Since $f = (p + 1 - 18)/36$,

$$\Theta_9(1) = 12(-1)^f h_0 + \Theta_6(1) = 12(-1)^f h_0 + 8Y + 2X,$$

$$p \equiv 17 \pmod{36}. \qquad (2.12), (6.6)$$

Now let $Q = g$. By (2.5)

$$\Phi_6(g^9) = -\Phi_6(g^3), \qquad \Phi_2(g^9) = \Phi_2(g) = 4Y. \qquad (5.8)$$

Theorem 2 implies

$$\Theta_3(g^3) = -\Theta_3(g), \qquad \Theta_1(g^9) = \Theta_1(g) = -4Y. \qquad (5.3), (5.8)$$

$$2\Lambda_3(g) = \Phi_6(g^3) + \Theta_3(g),$$

by (2.3) and (2.4). If $p \equiv 1 \pmod{12}$,

$$-\Phi_6(g^3) = -2\Lambda_3(g) - \Theta_1(g). \qquad \text{(2.11), Theorem 2}$$

$$\text{(7.1)} \qquad \Phi_6(g^9) = -\Phi_6(g^3) = 4Y[1 - 2(-3\,|\,p)_4],$$

by (5.13), (5.3), and (5.8). If $p \equiv 5 \pmod{12}$,

$$-\Theta_3(g) = -2\Lambda_3(g) + \Phi_2(g^3). \qquad \text{Theorem 1}$$

$$\text{(7.2)} \qquad \Theta_3(g^3) = -\Theta_3(g) = 4(-3g\,|\,p)_4X - 4Y. \qquad \text{(5.12), (5.8)}$$

Theorem 4 yields, for $p \equiv 1 \pmod{36}$,

$$\Phi_{18}(g^9) = 18(-1)^fD_{36}(9, 18) = (-1)^f[12H_9 + 6D_{12}(9, 6)] = 12(-1)^fH_9 - \Phi_6(g^3),$$

where $H_9 = D_{36}(9, 18) + D_{36}(3, 18)$, by (3.14). By (7.1) $\Phi_{18}(g^9) = 12(-1)^fH_9 + 4Y[1 - 2(-3\,|\,p)_4]$.

If $p \equiv 17 \pmod{36}$, set $h_9 = d_9 + d_3$. By (4.13),

$$\begin{aligned}\Theta_9(g) &= 18(-1)^fd_9 = (-1)^f[12h_9 + 6(d_9 + d_{21} + d_{33})]\\ &= 12(-1)^fh_9 - \Theta_3(g) = 12(-1)^fh_9 - 4Y + 4(-3g\,|\,p)_4X. \qquad \text{(7.2)}\end{aligned}$$

Both H_9 and h_9 appear in quadratic decompositions of p in six variables, as the second term in (3.35) and (4.18), respectively.

The evaluation of $\Lambda_9(Q)$ can be summarized as follows:

$p \pmod{36}$	$\Lambda_9(1)$	$\Lambda_9(g)$
1	$6(-1)^fH_0 - 2X(-3\,|\,p)_4$	$6(-1)^fH_9 - 4Y(-3\,|\,p)_4$
5, 29	$4Y$	$2X(-3g\,|\,p)_4$
13, 25	$-2X(-3\,|\,p)_4$	$-4Y(-3\,|\,p)_4$
17	$6(-1)^fh_0 + 4Y$	$6(-1)^fh_9 + 2X(-3g\,|\,p)_4$

Comparing the above with (5.11), (5.12), and (5.13) reveals that $\Lambda_9(1) = \Lambda_3(1)$, $\Lambda_9(g) = -\Lambda_3(g)$, $p \not\equiv 1, 17 \pmod{36}$.

If n is odd, $\Lambda_{2n}(Q)$ can be expressed as follows. (See [16, Theorem 5.6].)

$$\begin{aligned}2\Lambda_{2n}(Q) &= \Omega_{2n}(Q) + \Theta_{2n}(Q) = \Psi_{4n}(Q^{2n}) + \Theta_n(Q^2), && \text{(2.3), (2.4), (2.12)}\\ &= \Psi_{2n}(Q^{2n}) + \Phi_{2n}(Q^{2n}) + \chi(Q)\Theta_n(1), && \text{(2.8), Theorem 2}\\ &= \Psi_{2n}(1) + \chi(Q)[\Phi_{2n}(1) + \Theta_n(1)], && \text{(2.5), (2.6)}\\ &= 2\Phi_n(1) + 2\chi(Q)\Lambda_n(1), && \text{(2.8), (2.9), (2.4), (2.3)}\end{aligned}$$

$$\text{(7.3)} \qquad \Lambda_{2n}(Q) = \Phi_d(1) + \chi(Q)\Lambda_n(1), \quad d = (p - 1, n). \qquad \text{Theorem 1}$$

Let $n = 9$.

$$\Phi_9(1) = \begin{cases} -1 & p \equiv 5 \pmod{6}, \qquad (5.2) \\ -1 - 2A, & p \equiv 7,\ 13 \pmod{18}, \qquad (6.5) \\ 9B_9(-2\,\mathrm{Ind}\,2,\ 1) - (p-1), & p \equiv 1 \pmod{18}. \qquad (3.21) \end{cases}$$

$B_9(-2\ \mathrm{Ind}\ 2,\ 1)$ appears in a six-variable quadratic decomposition of $4p$ given by (3.31) with $e = 9$.

$p \pmod{36}$	$\Lambda_{18}(Q)$
1	$9B_9(-2\,\mathrm{Ind}\,2,\ 1) - (p-1) + \chi(Q)[6(-1)^f H_0 - 2(-3 \mid p)_4 X]$
5, 29	$-1 + 4\chi(Q)Y$
7, 31	$-1 - 2A$
11, 23, 35	-1
13, 25	$-1 - 2A - 2\chi(Q)(-3 \mid p)_4 X$
17	$-1 + \chi(Q)[6(-1)^f b_0 + 4Y]$
19	$9B_9(-2\,\mathrm{Ind}\,2,\ 1) - (p-1)$

8. Evaluation of $\Lambda_7(Q)$ and $\Lambda_{14}(Q)$. For $p \equiv 3 \pmod 4$, $\Lambda_7(Q) = 0$, by (2.1).

$$2\Lambda_7(Q) = \Omega_7(Q) + \Theta_7(Q) = \Phi_{14}(Q^7) + \Theta_7(Q).$$

Assuming $p \equiv 1 \pmod 4$, apply the reduction procedures of §2:

$$\begin{aligned} \Phi_{14}(Q^7) &= \Phi_2(Q^7), && p \not\equiv 1 \pmod{28}, \\ \Theta_7(Q) &= \Theta_1(Q^7) = -\Phi_2(Q^7), && p \not\equiv 13 \pmod{28}. \qquad (5.3) \end{aligned}$$

If $p \equiv 1 \pmod{28}$, by (3.22),

$$\Phi_{14}(1) = 14(-1)^f D_{28}(0,\ 14).$$
$$\Phi_{14}(g^7) = -14(-1)^f D_{28}(21,\ 14) = 14(-1)^f D_{28}(7,\ 14),$$

by Theorem 4. According to (3.30) with $e = 28$, both $D_{28}(0,\ 14)$ and $D_{28}(7,\ 14)$ are coordinates in a quadratic decomposition of p in eight variables.

If $p \equiv 13 \pmod{28}$, (2.12) and (4.12) imply that

$$\Phi_7(1) = \Theta_{14}(1) = -14(-1)^f d_0 \cdot \Theta_7(g) = 14\chi(2) d_7 = -14(-1)^f d_7,$$

by (4.13). d_0 and d_7 are the first two coordinates in the eight-variable decomposition of p given by (4.15) with $e = 28$. Hence by (5.7) and (5.8),

$$\Lambda_7(1) = \begin{cases} X + 7(-1)^f D_{28}(0,\ 14), & p \equiv 1 \pmod{28}, \\ -X - 7(-1)^f d_0, & p \equiv 13 \pmod{28}, \\ 0, & \text{otherwise}, \end{cases}$$

$$\Lambda_7(g) = \begin{cases} 2Y + 7(-1)^f D_{28}(7, 14), & p \equiv 1 \pmod{28}, \\ -2Y - 7(-1)^f d_7, & p \equiv 13 \pmod{28}, \\ 0, & \text{otherwise.} \end{cases}$$

$$\Lambda_{14}(Q) = \chi(Q)\,\Lambda_7(1) + \Phi_d(1), \quad d = (p-1, 7). \qquad (7.3)$$

If $p \equiv 1 \pmod{14}$, $\Phi_7(1) = 7B_7(-2 \text{ Ind } 2, 1) - (p-1)$, by (3.21); otherwise $\Phi_1(1) = -1$, by (5.2). By (7.3):

$p \pmod{28}$	$\Lambda_{14}(Q)$
1	$7B_7(-2\,\text{Ind}\ 2, 1) - (p-1) + \chi(Q)[X + 7(-1)^f D_{28}(0, 14)]$
13	$-1 + \chi(Q)[-X - 7(-1)^f d_0]$
15	$7B_7(-2\,\text{Ind}\ 2, 1) - (p-1)$
otherwise	-1

$B_7(-2 \text{ Ind } 2, 1)$ is embedded in a six-variable quadratic decomposition of $72p$[8, (33)].

9. **Another expression for $\Lambda_{10}(Q)$.** The Jacobi sum $R_3(1, 1) = B_3(0, 1) + B_3(1, 1)\beta + B_3(2, 1)\beta^2$ is associated with the binary quadratic form

$$4p = L^2 + 27M^2, \quad L \equiv 1 \pmod 3): \tag{9.1}$$

$$L = 2B_3(0, 1) - B_3(1, 1) - B_3(2, 1), \quad 3M = B_3(1, 1) - B_3(2, 1). \quad [7, \text{p. } 397] \tag{9.2}$$

$R_5(1, 1) = \Sigma_{j=0}^4 B_5(j, 1)\beta^j$ is associated with the quaternary quadratic form

$$\begin{aligned} &16p = x^2 + 50u^2 + 50v^2 + 125w^2, \\ &\qquad\qquad xw = v^2 - u^2 - 4uv, \quad x \equiv 1 \pmod 5). \quad [7, \text{p. } 402] \end{aligned} \tag{9.3}$$

In studying Jacobi sums of order six one encounters a second binary quadratic form for primes $\equiv 1 \pmod 3$):

$$p = A^2 + 3B^2, \quad A \equiv 1 \pmod 3). \quad [7, \text{pp. } 408\text{–}410] \tag{9.4}$$

Relating this form, already alluded to in (5.18), to (9.1) involves the index of 2, modulo 3. However, in (9.4), p has a coefficient of 1. This form, furthermore, is used in evaluating $\Lambda_6(Q)$, $p \equiv 1 \pmod 3$). Notice that in (5.19) there is no reference to Ind 2.

By contrast, the evaluation of $\Lambda_{10}(Q)$ [16, (7.6)] which is expressed in terms of the coordinates of (9.3), has five cases, depending upon Ind 2 (mod 5). One may ask for another quaternary quadratic form for $p \equiv 1 \pmod 5$) which would provide a simpler expression for $\Lambda_{10}(Q)$. Such a form is developed here. (Attempts to generalize to $p \equiv 1 \pmod 7$) failed; an appropriate quadratic form in six variables was not discovered.)

Let $e = 5$. Define

$$t_j = B_5(j - 2\operatorname{Ind} 2,\ 1) - (p-1)/5; \qquad t_j = \Phi_5(g^j)/5, \tag{9.5}$$

by (3.21). By setting $n = 0$, $v = 1$ in (3.12) and comparing with (3.1) one may deduce that $\Sigma_{j=0}^{4} \beta_5(j,\ 1) = p - 2$;

$$t_0 + t_1 + t_2 + t_3 + t_4 = -1 \tag{9.6}$$

is an immediate consequence.

$$R_5(1,\ 1) = \sum_{i=0}^{4} B_5(i,\ 1)\beta^i$$

$$= \beta^{-2\operatorname{Ind} 2} \sum_{j=0}^{4} [B_5(j - 2\operatorname{Ind} 2,\ 1) - (p-1)/5]\beta^j = \beta^{-2\operatorname{Ind} 2} \sum_{j=0}^{4} t_j \beta^j.$$

Since, according to (3.4), $|R_5(1,\ 1)|^2 = p$, $|\Sigma_{j=0}^{4} t_j\beta^j|^2 = p$, so that

$$p = \sum_{j=0}^{4} t_j^2 - A, \tag{9.7}$$

$$A = t_0t_1 + t_1t_2 + t_2t_3 + t_3t_4 + t_4t_0 = t_0t_2 + t_1t_3 + t_2t_4 + t_3t_0 + t_4t_1.$$

Define

$$4X = 5t_0 + 1, \qquad 4U = t_1 + t_2 - t_3 - t_4,$$

$$4V = t_1 - t_2 + t_3 - t_4, \qquad 4W = t_1 - t_2 - t_3 + t_4.$$

Theorem 8. *X, U, V, and W are integers satisfying $X^2 + 5U^2 + 5V^2 + 5W^2 = p$, $XW = V^2 - U^2 - UV$.*

Proof. t_0 is odd, while t_1, t_2, t_3, and t_4 are even [15, p. 123]. From the last equation in (9.7) drop all products of two even numbers: $t_0(t_1 - t_2 - t_3 + t_4) \equiv 0 \pmod 4$. Since t_0 is odd, W is an integer. Then $U = W + (t_2 - t_4)/2$ and $V = W + (t_3 - t_4)/2$ are integers. Finally by (9.6), $X = t_0 - (t_1 + t_2 + t_3 + t_4)/4 = t_0 - W - (t_2 + t_3)/2$ is an integer. Now

$$X^2 + 5U^2 + 5V^2 + 5W^2 = [(4t_0 - t_1 - t_2 - t_3 - t_4)^2 + 5(t_1 + t_2 - t_3 - t_4)^2 + 5(t_1 - t_2 + t_3 - t_4)^2 + 5(t_1 - t_2 - t_3 + t_4)^2]/16$$

$$= \sum_{j=0}^{4} t_j^2 - \frac{1}{2} \sum_{j=0}^{3} \sum_{k=j+1}^{4} t_jt_k = p,$$

by (9.7).

To show that X, U, V, and W also satisfy $XW = V^2 - U^2 - UV$, solve for t_0, t_1, t_2, t_3, and t_4 in terms of X, U, V, W, and a constant and substitute into the last equation in (9.7).

$$\Lambda_{10}(Q) = \chi(Q)\Lambda_5(1) + \Phi_d(1), \qquad d = (p-1, 5). \qquad (7.3)$$

If $p \not\equiv 1 \pmod{10}$, $\Phi_1(1) = -1$, by (5.2). If $p \equiv 1 \pmod{10}$, $\Phi_5(1) = 5t_0$, by (9.5). Thus

$$\Lambda_{10}(Q) = \chi(Q)\Lambda_5(1) + \begin{cases} 4X - 1, & p \equiv 1 \pmod{10}, \\ -1, & \text{otherwise.} \end{cases}$$

$\Lambda_5(1)$ was given by Brewer [1]. X satisfies the equations in Theorem 8. Its sign is chosen so that $X \equiv 4 \pmod 5$. That X is thus defined uniquely can be deduced from [7, Theorem 8].

10. **Conclusion.** The evaluations of Brewer sums presented here may serve as a guide to the evaluation of Brewer sums of other orders by means of cyclotomy. There may be extensions in other directions, as suggested by [3].

This paper is comprised of the principal contributions of the dissertation of the first author, completed under the direction of the second, several results of the latter, and results from the dissertation, completed under Professor Albert L. Whiteman, of the third author with subsequent extensions.

The formulation of many of the theorems in this paper was aided considerably by studying tables of various character sums. We wish to express our gratitude to the University of Pittsburgh Computer Center for granting access to its IBM 7090/1401 system, partially supported by National Science Foundation grant G-11309.

BIBLIOGRAPHY

1. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. 99 (1961), 241–245. MR 22 #10959.

2. ———, *On primes of the form $u^2 + 5v^2$*, Proc. Amer. Math. Soc. 17 (1966), 502–509. MR 32 #5610.

3. P. Chowla, *A new proof and generalization of some theorems of Brewer*, Norske Vid. Selsk. Forh. (Trondheim) 41 (1968), 1–3. MR 40 #5574.

4. S. Chowla, *A formula similar to Jacobsthal's for the explicit value of x in $p = x^2 + y^2$ where p is a prime of the form $4k+1$*, Proc. Lahore Philos. Soc. 7 (1945), 2 pp. MR 7, 243.

5. ———, *The last entry in Gauss's diary*, Proc. Nat. Acad. Sci. U.S.A. 35 (1949), 244–246. MR 10, 592.

6. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 57 (1934), 151–182.

7. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.

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

9. ———, *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), 187–200.

10. G. Eisenstein, *Zur Theorie der quadratischen Zerfallung der Primzahlen* $8n+3$, $7n+2$ *und* $7n+4$, J. Reine Angew. Math. 37 (1848), 97–126.

11. E. Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n+1$ *als Summe zweier Quadrate*, J. Reine Angew. Math. 132 (1907), 238–245.

12. E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacific J. Math. 5 (1955), 103–118. MR 16, 798.

13. W. J. LeVeque, *Topics in number theory*. Vol. I, Addison-Wesley, Reading, Mass., 1956. MR 18, 283.

14. J. B. Muskat, *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. 134 (1968), 483–502. MR 38 #1075.

15. T. Pepin, *Mémoire sur les lois de réciprocité relatives aux résidues de puissances*, Pontif. Accad. Sci. Rome 31 (1877), 40–148.

16. S. F. Robinson, *Theorems on Brewer sums*, Pacific J. Math. 25 (1968), 587–596. MR 37 #2706.

17. L. von Schrutka, *Eine Beweis für die Zerlegbarkeit der Primzahlen von der Form* $6n+1$ *in ein einfaches und ein dreifaches Quadrat*, J. Reine Angew. Math. 140 (1911), 256–265.

18. L. Stickelberger, *Über eine Verallgemeinerung der Kreisteilung*, Math. Ann. 37 (1890), 321–367.

19. H. Walum, *Finite Fourier series and Jacobsthal sums*, Dissertation, University of Colorado, Boulder, Col., 1962.

20. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Indust., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann, Paris, 1948. (2ième partie, IV). MR 10, 262.

21. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), 89–99. MR 13, 626.

22. ———, *The sixteenth power residue character of* 2, Canad. J. Math. 6 (1954), 364–373. MR 16, 14.

23. ———, *The cyclotomic numbers of order ten*, Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, R. I., 1960, pp. 95–111. MR 22 #4682.

24. ———, *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), 53–76. MR 22 #9480.

25. ———, *A theorem of Brewer on character sums*, Duke Math. J. 30 (1963), 545–552. MR 27 #4801.

26. ———, *Theorems on Brewer and Jacobsthal sums*. I, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R. I., 1965, pp. 49–55. MR 31 #137.

27. ———, *Theorems on Brewer and Jacobsthal sums*. II, Michigan Math. J. 12 (1965), 65–80. MR 36 #132.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PITTSBURGH, PITTSBURGH, PENNSYLVANIA 15213

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90007

DEPARTMENT OF MATHEMATICS, UNIVERSIDAD TECHNICA FEDERICO, SANTA MARIA, VALPARAISO, CHILE (Current address of R. E. Giudici)

DEPARTMENT OF MATHEMATICS, EASTERN WASHINGTON STATE COLLEGE, CHENEY, WASHINGTON 99004 (Current address of S. F. Robinson)

DEPARTMENT OF MATHEMATICS, BAR-ILAN UNIVERSITY, RAMAT-GAN, ISRAEL (Current address of J. B. Muskat)