JACOBI SUMS AND A THEOREM OF BREWER

PHILIP A. LEONARD AND KENNETH S. WILLIAMS*

1. Introduction. Throughout \( p \) will denote an odd prime, and \((\cdot/p)\) the familiar Legendre symbol. It is well known that \( p = c^2 + 2d^2 \) if and only if \( p = 8k + 1 \) or \( p = 8k + 3 \), and that in these cases \( c \) is unique if we require \( c \equiv (-1)^{k+1} \pmod{4} \). In 1961, Brewer [1] related this representation of \( p \) to the character sum

\[
B = \sum_{x=0}^{n-1} \left( \frac{(x + 2)(x^2 - 2)}{p} \right).
\]

More precisely, he proved

**Theorem.**

\[
B = \begin{cases} 
0, & \text{if } p \neq c^2 + 2d^2, \\
2c, & \text{if } p = c^2 + 2d^2 \text{ and } c \equiv (-1)^{k+1} \pmod{4}.
\end{cases}
\]

We present a variant of Whiteman's proof [6] of this result, using simple properties of Jacobi sums, with the view that this is more natural than the use of Jacobsthal sums [6], modular curves [5] (see Theorem 1) or the theory of cyclotomy [3] in other existing proofs.

For multiplicative characters \( \psi \) and \( \lambda \) of \( \text{GF}(p^r) \), the Jacobi sum \( J(\psi, \lambda) \) is defined by

\[
J(\psi, \lambda) = \sum_{\alpha + \beta = 1} \psi(\alpha)\lambda(\beta).
\]

If \( \psi, \lambda \) and \( \psi\lambda \) are non-trivial, these sums satisfy [4]

\[
J(\psi, \lambda) = \frac{G(\psi)G(\lambda)}{G(\psi\lambda)},
\]

where \( G(\psi) \) is the Gaussian sum \( G(\psi) = \sum_{\alpha} \psi(\alpha) \exp(2\pi i \text{tr}(\alpha)/p) \), with \( \text{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}} \), and therefore as \( |G(\psi)| = p^{r/2} \),

\[
|J(\psi, \lambda)|^2 = p^r.
\]

Received by the editors June 24, 1973.

*The research of both authors was supported by the National Research Council of Canada under grant A-7233.
The Gaussian sums also satisfy

\[(1.5)\quad G(\psi)G(\bar{\psi}) = \psi(-1)p',\]

where \(\bar{\psi}\) is the character conjugate to \(\psi\). The particular Jacobi sums of interest will be studied in § 4.

It is convenient to introduce \(\theta\), an element of \(GF(p^2)\) of multiplicative order \(p + 1\), and the notation \(\overline{\theta} = \theta^p\), so that \(\theta \overline{\theta} = 1\). (Similarly, the integers \(x, \bar{x}\) among \(1, 2, \cdots p - 1\) are related by \(x\bar{x} \equiv 1 \pmod{p}\)). We note the relation

\[(1.6)\quad (\theta^n + 1)^{p-1} = \theta^{np}\quad \text{for } 1 \leq n \leq p + 1, \quad n \not\equiv (p + 1)/2,\]

which follows from \((\theta^n + 1)^p = \theta^{np} + \theta^{n(p+1)} = \theta^{np}(\theta^n + 1)\).

2. Transformation formulae. The following result contains two simple formulae which are useful in the argument.

**Lemma 2.1.** Let \(F\) be a complex-valued function of period \(p\). Then

\[(2.1)\quad \sum_{x=0}^{p-1} \left( \frac{x + 2}{p} \right) F(x) + \sum_{x=0}^{p-1} \left( \frac{x - 2}{p} \right) F(x) = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) F(x + \bar{x}),\]

and

\[(2.2)\quad \sum_{x=0}^{p-1} \left( \frac{x + 2}{p} \right) F(x) - \sum_{x=0}^{p-1} \left( \frac{x - 2}{p} \right) F(x) = \sum_{n=1}^{p+1} (-1)^n F(\theta^n + \bar{\theta}^n).\]

**Proof.** For (2.1), see [7]. The observation of Brewer [1] and Whiteman [6] that the number of solutions of \(x = \theta^n + \bar{\theta}^n, 1 \leq n \leq p + 1\), is \(1 - ((x^2 - 4)/p)\), gives

\[(2.3)\quad \sum_{x=0}^{p-1} G(x) - \sum_{x=0}^{p-1} \left( \frac{x^2 - 4}{p} \right) G(x) = \sum_{n=1}^{p+1} G(\theta^n + \bar{\theta}^n),\]

for any complex-valued function \(G\) of period \(p\). Setting \(G(x) = ((x + 2)/p)F(x)\), we obtain (2.2) as \(((\theta^n + \bar{\theta}^n + 2)/p) = (-1)^n, 1 \leq n \leq p + 1, n \not\equiv (p + 1)/2\). This assertion follows from (1.6) and Euler's criterion, since

\[\left( \theta^n + \bar{\theta}^n + 2 \right)^{(p-1)/2} = \left( \left( \theta^n + 1 \right)^2 \bar{\theta}^n \right)^{(p-1)/2} \]

\[= \theta^{np} \bar{\theta}^{n(p-1)/2} = \theta^n (p+1)^{1/2} = (-1)^n\]
for the indicated values of $n$.

3. Applications; the trivial cases. We apply Lemma 2.1 to $F(x) = ((x^2 - 2)/p)$. For $p \equiv 1 \pmod{4}$, (2.1) gives

$$2B = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) \left( \frac{(x + \bar{x})^2 - 2}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^4 + 1}{p} \right)$$

(3.1)

$$= \sum_{x=0}^{p-1} \left( \frac{x^8 + 1}{p} \right) - \sum_{x=0}^{p-1} \left( \frac{x^4 + 1}{p} \right).$$

If $p \equiv 5 \pmod{8}$, the biquadratic and octic residues modulo $p$ coincide, so that $B = 0$ in this case.

For $p \equiv 3 \pmod{4}$, (2.2) gives

$$2B = \sum_{n=1}^{p+1} (-1)^n \left( \frac{\theta^{2n} + \bar{\theta}^{2n}}{p} \right)$$

(3.2)

$$= \sum_{n=1}^{p+1} \left( \frac{\theta^{4n} + \bar{\theta}^{4n}}{p} \right) - \sum_{n=1}^{p+1} \left( \frac{\theta^{2n} + \bar{\theta}^{2n}}{p} \right).$$

As $\theta^{(p+1)/2} = -1$ and $(-1/p) = -1$, the transformation $n \rightarrow (p + 1)/4 + n$ shows that the second term in (3.2) is its own negative, and so $2B = \sum_{n=1}^{p+1} ((\theta^{4n} + \bar{\theta}^{4n})/p)$ in this case. If $p \equiv 7 \pmod{8}$, the transformation $n \rightarrow (p + 1)/8 + n$ applied to (3.3) shows that $2B = -2B$, so that $B = 0$ in this case as well.

4. The Jacobi sums. For $p \equiv 1 \pmod{8}$ and $p \equiv 3 \pmod{8}$, some special Jacobi sums are needed. First, let $D$ denote the ring of integers of the number field $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\omega)$, where $\omega = \exp(2\pi i/8)$. $D$ is a unique factorization domain. If $\pi$ denotes a prime factor of $p$ in $D$, then $k = D/(\pi)$ is a field of $N(\pi)$ elements, where

$$N(\pi) = \begin{cases} p & \text{if } p \equiv 1 \pmod{8}, \\ p^2 & \text{if } p \equiv 3 \pmod{8}. \end{cases}$$

(4.1)

We define a character $\chi = \chi_\pi$ of $k$ by specifying

$$\chi(\xi) = \omega^\xi \quad \text{if } \xi^{N(\pi)-1}/8 \equiv \omega^\xi \pmod{\pi},$$

(4.2)

for elements $\xi$ of $D$ not divisible by $\pi$. The function $\chi$ defined by (4.2) is related to the Legendre symbol by

$$\left( \frac{a}{p} \right) = \begin{cases} \chi^4(a) & \text{if } p \equiv 1 \pmod{8}, \\ \chi(a) & \text{if } p \equiv 3 \pmod{8}, \end{cases} \text{for all } a \in \mathbb{Z}.$$  

(4.3)

When $p \equiv 3 \pmod{8}$ we have

$$\theta^{(p^3 - 1)/8} = (\theta^{(p + 1)/4})^{(p - 1)/2} = (\pm i)^{(p - 1)/2} = \pm i,$$

so that $\chi(\theta) = \pm i$. 
Replacing $\theta$ by $-\theta$ if necessary we can assume without loss of generality that $\chi(\theta) = i$.

Since our Gauss and Jacobi sums involve only characters which are powers of $\chi$, we set $J(m, n) = J(\chi^m, \chi^n)$ and $G(m) = G(\chi^m)$ to simplify notation. Also, $\bar{\alpha}$ and $\alpha'$ denote the conjugates of $\alpha$ in $D$ with respect to $i$ and $\sqrt{2}$, respectively. Thus $\bar{\omega}' = \omega^3$, for example.

For $p = 8k + 1$, the central role is played by the Jacobi sum $J(1, 4)$.

**Lemma 4.1.** For $p = 8k + 1$, $J(1, 4) = \pm \pi \bar{\pi}'$.

**Proof.** As $\sum_{y=0}^{p-1} y^n \equiv 0 \pmod{p}$ wherever $p - 1 \nmid n$, we have

\begin{equation}
J(1, 4) \equiv \sum_{y=0}^{p-1} y^{p-1/8}(1 - y)^{(p-1)/2} \equiv 0 \pmod{\pi} \text{ in } D.
\end{equation}

Since $y^{(p-1)/8} \equiv \omega^x \pmod{\pi}$ implies $y^{3(p-1)/8} \equiv \omega^x \pmod{\pi}$, we have

\begin{equation}
J(1, 4) \equiv \sum_{y=0}^{p-1} y^{3(p-1)/8}(1 - y)^{(p-1)/2} \equiv 0 \pmod{\pi'} \text{ in } D.
\end{equation}

As $\pi$ and $\pi'$ are non-associated primes of $D$, (4.4) and (4.5) imply

\begin{equation}
J(1, 4) = \gamma \pi \bar{\pi}', \text{ for some } \gamma \in D.
\end{equation}

Now by (1.3) and (1.5), $J(1, 4) = J(3, 4) = G(3)G(4)/G(7) = G(1)G(4)/G(5) = J(1, 4)$ showing that $J(1, 4)$ is in $Z[\sqrt{-2}]$. Since $\pi \bar{\pi}'$ is in $Z[\sqrt{-2}]$, $\gamma$ is in $Z[\sqrt{-2}]$ as well. Computing norms in (4.6) gives, by (1.4), that $\gamma$ is a unit of $Z[\sqrt{-2}]$, so $\gamma = \pm 1$ as required.

**Lemma 4.2.** For $p = 8k + 1$, $J(1, 4) = c + d \sqrt{-2}$, where $c \equiv (-1)^{k+1} \pmod{4}$ and $p = c^2 + 2d^2$.

**Proof.** By lemma 4.1 and its proof, $J(1, 4)$ is a prime factor of $p$ in $Z[\sqrt{-2}]$. Thus, since we do not distinguish $d$ from $-d$, $J(1, 4) = \pm (c + d \sqrt{-2})$, with $d$ even and $c \equiv (-1)^{k+1} \pmod{4}$. The correct sign is obtained by using an idea of Davenport and Hasse [2]. For $1 \leq y \leq p - 2$, $((y + 1)/p) + 1 \equiv 0 \pmod{2}$, and

\begin{equation}
\chi(y) = \begin{cases} 
1, & \text{if } \left( \frac{y}{p} \right) = 1, \\
\omega, & \text{if } \left( \frac{y}{p} \right) = -1 
\end{cases} \pmod{\sqrt{-2}},
\end{equation}

so that
After some simplification of (4.7) we obtain

\[ \sum_{v=1}^{p-2} \{ \chi(y) - 1 \} \left\{ \left( \frac{y + 1}{p} \right) + 1 \right\} \]

\[ \left( \frac{y}{p} \right) = 1 \]

(4.7)

\[ + \sum_{v=1}^{p-2} \{ \chi(y) - \omega \} \left\{ \left( \frac{y + 1}{p} \right) + 1 \right\} \equiv 0 (\text{mod } 2\sqrt{2}). \]

\[ \left( \frac{y}{p} \right) = -1 \]

As \( d \) is even, we have

\[ J(1, 4) = \frac{1}{2} (p - 5) + \frac{\omega}{2} (p - 1) + \chi(-1) (\text{mod } 2\sqrt{2}), \]

or

(4.8) \[ J(1, 4) \equiv (-1)^k - 2 \equiv (-1)^{k+1} \equiv c (\text{mod } 2\sqrt{2}). \]

For \( p = 8k + 3 \), the central role is played by a factor of the Jacobi sum \( J(1, 3) \). Following Whiteman, we consider the Eisenstein sum

\[ (4.9) \quad K = \sum_{b=0}^{p-1} \chi(1 + bi), \]

which satisfies (see [6], lemma 2)

(4.10) \[ K \bar{K} = p, \]

and also (as can be shown by a straightforward calculation)

(4.11) \[ J(1, 3) = -K^2, \]

showing that \( K \) is indeed a factor of the Jacobi sum \( J(1, 3) \).

**Lemma 4.3.** For \( p = 8k + 3 \), let \( L = \sum_{n=1}^{p+1} \chi(\theta^n + 1) \). Then \( L \) is in \( Z[\sqrt{-2}] \), and \( -\bar{L} = K \).

**Proof.**

\[ L' = \sum_{n=1}^{p+1} [\chi(\theta^n + 1)]^3 = \sum_{n=1}^{p+1} [\chi(\theta^n + 1)]^p \]

\[ = \sum_{n=1}^{p+1} \chi(\theta^{np} + 1) = \sum_{n=1}^{p+1} \chi(\theta^n + 1) = L, \]
so that $L$ is in $\mathbb{Z}\sqrt{-2}$. For $0 \leq b \leq p - 1$, the numbers $(1 - bi)/(1 + bi)$ are distinct, and different from $-1$. As $((1 - bi)/(1 + bi))^p = (1 + bi)/(1 - bi)$, each of them satisfies $y^{p+1} = 1$, and so these $p$ elements of $\text{GF}(p^2)$ are simply $\theta^n$, $1 \leq n \leq p + 1$, $n \neq (p + 1)/2$. Therefore

\[
\left\{ \theta^n + 1 \mid 1 \leq n \leq p + 1, n \neq \frac{p+1}{2} \right\}
= \left\{ \frac{2}{1 + bi} \mid 0 \leq b \leq p + 1 \right\},
\]

so that

\[
K = \sum_{b=0}^{p-1} x(1 + bi) = \sum_n' x \left( \frac{2}{\theta^n + 1} \right)
= - \sum_n' \tilde{x}(\theta^n + 1) = -L,
\]

as required, where the dash ('') indicates that the summation is over those $n$ satisfying $1 \leq n \leq p + 1$, $n \neq (p + 1)/2$.

**Lemma 4.4.** For $p = 8k + 3 = c^2 + 2d^2$, with $c \equiv (-1)^{k+1}(\text{mod } 4)$, we have $L = \pm (c + d\sqrt{-2})$. (The ambiguity of sign is resolved in § 5).

**Proof.** From (4.10) and lemma 4.3 we have $p = L\bar{L} = n\pi$, so that $L = \pm \pi$ or $\pm \bar{n}$, showing that $L$ can be written in the form $\pm(c + d\sqrt{-2})$ with $c \equiv (-1)^{k+1}(\text{mod } 4)$ and $c^2 + 2d^2 = p$.

5. Completion of the proof. For $p = 8k + 1$, we have

\[
\sum_{x=0}^{p-1} \left( \frac{x^8 + 1}{p} \right)
= \sum_{x=0}^{p-1} \left( \frac{x + 1}{p} \right)\{1 + x(x) + x^2(x) + \cdots + x^7(x)\},
\]

and

\[
\sum_{x=0}^{p-1} \left( \frac{x^4 + 1}{p} \right)
= \sum_{x=0}^{p-1} \left( \frac{x + 1}{p} \right)\{1 + x^2(x) + x^4(x) + x^6(x)\},
\]

where $x$ is any element of $\text{GF}(p^2)$.
which, with (3.1) gives

\[(5.3) \quad 2B = J(1, 4) + \overline{J(1, 4)}' + J(1, 4)' + \overline{J(1, 4)}.
\]

From lemma 4.2, \(2B = 4c\), so that \(B = 2c\) as required.

For \(p = 8k + 3\), we rewrite (3.3) by introducing \(\chi\), and obtain

\[(5.4) \quad 2B = \sum_{n=1}^{p+1} \chi(\theta^{8n} + 1) = \sum_{n=1}^{p+1} \chi(\theta^{4n} + 1),
\]

as \(p + 1 = 4(2k + 1)\) implies that the fourth powers and eighth powers in the cyclic group \(<\theta>\) coincide. Setting

\[S_j = \sum_{n=1}^{p+1} \chi(\theta^{4n+j} + 1), \quad \text{for } j = 0, 1, 2, 3,
\]

we have the equalities

\[(5.5) \quad 4L = S_0 + S_1 + S_2 + S_3 = \pm 4(c + d\sqrt{-2}).
\]

Now (see [6], p. 551) \(S_1 = iS_3\) and \(S_2 = 0\), giving

\[(5.6) \quad \pm 4(c + d\sqrt{-2}) = 2B + (1 + i)S_3.
\]

From (1.6) we obtain, for \(p = 8k + 3\), as \(\chi(\theta) = i\), \(\chi^2(\theta^m + 1) = \{\chi(\theta^m + 1)\}^{p-1} = \chi(\theta^{mp}) = \{\chi(\theta^m)\}^3 = \omega^{6m}\), so that

\[(5.7) \quad \chi(\theta^m + 1) = \pm \omega^{3m}.
\]

Hence \(\chi(\theta^{4n+3} + 1) = \pm \omega\), so that \(S_3 = e\omega\), where \(e \in \mathbb{Z}\), giving

\[(5.8) \quad (1 + i)S_3 = e\sqrt{-2}.
\]

From (5.5), (5.6) and (5.8) we have \(B/2 = S_0/4 = \pm c\). But

\[S_0/4 = \frac{1}{4} \sum_{n=1}^{p+1} \chi(\theta^{4n} + 1) = \sum_{n=1}^{2k+1} \chi(\theta^{4n} + 1)
\]

\[= \sum_{n=1}^{2k} \chi(\theta^{4n} + 1) - 1,
\]

and

\[\sum_{n=k+1}^{2k} \chi(\theta^{4n} + 1) = \sum_{m=1}^{k} \chi(\theta^{-4m} + 1) = \sum_{m=1}^{k} \chi(\theta^{4m} + 1).
\]
Since (from (5.7)) $X(\theta^4 + 1) = \pm 1$, we have

$$\frac{B}{2} = 2 \sum_{m=1}^{k} X(\theta^4 + 1) - 1 \equiv 2k - 1 \equiv (-1)^k + 1 \equiv c \pmod{4}.$$ 

Since $c$ is odd and $B/2 = \pm c$, we must have $B/2 = c$. This completes the proof.

References


Arizona State University, Tempe, Arizona 85281
Carleton University, Ottawa, Ontario, Canada

Rocky Mountain J. Math. 6 (1976), 509.

ERRATUM, VOLUME 5


In the statement and proof of Lemma 4.2, the factor $X(-1)$ should appear with each occurrence of $J(1, 4)$.

The right-hand side of (5.3) should also contain the factor $X(-1)$.

In the line following (4.6), for $J(1, 4)$ read $J(1, 4)'$.

We are grateful to Professors B. Berndt and R. Evans for pointing out the omission of $X(-1)$. 