PACIFIC JOURNAL OF MATHEMATICS
Vol. 99, No. 2, 1982

RESOLUTION OF AMBIGUITIES IN THE EVALUATION OF CUBIC AND QUARTIC JACOBSTHAL SUMS

RICHARD H. HUDSON AND KENNETH S. WILLIAMS

If $p \equiv 1 \pmod{2k}$ is a prime, the Jacobsthal sum $\Phi_k(D)$ is defined by

$$\Phi_k(D) = \sum_{x=1}^{p-1} \left(\frac{x(x^k+D)}{p}\right) \quad (k = 2, 3, \cdots) .$$

It is shown how to evaluate $\Phi_2(D)$ and $\Phi_3(D)$ for any integer D.

1. Introduction. The Jacobsthal sum $\Phi_k(D)$ is defined for primes $p \equiv 1 \pmod{2k}$ by

$$(1.1) \qquad \Phi_k(D) = \sum_{x=1}^{p-1} \left(\frac{x(x^k + D)}{p}\right) , \quad k = 2, 3, \cdots ,$$

where $\left(\frac{\ }{p}\right)$ is the Legendre symbol, and D is an integer not divisible by p. It is well-known (see for example [8: p. 104]) that

$$(1.2) \qquad \Phi_k(Dm^k) = \left(\frac{m}{p}\right)^{k-1} \Phi_k(D) , \quad m \not\equiv 0 \pmod{p} .$$

In this paper, we show how to resolve the sign ambiguities in the evaluations of $\Phi_2(D)$ and $\Phi_3(D)$. (For a discussion of Jacobsthal sums see, for example, [7], [14], [1].)

2. $k = 2$. In this case $p \equiv 1 \pmod 4$ and there are integers a and b such that

$$(2.1) \qquad p = a^2 + b^2 , \quad a \equiv 1 \pmod 4 , \quad b \equiv 0 \pmod 2 ,$$

with a and $|b|$ unique. Relation (1.2) gives in this case

$$(2.2) \qquad \Phi_2(Dm^2) = \left(\frac{m}{p}\right) \Phi_2(D) , \quad m \not\equiv 0 \pmod{p} ,$$

so that it suffices to consider $\Phi_2(D)$ for squarefree D. Choosing m such that $m^2 \equiv -1 \pmod{p}$ in (2.2), we have

$$(2.3) \qquad \Phi_2(-D) = (-1)^{(p-1)/4} \Phi_2(D) ,$$

so that we may take D positive. Jacobsthal [7: pp. 240-241] has evaluated $\Phi_2(1)$. He has shown that

$$(2.4) \qquad \Phi_2(1) = -2a ,$$

and thus, by (2.2), for any D with $(D/p) = +1$, say $D \equiv E^2 \pmod{p}$, one has

$$\Phi_2(D) = -\left(\frac{E}{p}\right)2a . \tag{2.5}$$

Thus it suffices to consider $\Phi_2(D)$ for quadratic nonresidues D. Emma Lehmer [8: p. 107] has shown that, if $(2/p) = -1$,

$$\Phi_2(2) = \mp 2b \quad \text{according as} \quad b \equiv \pm 2 \pmod 8 \tag{2.6}$$

and it follows from the work of Brewer [2: p. 243] and (2.3), that, if $(3/p) = -1$,

$$\Phi_2(3) = \pm(-1)^{(p-1)/4} 2b \quad \text{according as} \quad a \equiv \pm b \pmod 3 . \tag{2.7}$$

Jacobsthal [7: p. 241] has shown, for an arbitrary D satisfying $(D/p) = -1$, that

$$\Phi_2(D) = \pm 2b , \tag{2.8}$$

and we begin in Theorem 1 by showing how to determine the correct sign in (2.8), when D is an odd prime q satisfying $(q/p) = -1$. Afterwards we illustrate how to prove the results for composite D.

Let q be an odd prime satasfying $(q/p) = -1$, so that $ab \not\equiv 0 \pmod q$. If $q \equiv 1 \pmod 4$, there are unique positive integers r and s such that

$$q = r^2 + s^2 , \quad r \equiv 1 \pmod 2 , \quad s \equiv 0 \pmod 2 . \tag{2.9}$$

Clearly r and s are not divisible by q. We define a set K, depending only on q, by

$$\begin{aligned} K = \Big\{k \colon -\frac{1}{2}(q-1) \leqq k \leqq \frac{1}{2}(q-1) ,& \\ r(sk+r)^{(q-1)/4} - s(sk-r)^{(q-1)/4} \equiv 0 \pmod q\Big\} .& \end{aligned} \tag{2.10}$$

Clearly $0 \notin K$. It is known that (see for example [4: p. 65])

$$q^{(p-1)/4} \equiv \pm a/b \pmod p \quad \text{according as} \quad a \equiv \pm kb \pmod q \tag{2.11}$$

for some $k \in K$.

If $q \equiv 3 \pmod 4$, we define K by

$$\begin{aligned} K = \Big\{k \colon -\frac{1}{2}(q-1) \leqq k \leqq \frac{1}{2}(q-1) ,& \\ (k+i)^{(q+1)/4} - i(k-i)^{(q+1)/4} \equiv 0 \pmod q\Big\} .& \end{aligned} \tag{2.12}$$

Again we have $0 \notin K$. Further

$$(2.13) \qquad (-q)^{(p-1)/4} \equiv \pm a/b \pmod p \quad \text{according as} \quad a \equiv \pm kb \pmod q$$

for some $k \in K$.

We prove the following theorem.

THEOREM 1. *Let p be a prime congruent to 1 modulo 4 and define a and b by (2.1). Let q be an odd prime satisfying $(q/p) = -1$. Then, if $q \equiv 1 \pmod 4$,*

$$(2.14) \quad \Phi_2(q) = \pm 2b \quad \textit{according as} \quad a \equiv \pm kb \pmod q \quad \textit{for some} \quad k \in K\,;$$

if $q \equiv 3 \pmod 4$,

$$(2.15) \quad \Phi_2(q) = \pm(-1)^{(p-1)/4}2b\,, \quad \textit{if} \quad a \equiv kb \pmod q \quad \textit{for some} \quad k \in K\,.$$

Proof. Emma Lehmer [10: p. 65] has proved that for $D \not\equiv 0 \pmod p$,

$$(2.16) \qquad D^{(p-1)/4} \equiv \Phi_2(D)/\Phi_2(1) \pmod p\,.$$

Taking $D = q \equiv 1 \pmod 4$ in (2.16), and appealing to (2.4) and (2.11), we obtain

$$\Phi_2(q) \equiv \begin{cases} +2b \pmod p\,, & \text{if} \quad a \equiv kb \pmod q \quad \text{for some} \quad k \in K\,, \\ -2b \pmod p\,, & \text{if} \quad a \equiv -kb \pmod q \quad \text{for some} \quad k \in K\,. \end{cases}$$

Since $\Phi_2(q) = \pm 2b$, by (2.8), and as $2b \not\equiv 0 \pmod p$, we obtain (2.14). The case $q \equiv 3 \pmod 4$ is similar.

We illustrate Theorem 1 by giving $\Phi_2(q)$ for odd primes $q \leqq 19$ satisfying $(q/p) = -1$; $\alpha(p) = (p-1)/4$ with the upper signs and $(p+3)/4$ with the lower signs.

q	$\Phi_2(q)$	k satisfying $a \equiv kb \pmod q$
3	$(-1)^{\alpha(p)}2b$	± 1
5	$\pm 2b$	∓ 1
7	$(-1)^{\alpha(p)}2b$	$\mp 2,\ \mp 3$
11	$(-1)^{\alpha(p)}2b$	$\mp 1,\ \mp 3,\ \mp 4$
13	$\pm 2b$	$\pm 1,\ \pm 2,\ \mp 6$
17	$\pm 2b$	$\pm 2,\ \mp 3,\ \pm 6,\ \pm 8$
19	$(-1)^{\alpha(p)}2b$	$\pm 1,\ \mp 3,\ \pm 6,\ \mp 7,\ \pm 8$

The case $q = 3$ constitutes the result of Brewer (2.7).

We remark that these results can be combined to determine $\Phi_2(D)$ when D is composite and $(D/p) = -1$. We treat the case $D = 6 = 2\times 3$. If $(6/p) = -1$, we have $(2/p) = +1$, $(3/p) = -1$, or $(2/p) =$

-1, $(3/p) = +1$. In the former case, we have

$$\Phi_2(2) = -\left(\frac{2}{p}\right)_4 2a = -(-1)^{b/4}2a\,, \tag{2.17}$$

and

$$\Phi_2(3) = \pm 2b \quad \text{according as} \quad a \equiv \pm b \pmod 3\,. \tag{2.18}$$

From (2.16) we obtain

$$\Phi_2(6) \equiv \frac{\Phi_2(2)\Phi_2(3)}{\Phi_2(1)} \pmod p\,, \tag{2.19}$$

and so

$$\Phi_2(6) \equiv \begin{cases} (-1)^{b/4}2b \pmod p\,, & \text{if} \quad a \equiv b \pmod 3\,, \\ (-1)^{b/4+1}2b \pmod p\,, & \text{if} \quad a \equiv -b \pmod 3\,. \end{cases}$$

Hence, by (2.8), we have

$$\Phi_2(6) = \begin{cases} (-1)^{b/4}2b\,, & \text{if} \quad a \equiv b \pmod 3\,, \\ (-1)^{b/4+1}2b\,, & \text{if} \quad a \equiv -b \pmod 3\,. \end{cases} \tag{2.20}$$

The case when $(2/p) = -1$, $(3/p) = +1$ can be treated similarly.

3. $k = 3$. In this case $p \equiv 1 \pmod 6$ and there are integers L and M such that

$$4p = L^2 + 27M^2\,, \quad L \equiv 1 \pmod 3\,, \tag{3.1}$$

with L and $|M|$ unique. Clearly we have $L \equiv M \pmod 2$. Relation (1.2) gives in this case

$$\Phi_3(Dm^3) = \Phi_3(D)\,, \quad m \not\equiv 0 \pmod p\,, \tag{3.2}$$

so that it suffices to consider $\Phi_3(D)$ for cubefree D. Clearly $\Phi_3(-D) = \Phi_3(D)$, so that we may take D positive. It follows from the work of von Schrutka [13: p. 258] (see also Chowla [3: p. 246], Whiteman [14: p. 96]) that

$$\Phi_3(1) = \begin{cases} L - 1\,, & \text{if} \quad L \equiv M \equiv 0 \pmod 2\,, \\ \frac{1}{2}(-L + 9M - 2)\,, & \text{if} \quad L \equiv M \equiv 1 \pmod 2 \\ & \text{and} \quad L \equiv M \pmod 4\,, \\ \frac{1}{2}(-L - 9M - 2)\,, & \text{if} \quad L \equiv M \equiv 1 \pmod 2 \\ & \text{and} \quad L \equiv -M \pmod 4\,. \end{cases} \tag{3.3}$$

From (3.2), $\Phi_3(k) = \Phi_3(1)$ for any cubic residue k modulo p, so that (3.3) gives unambiguously the value of $\Phi_3(k)$ for any cubic residue $k \pmod p$. Now 2 is a cubic residue $\pmod p$ if and only if $L \equiv M \equiv 0$

(mod 2) [6: p. 68]. Thus we have

$$\Phi_3(1) = \Phi_3(2) = \Phi_3(4) = L - 1\,, \quad \text{if} \quad 2 \text{ is a cubic residue} \pmod p\,. \tag{3.4}$$

When 2 is not a cubic residue $\pmod p$, so that $L \equiv M \equiv 1 \pmod 2$, Emma Lehmer [8: p. 112] has proved that

$$\Phi_3(2) = \begin{cases} \frac{1}{2}(-L - 9M - 2)\,, & \text{if} \quad L \equiv M \pmod 4\,, \\ \frac{1}{2}(-L + 9M - 2)\,, & \text{if} \quad L \equiv -M \pmod 4\,, \end{cases} \tag{3.5}$$

and

$$\Phi_3(4) = L - 1\,. \tag{3.6}$$

For an arbitrary cubic nonresidue D, it is known that

$$\Phi_3(D) = \begin{cases} (\frac{1}{2}(-L - 9M - 2)\,, & \text{if} \quad L \equiv M \equiv 0 \pmod 2\,, \\ \quad \text{or} & \\ \frac{1}{2}(-L + 9M - 2)\,, & \end{cases} \tag{3.7}$$

$$\Phi_3(D) = \begin{cases} L - 1 & \text{if} \quad L \equiv M \equiv 1 \pmod 2 \quad \text{and} \\ \quad \text{or} & \\ \frac{1}{2}(-L - 9M - 2)\,, & \quad L \equiv M \pmod 4\,, \end{cases} \tag{3.8}$$

and

$$\Phi_3(D) = \begin{cases} L - 1 & \text{if} \quad L \equiv M \equiv 1 \pmod 2 \quad \text{and} \\ \quad \text{or} & \\ \frac{1}{2}(-L + 9M - 2)\,, & \quad L \equiv -M \pmod 4\,. \end{cases} \tag{3.9}$$

It is our purpose in Theorem 2 to show how to eliminate the ambiguities in (3.7), (3.8), and (3.9) when D is an odd prime q, which is a cubic nonresidue $\pmod p$. (As q is a cubic nonresidue $\pmod p$ we have $LM \not\equiv 0 \pmod q$ [9: p. 26].)

Our starting point is the congruence

$$q^{(p-1)/3} \equiv (\Phi_3(q) + 1)/(\Phi_3(1) + 1) \pmod p\,, \tag{3.10}$$

which is given in [10: p. 66]. From (3.10) we obtain

$$\Phi_3(q) \equiv -1 + q^{(p-1)/3}(\Phi_3(1) + 1) \pmod p\,. \tag{3.11}$$

For $q \geqq 5$, one of us [15: p. 282] has shown that there exists a set of integers $\mathscr{L}$ (depending only on q) such that

$$q^{(p-1)/3} \equiv \begin{cases} (L + 9M)/(L - 9M) \pmod p\,, & \text{if} \quad L \equiv kM \pmod q \\ & \qquad \text{for some} \quad k \in \mathscr{L}\,, \\ (L - 9M)/(L + 9M) \pmod p\,, & \text{if} \quad L \equiv -kM \pmod q \\ & \qquad \text{for some} \quad k \in \mathscr{L}\,. \end{cases} \tag{3.12}$$

It is shown in [15] that, if $q \equiv 1 \pmod 3$,

$$(3.13)\qquad \mathscr{L} = \{-\tfrac{1}{2}(q-1) \leqq k \leqq \tfrac{1}{2}(q-1) : (k^2+27)^{2(q-1)/3}(k+3+6w)^{2(q-1)/3} \equiv w \pmod q\}\,,$$

and, if $q \equiv 2 \pmod 3$,

$$(3.14)\qquad \mathscr{L} = \{-\tfrac{1}{2}(q-1) \leqq k \leqq \tfrac{1}{2}(q-1) : (k^2+27)^{(q-2)/3}(k+3+6w)^{(q+1)/3} \equiv w \pmod q\}\,,$$

where $w = \exp(2\pi i/3) = \frac{1}{2}(-1+\sqrt{-3})$. In particular, we have (see [15: p. 283])

$$\mathscr{L} = \{+1, -2\}\,, \quad \text{if} \quad q = 5\,,$$
$$\mathscr{L} = \{+2, -3\}\,, \quad \text{if} \quad q = 7\,,$$
$$\mathscr{L} = \{-1, -2, -3, +5\}\,, \quad \text{if} \quad q = 11\,.$$

Appealing to (3.3), (3.7), (3.8), (3.9), (3.11), and (3.12), we obtain

THEOREM 2. *Let p be a prime congruent to* 1 *modulo* 6 *and define L and M by* (3.1). *Let $q \geqq 5$ be an odd prime, which is a cubic nonresidue* (mod p). *Then*

$$\Phi_3(q) = \begin{cases} L-1\,, & \textit{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv M \pmod 4 \textit{ and} \\ & L \equiv -kM \pmod q \textit{ for some } k \in \mathscr{L}, \\ & \textit{or} \\ & L \equiv M \equiv 1 \pmod 2\,,\ L \equiv -M \pmod 4 \textit{ and} \\ & L \equiv kM \pmod q \textit{ for some } k \in \mathscr{L}, \\ \frac{1}{2}(-L+9M-2)\,, & \\ & \textit{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv -M \pmod 4 \textit{ and} \\ & L \equiv -kM \pmod q \textit{ for sone } k \in \mathscr{L}, \\ & \textit{or} \\ & L \equiv M \equiv 0 \pmod 2 \textit{ and } L \equiv kM \pmod q \\ & \textit{for some } k \in \mathscr{L}, \\ \frac{1}{2}(-L-9M-2)\,, & \\ & \textit{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv M \pmod 4 \textit{ and} \\ & L \equiv kM \pmod q \textit{ for some } k \in \mathscr{L}, \\ & \textit{or} \\ & L \equiv M \equiv 0 \pmod 2 \textit{ and } L \equiv -kM \pmod q \\ & \textit{for some } k \in \mathscr{L}. \end{cases}$$

We now treat the case $q = 3$. We have from [15: Theorem 1]

$$(3.15)\quad 3^{(p-1)/3} = \begin{cases} (L+9M)/(L-9M) \pmod p\,, & \text{if } M \equiv -1 \pmod 3\,, \\ (L-9M)/(L+9M) \pmod p\,, & \text{if } M \equiv 1 \pmod 3\,. \end{cases}$$

As in the proof of Theorem 2 we obtain

THEOREM 3. *Let p be a prime congruent to* 1 *modulo* 6, *for which* 3 *is a cubic nonresidue* (mod p). *Then*

$$\Phi_3(3) = \begin{cases} L-1\,, & \text{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv M \pmod 4 \text{ and} \\ & M \equiv 1 \pmod 3\,, \\ & \text{or} \\ & L \equiv M \equiv 1 \pmod 2\,,\ L \equiv -M \pmod 4 \text{ and} \\ & M \equiv -1 \pmod 3\,, \\ \frac{1}{2}(-L-9M-2)\,, & \\ & \text{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv M \pmod 4 \text{ and} \\ & M \equiv -1 \pmod 3\,, \\ & \text{or} \\ & L \equiv M \equiv 0 \pmod 2 \text{ and } M \equiv 1 \pmod 3\,, \\ \frac{1}{2}(-L+9M-2)\,, & \\ & \text{if } L \equiv M \equiv 1 \pmod 2\,,\ L \equiv -M \pmod 4 \text{ and} \\ & M \equiv 1 \pmod 3\,, \\ & \text{or} \\ & L \equiv M \equiv 0 \pmod 2 \text{ and } M \equiv -1 \pmod 3\,. \end{cases}$$

We remark that $\Phi_3(q^2)$, where q is a prime, which is a cubic nonresidue (mod p), is easily determined using Theorems 2 and 3 and the relation

$$(3.16)\qquad \Phi_3(1) + \Phi_3(q) + \Phi_3(q^2) = -3\,,$$

see for example [14: p. 92]. Moreover, as in § 2, we can treat $\Phi_3(D)$ for composite D.

Finally we remark that the ideas of this paper can be used in conjunction with results in [10], [11] and [16] to treat $\Phi_5(D)$ and $\Phi_7(D)$ for certain values of D.

REFERENCES

1. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory, **11** (1979), 349-398.
2. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc., **99** (1961), 241-245.
3. S. Chowla, *The last entry in Gauss's diary*, Proc. Nat. Acad. Sci. U.S.A., **35** (1949), 244-246.
4. T. Gosset, *On the law of quartic reciprocity*, Mess. Math., **41** (1911), 65-90.

5. R. H. Hudson and K. S. Williams, *An application of Western's formulae to the evaluation of certain Jacobsthal sums*, (to appear in Acta Arithmetica).

6. C. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math., **2** (1827), 66–69.

7. E. Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n+1$ *als Summe zweier Quadrate*, J. Reine Angew. Math., **132** (1907), 238–245.

8. Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod p$, Pacific J. Math., **5** (1955), 103–118.

9. ———, *Criteria for cubic and quartic residuacity*, Mathematika, **5** (1958), 20–29.

10. ———, *On Euler's criterion*, J. Austral. Math. Soc., **1** (1959), 64–70.

11. B. S. Nashier and A. R. Rajwade, *Determination of a unique solution of the quadratic partition for primes* $p \equiv 1 \pmod 7$, Pacific J. Math., **72** (1977), 513–521.

12. T. Pepin, *Mémoire sur les lois de reciprocité relatives aux résidus de puissances*, Accademia pontificia dei nuovi lincei. Atti, **31** (1878), 40–148.

13. L. von Schrutka, *Ein Beweis für die Zerlegbarkeit der Primzahlen der Form* $6n+1$ *in ein einfaches und ein dreifaches Quadrat*, J. Reine Angew. Math., **140** (1911), 252–265.

14. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math., **74** (1952), 89–99.

15. K. S. Williams, *On Euler's criterion for cubic nonresidues*, Proc. Amer. Math. Soc., **49** (1975), 277–283.

16. ———, *On Euler's criterion for quintic nonresidues*, Pacific J. Math., **61** (1975), 543–550.

Received February 15, 1980 and in revised form October 27, 1980. Research by the second author was supported by Natural Sciences and Engineering Research Council of Canada Grant No. A-7233.

UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SC 29208
AND
CARLETON UNIVERSITY
OTTAWA, ONTARIO CANADA KIS 5B6