ILLINOIS JOURNAL OF MATHEMATICS
Volume 23, Number 3, September, 1979

SUMS OF GAUSS, EISENSTEIN, JACOBI, JACOBSTHAL, AND BREWER

BY
BRUCE C. BERNDT AND RONALD J. EVANS

1. Introduction

In [1], we evaluated certain Gauss, Jacobi, and Jacobsthal sums over the finite field $GF(p)$, where p is an odd prime. One of the main objects of this paper is to evaluate such sums over $GF(p^2)$.

In Chapter 2, we give the basic theorems which relate the sums of Eisenstein, Gauss, Jacobi, and Jacobsthal. In Chapter 3, Jacobi sums associated with characters on $GF(p)$ of orders 5, 10, and 16 are evaluated, and the values of certain Jacobsthal sums over $GF(p)$ are determined. The formulae for these Jacobi sums and the Jacobi sums evaluated in [1] are utilized in Chapter 4, wherein we evaluate Jacobi and Eisenstein sums associated with characters on $GF(p^2)$ of orders 3, 4, 5, 6, 8, 10, 12, 16, 20, and 24. All of the evaluations in Chapters 3 and 4 are effected in terms of parameters that appear in the representations of the primes p as binary or quartic integral quadratic forms.

Many of the results of Chapters 3 and 4 are new, but some have been obtained elsewhere by the use of the theory of cyclotomic numbers. (In particular, see [7].) In contrast, our approach is via Jacobi and Eisenstein sums, as in [1] and [15]. For our purposes, this approach is perhaps simpler and more natural.

Another goal of this paper is to give a self-contained, systematic treatment of Brewer character sums. Several Brewer sums have been evaluated in the literature by a variety of methods. In Section 5.2, we develop a unified theory of Brewer sums. In particular, we express generalized Brewer sums $\Lambda_n(a)$ in terms of Jacobsthal sums over $GF(p)$ and Eisenstein sums, and so generalize a theorem of Robinson [23]. Our proofs do not depend upon the theory of cyclotomy, as do most existing proofs and explicit determinations. In Section 5.3, we apply our theory to give mostly new proofs of known formulae for $\Lambda_n(a)$ when $n = 1, 2, 3, 4, 5, 6, 8, 10$, and 12.

In Chapter 6, using primarily Theorem 2.7 and the formulae for Jacobi sums in Chapter 4, we evaluate certain Jacobsthal sums over $GF(p^2)$. In Chapter 7, using primarily Theorem 2.12 and the formulae for Eisenstein sums in Chapter 4, we evaluate the Gauss sums $\mathcal{G}_k = \sum_{\alpha \in GF(p^2)} e^{2\pi i \operatorname{tr}(\alpha^k)/p}$, for $k = 2, 3, 4, 6, 8$, and 12. Most of the results of Chapters 6 and 7 appear to be new.

Received December 6, 1977.

The beautiful Hasse–Davenport theorem on products of Gauss sums [4], [9, p. 464] is often useful in evaluating character sums. For example, it is used by Giudici, Muskat, and Robinson [7, p. 340] to evaluate the Brewer sum $\Lambda_{12}(a)$. In this paper, only a very special case of the Hasse–Davenport theorem is used, namely Theorem 2.3, for which a very elementary proof exists. In Chapter 8, we show how to obtain an elementary proof in other special cases.

This paper makes heavy use of the results in [1], but together with [1], forms an almost completely self-contained unit. Moreover, the methods are for the most part elementary. The only non-elementary result used is Stickelberger's theorem [11, pp. 94, 97], for the purpose of evaluating certain bidecic and biduodecic Jacobi and Eisenstein sums in Chapter 4.

2. Notation and general theorems

Let Q denote the field of rational numbers. Given a primitive complex mth root of unity ζ and an integer t with $(t, m)=1$, define $\sigma_t \in Gal(Q(\zeta)/Q)$ by $\sigma_t(\zeta)=\zeta^t$. Let Ω denote the ring of all algebraic integers.

Throughout the first 7 chapters, p denotes an odd prime, and χ, ψ, λ, and Λ denote characters on $GF(p^r)$, where $GF(p^r)$ denotes a field of p^r elements. We also let $GF(p^r)^*=GF(p^r)-\{0\}$. The quadratic character on $GF(p^r)$ is denoted by ϕ. If χ is a character on $GF(p^r)$ with $r\geq 2$, then the restriction of χ to $GF(p)$ will be denoted by χ_1. The symbols $\sum_\alpha$ and $\sum_{\alpha\neq\beta}$ indicate that the sum is over all the elements α in $GF(p^r)$ and $GF(p^r)-\{\beta\}$, respectively. When a Roman letter is used to denote an element of $GF(p^r)$ instead of a Greek letter, it will always be the case that $r=1$.

The Gauss sum $G_r(\chi)$ is defined by

$$G_r(\chi)=\sum_\alpha \chi(\alpha)e^{2\pi i\,\mathrm{tr}(\alpha)/p},$$

where $\mathrm{tr}(\alpha)=\mathrm{tr}\,\alpha=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{r-1}}$. If χ is nonprincipal, $G_r(\chi)$ satisfies the fundamental property [10, p. 132]

$$G_r(\chi)G_r(\bar{\chi})=\chi(-1)p^r. \tag{2.1}$$

The Jacobi sum $J_r(\chi, \psi)$ is defined by

$$J_r(\chi, \psi)=\sum_\alpha \chi(\alpha)\psi(1-\alpha).$$

Put $J_r(\chi, \chi)=J_r(\chi)$ and $K_r(\chi)=\chi(4)J_r(\chi)$. We drop the subscript r from G_r, J_r, and K_r when $r=1$. The following two results are basic properties of Jacobi sums [10, pp. 93, 133].

THEOREM 2.1. *If χ is nonprincipal, we have $J_r(\chi, \bar{\chi}) = -\chi(-1)$.*

THEOREM 2.2. *If χ, ψ, and $\chi\psi$ are nonprincipal, then*

$$J_r(\chi, \psi) = \frac{G_r(\chi)G_r(\psi)}{G_r(\chi\psi)}.$$

In particular, by (2.1), $|J_r(\chi, \psi)| = p^{r/2}$.

The following two theorems are proved in [1] for $r = 1$; the proofs of the more general results follow along precisely the same lines. Theorem 2.3 is a special case of a theorem of Davenport and Hasse [4], [9, p. 464] which will be further discussed in Chapter 8.

THEOREM 2.3. *If χ is nonprincipal, we have $K_r(\chi) = J_r(\chi, \phi)$.*

THEOREM 2.4. *Let χ have even order $2k$. Then*

(i) $K_r(\chi) = \phi(-1)K_r(\chi^{k-1})$,
(ii) $K_r(\chi) = \chi(-1)J_r(\chi, \chi^{k-1})$.

The following result is well known and easily proved [8, p. 82].

LEMMA 2.5. *Let $f(x) = ax^2 + bx + c$, where a, b, and c are integers. Let $d = b^2 - 4ac$. Then if $p \nmid ad$,*

$$\sum_n \left(\frac{f(n)}{p}\right) = -\left(\frac{a}{p}\right).$$

Let n be a positive integer and let $\beta \in GF(p^r)^*$. The Jacobsthal sum $\phi_{n,r}(\beta) = \phi_n(\beta)$ is defined by

$$\phi_n(\beta) = \sum_\alpha \phi(\alpha)\phi(\alpha^n + \beta).$$

Define a related sum $\psi_{n,r}(\beta) = \psi_n(\beta)$ by

$$\psi_n(\beta) = \sum_\alpha \phi(\alpha^n + \beta).$$

The proofs of the following three results follow along the same lines as the proofs for $r = 1$ [1, Chapter 2].

THEOREM 2.6. *For each natural number n, we have $\psi_{2n}(\beta) = \phi_n(\beta) + \psi_n(\beta)$.*

THEOREM 2.7. *Let χ have order $2n$. Then*

$$\phi_n(\beta) = \chi(-1) \sum_{j=0}^{n-1} \chi^{n+2j+1}(\beta)K_r(\chi^{2j+1}).$$

THEOREM 2.8. *Let χ have order $2n$. Then*

$$\psi_n(\beta) = \phi(\beta) \sum_{i=1}^{n-1} \chi^{2i}(\beta)K_r(\chi^{2i}).$$

In the remainder of this chapter, $r=2$, and so χ is a character on $GF(p^2)$. Fix a generator τ of the cyclic group $GF(p^2)^*$ and write $\gamma=\tau^{(p+1)/2}$ and $g=\gamma^2$. Observe that g is a primitive root (mod p) and that $\gamma^p=-\gamma$. We also have $GF(p^2)=\{a+b\gamma\colon a, b\in GF(p)\}$.

LEMMA 2.9. *If χ has order m, then χ_1 has order $m/(m, p+1)$. In particular, if $m \mid (p+1)$, then χ_1 is principal, and if $m \mid 2(p+1)$ but $m \nmid (p+1)$, then χ_1 is the quadratic character* (mod p).

Proof. Since χ has order m, $\chi(\tau)$ is a primitive mth root of unity. Hence, $\chi_1(g)=\chi(\tau^{p+1})$ is a primitive $m/(m, p+1)$th root of unity. Q.E.D.

The Eisenstein sum $E(\chi)$ associated with the character χ on $GF(p^2)$ is defined by

$$E(\chi)=\sum_{b=0}^{p-1}\chi(1+b\gamma).$$

We now establish some properties of $E(\chi)$.

THEOREM 2.10. *We have $E(\chi)=E(\chi^p)$.*

Proof. Since $(1+b\gamma)^p=1+b^p\gamma^p=1-b\gamma$ for all $b\in GF(p)$,

$$E(\chi)=\sum_b\chi(1-b\gamma)=\sum_b\chi^p(1+b\gamma)=E(\chi^p). \qquad \text{Q.E.D.}$$

THEOREM 2.11. *Let χ have order m, where $m>1$ and $m \mid (p+1)$. Then*

$$E(\chi)=-\chi(\gamma)=-(-1)^{(p+1)/m}.$$

Proof. Since $\chi(\tau)$ is a primitive mth root of unity, $\chi(\gamma)=\chi(\tau^{(p+1)/2})$ is a primitive $m/(m, (p+1)/2)$th root of unity. This proves the second equality.

Since, by Lemma 2.9, χ_1 is principal,

$$\begin{aligned}
0&=\sum_\alpha\chi(\alpha)\\
&=\sum_{a,b=0}^{p-1}\chi(a+b\gamma)\\
&=\sum_{b=0}^{p-1}\chi(b\gamma)+\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\chi(a+b\gamma)\\
&=\chi(\gamma)\sum_{b=0}^{p-1}\chi_1(b)+\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\chi(a+ab\gamma)\\
&=(p-1)\chi(\gamma)+E(\chi)\sum_{a=1}^{p-1}\chi(a)\\
&=(p-1)\{\chi(\gamma)+E(\chi)\},
\end{aligned}$$

from which the desired result follows. Q.E.D.

THEOREM 2.12. *Let χ have order m. Then*

$$\begin{aligned} G_2(\chi) &= \bar{\chi}(2)E(\chi)G(\chi_1) && \text{if } m \nmid (p+1), \\ &= p\chi(\gamma) = p(-1)^{(p+1)/m} && \text{if } m>1 \text{ and } m \mid (p+1), \\ &= -1 && \text{if } m=1. \end{aligned}$$

Proof. Let $\alpha \in GF(p^2)$. Then $\alpha = a+b\gamma$ for some pair $a, b \in GF(p)$, and $\operatorname{tr} \alpha = \alpha + \alpha^p = 2a$. Hence,

$$\begin{aligned} G_2(\chi) &= \sum_{a,b=0}^{p-1} \chi(a+b\gamma)e^{4\pi i a/p} \\ &= \sum_{b=0}^{p-1} \chi(b\gamma) + \sum_{a=1}^{p-1}\sum_{b=0}^{p-1} \chi(a+ab\gamma)e^{4\pi i a/p} \\ &= \chi(\gamma)\sum_{b=0}^{p-1} \chi_1(b) + E(\chi)\sum_{a=1}^{p-1} \chi(a)e^{4\pi i a/p} \\ &= \chi(\gamma)\sum_{b=0}^{p-1} \chi_1(b) + \bar{\chi}(2)E(\chi)G(\chi_1). \end{aligned}$$

The result now follows from Lemma 2.9 and Theorem 2.11. Q.E.D.

Results similar to Theorems 2.10, 2.11, and 2.12 have been proved by Whiteman [30, p. 69]. See also [7, pp. 330–331].

COROLLARY 2.13. *Let χ have order m, where $m \nmid (p+1)$. Then $|E(\chi)| = \sqrt{p}$.*

Proof. The result is an immediate consequence of Lemma 2.9, Theorem 2.12, and (2.1). Q.E.D.

THEOREM 2.14. *Let χ have order m. Then*

$$\begin{aligned} K_2(\chi) &= p^2-2, && \text{if } m=1, \\ &= -1, && \text{if } m=2, \\ &\ p, && \text{if } m>2 \text{ and } m \mid (p+1), \\ &= -\left(\frac{-1}{p}\right)E^2(\chi), && \text{if } m \mid 2(p+1) \text{ but } m \nmid (p+1), \\ &= \frac{E^2(\chi)}{E(\chi^2)}K(\chi_1), && \text{if } m \nmid 2(p+1). \end{aligned}$$

Proof. Proceeding by a standard argument [10, pp. 93, 94], we have

$$\begin{aligned} G_2^2(\chi) &= \sum_{\alpha} \chi(\alpha)e^{2\pi i \operatorname{tr}(\alpha)/p} \sum_{\beta} \chi(\beta)e^{2\pi i \operatorname{tr}(\beta)/p} \\ &= \sum_{\alpha,\beta} \chi(\alpha\beta)e^{2\pi i \operatorname{tr}(\alpha+\beta)/p} \\ &= \sum_{\rho} \left\{ \sum_{\alpha+\beta=\rho} \chi(\alpha\beta) \right\} e^{2\pi i \operatorname{tr}(\rho)/p} \\ &= G_2(\chi^2)J_2(\chi) + \chi(-1)\sum_{\alpha} \chi^2(\alpha). \end{aligned}$$

The result now follows from Lemma 2.9 and Theorem 2.12, with the use of Theorem 2.2 in the case $m \nmid 2(p+1)$. Q.E.D.

The last two cases of Theorem 2.14 can be consolidated into the one case

$$K_2(\chi)=\frac{E^2(\chi)}{E(\chi^2)}K(\chi_1) \quad \text{if} \quad m \nmid (p+1). \tag{2.2}$$

To see this, first observe that when $m \mid 2(p+1)$ but $m \nmid (p+1)$, χ_1 has order 2. Thus, by Theorem 2.1, $K(\chi_1)=-\left(\frac{-1}{p}\right)$. Also, observe that, by Theorem 2.11, $E(\chi^2)=1$.

The following useful result is due to J. Muskat, and we are grateful for his permission to include it here.

THEOREM 2.15. *Let χ have even order $m=2n$ with $m \nmid (p+1)$. Then*

$$E(\chi^{n-1})=(-1)^{(p+1)/2}\frac{E(\chi)}{E(\chi^2)}K(\chi_1).$$

Proof. Let $R=E(\chi^{n-1})E(\chi^2)/E(\chi)$. First, suppose that $n \nmid (p+1)$. By Theorem 2.12,

$$E(\chi)=\chi(2)G_2(\chi)/G(\chi_1), \quad E(\chi^2)=\chi^2(2)G_2(\chi^2)/G(\chi_1^2)$$

and

$$E(\chi^{n-1})=\chi^{n-1}(2)G_2(\chi^{n-1})/G(\chi_1^{n-1}).$$

Thus,

$$\begin{aligned} R&=\chi^n(2)\frac{G_2(\chi^{n-1})G_2(\chi^{n+1})G_2(\chi^2)}{G_2(\chi)G_2(\chi^{n+1})}\frac{G(\chi_1)G(\chi_1)}{G(\chi_1^{n-1})G(\chi_1)G(\chi_1^2)}\\ &=\chi^n(2)\frac{\chi(-1)p^2G_2(\chi^2)}{G_2(\chi)G_2(\chi^{n+1})}\frac{J(\chi_1)}{\chi_1(-1)p}, \end{aligned}$$

by (2.1). By Theorem 2.3,

$$\chi(4)\frac{G_2^2(\chi)}{G_2(\chi^2)}=\frac{G_2(\chi)G_2(\phi)}{G_2(\chi^{n+1})},$$

or

$$G_2(\chi)G_2(\chi^{n+1})=\bar{\chi}(4)G_2(\phi)G_2(\chi^2).$$

Thus, by the above and Theorem 2.12,

$$R=\frac{\chi^{n+2}(2)pJ(\chi_1)}{G_2(\phi)}=\frac{\chi^{n+2}(2)pJ(\chi_1)}{p(-1)^{(p+1)/2}}=(-1)^{(p+1)/2}K(\chi_1).$$

This proves the theorem for $n \nmid (p+1)$.

Suppose next that $n \mid (p+1)$. Note that $p+1 \equiv n \pmod{2n}$, for if not, then $2n \mid (p+1)$, which is a contradiction. Thus, $E(\chi^{n-1}) = E(\chi^p)$, so $E(\chi^{n-1}) = E(\chi)$ by Theorem 2.10. By Theorem 2.11 and the above considerations, we then have $R = E(\chi^2) = -(-1)^{(p+1)/n} = 1$. By Lemma 2.9, χ_1 has order 2. Thus, by Theorem 2.1,

$$K(\chi_1) = J(\chi_1) = -\chi_1(-1) = (-1)^{(p+1)/2}.$$

This completes the proof. Q.E.D.

THEOREM 2.16. *Let χ have order m with $m \nmid (p+1)$. Then $E(\chi^{p+1}) = -K(\chi_1)$.*

Proof. First, for $b \in GF(p)$, note that $(1+b\gamma)^p = 1 - b\gamma$. Thus,

$$\begin{aligned} E(\chi^{p+1}) &= \sum_b \chi^p(1+b\gamma)\chi(1+b\gamma) \\ &= \sum_b \chi(1-b\gamma)\chi(1+b\gamma) \\ &= \sum_b \chi_1(1-gb^2) \\ &= \sum_n \chi_1(n)\left\{1 + \left(\frac{g^{-1}(1-n)}{p}\right)\right\}, \end{aligned}$$

since the expression in braces counts the number of solutions $b \pmod p$ to $1 - gb^2 \equiv n \pmod p$. By Lemma 2.9, χ_1 is nonprincipal, and so

$$E(\chi^{p+1}) = \sum_n \chi_1(n)\left(\frac{g(1-n)}{p}\right) = -\sum_n \chi_1(n)\left(\frac{1-n}{p}\right) = -K(\chi_1),$$

by Theorem 2.3. Q.E.D.

We will find it convenient to define

$$T(\chi) = \operatorname{card}\{1 + b\gamma \colon b \in GF(p), \chi(1+b\gamma) = 1\}.$$

Thus, if χ has order m, $T(\chi)$ is the number of mth power residues in $GF(p^2)$ of the form $1+b\gamma$ with $b \in GF(p)$. Observe that $T(\chi)$ is odd, since if $\chi(1+b\gamma) = 1$, then $\chi(1-b\gamma) = \chi^p(1+b\gamma) = 1$. (In the notation of [7, p. 331], $T(\chi) = a_0$.) The next result is similar to a result in [7, equation (4.6)].

THEOREM 2.17. *If χ has order m, then $T(\chi) = (1/m)\sum_{j=0}^{m-1} E(\chi^j)$.*

Proof. We have

$$\sum_{j=0}^{m-1} E(\chi^j) = \sum_{b=0}^{p-1} \sum_{j=0}^{m-1} \chi^j(1+b\gamma) = mT(\chi). \qquad \text{Q.E.D.}$$

In Chapter 4, we will record evaluations of $T(\chi)$ in a few interesting cases.

3. Jacobi and Jacobsthal sums over $GF(p)$

3.1. Quintic and decic Jacobi sums

THEOREM 3.1. *Let* $p \equiv 1 \pmod{10}$, *and let* χ *be a character* $(\bmod p)$ *of order* 10. *Then*

$$\left(\frac{-1}{p}\right)K(\chi) = a_{10} + b_{10}\sqrt{5} + ic_{10}\sqrt{5+2\sqrt{5}} + id_{10}\sqrt{5-2\sqrt{5}}, \tag{3.1}$$

where a_{10}, b_{10}, c_{10}, *and* d_{10} *are integers such that*

(i) $a_{10} \equiv -1 \pmod 5$,
(ii) $a_{10}^2 + 5b_{10}^2 + 5c_{10}^2 + 5d_{10}^2 = p$,
(iii) $a_{10}b_{10} = d_{10}^2 - c_{10}^2 - c_{10}d_{10}$.

Furthermore, (ii) *and* (iii) *determine* $|a_{10}|$, $|b_{10}|$, *and* $\{|c_{10}|, |d_{10}|\}$ *uniquely.*

Proof. Let $\zeta = \exp(2\pi i/10)$, and note that

$$i\sqrt{5+2\sqrt{5}} = \zeta - \bar{\zeta} + \zeta^2 - \bar{\zeta}^2 \quad \text{and} \quad i\sqrt{5-2\sqrt{5}} = -\zeta + \bar{\zeta} + \zeta^2 - \bar{\zeta}^2, \tag{3.2}$$

It is easily seen that $\{1, \sqrt{5}, i\sqrt{5+2\sqrt{5}}, i\sqrt{5-2\sqrt{5}}\}$ is a basis for $Q(\zeta)$ over Q. Hence, the representation (3.1) immediately follows, where a_{10}, b_{10}, c_{10}, and d_{10} are rational numbers such that (ii) and (iii) hold.

We now show that a_{10}, b_{10}, c_{10}, and d_{10} are integers. We have

$$\begin{aligned} K(\chi) + K(\chi^6) &= \sum_{n=2}^{p-1} \chi(4n(1-n))\left\{1 + \left(\frac{4n(1-n)}{p}\right)\right\} \\ &= 2 \sum_{\substack{n=2 \\ \phi(n(1-n))=1}}^{p-1} \chi(4n(1-n)) \\ &= 2 + 4 \sum_{\substack{n=2 \\ \phi(n(1-n))=1}}^{(p-1)/2} \chi(4n(1-n)). \end{aligned} \tag{3.3}$$

By Theorem 2.4(i),

$$K(\chi^6) = \left(\frac{-1}{p}\right)K(\bar{\chi}).$$

Thus, if $\left(\frac{-1}{p}\right) = 1$, we deduce from (3.3) that $\operatorname{Re} K(\chi) - 1 \in 2\Omega$; if $\left(\frac{-1}{p}\right) = -1$, we deduce that $i \operatorname{Im} K(\chi) - 1 \in 2\Omega$. Hence, if $\left(\frac{-1}{p}\right) = -1$, then

$$p - \{\operatorname{Re} K(\chi)\}^2 + 1 = \{\operatorname{Im} K(\chi)\}^2 + 1 \in 4\Omega,$$

and so $\operatorname{Re} K(\chi)\in 2\Omega$. Since, by (3.1),

$$\operatorname{Re} K(\chi)=\left(\frac{-1}{p}\right)(a_{10}+b_{10}\sqrt{5}),$$

and since all algebraic integers in $Q(\sqrt{5})$ have the form $a+b\sqrt{5}$, where either a and b are integers or both $2a$ and $2b$ are odd integers, it follows, in either case, that a_{10} and b_{10} are integers. Therefore, by (3.1), we have

$$\alpha\equiv c_{10}\sqrt{5+2\sqrt{5}}+d_{10}\sqrt{5-2\sqrt{5}}\in\Omega.$$

Since

$$\alpha\sqrt{5+2\sqrt{5}}=5c_{10}+(2c_{10}+d_{10})\sqrt{5}, \tag{3.4}$$

either $5c_{10}$ and $(2c_{10}+d_{10})$ are both integers, or $10c_{10}$ and $2(2c_{10}+d_{10})$ are both odd integers. Letting $N\beta$ denote the norm of an algebraic integer β, we have $N(\sqrt{5+2\sqrt{5}})=5$. Thus, by (3.4), $5\mid N\{2(5c_{10}+(2c_{10}+d_{10})\sqrt{5})\}$, and so $5\mid 10c_{10}$. Hence, $2c_{10}$ is an integer. Consequently, $2d_{10}$ is also an integer. From (ii),

$$4(p-a_{10}^2-5b_{10}^2)=5\{(2c_{10})^2+(2d_{10})^2\}.$$

If $2c_{10}$ were odd, this would yield the contradiction that $0\equiv 1+(2d_{10})^2 \pmod 4$. Thus, $2c_{10}$ is even, i.e., c_{10} is an integer. From (ii), it follows that d_{10} is also an integer.

Raising each side of (3.1) to the fifth power and employing Theorem 2.1, we get

$$-1=\left(\frac{-1}{p}\right)K(\chi^5)\equiv a_{10} \pmod{5\Omega}.$$

Thus, $a_{10}\equiv -1 \pmod 5$. The last statement of the theorem on uniqueness follows from a theorem of Muskat and Zee [17]. Q.E.D.

COROLLARY 3.2. *Let $p\equiv 1 \pmod{10}$, and let χ be a character $\pmod p$ of order 10. Suppose that 2 is not a quintic residue $\pmod p$. Then*

$$4\left(\frac{-1}{p}\right)J(\chi)=A+B\sqrt{5}+4iC\sin(2\pi/5)+4iD\sin(\pi/5),$$

where A, B, C, and D are integers such that $A\equiv 1 \pmod 5$ and $A^2+5B^2+10C^2+10D^2=16p$ with $AB=D^2-C^2-4CD$.

Proof. Suppose, for example, that $\chi(4)=\bar{\zeta}^2$, where $\zeta=\exp(2\pi i/10)$. (The proofs for the remaining three cases are completely analogous.) By Theorem 3.1 and (3.2),

$$\left(\frac{-1}{p}\right)J(\chi)=\zeta^2\{a_{10}+b_{10}\sqrt{5}+c_{10}(\zeta-\bar{\zeta}+\zeta^2-\bar{\zeta}^2)+d_{10}(-\zeta+\bar{\zeta}+\zeta^2-\bar{\zeta}^2)\}.$$

Using the facts that $\cos(\pi/5) = (\sqrt{5}+1)/4$ and $\cos(2\pi/5) = (\sqrt{5}-1)/4$, we find, after some manipulation, that

$$(3.5) \qquad 4\left(\frac{-1}{p}\right)J(\chi) = A + B\sqrt{5} + 4iC\sin(2\pi/5) + 4iD\sin(\pi/5),$$

where A, B, C, and D are integers with $A = -a_{10} + 5b_{10} - 5c_{10} - 5d_{10}$. By Theorem 3.1, $A \equiv 1 \pmod 5$. Since $\sin(2\pi/5) = \sqrt{10+2\sqrt{5}}/4$ and $\sin(\pi/5) = \sqrt{10-2\sqrt{5}}/4$, we deduce from (3.5) that $16p = A^2 + 5B^2 + 10C^2 + 10D^2$, where $AB = D^2 - C^2 - 4CD$. Q.E.D.

The representation for p given in Theorem 3.1 is due to Giudici, Muskat, and Robinson [7, p. 345]. The proof given here is more self-contained and less computational than that of [7]. Corollary 3.2 gives a representation for $16p$ found by Dickson [6, p. 402]. In this connection, see also a paper of Whiteman [27, p. 98].

By Theorem 2.4(i),

$$K(\chi) = \left(\frac{-1}{p}\right)K(\chi^4) \quad \text{and} \quad K(\chi^3) = \left(\frac{-1}{p}\right)K(\chi^2).$$

Hence, Theorem 3.1 yields the values of quintic as well as decic Jacobi sums.

3.2. Bioctic Jacobi sums

LEMMA 3.3. *Let $p \equiv 1 \pmod 8$. Then $2a_4 + 4a_8 \equiv p - 7 \pmod{32}$, where a_4 and a_8 are defined in* [1, *Theorems* 3.9 *and* 3.12].

Proof. Let

$$\eta = 1, \quad \text{if 2 is a quartic residue} \pmod p,$$
$$= -1, \quad \text{otherwise.}$$

By [1, Theorems 3.14 and 3.16], we have

$$a_4 \equiv (p-3)/2 + 4(1-\eta) \pmod{16} \quad \text{and} \quad a_8 \equiv 6\eta + 1 \pmod 8).$$

Thus, $2a_4 + 4a_8 \equiv 16\eta + p + 9 \equiv p - 7 \pmod{32}$. Q.E.D.

LEMMA 3.4. *Let c and d be rational, and let*

$$\alpha = c\sqrt{2+\sqrt{2}} + d\sqrt{2-\sqrt{2}} \in \Omega.$$

Then c and d are integers.

Proof. First, $2c + \sqrt{2}(c+d) = \alpha\sqrt{2+\sqrt{2}} \in \Omega$. Thus, $2c$ and $c+d$ are integers. Assume that c and d are not integers. Then both $2c$ and $2d$ are odd integers. Since the norm of $\alpha\sqrt{2+\sqrt{2}}$ is even, we see that $4c^2 - 2(c+d)^2$ is even. Thus,

$$(2c)^2-(2d)^2-2(2c)(2d)\equiv 0 \pmod 4.$$

Since $2c$ and $2d$ are odd, the above congruence yields $2\equiv 0 \pmod 4$, which is absurd. Thus, c and d are integers. Q.E.D.

THEOREM 3.5. *Let* $p\equiv 1 \pmod{16}$, *and let* χ *be a character* $(\bmod p)$ *of order* 16. *Then*

$$K(\chi)=a_{16}+b_{16}\sqrt{2}+ic_{16}\sqrt{2+\sqrt{2}}+id_{16}\sqrt{2-\sqrt{2}}, \tag{3.6}$$

where a_{16}, b_{16}, c_{16}, *and* d_{16} *are integers such that*

(i) $a_{16}\equiv -1 \pmod 8$,
(ii) $a_{16}^2+2b_{16}^2+2c_{16}^2+2d_{16}^2=p$,
(iii) $2a_{16}b_{16}=d_{16}^2-c_{16}^2-2c_{16}d_{16}$.

Furthermore, b_{16}, c_{16}, *and* d_{16} *are even, and* (ii) *and* (iii) *determine* $|a_{16}|$, $|b_{16}|$, *and* $\{|c_{16}|, |d_{16}|\}$ *uniquely.*

Proof. Observe that $2\cos(\pi/8)=\sqrt{2+\sqrt{2}}$. It is then easily seen that the subgroup $\langle\sigma_7\rangle\subset Gal(Q(e^{2\pi i/16})/Q)$ has fixed field $Q(i\sqrt{2+\sqrt{2}})$. By Theorem 2.4(i), σ_7 fixes $K(\chi)$, and so $K(\chi)\in Q(i\sqrt{2+\sqrt{2}})$. Now $\{1, \sqrt{2}, i\sqrt{2+\sqrt{2}}, i\sqrt{2-\sqrt{2}}\}$ form a basis for $Q(i\sqrt{2+\sqrt{2}})$ over Q. Thus, we immediately conclude that $K(\chi)$ has the representation given in (3.6), where a_{16}, b_{16}, c_{16}, and d_{16} are rational numbers such that (ii) and (iii) hold.

We next show that a_{16}, b_{16}, c_{16}, and d_{16} are integral. Now,

$$\sum_{j=0}^{15} K(\chi^j)=16\,|S|, \tag{3.7}$$

where $S=\{n: 0\le n\le p-1, \chi(4n(1-n))=1\}$. Since $\sigma_3(\sqrt{2})=-\sqrt{2}$, it follows from (3.6) that $\mathrm{Re}\{K(\chi)+K(\chi^3)\}=2a_{16}$. By Theorem 2.4(i), $K(\chi)=K(\chi^7)$ and $K(\chi^3)=K(\chi^5)$. By Theorem 2.1, $K(\chi^8)=-1$. Using also the evaluations of quartic and octic Jacobi sums from [1, Theorems 3.9 and 3.12], we deduce from (3.7) that

$$16\,|S|=8a_{16}+4a_8+2a_4+p-3. \tag{3.8}$$

By Lemma 3.3 and (3.8),

$$16\,|S|\equiv 8a_{16}-8 \pmod{32}. \tag{3.9}$$

Now, the transformation $n\to 1-n$ leaves $\chi(4n(1-n))$ unchanged. Since $n\not\equiv 1-n \pmod p$ except when $n\equiv (p+1)/2 \pmod p$, we see that $16\,|S|\equiv 16 \pmod{32}$. Thus, by (3.9),

$$a_{16}\equiv -1 \pmod 4. \tag{3.10}$$

Proceeding as in (3.3), we find that

$$2\,\mathrm{Re}\,K(\chi)=K(\chi)+K(\chi^9)=2+4\sum_{\substack{n=2\\ \phi(n(1-n))=1}}^{(p-1)/2}\chi(4n(1-n)).$$

Thus, $\mathrm{Re}\,K(\chi)-1\in 2\Omega$, and so by (3.6), $a_{16}-1+b_{16}\sqrt{2}\in 2\Omega$. Since $a_{16}-1$ is even by (3.10), we conclude that b_{16} is an integer. Thus, by (3.6), $c_{16}\sqrt{2+\sqrt{2}}+d_{16}\sqrt{2-\sqrt{2}}\in\Omega$. Hence, by Lemma 3.4, c_{16} and d_{16} are integers. Since $a_{16}^2\equiv p\equiv 1 \pmod 8$ by (3.10), it follows from (ii) that c_{16} and d_{16} are even. Furthermore, using (iii) and (3.10), we have

$$\begin{aligned}2b_{16}^2+2c_{16}^2+2d_{16}^2&=2b_{16}^2+2(d_{16}^2-2c_{16}d_{16}-2a_{16}b_{16})+2d_{16}^2\\&\equiv 2b_{16}^2+4b_{16}\equiv 0 \pmod{16}.\end{aligned}$$

Thus, by (ii), $a_{16}^2\equiv 1 \pmod{16}$. Hence, by (3.10), $a_{16}\equiv -1 \pmod 8$. The claim on uniqueness at the end of the theorem was established by Muskat and Zee [17]. Q.E.D.

THEOREM 3.6. *Let* $p\equiv 1 \pmod{16}$ *and write* $p=a_{16}^2+2b_{16}^2+2c_{16}^2+2d_{16}^2$ *with* $2a_{16}b_{16}=d_{16}^2-c_{16}^2-2c_{16}d_{16}$. *Then*

$$\begin{aligned}b_{16}&\equiv 0 \pmod 4, &&\textit{if 2 is a quartic residue} \pmod p,\\&\equiv 2 \pmod 4, &&\textit{otherwise.}\end{aligned}$$

Proof. Let χ be a character $(\mathrm{mod}\ p)$ of order 16. We may assume that a_{16} and b_{16} are as given in (3.6). By Theorem 2.4(i), $K(\bar{\chi})=K(\chi^9)$. Hence, by Theorem 2.3,

$$\begin{aligned}2(a_{16}+b_{16}\sqrt{2})&=2\,\mathrm{Re}\,K(\chi)\\&=K(\chi)+K(\chi^9)\\&=\sum_{n=1}^{p-1}\chi(n)\left(\frac{1-n}{p}\right)\left\{1+\left(\frac{n}{p}\right)\right\}\\&=\sum_{n=1}^{p-1}\chi^2(n)\left(\frac{1-n^2}{p}\right).\end{aligned}$$

Let $\psi=\chi^2$. Since $\psi(-1)=1$, it again follows from Theorem 2.3 that

$$\begin{aligned}2(a_{16}+b_{16}\sqrt{2})&=\sum_{n=1}^{p-1}\psi(n)\left(\frac{1-n}{p}\right)\left(\frac{1+n}{p}\right)\\&=-2K(\psi)+\sum_{n=1}^{p-1}\psi(n)\left\{1+\left(\frac{1-n}{p}\right)\right\}\left\{1+\left(\frac{1+n}{p}\right)\right\}\\&=4-2K(\psi)+2\sum_{n=2}^{(p-1)/2}\psi(n)\left\{1+\left(\frac{1-n}{p}\right)\right\}\left\{1+\left(\frac{1+n}{p}\right)\right\}.\end{aligned}$$

Thus, $a_{16}+b_{16}\sqrt{2}\equiv 2-K(\psi) \pmod{4\Omega}$. By [1, Theorem 3.12], $K(\psi)=a_8+ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2+2b_8^2=p$ and $a_8\equiv -1 \pmod 4$, and by Theorem 3.5, $a_{16}\equiv -1 \pmod 4$. Hence,

$$b_{16}\sqrt{2}\equiv 2-a_8-a_{16}-ib_8\sqrt{2}\equiv -ib_8\sqrt{2} \pmod{4\Omega}.$$

The result now follows from [1, Theorem 3.15]. Q.E.D.

3.3. Jacobsthal sums

THEOREM 3.7. *Let $p=10k+1$ and $p \nmid a$. Suppose that χ is a character* (mod p) *of order* 10, *and assume that χ is chosen such that $\chi^2(a)=e^{2\pi i/5}$ in the case that a is a quintic nonresidue* (mod p). *Then, in the notation of* (3.1),

$$\begin{aligned}\phi_5(a)&=-1+4a_{10}, && \text{if } a \text{ is a quintic residue} \pmod p,\\ &=-1-a_{10}-5b_{10}+5c_{10}-5d_{10}, && \text{otherwise.}\end{aligned}$$

Proof. For $\sigma_3\in Gal(Q(e^{2\pi i/10})/Q)$, we have $\sigma_3(\sqrt{5})=-\sqrt{5}$. Furthermore, by (3.2), $\sigma_3(i\sqrt{5+2\sqrt{5}})=i\sqrt{5-2\sqrt{5}}$ and $\sigma_3(i\sqrt{5-2\sqrt{5}})=-i\sqrt{5+2\sqrt{5}}$. Thus, by Theorem 3.1,

$$(-1)^kK(\chi)=a_{10}+b_{10}\sqrt{5}+ic_{10}\sqrt{5+2\sqrt{5}}+id_{10}\sqrt{5-2\sqrt{5}} \tag{3.11}$$

and

$$(-1)^kK(\chi^3)=a_{10}-b_{10}\sqrt{5}+ic_{10}\sqrt{5-2\sqrt{5}}-id_{10}\sqrt{5+2\sqrt{5}}. \tag{3.12}$$

Using (3.11), (3.12), and Theorem 2.1 in Theorem 2.7, we obtain

$$\begin{aligned}\phi_5(a)&=(-1)^k\{2\operatorname{Re}\{\bar\chi^4(a)K(\chi)+\bar\chi^2(a)K(\chi^3)\}+K(\chi^5)\}\\ &=2\operatorname{Re}\{\bar\chi^4(a)(a_{10}+b_{10}\sqrt{5}+ic_{10}\sqrt{5+2\sqrt{5}}+id_{10}\sqrt{5-2\sqrt{5}})\\ &\quad+\bar\chi^2(a)(a_{10}-b_{10}\sqrt{5}+ic_{10}\sqrt{5-2\sqrt{5}}-id_{10}\sqrt{5+2\sqrt{5}})\}-1.\end{aligned}$$

The desired evaluations of $\phi_5(a)$ now follow. The computations are facilitated by the use of (3.2). Q.E.D.

THEOREM 3.8. *With the hypotheses and notations of Theorem* 3.7, *we have*

$$\begin{aligned}\psi_5(a)&=4\left(\frac{a}{p}\right)a_{10}, && \text{if } a \text{ is a quintic residue} \pmod p,\\ &=\left(\frac{a}{p}\right)\{-a_{10}-5b_{10}-5c_{10}+5d_{10}\}, && \text{otherwise.}\end{aligned}$$

Proof. From (3.11), (3.12), and Theorem 2.4(i), we get

$$K(\chi^2)=(-1)^kK(\chi^3)=a_{10}-b_{10}\sqrt{5}+ic_{10}\sqrt{5-2\sqrt{5}}-id_{10}\sqrt{5+2\sqrt{5}}$$

and

$$K(\chi^4) = (-1)^k K(\chi) = a_{10} + b_{10}\sqrt{5} + ic_{10}\sqrt{5+2\sqrt{5}} + id_{10}\sqrt{5-2\sqrt{5}}.$$

Thus, by Theorem 2.8,

$$\psi_5(a) = 2\left(\frac{a}{p}\right) \operatorname{Re}\{\chi^2(a)(a_{10} - b_{10}\sqrt{5} + ic_{10}\sqrt{5-2\sqrt{5}} - id_{10}\sqrt{5+2\sqrt{5}})$$

$$+ \chi^4(a)(a_{10} + b_{10}\sqrt{5} + ic_{10}\sqrt{5+2\sqrt{5}} + id_{10}\sqrt{5-2\sqrt{5}})\}.$$

The desired values for $\psi_5(a)$ now follow. Q.E.D.

With the use of Theorem 2.6, $\psi_{10}(a)$ can also be evaluated. A less elementary proof of Theorem 3.8 has been given by Rajwade [19], [20]. (See also [22].) Theorem 3.8 extends results of E. Lehmer [12] and Whiteman [26], [27].

In the next theorem, columns indicate the residuacity of a. For example, if an x appears in the column headed by "quartic", it is assumed that a is a quartic residue (mod p); if no x appears in the column headed by "quartic", it is assumed that a is a quartic nonresidue (mod p).

THEOREM 3.9. *Let $p = 16k+1$ and suppose that $p \nmid a$. Let χ be a character* (mod p) *of order* 16 *chosen so that*

$$\bar{\chi}(a) = e^{2\pi i/16}, \quad \text{if } \left(\frac{a}{p}\right) = -1,$$

$$= e^{2\pi i/8}, \quad \text{if } \left(\frac{a}{p}\right) = 1 \quad \text{but } a \text{ is not a 4th power} \pmod p.$$

Then, in the notation of Theorem 3.5, *we have the following table of values for* $(-1)^k\phi_8(a)$.

$(-1)^k\phi_8(a)$	*quadratic*	*quartic*	*octic*	*bioctic*
$8a_{16}$	x	x	x	x
$-8a_{16}$	x	x	x	
0	x	x		
$8b_{16}$	x			
$-8d_{16}$				

Proof. By Theorem 2.4(i) and (3.6), we have

$$K(\chi) = K(\chi^7) = a_{16} + b_{16}\sqrt{2} + ic_{16}\sqrt{2+\sqrt{2}} + id_{16}\sqrt{2-\sqrt{2}}. \tag{3.13}$$

Applying $\sigma_3 \in Gal(Q(e^{2\pi i/16})/Q)$ to (3.13), we have

$$K(\chi^3) = K(\chi^5) = a_{16} - b_{16}\sqrt{2} - ic_{16}\sqrt{2-\sqrt{2}} + id_{16}\sqrt{2+\sqrt{2}}.$$

Therefore, by Theorem 2.7,

$$(-1)^k \phi_8(a) = 2\,\mathrm{Re}\,\{\bar{\chi}(a)(1+\bar{\chi}^6(a))K(\chi)\} + 2\,\mathrm{Re}\,\{\bar{\chi}^3(a)(1+\bar{\chi}^2(a))K(\chi^3)\},$$

and the results follow. Q.E.D.

With the use of Theorems 2.6 and 3.9 and the values of $\psi_8(a)$ found in [1, Theorem 4.7], $\psi_{16}(a)$ may be evaluated. In certain cases, a more explicit evaluation of $\phi_8(a)$ has been given [6].

4. Jacobi and Eisenstein sums over $GF(p^2)$

In this chapter, $r=2$, and so χ and λ are characters on $GF(p^2)$.

4.1 Quartic and octic sums. First, we consider the case $p=8k+1$. Let λ have order 16. Then λ_1 has order 8 by Lemma 2.9. As in [1, Theorem 3.12], write $K(\lambda_1) = a_8 + ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2 + 2b_8^2 = p$ and $a_8 \equiv -1 \pmod 4$. As in [1, Theorem 3.9], write $K(\lambda_1^2) = a_4 + ib_4$, where a_4 and b_4 are integers such that $a_4^2 + b_4^2 = p$ and $a_4 \equiv -\left(\frac{2}{p}\right) = -1 \pmod 4$. In the next theorem, we evaluate the octic sums $E(\lambda^2)$ and $K_2(\lambda^2)$ and the quartic sums $E(\lambda^4)$ and $K_2(\lambda^4)$.

THEOREM 4.1. *Let* $p=8k+1$, *and let* λ *have order* 16. *Write* $\chi=\lambda^2$. *Then in the notation above,*

(i) $E(\chi) = -a_8 + i(-1)^{k+1}b_8\sqrt{2}$ and $E(\chi^2) = -K(\chi_1) = -a_4 - ib_4$;
(ii) $K_2(\chi) = -E^2(\chi)$ *and* $K_2(\chi^2) = -K^2(\chi_1)$.

Proof. Part (ii) follows from part (i) and Theorem 2.14.

To prove (i), first observe that by Theorem 2.16, $E(\chi^2) = E(\chi^{p+1}) = -K(\chi_1)$. It remains to evaluate $E(\chi)$. By Theorem 2.16,

$$\begin{aligned} -a_8 - ib_8\sqrt{2} = -K(\lambda_1) = E(\lambda^{p+1}) &= E(\lambda^2), \quad \text{if } 2 \mid k, \\ &= E(\lambda^{10}), \quad \text{if } 2 \nmid k. \end{aligned}$$

In the case that $2 \mid k$, this is the desired result. In the case that $2 \nmid k$, replace λ by λ^5 to obtain $E(\chi) = -K(\lambda_1^5)$. Hence, by Theorem 2.4(i), $E(\chi) = -K(\bar{\lambda}_1)$. Q.E.D.

COROLLARY 4.2. *Let* $p=8k+1$, *and let* χ *have order* 8. *Then*

$$T(\chi) = \tfrac{1}{8}(p+1-2a_4-4a_8).$$

Proof. By applying Theorem 2.4(i) to $K(\lambda_1)$, we deduce from Theorem 4.1 that $E(\chi)=E(\chi^3)$. Thus, by Theorems 2.11, 2.17, and 4.1,

$$8T(\chi)=p+1+E(\chi^2)+E(\bar{\chi}^2)+2E(\chi)+2E(\bar{\chi})=p+1-2a_4-4a_8.$$

Q.E.D.

COROLLARY 4.3. *Let $p=8k+1$, and let χ have order 8. Then $T(\chi)\equiv$ 1 (mod 4).*

Proof. The result follows from Corollary 4.2 and Lemma 3.3. Q.E.D.

We now consider the case $p=8k+5$. Let χ have order 8. Then χ_1 has order 4 by Lemma 2.9. As in [1, Theorem 3.9], write $K(\chi_1)=a_4+ib_4$, where a_4 and b_4 are integers such that $a_4^2+b_4^2=p$ and $a_4\equiv-\left(\frac{2}{p}\right)=1 \pmod 4$.

THEOREM 4.4. *Let $p=8k+5$, and let χ have order 8. Then in the notation above,*

(i) $E(\chi)=-E(\chi^2)=K(\bar{\chi}_1)=a_4-ib_4$;
(ii) $K_2(\chi)=-p$ *and* $K_2(\chi^2)=-K^2(\bar{\chi}_1)$.

Proof. Part (ii) follows from (i) and Theorem 2.14.

To prove (i), first observe that by Theorem 2.16, $E(\bar{\chi}^2)=E(\chi^{p+1})=-K(\chi_1)$. Thus,

$$-E(\chi^2)=K(\bar{\chi}_1). \tag{4.1}$$

It remains to evaluate $E(\chi)$.

The subgroup $\langle\sigma_5\rangle$ of $Gal(Q(e^{2\pi i/8})/Q)=\{\sigma_5,\sigma_{-5},\sigma_1,\sigma_{-1}\}$ has fixed field $Q(i)$. Since σ_5 fixes $E(\chi)$ by Theorem 2.10, $E(\chi)\in Q(i)$. In particular, $A=\operatorname{Re}E(\chi)$ is an integer. By Theorem 2.11, $E(\chi^4)=1$. Thus, by (4.1), Theorem 2.17, and the fact that $E(\chi)=E(\chi^5)$,

$$8T(\chi)=p+1-2a_4+4A. \tag{4.2}$$

If A were even, (4.2) would yield the contradiction that $0\equiv 4 \pmod 8$. Thus, A is odd. Since $E(\chi)\in Q(i)$, it follows that

$$E(\chi)\in\{\pm K(\chi_1),\pm K(\bar{\chi}_1)\}.$$

Assume for the purpose of contradiction that $E(\chi)=\pm K(\chi_1)$. Then by (4.1) and Theorem 2.14,

$$K_2(\chi)=E^2(\chi)K(\chi_1)/E(\chi^2)=K^4(\chi_1)/p,$$

which contradicts the fact that $K^4(\chi_1)/p\notin\Omega$. Hence, $E(\chi)=\varepsilon K(\bar{\chi}_1)$, where $\varepsilon=\pm1$. It remains to show that $\varepsilon=1$.

By (4.2), $8T(\chi)=8k+6+2a_4(2\varepsilon-1)$. Since $T(\chi)$ is odd, we have

$$8\equiv 8k+6+2a_4(2\varepsilon-1) \pmod{16},$$

and so

$$1-4k \equiv a_4(2\varepsilon-1) \pmod 8. \tag{4.3}$$

If $a_4 \equiv 5-4k \pmod 8$, then

$$b_4^2 = p - a_4^2 \equiv 8k+5-(9-8k) \equiv -4 \pmod{16},$$

a contradiction. Hence, $a_4 \equiv 1-4k \pmod 8$, and so $\varepsilon = 1$ by (4.3). Q.E.D.

COROLLARY 4.5. *Let $p = 8k+5$, and let χ have order 8. Then,*

$$T(\chi) = \tfrac{1}{8}(p+1+2a_4).$$

Proof. Since $A = \operatorname{Re} E(\chi) = a_4$ by Theorem 4.4, the result follows from (4.2). Q.E.D.

We finally consider the case $p = 8k+3$. The quartic sums are trivially evaluated since $4 \mid (p+1)$, and so we evaluate only octic sums below.

THEOREM 4.6. *Let $p = 8k+3$, and let χ have order 8. Then:*

(i) $E(\chi) = a_8 + ib_8\sqrt{2}$, *where a_8 and b_8 are integers such that $a_8^2 + 2b_8^2 = p$ and $a_8 \equiv (-1)^k \pmod 4$;*
(ii) $K_2(\chi) = E^2(\chi)$.

Proof. Part (ii) follows from Theorem 2.14.

To prove (i), first observe that the subgroup $\langle\sigma_3\rangle$ of $Gal(Q(e^{2\pi i/8})/Q) = \{\sigma_3, \sigma_{-3}, \sigma_1, \sigma_{-1}\}$ has fixed field $Q(i\sqrt{2})$. Since σ_3 fixes $E(\chi)$ by Theorem 2.10, $E(\chi) \in Q(i\sqrt{2})$. Therefore $E(\chi) = a_8 + ib_8\sqrt{2}$ for some integers a_8 and b_8 such that $a_8^2 + 2b_8^2 = p$.

By Theorems 2.11 and 2.17 and the fact that $E(\chi) = E(\chi^3)$,

$$8T(\chi) = p+1+4a_8. \tag{4.4}$$

Since $T(\chi)$ is odd, $8 \equiv 8k+4+4a_8 \pmod{16}$, from which it follows that $a_8 \equiv 1-2k \equiv (-1)^k \pmod 4$. Q.E.D.

COROLLARY 4.7. *Let $p = 8k+3$, and let χ have order 8. Then*

$$T(\chi) = \tfrac{1}{8}(p+1+4a_8),$$

where a_8 is defined in Theorem 4.6.

Proof. This follows from (4.4). Q.E.D.

We remark that $T(\chi)$ is easily evaluated for octic χ when $p \equiv 7 \pmod 8$, for it can be seen from Theorems 2.11 and 2.17 that when χ has order m and $p = mk-1$, then

$$\begin{aligned} T(\chi) &= k, && \text{if } 2 \nmid k, \\ &= k-1, && \text{if } 2 \mid k. \end{aligned}$$

4.2. Cubic, sextic, and duodecic sums. First, we consider the case $p = 12k+1$. Let λ have order 24. Then λ_1 has order 12 by Lemma 2.9. As in [1, Theorem 3.9], write $K(\lambda_1^3) = a_4 + ib_4$, where a_4 and b_4 are integers such that $a_4^2 + b_4^2 = p$ and $a_4 \equiv (-1)^{k+1} \pmod 4$. As in [1, Theorem 3.19], write $K(\lambda_1) = a_{12} + ib_{12}$, where $a_{12} = a_4$ and $b_{12} = b_4$, if $3 \nmid a_4$, and $a_{12} = -a_4$ and $b_{12} = -b_4$, if $3 \mid a_4$. As in [1, Theorem 3.3], write $K(\lambda_1^2) = K(\lambda_1^4) = a_3 + ib_3\sqrt{3}$, where a_3 and b_3 are integers such that $a_3^2 + 3b_3^2 = p$ and $a_3 \equiv -1 \pmod 3$.

THEOREM 4.8. *Let $p = 12k+1$, and let λ have order 24. Write $\chi = \lambda^2$. Then in the notation above,*

(i)
$$E(\chi^4) = E(\chi^2) = -K(\chi_1) = -a_3 - ib_3\sqrt{3} \quad \textit{and} \quad E(\chi) = -a_{12} + i(-1)^{k+1} b_{12};$$

(ii)
$$K_2(\chi^4) = K_2(\chi^2) = -K^2(\chi_1) \quad \textit{and} \quad K_2(\chi) = -E^2(\chi);$$

(iii)
$$\begin{aligned} E(\chi) &= E(\chi^3), && \textit{if } 3 \nmid a_4, \\ &= -E(\chi^3), && \textit{if } 3 \mid a_4, \end{aligned}$$

and

$$K_2(\chi) = K_2(\chi^3).$$

Proof. The proofs of (i) and (ii) are similar to those of Theorem 4.1, and so we omit them. Using (i) and (ii) in conjunction with Theorems 4.1 and 4.4, we see that (iii) holds. Q.E.D.

We now consider the case $p = 12k+7$. Let χ have order 12. Then χ_1 has order 3 by Lemma 2.9. As in [1, Theorem 3.3], write $K(\chi_1) = a_3 + ib_3\sqrt{3}$, where a_3 and b_3 are integers such that $a_3^2 + 3b_3^2 = p$ and $a_3 \equiv -1 \pmod 3$.

THEOREM 4.9. *Let $p = 12k+7$, and let χ have order 12. Then in the notation above,*

(i) $(-1)^k E(\chi) = E(\chi^2) = -E(\chi^4) = K(\bar{\chi}_1) = a_3 - ib_3\sqrt{3}$;
(ii) $K_2(\chi) = p$ *and* $K_2(\chi^2) = K_2(\chi^4) = -K^2(\bar{\chi}_1)$.

Proof. Part (ii) follows from part (i) and Theorem 2.14.
To prove (i), we first observe that by Theorem 2.16,

$$E(\chi^4) = E(\chi^{2(p+1)}) = -K(\chi_1^2) = -K(\bar{\chi}_1), \tag{4.5}$$

as desired. By Theorem 2.15, with χ^2 in place of χ, we have

$$E(\chi^4) = E(\chi^2)K(\bar{\chi}_1)/E(\chi^4).$$

Thus, by (4.5),

$$E(\chi^2) = K(\bar{\chi}_1). \tag{4.6}$$

It remains to evaluate $E(\chi)$. Apply Theorem 2.15 and multiply both sides of the equality obtained therefrom by $E^2(\chi^2)E(\chi^7)$ to get

$$E^2(\chi^2)E(\chi^5)E(\chi^7) = E(\chi)E(\chi^7)E(\chi^2)K(\chi_1).$$

Applying Theorem 2.10, Corollary 2.13, and (4.6), we find that the above reduces to $E^2(\chi^2)p = E^2(\chi)p$. By (4.6), this last equality implies that $E(\chi) = \varepsilon K(\bar{\chi}_1)$, where $\varepsilon = \pm 1$. Cubing both sides of the latter equality, we find that

$$E(\chi^3) \equiv \varepsilon a_3^3 \equiv -\varepsilon \pmod{3\Omega}.$$

By Theorem 2.11, $E(\chi^3) = (-1)^{k+1}$. Hence, $\varepsilon = (-1)^k$, as desired. Q.E.D.

We finally consider the case $p = 12k+5$. The cubic and sextic sums are trivially evaluated since $6 \mid (p+1)$; thus, we evaluate only the duodecic sums in Theorem 4.10.

Let λ have order 24. Then λ_1 has order 4 by Lemma 2.9. As in [1, Theorem 3.9], write $K(\lambda_1) = a_4 + ib_4$, where a_4 and b_4 are integers such that $a_4^2 + b_4^2 = p$ and $a_4 \equiv (-1)^k \pmod 4$. Observe that $3 \nmid a_4$ and $3 \nmid b_4$, since $a_4^2 + b_4^2 = p \equiv -1 \pmod 3$.

THEOREM 4.10. *Let $p = 12k+5$, and let λ have order 24. Write $\chi = \lambda^2$. Then in the notation above,*

(i) $E(\chi) = \varepsilon_0 i E(\chi^3) = (-1)^k \varepsilon_0 b_4 - \varepsilon_0 i a_4,$

where $\varepsilon_0 = \varepsilon_0(\chi)$ is defined by $\varepsilon_0 = \pm 1$ and $\varepsilon_0 \equiv (-1)^{k+1} a_4 b_4 \pmod 3$. In other words, $E(\chi) = B - Ai$, where $B = \pm b_4$, $B \equiv -a_4 \pmod 3$, $A = \pm a_4$, and $A \equiv (-1)^{k+1} b_4 \pmod 3$.

(ii) $K_2(\chi) = -E^2(\chi) = -K_2(\chi^3).$

Proof. The first equality in (ii) follows from Theorem 2.14. Since $K_2(\chi^3) = -E^2(\chi^2)$ by Theorems 4.1 and 4.4, the second equality follows from part (i).

To prove (*i*) first observe that the subgroup $\langle \sigma_5 \rangle$ of $Gal(Q(e^{2\pi i/12})/Q) = \{\sigma_5, \sigma_{-5}, \sigma_1, \sigma_{-1}\}$ has fixed field $Q(i)$. Since σ_5 fixes $E(\chi)$ by Theorem 2.10, we have $E(\chi) \in Q(i)$. Thus, $E(\chi) = B - Ai$ for some integers A and B.

By Theorem 2.11, $E(\chi^6) = E(\chi^2) = E(\chi^{10}) = 1$ and $E(\chi^4) = E(\chi^8) = -1$. Noting also that $E(\chi) = E(\chi^5)$, we obtain, from Theorem 2.17, $12T(\chi) = p + 1 + 4B + 2\,\mathrm{Re}\, E(\chi^3)$. By Theorem 2.16,

$$\begin{aligned} E(\chi^3) = E(\lambda^6) = E(\lambda^{p+1}) &= -K(\lambda_1) = -a_4 - ib_4, \quad \text{if } 2 \mid k, \\ = E(\bar{\lambda}^{p+1}) &= -K(\bar{\lambda}_1) = -a_4 + ib_4, \quad \text{if } 2 \nmid k. \end{aligned}$$

Hence,

$$E(\chi^3) = -a_4 + i(-1)^{k+1} b_4. \tag{4.7}$$

Thus, $12T(\chi) = 12k + 6 + 4B - 2a_4$. Since $T(\chi)$ is odd,

$$12 \equiv 12k + 6 + 4B - 2a_4 \pmod{24},$$

which implies that $-1 + 2k + a_4 \equiv 2B \pmod 4$. Since $a_4 \equiv (-1)^k \equiv 1 - 2k \pmod 4$, we deduce that $0 \equiv 2B \pmod 4$, i.e., B is even. It follows that $iE(\chi) = A + Bi$, where A is odd. Hence, by (4.7), $iE(\chi) \in \{\pm E(\chi^3), \pm E(\bar{\chi}^3)\}$.

If $E(\chi)=\pm iE(\bar{\chi}^3)$, we find upon cubing each side that $E(\chi^3)\equiv \pm iE(\chi^3) \pmod{3\Omega}$, which is impossible. Thus,

$$E(\chi)=i\varepsilon E(\chi^3), \tag{4.8}$$

where $\varepsilon=\pm 1$. Cubing both sides of (4.8), we get $E(\chi^3)\equiv -i\varepsilon E(\bar{\chi}^3) \pmod{3\Omega}$. Thus, by (4.7),

$$-a_4+i(-1)^{k+1}b_4\equiv i\varepsilon a_4+(-1)^k\varepsilon b_4 \pmod{3\Omega}.$$

Comparing real parts, we find that $\varepsilon\equiv(-1)^{k+1}a_4b_4 \pmod 3$. The result now follows from (4.7) and (4.8). Q.E.D.

4.3. Biduodecic sums. First, we consider the case $p=24k+1$. Let λ have order 48. Then λ_1 has order 24 by Lemma 2.9. As in [1, Theorem 3.22], write $K(\lambda_1)=a_{24}+ib_{24}\sqrt{6}$, where a_{24} and b_{24} are integers such that $a_{24}^2+6b_{24}^2=p$ and $a_{24}\equiv a_8 \pmod 3$. (Here, a_8 is defined as in [1, Theorem 3.12].) The proof of the following theorem is similar to that of Theorem 4.1, and so we omit it.

THEOREM 4.11. *Let $p=24k+1$, and let λ have order 48. Write $\chi=\lambda^2$. Then, in the notation above,*

(i) $E(\chi)=-a_{24}+i(-1)^{k+1}b_{24}\sqrt{6}$;
(ii) $K_2(\chi)=-E^2(\chi)$.

We next consider the case $p=24k+7$.

THEOREM 4.12. *Let $p=24k+7$, and let χ have order 24. Then*

(i) $E(\chi)=a_{24}+ib_{24}\sqrt{6}$, *where a_{24} and b_{24} are integers such that $a_{24}^2+6b_{24}^2=p$ and $a_{24}\equiv(-1)^k \pmod 3$;*

(ii) $K_2(\chi)=E^2(\chi)$.

Proof. By Lemma 2.9, χ_1 has order 3. Thus, by Theorem 4.9(i),

$$E(\chi^2)=K(\bar{\chi}_1^2)=K(\chi_1). \tag{4.9}$$

Hence, part (ii) follows from Theorem 2.14.

By Theorem 2.15 and (4.9), $E(\chi^{11})=E(\chi)$. By Theorem 2.10, $E(\chi)=E(\chi^7)$. Thus, $E(\chi)$ is in the fixed field $Q(i\sqrt{6})$ of the subgroup $\langle\sigma_7,\sigma_{11}\rangle$ of $Gal(Q(e^{2\pi i/24})/Q)$. Therefore, we may write

$$E(\chi)=a_{24}+ib_{24}\sqrt{6}, \tag{4.10}$$

where a_{24} and b_{24} are integers such that $a_{24}^2+6b_{24}^2=p$. Therefore, cubing both sides of (4.10) and using Theorem 2.11, we obtain $(-1)^k=E(\chi^3)\equiv a_{24} \pmod 3$. Q.E.D.

We next consider the case $p=24k+13$. Let χ have order 24; then χ_1 has order 12 by Lemma 2.9. As at the beginning of Section 4.2, write $K(\chi_1)=a_{12}+ib_{12}$.

THEOREM 4.13. *Let $p = 24k + 13$, and let χ have order 24. Then, in the notation above,*

(i) $E(\chi) = K(\bar{\chi}_1) = a_{12} - ib_{12}$,
(ii) $K_2(\chi) = -p$.

Proof. By Theorem 4.8(i),

$$E(\chi^2) = -K(\bar{\chi}_1). \tag{4.11}$$

Thus, part (ii) follows from part (i) and Theorem 2.14.

By Theorem 2.15 and (4.11), $E(\chi^{11}) = E(\chi)K(\chi_1)/K(\bar{\chi}_1)$. By Theorem 2.10, $E(\chi^{11}) = E(\bar{\chi})$, and so $E^2(\bar{\chi}) = K^2(\chi_1)$. Thus, for $\delta = \pm 1$, $E(\chi) = \delta K(\bar{\chi}_1)$. Cubing both sides of the latter equality, we get $E(\chi^3) \equiv \delta^3 K(\bar{\chi}_1^3) \pmod{3\Omega}$. But, by Theorem 4.4, $E(\chi^3) = K(\bar{\chi}_1^3)$. Hence, $\delta = 1$ and $E(\chi) = K(\bar{\chi}_1)$. Q.E.D.

We next consider the case $p = 24k + 5$. Let χ have order 24. Then χ_1 has order 4 by Lemma 2.9. As in [1, Theorem 3.9], write $K(\chi_1) = a_4 + ib_4$, where a_4 and b_4 are integers such that $a_4^2 + b_4^2 = p$ and $a_4 \equiv 1 \pmod 4$. Observe that $3 \nmid a_4$ and $3 \nmid b_4$, since $a_4^2 + b_4^2 = p \equiv 2 \pmod 3$. As in Theorem 4.10, define $\varepsilon_0 = \varepsilon_0(\chi)$ by $\varepsilon_0 = \pm 1$ and $\varepsilon_0 \equiv -a_4 b_4 \pmod 3$.

THEOREM 4.14. *Let $p = 24k + 5$, and let χ have order 24. Then, in the notation above,*

(i) $E(\chi) = (\varepsilon_0 - i)(\frac{1}{2}e_{24}\sqrt{6} + if_{24})$,

where e_{24} and f_{24} are integers such that $3e_{24}^2 + 2f_{24}^2 = p$ and $f_{24} \equiv a_4 \pmod 3$;

(ii) $K_2(\chi) = i\varepsilon_0 E^2(\chi) = (e_{24}\sqrt{3} + if_{24}\sqrt{2})^2$.

Proof. By Theorem 4.10(i),

$$E(\chi^2) = -\varepsilon_0 i K(\chi_1). \tag{4.12}$$

Part (ii) now follows from part (i) and Theorem 2.14.

By Theorem 2.15 and (4.12),

$$E(\chi^{11}) = -\varepsilon_0 i E(\chi). \tag{4.13}$$

Note also that, by Theorem 2.10,

$$E(\chi) = E(\chi^5). \tag{4.14}$$

The subgroup $\langle \sigma_5, \sigma_{11} \rangle \subset Gal(Q(e^{2\pi i/24})/Q)$ has fixed field $Q(i\sqrt{6})$. From (4.13) and (4.14), it is not difficult to see that both σ_5 and σ_{11} fix $\frac{1}{2}\sqrt{6}(\varepsilon_0 + i)E(\chi)$. Thus,

$$\tfrac{1}{2}\sqrt{6}(\varepsilon_0 + i)E(\chi) = g_{24} + if_{24}\sqrt{6},$$

where f_{24} and g_{24} are integers such that $3p = g_{24}^2 + 6f_{24}^2$. Clearly, $g_{24} = 3e_{24}$

for some integer e_{24}. Hence,

$$E(\chi)=(\varepsilon_0-i)(\tfrac{1}{2}e_{24}\sqrt{6}+if_{24}), \tag{4.15}$$

where $p=3e_{24}^2+2f_{24}^2$.

Multiplying both sides of (4.15) by 2 and then cubing each side, we obtain

$$-E(\chi^3)\equiv(\varepsilon_0-i)^3 if_{24}\equiv -f_{24}+i\varepsilon_0 f_{24} \pmod{3\Omega}.$$

By Theorem 4.4, $E(\chi^3)=K(\bar{\chi}_1^3)=K(\chi_1)$, and so the above yields

$$-a_4-ib_4\equiv -f_{24}+i\varepsilon_0 f_{24} \pmod{3\Omega}.$$

Hence, $a_4\equiv f_{24} \pmod 3$. Q.E.D.

In order to examine the remaining cases $p\equiv 11, 17, 19 \pmod{24}$, we need the following lemma.

LEMMA 4.15. *Let χ have order 24, let $\theta=\exp(2\pi i/24)$, and let $\mathcal{O}$ denote the ring of algebraic integers in $Q(\theta)$. If $p\equiv 11 \pmod{24}$, then $E(\chi^5)/E(\chi)$ is a unit in $\mathcal{O}$; if $p\equiv 17$ or $19 \pmod{24}$, then $E(\chi^{11})/E(\bar{\chi})$ is a unit in $\mathcal{O}$.*

Proof. Suppose first that $p\equiv 11 \pmod{24}$. We must show that

$$\mathcal{O}E(\chi^5)=\mathcal{O}E(\chi). \tag{4.16}$$

It follows from Stickelberger's theorem [11, pp. 94, 97] that $\mathcal{O}G_2(\chi)=\mathcal{O}G_2(\chi^5)$. Thus, since χ_1 has order 2,

$$\mathcal{O}\frac{G_2(\chi)}{G(\chi_1)}=\mathcal{O}\frac{G_2(\chi^5)}{G(\chi_1^5)},$$

and (4.16) now follows with the use of Theorem 2.12.

Suppose now that $p\equiv 17$ or $19 \pmod{24}$. Then by Stickelberger's theorem, $\mathcal{O}G_2(\bar{\chi})=\mathcal{O}G_2(\chi^{11})$. The desired result now follows by an argument similar to that above. Q.E.D.

We now consider the case $p=24k+17$. Let λ have order 48; then λ_1 has order 8 by Lemma 2.9. As at the beginning of Section 4.1, write $K(\lambda)=a_8+ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2+2b_8^2=p$ and $a_8\equiv -1 \pmod 4$. Observe that $3\mid a_8$, since $a_8^2+2b_8^2=p\equiv 2 \pmod 3$. Write $\chi=\lambda^2$; then χ_1 has order 4. Again, as at the beginning of Section 4.1, write $K(\chi_1)=a_4+ib_4$, where a_4 and b_4 are integers such that $a_4^2+b_4^2=p$ and $a_4\equiv -1 \pmod 4$. Observe that $3\nmid a_4b_4$, since $a_4^2+b_4^2=p\equiv 2 \pmod 3$. As in Theorem 4.10, define $\varepsilon_0=\varepsilon_0(\chi)$ by $\varepsilon_0=\pm 1$ and $\varepsilon_0\equiv a_4b_4 \pmod 3$. Define $\delta_0=\delta_0(\chi)$ by $\delta_0=\pm 1$ and $\delta_0\equiv(-1)^k a_4b_8 \pmod 3$.

THEOREM 4.16. *Let $p=24k+17$, and let χ have order 24. Then, in the notation above,*

(i) $$E(\chi)=\frac{\delta_0(\varepsilon_0-i)}{\sqrt{2}}K(\bar{\chi}_1)=\frac{\delta_0(\varepsilon_0-i)}{\sqrt{2}}(a_4-ib_4),$$

(ii) $$K_2(\chi)=p.$$

Proof. By Theorem 4.10(i),

$$E(\chi^2) = -\varepsilon_0 iK(\bar{\chi}_1). \tag{4.17}$$

Part (ii) now follows from part (i) and Theorem 2.14.

By Theorem 2.15 and (4.17),

$$\frac{E(\chi^{11})}{E(\chi)} = -i\varepsilon_0 \frac{K(\chi_1)}{K(\bar{\chi}_1)}. \tag{4.18}$$

By Lemma 4.15, $E(\chi^{11})/E(\bar{\chi})$ is a unit. Clearly, σ_{11} fixes $E(\chi^{11})/E(\bar{\chi})$. Also, by Theorem 2.10, σ_{17} fixes $E(\chi^{11})/E(\bar{\chi})$. Hence, $E(\chi^{11})/E(\bar{\chi})$ is in the fixed field $Q(i\sqrt{2})$ of the subgroup $\langle\sigma_{11}, \sigma_{17}\rangle \subset Gal(Q(e^{2\pi i/24})/Q)$. It follows that $E(\chi^{11}) = \pm E(\bar{\chi})$. Thus, by (4.18), $E^2(\bar{\chi}) = \pm iK^2(\chi_1)$. It follows that $E(\chi)/K(\bar{\chi}_1)$ is a primitive 8th root of unity, and so we may write

$$E(\chi) = \frac{\delta(\varepsilon - i)}{\sqrt{2}} K(\bar{\chi}_1), \tag{4.19}$$

where $\delta = \pm 1$ and $\varepsilon = \pm 1$. It remains to show that $\delta = \delta_0$ and $\varepsilon = \varepsilon_0$. Cubing both sides of (4.19), we have

$$E(\chi^3) \equiv -\frac{\delta(\varepsilon + i)}{\sqrt{2}} K(\chi_1) \pmod{3\Omega}.$$

By Theorem 4.1(i), $E(\chi^3) = -a_8 + i(-1)^{k+1} b_8\sqrt{2}$. Hence,

$$i(-1)^{k+1} b_8\sqrt{2} \equiv -\frac{\delta(\varepsilon + i)}{\sqrt{2}} (a_4 + ib_4) \pmod{3\Omega}. \tag{4.20}$$

Multiplying both sides of (4.20) by $-\sqrt{2}$, we get

$$i(-1)^{k+1} b_8 \equiv \delta(\varepsilon + i)(a_4 + ib_4) \pmod{3\Omega}.$$

Comparing real and imaginary parts, we find that

$$\varepsilon \equiv a_4 b_4 \pmod 3 \quad \text{and} \quad \delta \equiv (-1)^k a_4 b_8 \pmod 3. \qquad \text{Q.E.D.}$$

We now consider the case $p = 24k + 19$. Let χ have order 24; then χ_1 has order 6 by Lemma 2.9. As in [1, Theorem 3.3], write $K(\chi_1) = -a_3 - ib_3\sqrt{3}$, where a_3 and b_3 are rational integers such that $a_3^2 + 3b_3^2 = p$ and $a_3 \equiv -1 \pmod 3$. As in Theorem 4.6, write $E(\chi^3) = a_8 + ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2 + 2b_8^2 = p$ and $a_8 \equiv (-1)^k \pmod 4$. Observe that $3 \mid b_8$ and $3 \nmid a_8$, since $a_8^2 + 2b_8^2 = p \equiv 1 \pmod 3$. Define δ_1 by $\delta_1 = \pm 1$ and $\delta_1 \equiv a_8 \pmod 3$.

THEOREM 4.17. *Let $p = 24k + 19$, and let χ have order 24. Then, in the notation above,*

(i) $E(\chi) = \delta_1 K(\bar{\chi}_1) = \delta_1(-a_3 + ib_3\sqrt{3})$,

(ii) $K_2(\chi) = p$.

Proof. By Theorem 4.9(i),

$$E(\chi^2) = -a_3 + ib_3\sqrt{3} = K(\bar{\chi}_1). \tag{4.21}$$

Part (ii) now follows from part (i) and Theorem 2.14.

By Lemma 4.15, $E(\chi^{11})/E(\bar{\chi})$ is a unit. Clearly, σ_{11} fixes $E(\chi^{11})/E(\bar{\chi})$, and by Theorem 2.10, σ_{19} does as well. Hence, $E(\chi^{11})/E(\bar{\chi})$ is in the fixed field $Q(i\sqrt{2})$ of the subgroup $\langle\sigma_{11}, \sigma_{19}\rangle \subset Gal(Q(e^{2\pi i/24})/Q)$. Hence, $E(\chi^{11}) = \pm E(\bar{\chi})$. By Theorem 2.15 and (4.21), $E(\chi^{11})/E(\chi) = K^2(\chi_1)/p$. It follows that

$$E(\chi) = \delta K(\bar{\chi}_1), \tag{4.22}$$

where $\delta \in \{\pm 1, \pm i\}$. Cube both sides of (4.22) and use Theorem 2.1 to get

$$a_8 \equiv a_8 + ib_8\sqrt{2} \equiv E(\chi^3) \equiv \delta^3 K(\bar{\chi}_1^3) \equiv \delta \pmod{3\Omega}.$$

Thus, $\delta = \delta_1$, and we are done. Q.E.D.

We next consider the case $p = 24k + 11$. Let χ have order 24. As in Theorem 4.6, write $E(\chi^3) = a_8 + ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2 + 2b_8^2 = p$ and $a_8 \equiv (-1)^{k+1} \pmod 4$. Observe that $3 \mid a_8$ and $3 \nmid b_8$, since $a_8^2 + 2b_8^2 = p \equiv 2 \pmod 3$.

THEOREM 4.18. *Let $p = 24k + 11$, and let χ have order 24. Then, in the notation above,*

(i) $E(\chi) = e_{24}\sqrt{3} + if_{24}\sqrt{2}$ *where e_{24} and f_{24} are integers such that $3e_{24}^2 + 2f_{24}^2 = p$ and $f_{24} \equiv b_8 \pmod 3$,*

(ii) $K_2(\chi) = E^2(\chi)$.

Proof. Part (ii) follows from Theorem 2.14.

To prove (i), first observe that σ_{11} fixes $E(\chi^5)/E(\chi)$ by Theorem 2.10. Clearly, σ_{-5} fixes $E(\chi^5)/E(\chi)$. Thus, by Lemma 4.15, $E(\chi^5)/E(\chi)$ is a unit in the fixed field $Q(i\sqrt{2})$ of $\langle\sigma_{-5}, \sigma_{11}\rangle \subset Gal(Q(e^{2\pi i/24})/Q)$. Hence,

$$E(\chi) = \varepsilon E(\chi^5), \tag{4.23}$$

where $\varepsilon = \pm 1$. Cubing both sides of (4.23), we find that

$$ib_8\sqrt{2} \equiv E(\chi^3) \equiv \varepsilon E(\bar{\chi}^9) = \varepsilon E(\bar{\chi}^3) \equiv -i\varepsilon b_8\sqrt{2} \pmod{3\Omega}.$$

Thus, $\varepsilon = -1$, and

$$E(\chi) = -E(\chi^5). \tag{4.24}$$

Thus, both σ_5 and σ_{11} fix $i\sqrt{2}E(\chi)$, and so $i\sqrt{2}E(\chi) \in Q(i\sqrt{6})$, the fixed field of $\langle\sigma_5, \sigma_{11}\rangle$. Therefore,

$$E(\chi) = e_{24}\sqrt{3} + if_{24}\sqrt{2}, \tag{4.25}$$

where e_{24} and f_{24} are integers such that $3e_{24}^2+2f_{24}^2=p$. Cubing both sides of (4.25), we get $ib_8\sqrt{2}\equiv E(\chi^3)\equiv if_{24}\sqrt{2} \pmod{3\Omega}$. Hence, $b_8\equiv f_{24} \pmod 3$. Q.E.D.

Another proof of Theorem 4.18(i) is given in [7, p. 340].

COROLLARY 4.19. *Let $p=24k+11$, and let χ have order 24. Then*

$$T(\chi)=\tfrac{1}{3}T(\chi^3)=\tfrac{1}{24}(p+1+4a_8).$$

Proof. By Theorem 2.11, $1=E(\chi^2)=E(\chi^6)=E(\chi^{10})$ and $-1=E(\chi^4)=E(\chi^8)=E(\chi^{12})$. By Theorem 2.10, $E(\chi)=E(\chi^{11})$, $E(\chi^5)=E(\chi^7)$, and $E(\chi^3)=E(\chi^9)$. Hence, by Theorem 2.17 and (4.24),

$$24T(\chi)=p+1+4\,\mathrm{Re}\,\{E(\chi^3)+E(\chi)+E(\chi^5)\}=p+1+4a_8. \tag{4.26}$$

By Corollary 4.7,

$$8T(\chi^3)=p+1+4a_8. \tag{4.27}$$

The corollary now follows trivially from (4.26) and (4.27). Q.E.D.

4.4. Quintic, decic, and bidecic sums. First, we consider the case $p=20k+1$. Let λ have order 40. Then λ_1 has order 20 by Lemma 2.9. As in [1, Theorem 3.9], write $K(\lambda_1^5)=a_4+ib_4$, where a_4 and b_4 are integers such that $a_4^2+b_4^2=p$ and $a_4\equiv(-1)^{k+1} \pmod 4$. As in [1, Theorem 3.34], write

$$\begin{aligned} K(\lambda_1)&=a_{20}+ib_{20}\sqrt{5}, &&\text{if } 5\nmid a_4,\\ &=i(a_{20}+ib_{20}\sqrt{5}), &&\text{if } 5\mid a_4,\end{aligned}$$

where a_{20} and b_{20} are integers such that $a_{20}^2+5b_{20}^2=p$, $a_{20}\equiv a_4 \pmod 5$, if $5\nmid a_4$, and $a_{20}\equiv b_4 \pmod 5$, if $5\mid a_4$. Put $\chi=\lambda^2$. As in (3.1), write

$$K(\chi_1)=a_{10}+b_{10}\sqrt{5}+ic_{10}\sqrt{5+2\sqrt{5}}+id_{10}\sqrt{5-2\sqrt{5}}.$$

Then by (3.12) and the remark at the end of Section 3.1,

$$K(\chi_1^2)=a_{10}-b_{10}\sqrt{5}+ic_{10}\sqrt{5-2\sqrt{5}}-id_{10}\sqrt{5+2\sqrt{5}}.$$

THEOREM 4.20. *Let $p=20k+1$, and let λ have order 40. Then, in the notation above*:

(i) $$E(\chi^4)=-K(\chi_1^2)=-a_{10}+b_{10}\sqrt{5}-ic_{10}\sqrt{5-2\sqrt{5}}+id_{10}\sqrt{5+2\sqrt{5}},$$

$$E(\chi^2)=-K(\chi_1)=-a_{10}-b_{10}\sqrt{5}-ic_{10}\sqrt{5+2\sqrt{5}}-id_{10}\sqrt{5-2\sqrt{5}},$$

and

$$E(\chi) = -a_{20} + i(-1)^{k+1} b_{20}\sqrt{5}, \quad \text{if } 5 \nmid a_4,$$
$$= i(-1)^{k+1} a_{20} + b_{20}\sqrt{5}, \quad \text{if } 5 \mid a_4;$$

(ii) $K_2(\chi^4) = -K^2(\chi_1^2)$, $K_2(\chi^2) = -K^2(\chi_1)$, *and* $K_2(\chi) = -E^2(\chi)$.

Proof. To prove (i), first observe that by Theorem 2.16,

$$E(\chi^4) = E(\chi^{2(p+1)}) = -K(\chi_1^2) \quad \text{and} \quad E(\chi^2) = E(\chi^{p+1}) = -K(\chi_1).$$

Also, by Theorem 2.16,

$$-K(\lambda_1) = E(\lambda^{p+1}) = E(\chi), \quad \text{if } 2 \mid k,$$
$$= E(\chi^{11}), \quad \text{if } 2 \nmid k.$$

In the case $2 \mid k$, this yields the desired result. In the case $2 \nmid k$, replace λ by λ^{11} above to obtain $E(\chi) = -K(\lambda_1^{11}) = -K(\bar{\lambda}_1)$, by Theorem 2.4(i). This proves part (i).

By Theorem 2.14,

$$K_2(\chi^4) = E^2(\chi^4) K(\chi_1^4)/E(\chi^8). \tag{4.28}$$

By part (i),

$$E(\chi^4) = -K(\chi_1^2). \tag{4.29}$$

Replacing χ by $\bar{\chi}^3$ in (4.29), we have

$$E(\chi^8) = -K(\chi_1^4). \tag{4.30}$$

Combining (4.28)–(4.30), we conclude that $K_2(\chi^4) = -K^2(\chi_1^2)$. Similarly, the other two equalities in part (ii) follow from part (i) and Theorem 2.14. Q.E.D.

We next consider the case $p = 20k + 11$. Let χ have order 20; thus, χ_1 has order 5. In view of (3.11), (3.12), and the remark at the end of Section 3.1, write

$$K(\chi_1^2) = a_{10} + b_{10}\sqrt{5} + ic_{10}\sqrt{5 + 2\sqrt{5}} + id_{10}\sqrt{5 - 2\sqrt{5}}$$

and

$$K(\chi_1) = a_{10} - b_{10}\sqrt{5} + ic_{10}\sqrt{5 - 2\sqrt{5}} - id_{10}\sqrt{5 + 2\sqrt{5}}.$$

THEOREM 4.21. *Let* $p = 20k + 11$, *and let* χ *have order* 20. *Then, in the notation above:*

(i) $E(\chi^4) = -K(\chi_1^2) = -a_{10} - b_{10}\sqrt{5} - ic_{10}\sqrt{5 + 2\sqrt{5}} - id_{10}\sqrt{5 - 2\sqrt{5}}$,

$E(\chi^2) = K(\bar{\chi}_1) = a_{10} - b_{10}\sqrt{5} - ic_{10}\sqrt{5 - 2\sqrt{5}} + id_{10}\sqrt{5 + 2\sqrt{5}}$,

$E(\chi) = (-1)^{k+1} K(\bar{\chi}_1)$;

(ii) $K_2(\chi^4) = -K^2(\chi_1^2)$, $K_2(\chi^2) = -K^2(\bar{\chi}_1)$, *and* $K_2(\chi) = p$.

Proof. Part (ii) follows easily from part (i) and Theorem 2.14.

By Theorem 2.16,

$$E(\chi^{12})=E(\chi^{p+1})=-K(\chi_1). \tag{4.31}$$

Replacing χ by $\bar{\chi}^3$ in (4.31), we obtain

$$E(\chi^4)=-K(\chi_1^2), \tag{4.32}$$

as desired.

By Theorem 2.15, $E(\chi^8)=E(\chi^2)K(\chi_1^2)/E(\chi^4)$. Thus, by (4.31) and (4.32),

$$E(\chi^2)=K(\bar{\chi}_1), \tag{4.33}$$

as desired.

By Theorem 2.15 and (4.33),

$$\frac{E(\chi^9)}{E(\chi)}=\frac{K(\chi_1)}{E(\chi^2)}=\frac{K^2(\chi_1)}{p}.$$

By Theorem 2.10, $E(\chi^9)=E(\bar{\chi})$, and so $E^2(\bar{\chi})=K^2(\chi_1)$. Therefore,

$$E(\chi)=\delta K(\bar{\chi}_1), \tag{4.34}$$

where $\delta=\pm 1$. Raising both sides of (4.34) to the fifth power and using Theorem 2.11, we obtain

$$(-1)^k=E(\chi^5)\equiv \delta K(\bar{\chi}_1^5)=\delta(p-2)\equiv -\delta \pmod 5.$$

Thus, $\delta=(-1)^{k+1}$ and $E(\chi)=(-1)^{k+1}K(\bar{\chi}_1)$. This completes the proof of part (i). Q.E.D.

We finally consider the case $p=20k+9$. The quintic and decic sums are trivially evaluated since $10 \mid (p+1)$, and so we evaluate only bidecic sums in the next theorem.

Let χ have order 20. In view of Theorems 4.1 and 4.4, we may write $E(\chi^5)=-a_4+ib_4$, where a_4 and b_4 are integers such that $a_4^2+b_4^2=p$ and $a_4\equiv(-1)^{k+1} \pmod 4$. Observe that exactly one of the pair a_4, b_4 is divisible by 5, since $a_4^2+b_4^2=p\equiv -1 \pmod 5$.

THEOREM 4.22. *Let $p=20k+9$, and let χ have order* 20. *Then*

(i)
$$\begin{aligned} E(\chi)&=a_{20}+ib_{20}\sqrt{5}, && \text{if } 5 \nmid a_4,\\ &=i(a_{20}+ib_{20}\sqrt{5}), && \text{if } 5 \mid a_4, \end{aligned}$$

where a_{20} and b_{20} are integers such that $a_{20}^2+5b_{20}^2=p$, $a_{20}\equiv -a_4 \pmod 5$, if $5 \nmid a_4$, and $a_{20}\equiv b_4 \pmod 5$, if $5 \mid a_4$;

(ii)
$$K_2(\chi)=-E^2(\chi).$$

Proof. Part (ii) follows immediately from Theorem 2.14.

To prove (i), first observe that the subgroup $\langle\sigma_{-3}\rangle\subset Gal(Q(e^{2\pi i/20})/Q)$ has fixed field $Q(i)$. By Theorem 2.10, $E(\chi)=E(\chi^9)$. Hence, σ_{-3} fixes

$E(\chi^3)/E(\chi)$. By the same argument as in the proof of Lemma 4.15, it is easily shown that $E(\chi^3)/E(\chi)$ is a unit in $Q(e^{2\pi i/20})\cap\Omega$. Hence,

$$E(\chi^3)=\delta E(\chi), \tag{4.35}$$

where $\delta\in\{\pm1, \pm i\}$. Raising each side of (4.35) to the fifth power, we get

$$-a_4-ib_4=E(\chi^{15})\equiv\delta E(\chi^5)=\delta(-a_4+ib_4) \pmod{5\Omega}.$$

Thus,

$$E(\chi^3)=\delta E(\chi) \quad \text{with} \quad \delta=\begin{cases}1, & \text{if } 5\nmid a_4,\\ -1, & \text{if } 5\mid a_4.\end{cases} \tag{4.36}$$

Suppose that $5\nmid a_4$. Then, by (4.36), σ_3 fixes $E(\chi)$, and so $E(\chi)\in Q(i\sqrt{5})$, the fixed field of $\langle\sigma_3\rangle\subset Gal(Q(e^{2\pi i/20})/Q)$. Hence,

$$E(\chi)=a_{20}+ib_{20}\sqrt{5}, \tag{4.37}$$

where a_{20} and b_{20} are integers such that $a_{20}^2+5b_{20}^2=p$. Raising each side of (4.37) to the fifth power, we obtain

$$-a_4\equiv E(\chi^5)\equiv a_{20} \pmod{5\Omega},$$

and so $a_{20}\equiv -a_4 \pmod 5$.

Suppose next that $5\mid a_4$. Then, by (4.36), σ_3 fixes $iE(\chi)$. Hence, $iE(\chi)\in Q(i\sqrt{5})$, and so

$$E(\chi)=i(a_{20}+ib_{20}\sqrt{5}), \tag{4.38}$$

where a_{20} and b_{20} are integers such that $a_{20}^2+5b_{20}^2=p$. Raising each side of (4.38) to the fifth power, we obtain

$$ib_4\equiv E(\chi^5)\equiv ia_{20} \pmod{5\Omega},$$

and so $b_4\equiv a_{20} \pmod 5$. Q.E.D.

COROLLARY 4.23. *Let $p=20k+9$, and let χ have order* 20. *Then*

$$\begin{aligned} T(\chi)&=\tfrac{1}{5}\{T(\chi^5)+2a_{20}\}=\tfrac{1}{20}(p+1-2a_4+8a_{20}), && \text{if } 5\nmid a_4,\\ &=\tfrac{1}{5}T(\chi^5)=\tfrac{1}{20}(p+1-2a_4), && \text{if } 5\mid a_4. \end{aligned}$$

Proof. By Theorem 2.11, $1=E(\chi^2)=E(\chi^6)=E(\chi^{10})$ and $-1=E(\chi^4)=E(\chi^8)$. By Theorem 2.10, $E(\chi)=E(\chi^9)$ and $E(\chi^3)=E(\chi^7)$. Hence, by Theorem 2.17,

$$20T(\chi)=p+1-2a_4+4\,\mathrm{Re}\,\{E(\chi)+E(\chi^3)\}. \tag{4.39}$$

By Theorems 2.11 and 2.17,

$$4T(\chi^5)=p+1-2a_4. \tag{4.40}$$

The result now follows from (4.36), (4.39), (4.40), and Theorem 4.22.

COROLLARY 4.24. *Let $p=20k+9$, and let χ have order* 20. *Then* $T(\chi)\equiv 1 \pmod 4$.

Proof. First,

$$E(\chi)+E(\chi^6)+E(\chi^{11})+E(\chi^{16})$$
$$=\sum_{b=0}^{p-1}\chi(1+b\gamma)\{1+\chi^5(1+b\gamma)+\chi^{10}(1+b\gamma)+\chi^{15}(1+b\gamma)\}$$
$$=4\sum_{b\in S}\chi(1+b\gamma),$$

where $S=\{b: 0\le b\le p-1, \chi^5(1+b\gamma)=1\}$. Since $E(\chi^6)=1$, $E(\chi^{16})=-1$, and $E(\chi^{11})=E(\bar{\chi})$ by Theorem 2.10, $2\operatorname{Re}E(\chi)=4\sum_{b\in S}\chi(1+b\gamma)$. Thus,

$$\operatorname{Re}E(\chi)\in 2\Omega. \tag{4.41}$$

Secondly, for each prime p with $p\equiv 1 \pmod 4$, write $p=a_4^2+b_4^2$, where a_4 and b_4 are integers with $a_4\equiv -\left(\frac{2}{p}\right) \pmod 4$. It is then not hard to show that $a_4\equiv \frac{1}{2}(p-3) \pmod 8$. (This congruence can be refined; see [1, Theorem 3.16].) Hence,

$$\tfrac{1}{4}(p+1-2a_4)\equiv 1 \pmod 4.$$

Moreover, if $5\nmid a_4$, then a_{20} is even by Theorem 4.22 and (4.41). The result now follows from Corollary 4.23. Q.E.D.

COROLLARY 4.25. *Let $p=20k+9=a^2+b^2=u^2+5v^2$ with a odd. Then $5\mid a$ if and only if $2\mid v$.*

Proof. We have $a^2=a_4^2$, $b^2=b_4^2$, $u^2=a_{20}^2$, and $v^2=b_{20}^2$, by Theorem 4.22. If $5\mid a$, then $2\mid b_{20}$ by Theorem 4.22 and (4.41), i.e., $2\mid v$. If $5\nmid a$, then $2\mid a_{20}$ by Theorem 4.22 and (4.41), i.e., $2\mid u$. Q.E.D.

An analogous result for $p=20k+1$ is similarly proved in [1, Corollary 3.35]. Proofs of Corollary 4.25 have also been given by Muskat and Whiteman [16] and E. Lehmer [13], [14].

4.5 Bioctic sums. Let $p=16k+1$. Let λ have order 32; then λ_1 has order 16 by Lemma 2.9. Put $\chi=\lambda^2$. As in Theorem 3.5, write

$$K(\lambda_1)=a_{16}+b_{16}\sqrt{2}+ic_{16}\sqrt{2+\sqrt{2}}+id_{16}\sqrt{2-\sqrt{2}},$$

where a_{16}, b_{16}, c_{16}, and d_{16} are integers such that $p=a_{16}^2+2b_{16}^2+2c_{16}^2+2d_{16}^2$, $2a_{16}b_{16}=d_{16}^2-c_{16}^2-2c_{16}d_{16}$, $a_{16}\equiv -1 \pmod 8$, and b_{16}, c_{16}, and d_{16} are even.

THEOREM 4.26. *Let $p=16k+1$, and let λ have order* 32. *Then, in the* *notation above,*

(i) $E(\chi)=-a_{16}-b_{16}\sqrt{2}+i(-1)^{k+1}(c_{16}\sqrt{2+\sqrt{2}}+d_{16}\sqrt{2-\sqrt{2}})$,
(ii) $K_2(\chi)=-E^2(\chi)$.

Proof. Part (ii) follows immediately from Theorems 2.14 and 4.1(i).
By Theorem 2.16,

$$\begin{aligned}-K(\lambda_1)=E(\lambda^{p+1})&=E(\lambda^2), &&\text{if } 2\mid k,\\ &=E(\lambda^{18}), &&\text{if } 2\nmid k.\end{aligned}$$

In the case that k is even, this is the desired result. In the case that k is odd, replace λ by λ^7 above to obtain $E(\bar{\chi})=-K(\lambda_1^7)$. Applying Theorem 2.4(i), we find that $E(\chi)=-K(\bar{\lambda}_1)$. Q.E.D.

Let $p=16k+9$. Let χ have order 16; then χ_1 has order 8 by Lemma 2.9. As in [1, Theorem 3.12], write $K(\chi_1)=a_8+ib_8\sqrt{2}$, where a_8 and b_8 are integers such that $a_8^2+2b_8^2=p$ and $a_8\equiv-1 \pmod 4$.

THEOREM 4.27. *Let $p=16k+9$, and let χ have order 16. Then, in the notation above,*

(i) $E(\chi)=-K(\bar{\chi}_1)=-a_8+ib_8\sqrt{2}$,
(ii) $K_2(\chi)=-p$.

Proof. By Theorem 4.1,

$$E(\chi^2)=-K(\bar{\chi}_1). \tag{4.42}$$

Part (ii) now follows from part (i), (4.42), and Theorem 2.14.

By Theorem 2.15 and (4.42), we have $E(\chi^7)=E(\chi)K(\chi_1)/K(\bar{\chi}_1)$. By Theorem 2.10, $E(\chi^7)=E(\bar{\chi})$, and so $E^2(\bar{\chi})=K^2(\chi_1)$. Thus,

$$E(\chi)=\delta K(\bar{\chi}_1), \tag{4.43}$$

where $\delta=\pm1$. By Theorem 2.17,

$$16T(\chi)=\sum_{j=0}^{15}E(\chi^j)=8T(\chi^2)+\sum_{j=0}^{7}E(\chi^{2j+1})=8T(\chi^2)+4\,\mathrm{Re}\,\{E(\chi)+E(\chi^3)\},$$

since, by Theorem 2.10, $E(\chi^7)=E(\bar{\chi})$ and $E(\chi^5)=E(\bar{\chi}^3)$. By Theorem 2.4(i), $K(\bar{\chi}_1)=K(\bar{\chi}_1^3)$. Thus, from (4.43), $E(\chi^3)=E(\chi)$. Hence,

$$2T(\chi)=T(\chi^2)+\mathrm{Re}\,E(\chi)=T(\chi^2)+\delta a_8,$$

by (4.43). By Corollary 4.3, $T(\chi^2)\equiv1 \pmod 4$. Hence, the above yields $2\equiv1+\delta a_8 \pmod 4$. Since $a_8\equiv-1 \pmod 4$, we conclude that $\delta=-1$. Hence, by (4.43), $E(\chi)=-K(\bar{\chi}_1)$. Q.E.D.

THEOREM 4.28. *Let $p=16k+7$, and let χ be a character of order 16. Then*

$$E(\chi)=a_{16}+b_{16}\sqrt{2}+ic_{16}\sqrt{2+\sqrt{2}}+id_{16}\sqrt{2-\sqrt{2}}, \tag{4.44}$$

where a_{16}, b_{16}, c_{16}, and d_{16} are odd integers such that $a_{16}\equiv(-1)^k \pmod 8$,

$$a_{16}^2+2b_{16}^2+2c_{16}^2+2d_{16}^2=p, \tag{4.45}$$

and

$$2a_{16}b_{16}=d_{16}^2-c_{16}^2-2c_{16}d_{16}. \tag{4.46}$$

Equalities (4.45) *and* (4.46) *determine* $|a_{16}|$, $|b_{16}|$, *and* $\{|c_{16}|, |d_{16}|\}$ *uniquely.*
Lastly, $K_2(\chi)=E^2(\chi)$.

Proof. The last statement follows immediately from Theorem 2.14.
To prove the first part, proceed as in the proof of Theorem 3.5. Since the subgroup $\langle\sigma_7\rangle$ of $Gal(Q(e^{2\pi i/16})/Q)$ has fixed field $Q(i\sqrt{2+\sqrt{2}})$, and since σ_7 fixes $E(\chi)$ by Theorem 2.10, we deduce that $E(\chi)$ has the representation given in (4.44), where a_{16}, b_{16}, c_{16}, and d_{16} are rational numbers such that (4.45) and (4.46) hold. By Theorem 2.10, $E(\chi)=E(\chi^7)$ and $E(\chi^3)=E(\chi^5)$. Also, $\sigma_3(\sqrt{2})=-\sqrt{2}$. Furthermore, by Theorem 2.11, $1=E(\chi^2)=E(\chi^6)=E(\chi^{10})=E(\chi^{14})$ and $-1=E(\chi^4)=E(\chi^8)=E(\chi^{12})$. Using all of this information in Theorem 2.17, we find, with the help of (4.44), that

$$16T(\chi)=\sum_{j=0}^{7} E(\chi^{2j+1})+\sum_{j=0}^{7} E(\chi^{2j})=8a_{16}+p+1. \tag{4.47}$$

Since $T(\chi)$ is odd, we have $16\equiv 8a_{16}+p+1 \pmod{32}$. Thus,

$$a_{16}\equiv 1-2k\equiv(-1)^k \pmod 4, \tag{4.48}$$

and a_{16} is an integer.
By Theorem 2.10,

$$\begin{aligned}2(a_{16}+b_{16}\sqrt{2})&=E(\chi)+E(\bar{\chi})=E(\chi)+E(\chi^9)\\ &=\sum_{b=0}^{p-1}\chi(1+b\gamma)\{1+\phi(1+b\gamma)\}=2\sum_{\substack{0\le b\le p-1\\ \phi(1+b\gamma)=1}}\chi(1+b\gamma)\in 2\Omega.\end{aligned}$$

Thus, $a_{16}+b_{16}\sqrt{2}\in\Omega$, and so b_{16} is an integer. Hence, by (4.44), $c_{16}\sqrt{2+\sqrt{2}}+d_{16}\sqrt{2-\sqrt{2}}\in\Omega$. From Lemma 3.4, we deduce that c_{16} and d_{16} are integers. Thus, a_{16}, b_{16}, c_{16}, and d_{16} are integers.

From (4.46), c_{16} and d_{16} have the same parity. Suppose that c_{16} and d_{16} are even. Then by (4.46) and (4.48), b_{16} is even. Hence, by (4.45), $p\equiv a_{16}^2\equiv 1 \pmod 8$, which is a contradiction. Thus, c_{16} and d_{16} are odd, and so, by (4.46), b_{16} is odd. Hence, by (4.45), $p\equiv a_{16}^2+6 \pmod{16}$. Since $p\equiv 7 \pmod{16}$, we have $a_{16}^2\equiv 1 \pmod{16}$. Hence, by (4.48), $a_{16}\equiv(-1)^k \pmod 8$. The claim on uniqueness in the theorem was shown by Muskat and Zee [17]. Q.E.D.

5. Brewer sums

5.1 Brewer polynomials. For each natural number n and each complex number $a \neq 0$, the generalized Brewer polynomial $V_n(x, a)$ is defined by [3] $V_1(x, a) = x$, $V_2(x, a) = x^2 - 2a$, and

$$V_{n+1}(x, a) = xV_n(x, a) - aV_{n-1}(x, a), \quad n \geq 2.$$

The ordinary Brewer polynomial $V_n(x)$ is defined by [2] $V_n(x) = V_n(x, 1)$. Note that $V_n(x, a)$ is even or odd according as n is even or odd. In this section, we present some basic facts about $V_n(x, a)$.

PROPOSITION 5.1. *For* $n \geq 1$, $V_n(y + ay^{-1}, a) = y^n + a^n y^{-n}$.

Proof. The result follows easily by induction on n. Q.E.D.

PROPOSITION 5.2. *For* $n \geq 1$,

$$V_n(x, a) = \left(\frac{x + \sqrt{x^2 - 4a}}{2}\right)^n + \left(\frac{x - \sqrt{x^2 - 4a}}{2}\right)^n.$$

Proof. Letting $y = (x + \sqrt{x^2 - 4a})/2$ in Proposition 5.1, we readily achieve the desired result. Q.E.D.

PROPOSITION 5.3. *For each odd prime p,* $x^{-1}V_p(x)$ *is an irreducible polynomial over Q.*

Proof. By Proposition 5.2, $x^{-1}V_p(x)$ is an Eisenstein polynomial with constant term $(-1)^{(p-1)/2}p$. Q.E.D.

PROPOSITION 5.4. *For each pair of natural numbers k and n,* $V_{kn}(x) = V_n(V_k(x))$.

Proof. For $x = y + y^{-1}$, $y \neq 0$, the result holds by Proposition 5.1. Hence, the result holds for all x. Q.E.D.

PROPOSITION 5.5. *For each pair of complex numbers a, b, we have*

$$V_n(x\sqrt{a}, ab) = a^{n/2}V_n(x, b).$$

Proof. The result follows readily by induction on n. Q.E.D.

Define the polynomial $F_n(x, a)$ by

$$F_n(x, a) = V_{2n}(\sqrt{x}, a).$$

Put $F_n(x, 1) = F_n(x)$.

PROPOSITION 5.6. *We have* $F_n(xa, a) = a^n F_n(x)$.

Proof. By Proposition 5.5,

$$F_n(xa, a) = V_{2n}(\sqrt{xa}, a) = a^n V_{2n}(\sqrt{x}) = a^n F_n(x). \qquad \text{Q.E.D.}$$

PROPOSITION 5.7. *We have* $F_n(x + 2) = V_n(x)$.

Proof. By Proposition 5.4,

$$F_n(x+2) = V_{2n}(\sqrt{x+2}) = V_n(V_2(\sqrt{x+2})) = V_n(x). \qquad \text{Q.E.D.}$$

5.2 Theory of Brewer sums. In the remainder of the chapter, p denotes an odd prime, and a is an integer such that $p \nmid a$. If n is a positive integer, the generalized Brewer sum $\Lambda_n(a)$ is defined by

$$\Lambda_n(a) = \sum_j \left(\frac{V_n(j, a)}{p}\right).$$

The ordinary Brewer sum Λ_n is defined by $\Lambda_n = \Lambda_n(1)$. These sums were first introduced by Brewer [2], [3].

For $n \geq 1$, define

$$\Omega_n(a) = \sum_{j \neq 0} \left(\frac{j^n + a^n j^{-n}}{p}\right).$$

Put $\Omega_n(1) = \Omega_n$. Let $d = (n, p-1)$. As j runs through the elements of $GF(p)^*$, j^n runs through the same elements as j^d does, with the same multiplicity. Thus, we can write

$$\Omega_n(a) = \sum_{j \neq 0} \left(\frac{j^d + a^n j^{-d}}{p}\right). \tag{5.1}$$

Recall that τ is a generator of $GF(p^2)^*$ and that $\gamma = \tau^{(p+1)/2}$. Define $\theta = \tau^{p-1}$, and let $\mathscr{C} = \langle \theta \rangle$. Thus, $\mathscr{C}$ is a cyclic subgroup of $GF(p^2)^*$ of order $p+1$. For $0 \leq n \leq p-1$, we have $(1+\gamma n)^{p-1} = (1-\gamma n)/(1+\gamma n)$, and, hence, the p elements $(1+\gamma n)^{p-1}$ are distinct elements of $\mathscr{C}$. Hence,

$$\mathscr{C} = \{(1-\gamma n)/(1+\gamma n) \colon 0 \leq n \leq p-1\} \cup \{-1\}.$$

If $x = a + b\gamma$ with $a, b \in GF(p)$, then

$$x + x^p = (a+b\gamma) + (a+b\gamma)^p = (a+b\gamma) + (a-b\gamma) = 2a \in GF(p). \tag{5.2}$$

Hence, if $y \in \mathscr{C}$, then $y + y^{-1} = y + y^p \in GF(p)$. Thus, we can define, for each natural number n

$$\Theta_n = \sum_{y \in \mathscr{C}} \left(\frac{y^n + y^{-n}}{p}\right).$$

Let $D = (n, p+1)$. As y runs through the elements of $\mathscr{C}$, y^n runs through the same elements as y^D does, with the same multiplicity. Thus,

$$\Theta_n = \Theta_D = \sum_{y \in \mathscr{C}} \left(\frac{y^D + y^{-D}}{p}\right). \tag{5.3}$$

Recall that $g = \gamma^2 = \tau^{p+1}$ is a primitive root $(\bmod\, p)$. If $y \in \mathscr{C}$, then $(\tau y)^p =$

$g(\tau y)^{-1}$, and so by (5.2),

$$(\tau y)^n + g^n(\tau y)^{-n} = (\tau y)^n + (\tau y)^{np} \in GF(p).$$

Hence, we may define

$$\Theta_n(g) = \sum_{y \in \mathscr{C}} \left(\frac{(\tau y)^n + (\tau y)^{np}}{p}\right) = \sum_{y \in \mathscr{C}} \left(\frac{(\tau y)^n + g^n(\tau y)^{-n}}{p}\right).$$

For completeness, we give a proof of the following lemma of Brewer [2].

LEMMA 5.8. *For* $n \geq 1$, $2\Lambda_n = \Omega_n + \Theta_n$.

Proof. Let

$$S = \left\{m \in GF(p): \left(\frac{m^2-4}{p}\right) = 1\right\} \quad \text{and} \quad T = \left\{m \in GF(p): \left(\frac{m^2-4}{p}\right) = -1\right\}.$$

Then $GF(p) = S \cup T \cup \{-2, 2\}$, and by Lemma 2.5, $|S| = (p-3)/2$ and $|T| = (p-1)/2$. Let $y = a + b\gamma \in \mathscr{C} - \{-1, 1\}$, where $a, b \in GF(p)$. Then

$$(y + y^{-1})^2 - 4 = (y - y^{-1})^2 = (y - y^p)^2 = \{(a + b\gamma) - (a - b\gamma)\}^2 = 4b^2 g.$$

Thus, $\left(\frac{(y+y^{-1})^2-4}{p}\right) = -1$, and so $y + y^{-1} \in T$. By Proposition 5.1, it follows that

$$\Theta_n = \sum_{y \in \mathscr{C}} \left(\frac{V_n(y+y^{-1})}{p}\right) = 2\sum_{m \in T} \left(\frac{V_n(m)}{p}\right) + \sum_{m \in \{-2, 2\}} \left(\frac{V_n(m)}{p}\right).$$

Since $(j + j^{-1})^2 - 4 = (j - j^{-1})^2$, we also have

$$\Omega_n = \sum_{j \neq 0} \left(\frac{V_n(j+j^{-1})}{p}\right) = 2\sum_{m \in S} \left(\frac{V_n(m)}{p}\right) + \sum_{m \in \{-2, 2\}} \left(\frac{V_n(m)}{p}\right).$$

Addition of the above two equalities gives

$$\Theta_n + \Omega_n = 2\sum_{m} \left(\frac{V_n(m)}{p}\right) = 2\Lambda_n. \qquad \text{Q.E.D.}$$

The following theorem enables one to evaluate any ordinary Brewer sum in terms of Eisenstein sums and the Jacobsthal sums $\phi_n(a)$ and $\psi_n(a)$ over $GF(p)$ defined in Chapter 2.

THEOREM 5.9. *Let* $n \geq 1$, $d = (n, p-1)$, *and* $D = (n, p+1)$. *If n is odd, we have*

$$\begin{aligned} 2\Lambda_n &= 0, && \textit{if } p \equiv 3 \pmod 4, \\ &= \phi_{2d}(1) + \left(\frac{2}{p}\right) \sum_{j=0}^{2D-1} E(\psi^{2j+1}), && \textit{if } p \equiv 1 \pmod 4, \end{aligned}$$

where ψ is any character on $GF(p^2)$ of order $4D$. If n is even, we have

$$2\Lambda_n = -1+\psi_{2d}(1), \qquad \text{if } (p+1)/D \text{ is odd,}$$
$$= -1+\psi_{2d}(1)+\left(\frac{2}{p}\right)\sum_{j=0}^{D-1} E(\chi^{2j+1}), \quad \text{if } (p+1)/D \text{ is even,}$$

where χ is any character on $GF(p^2)$ of order $2D$.

Proof. First, suppose that n is odd and that $p \equiv 3 \pmod 4$. Replacing j by $-j$ in (5.1) and replacing y by $-y$ in (5.3), we find that $\Omega_d = -\Omega_d$ and $\Theta_D = -\Theta_D$, respectively, and so by Lemma 5.8, $\Lambda_n = 0$.

Secondly, suppose that n is odd and that $p \equiv 1 \pmod 4$. Clearly, $\Omega_d = \phi_{2d}(1)$. By Lemma 5.8, it remains to evaluate Θ_D. Let λ be a character on $GF(p^2)$ of order $2D(p-1)$, and let $\psi = \lambda^{(p-1)/2}$. Then ψ has order $4D$. By Lemma 2.9, ψ_1 has order 2. Thus,

$$\Theta_D = \sum_{y\in\mathscr{C}} \psi(y^D+y^{-D}) = \sum_{y\in\mathscr{C}} \bar{\psi}^D(y)\psi(y^{2D}+1).$$

Now, $\lambda(\tau)$ is a primitive $2D(p-1)$th root of unity. Since $\theta = \tau^{p-1}$, $\lambda(\theta)$ is a primitive $2D$th root of unity. Since $p = 1 \pmod 4$, it follows that $\psi^D(\theta) = 1$. By the definition of $\mathscr{C}$, we then have $\psi^D(y) = 1$ for $y \in \mathscr{C}$. We thus get

$$\begin{aligned}\Theta_D &= \sum_{y\in\mathscr{C}} \psi(y^{2D}+1) = \sum_{y\in\mathscr{C}} \psi(y+1)\sum_{j=1}^{2D}\lambda^j(y)\\ &= \sum_{m=0}^{p-1} \psi\left(\frac{2}{1+m\gamma}\right)\sum_{j=1}^{2D}\lambda^j((1+m\gamma)^{p-1})\\ &= \sum_{j=1}^{2D}\sum_{m=0}^{p-1} \psi(2)\psi^{2j-1}(1+m\gamma)\\ &= \left(\frac{2}{p}\right)\sum_{j=0}^{2D-1} E(\psi^{2j+1}).\end{aligned}$$

Finally, suppose that n is even. Then d and D are even, and it is easy to see that

$$\Omega_d = -1+\psi_{2d}(1). \tag{5.4}$$

Assume that $(p+1)/D$ is even. Then $p \equiv 3 \pmod 4$. Replacing y by $y\theta^{(p+1)/(2D)}$ in (5.3), we see that $\Theta_D = -\Theta_D$. Thus. $\Theta_D = 0$, and so by Lemma 5.8 and (5.4), we achieve the desired result. Now assume that $(p+1)/D$ is odd. It remains to calculate Θ_D. Let μ be a character on $GF(p^2)$ of order $D(p-1)$, and let $\chi = \mu^{(p-1)/2}$. Thus, χ has order $2D$, and by Lemma 2.9, χ_1 has order 2. Hence, we can write

$$\Theta_D = \sum_{y\in\mathscr{C}} \chi(y^D+y^{-D}) = \sum_{y\in\mathscr{C}} \bar{\chi}^D(y)\chi(y^{2D}+1).$$

Since $\theta = \tau^{p-1}$, $\mu(\theta)$ is a primitive Dth root of unity. Thus, $\chi^D(\theta) = 1$. By the definition of $\mathscr{C}$, it follows that $\chi^D(y) = 1$ for $y \in \mathscr{C}$. Furthermore, since $(2D, p+1) = D$, the sequence $\langle y^{2D} : y \in \mathscr{C}\rangle$ is a permutation of the sequence

$\langle y^D : y \in \mathscr{C}\rangle$. Hence,

$$\begin{aligned}\Theta_D &= \sum_{y\in\mathscr{C}} \chi(y^{2D}+1) = \sum_{y\in\mathscr{C}} \chi(y^D+1)\\ &= \sum_{y\in\mathscr{C}} \chi(y+1) \sum_{j=1}^{D} \mu^j(y)\\ &= \sum_{m=0}^{p-1} \chi(2)\bar{\chi}(1+m\gamma) \sum_{j=1}^{D} \mu^j((1+m\gamma)^{p-1})\\ &= \sum_{j=1}^{D}\sum_{m=0}^{p-1} \chi(2)\chi^{2j-1}(1+m\gamma)\\ &= \left(\frac{2}{p}\right)\sum_{j=0}^{D-1} E(\chi^{2j+1}).\end{aligned}$$

Using the above and (5.4) in Lemma 5.8, we complete the proof. Q.E.D.

The following corollary generalizes a result of Robinson [23].

COROLLARY 5.10. *Let n be odd. Then*

$$2(\Lambda_{2n}-\Lambda_n) = -1+\psi_{2d}(1) = 2\phi_d(1).$$

Let n be even. If $p \equiv 1 \pmod 4$, then

$$\begin{aligned}2(\Lambda_{2n}-\Lambda_n) &= \phi_{2d}(1), && \textit{if } (p-1)/d \textit{ is even},\\ &= 0, && \textit{if } (p-1)/d \textit{ is odd}.\end{aligned}$$

If $p \equiv 3 \pmod 4$, then

$$\begin{aligned}2(\Lambda_{2n}-\Lambda_n) &= 0, && \textit{if } (p+1)/D \not\equiv 2 \pmod 4,\\ &= \left(\frac{2}{p}\right)\sum_{j=0}^{2D-1} E(\psi^{2j+1}), && \textit{if } (p+1)/D \equiv 2 \pmod 4,\end{aligned}$$

where ψ is any character of order $4D$ on $GF(p^2)$.

Proof. Let n be odd. Then $\left(\frac{m}{p}\right) = \left(\frac{m^{-d}}{p}\right)$ for each $m \in GF(p)^*$, and so

$$\phi_d(1) = \sum_{m\neq 0} \left(\frac{m}{p}\right)\left(\frac{m^d+1}{p}\right) = \sum_{m\neq 0}\left(\frac{m^d+1}{p}\right) = -1+\psi_d(1).$$

Since $\psi_{2d}(1) = \phi_d(1)+\psi_d(1)$ by Theorem 2.6, it follows that $-1+\psi_{2d}(1) = 2\phi_d(1)$.

All of the remaining equalities given in Corollary 5.10 follow directly from Theorem 5.9, with the use of Theorem 2.6 in some instances. Q.E.D.

We now define a sum B_n, very closely related to Λ_n, by

$$B_n = \sum_j \left(\frac{j+2}{p}\right)\left(\frac{V_n(j)}{p}\right).$$

The evaluation of B_2 was first achieved by Brewer [2]. Later proofs have been given by Whiteman [28], Rajwade [21], and Leonard and Williams [15]. In [1, Theorem 4.12], B_6 is evaluated. Corollary 5.10, in fact, gives a formula for B_n, as the following theorem shows.

THEOREM 5.11. *For* $n \geq 1$, $B_n = \Lambda_{2n} - \Lambda_n$.

Proof. By Proposition 5.4, $V_{2n}(x) = V_n(x^2-2)$. Hence,

$$\begin{aligned}\Lambda_{2n} &= \sum_j \left(\frac{V_n(j^2-2)}{p}\right) = \sum_j \left(\frac{V_n(j-2)}{p}\right)\left\{1+\left(\frac{j}{p}\right)\right\}\\ &= \sum_j \left(\frac{V_n(j)}{p}\right)\left\{1+\left(\frac{j+2}{p}\right)\right\} = \Lambda_n + B_n. \quad \text{Q.E.D.}\end{aligned}$$

The rest of this section is devoted to obtaining formulas for the generalized Brewer sums $\Lambda_n(a)$ analogous to the formulae for ordinary Brewer sums given in Theorem 5.9.

THEOREM 5.12. *For* $n \geq 1$,

$$\Lambda_{2n}(a) = \left(\frac{a}{p}\right)^{n+1}(\Lambda_{2n} - \Lambda_n) + \left(\frac{a}{p}\right)^n \Lambda_n.$$

Proof. Using Propositions 5.6 and 5.7, we get

$$\begin{aligned}\Lambda_{2n}(a) &= \sum_j \left(\frac{V_{2n}(j, a)}{p}\right) = \sum_j \left(\frac{F_n(j^2, a)}{p}\right)\\ &= \sum_j \left(\frac{F_n(j, a)}{p}\right)\left\{1+\left(\frac{j}{p}\right)\right\}\\ &= \sum_j \left(\frac{F_n(ja, a)}{p}\right)\left\{1+\left(\frac{ja}{p}\right)\right\}\\ &= \sum_j \left(\frac{a^n F_n(j)}{p}\right)\left\{1+\left(\frac{ja}{p}\right)\right\}\\ &= \sum_j \left(\frac{a^n F_n(j+2)}{p}\right)\left\{1+\left(\frac{a}{p}\right)\left(\frac{j+2}{p}\right)\right\}\\ &= \left(\frac{a}{p}\right)^n \sum_j \left(\frac{V_n(j)}{p}\right) + \left(\frac{a}{p}\right)^{n+1} \sum_j \left(\frac{V_n(j)}{p}\right)\left(\frac{j+2}{p}\right)\\ &= \left(\frac{a}{p}\right)^n \Lambda_n + \left(\frac{a}{p}\right)^{n+1} B_n.\end{aligned}$$

The result now follows from Theorem 5.11. Q.E.D.

Theorem 5.12 is very important, for it indicates that every generalized Brewer sum $\Lambda_{2n}(a)$ can be evaluated in terms of ordinary Brewer sums. Thus, for the remainder of this section, we need only examine $\Lambda_n(a)$ for odd n. Moreover, if g is a primitive root (mod p), we deduce from Proposition 5.5 that $V_n(g^k x, g^{2k} b) = g^{kn} V_n(x, b)$, where k is a positive integer. Hence,

$$\Lambda_n(g^{2k}b) = (-1)^{kn}\Lambda_n(b). \tag{5.5}$$

Therefore, all generalized Brewer sums can be expressed in terms of Λ_n or $\Lambda_n(g)$. Thus, it remains to evaluate $\Lambda_n(g)$, for odd n. We do this in the next theorem. First, we give, for completeness, a proof of the generalized Brewer lemma [3]. Recall that $g = \tau^{p+1}$.

LEMMA 5.13. *For* $n \geq 1$, $2\Lambda_n(g) = \Omega_n(g) + \Theta_n(g)$.

Proof. Let

$$S_g = \left\{m \in GF(p)\colon \left(\frac{m^2-4g}{p}\right) = 1\right\} \quad \text{and} \quad T_g = \left\{m \in GF(p)\colon \left(\frac{m^2-4g}{p}\right) = -1\right\}$$

Now $GF(p) = S_g \cup T_g$, and by Lemma 2.5, $|S_g| = (p-1)/2$ and $|T_g| = (p+1)/2$. Using Proposition 5.1, we proceed as in the proof of Lemma 5.8 to deduce that

$$\Theta_n(g) = \sum_{y \in \mathscr{C}} \left(\frac{V_n(\tau y + g(\tau y)^{-1}, g)}{p}\right) = 2 \sum_{m \in T_g} \left(\frac{V_n(m, g)}{p}\right).$$

Similarly,

$$\Omega_n(g) = \sum_{j \neq 0} \left(\frac{V_n(j + gj^{-1}, g)}{p}\right) = 2 \sum_{m \in S_g} \left(\frac{V_n(m, g)}{p}\right).$$

By addition of the above equalities, the desired result follows. Q.E.D.

THEOREM 5.14. *Let n be odd, $d = (n, p-1)$, and $D = (n, p+1)$. Then*

$$\begin{aligned} 2\Lambda_n(g) &= 0, && \text{if } p \equiv 3 \pmod 4,\\ &= (-1)^{(n-d)/2}\phi_{2d}(g^d) \\ &\quad + (-1)^{(n-D)/2}\left(\frac{2}{p}\right) i \sum_{j=0}^{2D-1} (-1)^j E(\psi^{2j+1}), && \text{if } p \equiv 1 \pmod 4, \end{aligned}$$

where ψ is any character on $GF(p^2)$ of order $4D$ chosen such that $\psi^D(\tau) = -i$.

Proof. By Lemma 5.13 and (5.1),

$$2\Lambda_n(g) = \sum_{j \neq 0} \left(\frac{j^d + g^n j^{-d}}{p}\right) + \sum_{y \in \mathscr{C}} \left(\frac{(\tau y)^n + (\tau y)^{np}}{p}\right). \tag{5.6}$$

If $p \equiv 3 \pmod 4$, then replacing j by $-j$ and y by $-y$ in (5.6), we have $2\Lambda_n(g) = -2\Lambda_n(g)$, and so $\Lambda_n(g) = 0$. Suppose now that $p \equiv 1 \pmod 4$. Replacing j by $g^{(n-d)/(2d)}j$, we find that the first sum on the right side of (5.6) becomes

$$\Omega_n(g) = (-1)^{(n-d)/2} \sum_{j \neq 0} \left(\frac{j^d + g^d j^{-d}}{p}\right) = (-1)^{(n-d)/2} \phi_{2d}(g^d).$$

It thus remains to evaluate the second sum $\Theta_n(g)$ on the right side of (5.6).

Let λ be a character on $GF(p^2)$ of order $2D(p-1)$ chosen so that $\lambda^{D(p-1)/2}(\tau) = -i$. Let $\psi = \lambda^{(p-1)/2}$. Thus, $\psi^D(\tau) = -i$, ψ has order $4D$, and, by Lemma 2.9, ψ_1 has order 2. Since $\lambda(\theta)$ is a primitive $2D$th root of unity, $\psi^D(y) = 1$ for all $y \in \mathscr{C}$. Thus,

$$\Theta_n(g) = \sum_{y \in \mathscr{C}} \psi^n(\tau y)\psi(1 + (\tau y)^{n(p-1)}) = \sum_{y \in \mathscr{C}} \psi^n(\tau)\psi(1 + \theta^n y^{n(p-1)}).$$

Since $2D = (n(p-1), p+1)$, the sequence $\langle y^{n(p-1)} : y \in \mathscr{C}\rangle$ is a permutation of $\langle y^{2D} : y \in \mathscr{C}\rangle$. Thus,

$$\bar{\psi}^n(\tau)\Theta_n(g) = \sum_{y \in \mathscr{C}} \psi(1 + \theta^n y^{2D}) = \sum_{y \in \mathscr{C}} \psi(1 + \theta^n y) \sum_{j=1}^{2D} \lambda^j(y).$$

Replacing y by $y\theta^{-n}$, we get

$$\begin{aligned}
\bar{\psi}^n(\tau)\Theta_n(g) &= \sum_{y \in \mathscr{C}} \psi(1+y) \sum_{j=1}^{2D} \lambda^{-jn}(\theta)\lambda^j(y) \\
&= \sum_{m=0}^{p-1} \psi\left(\frac{2}{1+m\gamma}\right) \sum_{j=1}^{2D} \lambda^{-jn(p-1)}(\tau)\lambda^{j(p-1)}(1+m\gamma) \\
&= \psi(2) \sum_{j=1}^{2D} \psi^{-2j}(\tau^n) \sum_{m=0}^{p-1} \psi^{2j-1}(1+m\gamma) \\
&= \psi(2) \sum_{j=1}^{2D} \bar{\psi}^{2j}(\tau^n) E(\psi^{2j-1}).
\end{aligned}$$

Hence,

$$\Theta_n(g) = \left(\frac{2}{p}\right) \sum_{j=0}^{2D-1} \bar{\psi}^{2j+1}(\tau^n) E(\psi^{2j+1}).$$

As $D-1$ and $n/D-1$ are both even, $n/D - 1 \equiv D(n/D-1) = n - D \pmod 4$. Hence, since $\psi(\tau^D) = -i$, $\bar{\psi}(\tau^n) = i^{n/D} = i^{n-D+1} = i(-1)^{(n-D)/2}$. Thus, $\bar{\psi}^{2j+1}(\tau^n) = i(-1)^j(-1)^{(n-D)/2}$, and the result follows. Q.E.D.

5.3 Special cases of Brewer sums. In this section, we apply the results of Section 5.2 to illustrate the evaluation of generalized Brewer sums $\Lambda_n(a)$ for certain small values of n. The formulae for $\Lambda_n(a)$ given here, except those for $\Lambda_5(a)$, may be found in the paper of Giudici, Muskat, and Robinson [7]. We do not use the theory of cyclotomy as in [7], and our method is perhaps simpler and more systematic.

By (5.5), it suffices to evaluate $\Lambda_n = \Lambda_n(1)$ and $\Lambda_n(g)$. When $n = 2k$, $\Lambda_n(g)$ can be simply determined from Λ_{2k} and Λ_k, by Theorem 5.12. When n is odd, we need evaluate Λ_n and $\Lambda_n(g)$ only when $p \equiv 1 \pmod 4$, since when $p \equiv 3 \pmod 4$, $\Lambda_n = \Lambda_n(g) = 0$ by Theorems 5.9 and 5.14.

Let $d = (n, p-1)$ and $D = (n, p+1)$. Set

$$S_1 = \left(\frac{2}{p}\right) \sum_{j=0}^{2D-1} E(\psi^{2j+1}) \quad \text{and} \quad S_2 = \left(\frac{2}{p}\right) \sum_{j=0}^{D-1} E(\chi^{2j+1}),$$

where ψ and χ have orders $4D$ and $2D$, respectively, as in Theorem 5.9. Set

$$S_3 = i\left(\frac{2}{p}\right) \sum_{j=0}^{2D-1} (-1)^j E(\psi^{2j+1}),$$

where ψ has order $4D$, as in Theorem 5.14.

When $p \equiv 1 \pmod 3$, write $p = A_3^2 + 3B_3^2$ with $A_3 \equiv 1 \pmod 3$. When $p \equiv 1 \pmod 4$, write $p = A_4^2 + B_4^2$ with $A_4 \equiv 1 \pmod 4$. When $p \equiv 1 \pmod{12}$, write $p = A_{12}^2 + B_{12}^2$ with $A_{12} = \pm A_4$ according as $3 \nmid A_4$ and $3 \mid A_4$, respectively (see [1, Theorem 3.19]). When $p = 8k+1$ or $8k+3$, write $p = A_8^2 + 2B_8^2$ with $A_8 \equiv (-1)^k \pmod 4$. When $p = 16k+1$ or $16k+7$, write $p = A_{16}^2 + 2B_{16}^2 + 2C_{16}^2 + 2D_{16}^2$ with $A_{16} \equiv (-1)^k \pmod 8$ and $2A_{16}B_{16} = D_{16}^2 - C_{16}^2 - 2C_{16}D_{16}$. When $p \equiv 1 \pmod{24}$, write $p = A_{24}^2 + 6B_{24}^2$ with $A_{24} = A_8 \pmod 3$. When $p \equiv 1 \pmod{10}$, write $p = A_{10}^2 + 5B_{10}^2 + 5C_{10}^2 + 5D_{10}^2$ with $A_{10} \equiv 1 \pmod 5$ and $A_{10}B_{10} = D_{10}^2 - C_{10}^2 - C_{10}D_{10}$. The notation in the case $p \equiv 1 \pmod{20}$ is more involved, and we defer it until the discussion of $\Lambda_5(a)$.

We proceed to evaluate $\Lambda_n(a)$ for $n = 1, 2, 3, 4, 5, 6, 8, 10$, and 12.

5.31 The sums $\Lambda_1(a)$, $\Lambda_2(a)$, $\Lambda_3(a)$, and Λ_6. Trivially, $\Lambda_1(a) = 0$. By Lemma 2.5, $\Lambda_2(a) = -1$. Since $\Lambda_3(a) = \phi_2(-3a)$, it follows from [1, Theorem 4.4] that for $p \equiv 1 \pmod 4$,

$$\begin{aligned} (5.7) \qquad \Lambda_3(a) &= -2A_4, && \text{if } -3a \text{ is a quartic residue } (\bmod p), \\ &= 2A_4, && \text{if } -3a \text{ is a quadratic residue but a quartic non-residue} \\ &= \pm 2\,|B_4|, && \text{otherwise.} \end{aligned}$$

For $a = 1$, (5.7) was first observed by Brewer [2]. We can alternatively evaluate $\Lambda_3(1)$ by the use of Theorem 5.9. (By Theorem 5.14, we can also alternatively determine $\Lambda_3(g)$.) To evaluate $\Lambda_3(1)$, we thus complete the table below, where $n = 3$.

$p \pmod{12}$	d	$\phi_{2d}(1)$	D	S_1
1	3	$-2A_4 - 4A_{12}$	1	$2A_4$
5	1	$-2A_4$	3	$2A_4 \pm 4\,|B_4|$

The values of $\phi_2(1)$ and $\phi_6(1)$ are found in [1, Theorems 4.4 and 4.8], and the values of S_1 are determined from Theorems 4.1, 4.4, and 4.10. By Theorem 5.9, we then deduce the following theorem.

THEOREM 5.15. *If* $p \equiv 3 \pmod 4$, $\Lambda_3(a)=0$. *If* $p \equiv 1 \pmod 4$, *then*

$$\begin{aligned} \Lambda_3 &= -2A_{12}, && \text{if } p \equiv 1 \pmod{12}, \\ &= \pm 2\,|B_4|, && \text{if } p \equiv 5 \pmod{12}. \end{aligned}$$

Combining (5.7) and Theorem 5.15, we deduce the following interesting consequence of the law of quartic reciprocity. When $p \equiv 1 \pmod 4$, -3 is a quartic residue $(\bmod\, p)$ if and only if $p \equiv 1 \pmod{12}$ and $3 \nmid a_4$.

In order to calculate Λ_6, we form the following table for $n=3$.

$p \pmod{12}$	Λ_3	d	$\phi_d(1)$
1	$-2A_{12}$	3	$-1-2A_3$
5	$\pm 2\,\|B_4\|$	1	-1
7	0	3	$-1-2A_3$
11	0	1	-1

The values for Λ_3, $\phi_1(1)$, and $\phi_3(1)$ are found in Theorem 5.15, Lemma 2.5, and [1, Theorem 4.2], respectively. Since $\Lambda_6 = \Lambda_3 + \phi_d(1)$ by Corollary 5.10 with $n=3$, we obtain the theorem below, due to Robinson [23].

THEOREM 5.16. *We have*

$$\begin{aligned} \Lambda_6 &= -1-2A_3-2A_{12}, && \text{if } p \equiv 1 \pmod{12}, \\ &= -1 \pm 2\,|B_4|, && \text{if } p \equiv 5 \pmod{12}, \\ &= -1-2A_3, && \text{if } p \equiv 7 \pmod{12}, \\ &= -1, && \text{if } p \equiv 11 \pmod{12}. \end{aligned}$$

5.32 The sum Λ_4. To determine Λ_4 we complete the following table for $n=4$.

$p \pmod 8$	d	D	$(p+1)/D$	$-1+\psi_{2d}(1)$	S_2
1	4	2	odd	$-2-2A_4-4A_8$	$2A_4$
3	2	4	odd	-2	$-4A_8$
5	4	2	odd	$-2-2A_4$	$2A_4$
7	2	4	even	-2	—

In the determination of $\psi_{2d}(1)$, we have used the facts that $\psi_4(1) = \psi_2(1)$ when $p \equiv 3 \pmod 4$, and $\psi_8(1) = \psi_4(1)$ when $p \equiv 5 \pmod 8$. The value of

$\psi_2(1)$ is obtained from Lemma 2.5, and the values for $\psi_4(1)$ and $\psi_8(1)$ are found in [1, Theorems 4.5 and 4.7]. The values for S_2 are obtained from Theórems 4.1, 4.4, and 4.6, with the aid of Theorem 2.10 in the case $p \equiv 3 \pmod 8$. By Theorem 5.9 and the table above, we deduce the next theorem due originally to Brewer [2]. Proofs have also been given by Whiteman [28] and Leonard and Williams [15].

THEOREM 5.17. *We have*

$$\Lambda_4 = -1 - 2A_8, \quad \text{if } p \equiv 1 \text{ or } 3 \pmod 8,$$
$$= -1, \quad \text{if } p \equiv 5 \text{ or } 7 \pmod 8.$$

5.33 The sum Λ_{12}. To calculate Λ_{12}, we compose two tables for $n = 6$, the first for $p \equiv 1 \pmod 4$ and the second for $p \equiv 3 \pmod 4$.

$p \pmod{24}$	Λ_6	d	$\phi_{2d}(1)$
1	$-1-2A_3-2A_{12}$	6	$-4A_8-8A_{24}$
5	$-1\pm 2\lvert B_4\rvert$	2	0
13	$-1-2A_3-2A_{12}$	6	0
17	$-1\pm 2\lvert B_4\rvert$	2	$-4A_8$

$p \pmod{24}$	D	$(p+1)/D \pmod 4$	S_1	Λ_6
7	2	0	—	$-1-2A_3$
11	6	2	$-4A_8$	-1
19	2	2	$-4A_8$	$-1-2A_3$
23	6	0	—	-1

The values for Λ_6 are found in Theorem 5.16, and the nonzero values for $\phi_4(1)$ and $\phi_{12}(1)$ are found in [1, Theorems 4.6 and 4.10]. Theorems 4.6, 4.18, and 2.10 and (4.24) are used in the calculations of S_1. Using the above two tables and Corollary 5.10 with $n = 6$, we deduce the following theorem.

THEOREM 5.18. *We have the following table of values for* Λ_{12}.

$p \pmod{24}$	Λ_{16}
1	$-1-2A_3-2A_{12}-2A_8-4A_{24}$
5	$-1\pm 2\lvert B_4\rvert$
7	$-1-2A_3$
11	$-1-2A_8$
13	$-1-2A_3-2A_{12}$
17	$-1-2A_8\pm 2\lvert B_4\rvert$
19	$-1-2A_8-2A_3$
23	-1

5.34 The sum Λ_8. To calculate Λ_8, we form the following two tables for $n=4$, the first for $p\equiv 1 \pmod 4$ and the second for $p\equiv 3 \pmod 4$.

$p \pmod{16}$	d	$(p-1)/d$	$\phi_{2d}(1)$	Λ_4
1	4	even	$-8A_{16}$	$-1-2A_8$
5	4	odd	—	-1
9	4	even	0	$-1-2A_8$
13	4	odd	—	-1

$p \pmod{16}$	D	$(p+1)/D \pmod 4$	S_1	Λ_4
3	4	1	—	$-1-2A_8$
7	4	2	$8A_{16}$	-1
11	4	3	—	$-1-2A_8$
15	4	0	—	-1

The values of Λ_4 were determined in Theorem 5.17, and the value of $\phi_8(1)$ for $p\equiv 1 \pmod{16}$ is given in Theorem 3.9. The value of S_1 for $p\equiv 7 \pmod{16}$ was calculated in (4.47). Using the above two tables and Corollary 5.10 with $n=4$, we deduce the following theorem.

THEOREM 5.19. *We have*

$$\begin{aligned}\Lambda_8&=-1-2A_8-4A_{16}, && \textit{if } p\equiv 1 \pmod{16},\\ &=-1, && \textit{if } p\equiv 5,\ 13, \textit{ or } 15 \pmod{16},\\ &=-1-2A_8, && \textit{if } p\equiv 3,\ 9, \textit{ or } 11 \pmod{16},\\ &=-1+4A_{16} && \textit{if } p\equiv 7 \pmod{16}.\end{aligned}$$

5.35 The sums $\Lambda_5(a)$, Λ_{10}. Let $n=5$. Let χ be a character on $GF(p^2)$ of order 40 and let $\psi=\chi^{10/D}$. Then ψ has order $4D$. Assume that χ is chosen so that $\chi^{10}(\tau)=-i$, and so, as in Theorem 5.14, $\psi^D(\tau)=-i$. Observe that χ_1^5 has order 4 and that

$$\chi_1^5(g)=\{\chi^{10}(\tau)\}^{(p+1)/2}=(-i)^{(p+1)/2}=-i\left(\frac{2}{p}\right). \tag{5.8}$$

As in [1, Theorem 3.9], write

$$K(\chi_1^5)=-\left(\frac{2}{p}\right)A_4+iB_4, \tag{5.9}$$

where $p=A_4^2+B_4^2$ and $A_4\equiv 1 \pmod 4$. By Theorems 4.1 and 4.4,

$$E(\psi^D)=\left(\frac{2}{p}\right)(A_4-iB_4). \tag{5.10}$$

When $p \equiv 1$ or 9 (mod 20), write $p = A_{20}^2 + 5B_{20}^2$ with $A_{20} \equiv A_4 \pmod 5$, if $5 \nmid A_4$, and $A_{20} \equiv B_4 \pmod 5$, if $5 \mid A_4$. In the case $p \equiv 1 \pmod{20}$, $d = 5$ and χ_1 has order 20; thus, we can write, as in [1, Theorem 3.34],

$$(5.11) \qquad \begin{aligned} K(\chi_1) &= i(A_{20} + iB_{20}\sqrt{5}), && \text{if } 5 \mid A_4, \\ &= -\left(\frac{2}{p}\right)A_{20} + iB_{20}\sqrt{5}, && \text{if } 5 \nmid A_4. \end{aligned}$$

In the case $p \equiv 9 \pmod{20}$, $D = 5$ and ψ has order 20; thus, we can write, in view of Theorem 4.22,

$$(5.12) \qquad \begin{aligned} E(\psi) &= i\left(-\left(\frac{2}{p}\right)A_{20} + iB_{20}\sqrt{5}\right), && \text{if } 5 \mid A_4, \\ &= \left(\frac{2}{p}\right)A_{20} + iB_{20}\sqrt{5}, && \text{if } 5 \nmid A_4. \end{aligned}$$

For $p \equiv 1 \pmod 4$, we have by Theorems 5.9 and 5.14, respectively,

$$(5.13) \qquad 2\Lambda_5 = \phi_{2d}(1) + S_1$$

and

$$(5.14) \qquad 2\Lambda_5(g) = \phi_{2d}(g^d) + S_3.$$

We proceed to verify the entries in the tables below.

p (mod 20)	d	$\phi_{2d}(1)$	D	S_1
1	5	$-2A_4$, if $5 \mid A_4$ $-2A_4 - 8A_{20}$, if $5 \nmid A_4$	1	$2A_4$
9	1	$-2A_4$	5	$2A_4$, if $5 \mid A_4$ $2A_4 + 8A_{20}$, if $5 \nmid A_4$
13, 17	1	$-2A_4$	1	$2A_4$

p (mod 20)	d	$\phi_{2d}(g^d)$	D	S_3
1	5	$-2B_4 - 8A_{20}$, if $5 \mid A_4$ $-2B_4$, if $5 \nmid A_4$	1	$2B_4$
9	1	$-2B_4$	5	$2B_4 + 8A_{20}$, if $5 \mid A_4$ $2B_4$, if $5 \nmid A_4$
13, 17	1	$-2B_4$	1	$2B_4$

The values of $\phi_{2d}(1)$ are immediately obtained from [1, Theorems 4.4 and 4.13].

We next calculate S_1. If $D=1$, then by (5.10),

$$S_1=2\left(\frac{2}{p}\right)\operatorname{Re}E(\psi)=2A_4,$$

as desired. Suppose that $D=5$. Then $p\equiv 9 \pmod{20}$, ψ has order 20, and $E(\psi)=E(\psi^9)$ and $E(\psi^3)=E(\psi^7)$, by Theorem 2.10. Thus,

$$S_1=2\left(\frac{2}{p}\right)\operatorname{Re}\{2E(\psi)+2E(\psi^3)+E(\psi^5)\}.$$

The desired expressions for S_1 now follow from (5.10), (5.12), and the fact that $i\sqrt{5}$ is fixed by $\sigma_3\in Gal(Q(e^{2\pi i/20})/Q)$.

We next establish the formulas for $\phi_{2d}(g^d)$. Suppose first that $d=1$. By the proof in [1, Theorem 4.4], $\phi_2(g)=2\operatorname{Re}\{\chi_1^5(-g)K(\bar{\chi}_1^5)\}$, and so by (5.8) and (5.9), $\phi_2(g)=-2B_4$, as desired. Now suppose that $d=5$. Then $p\equiv 1 \pmod{20}$, and χ_1 has order 20. By (5.8), (5.9), (5.11), and the proof in [1, Theorem 4.13], we obtain the desired expressions for $\phi_{10}(g^5)$.

Lastly, we calculate S_3. If $D=1$, then by (5.10),

$$S_3=i\left(\frac{2}{p}\right)\{E(\psi)-E(\bar{\psi})\}=2B_4,$$

as desired. Suppose that $D=5$. Proceeding in the same manner as in the calculation of S_1 above, we get

$$S_3=-2\left(\frac{2}{p}\right)\operatorname{Im}\{2\,E(\psi)-2E(\psi^3)+E(\psi^5)\}.$$

By (5.10), (5.12), and the fact that $i\sqrt{5}$ is fixed by $\sigma_3\in Gal(Q(e^{2\pi i/20})/Q)$, we obtain the desired expressions for S_3.

From (5.13), (5.14), and the tables, we obtain new proofs of the following remarkable theorems of Brewer [2], [3].

THEOREM 5.20. *We have* $\Lambda_5=0$ *unless* $p\equiv 1$ *or* $9 \pmod{20}$ *and* $5\nmid A_4$, *in which case*

$$\begin{aligned}\Lambda_5&=-4A_{20}, && \text{if } p\equiv 1 \pmod{20},\\ &=4A_{20}, && \text{if } p\equiv 9 \pmod{20}.\end{aligned}$$

THEOREM 5.21. *We have* $\Lambda_5(g)=0$ *unless* $p\equiv 1$ *or* $9 \pmod{20}$ *and* $5\mid A_4$, *in which case*

$$\begin{aligned}\Lambda_5(g)&=-4A_{20}, && \text{if } p\equiv 1 \pmod{20},\\ &=4A_{20}, && \text{if } p\equiv 9 \pmod{20}.\end{aligned}$$

Another proof of Theorem 5.20 has been given by Whiteman [29], [30].

We finally evaluate Λ_{10}. By Corollary 5.10 with $n=5$, we have $\Lambda_{10}=\Lambda_5+\phi_d(1)$. Using Theorem 5.20 to evaluate Λ_5 and using Lemma 2.5 and Theorem 3.7 to evaluate $\phi_1(1)$ and $\phi_5(1)$, respectively, we obtain the following theorem of Giudici, Muskat, and Robinson [7].

THEOREM 5.22. *We have*

$$\begin{aligned}
\Lambda_{10} &= -1, && \text{if } p\equiv 3, 7, 13, 17, \text{ or } 19 \pmod{20}, \\
& && \qquad \text{or if } p\equiv 9 \pmod{20} \text{ and } 5 \mid A_4, \\
&= -1-4A_{10}, && \text{if } p\equiv 11 \pmod{20}, \\
& && \qquad \text{or if } p\equiv 1 \pmod{20} \text{ and } 5 \mid A_4, \\
&= -1+4A_{20}, && \text{if } p\equiv 9 \pmod{20} \text{ and } 5 \nmid A_4, \\
&= -1-4A_{10}-4A_{20}, && \text{if } p\equiv 1 \pmod{20} \text{ and } 5 \nmid A_4.
\end{aligned}$$

6. Jacobsthal sums over $GF(p^2)$

Throughout the chapter, χ is a character on $GF(p^2)$ and $\beta\in GF(p^2)^*$. We shall evaluate, for certain natural numbers n, $\phi_n(\beta)$ and $\psi_n(\beta)$ over $GF(p^2)$. Because the evaluation of $\psi_{2n}(\beta)$ is usually trivial by Theorem 2.6, we shall not record any evaluations of $\psi_{2n}(\beta)$. We shall generally express $\phi_n(\beta)$ and $\psi_n(\beta)$ in terms of parameters depending only on p, e.g., a_4 and $|b_4|$. As with Jacobsthal sums over $GF(p)$, sign ambiguities often occur. The same proofs actually yield "more precise" formulations in terms of parameters occurring in the formulae for $K_2(\chi)$, e.g., a_4 and b_4. The ambiguity associated with the "$\pm$" sign does not explicitly occur in such formulations, but there is generally no simple way of determining the sign of the parameters, e.g., b_4, depending on χ, other than by the direct calculation of $K_2(\chi)$. We use the "more precise" formulations in Theorems 6.16 and 6.18, because more aesthetic statements of the theorems are then possible; generally, however, such formulations are more complicated to state.

The Jacobsthal sums $\phi_2(1)$, $\phi_3(4)$, and $\phi_4(1)$ are evaluated over arbitrary finite fields in Storer's book [25, pp. 56, 62, and 78].

THEOREM 6.1. *Let $p\equiv 1 \pmod 4$. Write $p=a_4^2+b_4^2$, where a_4 is odd. Then*

$$\begin{aligned}
\phi_2(\beta) &= 2p-4a_4^2, && \text{if } \beta \text{ is a 4th power in } GF(p^2), \\
&= -2p+4a_4^2, && \text{if } \beta \text{ is a square but not a 4th power}, \\
&= \pm 4\,|a_4b_4|, && \text{otherwise}.
\end{aligned}$$

Proof. Let χ have order 4. Then χ_1 has order 2, and so $\chi(-1)=1$. By Theorem 2.7,

$$\phi_2(\beta)=\bar{\chi}(\beta)K_2(\chi)+\chi(\beta)K_2(\bar{\chi}). \tag{6.1}$$

If $p \equiv 1 \pmod 8$, then by Theorem 4.1,

$$K_2(\chi) = -E^2(\chi) = -(a_4 + ib_4)^2 = p - 2a_4^2 - 2a_4b_4i.$$

If $p \equiv 5 \pmod 8$, then by Theorem 4.4,

$$K_2(\chi) = -(a_4 - ib_4)^2 = p - 2a_4^2 + 2a_4b_4i.$$

The evaluations now follow from (6.1). Q.E.D.

THEOREM 6.2. *Let $p \equiv 3 \pmod 4$. Then*

$$\begin{aligned} \phi_2(\beta) &= 2p, && \text{if } \beta \text{ is a 4th power in } GF(p^2), \\ &= -2p, && \text{if } \beta \text{ is a square but not a 4th power}, \\ &= 0, && \text{otherwise}. \end{aligned}$$

Proof. Let χ have order 4. Thus, χ_1 is trivial, and (6.1) holds. By Theorem 2.14, $K_2(\chi) = K_2(\chi^3) = p$. The theorem now follows from (6.1). Q.E.D.

THEOREM 6.3. *Let $p \equiv 1$ or $3 \pmod 8$ and write $p = a_8^2 + 2b_8^2$. Then*

$$\begin{aligned} \phi_4(\beta) &= -4(2a_8^2 - p), && \text{if } \beta \text{ is an 8th power in } GF(p^2), \\ &= 4(2a_8^2 - p), && \text{if } \beta \text{ is a 4th power but not an 8th power}, \\ &= 0, && \text{if } \beta \text{ is a square but not a 4th power}, \\ &= \pm 8\,|a_8b_8|, && \text{otherwise} \end{aligned}$$

Proof. Let $p = 8k + 1$, and let χ have order 8. Note that $\chi(-1) = 1$. By Theorems 2.4(i) and 4.1, $K_2(\chi^3) = K_2(\chi) = -E^2(\chi) = -(-a_8 + i(-1)^{k+1}b_8\sqrt{2})^2$. Thus, by Theorem 2.7, we get

$$\begin{aligned} \phi_4(\beta) &= 2\,\mathrm{Re}\,\{\bar{\chi}^3(\beta)K_2(\chi) + \bar{\chi}(\beta)K_2(\chi^3)\} \\ &= -2\,\mathrm{Re}\,\{(\bar{\chi}^3(\beta) + \bar{\chi}(\beta))(-a_8 + i(-1)^{k+1}b_8\sqrt{2})^2\}. \end{aligned}$$

The results now follow for $p \equiv 1 \pmod 8$.

If $p \equiv 3 \pmod 8$ and χ has order 8, then by Theorems 2.4(i) and 4.6, $K_2(\chi^3) = K_2(\chi) = (a_8 + ib_8\sqrt{2})^2$. Here, χ_1 has order 2, and so $\chi(-1) = \left(\frac{-1}{p}\right) = -1$. Thus, by Theorem 2.7, we obtain

$$\phi_4(\beta) = -2\,\mathrm{Re}\,\{(\bar{\chi}^3(\beta) + \bar{\chi}(\beta))(a_8 + ib_8\sqrt{2})^2\}.$$

The theorem for $p \equiv 3 \pmod 8$ now follows. Q.E.D.

THEOREM 6.4. *Let* $p \equiv 5$ *or* $7 \pmod 8$. *Then*

$$\begin{aligned} \phi_4(\beta) &= 4p, && \text{if } \beta \text{ is an 8th power in } GF(p^2), \\ &= -4p, && \text{if } \beta \text{ is a 4th power but not an 8th power}, \\ &= 0, && \text{otherwise.} \end{aligned}$$

Proof. Let χ have order 8. Suppose first that $p \equiv 5 \pmod 8$. Then χ_1 has order 4 from which it follows that $\chi(-1) = -1$. By Theorems 2.4(i) and 4.4, $K_2(\chi^3) = K_2(\chi) = -p$. If $p \equiv 7 \pmod 8$, then χ_1 is the trivial character, and so $\chi(-1) = 1$. By Theorems 2.4(i) and 2.14, $K_2(\chi^3) = K_2(\chi) = p$. In either case, Theorem 2.7 yields

$$\phi_4(\beta) = 2p \operatorname{Re}\{\bar{\chi}^3(\beta) + \bar{\chi}(\beta)\},$$

from which the desired evaluations follow. Q.E.D.

THEOREM 6.5. *Let* $p \equiv 1 \pmod 6$ *and write* $p = a_3^2 + 3b_3^2$. *Then*

$$\begin{aligned} \psi_3(\beta) &= 2\phi(\beta)(p - 2a_3^2), && \text{if } \beta \text{ is a cube in } GF(p^2), \\ &= \phi(\beta)(-p + 2a_3^2 + 6\eta_3\,|a_3b_3|), && \text{otherwise,} \end{aligned}$$

where $\eta_3 = \pm 1$.

Proof. Let χ have order 6. If $p \equiv 1 \pmod{12}$, we find from Theorem 4.8 that

$$K_2(\chi^2) = -(a_3 + ib_3\sqrt{3})^2.$$

If $p \equiv 7 \pmod{12}$, Theorem 4.9 shows that

$$K_2(\chi^2) = -(a_3 - ib_3\sqrt{3})^2.$$

Thus, by Theorem 2.8,

$$\begin{aligned} \psi_3(\beta) &= 2\phi(\beta) \operatorname{Re}\{\chi^2(\beta) K_2(\chi^2)\} \\ &= 2\phi(\beta) \operatorname{Re}\{\chi^2(\beta)(p - 2a_3^2 \pm 2ia_3b_3\sqrt{3})\}. \end{aligned} \tag{6.2}$$

The results now follow. Q.E.D.

THEOREM 6.6. *Let* $p \equiv 5 \pmod 6$. *Then*

$$\begin{aligned} \psi_3(\beta) &= 2p\phi(\beta), && \text{if } \beta \text{ is a cube in } GF(p^2), \\ &= -p\phi(\beta), && \text{otherwise.} \end{aligned}$$

Proof. Let χ have order 6. By Theorem 2.14, $K_2(\chi^2) = p$. Thus, by Theorem 2.8, $\psi_3(\beta) = 2p\phi(\beta) \operatorname{Re} \chi^2(\beta)$, from which the theorem is easily concluded. Q.E.D.

THEOREM 6.7. *Let* $p \equiv 1 \pmod 6$ *and write* $p = a_3^2 + 3b_3^2$. *Then*

$$\begin{aligned} \phi_3(\beta) &= 2p - 1 - 4a_3^2, && \text{if } \beta \text{ is a cube in } GF(p^2), \\ &= -p - 1 + 2a_3^2 - 6\eta_3\,|a_3b_3|, && \text{otherwise,} \end{aligned}$$

where η_3 *is as in Theorem* 6.5.

Proof. Let χ be as in the proof of Theorem 6.5. Then $\chi(-1)=1$. By Theorem 2.14, $K_2(\chi^3)=-1$. Hence, by Theorem 2.7, Theorem 2.4(i), and (6.2),

$$\begin{aligned}\phi_3(\beta)&=-1+2\operatorname{Re}\{\bar{\chi}^2(\beta)K_2(\chi)\}\\&=-1+2\operatorname{Re}\{\bar{\chi}^2(\beta)K_2(\chi^2)\}\\&=-1+\phi(\beta)\psi_3(\beta^{-1}).\end{aligned}$$

The result now follows from Theorem 6.5 and (6.2). Q.E.D.

THEOREM 6.8. *Let $p\equiv 5 \pmod 6$. Then*

$$\begin{aligned}\phi_3(\beta)&=2p-1, &&\textit{if } \beta \textit{ is a cube in } GF(p^2),\\&=-p-1, &&\textit{otherwise.}\end{aligned}$$

Proof. Let χ have order 6. As χ_1 is trivial, $\chi(-1)=1$. By Theorem 2.14, $K(\chi^3)=-1$ and $K(\chi)=p$. By Theorem 2.7, we then get $\phi_3(\beta)=-1+2p\operatorname{Re}\bar{\chi}^2(\beta)$, from which the theorem is immediate. Q.E.D.

In most of the following theorems, the values of $\phi_n(\beta)$ will be displayed in tables. Columns will indicate the residuacity of β in $GF(p^2)$. Thus, for example, if an x appears in the column headed by "cubic," it is assumed that β is a cube in $GF(p^2)$; if no x appears in the column headed by "8th," then it is assumed that β is not an 8th power in $GF(p^2)$.

THEOREM 6.9. *Let $p=12k+1$. Write $p=a_4^2+b_4^2$, where a_4 is odd. Then we have the following table of values for $\phi_6(\beta)$:*

$\phi_6(\beta)$	square	cube	4th
$6(p-2a_4^2)$	x	x	x
$-6(p-2a_4^2)$	x	x	
0	x		x
0	x		
$\pm 4\,\lvert a_4b_4\rvert$		x	
$\pm 8\,\lvert a_4b_4\rvert$			

Proof. Let χ have order 12. Then $\chi(-1)=1$. By Theorems 2.4(i) and 4.8,

$$K_2(\chi)=K_2(\chi^3)=K_2(\chi^5)=-(a_4\pm ib_4)^2.$$

Thus, by Theorem 2.7,

$$\phi_6(\beta)=-2\operatorname{Re}\{(\bar{\chi}(\beta)+\bar{\chi}^3(\beta)+\bar{\chi}^5(\beta))(a_4\pm ib_4)^2\}.$$

Now,

$$\chi(\beta)+\chi^3(\beta)+\chi^5(\beta)=3,\ -3,\ 0,\ 0,\ \pm i,\ \pm 2i, \tag{6.3}$$

according as β is on lines 1, 2, 3, 4, 5, or 6, respectively, of the table. The theorem now follows by the consideration of each of the six cases. Q.E.D.

THEOREM 6.10. *Let* $p=12k+5$. *Write* $p=a_4^2+b_4^2$, *where* a_4 *is odd. Then we have the following table of values for* $\phi_6(\beta)$:

$\phi_6(\beta)$	square	cube	4th
$-2(p-2a_4^2)$	x	x	x
$2(p-2a_4^2)$	x	x	
$4(p-2a_4^2)$	x		x
$-4(p-2a_4^2)$	x		
$\pm 12\,\lvert a_4b_4\rvert$		x	
0			

Proof. Let χ have order 12. Then $\chi(-1)=1$. By Theorems 2.4(i) and 4.10,

$$K_2(\chi)=K_2(\chi^5)=-K_2(\chi^3)=-(ia_4\pm b_4)^2.$$

Thus, by Theorem 2.7,

$$\phi_6(\beta)=2\,\mathrm{Re}\,\{(\bar\chi(\beta)-\bar\chi^3(\beta)+\bar\chi^5(\beta))(2a_4^2-p\pm 2ia_4b_4)\}.$$

Now,

$$\chi(\beta)-\chi^3(\beta)+\chi^5(\beta)=1,-1,-2,2,\pm 3i, \quad\text{or}\quad 0,$$

according as β is in lines 1, 2, 3, 4, 5, or 6, respectively, of the table. The result follows. Q.E.D.

THEOREM 6.11. *Let* $p\equiv 3 \pmod 4$. *Then*

$$\begin{aligned}\phi_6(\beta)&=6p, && \text{if } \beta \text{ is a 12th power in } GF(p^2),\\ &=-6p, && \text{if } \beta \text{ is a 6th power but not a 12th power},\\ &=0, && \text{otherwise}.\end{aligned}$$

Proof. Let χ have order 12. If $p\equiv 7 \pmod{12}$, χ_1 has order 3, and so $\chi(-1)=1$. If $p\equiv 11 \pmod{12}$, $\chi(-1)=1$ as χ_1 is trivial. Now $K_2(\chi^5)=K_2(\chi)=p$ by Theorem 2.4(i) and by Theorem 4.9, if $p\equiv 7 \pmod{12}$, and by Theorem 2.14, if $p\equiv 11 \pmod{12}$. In both cases, $K_2(\chi^3)=p$ by Theorem 2.14. Thus, Theorem 2.7 yields

$$\phi_6(\beta)=2p\,\mathrm{Re}\,\{\bar\chi(\beta)+\bar\chi^3(\beta)+\bar\chi^5(\beta)\}.$$

With the aid of (6.3), the results now follow. Q.E.D.

THEOREM 6.12. *Let* $p=24k+1$. *Write* $p=a_8^2+2b_8^2=a_{24}^2+6b_{24}^2$. *Then we* *have the following table for* $\phi_{12}(\beta)$:

$\phi_{12}(\beta)$	square	cube	4th	8th
$12p-8a_8^2-16a_{24}^2$	x	x	x	x
$-12p+8a_8^2+16a_{24}^2$	x	x	x	
$-8a_8^2+8a_{24}^2$	x		x	x
$8a_8^2-8a_{24}^2$	x		x	
0	x	x		
0	x			
$\pm 8\lvert a_8b_8\rvert$		x		
$\pm 8\lvert a_8b_8\rvert \pm 24\lvert a_{24}b_{24}\rvert$				

Proof. Let χ have order 24. Then χ_1 has order 12 and $\chi(-1)=1$. Since $\{\sigma_5, \sigma_7, \sigma_{11}\} \subset Gal(Q(e^{2\pi i/24})/Q)$ fixes $i\sqrt{6}$, we deduce from Theorem 4.11 that

$$K_2(\chi)=K_2(\chi^5)=K_2(\chi^7)=K_2(\chi^{11})=-(-a_{24}+i(-1)^{k+1}b_{24}\sqrt{6})^2.$$

By Theorems 2.4(i) and 4.1, $K_2(\chi^3)=K_2(\chi^9)=-(a_8\pm ib_8\sqrt{2})^2$. Thus, by Theorem 2.7, we get

$$\phi_{12}(\beta)=-2\,\mathrm{Re}\,\{(\chi(\beta)+\chi^5(\beta)+\chi^7(\beta)+\chi^{11}(\beta))(a_{24}\pm ib_{24}\sqrt{6})^2$$

$$+(\chi^3(\beta)+\chi^9(\beta))(a_8\pm ib_8\sqrt{2})^2\}$$

$$=-2\,\mathrm{Re}\,\{\chi(\beta)(1+\chi^4(\beta))(1+\chi^6(\beta))(2a_{24}^2-p\pm 2ia_{24}b_{24}\sqrt{6})$$

$$+\chi^3(\beta)(1+\chi^6(\beta))(2a_8^2-p\pm 2ia_8b_8\sqrt{2})\}.$$

The theorem now follows upon the examination of each of the cases. The last case is facilitated by the observation that $\cos(\pi/12)=(\sqrt{6}+\sqrt{2})/4$ and $\sin(\pi/12)=(\sqrt{6}-\sqrt{2})/4$. Q.E.D.

The next theorem summarizes the values of $\phi_{12}(\beta)$ for $p\equiv 5$, 7, 11, 13, 17, 19, and 23 (mod 24). The proofs are very similar to the proof of Theorem 6.12, and so we omit them. Below the residue class designation of p, we give the quadratic representations (if any) of p used in the evaluations below. The eight rows of values in the tables correspond in order to the residuacities of β found in the table of Theorem 6.12.

THEOREM 6.13. *For* $p\equiv 5$, 7, 11, 13, 17, 19, *and* 23 (mod 24), *we have* *the following table of values for* $\phi_{12}(\beta)$:

$p\equiv 5 \pmod{24}$ $p=3e_{24}^2+2f_{24}^2$	$p\equiv 7 \pmod{24}$ $p=a_{24}^2+6b_{24}^2$	$p\equiv 11 \pmod{24}$ $p=a_8^2+2b_8^2$ $p=3e_{24}^2+2f_{24}^2$
$12p-48e_{24}^2$	$-4p+16a_{24}^2$	$12p-8a_8^2-48e_{24}^2$
$-12p+48e_{24}^2$	$4p-16a_{24}^2$	$-12p+8a_8^2+48e_{24}^2$
$24e_{24}^2$	$48b_{24}^2$	$-8a_8^2+24e_{24}^2$
$-24e_{24}^2$	$-48b_{24}^2$	$8a_8^2-24e_{24}^2$
0	0	0
0	0	0
0	0	$\pm 8\,\lvert a_8b_8\rvert$
$\pm 24\,\lvert e_{24}f_{24}\rvert$	$\pm 24\,\lvert a_{24}b_{24}\rvert$	$\pm 8\,\lvert a_8b_8\rvert \pm 24\,\lvert e_{24}f_{24}\rvert$

$p\equiv 13, 23 \pmod{24}$	$p\equiv 17 \pmod{24}$ $p=a_8^2+2b_8^2$	$p\equiv 19 \pmod{24}$ $p=a_8^2+2b_8^2$
$12p$	$12p-8a_8^2$	$-4p-8a_8^2$
$-12p$	$-12p+8a_8^2$	$4p+8a_8^2$
0	$-8a_8^2$	$16b_8^2$
0	$8a_8^2$	$-16b_8^2$
0	0	0
0	0	0
0	$\pm 8\,\lvert a_8b_8\rvert$	$\pm 8\,\lvert a_8b_8\rvert$
0	$\pm 8\,\lvert a_8b_8\rvert$	$\pm 8\,\lvert a_8b_8\rvert$

THEOREM 6.14. *Let* $p=20k+1$ *or* $20k+9$. *Write* $p=a_4^2+b_4^2$, *where* a_4 *is odd, and* $p=a_{20}^2+5b_{20}^2$, *as in Theorems* 4.20 *and* 4.22. *Then we have the following table*:

$\phi_{10}(\beta)$, if $5\nmid a_4$	$\phi_{10}(\beta)$, if $5\mid a_4$	square	4th	5th
$10p-4a_4^2-16a_{20}^2$	$-6p-4a_4^2+16a_{20}^2$	x	x	x
$-10p+4a_4^2+16a_{20}^2$	$6p+4a_4^2-16a_{20}^2$	x		x
$\pm 4\,\lvert a_4b_4\rvert$	$\pm 4\,\lvert a_4b_4\rvert$			x
$-4a_4^2+4a_{20}^2$	$4b_4^2-4a_{20}^2$	x	x	
$4a_4^2-4a_{20}^2$	$-4b_4^2+4a_{20}^2$	x		
$\pm 4\,\lvert a_4b_4\rvert \pm 20\,\lvert a_{20}b_{20}\rvert$	$\pm 4\,\lvert a_4b_4\rvert \pm 20\,\lvert a_{20}b_{20}\rvert$			

Proof. Let χ have order 20. If $p\equiv 1 \pmod{20}$, then χ_1 has order 10 and $\chi(-1)=1$. If $p\equiv 9 \pmod{20}$, then χ_1 has order 2 and $\chi(-1)=1$.

By Theorems 4.1 and 4.4, $K_2(\chi^5)=-(a_4\pm ib_4)^2$. Since $i\sqrt{5}$ is fixed by $\{\sigma_3,\sigma_7,\sigma_{11}\}\subset Gal(Q(e^{2\pi i/20})/Q)$, it follows from Theorems 4.20 and 4.22 that

$$K_2(\chi^9)=K_2(\chi)=K_2(\chi^3)=K_2(\chi^7)=\varepsilon(a_{20}\pm ib_{20}\sqrt{5})^2,$$

where $\varepsilon=-1$ or 1 according as $5\nmid a_4$ or $5\mid a_4$, respectively. Thus, by Theorem 2.7,

$$\begin{aligned}\phi_{10}(\beta)=2\operatorname{Re}\{\chi(\beta)(1+\chi^2(\beta))(1+\chi^6(\beta))\varepsilon(2a_{20}^2-p\pm 2ia_{20}b_{20}\sqrt{5})\\ +\chi^5(\beta)(p-2a_4^2\pm 2ia_4b_4)\}.\end{aligned}$$

The evaluations now follow. The last case is facilitated by the observations that $\cos(\pi/5)=(\sqrt{5}+1)/4$ and $\cos(2\pi/5)=(\sqrt{5}-1)/4$. Q.E.D.

THEOREM 6.15. *Let $p\equiv 11$ or 19 (mod 20). Then*

$$\begin{aligned}\phi_{10}(\beta)&=10p, && \text{if } \beta \text{ is a 20th power in } GF(p^2),\\ &=-10p, && \text{if } \beta \text{ is a 10th power but not a 20th power},\\ &=0, && \text{otherwise.}\end{aligned}$$

Proof. Let χ have order 20. Then $\chi(-1)=1$. By Theorems 2.14 and 4.21, $K(\chi^j)=p$ for each odd integer j. Thus, by Theorem 2.7,

$$\phi_{10}(\beta)=2p\operatorname{Re}\sum_{j=0}^{4}\chi^{2j+1}(\beta),$$

and the result follows. Q.E.D.

Let $p=10k+1$ and let χ have order 10. By Theorems 4.20 and 4.21 and the remark at the end of Section 3.1, $K_2(\chi)=-K^2(\chi_1^2)$. In view of Theorem 3.1, we may write

$$K_2(\chi)=-\{a_{10}+b_{10}\sqrt{5}+ic_{10}\sqrt{5+2\sqrt{5}}+id_{10}\sqrt{5-2\sqrt{5}}\}^2, \tag{6.4}$$

where the integers a_{10}, b_{10}, c_{10}, and d_{10} satisfy (i), (ii), and (iii) of Theorem 3.1.

THEOREM 6.16. *Let $p=10k+1$. Fix $\beta\in GF(p^2)^*$. Let χ have order 10 and assume that χ is chosen such that $\bar{\chi}^4(\beta)=e^{2\pi i/5}$ when β is not a fifth power in $GF(p^2)$. Then, in the notation above, if β is a fifth power in $GF(p^2)$,*

$$\phi_5(\beta)=-1+4(p-2a_{10}^2-10b_{10}^2)\quad\textit{and}\quad \psi_5(\beta)=4\phi(\beta)(p-2a_{10}^2-10b_{10}^2);$$

otherwise,

$$\phi_5(\beta)=$$
$$-1-p+2a_{10}^2+10b_{10}^2-20a_{10}b_{10}+30b_{10}c_{10}+10(a_{10}c_{10}+a_{10}d_{10}-b_{10}d_{10})$$

and

$\psi_5(\beta)=$

$\phi(\beta)\{-p+2a_{10}^2+10b_{10}^2-20a_{10}b_{10}-30b_{10}c_{10}-10(a_{10}c_{10}+a_{10}d_{10}-b_{10}d_{10})\}.$

Proof. By Theorem 2.7,

$$\phi_5(\beta)=K_2(\chi^5)+2\operatorname{Re}\{\bar{\chi}^4(\beta)K_2(\chi)+\bar{\chi}^2(\beta)K_2(\chi^3)\}.$$

By Theorems 2.8 and 2.4(i),

$$\psi_5(\beta)=2\phi(\beta)\operatorname{Re}\{\chi^4(\beta)K_2(\chi)+\chi^2(\beta)K_2(\chi^3)\}.$$

By Theorem 2.14, $K_2(\chi^5)=-1$. Applying $\sigma_3\in Gal(Q(e^{2\pi i/10})/Q)$ to (6.4), we have

$$K_2(\chi^3)=-\{a_{10}-b_{10}\sqrt{5}+ic_{10}\sqrt{5-2\sqrt{5}}-id_{10}\sqrt{5+2\sqrt{5}}\}^2.$$

The result now follows. The computations are facilitated by the use of (3.2). Q.E.D.

Example. Let $p=11$. Choose $\gamma\in GF(p^2)$ so that $\gamma^2=2$. Thus, $\tau=2+\gamma$ generates $GF(p^2)^*$. Then $a_{10}=-1$ and $|b_{10}|=1$. If $\beta=1$, then $\phi_5(\beta)=-5$ and $\psi_5(\beta)=-4$. If $\beta=\tau$ or τ^{-1}, then $b_{10}=-1$, $c_{10}=0$, $|d_{10}|=1$, $\phi_5(\beta)=-20$, and $\psi_5(\beta)=19$. If $\beta=\tau^2$, then $b_{10}=1$, $c_{10}=1$, $d_{10}=0$, $\phi_5(\beta)=40$, and $\psi_5(\beta)=1$. If $\beta=\tau^{-2}$, then $b_{10}=1$, $c_{10}=-1$, $d_{10}=0$, $\phi_5(\beta)=0$, and $\psi_5(\beta)=41$.

THEOREM 6.17. *Let* $p\equiv 9 \pmod{10}$. *Then*

$$\begin{aligned}\phi_5(\beta)&=-1+4p, && \text{if } \beta \text{ is a 5th power in } GF(p^2),\\ &=-1-p, && \text{otherwise,}\end{aligned}$$

and $\psi_5(\beta)=\phi(\beta)\{1+\phi_5(\beta)\}$.

Proof. Let χ have order 10. Then χ_1 is trivial and $\chi(-1)=1$. By Theorem 2.14, $K_2(\chi^5)=-1$ and $K_2(\chi^j)=p$ for $1\le j\le 4$. Hence, by Theorems 2.7 and 2.8, respectively,

$$\phi_5(\beta)=-1+2p\operatorname{Re}\{\chi^2(\beta)+\chi^4(\beta)\} \text{ and } \psi_5(\beta)=2\phi(\beta)p\operatorname{Re}\{\chi^2(\beta)+\chi^4(\beta)\}.$$

The theorem now follows. Q.E.D.

Let $p=16k+1$ or $16k+7$. Let χ have order 16. If $p\equiv 1 \pmod{16}$, then χ_1 has order 8 and $\chi(-1)=1$. If $p\equiv 7 \pmod{16}$, then χ_1 has order 2 and $\chi(-1)=-1$. By Theorem 2.4(i), $K_2(\chi)=K_2(\chi^7)$. In view of Theorems 4.26 and 4.28, we may thus write

(6.5)

$$\chi(-1)K_2(\chi)=\chi(-1)K_2(\chi^7)=-\{A_{16}+B_{16}\sqrt{2}+iC_{16}\sqrt{2+\sqrt{2}}+iD_{16}\sqrt{2-\sqrt{2}}\}^2,$$

where A_{16}, B_{16}, C_{16}, and D_{16} are integers such that $A_{16} \equiv (-1)^k \pmod 8$,

$$p = A_{16}^2 + 2B_{16}^2 + 2C_{16}^2 + 2D_{16}^2, \quad \text{and} \quad 2A_{16}B_{16} = D_{16}^2 - C_{16}^2 - 2C_{16}D_{16}.$$

THEOREM 6.18. *Let $p = 16k+1$ or $16k+7$. Fix $\beta \in GF(p^2)^*$. Let χ have order 16 and assume that χ is chosen such that*

$$\begin{aligned} \bar{\chi}(\beta) &= e^{2\pi i/16}, \quad \text{if } \beta \text{ is not a square in } GF(p^2), \\ &= e^{2\pi i/8}, \quad \text{if } \beta \text{ is a square but not a 4th power.} \end{aligned}$$

Then, in the notation above, we have the following table:

$\phi_8(\beta)$	square	4th	8th	16th
$8(p-2A_{16}^2-4B_{16}^2)$	x	x	x	x
$-8(p-2A_{16}^2-4B_{16}^2)$	x	x	x	
0	x	x		
$-32A_{16}B_{16}$	x			
$16(A_{16}D_{16}+B_{16}C_{16}-B_{16}D_{16})$				

Proof. Applying $\sigma_3 \in Gal(Q(e^{2\pi i/16})/Q)$ to (6.5), we have

$$\chi(-1)K_2(\chi^3) = \chi(-1)K_2(\chi^5) = -\{A_{16} - B_{16}\sqrt{2} - iC_{16}\sqrt{2-\sqrt{2}} + iD_{16}\sqrt{2+\sqrt{2}}\}^2.$$

By Theorem 2.7,

$$\phi_8(\beta) = 2\,\mathrm{Re}\,\{\bar{\chi}(\beta)(1+\bar{\chi}^6(\beta))\chi(-1)K_2(\chi)\} + 2\,\mathrm{Re}\,\{\bar{\chi}^3(\beta)(1+\bar{\chi}^2(\beta))\chi(-1)K_2(\chi^3)\}.$$

The evaluations now follow. Q.E.D.

Example. Let $p=7$. Choose $\gamma \in GF(p^2)$ so that $\gamma^2 = 3$. Thus, $\tau = 1+\gamma$ generates $GF(p^2)^*$. If $\beta = \tau$ or τ^2, then $A_{16} = B_{16} = C_{16} = 1$ and $D_{16} = -1$. Thus, $\phi_8(\beta) = 16$, if $\beta = \tau$, and $\phi_8(\beta) = -32$, if $\beta = \tau^2$. Also, $\phi_8(\beta) = 8$, -8, and 0 according as $\beta = \tau^{16}$, τ^8, and τ^4, respectively.

THEOREM 6.19. *Let $p \equiv 9$ or $15 \pmod{16}$. Then*

$$\begin{aligned} \phi_8(\beta) &= 8p, \quad \text{if } \beta \text{ is a 16th power in } GF(p^2), \\ &= -8p, \quad \text{if } \beta \text{ is an 8th power but not a 16th power,} \\ &= 0, \quad \text{otherwise.} \end{aligned}$$

Proof. Let χ have order 16. If $p \equiv 9 \pmod{16}$, then χ_1 has order 8 and $\chi(-1) = -1$. If $p \equiv 15 \pmod{16}$, then χ_1 is the trivial character and $\chi(-1) = 1$. By Theorems 2.14 and 4.27, $K_2(\chi^j) = \chi(-1)p$ for odd j. Theorem 2.7 thus yields

$$\phi_8(\beta) = 2p \operatorname{Re} \sum_{j=0}^{3} \chi^{2j+1}(\beta),$$

and the result follows. Q.E.D.

7. Gauss sums over $GF(p^2)$

In this chapter, we evaluate the Gauss sum

$$\mathcal{G}_k = \sum_{\alpha \in GF(p^2)} e^{2\pi i \operatorname{tr}(\alpha^k)/p}$$

for $k = 2$, 3, 4, 6, 8, and 12. We could similarly evaluate other Gauss sums, e.g., $\mathcal{G}_{24}$, but we omit these evaluations for brevity.

Generalizations of Theorems 7.1 and 7.2 have been given by Myerson [18]. Theorem 7.1 was proved by Stickelberger [24, p. 341].

THEOREM 7.1. *For each odd prime p, we have $\mathcal{G}_2 = G_2(\phi) = (-1)^{(p+1)/2}p$.*

Proof. Using Theorem 2.12, we find that

$$\mathcal{G}_2 = \sum_{\alpha} \{1 + \phi(\alpha)\} e^{2\pi i \operatorname{tr}(\alpha)/p} = G_2(\phi) = (-1)^{(p+1)/2}p. \qquad \text{Q.E.D.}$$

THEOREM 7.2. *Write $p = a_4^2 + b_4^2$ with $a_4 \equiv -\left(\frac{2}{p}\right) \pmod 4$ when $p \equiv 1 \pmod 4$. Then*

$$\begin{aligned} \mathcal{G}_4 &= -p - 2\left(\frac{2}{p}\right) a_4\sqrt{p}, \quad \text{if } p \equiv 1 \pmod 4, \\ &= p + 2(-1)^{(p+1)/4} p, \quad \text{if } p \equiv 3 \pmod 4. \end{aligned}$$

Proof. Let χ have order 4. Then, since $G_2(\phi) = (-1)^{(p+1)/2}p$ by Theorem 7.1, we have

$$\mathcal{G}_4 = (-1)^{(p+1)/2}p + G_2(\chi) + G_2(\bar{\chi}). \tag{7.1}$$

First, suppose that $p \equiv 1 \pmod 4$. Then χ_1 has order 2. Hence, by (7.1) and Theorem 2.12, we find that

$$\mathcal{G}_4 = -p + \left(\frac{2}{p}\right)\{E(\chi) + E(\bar{\chi})\}\sqrt{p},$$

from which the result follows by Theorems 4.1 and 4.4.

Secondly, suppose that $p \equiv 3 \pmod 4$. Then χ_1 is the trivial character. The result now follows immediately from (7.1) and Theorem 2.12. Q.E.D.

THEOREM 7.2. *Write $p = a_4^2 + b_4^2$ with $a_4 \equiv -\left(\frac{2}{p}\right) \pmod 4$ when $p \equiv 1$*

(mod 4). *Write* $p=a_8^2+2b_8^2$ *with* $a_8\equiv(-1)^{(p-3)/8}$ (mod 4) *when* $p\equiv 3$ (mod 8). *Then*

$$\begin{aligned}\mathcal{G}_8&=-p-2a_4\sqrt{p}\pm 2a_8(2p+2a_4\sqrt{p})^{1/2}, &&\text{if } p\equiv 1 \pmod 8,\\ &=-p-4ia_8\sqrt{p}, &&\text{if } p\equiv 3 \pmod 8,\\ &=-p+2a_4\sqrt{p}\pm 4i\,|b_4|\,p(2p+2a_4\sqrt{p})^{-1/2}, &&\text{if } p\equiv 5 \pmod 8,\\ &=3p+4(-1)^{(p+1)/8}p, &&\text{if } p\equiv 7 \pmod 8.\end{aligned}$$

Proof. Let χ have order 8. Then

$$\mathcal{G}_8=\mathcal{G}_4+S_8, \tag{7.2}$$

where $S_8=G_2(\chi)+G_2(\bar{\chi})+G_2(\chi^3)+G_2(\bar{\chi}^3)$. We have evaluated $\mathcal{G}_4$ in Theorem 7.2, and it remains to evaluate S_8.

First, suppose that $p\equiv 1$ (mod 8). Then χ_1 has order 4 and $\chi(-1)=1$. By Theorem 2.12,

$$G_2(\chi)=\bar{\chi}_1(2)E(\chi)G(\chi_1) \quad\text{and}\quad G_2(\chi^3)=\chi_1(2)E(\chi^3)G(\bar{\chi}_1).$$

Since $\sigma_3\in Gal(Q(e^{2\pi i/8})/Q)$ fixes $i\sqrt{2}$, Theorem 4.1 shows that

$$E(\chi^3)=E(\chi)=-a_8\pm ib_8\sqrt{2}.$$

Note that $\chi_1(2)=\pm 1$. Hence,

$$S_8=-2\chi_1(2)a_8\{G(\chi_1)+G(\bar{\chi}_1)\}=\pm 2a_8(2p+2a_4\sqrt{p})^{1/2},$$

as desired, where the last equality follows from [1, equation (3.10)].

Secondly, assume that $p\equiv 3$ (mod 8). Then χ_1 has order 2 and $\chi_1(2)=\left(\frac{2}{p}\right)=-1$. By Theorem 2.10, $E(\chi)=E(\chi^3)$. Thus, by Theorem 2.12, $G_2(\chi)=-i\sqrt{p}E(\chi)=G_2(\chi^3)$. Hence, by Theorem 4.6,

$$S_8=-2i\sqrt{p}\{E(\chi)+E(\bar{\chi})\}=-4ia_8\sqrt{p},$$

as desired.

Thirdly, suppose that $p\equiv 5$ (mod 8). Then χ_1 has order 4. Hence, $\chi_1(-1)=-1$ and $\chi_1(2)=\pm i$. By Theorem 2.10,

$$E(\chi^3)=E(\bar{\chi}^5)=E(\bar{\chi})=a_4+ib_4, \tag{7.3}$$

as in Theorem 4.4. Thus, by Theorem 2.12, $G_2(\chi)=\bar{\chi}_1(2)G(\chi_1)E(\chi)=G_2(\bar{\chi}^3)$. Hence,

$$S_8=2\bar{\chi}_1(2)\{G(\chi_1)E(\chi)-G(\bar{\chi}_1)E(\bar{\chi})\}=\pm 4i\,\mathrm{Re}\,\{G(\chi_1)E(\chi)\}. \tag{7.4}$$

Now set $R_6=G(\chi_1)+G(\bar{\chi}_1)$. By [1, equation (3.10)], $R_6=\pm i(2p+2a_4\sqrt{p})^{1/2}$. Let $D_6=G(\chi_1)-G(\bar{\chi}_1)$. Thus, D_6 is real and $2G(\chi_1)=D_6+R_6$. Hence, by

(7.3) and (7.4),

$$S_8 = \pm 2i(D_6 a_4 - iR_6 b_4). \tag{7.5}$$

We now compute D_6. By Theorems 2.2 and 4.4,

$$R_6 D_6 = G^2(\chi_1) - G^2(\bar{\chi}_1) = \{J(\chi_1) - J(\bar{\chi}_1)\}\sqrt{p} = -\{K(\chi_1) - K(\bar{\chi}_1)\}\sqrt{p} = -2ib_4\sqrt{p}.$$

Thus, $D_6 = -2ib_4\sqrt{p}/R_6$. Putting this in (7.5), we obtain

$$S_8 = \pm 2\,|b_4|\,(2a_4\sqrt{p} + R_6^2)/R_6 = \pm 4\,|b_4|\,p/R_6,$$

as desired.

Lastly, suppose that $p \equiv 7 \pmod 8$. By Theorem 2.12, $G_2(\chi^j) = (-1)^{(p+1)/8}p$ for each odd integer j. Thus, $S_8 = 4(-1)^{(p+1)/8}p$, as desired. Q.E.D.

For the purposes of evaluating $\mathscr{G}_3$ and $\mathscr{G}_6$, we recall some facts and notation from [1]. Let $p \equiv 1 \pmod 6$ and let χ have order 6. Then χ_1 is a character $(\mathrm{mod}\, p)$ of order 3, and [1, Theorems 3.3, 3.4]

$$K(\chi_1) = a_3 + ib_3\sqrt{3} \quad \text{and} \quad 2J(\chi_1) = r_3 + is_3\sqrt{3}, \tag{7.6}$$

where a_3, b_3, r_3, and s_3 are integers such that $p = a_3^2 + 3b_3^2$, $4p = r_3^2 + 3s_3^2$, and $r_3 \equiv -a_3 \equiv 1 \pmod 3$. Let $G_3 = \sum_n e^{2\pi i n^3/p}$ and define $\nu = \operatorname{sgn}\{s_3(G_3^2 - p)\}$. Then [1, Theorem 3.7],

$$2G(\chi_1) = G_3 + i\nu(4p - G_3^2)^{1/2}. \tag{7.7}$$

Define ε_3 by $\varepsilon_3 = \pm 1$ and $\varepsilon_3 \equiv |b_3| \pmod 3$. Define

$$\varepsilon_6 = \operatorname{sgn}\{(a_3 + \varepsilon_3\,|b_3|)(G_3^2 - p)\}.$$

When $\chi_1(2) = 1$, we have $\operatorname{sgn} b_3 = \operatorname{sgn} s_3$ [1, equation (3.1)]; hence,

$$b_3\nu = |b_3|\,\nu \operatorname{sgn} s_3 = |b_3| \operatorname{sgn}(G_3^2 - p), \tag{7.8}$$

when $\chi_1(2) = 1$. When $\chi_1(2) \neq 1$, define α by $\alpha = \pm 1$ and $\chi_1(2) = \exp(2\pi i\alpha/3)$. In [1], the proof of Theorem 3.8 and the paragraph immediately preceding Theorem 3.5 show that, respectively,

$$\alpha\nu = \varepsilon_6 \quad \text{and} \quad \alpha b_3 = -\varepsilon_3\,|b_3|. \tag{7.9}$$

THEOREM 7.4. *If* $p \equiv 5 \pmod 6$, *then* $\mathscr{G}_3 = 2p$. *If* $p \equiv 1 \pmod 6$, *then, in the notation above,*

$$\mathscr{G}_3 = -a_3G_3 - \{\operatorname{sgn}(G_3^2 - p)\}\,|b_3|\,(12p - 3G_3^2)^{1/2},$$

if 2 *is a cubic residue* $(\mathrm{mod}\, p)$,

$$= \tfrac{1}{2}G_3(a_3 - 3\varepsilon_3\,|b_3|) - \tfrac{1}{2}\varepsilon_6(a_3 + \varepsilon_3\,|b_3|)(12p - 3G_3^2)^{1/2},$$

if 2 *is a cubic nonresidue* $(\mathrm{mod}\, p)$.

Proof. Let χ have order 6. Then

$$\mathcal{G}_3 = G_2(\chi^2) + G_2(\bar{\chi}^2) = 2\,\mathrm{Re}\, G_2(\chi^2). \tag{7.10}$$

First, suppose that $p \equiv 5 \pmod 6$. Then by Theorem 2.12, $G_2(\chi^2) = p$, and the result follows from (7.10).

Secondly, let $p \equiv 1 \pmod 6$. Let b_3 and s_3 be as in (7.6). Then it can be deduced from Theorems 4.8 and 4.9 that $E(\chi^2) = -a_3 - ib_3\sqrt{3}$. Thus, by (7.10) and Theorem 2.12,

$$\begin{aligned} \mathcal{G}_3 &= 2\,\mathrm{Re}\,\{\bar{\chi}_1(2)G(\chi_1)(-a_3 + ib_3\sqrt{3})\} \\ &= -2a_3\,\mathrm{Re}\,\{\bar{\chi}_1(2)G(\chi_1)\} - 2b_3\sqrt{3}\,\mathrm{Im}\,\{\bar{\chi}_1(2)G(\chi_1)\}. \end{aligned} \tag{7.11}$$

If $\chi_1(2) = 1$, then the use of (7.7) in (7.11) yields

$$\mathcal{G}_3 = -a_3G_3 - b_3\nu(12p - 3G_3^2)^{1/2}.$$

The desired result in the case $\chi_1(2) = 1$ now follows from (7.8).

Suppose next that $\chi_1(2) \neq 1$. Then by (7.7),

$$4\bar{\chi}_1(2)G(\chi_1) = -G_3 + \alpha\nu(12p - 3G_3^2)^{1/2} + i\{-\alpha G_3\sqrt{3} - \nu(4p - G_3^2)^{1/2}\}. \tag{7.12}$$

From (7.11) and (7.12), we have

$$2\mathcal{G}_3 = a_3G_3 - \alpha\nu a_3(12p - 3G_3^2)^{1/2} + 3\alpha b_3G_3 + b_3\nu(12p - 3G_3^2)^{1/2}.$$

The desired result now follows from (7.9). Q.E.D.

THEOREM 7.5. *If $p \equiv 5 \pmod 6$, then $\mathcal{G}_6 = 2p + 3(-1)^{(p+1)/6}p$. If $p = 6k+1$, then, if 2 is a cubic residue* $\pmod p$,

$$\begin{aligned} \mathcal{G}_6 &= -p - 2a_3G_3, && \textit{if } k \textit{ is even}, \\ &= p - 2\{\mathrm{sgn}\,(G_3^2 - p)\}\,|b_3|\,(12p - 3G_3^2)^{1/2}, && \textit{if } k \textit{ is odd}; \end{aligned}$$

if 2 is a cubic nonresidue $\pmod p$,

$$\begin{aligned} \mathcal{G}_6 &= -p + a_3G_3 - \varepsilon_6 a_3(12p - 3G_3^2)^{1/2}, && \textit{if } k \textit{ is even}, \\ &= p - 3\varepsilon_3\,|b_3|\,G_3 - \varepsilon_3\varepsilon_6\,|b_3|\,(12p - 3G_3^2)^{1/2}, && \textit{if } k \textit{ is odd}. \end{aligned}$$

Proof. Let χ have order 6. Then

$$\mathcal{G}_6 = \mathcal{G}_2 + \mathcal{G}_3 + S_6, \tag{7.13}$$

where $S_6 = G_2(\chi) + G_2(\bar{\chi}) = 2\,\mathrm{Re}\, G_2(\chi)$.

First, suppose that $p \equiv 5 \pmod 6$. By Theorem 2.12, $G_2(\chi) = (-1)^{(p+1)/6}p$. The result thus follows from (7.13) and Theorems 7.1 and 7.4.

Secondly, let $p = 6k+1$. Let b_3 and s_3 be as in (7.6). It can be deduced from Theorems 4.8 and 4.9 that $E(\chi) = (-1)^{k+1}(a_3 + ib_3\sqrt{3})$. Thus, by

Theorem 2.12,

$$(7.14)\quad S_6 = 2(-1)^{k+1}\operatorname{Re}\{\bar\chi_1(2)G(\chi_1)(a_3+ib_3\sqrt{3})\}$$
$$= 2(-1)^{k+1}a_3\operatorname{Re}\{\bar\chi_1(2)G(\chi_1)\} + 2(-1)^k b_3\sqrt{3}\operatorname{Im}\{\bar\chi_1(2)G(\chi_1)\}.$$

By (7.11), (7.13), (7.14), and Theorem 7.1, we then get

$$\mathcal{G}_6 = -p - 4a_3\operatorname{Re}\{\bar\chi_1(2)G(\chi_1)\}, \quad \text{if } k \text{ is even},$$
$$= p - 4b_3\sqrt{3}\operatorname{Im}\{\bar\chi_1(2)G(\chi_1)\}, \quad \text{if } k \text{ is odd}.$$

The desired evaluations now follow from (7.7) and (7.8), if $\chi_1(2)=1$, and from (7.9) and (7.12), if $\chi_1(2)\neq 1$. Q.E.D.

THEOREM 7.6. *If $p\equiv 1 \pmod 4$, write $p=a_4^2+b_4^2$ with $a_4\equiv -\left(\frac{2}{p}\right) \pmod 4$. If moreover $p\equiv 1 \pmod{12}$, write $p=a_{12}^2+b_{12}^2$, where a_{12} is as given at the beginning of Section 4.2. If $p\equiv 5 \pmod{12}$, define ε_{12} by $\varepsilon_{12}=\pm 1$ and $\varepsilon_{12}\equiv -a_4|b_4| \pmod 3$. Let $\mathcal{G}_3$ and $\mathcal{G}_6$ be as given in Theorems 7.4 and 7.5, respectively. Then*

$$\mathcal{G}_{12} = \mathcal{G}_6 - 2\left(\frac{2}{p}\right)a_4\sqrt{p} - 2\left(\frac{2}{p}\right)a_{12}(G_3^2-2p)/\sqrt{p}, \quad \text{if } p=12k+1,$$
$$= -p - 2\left(\frac{2}{p}\right)a_4\sqrt{p} + 4\left(\frac{2}{p}\right)\varepsilon_{12}|b_4|\sqrt{p}, \quad \text{if } p=12k+5,$$
$$= \mathcal{G}_6 + 2(-1)^{k+1}\mathcal{G}_3 + 2(-1)^k p, \quad \text{if } p=12k+7,$$
$$= 5p + 6(-1)^{k+1}p, \quad \text{if } p=12k+11.$$

Proof. Let χ have order 12. Then $\chi(-1)=1$ and

$$\mathcal{G}_{12} = \mathcal{G}_6 + \mathcal{G}_4 - \mathcal{G}_2 + S_{12}, \quad \text{where} \quad S_{12} = 2\operatorname{Re} G_2(\chi) + 2\operatorname{Re} G_2(\chi^5).$$

We have already evaluated $\mathcal{G}_2$, $\mathcal{G}_4$, and $\mathcal{G}_6$, and so it remains to evaluate S_{12}.

First, suppose that $p=12k+1$. Then χ_1 has order 6. Since $i^5=i$, we deduce from Theorem 4.8 that $E(\chi^5)=E(\chi)=-a_{12}\pm ib_{12}$. Thus, by Theorem 2.12,

$$G_2(\chi) = \bar\chi_1(2)G(\chi_1)E(\chi) \quad \text{and} \quad G_2(\chi^5) = \chi_1(2)G(\bar\chi_1)E(\chi).$$

Hence, as desired,

$$S_{12} = -4a_{12}\operatorname{Re}\{\bar\chi_1(2)G(\chi_1)\} = -2\left(\frac{2}{p}\right)a_{12}(G_3^2-2p)/\sqrt{p},$$

where we have used the value of $G(\chi_1)$ from [1, Theorem 3.7(ii)].

Secondly, let $p=12k+5$. Then χ_1 has order 2. By Theorem 2.10, $E(\chi)=E(\chi^5)$. Hence, by Theorem 2.12,

$$G_2(\chi)=\left(\frac{2}{p}\right)\sqrt{p}E(\chi)=G_2(\chi^5).$$

Thus, by Theorem 4.10, we obtain the desired result

$$S_{12}=4\left(\frac{2}{p}\right)\sqrt{p}\operatorname{Re}E(\chi)=4\left(\frac{2}{p}\right)\varepsilon_{12}\,|b_4|\,\sqrt{p}.$$

Thirdly, let $p=12k+7$. Then χ_1 has order 3. Write $K(\chi_1)=a_3+ib_3\sqrt{3}$ as in (7.6). Then by Theorem 4.9,

$$E(\chi)=(-1)^{k+1}(-a_3+ib_3\sqrt{3}). \tag{7.15}$$

Now, by Theorem 2.10, $E(\chi^5)=E(\bar{\chi}^7)=E(\bar{\chi})$. Thus, by Theorem 2.12,

$$G_2(\chi)=\bar{\chi}_1(2)G(\chi_1)E(\chi) \quad \text{and} \quad G_2(\chi^5)=\chi_1(2)G(\bar{\chi}_1)E(\bar{\chi}).$$

Therefore, using (7.11) and (7.15), we obtain the desired result

$$S_{12}=4\operatorname{Re}\{\bar{\chi}_1(2)G(\chi_1)E(\chi)\}=2(-1)^{k+1}\mathscr{G}_3.$$

Finally, let $p=12k+11$. Then by Theorem 2.12, $G_2(\chi^j)=(-1)^{k+1}p$ for $j=1$, 5. Thus, $S_{12}=4(-1)^{k+1}p$, as desired. Q.E.D.

8. The Hasse–Davenport relation

In this chapter, p is *any* prime, $q=p^r$, ψ is a character on $GF(q)$ of order $l>1$, and χ is an arbitrary character on $GF(q)$ such that χ^l is nontrivial. As usual, ϕ is the quadratic character on $GF(q)$. Define

$$\eta_l(\chi)=\frac{\chi^l(l)G_r(\chi)}{G_r(\chi^l)}\prod_{j=1}^{l-1}\frac{G_r(\chi\psi^j)}{G_r(\psi^j)}. \tag{8.1}$$

By using Theorem 2.1, we may write $\eta_l(\chi)$ in the alternative form

$$\eta_l(\chi)=\chi^l(l)\prod_{j=1}^{l-1}\frac{J_r(\chi,\chi^j)}{J_r(\chi,\psi^j)}.$$

A remarkable theorem of Hasse and Davenport [4], [9, p. 464] asserts that $\eta_l(\chi)=1$ for each possible choice of χ. (We shall abbreviate this statement by "$\eta_l=1$".) This theorem is proved by the use of Stickelberger's prime ideal factorization of Gauss sums. An elementary proof that $\eta_l=1$ is much desired.

The proof of Theorem 8.1 below gives an elementary proof that $\eta_l=1$ under the assumption that $\eta_t=1$ for all primes t dividing l. Since an elementary proof that $\eta_2 = 1$ is well known (see the proofs for $r = 1$ in [1, Theorem 2.3], [9, p. 465] and the remarks immediately preceding Theorem 2.3 in this paper), we thus obtain an elementary proof that $\eta_l = 1$ whenever l is a power of 2. Moreover, the problem of providing an elementary proof that $\eta_l = 1$ is reduced to the (apparently unsolved) problem of providing an elementary proof that $\eta_t = 1$ for each prime t.

THEOREM 8.1. *Assume that $\eta_t = 1$ for each prime t dividing l. Then it follows elementarily that $\eta_l = 1$.*

Proof. Since all Gauss sums in the proof are over $GF(q)$, we suppress the subscript r.

If l is prime, there is nothing to prove; thus, assume that l is composite. As the induction hypothesis, assume that $\eta_u = 1$ for each integer u, $1 < u < l$. Define t to be the smallest prime divisor of l. We have

$$\prod_{k=0}^{l-1} G(\chi\psi^k) = \prod_{j=0}^{l/t-1} \prod_{i=0}^{t-1} G(\chi\psi^j\psi^{li/t}).$$

Since $\eta_t(\chi\psi^j) = 1$ by the induction hypothesis, it follows from (8.1) that

$$\begin{aligned}\prod_{k=0}^{l-1} G(\chi\psi^k) &= \prod_{j=0}^{l/t-1} \left\{\bar{\chi}^t(t)\bar{\psi}^{jt}(t)G(\chi^t\psi^{jt}) \prod_{i=1}^{t-1} G(\psi^{li/t})\right\} \\ &= \bar{\chi}^l(t)\bar{\psi}^{l(l/t-1)/2}(t)\left\{\prod_{i=1}^{t-1} G(\psi^{li/t})\right\}^{l/t} \prod_{j=0}^{l/t-1} G(\chi^t\psi^{jt}).\end{aligned}$$

Since $\eta_{l/t}(\chi^t) = 1$ by the induction hypothesis,

$$\prod_{j=0}^{l/t-1} G(\chi^t\psi^{jt}) = \bar{\chi}^l(l/t)G(\chi^l) \prod_{j=1}^{l/t-1} G(\psi^{tj}).$$

Thus,

$$\prod_{k=0}^{l-1} G(\chi\psi^k) = \bar{\chi}^l(l)G(\chi^l)\bar{\psi}^{l(l/t-1)/2}(t)\left\{\prod_{i=1}^{t-1} G(\psi^{li/t})\right\}^{l/t} \prod_{j=1}^{l/t-1} G(\psi^{tj}).$$

By (8.1), it remains to show that

$$\prod_{n=1}^{l-1} G(\psi^n) = \bar{\psi}^{l(l/t-1)/2}(t)\left\{\prod_{i=1}^{t-1} G(\psi^{li/t})\right\}^{l/t} \prod_{j=1}^{l/t-1} G(\psi^{tj}), \tag{8.2}$$

By (2.1), when $p > 2$, $G(\phi) = i_0 q^{1/2}$, where $i_0^2 = \phi(-1)$. For any character λ on $GF(q)$ of order m, it follows that

$$q^{(1-m)/2} \prod^{m-1} G(\lambda^n) = \begin{cases} 1, & \text{if } m \text{ is odd,} \\ i_0\lambda^{m(m-2)/8}(-1), & \text{if } m \text{ is even.} \end{cases} \tag{8.3}$$

It follows that both sides of (8.2) equal $q^{(l-1)/2}$ when l is odd. Thus, let l be even, and so $t=2$ and $p>2$. By (8.2) and (8.3), it remains to show that

$$(8.4) \qquad i_0\psi^{l(l-2)/8}(-1) = \phi^{l/2-1}(2)i_0^{l/2}, \quad \text{if } l/2 \text{ is odd,}$$
$$= \phi^{l/2-1}(2)i_0^{l/2+1}, \quad \text{if } l/2 \text{ is even.}$$

First, suppose that $l/2$ is odd. Then (8.4) holds because $i_0^2 = \phi(-1) = \psi^{l/2}(-1)$.

Secondly, suppose that $l/2$ is even. Then $i_0^2 = \phi(-1) = \psi^{l/2}(-1) = 1$. It thus remains to show that $\phi(2) = \psi^{l/4}(-1)$. Hence, we must show that

$$(8.5) \qquad \phi(2) = 1, \quad \text{if } 8 \mid (q-1),$$
$$= -1, \quad \text{otherwise.}$$

By an extension of the argument in the proof of Lemma 2.9 ϕ_1 has order $2/(2,(q-1)/(p-1))$. Hence,

$$(8.6) \qquad \phi(2) = 1, \quad \text{if } 2 \mid (q-1)/(p-1), \text{ i.e., } 2 \mid r,$$
$$= \left(\frac{2}{p}\right), \quad \text{otherwise.}$$

If $2 \mid r$, then q is an odd square, and so $8 \mid (q-1)$. Thus, (8.5) follows from (8.6) in the case $2 \mid r$. Assume now that $2 \nmid r$. Since $2 \nmid (q-1)/(p-1)$, $q-1$ and $p-1$ have the same number of factors of 2. Since $l/2$ is even and $l \mid (q-1)$, it follows that 4 divides both $q-1$ and $p-1$. Thus, 8 divides $q-1$ and $p-1$ if and only if $\left(\frac{2}{p}\right)=1$. Thus, (8.5) follows from (8.6). Q.E.D.

The authors are very grateful to Joseph Muskat for many helpful suggestions.

References

1. Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory. (to appear).
2. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc., vol. 99 (1961), pp. 241–245.
3. ———, *On primes of the form u^2+5v^2*, Proc. Amer. Math. Soc., vol. 17 (1966), pp. 502–509.
4. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math., vol. 172 (1934), pp. 151–182.
5. L. E. Dickson, *Cyclotomy, higher congruences, and Warings's problem*, Amer. J. Math., vol. 57 (1935), pp. 391–424.
6. Ronald J. Evans, *Resolution of sign ambiguities in Jacobi and Jacobsthal sums*, Pacific J. Math. (to appear).
7. Reinaldo E. Giudici, Joseph B. Muskat, and Stanley F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc., vol. 171 (1972), pp. 317–347.
8. Emil Grosswald, *The theory of numbers*, Macmillan, New York, 1966.
9. Helmut Hasse, *Vorlesungen über Zahlentheorie*, zweite Auflage, Springer-Verlag, Berlin, 1964.
10. Kenneth Ireland and Michael I. Rosen, *Elements of number theory*, Bogden and Quigley, Tarrytown-on-Hudson, 1972.

11. SERGE LANG, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
12. EMMA LEHMER, *On the quintic character of* 2, Bull. Amer. Math. Soc., vol. 55 (1949), p. 62.
13. ———, *On the quadratic character of the Fibonacci root*, Fibonacci Quart., vol. 4 (1966), pp. 135–138.
14. ———, *On some special quartic reciprocity laws*, Acta Arith., vol. 21 (1972), pp. 367–377.
15. PHILIP A. LEONARD and KENNETH S. WILLIAMS, *Jacobi sums and a theorem of Brewer*, Rocky Mountain J. Math., vol. 5 (1975), pp. 301–308; erratum, Rocky Mountain J. Math., vol. 6 (1976), p. 509.
16. JOSEPH B. MUSKAT and ALBERT L. WHITEMAN, *The cyclotomic numbers of order twenty*, Acta Arith., vol. 17 (1970), pp. 185–216.
17. JOSEPH B. MUSKAT and YUN-CHENG ZEE, *On the uniqueness of solutions of certain Diophantine equations*, Proc. Amer. Math. Soc., vol. 49 (1975), pp. 13–19.
18. GERRY MYERSON, *Period polynomials and Gauss sums for finite fields* (to appear).
19. A. R. RAJWADE, *On rational primes p congruent to* 1 (mod 3 *or* 5), Proc. Cambridge Philos. Soc., vol. 66 (1969), pp. 61–70.
20. ———, *On the congruence* $y^2 \equiv x^5 - a \pmod p$, Proc. Cambridge Philos. Soc., vol. 74 (1973), pp. 473–475.
21. ———, *Certain classical congruences via elliptic curves*, J. London Math. Soc. (2), vol. 8 (1974), pp. 60–62.
22. ———, *Notes on the congruence* $y^2 \equiv x^5 - a \pmod p$, Enseign. Math., vol. 21 (1975), pp. 49–56.
23. S. F. ROBINSON, *Theorems on Brewer sums*, Pacific J. Math., vol. 25 (1968), pp. 587–596.
24. L. STICKELBERGER, *Ueber eine Verallgemeinerung der Kreistheilung*, Math. Ann., vol. 37 (1890), pp. 321–367.
25. THOMAS STORER, *Cyclotomy and difference sets*, Markham, Chicago, 1967.
26. ALBERT LEON WHITEMAN, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J., vol. 16 (1949), pp. 619–626.
27. ———, *Cyclotomy and Jacobsthal sums*, Amer. J. Math., vol. 74 (1952), pp. 89–99.
28. ———, *A theorem of Brewer on character sums*, Duke Math. J., vol. 30 (1963), pp. 545–552.
29. ———, *Theorems on Brewer and Jacobsthal sums. I*, Proc. Symp. Pure Math., vol. 8, Amer. Math. Soc., Providence, 1965, pp. 44–55.
30. ———, *Theorems on Brewer and Jacobsthal sums. II*. Michigan Math. J., vol. 12 (1965), pp. 65–80.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS

UNIVERSITY OF CALIFORNIA AT SAN DIEGO
LA JOLLA, CALIFORNIA