JOURNAL OF NUMBER THEORY 11, 349–398 (1979)

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_6, G_{12}, and G_{24} in terms of G_3. 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.

0022-314X/79/030349-50$02.00/0

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_{16}, 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 χ and ψ 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 χ and ψ denote nontrivial characters (mod p). We let φ 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 $\sum_{n \neq a}$ indicates that the summation is over a complete residue system (mod p) with the term corresponding to $n \equiv a \pmod{p}$ omitted. The ring of all algebraic integers is denoted by Ω.

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

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

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]

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

If χ is a character (mod p) of order 24, for $1 \leqslant j \leqslant 11$, 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_6, and R_8 are independent of the choice of χ.

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

THEOREM 2.1. *If χ is a nontrivial character* (mod p), *then*

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

THEOREM 2.2. *If χ, ψ, and $\chi\psi$ are nontrivial characters* (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 ψ is any nontrivial character* (mod p) *and φ is the quadratic character* (mod p), *then*

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

Proof. If m is an integer, the number of solutions n to $n(1 - n) \equiv m$ (mod p) is $1 + \varphi(1 - 4m)$. Thus,

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

$$= \sum_m \psi(m)\, \varphi(1 - 4m) = \bar{\psi}(4) \sum_m \psi(m)\, \varphi(1 - m) = \bar{\psi}(4)\, J(\psi, \varphi). \quad \blacksquare$$

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 ψ be a character* (mod p) *of order exceeding* 2, *and let φ be the quadratic character* (mod p). *Then*

$$\text{(i)} \qquad K(\psi) = \left(\frac{-1}{p}\right) K(\bar{\psi}\varphi)$$

and

$$\text{(ii)} \qquad K(\psi) = \psi(-1)\, J(\psi, \bar{\psi}\varphi).$$

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,

$$\frac{K(\bar{\psi}\varphi)}{K(\psi)} = \frac{G(\chi_\tau \varphi)\, G(\varphi)}{G(\bar{\psi})} \frac{G(\psi\varphi)}{G(\psi)\, G(\varphi)} = \varphi(-1) = \left(\frac{-1}{p}\right),$$

which proves (i).

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

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

$$= \frac{G(\psi)\, G(\overline{\chi_\tau}\varphi)}{G(\varphi)\, \varphi(-1)} \frac{G(\bar{\psi})}{G(\bar{\psi}\varphi)\, G(\varphi)} = \psi(-1). \quad \blacksquare$$

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

THEOREM 2.5. *Let ψ be a character* (mod p) *of order* $2k$. *Then*

$$\text{(i)} \qquad K(\psi) = \left(\frac{-1}{p}\right) K(\psi^{k-1})$$

and

$$\text{(ii)} \qquad K(\psi) = \psi(-1)\, J(\psi, \psi^{k-1}).$$

In Section 3, we prove several theorems (e.g., Theorem 3.3) showing that for certain m, $K(\chi) = a + ibd^{1/2}$ whenever χ 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 χ; in fact, $b = b(\chi) = -b(\bar{\chi})$. On the other hand, a will

frequently be independent of the choice of χ. 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 $\sigma_t \in \mathrm{Gal}(Q(\zeta)/Q)$, where Q denotes the field of rational numbers, by $\sigma_t(\zeta) = \zeta^t$. Note that if χ 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

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

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

THEOREM 2.7. *Let χ be a character* (mod p) *of order $2n$. Then*

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

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

$$\begin{aligned}
\varphi_n(a) &= \sum_m \left(\frac{m}{p}\right)\left(\frac{m^n + a}{p}\right) = \sum_m \chi^n(m)\, \chi^n(m^n + a) \\
&= \sum_m \chi(m^n)\, \chi^n(m^n + a) \\
&= \sum_m \chi(m)\, \chi^n(m + a) \sum_{j=0}^{n-1} \chi^{2j}(m)
\end{aligned}$$

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

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

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

by Theorem 2.3. ∎

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

$$|\varphi_n(a)| \leqslant n p^{1/2},$$

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 χ be a character* (mod 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

$$|\psi_n(a)| \leqslant (n-1)p^{1/2}$$

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.

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 χ is a character $(\bmod p)$ of order 6. Observe that $\chi(-1) = \chi^3(-1) = (-1/p)$.

THEOREM 3.1. *We have*

$$\text{(i)} \quad G^3(\chi^2) = pJ(\chi^2)$$

and

$$\text{(ii)} \quad G(\chi) = \bar{\chi}(4)\, p^{-1/2} i^* G^2(\chi^2).$$

Proof. Since, by Theorem 2.2,

$$J(\chi^2) = \frac{G^2(\chi^2)}{G(\chi^4)} = \frac{G^3(\chi^2)}{p},$$

(i) holds.

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

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

and (ii) follows. ∎

THEOREM 3.2. *We have*

$$J(\chi^2) \equiv -1 \pmod{3\Omega}.$$

Proof. First, observe that

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

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). ∎

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 $(-1 \pm i\sqrt{3})/2$, 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,

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

from which the congruence $a_3 \equiv -1 \pmod 3$ is immediate. ∎

When 2 is a cubic nonresidue (mod p), define α 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

$$r_3 = 2a_3,\ s_3 = 2b_3, \text{ if 2 is a cubic residue (mod } p), \tag{3.1}$$

and

$$r_3 = -a_3 - 3\alpha b_3,\ s_3 = \alpha a_3 - b_3, \text{ if 2 is a cubic nonresidue (mod } p). \tag{3.2}$$

By Theorem 3.2,

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

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 (mod 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 $s_3 \equiv 0 \pmod 3$. Thus, by (3.1) and (3.2),

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

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 ϵ_3 by $\epsilon_3 = \pm 1$, where $\epsilon_3 \equiv |b_3| \pmod 3$. By (3.3), $-\alpha \operatorname{sgn} b_3 \equiv |b_3| \pmod 3$, and so $\epsilon_3 = -\alpha \operatorname{sgn} b_3$. By (3.2), $r_3 = -a_3 + 3\epsilon_3 |b_3|$, and this is a formula for r_3 in terms of variables independent of χ. Also, by (3.2), $s_3 = \alpha(a_3 + \epsilon_3 |b_3|)$.

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

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

Proof. By Theorem 3.3,

$$2J(\chi) = 2\bar{\chi}(4)\,K(\chi) = 2\left(\frac{-1}{p}\right)\bar{\chi}(4)\,K(\chi^2)$$

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

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

$$u_3 = 2\left(\frac{-1}{p}\right)a_3, \qquad v_3 = 2\left(\frac{-1}{p}\right)b_3, \qquad \text{if 2 is a cubic residue (mod } p), \tag{3.4}$$

and

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

$$\text{if 2 is a cubic nonresidue (mod } p). \tag{3.5}$$

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 $u_3 = -(-1/p)(a_3 + 3\epsilon_3 \mid b_3 \mid)$ and $v_3 = \alpha(-1/p)(-a_3 + \epsilon_3 \mid b_3 \mid)$.

The equation $x^2 + 3y^2 = 4p$ clearly has the following three pairs (x, y) of solutions in positive integers:

$$(2 \mid a_3 \mid, 2 \mid b_3 \mid), \quad (\mid a_3 - 3b_3 \mid, \mid a_3 + b_3 \mid), \quad \text{and} \quad (\mid a_3 + 3b_3 \mid, \mid a_3 - b_3 \mid).$$

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 $(\mid r_3 \mid, \mid s_3 \mid)$ and $(\mid u_3 \mid, \mid v_3 \mid)$. These may be distinguished by using the facts that $3 \mid s_3$ but $3 \nmid v_3$.

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,

$$G_3 = \sum_n e^{2\pi i n/p}\{1 + \chi^2(n) + \chi^4(n)\} = G(\chi^2) + \overline{G(\chi^2)},$$

which implies that G_3 is real. Similarly, we see that the algebraic conjugates of G_3, namely $\sum_n e^{2\pi i n^3 g/p}$ and $\sum_n e^{2\pi i n^3 g^2/p}$, where g is a primitive root (mod p), are real.

Hence,

$$\begin{aligned} G_3^3 &= G^3(\chi^2) + \overline{G^3(\chi^2)} + 3pG_3 \\ &= pJ(\chi^2) + pJ(\bar{\chi}^2) + 3pG_3 \\ &= pr_3 + 3pG_3, \end{aligned}$$

where we have used Theorem 3.1(i) and Theorem 3.4. ∎

Since

$$G_3 = G(\chi^2) + G(\bar{\chi}^2), \tag{3.6}$$

it is not hard to show, with the use of Theorem 3.6, that $\mid G_3 \mid < 2p^{1/2}$. 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 $\mathscr{P}$-functions. See also [41] in this connection. In [8], Cassels gives some equivalent formulations of his conjecture.

THEOREM 3.7. *We have*

$$\text{(i)} \quad G(\chi^2) = \tfrac{1}{2}(G_3 + i\nu(4p - G_3^2)^{1/2})$$

and

$$\text{(ii)} \quad G(\chi) = \tfrac{1}{2}i^*\bar{\chi}(4)\, p^{-1/2}(G_3^2 - 2p + i\nu G_3(4p - G_3^2)^{1/2}),$$

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

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

$$\operatorname{Im}\{G^3(\chi^2)\} = \tfrac{1}{2}\nu(G_3^2 - p)(4p - G_3^2)^{1/2} = \tfrac{1}{2}ps_3\sqrt{3},$$

from which the desired expression for ν follows.

Finally, (ii) follows from (i) with the use of Theorem 3.1(ii). ∎

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*

$$G_6 = G_3 + \tfrac{1}{2}i^*p^{-1/2}\{(4p - G_3^2) + \epsilon_6 G_3(12p - 3G_3^2)^{1/2}\},$$

where $\epsilon_6 = \operatorname{sgn}\{(a_3 + \epsilon_3 |\, b_3\,|)(G_3^2 - p)\}$.

Proof. Subsequently using (3.6), we find that

$$\begin{aligned} G_6 &= \sum_n e^{2\pi in/p}\left\{\sum_{j=1}^{5} x^j(n)\right\} \\ &= G(\chi) + G(\bar{\chi}) + G(\chi^2) + G(\bar{\chi}^2) + G(\chi^3) \\ &= R_4 + G_3 + i^*p^{1/2}, \end{aligned} \tag{3.7}$$

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 $\bar{\chi}(4) = -(1 + i\alpha\sqrt{3})/2$, and Theorem 3.7(ii) yields

$$R_4 = -\tfrac{1}{2}i^*p^{-1/2}(G_3^2 - 2p - \nu\alpha G_3(12p - 3G_3^2)^{1/2}). \tag{3.8}$$

By the remark immediately preceding Theorem 3.5, $s_3 = \alpha(a_3 + \epsilon_3 \mid b_3 \mid)$. Hence, $\nu\alpha = \epsilon_6$. 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 χ is a character (mod 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 $a_4 \equiv -(2/p) \pmod 4$.

Proof. Since $\chi(n)$ is an algebraic integer in $Q(i)$ 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,

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

$$= \sum_{n=2}^{p-1} \chi(1-n)\left\{\left(\frac{n}{p}\right) - 1\right\} - 1.$$

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

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

Therefore, 8 divides

$$|(a_4 + p) + ib_4|^2 = a_4^2 + b_4^2 + p^2 + 2a_4 p = p(p + 1 + 2a_4).$$

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*

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

Proof. Since $p \equiv 1 \pmod 4$,

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

where

$$R_6 = G(\chi) + G(\bar{\chi}). \tag{3.9}$$

It remains to show that

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

By (3.9) and Theorem 3.9, we find that

$$\begin{aligned} R_6^2 &= G(\chi^2) J(\chi) + G(\bar{\chi}^2) J(\bar{\chi}) + 2\chi(-1) p \\ &= \left(\frac{2}{p}\right) p^{1/2} K(\chi) + \left(\frac{2}{p}\right) p^{1/2} K(\bar{\chi}) + 2\left(\frac{2}{p}\right) p \\ &= 2\left(\frac{2}{p}\right)(p + a_4 p^{1/2}). \quad \blacksquare \end{aligned}$$

The proof in Hasse's text [24, pp. 489–494] also uses Jacobi sums. For older proofs that involve an additional sign ambiguity, see Fricke'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 $p \equiv 5 \pmod 8$, Re G_4 is evaluated in [32].

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

The following theorem was proved by Leonard and Williams [38, p. 304] using the arithmetic of $Q(i, \sqrt{2})$. (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 $Q(i, \sqrt{2})$.

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 $G = \mathrm{Gal}(Q(\theta)/Q) = \{\sigma_t : t = 1, 3, -1, -3\}$. 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, σ_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,

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

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

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

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

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 Ω. 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

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

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 $c_4 = \mathrm{Re}\{J(\chi)\}$ and $c_8 = \mathrm{Re}\{J(\psi)\}$ can be refined, as is seen in the following discussion.

THEOREM 3.14. *We have*

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

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

$$d_8 \equiv \begin{cases} 0 \pmod 4, & \text{if } \eta = (-1)^k, \\ 2 \pmod 4, & \text{if } \eta = (-1)^{k+1}. \end{cases}$$

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 $d_8 \equiv 2 \pmod 4$, which is true if and only if $d_8^2 \equiv 4 \pmod{32}$, 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*

$$c_4 \equiv \begin{cases} (3p-5)/2 + 16\left\{1 - \left(\frac{2}{p}\right)_8\right\} \pmod{64}, & \text{if } 2 \mid k \text{ and } \eta = 1, \\ (3p-53)/2 \pmod{64}, & \text{if } 2 \mid k \text{ and } \eta = -1, \\ (15-p)/2 + 16\left\{1 + \left(\frac{2}{p}\right)_8\right\} \pmod{64}, & \text{if } 2 \nmid k \text{ and } \eta = 1, \\ (31-p)/2 \pmod{64}, & \text{if } 2 \nmid k \text{ and } \eta = -1. \end{cases}$$

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

$$J(\chi, \chi^2) = -J(\chi) = -c_4 - id_4 . \tag{3.11}$$

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

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

Using (3.11) and Theorem 2.1, we can expand in (3.12) to obtain $16N = p - 7 - 2c_4$. Thus, $c_4 \equiv (p-7)/2 \pmod{16}$, 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:

$$\begin{aligned} J(\psi) &= J(\psi^3) = \psi(4)\, J(\psi^3, \psi^4) = \bar{\psi}(4)\, J(\psi, \psi^4) \\ &= \bar{\psi}(-4)\, J(\psi, \psi^3) = \psi(-1)\, J(\psi, \psi^6) = \psi(-1)\, J(\psi^2, \psi^3) \end{aligned} \quad (3.13)$$

and

$$J(\psi^2) = \psi(-4)\, J(\psi, \psi^2) = \psi(-4)\, J(\psi^2, \psi^5) = \bar{\psi}(4)\, J(\psi, \psi^5). \quad (3.14)$$

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

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

We have

$$64M = \sum_{n=2}^{p-1} \{1 + \psi(n) + \cdots + \psi^7(n)\}\{1 + \psi(1-n) + \cdots + \psi^7(1-n)\}. \quad (3.16)$$

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

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

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*

$$G_8 = p^{1/2} + R_6 \pm \{(a_8 + p^{1/2})(2\eta R_6 + 4(-1)^k p^{1/2})\}^{1/2},$$

where $R_6 = \pm\{2(p + a_4 p^{1/2})\}^{1/2}$.

Proof. First

$$G_8 = \sum_n e^{2\pi i n/p} \sum_{j=1}^{7} \psi^j(n) = p^{1/2} + R_6 + R_3 + R_9,$$

where R_6 is defined by (3.9) and where

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

By (3.10), it remains to show that

$$R_3 + R_9 = \pm\{(a_8 + p^{1/2})(2\eta R_6 + 4(-1)^k p^{1/2})\}^{1/2}. \tag{3.19}$$

Now,

$$\begin{aligned} R_3^2 &= G(\psi^2)\, J(\psi) + G(\bar{\psi}^2)\, J(\bar{\psi}) + 2\psi(-1)p \\ &= G(\chi)\, \bar{\chi}(2)\, K(\psi) + G(\bar{\chi})\, \chi(2)\, K(\bar{\psi}) + 2\psi(-1)p. \end{aligned}$$

Similarly,

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

Since $\chi(2) = \bar{\chi}(2) = \eta$ and $K(\psi) = K(\psi^3)$ by Theorem 2.5(i),

$$\begin{aligned} R_3^2 + R_9^2 &= \eta\{G(\chi) + G(\bar{\chi})\}\{K(\psi) + K(\bar{\psi})\} + 4\psi(-1)p \\ &= 2\eta a_8 R_6 + 4\psi(-1)p, \end{aligned} \tag{3.20}$$

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

$$\begin{aligned} G(\bar{\psi})\,G(\psi^3) &= \frac{G(\bar{\psi})}{G(\psi)}\,p^{1/2}\psi(-1)\,\psi(4)\,\frac{G^2(\psi)}{G(\psi^2)} \\ &= p^{1/2}\eta G(\bar{\chi}). \end{aligned}$$

By the two calculations above and Theorem 3.12, we find that

$$\begin{aligned} 2R_3R_9 &= 2p^{1/2}\{\psi(-1)\,K(\psi) + \psi(-1)\,K(\bar{\psi}) + \eta G(\bar{\chi}) + \eta G(\chi)\} \\ &= 2p^{1/2}\{2\psi(-1)\,a_8 + \eta R_6\}. \end{aligned} \tag{3.21}$$

Thus, by (3.20) and (3.21),

$$(R_3 + R_9)^2 = (a_8 + p^{1/2})(2\eta R_6 + 4\psi(-1)\,p^{1/2}),$$

from which (3.19) follows. ∎

3.4. *Duodecic Gauss and Jacobi sums.* Throughout this section, $p \equiv 1 \pmod{12}$ and ψ is a character $(\bmod p)$ 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 $\mathrm{Gal}(Q(\theta)/Q) = \{\sigma_t : t = 1, 5, -1, -5\}$. Observe that $Q(i)$ is the fixed field of $\langle\sigma_5\rangle = \{\sigma_5, \sigma_1\}$. By Theorem 2.5(i), $K(\psi) = K(\psi^5)$. Hence, σ_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,

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

Since the substitution $n \to 1 - n$ 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 $(\pm\sqrt{3} \pm i)/2$, $(\pm 1 \pm i\sqrt{3})/2$, ± 1, and $\pm i$. Thus, there are integers m_j, $1 \leqslant j \leqslant 6$, such that

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

Thus, $m_5 = m_6$, and so $a - 1 = 2(m_1 + m_5)$. 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

$$K(\psi) = \pm K(\psi^3) \tag{3.22}$$

or

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

Assume for the purpose of contradiction that (3.23) holds. Then $\bar{\chi}(2)\, G^2(\bar{\psi})/G(\bar{\psi}^2) = \pm G^2(\psi^3)/G(\psi^6)$, and so $G^2(\psi^3) = \pm p^{1/2}\bar{\chi}(2)\, G^2(\bar{\psi})/G(\bar{\psi}^2)$. Thus,

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

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 $\epsilon = \pm 1$,

$$K(\psi^3) = \epsilon K(\psi). \tag{3.24}$$

Cubing each side of (3.24), we obtain

$$K(\bar{\psi}^3) \equiv \epsilon K(\psi^3) \pmod{3\Omega}.$$

Thus,

$$a_4 - ib_4 \equiv \epsilon(a_4 + ib_4) \pmod{3\Omega}.$$

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 $3 \mid a_4$, then $\epsilon = -1$, and if $3 \nmid a_4$, then $\epsilon = 1$. 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 (mod p), and that

$$G_6 = G_3 + \tfrac{1}{2}p^{-1/2}\{4p - G_3^2 + \epsilon_6 G_3(12p - 3G_3^2)^{1/2}\},$$

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

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

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

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

Proof. First, by (3.7),

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

where

$$R_2 = G(\psi) + G(\bar{\psi}) \qquad \text{and} \qquad R_{10} = G(\psi^5) + G(\bar{\psi}^5). \tag{3.25}$$

It remains to show that

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

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

$$R_2^2 = G(\psi^2)\,\bar{\psi}(4)\,K(\psi) + G(\bar{\psi}^2)\,\psi(4)\,K(\bar{\psi}) + 2\psi(-1)\,p$$

and

$$R_{10}^2 = G(\bar{\psi}^2)\,\psi(4)\,K(\psi^5) + G(\psi^2)\,\bar{\psi}(4)\,K(\bar{\psi}^5) + 2\psi(-1)\,p.$$

By Theorem 2.5(i), $K(\psi) = K(\psi^5)$. Thus,

$$R_2^2 + R_{10}^2 = \{G(\psi^2)\,\bar{\psi}(4) + G(\bar{\psi}^2)\,\psi(4)\}\{K(\psi) + K(\bar{\psi})\} + 4\psi(-1)\,p$$
$$= 4a_{12}\,\mathrm{Re}\{\bar{\chi}(2)\,G(\chi)\} + 4\psi(-1)\,p, \tag{3.27}$$

by Theorem 3.19. By Theorem 2.5(ii),

$$G(\psi)\,G(\psi^5) = p^{1/2}J(\psi, \psi^5) = p^{1/2}\psi(-1)\,K(\psi) = p^{1/2}\psi(-4)\,J(\psi). \tag{3.28}$$

Multiplying (3.28) by $G(\bar{\psi})/G(\psi)$, we have

$$G(\bar{\psi})\,G(\psi^5) = p^{1/2}\psi(-4)\,\frac{G^2(\psi)}{G(\psi^2)}\,\frac{G(\bar{\psi})}{G(\psi)}$$
$$= p^{1/2}\psi(4)\,G(\bar{\psi}^2) = p^{1/2}\chi(2)\,G(\bar{\chi}). \tag{3.29}$$

Thus, by (3.28) and (3.29),

$$2R_2R_{10} = 2p^{1/2}\{\psi(-1)\,K(\psi) + \psi(-1)\,K(\bar{\psi}) + \chi(2)\,G(\bar{\chi}) + \bar{\chi}(2)\,G(\chi)\}. \tag{3.30}$$

Since $\psi(-1) = (2/p)$, we deduce from (3.27) and (3.30) that

$$(R_2 + R_{10})^2 = (2a_{12} + 2p^{1/2})\left(2\,\mathrm{Re}\{\bar{\chi}(2)\,G(\chi)\} + 2\left(\frac{2}{p}\right)p^{1/2}\right).$$

By Theorem 3.7(ii),

$$2\,\mathrm{Re}\{\bar{\chi}(2)\,G(\chi)\} = p^{-1/2}\left(\frac{2}{p}\right)(G_3^2 - 2p).$$

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. *Biquodecic Gauss and Jacobi sums.* Throughout this section, $p \equiv 1 \pmod{24}$, χ is a character (mod p) of order 24, and $\psi = \chi^2$. Write $K(\chi^3) = a_8 + ib_8\sqrt{2}$, 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 $G = \mathrm{Gal}(Q(\theta)/Q)$, 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 $\mathcal{O}x$ designates the principal ideal in $\mathcal{O}$ 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* $a_{24} \equiv a_8 \pmod 3$.

Proof. Observe that $\sqrt{2} = \theta^3 + \bar{\theta}^3$, $\sqrt{3} = \theta^2 + \bar{\theta}^2$, and $i = \theta^6$. Since σ_5 maps $\sqrt{2}$, $\sqrt{3}$, and i to $-\sqrt{2}$, $-\sqrt{3}$, and i, respectively, and σ_{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 $\langle \sigma_5, \sigma_{11} \rangle = \{\sigma_5, \sigma_{11}, \sigma_7, \sigma_1\}$. Similarly, $Q(i\sqrt{2})$ is the fixed field of $\langle \sigma_{-5}, \sigma_{11} \rangle$. Since, by Theorem 2.5(i), $K(\chi) = K(\chi^{11})$, σ_{11} fixes $K(\chi)/K(\chi^5)$. Also, σ_{-5} fixes $K(\chi)/K(\chi^5)$, since, by cross multiplication, $K(\chi)/K(\chi^5) = K(\bar{\chi}^5)/K(\bar{\chi})$. Hence, $K(\chi)/K(\chi^5) \in Q(i\sqrt{2})$.

Therefore, by Lemma 3.21,

$$K(\chi) = \epsilon K(\chi^5). \tag{3.31}$$

Cubing both sides of (3.31), we find that

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

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

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

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

$$3 \mid b_8, \tag{3.33}$$

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 $\langle \sigma_5, \sigma_{11} \rangle$, and hence $K(\chi) \in Q(i\sqrt{6})$. Therefore, there exists rational integers a_{24} and b_{24} such that

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

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

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

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 $3 \mid b_8$ by (3.33), one may take $x = a_8$ and $y = b_8/6$.

We proceed to prove a series of lemmas necessary for the evaluation of G_{24} given in Theorem 3.32. Write $2J(\chi^8) = r_3 + is_3\sqrt{3}$, as in Theorem 3.4; $K(\chi^6) = a_4 + ib_4$, as in Theorem 3.9; and $K(\chi^3) = a_8 + ib_8\sqrt{2}$, as in Theorem 3.12. Define $\nu = \operatorname{sgn}\{s_3(G_3^2 - p)\}$, as in Theorem 3.7. Recall that

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

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 $\chi^4(4) = \omega^\alpha$, with $\alpha = \pm 1$, as we did preceding Theorem 3.4. Then

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

Recall from Theorem 3.8 the definition

$$\epsilon_6 = \nu\alpha = \operatorname{sgn}\{(a_3 + \epsilon_3 \mid b_3 \mid)(G_3^2 - p)\}.$$

Recall from (3.25) and (3.26) that

$$T \equiv R_2 + R_{10} = 2\operatorname{Re}\{G(\bar{\psi}) + G(\psi^5)\} = \pm p^{-1/2}G_3(2p + 2a_{12}p^{1/2})^{1/2}. \tag{3.37}$$

Also recall from (3.9) and (3.10) that

$$R_6 = G(\chi^6) + G(\bar{\chi}^6) = \pm(2p + 2a_4p^{1/2})^{1/2}.$$

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

$$2\operatorname{Re}\{\bar{\psi}(2)\,G(\psi) + \psi(2)\,G(\psi^5)\}$$
$$= \begin{cases} \eta T, & \text{if 2 is a cubic residue (mod } p), \\ -\eta T/2 + \frac{1}{2}\eta\epsilon_6(\operatorname{sgn} T)\,p^{-1/2}(12p - 3G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2}, & \text{otherwise.} \end{cases}$$

Proof. First,

$$\begin{aligned} &2\operatorname{Re}\{\bar{\psi}(2)\,G(\psi) + \psi(2)\,G(\psi^5)\} \\ &\quad = \psi(2)\{G(\bar{\psi}) + G(\psi^5)\} + \bar{\psi}(2)\{G(\psi) + G(\bar{\psi}^5)\} \\ &\quad = \{\operatorname{Re}\psi(2)\}T - 2\{\operatorname{Im}\psi(2)\}\operatorname{Im}\{G(\bar{\psi}) + G(\psi^5)\}. \end{aligned}$$

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 $\psi(2) = -\eta/2$ and Im $\psi(2) = \alpha\eta\sqrt{3}/2$. As $\epsilon_6 = \alpha\nu$, it remains to show that

$$\operatorname{Im}\{G(\bar{\psi}) + G(\psi^5)\} = -\tfrac{1}{2}\nu(\operatorname{sgn} T)\, p^{-1/2}(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2}.$$

Now,

$$\begin{aligned} |G(\bar{\psi}) + G(\psi^5)|^2 &= 2p + 2\operatorname{Re}\{G(\psi)\, G(\psi^5)\} \\ &= 2p + 2p^{1/2} \operatorname{Re} J(\psi, \psi^5) = 2p + 2p^{1/2} \operatorname{Re} K(\psi) \\ &= 2p + 2p^{1/2}a_{12}, \end{aligned}$$

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

$$\operatorname{Re}\{G(\bar{\psi}) + G(\psi^5)\} = T/2 = \tfrac{1}{2}p^{-1/2}G_3(\operatorname{sgn} T)(2p + 2a_{12}p^{1/2})^{1/2}, \quad (3.38)$$

we have

$$\operatorname{Im}\{G(\bar{\psi}) + G(\psi^5)\} = \tfrac{1}{2}\epsilon p^{-1/2}(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2}, \quad (3.39)$$

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

By (3.38) and (3.39),

$$\operatorname{Im}\{G(\bar{\psi}) + G(\psi^5)\}^2 = \tfrac{1}{2}\epsilon p^{-1}G_3(\operatorname{sgn} T)(4p - G_3^2)^{1/2}(2p + 2a_{12}p^{1/2}). \quad (3.40)$$

On the other hand, from (3.29),

$$\begin{aligned} \{G(\bar{\psi}) + G(\psi^5)\}^2 &= G^2(\bar{\psi}) + G^2(\psi^5) + 2G(\bar{\psi})\, G(\psi^5) \\ &= J(\bar{\psi})\, G(\bar{\psi}^2) + J(\psi^5)\, G(\bar{\psi}^2) + 2p^{1/2}\psi(4)\, G(\bar{\psi}^2) \\ &= \psi(4)\, G(\bar{\psi}^2)\{K(\bar{\psi}) + K(\psi) + 2p^{1/2}\} \\ &= \psi^2(2)\, G(\bar{\psi}^2)(2p^{1/2} + 2a_{12}), \end{aligned}$$

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

$$\operatorname{Im}\{G(\bar{\psi}) + G(\psi^5)\}^2 = -\tfrac{1}{2}\nu p^{-1/2}G_3(4p - G_3^2)^{1/2}(2p^{1/2} + 2a_{12}).$$

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

LEMMA 3.24. *We have*

$$2\operatorname{Re}\{\bar{\chi}(4)\, G(\chi^8)\} = \begin{cases} \eta G_3, & \text{if 2 is a cubic residue (mod } p), \\ -\tfrac{1}{2}\eta G_3 + \tfrac{1}{2}\eta\epsilon_6(12p - 3G_3^2)^{1/2}, & \text{otherwise.} \end{cases}$$

Proof. Since

$$G(\chi^8) = \tfrac{1}{2}\{G_3 + i\nu(4p - G_3^2)^{1/2}\}$$

by Theorem 3.7(i), and since $\epsilon_6 = \nu\alpha$, the result follows from (3.35) and (3.36). ∎

LEMMA 3.25. *Let β be defined by $\beta = \pm 1$ and $\beta \equiv -\eta a_8 \pmod 3$. Then*

$$J(\chi^5, \chi^8) = \beta\chi(4)\, K(\chi). \tag{3.41}$$

Proof. Recall from Theorem 3.22 that $K(\chi) = K(\chi^5)$. From Theorem 2.5(i), $K(\chi) = K(\chi^{11})$. Hence,

$$J(\chi^5) = \chi^4(2)\, J(\chi) \qquad \text{and} \qquad J(\chi^{11}) = \chi^4(2)\, J(\chi),$$

and so

$$G^2(\chi^5) = \chi^4(2)\, G(\chi^{10})\, J(\chi) \qquad \text{and} \qquad G^2(\chi^{11}) = \chi^4(2)\, G(\bar{\chi}^2)\, J(\chi).$$

It follows that

$$\begin{aligned} J^2(\chi^5, \chi^8) &= G^2(\chi^5)\, G^2(\chi^8)/G^2(\chi^{13}) \\ &= p^{-2}\chi^8(2)\, G(\bar{\chi}^2)\, G(\chi^{10})\, G^2(\chi^8)\, J^2(\chi). \end{aligned} \tag{3.42}$$

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

$$\begin{aligned} \beta_0^2 &= p^{-2}G(\bar{\chi}^2)\, G(\chi^{10})\, G^2(\chi^8) \\ &= p^{-3/2}G(\bar{\chi}^2)\, G(\chi^{10})\, \chi^4(4)\, G(\chi^4) \\ &= p^{-3/2}\psi^4(2)\, G(\bar{\psi})\, G(\psi^2)\, G(\psi^5) \\ &= p^{-1/2}\psi^4(2)\, G(\psi)\, G(\psi^5)/J(\psi) \\ &= \psi^4(2)\, J(\psi, \psi^5)/J(\psi) \\ &= J(\psi, \psi^5)/K(\psi) \\ &= 1, \end{aligned}$$

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

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

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

$$\begin{aligned} &\delta = \pm 1 \quad \text{and} \quad \delta \equiv a_8 a_4 \eta \pmod 3, \quad \text{if} \quad 3 \nmid a_4, \\ &\delta = \pm i \quad \text{and} \quad i\delta \equiv a_8 b_4 \eta \pmod 3, \quad \text{if} \quad 3 \mid a_4. \end{aligned} \tag{3.43}$$

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

LEMMA 3.26. *We have*

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

Proof. First,

$$G^2(\chi) = G(\chi^2)\, J(\chi) = G(\chi^2)\, \bar{\chi}(4)\, K(\chi)$$

and

$$G^2(\chi^5) = G(\chi^{10})\, J(\chi^5) = G(\chi^{10})\, \bar{\chi}^5(4)\, K(\chi^5).$$

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

$$J^2(\chi, \chi^5) = \frac{G^2(\chi)\, G^2(\chi^5)}{G^2(\chi^6)} = \frac{G(\chi^2)\, G(\chi^{10})\, K^2(\chi)}{G^2(\chi^6)} = \frac{J(\chi^2, \chi^{10})\, K^2(\chi)}{J(\chi^6)}.$$

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

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

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 $\Lambda = \chi^3$. Cubing both sides of $J(\chi, \chi^5) = \delta_0 K(\chi)$, we have

$$J(\Lambda, \bar{\Lambda}^3) \equiv \delta_0 K(\Lambda) \pmod{3\Omega}.$$

Thus,

$$\begin{aligned}\delta_0 &\equiv K(\Lambda)\, J(\Lambda^3, \bar{\Lambda}) = \Lambda(4)\, J(\Lambda)\, J(\Lambda^3, \bar{\Lambda}) \\ &= \frac{\eta G^2(\Lambda)\, G(\Lambda^3)\, G(\bar{\Lambda})}{G(\Lambda^2)^2} = \frac{\eta p \Lambda(-1)\, G(\Lambda)\, G(\Lambda^3)}{G^2(\Lambda^2)} \\ &= \frac{\eta p \Lambda(-1)\, J(\Lambda, \Lambda^3)}{J(\Lambda^2)} \pmod{3\Omega}.\end{aligned}$$

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

$$\begin{aligned}\delta_0 &\equiv \eta J(\bar{\Lambda}^2)\, K(\Lambda) = \eta K(\bar{\Lambda}^2)\, K(\Lambda) \\ &= \eta(a_4 - ib_4)(a_8 + ib_8\sqrt{2}) \equiv \eta a_8(a_4 - ib_4) \pmod{3\Omega},\end{aligned}$$

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 $i\delta_0 \equiv \eta a_8 b_4 \pmod 3$. ∎

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

$$\epsilon_{24} \equiv \begin{cases} (\operatorname{sgn} R_6)\, a_8 a_4 \eta \pmod 3, & \text{if } 3 \nmid a_4, \\ (\operatorname{sgn} R_6)\, a_8 \mid b_4 \mid \eta \pmod 3, & \text{if } 3 \mid a_4. \end{cases}$$

Then

$$2 \operatorname{Re}\{\delta G(\chi^6)\} = \epsilon_{24}(2p + 2a_{12}p^{1/2})^{1/2}.$$

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

$$2 \operatorname{Re} G(\chi^6) = R_6 = (\operatorname{sgn} R_6)(2p + 2a_4 p^{1/2})^{1/2},$$

we have

$$2G(\chi^6) = R_6 + i\epsilon(2p - 2a_4 p^{1/2})^{1/2}, \tag{3.44}$$

where ϵ is either $+1$ or -1. Hence,

$$4G^2(\chi^6) = 4a_4 p^{1/2} + 4i\epsilon(\operatorname{sgn} R_6)\, p^{1/2} \mid b_4 \mid. \tag{3.45}$$

However,

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

By (3.45) and (3.46),

$$\epsilon = (\operatorname{sgn} b_4)(\operatorname{sgn} R_6).$$

By (3.44) and the above,

$$2\delta G(\chi^6) = \delta R_6 + i\delta(\operatorname{sgn} b_4)(\operatorname{sgn} R_6)(2p - 2a_4 p^{1/2})^{1/2}.$$

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

$$2 \operatorname{Re}\{\delta G(\chi^6)\} = \delta R_6 = \delta(\operatorname{sgn} R_6)(2p + 2a_{12} p^{1/2})^{1/2},$$

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,

$$2 \operatorname{Re}\{\delta G(\chi^6)\} = i\,\delta(\operatorname{sgn} b_4)(\operatorname{sgn} R_6)(2p - 2a_4 p^{1/2})^{1/2},$$

and the result follows from (3.43). ∎

LEMMA 3.28. *We have*

$$G(\bar{\chi})\, G(\chi^5) = \beta\chi(-4)\, p^{1/2} G(\bar{\chi}^8).$$

Proof. By Lemma 3.25 and Theorem 2.3,

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

Applying σ_5 to the above, we get

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

Hence,

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

and so

$$G(\chi^5) = \beta\chi(4)\, p^{-1/2} G(\chi)\, G(\bar{\chi}^8).$$

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

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

LEMMA 3.30. *We have*

$$G(\chi)\,G(\chi^7) = \beta\bar{\chi}(-4)\,K(\chi)\,G(\chi^8).$$

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

$$G(\chi^5)\,G(\chi^{11}) = \beta\chi(-4)\,K(\chi)\,G(\bar{\chi}^8).$$

Putting χ^5 in place of χ, we deduce that

$$G(\chi)\,G(\chi^7) = \beta\bar{\chi}(-4)\,K(\chi^5)\,G(\chi^8),$$

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

LEMMA 3.31. *We have*

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

where δ *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),

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

Multiplying these two equalities, we find that

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

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

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

$$G_{24} = G_{12} \pm \{(a_8 + p^{1/2})(2\eta R_6 + 4(-1)^k\,p^{1/2})\}^{1/2} \pm W,$$

where, if 2 *is a cubic residue* (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* (mod p),

$$W = (a_{24} + p^{1/2})^{1/2}\{-\eta T + \eta\epsilon_6(\text{sgn } T)\, p^{-1/2}(12p - 3G_3^2)^{1/2}(2p + 2a_{12}p^{1/2})^{1/2} + 8(-1)^k p^{1/2} + 4\epsilon_{24}(2p + 2a_{12}p^{1/2})^{1/2} - 2\beta\eta(-1)^k(\epsilon_6(12p - 3G_3^2)^{1/2} - G_3)\}^{1/2}.$$

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

$$G_{24} = \sum_n e^{2\pi i n/p} \sum_{j=1}^{23} \chi^j(n) = G_{12} + (R_3 + R_9) + (R_1 + R_5 + R_7 + R_{11})$$

$$= G_{12} \pm \{(a_8 + p^{1/2})(2\eta R_6 + 4\chi(-1)\, p^{1/2})\}^{1/2} + (R_1 + R_5 + R_7 + R_{11}).$$

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

Now,

$$R_1^2 = G(\psi)\, J(\chi) + G(\bar{\psi})\, J(\bar{\chi}) + 2\chi(-1)p$$
$$= \bar{\psi}(2)\, G(\psi)\, K(\chi) + \psi(2)\, G(\bar{\psi})\, K(\bar{\chi}) + 2\chi(-1)p.$$

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

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

Thus, by Theorem 3.22,

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

Replacing χ by χ^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,

$$R_1^2 + R_5^2 + R_7^2 + R_{11}^2 = 4a_{24}\, \text{Re}\{\bar{\psi}(2)\, G(\psi) + \psi(2)\, G(\psi^5)\} + 8\chi(-1)\, p. \tag{3.47}$$

By Lemmas 3.26 and 3.28,

$$R_1 R_5 = 2\, \text{Re}\{\delta K(\chi)\, G(\chi^6) + \beta\chi(-4)\, p^{1/2} G(\bar{\chi}^8)\}. \tag{3.48}$$

Since both σ_5 and σ_{11} fix $K(\chi^5)$ by Theorems 3.22 and 2.5(i), respectively, we have $K(\chi) = K(\chi^7)$. Thus, replacing χ by χ^7 in (3.48), we get

$$R_7R_{11} = 2\,\mathrm{Re}\{\delta K(\chi)\, G(\bar{\chi}^6) + \beta\chi(-4)\, p^{1/2}G(\bar{\chi}^8)\}, \tag{3.49}$$

since $\delta(\chi^7) = \overline{\delta(\chi)}$. By Lemmas 3.30 and 3.31,

$$R_1R_7 = 2\,\mathrm{Re}\{\beta\bar{\chi}(-4)\, K(\chi)\, G(\chi^8) + \delta p^{1/2}G(\chi^6)\}. \tag{3.50}$$

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

$$R_5R_{11} = 2\,\mathrm{Re}\{\beta\chi(-4)\, K(\chi)\, G(\bar{\chi}^8) + \delta p^{1/2}G(\chi^6)\}. \tag{3.51}$$

By Theorem 2.5(ii) and Lemma 3.29,

$$R_1R_{11} = 2\,\mathrm{Re}\{\chi(-1)\, p^{1/2}K(\chi) + \bar{\chi}(4)\, p^{1/2}G(\chi^2)\}. \tag{3.52}$$

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

$$R_5R_7 = 2\,\mathrm{Re}\{\chi(-1)\, p^{1/2}K(\chi) + \chi(4)\, p^{1/2}G(\chi^{10})\}. \tag{3.53}$$

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

$$\begin{aligned}(R_1 + R_5 + R_7 + R_{11})^2 &= (a_{24} + p^{1/2})\{4\,\mathrm{Re}\{\bar{\psi}(2)\, G(\psi) + \psi(2)\, G(\psi^5)\} \\ &\quad + 8\chi(-1)\, p^{1/2} + 8\beta\chi(-1)\,\mathrm{Re}\{\bar{\chi}(4)\, G(\chi^8)\} + 8\,\mathrm{Re}\{\delta G(\chi^6)\}\}.\end{aligned}$$

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, $p \equiv 1 \pmod{20}$, χ is a character (mod 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 $Q(\theta)$. Note that $G = \mathrm{Gal}(Q(\theta)/Q) = \{\sigma_t\colon t = \pm 1, \pm 3, \pm 7, \pm 9\}$.

LEMMA 3.33. *$K(\chi)/K(\chi^3)$ is a unit in $\mathcal{O}$.*

Proof. By Stickelberger's theorem [28, pp. 94, 97],

$$\mathcal{O}K(\chi) = \mathcal{O}G^2(\chi)/G(\chi^2) = \mathcal{O}G^2(\chi^3)/G(\chi^6) = \mathcal{O}K(\chi^3). \quad ∎$$

THEOREM 3.34. *If $5 \nmid a_4$, then there exist rational integers a_{20} and b_{20} such that*

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

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

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

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

Proof. Observe that $Q(i)$ is the fixed field of $\langle \sigma_{-3} \rangle = \langle \sigma_1, \sigma_{-3}, \sigma_9, \sigma_{-7} \rangle$. Since $K(\chi^9) = K(\chi)$ by Theorem 2.5(i), σ_{-3} fixes $K(\chi)/K(\chi^3)$. Thus $K(\chi)/K(\chi^3) \in Q(i)$. Therefore, by Lemma 3.33,

$$K(\chi) = \epsilon K(\chi^3) \tag{3.54}$$

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

$$a_4 + ib_4 = K(\chi^5) \equiv \epsilon K(\chi^{15}) = \epsilon(a_4 - ib_4) \pmod{5\Omega}. \tag{3.55}$$

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 σ_3 fixes $K(\chi)$, we deduce that $K(\chi) \in Q(i\sqrt{5})$. Hence,

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

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

$$a_4 + ib_4 = K(\chi^5) \equiv a_{20} \pmod{5\Omega}.$$

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 σ_3 fixes $iK(\chi)$, we have $iK(\chi) \in Q(i\sqrt{5})$, and thus

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

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

$$a_4 + ib_4 = K(\chi^5) \equiv ia_{20} \pmod{5\Omega}. \quad \blacksquare$$

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 χ have order 20. Then

$$K(\chi) = 1 + 2 \sum_{2 \leqslant n \leqslant (p-1)/2} \chi(4n(1-n)) \equiv 1 \pmod{2\Omega}. \tag{3.58}$$

Also, since $K(\chi^{11}) = K(\bar{\chi})$ by Theorem 2.5(i), we have

$$\begin{aligned} \operatorname{Re} K(\chi) &= \tfrac{1}{2}\{K(\chi) + K(\chi^{11})\} \\ &= \tfrac{1}{2} \sum_{n=2}^{p-1} \chi(4n(1-n))\{1 + \chi^{10}(4n(1-n))\} \\ &= \sum_{n \in S} \chi(4n(1-n)) \\ &= 1 + 2 \sum_{\substack{2 \leqslant n \leqslant (p-1)/2 \\ n \in S}} \chi(4n(1-n)) \\ &\equiv 1 \pmod{2\Omega}, \end{aligned}$$

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

$$\operatorname{Im} K(\chi) \in 2\Omega. \tag{3.59}$$

Now, $a^2 = a_4^2$, $b^2 = b_4^2$, $u^2 = a_{20}^2$, 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,

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

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

Proof. Let χ 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

$$\psi_3(a) = \left(\frac{a}{p}\right)\chi^2(a)\,K(\chi^2) + \left(\frac{a}{p}\right)\bar{\chi}^2(a)\,K(\bar{\chi}^2)$$

$$= 2\left(\frac{a}{p}\right)\mathrm{Re}\{\chi^2(a)(a_3 + ib_3\sqrt{3})\}, \tag{4.1}$$

and the desired results follow. ∎

THEOREM 4.2. *Let $p \equiv 1 \pmod 6$. Then in the notation of Theorem* 3.3,

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

where η_3 has the same designation as in Theorem 4.1.

Proof. Let χ 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

$$\varphi_3(a) = -1 + \chi(-1)\,\chi^4(a)\,K(\chi) + \chi(-1)\,\chi^2(a)\,K(\bar{\chi})$$

$$= -1 + \chi^4(a)\,K(\chi^2) + \overline{\chi^4(a)\,K(\chi^2)}.$$

The result now follows from (4.1). ∎

THEOREM 4.3. *Let $p \equiv 1 \pmod 6$. Then*

$$\psi_6(a) = \begin{cases} -1 + 2\left\{1 + \left(\frac{a}{p}\right)\right\}a_3, & \text{if } a \text{ is a cubic residue (mod } p), \\ -1 - \left(\frac{a}{p}\right)(a_3 + 3\eta_3 \mid b_3 \mid) - (a_3 - 3\eta_3 \mid b_3 \mid), & \text{otherwise,} \end{cases}$$

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

$$\eta_3 \equiv \begin{cases} \mid b_3 \mid \pmod 3, & \text{if } 2a \text{ is a cubic residue (mod } p), \\ -\mid b_3 \mid \pmod 3, & \text{if } 4a \text{ is a cubic residue (mod } p). \end{cases}$$

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*

$$\varphi_2(a) = \begin{cases} 2c_4, & \text{if } a \text{ is a quartic residue (mod } p), \\ -2c_4, & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod } p), \\ \pm 2 \mid d_4 \mid, & \text{otherwise.} \end{cases}$$

Proof. Let χ be a character (mod p) of order 4. Then

$$\varphi_2(a) = \bar{\chi}(-a)\, K(\chi) + \chi(-a)\, K(\bar{\chi}),$$

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*

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

Proof. By an elementary calculation [23, p. 82], $\psi_2(a) = -1$. 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*

$$\varphi_4(a) = \begin{cases} 4(-1)^{(p-1)/8}\, a_8, & \text{if } a \text{ is an octic residue (mod } p), \\ -4(-1)^{(p-1)/8}\, a_8, & \text{if } a \text{ is a quartic residue but an octic nonresidue (mod } p), \\ 0, & \text{if } a \text{ is a quadratic residue but a quartic nonresidue (mod } p), \\ \pm 4 \mid b_8 \mid, & \text{otherwise.} \end{cases}$$

Proof. Let χ be a character (mod p) of order 8. Then

$$\begin{aligned}\varphi_4(a) &= \bar{\chi}^3(-a)\,K(\chi) + \chi^3(-a)\,K(\bar{\chi}) + \bar{\chi}(-a)\,K(\chi^3) + \chi(-a)\,K(\bar{\chi}^3)\\ &= \{\bar{\chi}^3(-a) + \bar{\chi}(-a)\}\,K(\chi) + \{\chi^3(-a) + \chi(-a)\}\,K(\bar{\chi}),\end{aligned}$$

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* $p \equiv 1 \pmod 8$. *Then*

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

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 Whiteman [56, 57], Burde [6], and Morlaye [43]. Theorem 4.5 was apparently first stated by Chowla [11] and has also been observed by Whiteman [57], and by Singh and Rajwade [51]. Theorem 4.6 is due to Whiteman [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 $\varphi_n(a)$ 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* $p \equiv 1 \pmod{12}$. *If* $3 \mid a_4$, *we have*

$\varphi_6(a)$	quadratic	cubic	quartic
$-2c_4$	$\times$	$\times$	$\times$
$2c_4$	$\times$	$\times$	
$4c_4$	$\times$		$\times$
$-4c_4$	$\times$		
0			
$\pm 6 \mid d_4 \mid$		$\times$	

If $3 \nmid a_4$, *we have*

$\varphi_6(a)$	quadratic	cubic	quartic
$6c_4$	×	×	×
$-6c_4$	×	×	
0	×		×
0	×		
$\pm 4 \mid d_4 \mid$			
$\pm 2 \mid d_4 \mid$		×	

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

$$\varphi_6(a) = \psi^7(-a) \sum_{j=0}^{5} \psi^{2j}(a)\, K(\psi^{2j+1}),$$

by Theorem 2.7. By Theorem 2.5(i), $K(\psi) = K(\psi^5)$. Thus,

$$\begin{aligned}\varphi_6(a) &= \psi(-1)\,\psi^6(a)\{(\psi(a) + \psi^5(a))\, K(\psi) \\ &\quad + (\bar{\psi}(a) + \bar{\psi}^5(a))\, K(\bar{\psi}) + \psi^3(a)\, K(\psi^3) + \bar{\psi}^3(a)\, K(\bar{\psi}^3)\} \\ &= 2\psi(-1)\left(\frac{a}{p}\right) \operatorname{Re}\{(\psi(a) + \psi^5(a))\, K(\psi) + \psi^3(a)\, K(\psi^3)\}. \qquad (4.2)\end{aligned}$$

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

$$\varphi_6(a) = 2\psi(-1)\left(\frac{a}{p}\right) \operatorname{Re}\{h(a)(a_4 + ib_4)\}, \qquad (4.3)$$

where

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

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

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 $3 \nmid a_4$. Then by Theorem 3.19, (4.2) yields

$$\varphi_6(a) = 2\psi(-1)\left(\frac{a}{p}\right) \operatorname{Re}\{k(a)(a_4 + ib_4)\}, \qquad (4.5)$$

where

$$k(a) = \psi(a) + \psi^3(a) + \psi^5(a)$$
$$= \begin{cases} 3\psi(a), & \text{if } a \text{ is both a quadratic and a cubic residue (mod } p), \\ 0, & \text{if } a \text{ is a quadratic residue and a cubic nonresidue (mod } p) \\ \dfrac{i}{\operatorname{Im} \psi(a)}, & \text{if } a \text{ is a quadratic nonresidue (mod } p). \end{cases} \tag{4.6}$$

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

THEOREM 4.9. *Let* $p \equiv 1 \pmod{12}$. *If* $3 \mid a_4$, *we have the following table*:

$\psi_{12}(a)$	quadratic	cubic	quartic
$-1 + 4a_3 - 2c_4$	×	×	×
$-1 + 4a_3 + 2c_4$	×	×	
$-1 - 2a_3 + 4c_4$	×		×
$-1 - 2a_3 - 4c_4$	×		
$-1 \pm 6 \mid b_3 \mid$			
$-1 \pm 6 \mid d_4 \mid$		×	

If $3 \nmid a_4$, *we have the following table*:

$\psi_{12}(a)$	quadratic	cubic	quartic
$-1 + 4a_3 + 6c_4$	×	×	×
$-1 + 4a_3 - 6c_4$	×	×	
$-1 - 2a_3$	×		×
$-1 - 2a_3$	×		
$-1 \pm 6 \mid b_3 \mid \pm 4 \mid d_4 \mid$			
$-1 \pm 2 \mid d_4 \mid$		×	

Proof. The tables follow at once from Theorems 2.6, 4.3, and 4.8. ∎

THEOREM 4.10. *Let* $p = 24k + 1$. *Then we have the following table of values for* $(-1)^k \varphi_{12}(a)$:

$(-1)^k\ \varphi_{12}(a)$	quadratic	cubic	quartic	octic
$8a_{24} + 4a_8$	×	×	×	×
$-8a_{24} - 4a_8$	×	×	×	
$-4a_{24} + 4a_8$	×		×	×
$4a_{24} - 4a_8$	×		×	
0	×	×		
0	×			
$\pm 4 \mid b_8 \mid$		×		
$\pm 12 \mid b_{24} \mid \pm 4 \mid b_8 \mid$				

Proof. Let χ have order 24. Write $K(\chi) = a_{24} + ib_{24}\sqrt{6}$ as in Theorem 3.22 and write $K(\chi^3) = a_8 + ib_8\sqrt{2}$ as in Theorem 3.12. Now

$$\varphi_{12}(a) = \chi^{13}(-a) \sum_{j=0}^{11} \chi^{2j}(a)\, K(\chi^{2j+1}),$$

by Theorem 2.7. By Theorem 2.5(i) and Theorem 3.22, we know that $K(\chi) = K(\chi^5) = K(\chi^7) = K(\chi^{11})$. Also, by Theorem 2.5(i), $K(\chi^3) = K(\chi^9)$. Thus, the above becomes

$$\begin{aligned}\varphi_{12}(a) &= 2\chi(-1)\left(\frac{a}{p}\right) \mathrm{Re}(\{\chi(a) + \chi^5(a) + \chi^7(a) + \chi^{11}(a)\}\, K(\chi) \\ &\quad + \{\chi^3(a) + \chi^9(a)\}\, K(\chi^3)) \\ &= 2\chi(-1)\left(\frac{a}{p}\right) \mathrm{Re}(\chi(a)\{1 + \chi^4(a)\}\{1 + \chi^6(a)\}(a_{24} + ib_{24}\sqrt{6}) \\ &\quad + \chi^3(a)\{1 + \chi^6(a)\}(a_8 + ib_8\sqrt{2})).\end{aligned}$$

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 $\psi_{24}(a)$:*

$\psi_{24}(a)$	quadratic	cubic	quartic	octic
$-1 + 4a_3 - 2c_4 + (-1)^k\{8a_{24} + 4a_8\}$	×	×	×	×
$-1 + 4a_3 - 2c_4 - (-1)^k\{8a_{24} + 4a_8\}$	×	×	×	
$-1 - 2a_3 + 4c_4 - (-1)^k\{4a_{24} - 4a_8\}$	×		×	×
$-1 - 2a_3 + 4c_4 + (-1)^k\{4a_{24} - 4a_8\}$	×		×	
$-1 + 4a_3 + 2c_4$	×	×		
$-1 - 2a_3 - 4c_4$	×			
$-1 \pm 6 \mid d_4 \mid \pm 4 \mid b_8 \mid$		×		
$-1 \pm 6 \mid b_3 \mid \pm 12 \mid b_{24} \mid \pm 4 \mid b_8 \mid$				

If $3 \nmid a_4$, *we have the following table*:

$\psi_{24}(a)$	quadratic	cubic	quartic	octic
$-1 + 4a_3 + 6c_4 + (-1)^k\{8a_{24} + 4a_8\}$	×	×	×	×
$-1 + 4a_3 + 6c_4 - (-1)^k\{8a_{24} + 4a_8\}$	×	×	×	
$-1 - 2a_3 - (-1)^k\{4a_{24} - 4a_8\}$	×		×	×
$-1 - 2a_3 + (-1)^k\{4a_{24} - 4a_8\}$	×		×	
$-1 + 4a_3 - 6c_4$	×	×		
$-1 - 2a_3$	×			
$-1 \pm 2 \mid d_4 \mid \pm 4 \mid b_8 \mid$		×		
$-1 \pm 6 \mid b_3 \mid \pm 4 \mid d_4 \mid \pm 12 \mid b_{24} \mid \pm 4 \mid b_8 \mid$				

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*

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

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

$$\varphi_{12}(1) - \varphi_4(1) = 8(-1)^k a_{24}. \tag{4.7}$$

On the other hand, we have

$$\begin{aligned}\varphi_{12}(1) - \varphi_4(1) &= \sum_{n\neq 0}\left(\frac{n}{p}\right)\left\{\left(\frac{n^{12}+1}{p}\right) - \left(\frac{n^4+1}{p}\right)\right\} \\ &= \sum_{n\neq 0}\left(\frac{n+n^{-1}+2}{p}\right)\left\{\left(\frac{(n^3+n^{-3})^2-2}{p}\right) - \left(\frac{(n+n^{-1})^2-2}{p}\right)\right\} \\ &= \sum_m \left(\frac{m+2}{p}\right)\left\{\left(\frac{(m^3-3m)^2-2}{p}\right) - \left(\frac{m^2-2}{p}\right)\right\}\left\{1 + \left(\frac{4-m^2}{p}\right)\right\}.\end{aligned} \tag{4.8}$$

since the number of solutions n, $n \neq 0$, of the congruence $n + n^{-1} \equiv m$

(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 $(-1)^k \varphi_{10}(a)$:*

$(-1)^k \varphi_{10}(a)$	quadratic	quartic	quintic
$2a_4$	×	×	×
$-2a_4$	×		×
$\pm 2 \mid b_4 \mid \pm 8 \mid a_{20} \mid$			×
$2a_4 \pm 10 \mid b_{20} \mid$	×	×	
$-2a_4 \pm 10 \mid b_{20} \mid$	×		
$\pm 2 \mid b_4 \mid \pm 2 \mid a_{20} \mid$			

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

$(-1)^k \varphi_{10}(a)$	quadratic	quartic	quintic
$2a_4 + 8a_{20}$	×	×	×
$-2a_4 - 8a_{20}$	×		×
$\pm 2 \mid b_4 \mid$			×
$2a_4 - 2a_{20}$	×	×	
$-2a_4 + 2a_{20}$	×		
$\pm 2 \mid b_4 \mid \pm 10 \mid b_{20} \mid$			

Proof. Let χ 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

$$\begin{aligned}\varphi_{10}(a) &= \chi(-1) \sum_{j=0}^{9} \chi^{11+2j}(a)\, K(\chi^{2j+1}) \\ &= 2\chi(-1)\, \mathrm{Re}\{\chi^5(a)\, K(\bar{\chi}^5) + \chi^9(a)\, K(\bar{\chi}) \\ &\quad + \chi^7(a)\, K(\bar{\chi}^3) + \chi^3(a)\, K(\bar{\chi}^3) + \chi(a)\, K(\bar{\chi})\}. \qquad (4.9)\end{aligned}$$

Suppose first that $5 \mid a_4$. Then from the proof of Theorem 3.34, $K(\chi) = -K(\chi^3)$. Hence, by (4.9),

$$\chi(-1)\,\varphi_{10}(a) = 2\,\mathrm{Re}\{\chi^5(a)(a_4 - ib_4) + \chi(a)\{1 - \chi^2(a)\}\{1 - \chi^6(a)\}(-ia_{20} - b_{20}\sqrt{5})\}.$$

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),

$$\chi(-1)\,\varphi_{10}(a) = 2\,\mathrm{Re}\{\chi^5(a)(a_4 - ib_4) + \chi(a)\{1 + \chi^2(a)\}\{1 + \chi^6(a)\}(a_{20} - ib_{20}\sqrt{5})\}.$$

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 λ, every nonzero element of G can be written as a difference of two elements of H in exactly λ ways [40, p. 64]. 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 kth 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

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

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

$$|S_k|^2 = (p-1)/k + \lambda \sum_{n \neq 0} e^{2\pi i n/p} = (p-1)/k - \lambda,$$

where λ satisfies

$$(p-1)/k + \lambda(p-1) = \{(p-1)/k\}^2.$$

Hence, $\lambda = (p-1-k)/k^2$,

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

Conversely, suppose that (5.1) holds. Multiplying, expanding, and collecting terms in the product $S_k\bar{S}_k$, we see that there exist rational numbers a_n, $0 \leqslant n \leqslant p-1$, such that

$$\sum_{n=0}^{p-1} a_n e^{2\pi i n/p} = 0.$$

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, $0 \leqslant n \leqslant p-1$, 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 λ 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

$$|G_k + k - 1|^2 = (p+k-1)(k-1). \tag{5.2}$$

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,

$$G_4 = p^{1/2} \pm i(2p + 2a_4 p^{1/2})^{1/2}, \tag{5.3}$$

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 α and β 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 $p^{-1}G_3^4 = 3G_3^2 + r_3G_3$ by Theorem 3.6, we obtain the simplification

$$2G_3^2 + (2\alpha + r_3)\,G_3 + (p + \alpha^2 - \beta) = 0,$$

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,

$$(G_3 + \alpha)^2 + \frac{1}{4p}(4p - G_3^2 + \epsilon_6 G_3\{12p - 3G_3^2\}^{1/2})^2 = \beta.$$

After expanding and eliminating the terms involving G_3^3 and G_3^4, we obtain the simplification

$$G_3^2 + (4\alpha - r_3)\,G_3 - 2p = \epsilon_6(r_3 - G_3)(12p - 3G_3^2)^{1/2}.$$

After squaring both sides and eliminating the terms involving G_3^3 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,

$$G_8 = p^{1/2} + R_6 \pm i\{(a_8 + p^{1/2})(4p^{1/2} - 2\eta R_6)\}^{1/2}, \tag{5.4}$$

where $R_6 = \pm(2p + 2a_4p^{1/2})^{1/2}$, $a_4^2 + b_4^2 = a_8^2 + 2b_8^2 = p$, and a_4, $a_8 \equiv -1 \pmod 4$.

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),

$$G_8 = p^{1/2} + R_6 \pm i\{(1 - p^{1/2})(2R_6 - 4p^{1/2})\}^{1/2},$$

where $R_6 = \pm(2p + 6p^{1/2})^{1/2}$. 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),

$$\begin{aligned} 7p + 1 = |G_8 - 1|^2 &= 7p + 1 + p^{1/2}(4a_8 + 2a_4 - 2) \\ &\quad + 2R_6(p^{1/2} - \eta p^{1/2} - 1 - \eta a_8). \end{aligned}$$

The coefficient of R_6 must vanish, since $R_6 \notin Q(p^{1/2})$. 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. ∎

THEOREM 5.7. *Let $p \equiv 1 \pmod{12}$. 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 $p \equiv 1 \pmod{24}$, the result follows from Theorem 5.2. Thus, suppose that $p \equiv 13 \pmod{24}$. Assume that H_{12} or $H_{12} \cup \{0\}$ is a difference set. Then $|G_{12} + \alpha|^2 = \beta$, where α and β 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

$$\begin{aligned} G_{12} &= G_3 + p^{-1/2}(G_3^2 - p) \\ &\quad \pm i\{(2p + 2a_4p^{1/2})^{1/2} \pm p^{-1/2}G_3(2p + 2a_{12}p^{1/2})^{1/2}\}, \end{aligned}$$

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

$$G_{12} = G_3 + p^{-1/2}(G_3^2 - p) \pm iV(2p + 2a_4p^{1/2})^{1/2},$$

where

$$V = \begin{cases} 1 \pm p^{-1/2}G_3, & \text{if } 3 \nmid a_4, \\ 1 \pm (pb_4)^{-1}G_3(p - a_4p^{1/2}), & \text{if } 3 \mid a_4. \end{cases}$$

Therefore,

$$\beta = |G_{12} + \alpha|^2 = (G_3 + p^{-1/2}G_3^2 + \alpha - p^{1/2})^2 + 2V^2(p + a_4p^{1/2}). \tag{5.5}$$

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 $\alpha^2 - \beta = -11p$, $-8p + 2p^{1/2}(a_4 - \alpha + r_3) = 0$, 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

1. P. Barrucand and H. Cohn, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, *J. Reine Angew. Math.* **238** (1969), 67–70.
2. L. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics No. 182, Springer–Verlag, Berlin, 1971.
3. B. C. Berndt, Periodic Bernoulli numbers, summation formulas and applications, *in* "Theory and Application of Special Functions" (Richard A. Askey, Ed.), Academic Press, New York, 1975.
4. B. C. Berndt and S. Chowla, The reckoning of certain quartic and octic Gauss sums, *Glasgow Math. J.* **18** (1977), 153–155.
5. B. C. Berndt and R. J. Evans, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer, *Illinois J. Math.*, in press.
6. K. Burde, Über allgemeine Sequenzen der Länge 3 von Legendresymbolen, *J. Reine Angew. Math.* **272** (1975), 203–216.
7. J. W. S. Cassels, On Kummer sums, *Proc. London Math. Soc.* (3) **21** (1970), 19–27.
8. J. W. S. Cassels, Trigonometric sums and elliptic functions, *in* "Algebraic Number Theory" (S. Iyanaga, Ed.), pp. 1–7, Japan Society for the Promotion of Science, Tokyo, 1977.
9. S. Chowla, A property of biquadratic residues, *Proc. Nat. Acad. Sci. India Sect. A* **14** (1944), 45–46.
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).
11. S. Chowla, The last entry in Gauss's diary, *Proc. Nat. Acad. Sci. USA* **35** (1949), 244–246.

12. S. CHOWLA, "The Riemann Hypothesis and Hilbert's Tenth Problem," Gordon & Breach, New York, 1965.
13. H. DAVENPORT, "The Higher Arithmetic," Hutchinson, London, 1952.
14. H. DAVENPORT AND H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. Reine Angew. Math.* **172** (1934), 151–182.
15. L. E. DICKSON, Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.* **57** (1935), 391–424.
16. L. E. DICKSON, Cyclotomy and trinomial congruences, *Trans. Amer. Math. Soc.* **37** (1935), 363–380.
17. L. E. DICKSON, Cyclotomy when e is composite, *Trans. Amer. Math. Soc.* **38** (1935), 187–200.
18. R. J. EVANS, Bioctic Gauss sums and sixteenth power residue difference sets, *Acta Arith.*, in press.
19. R. J. EVANS, Resolution of sign ambiguities in Jacobi and Jacobsthal sums, *Pacific J. Math.*, in press.
20. R. J. EVANS, Unambiguous evaluations of bidecic Jacobi and Jacobsthal sums, *J. Australian Math. Soc.*, in press.
21. R. J. EVANS, The cyclotomic numbers of order twenty-four with applications to difference sets, in preparation.
22. R. FRICKE, "Lehrbuch der Algebra," Band I, Vieweg, Braunschweig, 1924.
23. E. GROSSWALD, "The Theory of Numbers," Macmillan Co., New York, 1966.
24. H. HASSE, "Vorlesungen über Zahlentheorie," zweite Auflage, Springer–Verlag, Berlin, 1964.
25. K. IRELAND AND M. I. ROSEN, "Elements of Number Theory," Bogden & Quigley, Tarrytown-on-Hudson, 1972.
26. E. JACOBSTHAL, Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate, *J. Reine Angew. Math.* **132** (1907), 238–245.
27. E. LANDAU, "Elementary Number Theory," 2nd ed., Chelsea, New York, 1958.
28. S. LANG, "Algebraic Number Theory," Addison–Wesley, Reading, Mass., 1970.
29. E. LEHMER, The quintic character of 2 and 3, *Duke Math. J.* **18** (1951), 11–18.
30. E. LEHMER, On residue difference sets, *Canad. J. Math.* **5** (1953), 425–432.
31. E. LEHMER, On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$, *Pacific J. Math.* **5** (1955), 103–118.
32. E. LEHMER, Problem 4636 with solution by L. Carlitz, *Amer. Math. Monthly* **63** (1956), 584–587.
33. E. LEHMER, On the location of Gauss sums, *Math. Tables Aids to Comput.* **10** (1956), 194–202.
34. E. LEHMER, On Euler's criterion, *J. Austral. Math. Soc.* **1** (1959), 64–70.
35. E. LEHMER, On Jacobi functions, *Pacific J. Math.* **10** (1960), 887–893.
36. E. LEHMER, On the quadratic character of the Fibonacci root, *Fibonacci Quart.* **4** (1966), 135–138.
37. E. LEHMER, On some special quartic reciprocity laws, *Acta Arith.* **21** (1972), 367–377.
38. P. A. LEONARD AND K. S. WILLIAMS, Jacobi sums and a theorem of Brewer, *Rocky Mountain J. Math.* **5** (1975), 301–308; Erratum, *Rocky Mountain J. Math.* **6** (1976), 509.
39. J. H. LOXTON, Some conjectures concerning Gauss sums, *J. Reine Angew. Math.* **297** (1978), 153–158.
40. H. B. MANN, "Addition Theorems," Wiley, New York, 1965.
41. A. D. MCGETTRICK, A result in the theory of Weierstrass elliptic functions, *Proc. London Math. Soc.* (3) **25** (1972), 41–54.
42. A. D. MCGETTRICK, On the biquadratic Gauss sum, *Proc. Cambridge Philos. Soc.* **71** (1972), 79–83.

43. B. MORLAYE, Démonstration élémentaire d'un théorème de Davenport et Hasse, *Enseignement Math.* **18** (1972), 269–276.
44. J. B. MUSKAT, The cyclotomic numbers of order fourteen, *Acta Arith.* **11** (1966), 263–279.
45. J. B. MUSKAT, On Jacobi sums of certain composite orders, *Trans. Amer. Math. Soc.* **134** (1968), 483–502.
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 Arith.* **19** (1970), 185–216.
48. T. NAGELL, "Introduction to Number Theory," 2nd ed., Chelsea, New York, 1964.
49. A. R. RAJWADE, On rational primes p congruent to 1 (mod 3 or 5), *Proc. Cambridge Philos. Soc.* **66** (1969), 61–70.
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 $y^2 \equiv x^4 - a \pmod{p}$, *Enseignement Math.* **20** (1974), 265–273.
52. H. J. S. SMITH, "Report on the Theory of Numbers," Chelsea, New York, 1965.
53. T. STORER, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.
54. A. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent, *Actualités Sci. Ind.*, No. 1041; *Publ. Inst. Math. Univ. Strasbourg* **7** (1945); Hermann, Paris, 1948.
55. A. E. WESTERN, Some criteria for the residues of eighth and other powers, *Proc. 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.
57. A. L. WHITEMAN, Cyclotomy and Jacobsthal sums, *Amer. J. Math.* **74** (1952), 89–99.
58. A. L. WHITEMAN, The sixteenth power residue character of 2, *Canad. J. Math.* **6** (1954), 364–373.
59. A. L. WHITEMAN, The cyclotomic numbers of order sixteen, *Trans. Amer. Math. Soc.* **86** (1957), 401–413.
60. A. L. WHITEMAN, The cyclotomic numbers of order twelve, *Acta Arith.* **6** (1960), 53–76.
61. A. L. WHITEMAN, The cylotomic numbers of order ten, Proc. Sym. Appl. Math., Vol. 10, pp. 95–111, Amer. Math. Soc., Providence, R. I., 1960.
62. K. S. WILLIAMS, Note on a cubic character sum, *Aequationes Math.* **12** (1975), 229–231.
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.