Sums of Gauss, Jacobi, and Jacobsthal*

BRUCE C. BERNDT

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

AND

RONALD J. EVANS

Department of Mathematics, University of California at San Diego, La Jolla, California 92093

Received February 2, 1979

DEDICATED TO PROFESSOR S. CHOWLA ON THE OCCASION OF HIS 70TH BIRTHDAY

1. INTRODUCTION

One of the primary motivations for this work is the desire to evaluate, for certain natural numbers \( k \), the Gauss sum

\[
G_k = \sum_{n=0}^{p-1} e^{2\pi i n^k/p},
\]

where \( p \) is a prime with \( p \equiv 1 \pmod{k} \). The evaluation of \( G_2 \) was first achieved by Gauss. The sums \( G_k \) for \( k = 3, 4, 5, \) and \( 6 \) have also been studied. It is known that \( G_3 \) is a root of a certain irreducible cubic polynomial. Except for a sign ambiguity, the value of \( G_4 \) is known. See Hasse's text [24, pp. 478-494] for a detailed treatment of \( G_3 \) and \( G_4 \), and a brief account of \( G_6 \). For an account of \( G_5 \), see a paper of E. Lehmer [29].

In Section 3, we shall determine \( G_8 \) (up to two sign ambiguities). Using our formula for \( G_8 \), the second author [18] has recently evaluated \( G_{16} \) (up to four sign ambiguities). We shall also evaluate \( G_8, G_{12}, \) and \( G_{24} \) in terms of \( G_8 \). For completeness, we include in Sections 3.1 and 3.2 short proofs of known results on \( G_3 \) and \( G_4 \); these results will be used frequently in the sequel. (We do not discuss \( G_5 \) since elaborate computations are involved, and \( G_5 \) is not needed in the sequel.)

While evaluations of \( G_k \) are of interest in number theory, they also have

* This paper was originally accepted for publication in the Rocky Mountain Journal of Mathematics. We are very grateful to the editors T. G. McLaughlin and W. R. Scott for permitting this paper to be released so that it can be published in this special issue dedicated to S. Chowla.

349
applications to combinatorial problems. In Section 5, we present some new theorems which enable us to apply our formulae for $G_k$ to give new proofs of important results of Chowla, Lehmer, and Whiteman on 4th, 6th, 8th, and 12th power residue difference sets. These proofs are considerably shorter than the original proofs by cyclotomy. Using theorems of Section 5 and the formula for $G_{18}$, the second author [18] has proved the nonexistence of 16th power residue difference sets and modified difference sets. This completes the work of Whiteman [59], who obtained partial results in 1957. Using our formula for $G_{24}$ together with a recently computed table of formulas for the cyclotomic numbers of order 24, the second author [21] has proved the nonexistence of 24th power residue difference sets and modified difference sets when either 2 is a cubic residue or 3 is a quartic residue (mod $p$). The remaining case can undoubtedly be settled using the formula for $G_{24}$, but very laborious calculations would appear to be involved. For good expositions on power residue difference sets, consult the books of Storer [53] and Baumert [2, p. 124]. A different approach to the study of difference sets by the use of Jacobi sums has been given by Yamamoto [64].

Our evaluations of Gauss sums are based on the determination of Jacobi sums

$$J(\chi, \psi) = \sum_{n=0}^{p-1} \chi(n) \psi(1 - n),$$

where $\chi$ and $\psi$ are characters (mod $p$). Most of the evaluations of Jacobi sums given here are known; see, in particular, a paper of Muskat [45]. However, in general, our proofs are shorter and more elementary than previous proofs; see, for example, Theorems 3.12 and 3.34. In evaluating one of Brewer's character sums, Leonard and Williams [38] use properties of Jacobi sums and remark that they view the approach via Jacobi sums as more natural than that using the theory of cyclotomy. It is this viewpoint that we have adopted in this paper. We do not employ cyclotomic numbers or any other of the traditional methods and results from the theory of cyclotomy. This is in contrast to the pioneering work of Dickson [15], [16], [17] and the important related later work of E. Lehmer [30], [31], [34], [35], Whiteman [59], [60], [61], Muskat [44], [45], and Muskat and Whiteman [47].

Our determinations of Jacobi sums lead naturally to some well-known criteria for residuacity. These criteria occur as corollaries at various points in Section 3. It is not our intention to systematically develop such results nor to provide the simplest possible proofs.

In 1907, Jacobsthal [26] evaluated the "Jacobsthal sum"

$$\varphi_n(a) = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \left(\frac{m^n + a}{p}\right)$$
for $n = 2$; here $(j/p)$ denotes the Legendre symbol, and $p \nmid a$. Since 1907, $\varphi_n(a)$ has been evaluated for certain other values of $n$ by several authors using a variety of methods. In Chapter 4, we present a unified, systematic treatment of Jacobsthal sums based upon our determinations of Jacobi sums. We include evaluations of some well-known results as well as several evaluations which appear to be new.

All of our evaluations are effected in terms of parameters that appear in the representations of the primes $p$ as binary quadratic forms. Some other evaluations of Gauss, Jacobi, and Jacobsthal sums over $GF(p)$ involving binary and quartic quadratic forms are given in a sequel [5] to this paper. There the authors also develop the theory of Jacobi and Eisenstein sums over $GF(p^2)$ and utilize this theory to give new formulae for Gauss and Jacobsthal sums over $GF(p^2)$.

Our objective in this paper is to be as completely self-contained and elementary as possible. The only nonelementary results used are Lemmas 3.21 and 3.33, which employ Stickelberger's theorem on the factorization of Gauss sums into prime ideals. These lemmas are needed to analyze bidecic and biduodecic Jacobi sums.

The authors are very grateful to J. Muskat, K. S. Williams, and E. Lehmer for several helpful comments.

2. Notation and Preliminary Results

Throughout this paper, $p$ denotes an odd prime and $\chi$ and $\psi$ denote nontrivial characters (mod $p$). We let $\varphi$ denote the quadratic character given by the Legendre symbol. The symbol $\sum_n$ means that the summation is extended over a complete residue system (mod $p$), while $\sum_{n \equiv a}$ indicates that the summation is over a complete residue system (mod $p$) with the term corresponding to $n \equiv a$ (mod $p$) omitted. The ring of all algebraic integers is denoted by $\Omega$.

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

$$G(\chi) = \sum_n \chi(n) e^{2\pi in/p}$$

and satisfies the fundamental property [25, pp. 91–92]

$$G(\chi) G(\bar{\chi}) = \chi(-1) p.$$

Define $i^*$ by

$$i^* = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ i, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$
Then [27, Theorem 212, p. 200]

$$G(\varphi) = i^k p^{1/2}.$$

If \( \chi \) is a character \((\text{mod} \: p)\) of order 24, for \( 1 \leq j \leq 11 \), we define

$$R_j = G(\chi^j) + G(\bar{\chi}^j).$$

These expressions will arise in our evaluation of \( G_k \). It is easily seen that \( R_1 + R_5 + R_7 + R_{11}, R_3 + R_9, R_2 + R_{10}, R_4, R_8, \) and \( R_6 \) are independent of the choice of \( \chi \).

The following are easily proved, basic properties of Jacobi sums [25, p. 93).

**Theorem 2.1.** If \( \chi \) is a nontrivial character \((\text{mod} \: p)\), then

$$J(\chi, \bar{\chi}) = -\chi(-1).$$

**Theorem 2.2.** If \( \chi, \psi, \) and \( \chi \psi \) are nontrivial characters \((\text{mod} \: p)\), then

$$J(\chi, \psi) = \frac{G(\chi) G(\psi)}{G(\chi \psi)}.$$

In particular, \( |J(\chi, \psi)| = p^{1/2}. \)

The properties of Gauss and Jacobi sums given above will be used repeatedly throughout the paper, usually without comment.

We set \( J(\chi, \chi) = J(\chi) \). It will be convenient to define a new character sum \( K(\chi) \) by

$$K(\chi) = \chi(4) J(\chi).$$

**Theorem 2.3.** If \( \psi \) is any nontrivial character \((\text{mod} \: p)\) and \( \varphi \) is the quadratic character \((\text{mod} \: p)\), then

$$K(\psi) = J(\psi, \varphi).$$

**Proof.** If \( m \) is an integer, the number of solutions \( n \) to \( n(1-n) = m \) \((\text{mod} \: p)\) is \( 1 + \varphi(1 - 4m) \). Thus,

$$J(\psi) = \sum_{n \neq 0, 1} \psi(n(1-n)) = \sum_m \psi(m) \{ 1 + \varphi(1 - 4m) \} = \sum_m \psi(m) \varphi(1 - 4m) = \bar{\varphi}(4) \sum_m \psi(m) \varphi(1 - m) = \bar{\varphi}(4) J(\psi, \varphi).$$

Theorem 2.3 is actually a special case of a deep theorem of Davenport and
Hasse [14, pp. 153–154]. (See also Hasse’s text [24, p. 464].) We shall discuss this theorem further in [5].

**THEOREM 2.4.** Let \( \psi \) be a character \((\text{mod } p)\) of order exceeding 2, and let \( \varphi \) be the quadratic character \((\text{mod } p)\). Then

\[
(i) \quad K(\psi) = \left(\frac{-1}{p}\right) K(\bar{\psi} \varphi)
\]

and

\[
(ii) \quad K(\psi) = \psi(-1) J(\psi, \bar{\psi} \varphi).
\]

**Proof.** By Theorem 2.3, \( K(\psi) = J(\psi, \varphi) \) and \( K(\bar{\psi} \varphi) = J(\bar{\psi} \varphi, \varphi) \). Also using Theorem 2.2, we have, as \( \bar{\psi} \varphi \) is nontrivial,

\[
\frac{K(\bar{\psi} \varphi)}{K(\psi)} = \frac{G(\bar{\psi} \varphi) G(\varphi)}{G(\bar{\psi}) G(\psi) G(\varphi)} = \varphi(-1) = \left(\frac{-1}{p}\right),
\]

which proves (i).

To prove (ii), observe that by (i) and Theorem 2.3,

\[
\frac{J(\psi, \bar{\psi} \varphi)}{K(\psi)} = \frac{J(\psi, \bar{\psi} \varphi)}{\varphi(-1) K(\bar{\psi} \varphi)} = \frac{J(\psi, \bar{\psi} \varphi)}{\varphi(-1) J(\bar{\psi} \varphi, \varphi)}
\]

\[
= \frac{G(\psi) G(\bar{\psi} \varphi)}{G(\varphi) \varphi(-1) G(\bar{\psi}) G(\bar{\psi} \varphi) G(\varphi)} = \psi(-1).
\]

The following theorem is an immediate consequence of Theorem 2.4 and will be used frequently in the sequel.

**THEOREM 2.5.** Let \( \psi \) be a character \((\text{mod } p)\) of order 2k. Then

\[
(i) \quad K(\psi) = \left(\frac{-1}{p}\right) K(\psi^{k-1})
\]

and

\[
(ii) \quad K(\psi) = \psi(-1) J(\psi, \psi^{k-1}).
\]

In Section 3, we prove several theorems (e.g., Theorem 3.3) showing that for certain \( m \), \( K(\chi) = a + ibd^{1/2} \) whenever \( \chi \) has order \( m \), where \( a \) and \( b \) are integers and \( d \) is a natural number. Thus, by Theorem 2.2, \(| K(\chi) |^2 = p = a^2 + db^2 \). (We remark that if \( p = a^2 + db^2 \), where \( a \) and \( b \) are integers and \( d \) is a fixed positive integer, then \( a \) and \( b \) are uniquely determined up to sign [48, Theorem 101, p. 188].) It should be noted that \( b \) is not independent of the choice of \( \chi \); in fact, \( b = b(\chi) = -b(\bar{\chi}) \). On the other hand, \( a \) will
frequently be independent of the choice of $\chi$. In certain cases, E. Lehmer [35] and the second author [19], [20] have resolved the sign ambiguity in $b(\chi)$.

If $\zeta = \exp(2\pi i/m)$ and $(t, m) = 1$, we define $\sigma_t \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where $\mathbb{Q}$ denotes the field of rational numbers, by $\sigma_t(\zeta) = \zeta^t$. Note that if $\chi$ is a character (mod $p$) whose order divides $m$, then $\sigma_t(J(\chi)) = J(\chi^t)$.

If $p \nmid a$, we define the Jacobsthal sum $\varphi_n(a)$ by

$$\varphi_n(a) = \sum_{m} \left( \frac{m}{p} \right) \left( \frac{m^n + a}{p} \right)$$

and the related sum $\psi_n(a)$ by

$$\psi_n(a) = \sum_{m} \left( \frac{m^n + a}{p} \right),$$

where $n$ is a positive integer. These two sums are connected by the following basic result.

**Theorem 2.6.** For any natural number $n$, we have

$$\psi_{2n}(a) = \psi_n(a) + \varphi_n(a).$$

**Proof.** The result is immediate since

$$\psi_{2n}(a) = \sum_{m} \left( \frac{m^{2n} + a}{p} \right) = \sum_{m} \left( \frac{m^n + a}{p} \right) \left( 1 + \left( \frac{m}{p} \right) \right).$$

Jacobsthal sums are connected with the sums $K(\chi)$ by the following important theorem.

**Theorem 2.7.** Let $\chi$ be a character (mod $p$) of order $2n$. Then

$$\varphi_n(a) = \chi(-1) \sum_{j=0}^{n-1} \chi^{n+2j+1}(a) \chi^{2j+1}(a).$$

**Proof.** Subsequently replacing $m$ by $-ma$ below, we have

$$\varphi_n(a) = \sum_{m} \left( \frac{m}{p} \right) \left( \frac{m^n + a}{p} \right) = \sum_{m} \chi^{n}(m) \chi^{n}(m^n + a)$$

$$= \sum_{m} \chi(m) \chi^{n}(m^n + a)$$

$$= \sum_{m} \chi(m) \chi^{n}(m \mid a) \sum_{j=0}^{n-1} \chi^{2j}(m)$$
Sums of Gauss

\[ = \chi(-1) \chi^{n+1}(a) \sum_{m} \chi(m) \chi^{n}(1 - m) \sum_{j=0}^{n-1} \chi^{2j}(am) \]

\[ = \chi(-1) \chi^{n+1}(a) \sum_{j=0}^{n-1} \chi^{2j}(a) J(\chi^{2j+1}, \chi^{n}) \]

\[ = \chi(-1) \sum_{j=0}^{n-1} \chi^{n+2j+1}(a) K(\chi^{2j+1}), \]

by Theorem 2.3. 

As an immediate consequence of Theorem 2.7 and Theorem 2.2, we get

\[ |\varphi_{n}(a)| \leq n p^{1/2}, \]

which is a special case of Weil's character sum estimates [54].

The proof of the next theorem follows along the same lines as the previous proof.

**Theorem 2.8.** Let \( \chi \) be a character \((\bmod p)\) of order \(2n\). Then

\[ \psi_{n}(a) = \left(\frac{a}{p}\right) \sum_{j=1}^{n-1} \chi^{2j}(a) K(\chi^{2j}). \]

The Weil estimate

\[ |\psi_{n}(a)| \leq (n - 1) p^{1/2} \]

is an easy consequence of Theorem 2.8.

Much notation will be defined in what follows. For the convenience of the reader, a table of notation, with the page number where the notation is defined, is given below.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_3, b_3 )</td>
<td>356</td>
</tr>
<tr>
<td>( a_4, b_4 )</td>
<td>361</td>
</tr>
<tr>
<td>( a_8, b_8 )</td>
<td>363</td>
</tr>
<tr>
<td>( a_{12}, b_{12} )</td>
<td>367</td>
</tr>
<tr>
<td>( a_{20}, b_{20} )</td>
<td>380, 381</td>
</tr>
<tr>
<td>( a_{24}, b_{24} )</td>
<td>371</td>
</tr>
<tr>
<td>( \chi )</td>
<td>357</td>
</tr>
<tr>
<td>( \beta )</td>
<td>374</td>
</tr>
<tr>
<td>( c_4, d_4 )</td>
<td>361</td>
</tr>
<tr>
<td>( c_8, d_8 )</td>
<td>363</td>
</tr>
<tr>
<td>( \delta )</td>
<td>375</td>
</tr>
<tr>
<td>( \epsilon_3 )</td>
<td>358</td>
</tr>
<tr>
<td>( \epsilon_6 )</td>
<td>360</td>
</tr>
<tr>
<td>( \epsilon_{24} )</td>
<td>376</td>
</tr>
<tr>
<td>( G_k )</td>
<td>349</td>
</tr>
<tr>
<td>( G(\chi) )</td>
<td>351</td>
</tr>
<tr>
<td>( i^* )</td>
<td>351</td>
</tr>
<tr>
<td>( J(\chi, \psi) )</td>
<td>350</td>
</tr>
<tr>
<td>( J(\chi) )</td>
<td>352</td>
</tr>
<tr>
<td>( K(\chi) )</td>
<td>352</td>
</tr>
<tr>
<td>( \eta )</td>
<td>363, 372</td>
</tr>
<tr>
<td>( \nu )</td>
<td>360</td>
</tr>
<tr>
<td>( \varphi )</td>
<td>351</td>
</tr>
<tr>
<td>( \sigma )</td>
<td>354</td>
</tr>
<tr>
<td>( \tau )</td>
<td>372</td>
</tr>
<tr>
<td>( \omega )</td>
<td>356</td>
</tr>
<tr>
<td>( \varphi_{n}(a) )</td>
<td>350, 354</td>
</tr>
<tr>
<td>( \Omega )</td>
<td>351</td>
</tr>
</tbody>
</table>
3. Evaluation of Gauss and Jacobi Sums

3.1. Cubic and sextic Gauss and Jacobi sums. Throughout this section, \( p \equiv 1 \pmod{6} \), and \( \chi \) is a character \((\text{mod} \ p)\) of order 6. Observe that \( \chi(-1) = \chi^6(-1) = (-1/p) \).

**Theorem 3.1.** We have

(i) \( G^3(\chi^2) = pJ(\chi^2) \)

and

(ii) \( G(\chi) = \chi(4) p^{-1/2} i^* G^3(\chi^2) \).

**Proof.** Since, by Theorem 2.2,

\[
J(\chi^2) = \frac{G^2(\chi^2)}{G(\chi^2)} - \frac{G^3(\chi^2)}{p},
\]

(i) holds.

Now, by Theorem 2.3, \( J(\chi^2) = \chi(4) J(\chi^2, \chi^3) \). Thus, by (i),

\[
\frac{G^3(\chi^2)}{p} = \frac{\chi(4) G(\chi^2)}{G(\chi^2)} = \frac{\chi(4) G(\chi)}{G(\chi^3)} = \frac{\chi(4) G(\chi)}{i^* \sqrt{p}},
\]

and (ii) follows. \( \blacksquare \)

**Theorem 3.2.** We have

\( J(\chi^6) \equiv -1 \pmod{3\Omega} \).

**Proof.** First, observe that

\[
G(\chi^2) = \sum_{n \neq 0} \chi^2(n) e^{2\pi i n/p} \equiv \sum_{n \neq 0} e^{2\pi i n/p} = -1 (\text{mod} (1 - \omega) \ \Omega),
\]

where \( \omega = \exp(2\pi i/3) \). Since \( 1 - \omega = i \sqrt{3} \bar{\omega} \), we have \( G(\chi^2) \equiv -1 \pmod{\sqrt{3} \ \Omega} \). Hence, \( G^3(\chi^2) \equiv -1 \pmod{3\Omega} \). The result now follows from Theorem 3.1(i). \( \blacksquare \)

**Theorem 3.3.** We have

\[
K(\chi^2) = a_3 + ib_3 \sqrt{3} = \left( \frac{-1}{p} \right) K(\chi),
\]

where \( a_3 \) and \( b_3 \) are rational integers such that \( a_3^2 + 3b_3^2 = p \) and \( a_3 \equiv -1 \pmod{3} \).
Proof. First,

\[ K(\chi^2) = \chi^2(4) J(\chi^2) = \chi^2(4) \sum_{n} \chi^2(n(1 - n)) \]

\[ = 1 + \sum_{n \neq (p+1)/2} \chi^2(4n(1 - n)) = 1 + 2 \sum_{n=2}^{(p-1)/2} \chi^2(4n(1 - n)). \]

Since each term in the last sum is 1 or \((-1 + i \sqrt{3})/2\), it follows that \(K(\chi^2) = a_3 + ib_3 \sqrt{3}\), where \(a_3\) and \(b_3\) are rational integers. Since \( |K(\chi^2)|^2 = p\), we have \(p = a_3^2 + 3b_3^2\). The equality \(K(\chi^2) = (-1/p) K(\chi)\) is a consequence of Theorem 2.5(i).

Lastly,

\[ p - 2 = K(\chi^6) = K(\chi^2)^3 = a_3^3 \equiv a_3 \pmod{3\Omega}, \]

from which the congruence \(a_3 \equiv -1 \pmod{3}\) is immediate.

When \(2\) is a cubic nonresidue \((\pmod{p})\), define \(\alpha\) by \(\chi(4) = \omega^\alpha\) and \(\alpha = \pm 1\).

**Theorem 3.4.** We have

\[ 2J(\chi^2) = r_3 + is_3 \sqrt{3}, \]

where \(r_3\) and \(s_3\) are rational integers such that \(r_3^2 + 3s_3^2 = 4p\), \(r_3 \equiv 1 \pmod{3}\), and \(s_3 \equiv 0 \pmod{3}\).

**Proof.** By Theorem 3.3,

\[ 2J(\chi^2) = 2\chi(4) K(\chi^2) = 2\chi(4)(a_3 + ib_3 \sqrt{3}). \]

Hence, \(2J(\chi^2) = r_3 + is_3 \sqrt{3}\), where

\[ r_3 = 2a_3, s_3 = 2b_3, \text{ if } 2 \text{ is a cubic residue (mod } p), \]

and

\[ r_3 = -a_3 - 3\alpha b_3, s_3 = \alpha a_3 - b_3, \text{ if } 2 \text{ is a cubic nonresidue (mod } p). \]

By Theorem 3.2,

\[ 2J(\chi^2) - 1 = (r_3 - 1) + is_3 \sqrt{3} = 0 \pmod{3\Omega}; \]

hence, \(r_3 \equiv 1 \pmod{3}\) and \(s_3 \equiv 0 \pmod{3}\).

By (3.1) and (3.2), \(r_3\) and \(s_3\) are both even when \(2\) is a cubic residue \((\pmod{p})\) and both odd otherwise, since \(a_3\) and \(b_3\) are of opposite parity.
By Theorems 3.3 and 3.4, $a_3 \equiv -1 \pmod{3}$ and $s_3 = 0 \pmod{3}$. Thus, by (3.1) and (3.2),

$$b_3 \equiv \begin{cases} 0 \pmod{3}, & \text{if } 2 \text{ is a cubic residue,} \\ \alpha \pmod{3}, & \text{otherwise.} \end{cases} \quad (3.3)$$

Thus, by the uniqueness of the representation of $p$ as a sum $x^2 + 3y^2$, we see that $2$ is a cubic residue (mod $p$) if and only if $p$ has the representation $p = x^2 + 27y^2$, where $x$ and $y$ are integers. This result, due to Gauss, is a special case of the cubic reciprocity law [25, p. 120].

Suppose that $2$ is a cubic nonresidue (mod $p$). Define $e_3$ by $e_3 = \pm 1$, where $e_3 \equiv \left\lfloor b_3 \right\rfloor \pmod{3}$. By (3.3), $-\alpha \text{ sgn } b_3 \equiv \left\lfloor b_3 \right\rfloor \pmod{3}$, and so $e_3 = -\alpha \text{ sgn } b_3$. By (3.2), $r_3 = -a_3 + 3e_3 \left\lfloor b_3 \right\rfloor$, and this is a formula for $r_3$ in terms of variables independent of $\chi$. Also, by (3.2), $s_3 = \alpha(a_3 + e_3 \left\lfloor b_3 \right\rfloor)$.

**Theorem 3.5.** We have

$$2J(\chi) = u_3 + iv_3 \sqrt{3},$$

where $u_3$ and $v_3$ are rational integers such that $u_3^2 + 3v_3^2 = 4p$, $u_3 \equiv (-1/p) \pmod{3}$, and

$$v_3 \equiv \begin{cases} 0 \pmod{3}, & \text{if } 2 \text{ is a cubic residue (mod } p), \\ -\alpha \left(\frac{-1}{p}\right) \pmod{3}, & \text{if } 2 \text{ is a cubic nonresidue.} \end{cases} \quad (3.4)$$

**Proof.** By Theorem 3.3,

$$2J(\chi) = 2\chi(4) K(\chi) = 2 \left(\frac{-1}{p}\right) \chi(4) K(\chi^2) = 2 \left(\frac{-1}{p}\right) \chi(4)(a_3 + ib_3 \sqrt{3}).$$

Thus, $2J(\chi) = u_3 + iv_3 \sqrt{3}$, where

$$u_3 = 2 \left(\frac{-1}{p}\right) a_3, \quad v_3 = 2 \left(\frac{-1}{p}\right) b_3, \quad \text{if } 2 \text{ is a cubic residue (mod } p),$$

and

$$u_3 = \left(\frac{-1}{p}\right)(3b_3\alpha - a_3), \quad v_3 = \left(\frac{-1}{p}\right)(-a_3\alpha - b_3),$$

if $2$ is a cubic nonresidue (mod $p$). \quad (3.5)

By Theorem 3.3, $a_3 \equiv -1 \pmod{3}$, and so $u_3 \equiv (-1/p) \pmod{3}$. The desired congruence for $v_3$ follows from (3.3).
By (3.4) and (3.5), \( u_3 \) and \( v_3 \) are both even when 2 is a cubic residue and both odd otherwise. If 2 is a cubic nonresidue, then
\[
u_3 = -(-1/p)(a_3 + 3e_3|b_3|) \quad \text{and} \quad v_3 = \alpha(-1/p)(-a_3 + e_3|b_3|).
\]

The equation \( x^2 + 3y^2 = 4p \) clearly has the following three pairs \((x, y)\) of solutions in positive integers:
\[
(2|a_3|, 2|b_3|), \quad (|a_3 - 3b_3|, |a_3 + b_3|), \quad \text{and} \quad (|a_3 + 3b_3|, |a_3 - b_3|).
\]

A slight modification of the proof in Nagell's book [48, pp. 190–191] shows that these are the only such solutions. Note that the first solution above involves even numbers and the last two involve odd numbers. In the case that 2 is a cubic nonresidue, it follows from Theorems 3.4 and 3.5 that the two odd solution pairs are \((|r_3|, |s_3|)\) and \((|u_3|, |v_3|)\). These may be distinguished by using the facts that \(3 \not| s_3\) but \(3 \not| u_3\).

We now evaluate the Gauss sums \(G_3\) and \(G_6\).

**Theorem 3.6.** \(G_3\) is one of the three real roots of \(x^3 - 3px - pr_3\).

**Proof.** First,
\[
G_3 = \sum_n e^{2\pi in/p} \{1 + \chi^2(n) + \chi^4(n)} = G(\chi^2) + \overline{G(\chi^2)},
\]
which implies that \(G_3\) is real. Similarly, we see that the algebraic conjugates of \(G_3\), namely \(\sum_n e^{2\pi in^2g/p}\) and \(\sum_n e^{2\pi in^2g^2/p}\), where \(g\) is a primitive root \((\text{mod} \ p)\), are real.

Hence,
\[
G_3^3 = G^3(\chi^2) + \overline{G^3(\chi^2)} + 3pG_3
= pJ(\chi^2) + pJ(\overline{\chi^2}) + 3pG_3
= pr_3 + 3pG_3,
\]
where we have used Theorem 3.1(i) and Theorem 3.4.

Since
\[
G_3 = G(\chi^2) + \overline{G(\chi^2)}, \quad (3.6)
\]
it is not hard to show, with the use of Theorem 3.6, that \(|G_3| < 2p^{1/2}\). Thus, it is easily seen that \(x^3 - 3px - pr_3\) has one root in each of the intervals \((-2p^{1/2}, -p^{1/2})\), \((-p^{1/2}, p^{1/2})\), and \((p^{1/2}, 2p^{1/2})\). No simple criterion is known for determining the interval in which \(G_3\) lies. For a good discussion of this problem, see Hasse's book [24, pp. 478–489]. See also a paper of E. Lehmer [33].

Cassels [7] has formulated an interesting conjecture which suggests a close
connection between the values of cubic Gauss sums and a certain product of Weierstrass $\varphi$-functions. See also \cite{41} in this connection. In \cite{8}, Cassels gives some equivalent formulations of his conjecture.

**Theorem 3.7.** We have

(i) $G(\chi^3) = \frac{1}{2}(G_3 + iv(4p - G_3^2)^{1/2})$

and

(ii) $G(\chi) = \frac{1}{2}i\tilde{\chi}(4)p^{-1/2}(G_3^2 - 2p + ivG_3(4p - G_3^2)^{1/2})$,

where $v = \text{sgn}\{s_3(G_3^2 - p)\}$.

**Proof.** Since $|G(\chi^2)|^2 = p$, it follows from (3.6) that $\text{Re}\{G(\chi^2)\} = \frac{1}{2}G_3$ and that $\text{Im}\{G(\chi^2)\} = \pm\frac{1}{2}(4p - G_3^2)^{1/2}$. Thus, (i) holds for some $v \in \{-1, 1\}$. Therefore, using Theorems 3.1 and 3.4, we find that

\[
\text{Im}\{G_3^2(\chi^2)\} = \frac{1}{2}v(G_3^2 - p)(4p - G_3^2)^{1/2} = \frac{1}{2}ps_3 \sqrt{3},
\]

from which the desired expression for $v$ follows.

Finally, (ii) follows from (i) with the use of Theorem 3.1(ii). $\blacksquare$

**Theorem 3.8.** If $2$ is a cubic residue (mod $p$), then

$G_6 = G_3 + i*p^{-1/2}(G_3^2 - p);$ if $2$ is a cubic nonresidue (mod $p$), then

$G_6 = G_3 + \frac{1}{2}i*p^{-1/2}((4p - G_3^2) + \epsilon_6G_3(12p - 3G_3^2)^{1/2}),$

where $\epsilon_6 = \text{sgn}\{(a_0 + \epsilon_6 | h_0 |)(G_3^2 - p))\}$.

**Proof.** Subsequently using (3.6), we find that

\[
G_6 = \sum_n e^{2\pi in/p} \left\{ \sum_{j=1}^b \chi_j(n) \right\} = G(\chi) + G(\bar{\chi}) + G(\chi^2) + G(\bar{\chi}^2) + G(\chi^3) = R_4 + G_3 + i*p^{1/2},
\]

where $R_4 = G(\chi) + G(\bar{\chi})$. If $2$ is a cubic residue, then by Theorem 3.7(ii), $R_4 = i*p^{-1/2}(G_3^2 - 2p)$, and the result follows. Suppose now that $2$ is a cubic nonresidue. Then $\tilde{\chi}(4) = -(1 + i\alpha \sqrt{3})/2$, and Theorem 3.7(ii) yields

\[
R_4 = -\frac{1}{2}i*p^{-1/2}(G_3^2 - 2p - \nu\alpha G_3(12p - 3G_3^2)^{1/2}).
\]
By the remark immediately preceding Theorem 3.5, \( s_3 = \alpha (a_3 + \epsilon_3 | b_3 \). Hence, \( \nu \alpha = \epsilon_3 \). Using this in (3.8) and then substituting (3.8) into (3.7), we obtain the desired formula for \( G_6 \).

### 3.2. Quartic Gauss and Jacobi sums

Throughout this section, \( p \equiv 1 \pmod{4} \), and \( \chi \) is a character \( \pmod{p} \) of order 4.

**Theorem 3.9.** We have

\[
K(\chi) = a_4 + ib_4,
\]

where \( a_4 \) and \( b_4 \) are integers such that \( a_4^2 + b_4^2 = p \) and \( a_4 = -(2/p) \pmod{4} \).

**Proof.** Since \( \chi(n) \) is an algebraic integer in \( \mathbb{Q}(i) \) for each rational integer \( n \), it follows that \( K(\chi) = a_4 + ib_4 \), where \( a_4 \) and \( b_4 \) are rational integers such that \( a_4^2 + b_4^2 = p \). Now, by Theorem 2.3,

\[
a_4 + ib_4 = K(\chi) = J(\chi, \chi^2) = \sum_{n=2}^{p-1} \chi(1 - n) \left( \frac{n}{p} \right) \\
= \sum_{n=2}^{p-1} \chi(1 - n) \left( \frac{n}{p} \right) - 1 - 1.
\]

Observe that for \( 2 \leq n \leq p - 1 \), \( (n/p) - 1 \equiv 0 \pmod{2} \) and that \( \chi(1 - n) \equiv 1 \pmod{(1 - i) \Omega} \), since \( \chi(1 - n) \) is a power of \( i \). Thus,

\[
a_4 + ib_4 \equiv \sum_{n=2}^{p-1} \left( \frac{n}{p} \right) - 1 - 1 = -p \pmod{2(1 - i) \Omega}.
\]

Therefore, 8 divides

\[
|a_4 + p + ib_4|^2 = a_4^2 + b_4^2 + p^2 + 2a_4p = p(p + 1 + 2a_4).
\]

Thus, \( a_4 \equiv -(p + 1)/2 \pmod{4} \), and so \( a_4 \equiv -(2/p) \pmod{4} \).

**Corollary 3.10.** We have

\[J(\chi) = c_4 + id_4,\]

where \( c_4 \) and \( d_4 \) are rational integers such that \( c_4^2 + d_4^2 = p \) and \( c_4 = (2/p) a_4 \equiv -1 \pmod{4} \).

**Proof.** The result follows from Theorem 3.9 and the fact that \( \chi(4) = (2/p) \).
Theorem 3.11. In the notation of Theorem 3.9, we have

\[ G_4 = p^{1/2} \pm 2 \left( \frac{2}{p} \right) \left( p + a_4 p^{1/2} \right)^{1/2}. \]

Proof. Since \( p \equiv 1 \pmod{4} \),

\[ G_4 = \sum_n e^{2\pi i n^2/p} (1 + \chi(n) + \chi^2(n) + \chi^3(n)) = p^{1/2} + R_6, \]

where

\[ R_6 = G(\chi) + G(\overline{\chi}). \tag{3.9} \]

It remains to show that

\[ R_6 = \pm 2 \left( \frac{2}{p} \right) \left( p + a_4 p^{1/2} \right)^{1/2}. \tag{3.10} \]

By (3.9) and Theorem 3.9, we find that

\[ R_6^2 = G(\chi^2) J(\chi) + G(\overline{\chi}^2) J(\overline{\chi}) + 2\chi(-1) p \]
\[ = \left( \frac{2}{p} \right) p^{1/2} K(\chi) + \left( \frac{2}{p} \right) p^{1/2} K(\overline{\chi}) + 2 \left( \frac{2}{p} \right) p \]
\[ = 2 \left( \frac{2}{p} \right) (p + a_4 p^{1/2}). \]

The proof in Hasse's text [24, pp. 489–494] also uses Jacobi sums. For older proofs that involve an additional sign ambiguity, see Frick's book [22, p. 443], for example. Special cases of \( G_4 \) are evaluated in a paper [4] by Chowla and the first named author. Loxton [39] has conjectured a beautiful formula for \( G(\chi) \) that determines the sign of \( G_4 \). McGettrick [42] has formulated a conjecture about \( G_4 \) that is analogous to that made by Cassels for cubic sums. Another class of quartic Gauss sums was claimed in [3, Corollary 6.2] to have been evaluated, but the formulas in that corollary are incorrect. For \( p \equiv 5 \pmod{8} \), \( \text{Re} \, G_4 \) is evaluated in [32].

3.3. Octic Gauss and Jacobi sums. Generally, throughout this section, \( p \equiv 1 \pmod{8} \), \( \psi \) is a character \( \pmod{p} \) of order 8, and \( \chi = \psi^2 \).

The following theorem was proved by Leonard and Williams [38, p. 304] using the arithmetic of \( \mathbb{Q}(i, \sqrt{2}) \). (Actually, their result is not quite correct see [38, Erratum]. Throughout Lemma 4.2 and its proof, and also four times in (5.3), \( J(1, 4) \) should be replaced by \( \chi(-1) J(1, 4) \).) We give here an elementary proof which does not make use of unique factorization in \( \mathbb{Q}(i, \sqrt{2}) \).
THEOREM 3.12. We have

\[ K(\psi) = a_8 + ib_8 \sqrt{2}, \]

where \( a_8 \) and \( b_8 \) are rational integers with \( a_8^2 + 2b_8^2 = p \) and \( a_8 \equiv -1 \pmod{4} \).

Proof. Let \( \theta = \exp(2\pi i/8) = (1 + i)/\sqrt{2} \). Then \( Q(\theta) = Q(i, \sqrt{2}) \). Let \( G = \text{Gal}(Q(\theta)/Q) = \{ \sigma_i : i = 1, 3, -1, -3 \} \). Observe that \( Q(i, \sqrt{2}) \) is the fixed field of \( \langle \sigma_3 \rangle = \{ \sigma_3, \sigma_1 \} \). By Theorem 2.5(i), \( K(\psi^3) = K(\psi) \). Hence, \( \sigma_3 \) fixes \( K(\psi) \), and so \( K(\psi) \in Q(i, \sqrt{2}) \). Thus, \( K(\psi) = a_8 + ib_8 \sqrt{2} \), where \( a_8 \) and \( b_8 \) are rational integers such that \( a_8^2 + 2b_8^2 = p \).

Now, by Theorem 2.3,

\[ a_8 + ib_8 \sqrt{2} = K(\psi) = J(\psi, \psi^4) = \sum_{n=2}^{p-1} \psi(1 - n) \left( \frac{n}{p} \right) \]

\[ = -1 + \sum_{n=2}^{p-1} \psi(1 - n) \left( \frac{n}{p} \right) - 1. \]

For \( 2 < n < p - 1 \), \( (n/p) - 1 \equiv 0 \pmod{2} \) and \( \psi(1 - n) \equiv 1 \pmod{(1 - \theta)\Omega} \), because \( \psi(1 - n) \) is a power of \( \theta \). Therefore,

\[ a_8 + ib_8 \sqrt{2} -1 + \sum_{n=2}^{p-1} \left( \frac{n}{p} \right) - 1 \] \[ \equiv -p \pmod{2(1 - \theta)\Omega}. \]

Thus, \( 32 - \prod_{\sigma \in G} \sigma(2(1 - \theta)) \) divides

\[ \prod_{\sigma \in G} \sigma(a_8 + p + ib_8 \sqrt{2}) = ((a_8 + p)^2 + 2b_8^2)^2 \]

in \( \Omega \). Thus, \( 8 \) divides \( (a_8 + p)^2 + 2b_8^2 = p^2 + p + 2pa_8 - p(p + 1 + 2a_8) \). Hence, \( a_8 \equiv -(p + 1)/2 \pmod{4} \), or \( a_8 \equiv -1 \pmod{4} \). □

Define

\[ \eta = \begin{cases} 1, & \text{if } 2 \text{ is a quartic residue (mod } p), \\ -1, & \text{otherwise}. \end{cases} \]

Observe that \( \eta = \chi(2) \).

COROLLARY 3.13. We have

\[ J(\psi) = c_8 + id_8 \sqrt{2}, \]

where \( c_8 \) and \( d_8 \) are rational integers such that \( c_8^2 + 2d_8^2 = p \) and \( c_8 \equiv \eta a_8 \equiv -\eta \pmod{4} \).
The congruences for $c_4 = \text{Re}\{J(x)\}$ and $c_8 = \text{Re}\{J(y)\}$ can be refined, as is seen in the following discussion.

**Theorem 3.14.** We have

$$
c_8 = \begin{cases} 
(p - 3)/2 \pmod{16}, & \text{if } \eta = 1 \text{ and } p \equiv 1 \pmod{16}, \\
(p - 23)/2 \pmod{32}, & \text{if } \eta = -1 \text{ and } p \equiv 1 \pmod{16}, \\
(7 - p)/2 \pmod{32}, & \text{if } \eta = 1 \text{ and } p \equiv 9 \pmod{16}, \\
(p + 17)/2 \pmod{64}, & \text{if } \eta = -1 \text{ and } p \equiv 9 \pmod{16}.
\end{cases}
$$

**Theorem 3.15.** Writing $p = 8k + 1$, we have

$$
d_s = \begin{cases} 
0 \pmod{4}, & \text{if } \eta = (-1)^k, \\
2 \pmod{4}, & \text{if } \eta = (-1)^{k+1}.
\end{cases}
$$

It is easily seen that Theorems 3.14 and 3.15 are equivalent. We demonstrate this, for example, in the case $\eta = -1, p \equiv 1 \pmod{16}$. In this case, Theorem 3.15 states that $d_s \equiv 2 \pmod{4}$, which is true if and only if $d_s^2 \equiv 4 \pmod{32}$, i.e., $p - c_8^2 \equiv 8 \pmod{64}$. This last congruence holds if and only if $c_8 \equiv (p - 23)/2 \pmod{32}$, since $c_8 \equiv 1 \pmod{4}$ by Corollary 3.13.

Theorem 3.15 gives a criterion for the quartic residuacity of 2 given by Barrucand and Cohn [1]. Williams [63] has given a very elementary proof which uses essentially only the law of quadratic reciprocity for the Legendre-Jacobi symbol. Muskat [45, Corollary 2], using cyclotomy, has proved a version of Theorem 3.14.

The next theorem characterizes $c_4$ modulo 16, if $p \equiv 5 \pmod{8}$, and modulo 64, if $p \equiv 1 \pmod{8}$. When $\eta = 1$, $\psi(2) = (2/p)_8$ equals 1 or $-1$ according as 2 is an octic residue (mod $p$) or not.

**Theorem 3.16.** If $p \equiv 5 \pmod{8}$, then $c_4 \equiv (p - 7)/2 \pmod{16}$. If $p = 8k + 1$, then

$$
c_4 = \begin{cases} 
(3p - 5)/2 + 16 \left\{ 1 - \left( \frac{2}{p} \right)_8 \right\} \pmod{64}, & \text{if } 2 \mid k \text{ and } \eta = 1, \\
(3p - 5)/2 \pmod{64}, & \text{if } 2 \mid k \text{ and } \eta = -1, \\
(15 - p)/2 + 16 \left\{ 1 + \left( \frac{2}{p} \right)_8 \right\} \pmod{64}, & \text{if } 2 \nmid k \text{ and } \eta = 1, \\
(31 - p)/2 \pmod{64}, & \text{if } 2 \nmid k \text{ and } \eta = -1.
\end{cases}
$$

**Proof.** First suppose that $p \equiv 5 \pmod{8}$. By Theorem 2.3 and Corollary 3.10,

$$
J(\chi, \chi^2) = -J(\chi) = -c_4 - id_4.
$$

(3.11)
Since \( \chi(2^{-1}) \neq 1 \), \( N = \text{card}\{n(\text{mod} \ p): \chi(n) = \chi(1 - n) = 1\} \) is even. Now,

\[
16N = \sum_{n=2}^{p-1} \{1 + \chi(n) + \chi^2(n) + \chi^3(n)\} \times \{1 + \chi(1 - n) + \chi^2(1 - n) + \chi^3(1 - n)\}. \tag{3.12}
\]

Using (3.11) and Theorem 2.1, we can expand in (3.12) to obtain \( 16N = p - 7 - 2c_4 \). Thus, \( c_4 \equiv (p - 7)/2 \) (mod 16), as desired.

Now suppose that \( p = 8k + 1 \). The following relations between Jacobi sums follow easily from Theorems 2.2, 2.3, and 2.4:

\[
J(\psi) = J(\psi^2) - J(4) = J(\psi^3, \psi^4) = J(\psi^3) = J(\psi, \psi^4) = \psi(-4) J(\psi, \psi^3) = \psi(-1) J(\psi, \psi^3) = J(\psi^2, \psi^3) \tag{3.13}
\]

and

\[
J(\psi^2) = \psi(-4) J(\psi, \psi^2) = \psi(-4) J(\psi^2, \psi^3) = \psi(-1) J(\psi, \psi^2). \tag{3.14}
\]

Let \( M = \text{card}\{n(\text{mod} \ p): \psi(n) = \psi(1 - n) = 1\} \). Then

\[
\begin{cases} 
2 \mid M, & \text{if } \eta = 1 \text{ and } \left(\frac{2}{p}\right)_8 = 1, \\
2 \nmid M, & \text{otherwise}. 
\end{cases} \tag{3.15}
\]

We have

\[
64M = \sum_{n=2}^{p-1} \{1 + \psi(n) + \ldots + \psi^2(n)\}\{1 + \psi(1 - n) + \ldots + \psi^2(1 - n)\}. \tag{3.16}
\]

As in Corollaries 3.13 and 3.10, write \( c_8 + id_8 \sqrt{2} \) and \( c_4 + id_4 \) for the left members of (3.13) and (3.14), respectively. Using Theorem 2.1, (3.11), (3.13), and (3.14), we can expand in (3.16) to obtain

\[
64M = \begin{cases} 
p - 23 + 18c_4 + 24c_8, & \text{if } 2 \mid k \text{ and } \eta = 1, \\
p - 23 - 6c_4, & \text{if } 2 \mid k \text{ and } \eta = -1, \\
p - 15 + 2c_4, & \text{if } 2 \nmid k \text{ and } \eta = 1, \\
p - 15 + 10c_4 - 8c_8, & \text{if } 2 \nmid k \text{ and } \eta = -1. 
\end{cases} \tag{3.17}
\]

By (3.17), (3.15), and Theorem 3.14, the result follows. 

Note that (3.17) yields another derivation of the cyclotomic numbers \((0, 0)_8\) given in the appendix of [31].

The following theorem is easily seen to be equivalent to Theorem 3.16.
**Theorem 3.17.** If $p \equiv 5 \pmod{8}$, then $d_4 \equiv 2 \pmod{4}$. If $p = 8k + 1$, then

$$d_4 \equiv \begin{cases} 4 \pmod{8}, & \text{if } \eta = -1, \\ 0 \pmod{16}, & \text{if } \left(\frac{2}{p}\right)_8 = (-1)^k, \\ 8 \pmod{16}, & \text{if } \left(\frac{2}{p}\right)_8 = (-1)^{k+1}. \end{cases}$$

One consequence of Theorem 3.17 is that 2 is a quartic residue (mod $p$) if and only if $p = x^2 + 64y^2$ for some integers $x$ and $y$. This result, due to Gauss, is a special case of the supplement to the biquadratic reciprocity law [52, p. 77]. Dirichlet gave a simple proof of Gauss's result which uses essentially only the law of quadratic reciprocity for the Legendre–Jacobi symbol; see [52, p. 72]. Another consequence of Theorem 3.17 is that 2 is an octic residue (mod $p$) if and only if either $p = x^2 + 256y^2 \equiv 1 \pmod{16}$ for some pair $x, y$ of integers, or $p = x^2 + 64y^2 \equiv 9 \pmod{16}$ for certain odd integers $x$ and $y$. This criterion for the octic character of 2 was first proved by Western [55]. Another proof, based on cyclotomy, has been given by Whiteman [58].

In the following theorem, we evaluate the Gauss sum $G_8$. Very special cases of the theorem are given in [4].

**Theorem 3.18.** Let $p = 8k + 1$. Then

$$G_8 = p^{1/2} + R_8 \pm \{(a_8 + p^{1/2})(2\eta R_8 + 4(-1)^k p^{1/2})\}^{1/2},$$

where $R_8 = \pm\{2(p + a_4 p^{1/2})\}^{1/2}$.

**Proof.** First

$$G_8 = \sum_n e^{2\pi in/p} \sum_{j=1}^7 \zeta^j(n) = p^{1/2} + R_8 + R_3 + R_9,$$

where $R_8$ is defined by (3.9) and where

$$R_3 = G(\psi) + G(\bar{\psi}) \quad \text{and} \quad R_9 = G(\psi^2) + G(\bar{\psi}^3). \quad (3.18)$$

By (3.10), it remains to show that

$$R_3 + R_9 = \pm\{(a_8 + p^{1/2})(2\eta R_8 + 4(-1)^k p^{1/2})\}^{1/2}. \quad (3.19)$$

Now,

$$R_3^2 = G(\psi^2) J(\psi) + G(\bar{\psi}^2) J(\bar{\psi}) + 2\psi(-1) p$$

$$= G(\chi) \bar{\chi}(2) K(\psi) + G(\bar{\chi}) \chi(2) K(\bar{\psi}) + 2\psi(-1) p.$$
Similarly, 
\[ R_9^2 = G(\chi) \chi(2) K(\psi^3) \mid G(\chi) \chi(2) K(\bar{\psi}^3) + 2\psi(-1) p. \]

Since \( \chi(2) = \bar{\chi}(2) = \eta \) and \( K(\psi) = K(\psi^3) \) by Theorem 2.5(i),
\[ R_9^2 + R_9^2 = \eta(G(\chi) + G(\bar{\chi})) \{K(\psi) + K(\bar{\psi})\} + 4\psi(-1) p \\
= 2\eta a_8 R_9 + 4\eta(-1) p, \quad (3.20) \]
by Theorem 3.12. By Theorem 2.5(ii),
\[ G(\psi) G(\psi^3) = G(\psi^4) J(\psi, \psi^3) = p^{1/2} \psi(-1) K(\psi). \]

Multiplying this by \( G(\bar{\psi}) / G(\psi) \), we get
\[ G(\bar{\psi}) G(\psi^3) = \frac{G(\bar{\psi})}{G(\psi)} p^{1/2} \psi(-1) \psi(4) \frac{G^2(\psi)}{G(\psi^3)} = p^{1/2} \eta G(\chi). \]

By the two calculations above and Theorem 3.12, we find that
\[ 2R_9 R_9 = 2p^{1/2} \psi(-1) K(\psi) + \psi(-1) K(\bar{\psi}) + \eta G(\chi) + \eta G(\chi) \\
= 2p^{1/2} \{2\psi(-1) a_8 + \eta R_9\}. \quad (3.21) \]

Thus, by (3.20) and (3.21),
\[ (R_9 + R_9)^2 = (a_8 + p^{1/2})(2\eta R_9 + 4\psi(-1) p^{1/2}), \]
from which (3.19) follows.

3.4. Duodecic Gauss and Jacobi sums. Throughout this section, \( p \equiv 1 \pmod{12} \) and \( \psi \) is a character \( \pmod{p} \) of order 12. Let \( \chi = \psi^2 \), and let \( K(\psi^3) = a_4 + ib_4 \) as in Theorem 3.9.

**Theorem 3.19.** We have
\[ K(\psi) = \begin{cases} -K(\psi^3), & \text{if } 3 \mid a_4, \\ K(\psi^3), & \text{if } 3 \nmid a_4. \end{cases} \]

In particular, we can write \( K(\psi) = a_{12} + ib_{12} \), where \( a_{12} = a_4 \) and \( b_{12} = b_4 \) if \( 3 \nmid a_4 \), and where \( a_{12} = -a_4 \) and \( b_{12} = -b_4 \) if \( 3 \mid a_4 \).

**Proof.** Let \( \theta = \exp(2\pi i/12) = (\sqrt{3} + i)/2 \). Then \( Q(\theta) = Q(i, \sqrt{3}) \) and \( \text{Gal}(Q(\theta)/Q) = \{ \sigma_t: t = 1, 5, -1, -5 \} \). Observe that \( Q(i) \) is the fixed field of \( \langle \sigma_5 \rangle = \{ \sigma_5, \sigma_1 \} \). By Theorem 2.5(i), \( K(\psi) = K(\psi^3) \). Hence, \( \sigma_5 \) fixes \( K(\psi) \), and
so $K(\psi) \in Q(i)$. Thus, $K(\psi) = a + ib$, where $a$ and $b$ are rational integers such that $a^2 + b^2 = p$. Therefore,

$$(a - 1) + ib = \psi(4) J(\psi) - 1 = \psi(4) \sum_{n = (p+1)/2} \psi(n(1 - n)).$$

Since the substitution $n \mapsto 1 - n$ leaves $\psi(n(1 - n))$ unchanged, each value $\psi(n(1 - n))$ in the above sum occurs an even number of times. The possible values of $\psi(n(1 - n))$ that can occur are $(\pm \sqrt{3} \pm i)/2$, $(\pm 1 \pm i \sqrt{3})/2$, $\pm 1$, and $\pm i$. Thus, there are integers $m_j$, $1 \leq j \leq 6$, such that

$$(a - 1) + ib = 2m_1 + 2m_2 + m_3(\sqrt{3} + i) + m_4(\sqrt{3} - i)$$
$$+ m_5(1 + i \sqrt{3}) + m_6(1 - i \sqrt{3})$$
$$= (2m_1 + m_5 + m_6) + i(2m_2 + m_3 - m_4) + \sqrt{3}(m_3 + m_4)$$
$$+ i \sqrt{3}(m_5 - m_6).$$

Thus, $m_5 = m_6$, and so $a - 1 = 2(m_1 + m_3)$. This proves that $a$ is odd. Since $a_4$ is odd, it follows from the "uniqueness" of the representation of $p$ as a sum of two squares that $a = \pm a_4$ and $b = \pm b_4$. Therefore, either

$$K(\psi) = \pm K(\psi^3) \quad (3.22)$$
or

$$K(\bar{\psi}) = \pm K(\psi^3). \quad (3.23)$$

Assume for the purpose of contradiction that (3.23) holds. Then

$$\tilde{\chi}(2) G^4(\bar{\psi})/G(\bar{\psi}^5) = \pm G^4(\psi^3)/G(\psi^5),$$
and so $G^2(\psi^5) = \pm p^{1/2} \tilde{\chi}(2) G^2(\bar{\psi})/G(\bar{\psi}^5)$.

Thus,

$$J^2(\psi, \psi^3) = \frac{G^2(\psi) G^2(\psi^3)}{G^2(\psi^4)} = \pm \frac{p^{5/2} \tilde{\chi}(2)}{G^2(\psi^4) G(\bar{\psi}^5)} = \pm \frac{p^{5/2} \tilde{\chi}(2)}{G^2(\chi^2) G(\tilde{\chi})}.$$  

By Theorem 3.1(ii), $G^2(\chi^2) = \chi(4) p^{1/2} G(\chi)$. Thus, $J^2(\psi, \psi^3) = \pm p$. Since $Q(\theta)$ contains $i$ and $J(\psi, \psi^3)$, we have $p^{1/2} \in Q(\theta) = Q(\sqrt{3}, i)$, which is absurd. Thus, (3.22) holds.

Write, for $\epsilon = \pm 1$,

$$K(\psi^3) = \epsilon K(\psi). \quad (3.24)$$

Cubing each side of (3.24), we obtain

$$K(\psi^9) \equiv \epsilon K(\psi^3) \pmod{3 \Omega}.$$
Thus,

$$a_4 - ib_4 = \varepsilon(a_4 + ib_4) \pmod{3\Omega}.$$ 

Since $a_4^2 + b_4^2 = p \equiv 1 \pmod{12}$, exactly one of the pair $a_4, b_4$ is divisible by 3. Thus, if $3 | a_4$, then $\varepsilon = -1$, and if $3 \nmid a_4$, then $\varepsilon = 1$. The result now follows from (3.24).

We now evaluate $G_{12}$. Recall from Theorem 3.8 that

$$G_6 = G_3 + p^{-1/2}(G_3^2 - p),$$

if 2 is a cubic residue $\pmod{p}$, and that

$$G_6 = G_3 + \frac{1}{2} p^{-1/2} \{4p - G_3^2 + \varepsilon_6 G_3(12p - 3G_3^2)^{1/2}\},$$

otherwise. Also recall from (3.9) and (3.10) that

$$R_6 = G(\psi^3) + G(\psi^3) = \pm \left\{ 2 \left( \frac{2}{p} \right) \left( p + a_4 p^{1/2} \right) \right\}^{1/2}.$$ 

**Theorem 3.20.** In the notation above, we have

$$G_{12} = G_6 + R_6 \pm p^{-1/2} G_3 \left\{ 2 \left( \frac{2}{p} \right) \left( p + a_{12} p^{1/2} \right) \right\}^{1/2}.$$ 

**Proof.** First, by (3.7),

$$G_{12} = \sum_n e^{2\pi in/p} \sum_{j=1}^{11} \psi^j(n) = G_6 + R_6 + R_2 + R_{10},$$

where

$$R_2 = G(\psi) + G(\psi) \quad \text{and} \quad R_{10} = G(\psi^3) + G(\psi^3). \quad (3.25)$$

It remains to show that

$$R_2 + R_{10} = \pm p^{-1/2} G_3 \left\{ 2 \left( \frac{2}{p} \right) \left( p + a_{12} p^{1/2} \right) \right\}^{1/2}. \quad (3.26)$$

By Theorem 2.2 and the definition of $K(\psi)$,

$$R_2^5 = G(\psi^3) \psi(4) K(\psi) + G(\psi^3) \psi(4) K(\psi) + 2\psi(-1) p$$

and

$$R_{10}^5 = G(\psi^3) \psi(4) K(\psi^3) + G(\psi^3) \psi(4) K(\psi^3) + 2\psi(-1) p.$$
By Theorem 2.5(i), \(K(\psi) = K(\psi^2)\). Thus,
\[
R_2^2 + R_{10} = \{G(\psi^2) \bar{\psi}(4) + G(\bar{\psi}^2) \psi(4)\}\{K(\psi) + K(\bar{\psi})\} + 4\psi(-1) p
\]
\[
= 4a_{12} \Re \{\bar{\chi}(2) G(\chi)\} + 4\psi(-1) p,
\]
(3.27)
by Theorem 3.19. By Theorem 2.5(ii),
\[
G(\psi) G(\psi^5) = p^{1/2} J(\psi, \psi^5) = p^{1/2} \psi(-1) K(\psi) = p^{1/2} \psi(-4) J(\psi).
\]
(3.28)
Multiplying (3.28) by \(G(\bar{\psi})/G(\psi)\), we have
\[
G(\bar{\psi}) G(\psi^5) = p^{1/2} \psi(-4) G(\psi) G(\psi^5) = p^{1/2} \chi(2) G(\chi).
\]
(3.29)
Thus, by (3.28) and (3.29),
\[
2R_2 R_{10} = 2p^{1/2} \psi(-1) K(\psi) + \psi(-1) K(\bar{\psi}) + \chi(2) G(\bar{\chi}) + \bar{\chi}(2) G(\chi).
\]
(3.30)
Since \(\psi(-1) = (2/p)\), we deduce from (3.27) and (3.30) that
\[
(R_2 + R_{10})^2 = (2a_{12} + 2p^{1/2}) \left(2 \Re \{\bar{\chi}(2) G(\chi)\} + 2 \left(\frac{2}{p}\right) p^{1/2}\right).
\]
By Theorem 3.7(ii),
\[
2 \Re \{\bar{\chi}(2) G(\chi)\} = p^{-1/2} \left(\frac{2}{p}\right) (G_3^2 - 2p).
\]
Therefore,
\[
(R_2 + R_{10})^2 = 2 \left(\frac{2}{p}\right) p^{-1/2} G_3^2 (a_{12} + p^{1/2}),
\]
and (3.26) follows.

3.5. Biduodecic Gauss and Jacobi sums. Throughout this section, \(p \equiv 1 \pmod{24}\), \(\chi\) is a character (mod \(p\)) of order 24, and \(\psi = \chi^2\). Write \(K(\chi^3) = a_8 + ib_9 \sqrt{2}\), as in Theorem 3.12. Let \(\theta = \exp(2\pi i/24)\), and let \(\mathcal{O}\) denote the ring of integers in \(Q(\theta)\). Let \(G = \Gal(Q(\theta)/Q)\), so that \(G = \{\sigma_t: t = \pm 1, \pm 5, \pm 7, \pm 11\}\).

**Lemma 3.21.** \(K(\chi)/K(\chi^5)\) is a unit in \(\mathcal{O}\).

**Proof.** By Stickelberger’s theorem [28, pp. 94, 97],
\[
\mathcal{O} K(\chi) = \mathcal{O} G^2(\chi)/G(\chi^2) = \mathcal{O} G^2(\chi^5)/G(\chi^{10}) = \mathcal{O} K(\chi^5),
\]
where $\mathfrak{a}x$ designates the principal ideal in $\mathfrak{a}$ generated by $x$. The result now follows. □

**Theorem 3.22.** We have

$$K(\chi) = K(\chi^5) = a_{24} + ib_{24} \sqrt{6},$$

where $a_{24}$ and $b_{24}$ are rational integers such that $a_{24}^2 + 6b_{24}^2 = p$ and $a_{24} = a_8$ (mod 3).

**Proof.** Observe that $\sqrt{2} = \theta^3 + \bar{\theta}^3$, $\sqrt{3} = \theta^2 + \bar{\theta}^2$, and $i = \theta^6$. Since $\sigma_5$ maps $\sqrt{2}$, $\sqrt{3}$, and $i$ to $-\sqrt{2}$, $-\sqrt{3}$, and $i$, respectively, and $\sigma_{11}$ maps $\sqrt{2}$, $\sqrt{3}$, and $i$ to $-\sqrt{2}$, $-\sqrt{3}$, and $i$, respectively, we see that $Q(i \sqrt{6})$ is the fixed field of $\langle \sigma_5, \sigma_{11}\rangle = \{\sigma_5, \sigma_{11}, \sigma_7, \sigma_3\}$. Similarly, $Q(i \sqrt{2})$ is the fixed field of $\langle \sigma_{-5}, \sigma_{11}\rangle$. Since, by Theorem 2.5(i), $K(\chi) = K(\chi^5)$, $\sigma_{11}$ fixes $K(\chi)/K(\chi^3)$. Also, $\sigma_{-5}$ fixes $K(\chi)/K(\chi^5)$, since, by cross multiplication, $K(\chi)/K(\chi^3) = K(\chi^5)/K(\chi)$. Hence, $K(\chi)/K(\chi^5) \in Q(i \sqrt{2})$.

Therefore, by Lemma 3.21,

$$K(\chi) = \epsilon K(\chi^5). \quad (3.31)$$

Cubing both sides of (3.31), we find that

$$K(\chi^3) \equiv \epsilon K(\chi^9) \pmod{3O}.$$

Since $K(\chi^3) = K(\chi^9)$ by Theorem 2.5(i),

$$a_8 + ib_8 \sqrt{2} \equiv \epsilon(a_8 - ib_8 \sqrt{2}) \pmod{3O}. \quad (3.32)$$

Since $a_8^2 + 2b_8^2 = p \equiv 1 \pmod{24}$, we have

$$3 \mid b_8, \quad (3.33)$$

for otherwise, $a_8^2 \equiv -1 \pmod{3}$, which is ludicrous.

We can now deduce from (3.32) that $a_8 \equiv \epsilon a_8 \pmod{3}$, and so $\epsilon = 1$. Hence, from (3.31), $K(\chi) = K(\chi^5)$. Thus, $K(\chi)$ is fixed by $\langle \sigma_5, \sigma_{24}\rangle$, and hence $K(\chi) \in Q(i \sqrt{6})$. Therefore, there exists rational integers $a_{24}$ and $b_{24}$ such that

$$K(\chi) = a_{24} + ib_{24} \sqrt{6}, \quad (3.34)$$

and $a_{24}^2 + 6b_{24}^2 = p$. Cubing each side of (3.34), we have

$$a_8 + ib_8 \sqrt{2} = K(\chi^3) \equiv a_{24}^3 = a_{24} \pmod{3O}.$$

Hence, $a_{24} \equiv a_8 \pmod{3}$. □
We remark that if \( p \equiv 1 \pmod{24} \), then \( p = x^2 + 72y^2 \), where \( x \) and \( y \) are rational integers. For, since \( 3 \mid b_9 \) by (3.33), one may take \( x - a_8 \) and \( y = b_9/6 \).

We proceed to prove a series of lemmas necessary for the evaluation of \( G_{24} \) given in Theorem 3.32. Write \( 2f(x^4) = r_3 + is_3 \sqrt{3} \), as in Theorem 3.4; \( K(x^5) = a_4 + ib_4 \), as in Theorem 3.9; and \( K(x^5) = a_8 + ib_8 \sqrt{2} \), as in Theorem 3.12. Define \( \nu = \text{sgn}(s_3(G_{32}^2 - p)) \), as in Theorem 3.7. Recall that

\[
\eta = \chi^6(2) = \begin{cases} 1, & \text{if } 2 \text{ is a quartic residue (mod } p), \\ -1, & \text{otherwise}. \end{cases}
\]

If 2 is a cubic residue (mod \( p \)), observe that

\[
\chi(4) = \psi(2) = \eta. \tag{3.35}
\]

Suppose that 2 is a cubic nonresidue (mod \( p \)). Then write \( \chi^6(4) = \omega^\alpha \), with \( \alpha = \pm 1 \), as we did preceding Theorem 3.4. Then

\[
\chi(4) = \eta \omega^\alpha = -\eta/2 \pm i\eta \sqrt{3}/2. \tag{3.36}
\]

Recall from Theorem 3.8 the definition

\[
e_6 = \nu \alpha = \text{sgn}(a_3 + e_6 | b_9 | (G_{32}^2 - p)).
\]

Recall from (3.25) and (3.26) that

\[
T = R_6 + R_{50} = 2 \text{Re}\{G(\psi) + G(\psi^5)\} = \pm p^{-1/2}G_6(2p + 2a_{12}p^{1/2})^{1/2}. \tag{3.37}
\]

Also recall from (3.9) and (3.10) that

\[
R_6 = G(\chi^6) + G(\chi^5) = \pm(2p + 2a_4p^{1/2})^{1/2}.
\]

**Lemma 3.23.** In the notation above, we have

\[
2 \text{Re}\{\psi(2) G(\psi) + \psi(2) G(\psi^5)\}
\]

\[
= \begin{cases} \eta T, & \text{if } 2 \text{ is a cubic residue (mod } p), \\ -\eta T/2 + \frac{1}{2} \eta e_6 (\text{sgn } T) p^{-1/2}(12p - 3G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2}, & \text{otherwise}. \end{cases}
\]

**Proof.** First,

\[
2 \text{Re}\{\psi(2) G(\psi) + \psi(2) G(\psi^5)\}
\]

\[
= \psi(2)[G(\psi) + G(\psi^5)] + \psi(2)[G(\psi) + G(\psi^5)]
\]

\[
= \{\text{Re } \psi(2)\} T - 2\{\text{Im } \psi(2)\} \text{Im}\{G(\psi) + G(\psi^5)\}.
\]
If 2 is a cubic residue (mod p), then, by (3.35), \( \psi(2) = \eta \), and the result follows.

Suppose that 2 is a cubic nonresidue (mod p). By (3.36), \( \Re \psi(2) = -\frac{\eta}{2} \) and \( \Im \psi(2) = \alpha \eta \sqrt{3}/2 \). As \( \epsilon_6 = \alpha \nu \), it remains to show that

\[
\Im\{G(\tilde{\psi}) + G(\psi^5)\} = -\frac{1}{2} \nu \text{sgn } T \left( p^{-1/2}(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2} \right) .
\]

Now,

\[
|G(\tilde{\psi}) + G(\psi^5)|^2 = 2p + 2 \Re\{G(\psi)G(\psi^5)\} = 2p + 2p^{1/2} \Re J(\psi, \psi^5) = 2p + 2p^{1/2} \Re K(\psi) = 2p + 2p^{1/2}a_{12} ,
\]

by Theorem 2.5(ii) and Theorem 3.19. Since, by (3.37),

\[
\Re\{G(\tilde{\psi}) + G(\psi^5)\} = T/2 = \frac{1}{2} p^{-1/2}G_3(\text{sgn } T)(2p + 2a_{12}p^{1/2})^{1/2} , (3.38)
\]

we have

\[
\Im\{G(\tilde{\psi}) + G(\psi^5)\} = \frac{1}{2} p^{-1/2}(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2} , (3.39)
\]

where \( \epsilon \) is either +1 or -1. It remains to show that \( \epsilon = -\nu \text{sgn } T \).

By (3.38) and (3.39),

\[
\Im\{G(\tilde{\psi}) + G(\psi^5)\}^2 = -\frac{1}{2} p^{-1/2}G_3(\text{sgn } T)(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2}) .
\]

On the other hand, from (3.29),

\[
\begin{align*}
|G(\tilde{\psi}) + G(\psi^5)|^2 &= G^2(\tilde{\psi}) + G^2(\psi^5) + 2G(\tilde{\psi})G(\psi^5) \\
&= J(\tilde{\psi})G(\tilde{\psi}^5) + J(\psi^5)G(\tilde{\psi}^5) + 2p^{1/2}\psi(4)G(\tilde{\psi}^5) \\
&= \psi(4)G(\tilde{\psi}^5)(K(\tilde{\psi}) + K(\psi) + 2p^{1/2}) \\
&= \psi^2(2)G(\tilde{\psi}^5)(2p^{1/2} + 2a_{12}),
\end{align*}
\]

since \( K(\psi^5) = K(\psi) \) by Theorem 2.5(i). Thus, by Theorem 3.7(ii),

\[
\Im\{G(\tilde{\psi}) + G(\psi^5)\}^2 = -\frac{1}{2} p^{-1/2}G_3(4p - G_3^2)^{1/2}(2p^{1/2} + 2a_{12}).
\]

Comparing this with (3.40), we find that \( \epsilon = -\nu \text{sgn } T \), as desired.

**Lemma 3.24.** We have

\[2 \Re \{ \chi(4)G(\chi^8) \} = \begin{cases} \eta G_3 & \text{if } 2 \text{ is a cubic residue (mod } p), \\
-\frac{1}{2} \eta G_3 + \frac{1}{2} \eta \epsilon_6 (12p - 3G_3^2)^{1/2}, & \text{otherwise.}
\end{cases}\]
Proof. Since
\[ G(\chi^5) = \frac{1}{2}(G_3 + iv(4p - G_3^2)^{1/2}) \]
by Theorem 3.7(i), and since \( \varepsilon_\beta = \nu \alpha \), the result follows from (3.35) and (3.36).

Lemma 3.25. Let \( \beta \) be defined by \( \beta = \pm 1 \) and \( \beta = -\eta a_3 \pmod{3} \). Then
\[ J(\chi^5, \chi^8) = \beta_1(4) K(\chi). \]  \hspace{1cm} (3.41)

Proof. Recall from Theorem 3.22 that \( K(\chi) = K(\chi^8) \). From Theorem 2.5(i), \( K(\chi) = K(\chi^{11}) \). Hence,
\[ J(\chi^5, \chi^8) = \chi^2(2) J(\chi) \quad \text{and} \quad J(\chi^{11}) = \chi^4(2) J(\chi), \]
and so
\[ G^2(\chi^5) = \chi^2(2) G(\chi^{10}) J(\chi) \quad \text{and} \quad G^2(\chi^{11}) = \chi^4(2) G(\chi^8) J(\chi). \]
It follows that
\[ J^2(\chi^5, \chi^8) = G^2(\chi^5) G^2(\chi^8)/G^2(\chi^{13}) = \frac{p^{-2}\chi^8(2) G(\chi^8) G(\chi^{10}) G^2(\chi^8) J^2(\chi)}. \]  \hspace{1cm} (3.42)
Set
\[ \beta_0 = J(\chi^5, \chi^8)/\chi(4) K(\chi). \]
It remains to show that \( \beta = \beta_0 \). Using (3.42) and then using Theorem 3.1(ii) in the form \( G^2(\chi^8) = p^{1/2}\chi^4(4) G(\chi^4) \), we obtain
\[ \beta_0^2 = \frac{p^{-2}G(\chi^8) G(\chi^{10}) G^2(\chi^8)}{G(\chi^8) G(\chi^{10}) \chi^2(4) G(\chi^4)} = \frac{p^{-8/2}\psi^4(2) G(\psi^2) G(\psi^8)}{p^{-1/2}\psi^4(2) G(\psi) G(\psi^5)/J(\psi) = \psi^4(2) J(\psi, \psi^5)/J(\psi) = J(\psi, \psi^5)/K(\psi) = 1, \]
by Theorem 2.5(ii).
Lastly, we must show that \( \beta_0 \equiv -\eta a_8 \pmod{3} \). Cubing both sides of (3.41), we have

\[
J(\chi^{15}, \chi^{24}) \equiv \beta_0 \chi^8(4) K(\chi^3) = \beta_0 \eta K(\chi^3) \pmod{3\Omega}.
\]

It follows from (3.33) and the equality \( J(\chi^{15}, \chi^{24}) = -1 \) that \( \beta_0 \equiv -\eta a_8 \pmod{3} \)

Define \( \delta = \delta(\chi) \) by

\[
\delta = \pm 1 \quad \text{and} \quad \delta \equiv a_8 a_4 \eta \pmod{3}, \quad \text{if} \quad 3 \nmid a_4,
\]

\[
\delta = \pm i \quad \text{and} \quad i\delta \equiv a_8 b_4 \eta \pmod{3}, \quad \text{if} \quad 3 \mid a_4.
\]

Observe that \( \delta \) is independent of the choice of \( \chi \) if and only if \( 3 \nmid a_4 \). Note that \( \delta(\chi) = \delta(\chi^5) \) and \( \delta(\chi^7) = \delta(\chi) \).

**Lemma 3.26.** We have

\[
J(\chi, \chi^5) = \delta K(\chi).
\]

**Proof.** First,

\[
G^2(\chi) = G(\chi^2) J(\chi) = G(\chi^5) \tilde{\chi}(4) K(\chi)
\]

and

\[
G^2(\chi^5) = G(\chi^{10}) J(\chi^5) = G(\chi^{10}) \tilde{\chi}^5(4) K(\chi^5).
\]

Hence, since \( K(\chi) = K(\chi^5) \),

\[
J^2(\chi, \chi^5) = \frac{G^2(\chi)}{G^2(\chi^5)} = \frac{G(\chi^2) G(\chi^{10}) K^2(\chi)}{G(\chi^5)^2} = \frac{J(\chi, \chi^5) K(\chi)}{J(\chi^5)}.
\]

Thus, by Theorem 2.5(ii) and Theorem 3.19,

\[
\left( \frac{\delta}{K(\chi)} \right)^2 \frac{J(\psi, \psi^5)}{J(\psi^3)} = \frac{K(\psi)}{K(\psi^3)} = \begin{cases} 1, & \text{if} \quad 3 \nmid a_4, \\ -1, & \text{if} \quad 3 \mid a_4. \end{cases}
\]

Letting \( \delta_0 = J(\chi, \chi^5)/K(\chi) \), we have shown that

\[
\delta = \begin{cases} \pm 1, & \text{if} \quad 3 \nmid a_4, \\ \pm i, & \text{if} \quad 3 \mid a_4. \end{cases}
\]

For brevity, put \( A = \chi^3 \). Cubing both sides of \( J(\chi, \chi^5) = \delta_0 K(\chi) \), we have

\[
J(A, A^3) = \delta_0 K(A) \pmod{3\Omega}.
\]
Thus,

\[ \delta_0 = K(A) J(A^2, \bar{A}) = A(4) J(A) J(\bar{A}, A) \]

\[ = \frac{\eta G^2(A) G(A^2) G(\bar{A})}{G(A^2)^2} = \frac{\eta p A(-1) G(A) G(A^2)}{G^2(A^2)} \]

\[ = \frac{\eta p A(-1) J(A, A^3)}{J(A^2)} \pmod{3\Omega}. \]

By Theorem 2.5(ii), \( J(A, A^3) = A(-1) K(A) \). Thus,

\[ \delta_0 = \eta J(\bar{A}^3) K(A) = \eta J(A) \bar{K}(A) \]

\[ = \eta(a_4 - ib_4)(a_8 + ib_8 \sqrt{2}) \equiv \eta a_8(a_4 - ib_4) \pmod{3\Omega}, \]

since \( 3 \mid b_8 \). If \( 3 \nmid a_4 \), then \( 3 \mid b_4 \), and we conclude that \( \delta_0 \equiv \eta a_8 a_4 \pmod{3} \). If \( 3 \mid a_4 \), we conclude that \( \delta_0 \equiv \eta a_8 b_4 \pmod{3} \).

**LEMMA 3.27.** Let \( \epsilon_{24} \) be defined by \( \epsilon_{24} = \pm 1 \) and

\[ \epsilon_{24} \equiv (\text{sgn } R_\delta) a_8 a_4 \eta \pmod{3}, \quad \text{if } 3 \nmid a_4, \]

\[ (\text{sgn } R_\delta) a_8 | b_4 | \eta \pmod{3}, \quad \text{if } 3 | a_4. \]

Then

\[ 2 \Re(\delta G(\chi^6)) = \epsilon_{24}(2p + 2a_4 p^{1/2})^{1/2}. \]

**Proof.** Since \( |G(\chi^6)|^2 = p \) and

\[ 2 \Re G(\chi^6) = R_\delta = (\text{sgn } R_\delta)(2p + 2a_4 p^{1/2})^{1/2}, \]

we have

\[ 2G(\chi^6) = R_\delta + i\epsilon(2p - 2a_4 p^{1/2})^{1/2}, \quad (3.44) \]

where \( \epsilon \) is either +1 or -1. Hence,

\[ 4G^2(\chi^6) = 4a_4 p^{1/2} + 4i\epsilon(\text{sgn } R_\delta) p^{1/2} | b_4 |. \quad (3.45) \]

However,

\[ 4G^2(\chi^6) = 4p^{1/2} J(\chi^6) = 4p^{1/2} K(\chi^4) = 4p^{1/2}(a_4 + ib_4). \quad (3.46) \]

By (3.45) and (3.46),

\[ \epsilon = (\text{sgn } b_4)(\text{sgn } R_\delta). \]
By (3.44) and the above,

$$2 \delta G(\chi^a) = \delta R_e + i \delta (\text{sgn } b_4)(\text{sgn } R_e)(2p - 2a_4 p^{1/2})^{1/2}. $$

If $3 \nmid a_4$, then $\delta$ is real by (3.43) and $a_4 = a_{12}$ by Theorem 3.19. Thus,

$$2 \text{Re}\{\delta G(\chi^a)\} = \delta R_e = \delta (\text{sgn } R_e)(2p + 2a_{12} p^{1/2})^{1/2},$$

and the result follows from (3.43). If $3 \mid a_4$, then $i \delta$ is real by (3.43) and $a_4 = -a_{12}$ by Theorem 3.19. Thus,

$$2 \text{Re}\{\delta G(\chi^a)\} = i \delta (\text{sgn } b_4)(\text{sgn } R_e)(2p - 2a_4 p^{1/2})^{1/2},$$

and the result follows from (3.43).

**Lemma 3.28.** We have

$$G(\chi) G(\chi^a) = \beta \chi(-4) p^{1/2} G(\bar{\chi}^a).$$

**Proof.** By Lemma 3.25 and Theorem 2.3,

$$J(\chi^5, \chi^8) = \beta \chi(4) J(\chi, \chi^{12}).$$

Applying $\sigma_5$ to the above, we get

$$J(\chi, \bar{\chi}^8) = \beta \bar{\chi}(4) J(\chi^5, \chi^{12}).$$

Hence,

$$G(\chi) G(\bar{\chi}^a) = \beta \bar{\chi}(4) G(\chi^5) G(\chi^{12}),$$

and so

$$G(\chi^a) = \beta \chi(4) p^{-1/2} G(\chi) G(\bar{\chi}^a).$$

The lemma now easily follows.

**Lemma 3.29.** We have

$$G(\chi) G(\bar{\chi}^{11}) = \bar{\chi}(4) p^{1/2} G(\chi^2).$$

**Proof.** By Theorem 2.5(ii), $J(\bar{\chi}, \bar{\chi}^{11}) = \chi(-1) K(\bar{\chi})$, and so

$$G(\bar{\chi}) G(\bar{\chi}^{11}) = \bar{\chi}(-4) p^{1/2} G^2(\bar{\chi})/G(\bar{\chi}^2).$$
Multiplying both sides by $G^2(\chi)/\chi(-1)p$, we obtain

$$G(\chi) G(\chi^{11}) = \bar{\chi}(4) p^{3/2}G(\bar{\chi}^2) = \bar{\chi}(4) p^{1/2}G(\chi^2).$$

**Lemma 3.30.** We have

$$G(\chi) G(\chi^7) = \beta \bar{\chi}(-4) K(\chi) G(\chi^5).$$

*Proof.* By Theorem 2.5(ii),

$$G(\chi) G(\chi^{11}) = \chi(-1) p^{1/2}K(\chi).$$

Multiplying this by the equality of Lemma 3.28 and rearranging, we find that

$$G(\chi^5) G(\chi^{11}) = \beta \bar{\chi}(-4) K(\chi) G(\chi^5).$$

Putting $\chi^5$ in place of $\chi$, we deduce that

$$G(\chi) G(\chi^7) = \beta \bar{\chi}(-4) K(\chi) G(\chi^5),$$

and the result follows since $K(\chi^5) = K(\chi)$ by Theorem 3.22.

**Lemma 3.31.** We have

$$G(\chi) G(\chi^7) = \delta p^{1/2}G(\chi^6),$$

where $\delta$ is defined by (3.43).

*Proof.* By Lemma 3.26,

$$G(\chi) G(\chi^5) = \delta K(\chi) G(\chi^6).$$

By Theorem 2.5(ii),

$$G(\chi) G(\chi^{11}) = \chi(-1) p^{1/2}K(\chi).$$

Multiplying these two equalities, we find that

$$G(\chi^5) G(\chi^{11}) = \delta p^{1/2}G(\chi^6).$$

The result follows upon the replacement of $\chi$ by $\chi^5$, since $\delta(\chi) = \delta(\chi^5)$.

**Theorem 3.32.** Let $p = 24k + 1$. Then

$$G_{24} = G_{12} \pm \{(a_8 + p^{1/2})(2\eta R_8 + 4(-1)^k p^{1/2})\}^{1/2} \pm W,$$
where, if 2 is a cubic residue \( \text{mod} \ p \),

\[
W = \{(a_{24} + p^{1/2})(2\eta T + 8(-1)^k p^{1/2}) + 4\beta\eta(-1)^k G_3 + 4\epsilon_{24}(2p + 2a_{12} p^{1/2})^{1/2} \}^{1/2},
\]

and where, if 2 is a cubic nonresidue \( \text{mod} \ p \),

\[
W = (a_{24} + p^{1/2})^{1/2}(\eta T + \eta \varepsilon_6 \text{sgn} \ T) p^{-1/2}(12p - 3G_3^{2^{1/2}}(2p + 2a_{12}p^{1/2})^{1/2} + 8(-1)^k p^{1/2} + 4\epsilon_{24}(2p + 2a_{12}p^{1/2})^{1/2} - 2\beta\eta(-1)^k \varepsilon_4(12p - 3G_3^{2^{1/2}} - G_3)^{1/2}.
\]

**Proof.** Let \( R_j = G(x^j) + G(\bar{x}^j) \) for \( j = 1, 5, 7, \) and 11. Then by (3.19), we have

\[
G_{24} = \sum_{x=0}^{23} e^{2\pi in/p} \sum_{j=1}^{23} x^j(n) = G_{12} + (R_3 + R_9) + (R_1 + R_5 + R_7 + R_{11})
\]

\[
= G_{12} + \{(a_8 + p^{1/2})(2\eta R_6 + 4\chi(-1)^k p^{1/2})^{1/2} + (R_1 + R_5 + R_7 + R_{11})
\]

It remains to show that \( (R_1 + R_5 + R_7 + R_{11})^2 = W^2 \).

Now,

\[
R_1^2 = G(\psi) J(\chi) + G(\bar{\psi}) J(\bar{\chi}) + 2\chi(-1)p
\]

\[
= \psi(2) G(\psi) K(\chi) + \psi(2) G(\bar{\psi}) K(\bar{\chi}) + 2\chi(-1)p.
\]

Replace \( \chi \) by \( \chi^{11} \). Since \( K(\chi) = K(\chi^{11}) \) by Theorem 2.5(i), we find that

\[
R_{11}^2 = \psi(2) G(\psi) K(\chi) + \psi(2) G(\bar{\psi}) K(\bar{\chi}) - 2\chi(-1)p.
\]

Thus, by Theorem 3.22,

\[
R_1^2 + R_{11}^2 = 4a_{24} \text{Re}\{\psi(2) G(\psi)\} + 4\chi(-1)p.
\]

Replacing \( \chi \) by \( \chi^5 \) in this equality, we find that

\[
R_5^2 + R_7^2 = 4a_{24} \text{Re}\{\psi(2) G(\psi^5)\} + 4\chi(-1)p.
\]

Thus,

\[
R_1^2 + R_5^2 + R_7^2 + R_{11}^2 = 4a_{24} \text{Re}\{\bar{\psi}(2) G(\psi) + \psi(2) G(\psi^5)\} + 8\chi(-1)p.
\]

(3.47)

By Lemmas 3.26 and 3.28,

\[
R_1 R_5 = 2 \text{Re}\{\delta K(\chi) G(\chi^6) + \beta \chi(-4)^{1/2} G(\bar{\chi}^6)\}.
\]

(3.48)
Since both \( \sigma_3 \) and \( \sigma_{11} \) fix \( K(\chi^5) \) by Theorems 3.22 and 2.5(i), respectively, we have \( K(\chi) = K(\chi^5) \). Thus, replacing \( \chi \) by \( \chi^2 \) in (3.48), we get

\[
R_7 R_{11} = 2 \text{Re}\{\delta K(\chi) G(\chi^6) + \beta \chi(-4) p^{1/2} G(\chi^6)\},
\]

since \( \delta(\chi^2) = \bar{\delta}(\chi) \). By Lemmas 3.30 and 3.31,

\[
R_1 R_7 = 2 \text{Re}\{\beta \chi(-4) K(\chi) G(\chi^6) | \delta p^{1/2} G(\chi^6)\}.
\]

Replacing \( \chi \) by \( \chi^5 \) in (3.50) and using the facts that \( K(\chi) = K(\chi^5) \) and \( \delta(\chi) = \delta(\chi^5) \), we find that

\[
R_5 R_{11} = 2 \text{Re}\\{\beta \chi(-4) K(\chi) G(\chi^6) + \delta p^{1/2} G(\chi^6)\}. \tag{3.51}
\]

By Theorem 2.5(ii) and Lemma 3.29,

\[
R_1 R_{11} = 2 \text{Re}\{\chi(-1) p^{1/2} K(\chi) + \chi(4) p^{1/2} G(\chi^6)\}. \tag{3.52}
\]

Replacing \( \chi \) by \( \chi^5 \) in (3.52) and using the fact that \( K(\chi) = K(\chi^5) \), we have

\[
R_5 R_7 = 2 \text{Re}\{\chi(-1) p^{1/2} K(\chi) + \chi(4) p^{1/2} G(\chi^{10})\}. \tag{3.53}
\]

Combining formulas (3.47)-(3.53), we deduce that

\[
(R_1 + R_5 + R_7 + R_{11})^2 = 4 \text{Re}\{\sum \phi(2) G(\psi) + \psi(2) G(\psi^5)\}
+ 8 \chi(-1) p^{1/2} + 8 \beta \chi(-1) \text{Re}\{\chi(4) G(\chi^6)\} + 8 \text{Re}\{\delta G(\chi^6)\}.
\]

By Lemmas 3.23, 3.24, and 3.27, \( (R_1 + R_5 + R_7 + R_{11})^2 = W^2 \).

3.6. Bidecic Jacobi sums. Throughout this section, \( p \equiv 1 \pmod{20} \), \( \chi \) is a character \( \pmod{p} \) of order 20, and \( \psi = \chi^2 \). Write \( K(\chi^5) = a_4 + ib_4 \), as in Theorem 3.9. Let \( \theta = \exp(2\pi i/20) \), and let \( \mathcal{O} \) denote the ring of integers in \( \mathbb{Q}(\theta) \). Note that \( G = \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) = \{\sigma_t: t = \pm 1, \pm 3, \pm 7, \pm 9\} \).

\begin{lemma}
K(\chi)/K(\chi^3) is a unit in \( \mathcal{O} \).
\end{lemma}

\begin{proof}
By Stickelberger's theorem [28, pp. 94, 97],

\[
\mathcal{O} K(\chi) = \mathcal{O} G^2(\chi)/G(\chi^2) = \mathcal{O} G^2(\chi^3)/G(\chi^5) = \mathcal{O} K(\chi^3).
\]

\end{proof}

\begin{theorem}
If \( 5 \nmid a_4 \), then there exist rational integers \( a_{20} \) and \( b_{20} \) such that

\[
K(\chi) = a_{20} + ib_{20} \sqrt{5},
\]

as in Theorem 3.9. Let \( \theta = \exp(2\pi i/20) \), and let \( \mathcal{O} \) denote the ring of integers in \( \mathbb{Q}(\theta) \). Note that \( G = \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) = \{\sigma_t: t = \pm 1, \pm 3, \pm 7, \pm 9\} \).

\end{proof}

\begin{lemma}
K(\chi)/K(\chi^3) is a unit in \( \mathcal{O} \).
\end{lemma}

\begin{proof}
By Stickelberger's theorem [28, pp. 94, 97],

\[
\mathcal{O} K(\chi) = \mathcal{O} G^2(\chi)/G(\chi^2) = \mathcal{O} G^2(\chi^3)/G(\chi^5) = \mathcal{O} K(\chi^3).
\]

\end{proof}

\begin{theorem}
If \( 5 \nmid a_4 \), then there exist rational integers \( a_{20} \) and \( b_{20} \) such that

\[
K(\chi) = a_{20} + ib_{20} \sqrt{5},
\]

as in Theorem 3.9. Let \( \theta = \exp(2\pi i/20) \), and let \( \mathcal{O} \) denote the ring of integers in \( \mathbb{Q}(\theta) \). Note that \( G = \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) = \{\sigma_t: t = \pm 1, \pm 3, \pm 7, \pm 9\} \).

\end{proof}
a_{20}^2 + 5b_{20}^2 = p, \text{ and } a_{20} \equiv a_4 \pmod{5}. \text{ If } 5 \mid a_4, \text{ then there exist rational integers } a_{20} \text{ and } b_{20} \text{ such that}

K(\chi) = i(a_{20} + ib_{20} \sqrt{5}),

a_{20}^2 + 5b_{20}^2 = p, \text{ and } a_{20} \equiv b_4 \pmod{5}.

Proof. Observe that \( Q(i) \) is the fixed field of \( \langle \sigma_{-3} \rangle = \langle a_1, \sigma_{-3}, \sigma_9, \sigma_{-7} \rangle \). Since \( K(\chi^p) = K(\chi) \) by Theorem 2.5(i), \( \sigma_{-3} \) fixes \( K(\chi)/K(\chi^3) \). Thus \( K(\chi)/K(\chi^3) \in Q(i) \). Therefore, by Lemma 3.33,

\[ K(\chi) = \epsilon K(\chi^3) \] (3.54)

for some \( \epsilon \in \{1, -1, i, -i\} \). Raising both sides of (3.54) to the fifth power, we find that

\[ a_4 + ib_4 = K(\chi^5) = \epsilon K(\chi^{15}) = \epsilon(a_4 - ib_4) \pmod{5} \] (mod 5Ω). (3.55)

Since \( a_4^2 + b_4^2 = p \equiv 1 \pmod{20} \), exactly one of the pair \( a_4, b_4 \) is divisible by 5. First, suppose that \( 5 \nmid a_4 \). Thus, by (3.55), \( \epsilon = 1 \), and so \( K(\chi) = K(\chi^3) \) by (3.54). As \( \sigma_3 \) fixes \( K(\chi) \), we deduce that \( K(\chi) \in Q(i \sqrt{5}) \). Hence,

\[ K(\chi) = a_{20} + ib_{20} \sqrt{5}, \] (3.56)

where \( a_{20} \) and \( b_{20} \) are certain rational integers. Raising both sides of (3.56) to the fifth power, we see that

\[ a_4 + ib_4 = K(\chi^5) \equiv a_{20} \pmod{5} \] (mod 5Ω).

Thus, \( a_{20} \equiv a_4 \pmod{5} \).

Finally, suppose that \( 5 \mid a_4 \). Then by (3.55), \( \epsilon = -1 \), and so \( K(\chi) = -K(\chi^3) \) by (3.54). As \( \sigma_3 \) fixes \( iK(\chi) \), we have \( iK(\chi) \in Q(i \sqrt{5}) \), and thus

\[ K(\chi) = i(a_{20} + ib_{20} \sqrt{5}), \] (3.57)

where \( a_{20} \) and \( b_{20} \) are certain rational integers. Raising both sides of (3.57) to the fifth power, we deduce that

\[ a_4 + ib_4 = K(\chi^5) \equiv ia_{20} \pmod{5} \] (mod 5Ω).

Hence, \( a_{20} \equiv b_4 \pmod{5} \).

We remark that \( 5 \nmid a_4 \) if and only if 5 is a biquadratic residue (mod \( p \)). This is not hard to prove with the use of the law of biquadratic reciprocity.

The following corollary was proved in [47, p. 198] with the use of cyclo-
tomy. See also papers of Lehmer [36, Theorem 1], [37, Corollary 1.1] and a paper of Muskat [46].

**Corollary 3.35.** Let \( p = 20k + 1 = a^2 + b^2 = u^2 + 5v^2 \) with \( a \) odd. Then \( 5 \mid a \) if and only if \( 2 \mid u \).

**Proof.** Let \( \chi \) have order 20. Then

\[
K(\chi) = 1 + 2 \sum_{2 \leq n < (p-1)/2} \chi(4n(1-n)) = 1 \pmod{2\Omega}. \tag{3.58}
\]

Also, since \( K(\chi^1) = K(\tilde{\chi}) \) by Theorem 2.5(i), we have

\[
\Re K(\chi) = \frac{1}{2} \{ K(\chi) + K(\chi^1) \} = \frac{1}{2} \sum_{n=2}^{p-1} \chi(4n(1-n))(1 + \chi^{10}(4n(1-n)))
= \sum_{n \in S} \chi(4n(1-n))
= 1 + 2 \sum_{2 \leq n < (p-1)/2} \chi(4n(1-n))
= 1 \pmod{2\Omega},
\]

where \( S = \{ n: 2 \leq n \leq p - 1 \text{ and } \chi^{10}(4n(1-n)) = 1 \} \). Thus, by (3.58) and the above,

\[
\Im K(\chi) \in 2\Omega. \tag{3.59}
\]

Now, \( a^2 = a_{20}^2, b^2 = b_{20}^2, u^2 = a_{20}^2, \) and \( v^2 = b_{20}^2 \). If \( 5 \mid a \), then \( 2 \mid a_{20} \) by (3.59) and Theorem 3.34, i.e., \( 2 \mid u \). If \( 5 \nmid a \), then \( 2 \mid b_{20} \) by (3.59) and Theorem 3.34, i.e., \( 2 \mid v \).

In [5], we prove the analogue of Corollary 3.35 for primes \( p = 20k + 9 \). K. S. Williams has a short unpublished proof of this analogue as well as of Corollary 3.35.

**4. Jacobsthal Sums**

Throughout the section, \( p \) is a prime and \( a \) is an integer such that \( p \nmid a \).

**Theorem 4.1.** Let \( p \equiv 1 \pmod{6} \). In the notation of Theorem 3.3,

\[
\psi_3(a) = \begin{cases} 
2 \left( \frac{a}{p} \right) a_3, & \text{if } a \text{ is a cubic residue (mod } p) , \\
- \left( \frac{a}{p} \right) (a_3 + 3\eta_3 \mid b_3) , & \text{otherwise,}
\end{cases}
\]

where \( \eta_3 = \eta_3(a) = \pm 1 \).
Proof. Let \( \chi \) have order 6, and write \( K(\chi^2) = a_3 + ib_3 \sqrt{3} \) as in Theorem 3.3. By Theorem 2.8, we have

\[
\psi_3(a) = \left( \frac{a}{p} \right) \chi(a) K(\chi^2) + \left( \frac{a}{p} \right) \chi^3(a) K(\overline{\chi}^{2})
\]

\[
= 2 \left( \frac{a}{p} \right) \text{Re}(\chi(a)(a_3 + ib_3 \sqrt{3})), \quad (4.1)
\]

and the desired results follow.

Theorem 4.2. Let \( p \equiv 1 \pmod{6} \). Then in the notation of Theorem 3.3,

\[
\varphi_3(a) = \begin{cases} 
-1 + 2a_3, & \text{if } a \text{ is a cubic residue } \pmod{p}, \\
-1 - (a_3 - 3\eta_3 | b_3 |), & \text{otherwise},
\end{cases}
\]

where \( \eta_3 \) has the same designation as in Theorem 4.1.

Proof. Let \( \chi \) have order 6 and write \( K(\chi^2) = a_3 + ib_3 \sqrt{3} \) as in Theorem 3.3. Then by Theorems 2.7, 2.1, and 2.5(i) we find that

\[
\psi_3(a) = -1 + \chi(-1) \chi^4(a) K(\chi) + \chi(-1) \chi^3(a) K(\overline{\chi}^{2})
\]

\[
= -1 + \chi^4(a) K(\chi^2) + \chi^3(a) K(\overline{\chi}^{2}).
\]

The result now follows from (4.1).

Theorem 4.3. Let \( p \equiv 1 \pmod{6} \). Then

\[
\psi_3(a) = \begin{cases} 
-1 + 2 \left( \frac{a}{p} \right) \left[1 + \left( \frac{a}{p} \right) \right] a_3, & \text{if } a \text{ is a cubic residue } \pmod{p}, \\
-1 - \left( \frac{a}{p} \right) (a_3 + 3\eta_3 | b_3 |) - (a_3 - 3\eta_3 | b_3 |), & \text{otherwise},
\end{cases}
\]

where \( \eta_3 = \pm 1 \).

Proof. The result is an immediate consequence of the two previous results and Theorem 2.6.

Various versions of Theorems 4.1–4.3 have been established by several authors. Thus, Theorem 4.1 has been proved by Rajwade [49] and Williams [62]. Different formulations of Theorem 4.2 are due to von Schrutka [50], Chowla [10], and Whiteman [56], [57]. Versions of Theorem 4.3 are due to Chowla [11] and Whiteman [57]. See also [24, pp. 171–175] for a proof of Theorem 4.1.
If 2 is a cubic nonresidue (mod p), it follows immediately from (3.3) and (4.1) that

\[ \eta_a = \begin{cases} b_3 \pmod{3} & \text{if } 2a \text{ is a cubic residue (mod p),} \\ -b_3 \pmod{3} & \text{if } 4a \text{ is a cubic residue (mod p).} \end{cases} \]

Thus, the sign ambiguities in Theorems 4.1–4.3 are resolved except when 2 is a cubic residue (mod p). This was first noticed by E. Lehmer [31, pp. 112–113, [34, p. 67].

**Theorem 4.4.** Let \( p \equiv 1 \pmod{4} \). Using the notation of Corollary 3.10, we have

\[ \varphi_4(a) = \begin{cases} 2c_4 & \text{if } a \text{ is a quartic residue (mod p),} \\ -2c_4 & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod p),} \\ \pm 2 | d_4 | & \text{otherwise.} \end{cases} \]

*Proof.* Let \( \chi \) be a character (mod p) of order 4. Then

\[ \varphi_4(a) = \overline{\chi}(a) K(\chi) + \chi(-a) K(\chi), \]

by Theorem 2.7. Now, \( K(\chi) = (2/p) J(\chi) = \chi(-1) J(\chi) \). Thus, the result follows from Corollary 3.10.

**Theorem 4.5.** Let \( p \equiv 1 \pmod{4} \). Then

\[ \psi_4(a) = \begin{cases} -1 + 2c_4 & \text{if } a \text{ is a quartic residue (mod p),} \\ -1 - 2c_4 & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod p),} \\ -1 \pm 2 | d_4 | & \text{otherwise.} \end{cases} \]

*Proof.* By an elementary calculation [23, p. 82], \( \psi_4(a) = -1 \). By Theorems 2.6 and 4.4, the proof is completed.

**Theorem 4.6.** Let \( p \equiv 1 \pmod{8} \). In the notation of Theorem 3.12, we have

\[ \varphi_4(a) = \begin{cases} 4(-1)^{(p-1)/8} a_8 & \text{if } a \text{ is an octic residue (mod p),} \\ -4(-1)^{(p-1)/8} a_8 & \text{if } a \text{ is a quartic residue but an octic nonresidue (mod p),} \\ 0 & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod p),} \\ \pm 4 | b_8 | & \text{otherwise.} \end{cases} \]
Proof. Let $\chi$ be a character (mod $p$) of order 8. Then
\[
\varphi_4(a) = \bar{\chi}^2(-a) K(\chi) + \chi^2(-a) K(\bar{\chi}) + \bar{\chi}(-a) K(\chi^3) + \chi(-a) K(\bar{\chi}^3)
\]
\[
= \{\bar{\chi}^2(-a) + \bar{\chi}(-a)\} K(\chi) + \{\chi^2(-a) + \chi(-a)\} K(\bar{\chi}),
\]
where we have used Theorems 2.7 and 2.5(i). The theorem now follows from Theorem 3.12 and the fact that $\chi(-1) = (-1)^{(p-1)/8}$.

**Theorem 4.7.** Let $p = 1$ (mod 8). Then
\[
\psi_8(a) = \begin{cases} 
-1 + 2c_4 + 4(-1)^{(p-1)/8} a_8, & \text{if } a \text{ is an octic residue (mod } p), \\
-1 + 2c_4 - 4(-1)^{(p-1)/8} a_8, & \text{if } a \text{ is a quartic residue, but an octic nonresidue (mod } p), \\
-1 - 2c_4, & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod } p), \\
-1 \pm 2 |d_4| \pm 4 |b_8|, & \text{otherwise.}
\end{cases}
\]

Proof. The result is immediate from Theorems 2.6, 4.5 and 4.6.

Theorem 4.4 is a famous theorem of Jacobsthal [26] and is the forerunner of all theorems of this type. Proofs of Jacobsthal’s theorem may be found in the books of Chowla [12, pp. 45-51], Hasse [24, pp. 167-170], Storer [53, pp. 47-48], and (briefly sketched) Davenport [13, p. 122]. Proofs may also be found in the papers of Whitman [56, 57], Burde [6], and Morlaye [43]. Theorem 4.5 was apparently first stated by Chowla [11] and has also been observed by Whitman [57], and by Singh and Rajwade [51]. Theorem 4.6 is due to Whitman [56, 57]. In certain cases, E. Lehmer [31] and the second-named author [19, 20] have removed the ambiguities of sign in some Jacobsthal sums.

In the following theorems, the values of $q_n(a)$ and $\psi_n(a)$ will be given in tables for convenience. Columns will indicate the quadratic, cubic, quartic, and octic residuacity of $a$. Thus, for example, if an $\times$ appears in the column headed by “cubic,” it is assumed that $a$ is a cubic residue (mod $p$); and if no $\times$ appears in the column headed by “quartic,” it is assumed that $a$ is a quartic nonresidue (mod $p$).

**Theorem 4.8.** Let $p = 1$ (mod 12). If $3 \mid a_4$, we have

<table>
<thead>
<tr>
<th>$\varphi_8(a)$</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-2c_4$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>$2c_4$</td>
<td>$\times$</td>
<td>$\times$</td>
<td></td>
</tr>
<tr>
<td>$4c_4$</td>
<td>$\times$</td>
<td></td>
<td>$\times$</td>
</tr>
<tr>
<td>$-4c_4$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\pm 6</td>
<td>d_4</td>
<td>$</td>
<td></td>
</tr>
</tbody>
</table>
If $3 \nmid a_4$, we have

<table>
<thead>
<tr>
<th>$\varphi_n(a)$</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$6c_4$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>$-6c_4$</td>
<td>$\times$</td>
<td>$\times$</td>
<td></td>
</tr>
<tr>
<td>$0$</td>
<td>$\times$</td>
<td></td>
<td>$\times$</td>
</tr>
<tr>
<td>$0$</td>
<td>$\times$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\pm 4 \mid d_4$</td>
<td></td>
<td></td>
<td>$\times$</td>
</tr>
<tr>
<td>$\pm 2 \mid d_4$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Proof.** Let $\psi$ have order 12 and write $K(\psi^3) = a_4 + ib_4$ as in Theorem 3.9. Now

$$\varphi_n(a) = \psi(-a) \sum_{j=0}^{5} \psi^{2j}(a) K(\psi^{2j+1}),$$

by Theorem 2.7. By Theorem 2.5(i), $K(\psi) = K(\psi^3)$. Thus,

$$\varphi_n(a) = \psi(-1) \psi^0(a) \{(\psi(a) + \psi^0(a)) K(\psi)$$

$$+ (\tilde{\psi}(a) + \tilde{\psi}^0(a)) K(\tilde{\psi}) + \psi^0(a) K(\psi^3) + \psi^0(a) K(\psi^5)\}$$

$$= 2\psi(-1) \left(\frac{a}{p}\right) \text{Re}\{\psi(a) + \psi^0(a)) K(\psi) + \psi^0(a) K(\psi^3)\}. \quad (4.2)$$

First, suppose that $3 \nmid a_4$. Then by Theorem 3.19, (4.2) may be rewritten as

$$\varphi_n(a) = 2\psi(-1) \left(\frac{a}{p}\right) \text{Re}\{h(a)(a_4 + ib_4)\}, \quad (4.3)$$

where

$$h(a) = -\psi(a) + \psi^3(a) - \psi^5(a)$$

$$= \begin{cases} 
-\frac{1}{\text{Re}\psi(a)}, & \text{if } a \text{ is a quadratic residue (mod } p), \\
0, & \text{if } a \text{ is neither a quadratic nor a cubic residue (mod } p), \\
-3\psi(a), & \text{if } a \text{ is a quadratic nonresidue and a cubic residue (mod } p). 
\end{cases} \quad (4.4)$$

By Corollary 3.10, $c_4 = \psi(-1) a_4$. The results in the first table now follow from (4.3) and (4.4) by considering the six different cases listed.

Secondly, suppose that $3 \mid a_4$. Then by Theorem 3.19, (4.2) yields

$$\varphi_n(a) = 2\psi(-1) \left(\frac{a}{p}\right) \text{Re}\{k(a)(a_4 + ib_4)\}, \quad (4.5)$$
where

\[ k(a) = \psi(a) + \psi^3(a) + \psi^5(a) \]

\[
= \begin{cases} 
3\psi(a), & \text{if } a \text{ is both a quadratic and a cubic residue (mod } p), \\
0, & \text{if } a \text{ is a quadratic residue and a cubic nonresidue (mod } p) \\
\frac{i}{\text{Im } \psi(a)}, & \text{if } a \text{ is a quadratic nonresidue (mod } p).
\end{cases}
\]

(4.6)

The results in the second table now follow from (4.5), (4.6), and the fact that 
\[ c_4 = \psi(-1) a_4. \]

\[ \text{THEOREM 4.9} \quad \text{Let } p \equiv 1 \text{ (mod 12). If } 3 \mid a_4, \text{ we have the following table:} \]

<table>
<thead>
<tr>
<th>(\psi_{12}(a))</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1 + 4a_3 - 2c_4)</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
</tr>
<tr>
<td>(-1 + 4a_3 + 2c_4)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 - 2a_3 + 4c_4)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 - 2a_3 - 4c_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 \pm 6 \mid b_3 \mid)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 \pm 6 \mid d_4 \mid)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If \(3 \nmid a_4\), we have the following table:

\[ \text{THEOREM 4.10} \quad \text{Let } p = 24k + 1. \text{ Then we have the following table of values for } (-1)^k \psi_{12}(a): \]

<table>
<thead>
<tr>
<th>(\psi_{12}(a))</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1 + 4a_3 + 6c_4)</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
</tr>
<tr>
<td>(-1 + 4a_3 - 6c_4)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 - 2a_3)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 - 2a_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 \pm 6 \mid b_3 \mid \pm 4 \mid d_4 \mid)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(-1 \pm 2 \mid d_4 \mid)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ \text{Proof. The tables follow at once from Theorems 2.6, 4.3, and 4.8.} \]

<table>
<thead>
<tr>
<th>(\psi_{12}(a))</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1 + 4a_3 + 6c_4)</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
</tr>
<tr>
<td>(-1 + 4a_3 - 6c_4)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
</tr>
</tbody>
</table>
Proof. Let $\chi$ have order 24. Write $K(\chi) = a_{24} + ib_{24} \sqrt{6}$ as in Theorem 3.22 and write $K(\chi^9) = a_{8} + ib_{8} \sqrt{2}$ as in Theorem 3.12. Now

$$\varphi_{12}(a) = \chi^{12}(-a) \sum_{j=0}^{11} \chi^{2j}(a) K(\chi^{2j+1}),$$

by Theorem 2.7. By Theorem 2.5(i) and Theorem 3.22, we know that $K(\chi) = K(\chi^9) = K(\chi^3) = K(\chi^1)$. Also, by Theorem 2.5(i), $K(\chi^5) = K(\chi^3)$. Thus, the above becomes

$$\varphi_{12}(a) = 2\chi(-1) \left(\frac{a}{p}\right) \text{Re} (\{\chi(a) + \chi^3(a) + \chi^7(a) + \chi^{11}(a)\} K(\chi)$$

$$+ \{\chi^8(a) + \chi^9(a)\} K(\chi^9)$$

$$= 2\chi(-1) \left(\frac{a}{p}\right) \text{Re}(\chi(a)\{1 + \chi^4(a)\}\{1 + \chi^6(a)\}(a_{24} + ib_{24} \sqrt{6})$$

$$+ \chi^8(a)(1 + \chi^6(a))(a_{8} + ib_{8} \sqrt{2})).$$

The theorem now follows by considering the various possibilities for $a$. The proof in the last case is facilitated by observing that $\cos(\pi/12) = (\sqrt{6} + \sqrt{2})/4$ and $\sin(\pi/12) = (\sqrt{6} - \sqrt{2})/4$. 

**Theorem 4.11.** Let $p = 24k + 1$. If $3 \mid a_4$, we have the following table of values for $\psi_{24}(a)$:

<table>
<thead>
<tr>
<th>$\psi_{24}(a)$</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
<th>octic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-1 + 4a_3 - 2c_4 + (-1)^k{8a_{24} + 4a_8}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 + 4a_3 - 2c_4 - (-1)^k{8a_{24} + 4a_8}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>$-1 - 2a_3 + 4c_4 - (-1)^k{4a_{24} - 4a_8}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>$-1 - 2a_3 + 4c_4 + (-1)^k{4a_{24} - 4a_8}$</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$-1 + 4a_3 + 2c_4$</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$-1 - 2a_3 - 4c_4$</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$-1 \pm 6 \mid d_4 \mid \pm 4 \mid b_8 \mid$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$-1 \pm 6 \mid b_3 \mid \pm 12 \mid b_{24} \mid \pm 4 \mid b_8 \mid$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If $3 \nmid a_4$, we have the following table:

<table>
<thead>
<tr>
<th>$\psi_2(a)$</th>
<th>quadratic</th>
<th>cubic</th>
<th>quartic</th>
<th>octic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-1 + 4a_3 + 6c_4 + (-1)^k{8a_{24} + 4a_6}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 + 4a_3 + 6c_4 - (-1)^k{8a_{24} + 4a_6}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 - 2a_3 - (-1)^k{4a_{24} - 4a_6}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 - 2a_3 + (-1)^k{4a_{24} - 4a_6}$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 + 4a_3 - 6c_4$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 - 2a_3$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 \pm 2 \mid d_4 \mid \pm 4 \mid b_6$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>$-1 \pm 6 \mid b_3 \mid \pm 4 \mid d_4 \mid \pm 12 \mid b_{24} \mid \pm 4 \mid b_6$</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

Proof. The tables follow from Theorems 2.6, 4.9, and 4.10.

The foregoing work readily yields simple formulas for $a_3$, $\pm b_3$, $c_4$, $\pm d_4$, $a_8$, and $\pm b_8$. We now derive from the above work a formula for $a_{24}$.

**Theorem 4.12.** Let $p = 24k + 1$. Then

$$a_{24} = \frac{1}{4}(-1)^k \sum_n \left(\frac{n + 2}{p}\right)\left(\frac{n^2 - 2}{p}\right)\left(\frac{n^4 - 4n^2 + 1}{p}\right) - 1.$$  

Proof. Letting $a = 1$ in Theorems 4.6 and 4.10, we find that

$$\varphi_{12}(1) - \varphi_4(1) = 8(-1)^ka_{24}. \quad (4.7)$$

On the other hand, we have

$$\varphi_{12}(1) - \varphi_4(1) = \sum_{n \neq 0} \left(\frac{n}{p}\right)\left(\frac{n^{12} + 1}{p}\right) - \left(\frac{n^4 + 1}{p}\right),$$

$$= \sum_{n \neq 0} \left(\frac{n + n^{-1} + 2}{p}\right)\left(\frac{(n^3 + n^{-3})^2 - 2}{p}\right) - \left(\frac{(n + n^{-1})^2 - 2}{p}\right),$$

$$= \sum_{m} \left(\frac{m + 2}{p}\right)\left(\frac{(m^2 - 3m)^2 - 2}{p}\right) - \left(\frac{m^2 - 2}{p}\right)\left(\frac{4 - m^2}{p}\right), \quad (4.8)$$

since the number of solutions $n$, $n \neq 0$, of the congruence $n + n^{-1} = m$
(mod p) is 1 + ((4 - m^2)/p). The result now follows from (4.7) and (4.8) since
\[
\left( \frac{m + 2}{p} \right) \left\{ 1 + \left( \frac{4 - m^2}{p} \right) \right\} = \left( \frac{m + 2}{p} \right) + \left( \frac{2 - m}{p} \right),
\]
and since \((m^3 - 3m)^2 - 2 = (m^2 - 2)(m^4 - 4m^2 + 1)\).

**Theorem 4.13.** Let \( p = 20k + 1 \). If \( 5 \mid a_4 \), we have the following table of values for \((-1)^k \varphi_{10}(a)\):

<table>
<thead>
<tr>
<th>((-1)^k \varphi_{10}(a))</th>
<th>quadratic</th>
<th>quartic</th>
<th>quintic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2a_4)</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
</tr>
<tr>
<td>(-2a_4)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(\pm 2 \mid b_4 \mid \pm 8 \mid a_{20} \mid)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2a_4 \pm 10 \mid b_{20} \mid)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
</tr>
<tr>
<td>(-2a_4 \pm 10 \mid b_{20} \mid)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(\pm 2 \mid b_4 \mid \pm 2 \mid a_{20} \mid)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If \( 5 \nmid a_4 \), we have the following table of values for \((-1)^k \varphi_{10}(a)\):

<table>
<thead>
<tr>
<th>((-1)^k \varphi_{10}(a))</th>
<th>quadratic</th>
<th>quartic</th>
<th>quintic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2a_4 + 8a_{20})</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
</tr>
<tr>
<td>(-2a_4 - 8a_{20})</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(\pm 2 \mid b_4 \mid)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2a_4 - 2a_{20})</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
</tr>
<tr>
<td>(-2a_4 + 2a_{20})</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(\pm 2 \mid b_4 \mid \pm 10 \mid b_{20} \mid)</td>
<td>(\times)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Proof.** Let \( \chi \) be a character (mod p) of order 20. Write \( K(\chi^5) = a_4 + ib_4 \) as in Theorem 3.9. As in Theorem 3.34, write \( K(\chi) = i(a_{20} + ib_{20} \sqrt{5}) \) if \( 5 \mid a_4 \) and \( K(\chi) = a_{20} + ib_{20} \sqrt{5} \) if \( 5 \nmid a_4 \). By Theorem 2.5(i), \( K(\chi) = K(\chi^9) \) and \( K(\chi^3) = K(\chi^7) \). Thus, using Theorem 2.7, we obtain

\[
\varphi_{10}(a) = \chi(-1) \sum_{j=0}^{9} \chi^{11+2j}(a) K(\chi^{2j+1}) = 2\chi(-1) \text{Re}(\chi^{5}(a) K(\chi^5) + \chi^{9}(a) K(\chi)) + \chi^{7}(a) K(\chi^3) + \chi^{2}(a) K(\chi^5) + \chi(a) K(\chi)).
\]
Suppose first that $5 \mid a_4$. Then from the proof of Theorem 3.34, $K(\chi) = -K(\chi^3)$. Hence, by (4.9),

$$\chi(-1) \varphi_{10}(a) = 2 \text{Re}(\chi^6(a)(a_4 - ib_4)) + \chi(a)(1 - \chi^2(a))(1 - \chi^4(a))(a_2 b_2 - b_2 a_2).$$

The first table now follows by the consideration of each of the six cases. The calculations in the latter three cases are aided by the facts $\cos(\pi/5) = (\sqrt{5} + 1)/4$ and $\cos(2\pi/5) = (\sqrt{5} - 1)/4$.

Secondly, suppose that $5 \nmid a_4$. Then from the proof of Theorem 3.34, $K(\chi) = K(\chi^3)$. Hence, by (4.9),

$$\chi(-1) \varphi_{10}(a) = 2 \text{Re}(\chi^6(a)(a_4 - ib_4)) + \chi(a)(1 + \chi^2(a))(1 - \chi^4(a))(a_2 b_2 - b_2 a_2).$$

The second table now follows in the same manner as above.

5. Difference Sets

We recall that a subset $H$ of a finite (additive) abelian group $G$ is said to be a difference set of $G$ if for some fixed natural number $\lambda$, every nonzero element of $G$ can be written as a difference of two elements of $H$ in exactly $\lambda$ ways [40, p. 641]. In the situation considered here, $G$ is the group of reduced residues (mod $p$), and $H = H_k$, where $H_k$ is the subset of $k$th power residues (mod $p$), where $p$ is an odd prime, and where $k$ is an integer exceeding 2.

For $p \equiv 1 \pmod{k}$, define

$$S_k = \sum_{r \in H_k} e^{2\pi ir/p}.$$ 

Thus, $S_k$ is related to the Gauss sum $G_k$ by $G_k = kS_k + 1$.

**Theorem 5.1.** Let $p \equiv 1 \pmod{k}$ with $p > k + 1$. Then

(i) $H_k$ is a difference set if and only if $|G_k - 1|^2 = p(k - 1) + 1$; and

(ii) $H_k \cup \{0\}$ is a difference set if and only if $|G_k + k - 1|^2 = (p + k - 1)(k - 1)$.

**Proof.** Suppose that $H_k$ is a difference set. Then

$$|S_k|^2 = (p - 1)/k + \lambda \sum_{n \neq 0} e^{2\pi in/p} = (p - 1)/k - \lambda.$$
where $\lambda$ satisfies
\[(p - 1)/k + \lambda(p - 1) = ((p - 1)/k)^2.\]

Hence, $\lambda = (p - 1 - k)/k^2$,
\[| S_k |^2 = \{p(k - 1) + 1\}/k^2, \quad \text{and} \quad | G_k - 1 |^2 = p(k - 1) + 1. \quad (5.1)\]

Conversely, suppose that (5.1) holds. Multiplying, expanding, and collecting terms in the product $S_k S_k$, we see that there exist rational numbers $a_n$, $0 < n < p$, such that
\[\sum_{n=0}^{p-1} a_n e^{2\pi in/p} = 0.\]

Thus, $\exp(2\pi i/p)$ is a root of the polynomial $a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}$ which thus must be divisible by $1 + x + \cdots + x^{p-1}$. Hence, all of the coefficients $a_n$, $0 \leq n \leq p - 1$, are equal, and so $H_k$ is a difference set. This proves (i).

Suppose that $H_k \cup \{0\}$ is a difference set. Then
\[| S_k + 1 |^2 = (p + k - 1)/k - \lambda,\]
where $\lambda$ satisfies
\[(p + k - 1)/k + \lambda(p - 1) = ((p + k - 1)/k)^2.\]

Hence, $\lambda = (p + k - 1)/k^2$,
\[| S_k + 1 |^2 = (p + k - 1)(k - 1)/k^2,\]
and
\[| G_k + k - 1 |^2 = (p + k - 1)(k - 1). \quad (5.2)\]

Conversely, if (5.2) holds, then it follows as above that $H_k \cup \{0\}$ is a difference set.

**Theorem 5.2.** If $p \equiv 1 \pmod{2k}$, then neither $H_k$ nor $H_k \cup \{0\}$ is a difference set.

**Proof.** Since $S_k$ has $k$ distinct conjugates over the rational numbers $Q$, the Galois extension $Q(S_k)$ over $Q$ has degree $k$. Since $p \equiv 1 \pmod{2k}$, we have $-1 \in H_k$. Hence, $S_k$ is real. If $H_k$ (respectively, $H_k \cup \{0\}$) is a difference set, then $| S_k |^2$ (respectively, $| S_k + 1 |^2$) is rational by Theorem 5.1.
Since also $S_k$ is real, we see that $S_k^2$ (respectively, $(S_k + 1)^2$) is rational. This contradicts the fact that $|Q(S_k):Q| = k > 2$.

**Corollary 5.3.** If $p \equiv 1 \pmod{k}$ and $k$ is odd, then neither $H_k$ nor $H_k \cup \{0\}$ is a difference set.

**Theorem 5.4.** Let $p \equiv 1 \pmod{4}$. Then

(i) $H_4$ is a difference set if and only if $p = 1 + 4a^2$, where $a$ is odd; and

(ii) $H_4 \cup \{0\}$ is a difference set if and only if $p = 9 + 4b^2$, where $b$ is odd.

**Proof.** We shall prove only (i), as the proof of (ii) is similar. If $p \equiv 1 \pmod{8}$, neither $H_4$ nor $H_4 \cup \{0\}$ is a difference set by Theorem 5.2. Thus, assume that $p \equiv 5 \pmod{8}$. By Theorems 3.9 and 3.11,

$$G_4 = p^{1/2} \pm i(2p + 2a_4p^{1/2})^{1/2},$$

(5.3)

where $a_4 \equiv 1 \pmod{4}$.

Suppose that $p = 1 + 4a^2$, where $a$ is odd. Then by (5.3), $|G_4 - 1|^2 = 3p + 1$. By Theorem 5.1(i), $H_4$ is a difference set.

Conversely, assume that $H_4$ is a difference set. Since $p \equiv 5 \pmod{8}$, we have, by Theorem 5.1(i) and (5.3),

$$3p + 1 = |G_4 - 1|^2 = 3p + 1 + 2(a_4 - 1)p^{1/2},$$

from which it is obvious that $a_4 = 1$. Since $p \equiv 5 \pmod{8}$, the representation $p = 1 + 4a^2$, where $a$ is odd, follows.

The first part of Theorem 5.4 is the forerunner of theorems of this type and is due to Chowla [9]. The second part of Theorem 5.4 is due to E. Lehmer [30]. Proofs of Theorem 5.4 may also be found in [40, pp. 91–92] and [53, pp. 49–50].

**Theorem 5.5.** If $p \equiv 1 \pmod{6}$, then neither $H_6$ nor $H_6 \cup \{0\}$ is a difference set.

**Proof.** If $p \equiv 1 \pmod{12}$, the result follows from Theorem 5.2. Thus, suppose that $p \equiv 7 \pmod{12}$. We may clearly assume that $p > 7$. Assume that $H_6$ or $H_6 \cup \{0\}$ is a difference set. Then $|G_6 + \alpha|^2 = \beta$, where $\alpha$ and $\beta$ are determined from Theorem 5.1. Note that $\alpha^2 - \beta = -5p$. 

First, suppose that 2 is a cubic residue (mod $p$). Then by Theorem 3.8, 
\[ G_6 = G_3 + ip^{-1/2}(G_3^2 - p) \]. Thus,
\[ (G_3 + \alpha)^2 + p^{-1}(G_3^2 - p)^2 = \beta. \]

Since $p^{-1}G_3^4 = 3G_3^8 + r_3G_3$ by Theorem 3.6, we obtain the simplification
\[ 2G_3^8 + (2\alpha + r_3)G_3 + (p + \alpha - \beta) = 0, \]
which contradicts the fact that $G_3$ has degree 3 over $Q$.

Finally, suppose that 2 is a cubic nonresidue (mod $p$). Then by Theorem 3.8,
\[ (G_3 + \alpha)^2 + \frac{1}{4p}(4p - G_3^2 + \epsilon G_3(12p - 3G_3^2)^{1/2})^2 = \beta. \]

After expanding and eliminating the terms involving $G_3^8$ and $G_3^4$, we obtain the simplification
\[ G_3^8 + (4\alpha - r_3)G_3 - 2p = \epsilon(r_3 - G_3)(12p - 3G_3^2)^{1/2}. \]

After squaring both sides and eliminating the terms involving $G_3^8$ and $G_3^4$, we obtain quadratic polynomials in $G_3$ on the left and right sides whose constant terms are $4p^2 + 2pr_3(4\alpha - r_3)$ and $18pr_3^2$, respectively. Since these two constant terms must be equal, we obtain the equality $p = 5r_3^2 - 2\alpha r_3$.

Thus, $r_3 \mid p$, and so $r_3 = 1$. Therefore $p = 5 - 2\alpha$, which contradicts the fact that $\alpha \in \{-1, 5\}$.

Theorem 5.5 and the following theorem were first established by E. Lehmer [30].

**Theorem 5.6.** Let $p \equiv 1 \pmod{8}$. Then

(i) $H_8$ is a difference set if and only if $p = 1 + 8c^2 - 9 + 64d^2$ for some integers $c$ and $d$;

and

(ii) $H_8 \cup \{0\}$ is a difference set if and only if $p = 49 + 8e^2 = 441 + 64f^2$ for some integers $e$ and $f$.

**Proof.** We prove (i) only, as the proof of (ii) is completely analogous.

If $p \equiv 1 \pmod{16}$, then $H_8$ and $H_8 \cup \{0\}$ are never difference sets by Theorem 5.2. Thus, in the remainder of the proof we assume that $p \equiv 9 \pmod{16}$. 
By Theorems 3.9, 3.12, and 3.18,

\[ G_8 = p^{1/2} + R_8 \pm i\{(a_8 + p^{1/2})(4p^{1/2} - 2\eta R_8)\}^{1/2}, \]  

(5.4)

where \( R_8 = \pm(2p + 2a_4 p^{1/2})^{1/2} \), \( a_4^2 + b_4^2 = a_8^2 + 2b_8^2 = p \), and \( a_4, a_8 \equiv -1 \,(\mod 4) \).

Suppose that \( p = 1 + 8c^2 = 9 + 64d^2 \). Then by Corollary 3.17, \( \eta = 1 \). Also, \( a_8 = -1 \) and \( a_4 = 3 \). Thus, by (5.4),

\[ G_8 = p^{1/2} + R_8 \pm i\{(1 - p^{1/2})(2R_8 - 4p^{1/2})\}^{1/2}, \]

where \( R_8 = \pm(2p + 6p^{1/2})^{1/2} \). Thus, \(|G_8 - 1|^2 = 7p + 1\), and so \( H_8 \) is a difference set by Theorem 5.1(i).

Conversely, suppose that \( H_8 \) is a difference set. By Theorem 5.1(i) and (5.4),

\[ 7p + 1 = |G_8 - 1|^2 = 7p + 1 + p^{1/2}(4a_4 + 2a_4 - 2) \]
\[ + 2R_8(p^{1/2} - \eta p^{1/2} - 1 - \eta a_8). \]

The coefficient of \( R_8 \) must vanish, since \( R_8 \notin Q(p^{1/2}) \). Thus, \( \eta = 1 \) and \( a_8 = -1 \). Consequently, \( a_4 = 3 \). Therefore, \( p = 1 + 2b_8^2 = 9 + b_4^2 \). By Corollary 3.17, \( 8 \mid b_4 \), and the result follows. \( \blacksquare \)

**Theorem 5.7.** Let \( p \equiv 1 \,(\mod 12) \). Then neither \( H_{12} \) nor \( H_{12} \cup \{0\} \) is a difference set.

**Proof.** For brevity, we give a proof only in the case that \( 2 \) is a cubic residue \((\mod p)\). The proof in the other case is very similar. If \( p \equiv 1 \,(\mod 24) \), the result follows from Theorem 5.2. Thus, suppose that \( p \equiv 13 \,(\mod 24) \).

Assume that \( H_{12} \) or \( H_{12} \cup \{0\} \) is a difference set. Then \(|G_{12} + \alpha|^2 = \beta\), where \( \alpha \) and \( \beta \) are determined by Theorem 5.1. Note that \( \alpha^2 - \beta = -11p \).

By Theorems 3.8, 3.9, 3.19, and 3.20, we have

\[ G_{12} = G_3 + p^{-1/2}(G_3^2 - p) \]
\[ \pm i(2p + 2a_4 p^{1/2})^{1/2} \pm p^{-1/2}G_3(2p + 2a_4 p^{1/2})^{1/2}, \]

where \( a_4^2 + b_4^2 = p \), \( a_4 = 1 \,(\mod 4) \), and \( a_{12} = a_4 \) if \( 3 \nmid a_4 \) and \( a_{12} = -a_4 \) if \( 3 \mid a_4 \). Thus,

\[ G_{12} = G_3 + p^{-1/2}(G_3^2 - p) \pm iV(2p + 2a_4 p^{1/2})^{1/2}, \]

where

\[ V = \begin{cases} 
1 \pm p^{-1/2}G_3, & \text{if } 3 \nmid a_4, \\
1 \pm (pb_4)^{-1}G_3(p - a_4 p^{1/2}), & \text{if } 3 \mid a_4.
\end{cases} \]
Therefore,

$$\beta = |G_{12} + \alpha|^2 = (G_3 + p^{-1/2}G_4^2 + \alpha - p^{1/2})^2 + 2V^2(p + a_4p^{1/2}).$$

(5.5)

Note that $2V^2(p + a_4p^{1/2})$ is a quadratic polynomial in $G_3$ with coefficients in $Q(p^{1/2})$ and has constant term $2p + 2a_4p^{1/2}$. Thus, after expanding the right side of (5.5) and eliminating the terms involving $G_3^3$ and $G_3^4$, we obtain a quadratic polynomial in $G_3$ over $Q(p^{1/2})$ with constant term $2p + 2a_4p^{1/2} + (\alpha - p^{1/2})^2 + 2r_3p^{1/2}$. Since $G_3$ has degree 3 over $Q$ and hence over $Q(p^{1/2})$, it follows from (5.5) that $\beta = 2p + 2a_4p^{1/2} + (\alpha - p^{1/2})^2 + 2r_3p^{1/2}$. Thus, since $x^2 - \beta = -11p, -8p + 2p^{1/2}(a_4 - \alpha + r_3) = 0$, which is impossible.

Theorem 5.7 is originally due to Whiteman [60], whose proof was considerably more involved.

Note added in proof. C. R. Matthews has proved the conjectures of Cassels on $G_3$ mentioned after Theorem 3.6. Matthews has also proved the conjectures of Loxton and McGettrick on $G_4$ discussed after Theorem 3.11 and so has eliminated the sign ambiguity in the determination of $G_4$. These results will appear in two papers in Inventiones Math.

The sign ambiguities for the Jacobsthal sums in Section 3.6 have recently been resolved by an elementary method by the second author.

References

10. S. Chowla, A formula similar to Jacobsthal's for the explicit value of $x$ in $p = x^2 + y^2$ where $p$ is a prime of the form $4k + 1$, Proc. Lahore Philos. Soc. 7 (1945).
43. B. MORLAYE, Démonstration élémentaire d’un théorème de Davenport et Hasse, 
44. J. B. MUSKAT, The cyclotomic numbers of order fourteen, Acta Arith. 11 (1966),
263–279.
46. J. B. MUSKAT, On simultaneous representations of primes by binary quadratic forms,
submitted for publication.
47. J. B. MUSKAT AND A. L. WHITEMAN, The cyclotomic numbers of order twenty, Acta
49. A. R. RAJWADE, On rational primes $p$ congruent to 1 (mod 3 or 5), Proc. Cambridge
50. L. VON SCHRUTKA, Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form
$6n + 1$ in ein einfaches und ein dreifaches Quadrat, J. Reine Angew. Math. 140 (1911),
252–265.
51. S. SINGH AND A. R. RAJWADE, The number of solutions of the congruence $y^2 \equiv x^4 - a$
54. A. WEIL, Sur les courbes algébriques et les variétés qui s’en déduisent, Actualités Sci.
London Math. Soc. (2) 9 (1911), 244–272.
56. A. L. WHITEMAN, Theorems analogous to Jacobsthal’s theorem, Duke Math. J. 16
(1949), 619–626.
58. A. L. WHITEMAN, The sixteenth power residue character of 2, Canad. J. Math. 6 (1954),
364–373.
(1957), 401–413.
60. A. L. WHITEMAN, The cyclotomic numbers of order twelve, Acta Arith. 6 (1960), 53–76.
63. K. S. WILLIAMS, Note on a result of Barrucand and Cohn, J. Reine Angew. Math. 285
(1976), 218–220.
64. K. YAMAMOTO, On Jacobi sums and difference sets, J. Combinatorial Theory 3 (1967),
146–181.