ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 5, Number 2, Spring 1975

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 $c \equiv (-1)^{k+1} (\mathrm{mod}\, 4)$. In 1961, Brewer [1] related this representation of p to the character sum

$$(1.1) \qquad B = \sum_{x=0}^{p-1} \left(\frac{(x+2)(x^2-2)}{p} \right).$$

More precisely, he proved

THEOREM.

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

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 ψ and λ of $GF(p^r)$, the Jacobi sum $J(\psi, \lambda)$ is defined by

$$(1.2) \qquad J(\psi, \lambda) = \sum_{\alpha+\beta=1} \psi(\alpha)\lambda(\beta).$$

If ψ, λ and $\psi\lambda$ are non-trivial, these sums satisfy [4]

$$(1.3) \qquad J(\psi, \lambda) = \frac{G(\psi)G(\lambda)}{G(\psi\lambda)},$$

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

$$(1.4) \qquad |J(\psi, \lambda)|^2 = p^r.$$

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

$$G(\psi)G(\bar{\psi}) = \psi(-1)p^r, \tag{1.5}$$

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

It is convenient to introduce θ, an element of $\mathrm{GF}(p^2)$ of multiplicative order $p + 1$, and the notation $\bar{\theta} = \theta^p$, so that $\theta\bar{\theta} = 1$. (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

$$(\theta^n + 1)^{p-1} = \theta^{np} \text{ for } 1 \leqq n \leqq p + 1, n \neq (p + 1)/2, \tag{1.6}$$

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*

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

and

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

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

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

for any complex-valued function G of period p. Setting $G(x) = ((x + 2)/p)F(x)$, we obtain (2.2) as $((\theta^n + \bar{\theta}^n + 2)/p) = (-1)^n$, $1 \leqq n \leqq p + 1$, $n \neq (p + 1)/2$. This assertion follows from (1.6) and Euler's criterion, since

$$\begin{aligned}(\theta^n + \bar{\theta}^n + 2)^{(p-1)/2} &= ((\theta^n + 1)^2 \bar{\theta}^n)^{(p-1)/2} \\ &= \theta^{np} \bar{\theta}^{n(p-1)/2} = \theta^{n(p+1)/2} = (-1)^n\end{aligned}$$

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

$$
\begin{aligned}
2B &= \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{(x+\bar{x})^2-2}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x^4+1}{p}\right) \\
&= \sum_{x=0}^{p-1}\left(\frac{x^8+1}{p}\right) - \sum_{x=0}^{p-1}\left(\frac{x^4+1}{p}\right).
\end{aligned} \tag{3.1}
$$

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

$$
\begin{aligned}
2B &= \sum_{n=1}^{p+1}(-1)^n\left(\frac{\theta^{2n}+\bar{\theta}^{2n}}{p}\right) \\
&= \sum_{n=1}^{p+1}\left(\frac{\theta^{4n}+\bar{\theta}^{4n}}{p}\right) - \sum_{n=1}^{p+1}\left(\frac{\theta^{2n}+\bar{\theta}^{2n}}{p}\right).
\end{aligned} \tag{3.2}
$$

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 $Q(\sqrt{2}, i) = Q(\omega)$, where $\omega = \exp(2\pi i/8)$. D is a unique factorization domain. If π denotes a prime factor of p in D, then $k = D/(\pi)$ is a field of $N(\pi)$ elements, where

$$
N(\pi) = \begin{cases} p & \text{if } p \equiv 1 \pmod 8, \\ p^2 & \text{if } p \equiv 3 \pmod 8. \end{cases} \tag{4.1}
$$

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

$$
\chi(\xi) = \omega^\lambda \quad \text{if } \xi^{(N(\pi)-1)/8} \equiv \omega^\lambda \pmod{\pi}, \tag{4.2}
$$

for elements ξ of D not divisible by π. The function χ defined by (4.2) is related to the Legendre symbol by

$$
\left(\frac{a}{p}\right) = \begin{cases} \chi^4(a) & \text{if } p \equiv 1 \pmod 8, \\ \chi(a) & \text{if } p \equiv 3 \pmod 8, \text{ for all } a \text{ in } Z. \end{cases} \tag{4.3}
$$

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

$$\theta^{(p^2-1)/8} = (\theta^{(p+1)/4})^{(p-1)/2} = (\pm i)^{(p-1)/2} = \pm i, \text{ so that } \chi(\theta) = \pm i.$$

Replacing θ 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 χ, we set $J(m, n) = J(\chi^m, \chi^n)$ and $G(m) = G(\chi^m)$ to simplify notation. Also, $\bar{\alpha}$ and α' denote the conjugates of α 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

$$(4.4) \qquad J(1,4) \equiv \sum_{y=0}^{p-1} y^{(p-1)/8}(1-y)^{(p-1)/2} \equiv 0 \pmod{\pi} \text{ in } D.$$

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

$$(4.5) \qquad J(1,4) \equiv \sum_{y=0}^{p-1} y^{3(p-1)/8}(1-y)^{(p-1)/2} \equiv 0 \pmod{\bar{\pi}'} \text{ in } D.$$

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

$$(4.6) \qquad J(1,4) = \gamma\pi\bar{\pi}', \quad \text{for some } \gamma \text{ in } D.$$

Now by (1.3) and (1.5), $\overline{J(1,4)} = J(3,4) = G(3)G(4)/G(7) = G(1)G(4)/G(5) = J(1,4)$ showing that $J(1,4)$ is in $Z[\sqrt{-2}]$. Since $\pi\bar{\pi}'$ is in $Z[\sqrt{-2}]$, γ is in $Z[\sqrt{-2}]$ as well. Computing norms in (4.6) gives, by (1.4), that γ 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 $1 \leqq y \leqq p-2$, $((y+1)/p) + 1 \equiv 0 \pmod 2$, and

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

so that

$$\sum_{\substack{y=1 \\ \left(\frac{y}{p}\right)=1}}^{p-2} \{\chi(y) - 1\} \left\{ \left(\frac{y+1}{p} \right) + 1 \right\} \tag{4.7}$$
$$+ \sum_{\substack{y=1 \\ \left(\frac{y}{p}\right)=-1}}^{p-2} \{\chi(y) - \omega\} \left\{ \left(\frac{y+1}{p} \right) + 1 \right\} \equiv 0 (\mathrm{mod}\, 2\sqrt{-2}).$$

After some simplification of (4.7) we obtain

$$J(1, 4) \equiv \frac{1}{2}(p-5) + \frac{\omega}{2}(p-1) + \chi(-1) \,(\mathrm{mod}\, 2\sqrt{-2}),$$

or

$$J(1, 4) \equiv (-1)^k - 2 \equiv (-1)^{k+1} \equiv c (\mathrm{mod}\, 2\sqrt{-2}). \tag{4.8}$$

As d is even, we have $J(1, 4) = c + d\sqrt{-2}$, completing the proof.

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

$$K = \sum_{b=0}^{p-1} \chi(1 + bi), \tag{4.9}$$

which satisfies (see [6], lemma 2)

$$K\bar{K} = p, \tag{4.10}$$

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

$$J(1, 3) = -K^2, \tag{4.11}$$

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.

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

so that L is in $Z[\sqrt{-2}]$. For $0 \leqq b \leqq p-1$, 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 $GF(p^2)$ are simply θ^n, $1 \leqq n \leqq p+1$, $n \neq (p+1)/2$. Therefore

$$\left\{\theta^n + 1 \,\middle|\, 1 \leqq n \leqq p+1, n \neq \frac{p+1}{2}\right\}$$
$$= \left\{\frac{2}{1+bi} \,\middle|\, 0 \leqq b \leqq p+1\right\},$$

so that

$$K = \sum_{b=0}^{p-1} \chi(1+bi) = {\sum_n}' \chi\left(\frac{2}{\theta^n+1}\right)$$
$$= -{\sum_n}' \bar{\chi}(\theta^n + 1) = -\bar{L},$$

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

LEMMA 4.4. *For* $p = 8k+3 = c^2 + 2d^2$, *with* $c \equiv (-1)^{k+1} (\mathrm{mod}\, 4)$, *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 $p = L\bar{L} = \pi\bar{\pi}$, so that $L = \pm\pi$ or $\pm\bar{\pi}$, showing that L can be written in the form $\pm(c + d\sqrt{-2})$ with $c \equiv (-1)^{k+1} (\mathrm{mod}\, 4)$ and $c^2 + 2d^2 = p$.

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

$$\sum_{x=0}^{p-1} \left(\frac{x^8+1}{p}\right) \tag{5.1}$$
$$= \sum_{x=0}^{p-1} \left(\frac{x+1}{p}\right)\{1 + \chi(x) + \chi^2(x) + \cdots + \chi^7(x)\},$$

and

$$\sum_{x=0}^{p-1} \left(\frac{x^4+1}{p}\right) \tag{5.2}$$
$$= \sum_{x=0}^{p-1} \left(\frac{x+1}{p}\right)\{1 + \chi^2(x) + \chi^4(x) + \chi^6(x)\},$$

which, with (3.1) gives

$$2B = J(1,4) + \overline{J(1,4)'} + J(1,4)' + \overline{J(1,4)}. \tag{5.3}$$

From lemma 4.2, $2B = 4c$, so that $B = 2c$ as required.

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

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

as $p + 1 = 4(2k + 1)$ implies that the fourth powers and eighth powers in the cyclic group $\langle \theta \rangle$ 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

$$\begin{aligned} 2B &= S_0, \\ 4L &= S_0 + S_1 + S_2 + S_3 = \pm 4(c + d\sqrt{-2}). \end{aligned} \tag{5.5}$$

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

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

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

$$\chi(\theta^m + 1) = \pm \omega^{3m}. \tag{5.7}$$

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

$$(1 + i)S_3 = e\sqrt{-2}. \tag{5.8}$$

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

$$\begin{aligned} S_0/4 &= \frac{1}{4}\sum_{n=1}^{p+1} \chi(\theta^{4n} + 1) = \sum_{n=1}^{2k+1} \chi(\theta^{4n} + 1) \\ &= \sum_{n=1}^{2k} \chi(\theta^{4n} + 1) - 1, \end{aligned}$$

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)) $\chi(\theta^{4m}+1) = \pm 1$, we have

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

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

References

1. B. W. Brewer, *On certain character sums,* Trans. Amer. Math. Soc. **99** (1961), 241–245.
2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen,* J. Reine Angew. Math. **57** (1935), 151–182.
3. R. E. Giudici, J. B. Muskat, and S. F. Robinson, *On the evaluation of Brewer's character sums,* Trans. Amer. Math. Soc. **171** (1972), 317–347.
4. K. Ireland and M. I. Rosen, *Elements of number theory* Bogden and Quigley, Tarrytown, New York, 1972.
5. A. R. Rajwade, *Arithmetic on curves with complex multiplication by* $\sqrt{-2}$, Proc. Camb. Phil. Soc. **64** (1968), 659–672.
6. A. L. Whiteman, *A theorem of Brewer on character sums,* Duke Math. J. **30** (1963), 545–552.
7. K. S. Williams, *On Salié's sum,* J. Number Theory 3 (1971), 316–317.

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