J. Austral. Math. Soc. (*Series A*) **28** (1979), 235–240

UNAMBIGUOUS EVALUATIONS OF BIDECIC JACOBI AND JACOBSTHAL SUMS

RONALD J. EVANS

(Received 30 October 1978; revised 24 January 1979)

Communicated by A. J. van der Poorten

Abstract

For a class of primes $p \equiv 1 \pmod{20}$ for which 2 is a quintic nonresidue, unambiguous evaluations of parameters of bidecic Jacobi and Jacobsthal sums (mod p) are presented, in terms of the partition $p = a^2+5b^2+5c^2+5d^2$, $ab = d^2-c^2-cd$. Similar results for sums of other orders have been obtained by E. Lehmer and by K. S. Williams.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): 10 G 05.

1. Introduction; decic sums

Throughout this note, $p = 10f+1$ is prime. (In Section 2, f will be assumed even.) Fix a primitive root $g \pmod{p}$ and a character $\chi \pmod{p}$ of order 10 such that $\chi(g) = e^{2\pi i/10}$. For characters $\lambda, \mu \pmod{p}$, define the Gauss sum

$$G(\lambda) = \sum_{n=1}^{p-1} \lambda(n)\, e^{2\pi i n/p}$$

and the Jacobi sums

$$J(\lambda,\mu) = \sum_{n=2}^{p-1} \lambda(n)\,\mu(1-n), \quad J(\lambda) = J(\lambda,\lambda), \quad K(\lambda) = \lambda(4)\,J(\lambda).$$

As is well known (see Ireland and Rosen (1972), p. 93)

(1) $G(\lambda)\,G(\bar{\lambda}) = \lambda(-1)p$, $J(\lambda,\bar{\lambda}) = -\lambda(-1)$ and $G(\lambda)\,G(\mu)/G(\lambda\mu) = J(\lambda,\mu)$

when λ, μ and $\lambda\mu$ are nontrivial. For $\alpha \not\equiv 0 \pmod{p}$, define the Jacobsthal sums

$$\varphi_n(\alpha) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right)\left(\frac{m^n+\alpha}{p}\right),$$

where the factors in the summands are Legendre symbols. The following basic

formula (Berndt and Evans (1979a), Theorem 2.7) expresses Jacobsthal sums in terms of Jacobi sums:

$$\varphi_n(\alpha) = \lambda(-1)\sum_{j=0}^{n-1} \lambda^{n+1+2j}(\alpha)\, K(\lambda^{2j+1}), \tag{2}$$

where λ has order $2n$.

It is known (see Berndt and Evans (1979b), Theorems 3.1, 3.7; Giudici *et al.* (1972), p. 345; Muskat and Zee (1975)) that there exist integers a, b, c, d such that

$$(-1)^f K(\chi) = a + b\sqrt{5} + ic(5+2\sqrt{5})^{\frac{1}{2}} + id(5-2\sqrt{5})^{\frac{1}{2}} \tag{3}$$

and

$$\varphi_5(\alpha) = \begin{cases} -1+4a & \text{if } \operatorname{ind}_g \alpha \equiv 0 \pmod 5, \\ -1-a-5b+5c-5d & \text{if } \operatorname{ind}_g \alpha \equiv 1 \pmod 5, \\ -1-a+5b-5c-5d & \text{if } \operatorname{ind}_g \alpha \equiv 2 \pmod 5, \\ -1-a+5b+5c+5d & \text{if } \operatorname{ind}_g \alpha \equiv 3 \pmod 5, \\ -1-a-5b-5c+5d & \text{if } \operatorname{ind}_g \alpha \equiv 4 \pmod 5, \end{cases} \tag{4}$$

where

$$a \equiv -1 \pmod 5, \quad p = a^2+5b^2+5c^2+5d^2 \quad \text{and} \quad ab = d^2-c^2-cd. \tag{5}$$

Moreover, the solutions $\pm(a, b, c, d)$ to the equations in (5) are essentially unique in the sense that the only other solutions in integers are $\pm(a, b, -c, -d)$, $\pm(a, -b, -d, c)$, $\pm(a, -b, d, -c)$.

Lehmer (1959, 1960) has given unambiguous determinations of decic Jacobi and Jacobsthal sums in the case that 2 is a quintic nonresidue (mod p), in terms of the parameters in Dickson's partition (Dickson (1935), p. 402):

$$16p = X^2+50U^2+50V^2+125W^2, \quad XW = V^2-U^2-4UV, \; X \equiv 1 \pmod 5. \tag{6}$$

In view of Giudici *et al.* (1972), p. 345 and Lehmer (1959), p. 68, the parameters in (5) and (6) are connected as follows:

(7)

If $\operatorname{ind}_g 2 \equiv 0 \pmod 5$,

$X = 4a, \quad W = -4b/5, \quad V = 2(3c-d)/5, \quad U = -2(c+3d)/5$

and

$a = 4X, \quad b = -5W/4, \quad c = (3V-U)/4, \quad d = -(3U+V)/4$;

if $\operatorname{ind}_g 2 \equiv 1 \pmod 5$,

$X = -a+5b-5c-5d$ and $16a = -X-25W+10V-20U$,

$5W = -a+b+3c-d$ and $16b = X+5W+10V$,

$5V = a+5b+c+3d$ and $16c = -X+15W+2V-4U$,

$5U = -2a-2c+4d$ and $16d = -X-5W+6V+8U$.

(If 2 is not a quintic residue (mod p), we may assume without loss of generality that $\mathrm{ind}_g 2 \equiv 1 \pmod 5$, by choosing g appropriately.) Relations in (7) can be used to reformulate the above-mentioned results of Lehmer to provide unambiguous determinations of the sums in (3) and (4), as follows.

THEOREM 1. *Let* $\mathrm{ind}_g 2 \equiv 1 \pmod 5$. *Then* (3) *and* (4) *hold with* a, b, c *and* d *uniquely determined by* (5) *together with the conditions*

$$b \equiv 1 \pmod 5 \quad \textit{and} \quad c \equiv 2d+1 \pmod 5.$$

To supplement Theorem 1, we remark that Lehmer (1951) showed that 2 is a quintic residue (mod p) if and only if the parameter X in (6) is even. Thus it follows easily from (7) that 2 is a quintic residue (mod p) if and only if $5 \mid b$.

In Section 2, Theorem 1 is applied to evaluate the parameters unambiguously in bidecic Jacobi and Jacobsthal sums for certain $p \equiv 1 \pmod{20}$. Similar evaluations for sums of other orders appear in the literature. For sums of orders 3, 4 and 6, see Lehmer (1955, 1959, 1960). For sums of orders 3, 5, 7 and 11, see Williams (1979). (See also the related papers of Leonard and Williams (1976), Nashier and Rajwade (1977), Rajwade (1975) and Williams (1975a, b).) For sums of orders 4, 8, 12 and 16, see Evans (1979). Finally, ambiguous signs in many different relations between Jacobi sums have been resolved by Muskat (1968) and Muskat and Zee (1973).

We conclude this section by discussing the relations between the Jacobi sums $K(\chi)$ and $J(\chi^i, \chi^j)$.

By Berndt and Evans (1979a), Theorems 2.3 and 2.5,

$$K(\chi) = J(\chi, \chi^5) = (-1)^f K(\chi^4) = (-1)^f J(\chi, \chi^4). \tag{8}$$

With application of the automorphism in $\mathrm{Gal}\,(Q(e^{2\pi i/10})/Q)$ defined by $e^{2\pi i/10} \to e^{6\pi i/10}$, it follows from (3) and (8) that

$$K(\chi^2) = (-1)^f K(\chi^3) = a - b\sqrt{5} + ic(5-2\sqrt{5})^{\frac{1}{2}} - id(5+2\sqrt{5})^{\frac{1}{2}}. \tag{9}$$

Moreover, it follows with the aid of (1), (8) and (9) that

$$\begin{cases} K(\chi) = \bar{\chi}^3(-4)\, J(\chi, \chi^2) = \bar{\chi}(-4)\, J(\chi^2, \chi^4) = \chi^2(4)\, J(\chi, \chi^7) = \chi(-4)\, J(\chi, \chi^8), \\ K(\chi^2) = \chi(4)\, J(\chi, \chi^6) = \chi^2(4)\, J(\chi^2) = J(\chi^2, \chi^5) = \chi^2(4)\, J(\chi^2, \chi^6) \\ \qquad\qquad = \chi(-4)\, J(\chi, \chi^3). \end{cases} \tag{10}$$

As a consequence of (8), (9) and (10), note that a determination of the Jacobi sum in (3) yields determinations of all Jacobi sums $J(\chi^i, \chi^j)$.

2. Bidecic sums

In this section, $p = 20k+1$. Fix a character $\lambda \pmod p$ of order 20 such that

https://doi.org/10.1017/S1446788700015731 Published online by Cambridge University Press

$\lambda(g) = e^{2\pi i/20}$. There exist integers x, y (see Berndt and Evans (1979a), Theorem 3.9) such that

$$J(\lambda^5) = -x+2iy, \tag{11}$$

where x and $|y|$ are uniquely determined by the conditions

$$p = x^2+4y^2, \quad x \equiv 1 \pmod 4.$$

There exist integers u, v (see Berndt and Evans (1979a), Theorem 3.34) such that

$$(-1)^k K(\lambda) = \begin{cases} u+iv\sqrt{5} & \text{if } 5 \nmid x, \\ iu-v\sqrt{5} & \text{if } 5 \mid x, \end{cases} \tag{12}$$

where $|u|$ and $|v|$ are uniquely determined by the condition

$$p = u^2+5v^2, \tag{13}$$

and where moreover

$$u \equiv \begin{cases} -x \pmod 5 & \text{if } 5 \nmid x \\ 2y \pmod 5 & \text{if } 5 \mid x. \end{cases} \tag{14}$$

It follows therefore from (2) (see the proof in Berndt and Evans (1979a), Theorem 4.13) that the Jacobsthal sum $\varphi_{10}(\alpha)$ has the values indicated below:

(15)

$\varphi_{10}(\alpha)$, if $5 \mid x$	$\varphi_{10}(\alpha)$, if $5 \nmid x$	$\operatorname{ind}_g \alpha \pmod{20}$
$-2x$	$-2x+8u$	0
$4y+8u$	$4y$	5
$-2x-10v$	$-2x-2u$	4
$-2x+10v$	$-2x-2u$	8
$4y-2u$	$4y+10v$	1
$-4y+2u$	$-4y+10v$	3

For those α not included above, the values of $\varphi_{10}(\alpha)$ can be found with use of the easily proved relations

$$\varphi_{10}(\alpha) = (-1)^k \varphi_{10}(-\alpha), \quad \varphi_{10}(\alpha^{-1}) = \left(\frac{\alpha}{p}\right)\varphi_{10}(\alpha).$$

Simple criteria for determining the sign of y in (11) are known in the case that 2 is a quartic nonresidue (mod p) (Lehmer (1955)) and also in the case that 2 is a quartic but not octic residue (mod p) for primes $p \equiv 1 \pmod{80}$ (Evans (1979)). Thus in these cases u is completely determined, by (14). No simple criterion in terms of $\operatorname{ind}_g 2$ is known in general to determine the sign of v, but in Theorem 2, we will give such a criterion in the case that $5 \mid x$ and 2 is a quintic nonresidue (mod p). We remark that the primes $p = 20k+1$ for which $5 \mid x$ are precisely those for which 5 is a quartic nonresidue—this is a simple consequence of the law of quartic reciprocity.

https://doi.org/10.1017/S1446788700015731 Published online by Cambridge University Press

THEOREM 2. *Let* 2 *be a quintic nonresidue* (mod p), *so that* b *may be uniquely determined as in Theorem* 1. *Suppose that* $5 \mid x$. *Then* (12) *and* (15) *hold with* v *uniquely determined by* (13) *together with the condition*

$$v \equiv (-1)^k b \pmod 4.$$

PROOF. Put $\chi = \lambda^2$. It suffices to prove more generally that

$$\pm 1 \equiv v \equiv (-1)^k b \pmod 4$$

with b defined by (3), regardless of whether or not 2 is a quintic residue (mod p). By Berndt and Evans (1979a), Theorem 2.5, $K(\lambda) = K(\bar{\lambda}^{11})$, and by (9), $K(\lambda)^6 = K(\bar{\lambda})$.[16] Hence

$$\sum_{j=0}^{3} K(\lambda^{5j+1}) = 2 \operatorname{Re}\{K(\lambda)+K(\chi^3)\} = 2a - 2b\sqrt{5} - 2(-1)^k v\sqrt{5}, \tag{16}$$

where the last equality follows from (9) and (12). By definition of $K(\lambda)$,

$$\sum_{j=0}^{3} K(\lambda^{5j+1}) = \sum_{n=1}^{p-1} \lambda(4n(1-n))\{1+t_n+t_n^2+t_n^3\},$$

where $t_n = \lambda^5(4n(1-n))$. Thus

$$\begin{aligned} \sum_{j=0}^{3} K(\lambda^{5j+1}) &= 4 \sum_{1 \le n < p, t_n = 1} \lambda(4n(1-n)) \\ &= 4 + 8 \sum_{2 \le n \le (p-1)/2, t_n = 1} \lambda(4n(1-n)). \end{aligned} \tag{17}$$

By (16) and (17), there is an algebraic integer η for which

$$4\eta = a - 2 - \sqrt{5}(b+(-1)^k v).$$

Thus

$$(a-2)^2 \equiv 5(b+(-1)^k v)^2 \pmod 8. \tag{18}$$

It is known (see Lehmer (1966), Theorem 1; Muskat and Whiteman (1970), p. 198; Lehmer (1972), Corollary 1.1; Berndt and Evans (1979a), Corollary 3.35) that $2 \mid u$, $2 \nmid v$ when $5 \mid x$. If a were odd, (18) would yield $1 \equiv 5 \pmod 8$. Thus $2 \mid a$, $2 \nmid b$. Then by (5), $2 \mid c$, $2 \mid d$ and $4 \mid a$. Therefore $b \equiv (-1)^k v \pmod 4$ by (18).

References

B. C. Berndt and R. J. Evans (1979a), 'Sums of Gauss, Jacobi, and Jacobsthal', *J. Number Theory* (to appear in 1979).

B. C. Berndt and R. J. Evans (1979b), 'Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer', *Illinois J. Math.* (to appear in 1979).

L. E. Dickson (1935), 'Cyclotomy, higher congruences and Waring's problem', *Amer. J. Math.* **57**, 391–424.

R. J. Evans (1979), 'Resolution of sign ambiguities of Jacobi and Jacobsthal sums', *Pacific J. Math.* (to appear in 1979).
R. E. Giudici, J. B. Muskat, and S. F. Robinson (1972), 'On the evaluation of Brewer's character sums', *Trans. Amer. Math. Soc.* **171,** 317–347.
K. Ireland and M. Rosen (1972), *Elements of number theory* (Bogden and Quigley, Tarrytown-on-Hudson).
E. Lehmer (1951), 'The quintic character of 2 and 3', *Duke Math. J.* **18,** 11–18.
E. Lehmer (1955), 'On the number solutions of $u^k + D \equiv \omega \pmod{p}$', *Pacific J. Math.* **55,** 103–118.
E. Lehmer (1959), 'On Euler's criterion', *J. Austral. Math. Soc.* **1,** 64–70.
E. Lehmer (1960), 'On Jacobi functions', *Pacific J. Math.* **10,** 887-893.
E. Lehmer (1966), 'On the quadratic character of the Fibonacci root', *Fibonacci Quart.* **4,** 135–138.
E. Lehmer (1972), 'On some special quartic reciprocity laws', *Acta Arith.* **21,** 367–377.
P. A. Leonard and K. S. Williams (1976), 'The eleventh power character of 2', *J. Reine Angew. Math.* **286,** 213–222.
J. B. Muskat (1968), 'On Jacobi sums of certain composite orders', *Trans. Amer. Math. Soc.* **134,** 483–502.
J. B. Muskat and A. L. Whiteman (1970), 'The cyclotomic numbers of order twenty', *Acta Arith.* **17,** 185–216.
J. B. Muskat and Y. C. Zee (1973), 'Sign ambiguities of Jacobi sums', *Duke Math. J.* **40,** 13–334.
J. B. Muskat and Y. C. Zee (1975), 'On the uniqueness of solutions of certain Diophantine equations', *Proc. Amer. Math. Soc.* **49,** 13–19.
B. S. Nashier and A. R. Rajwade (1977), 'Determination of a unique solution of the quadratic partition for primes $p \equiv 1 \pmod{7}$', *Pacific J. Math.* **72,** 513–521.
A. R. Rajwade (1975), 'Notes on the congruence $y^2 \equiv x^5 - a \pmod{p}$', *Enseign. Math.* **21,** 49–56.
K. S. Williams (1975a), 'On Euler's criterion for cubic nonresidues', *Proc. Amer. Math. Soc.* **49,** 277–283.
K. S. Williams (1975b), 'On Euler's criterion for quintic nonresidues', *Pacific J. Math.* **61,** 543-550.
K. S. Williams (1979) (unpublished).

Department of Mathematics
University of California, San Diego
La Jolla, California 92093
U.S.A.