PACIFIC JOURNAL OF MATHEMATICS
Vol. 110, No. 1, 1984

DETERMINATIONS OF JACOBSTHAL SUMS

RONALD J. EVANS

The sign ambiguities are resolved in evaluations of Jacobsthal sums $\Sigma_{m=1}^{p}(m(m^k + a)/p)$ for $k = 2, 3, 4, 6, 10$, and 12, where $(\ \ /p)$ denotes the Legendre symbol.

1. Introduction. For a positive even integer $e = 2n$, a prime $p = ef + 1$, and an integer a prime to p, define the Jacobsthal sum of order e by

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

where $(\ \ /p)$ denotes the Legendre symbol. In [**1**, §4], the values of Jacobsthal sums $\varphi_n(a)$ of orders $e = 4, 6, 8, 12, 20, 24$ are given up to some sign ambiguities. The purpose of this paper is to show how the precise values of $\varphi_n(a)$ can be found.

In §3, we give congruence conditions (mod p) which determine the correct choices of $\pm$ signs. The computational complexity of these determinations for large p is much less than that of computing $\varphi_n(a)$ directly from the definition.

In §4, we describe a method for determining the correct choices of $\pm$ signs by congruence conditions (mod a), when a is prime. If a is small compared with p, then the determinations in §4 (mod a) turn out to be computationally simpler than those in §3 (mod p).

The cases $e = 4, 6$ and $e = 8$ have already been treated by Hudson and Williams in [**2**] and [**3**], respectively. We employ different techniques based on Jacobi sums which work for all values $e = 4, 6, 8, 12, 20, 24$. Each of these values of e is considered in §3, but in §4, only the case $e = 12$ is treated, for brevity.

It will be convenient to introduce the notation $F_e(a)$ for the sum

$$F_e(a) = \sum_{m=1}^{p} \left(\frac{m(m^{e/2} - a)}{p} \right) = \varphi_n(-a). \tag{1}$$

An evaluation of $F_e(a)$ immediately yields one for $\varphi_n(a)$, since [**4**, (7)]

$$F_e(a) = \varphi_n(-a) = \varphi_n(a)(-1)^{fn+f}.$$

In the sequel, attention will be focused on $F_e(a)$.

2. Notation and Jacobi sums. For a character $\lambda \pmod p$, define the Jacobi sums

$$J(\lambda) = \sum_{m=1}^{p} \lambda(m)\lambda(1-m), \qquad K(\lambda) = \lambda(4)J(\lambda).$$

Write $p = ef + 1$. For each value of $e = 4, 6, 8, 12, 20, 24$, fix a character $\chi = \chi_e \pmod p$ of order e. Let P be the prime ideal divisor of p in $\mathbf{Z}[\exp(2\pi i/e)]$ chosen such that

$$\chi(\alpha) \equiv \alpha^{(p-1)/e} = \alpha^f \pmod P \tag{2}$$

for all $\alpha \in \mathbf{Z}[\exp(2\pi i/e)]$. It is easily seen that

$$K(\chi) \equiv 0 \pmod P. \tag{3}$$

In [**1**, §3] one finds the following evaluations of Jacobi sums $K(\chi)$ of orders $e = 4, 6, 8, 12, 20, 24$ in terms of parameters in quadratic partitions of p.

$$K(\chi_4) = a_4 + ib_4, \quad \text{where } p = a_4^2 + b_4^2,\ a_4 \equiv -(2/p) \pmod 4; \tag{4}$$

$$\left(\frac{-1}{p}\right) K(\chi_6) = K(\chi_6^2) = a_3 + ib_3\sqrt{3}, \tag{5}$$

$$\text{where } p = a_3^2 + 3b_3^2,\ a_3 \equiv -1 \pmod 3;$$

$$K(\chi_8) = a_8 + ib_8\sqrt{2}, \quad \text{where } p = a_8^2 + 2b_8^2,\ a_8 \equiv -1 \pmod 4; \tag{6}$$

$$K(\chi_{12}) = \begin{cases} -a_4 - ib_4, & \text{if } 3 \mid a_4, \\ a_4 + ib_4, & \text{if } 3 \nmid a_4, \end{cases} \tag{7}$$

where

$$K(\chi_{12}^3) = a_4 + ib_4 \quad \text{as in (4)};$$

$$K(\chi_{24}) = a_{24} + ib_{24}\sqrt{6}, \quad \text{where } p = a_{24}^2 + 6b_{24}^2, \tag{8}$$

$$a_{24} \equiv a_8 \pmod 3, \quad \text{with } K(\chi_{24}^3) = a_8 + ib_8\sqrt{2} \quad \text{as in (6)};$$

$$K(\chi_{20}) = \begin{cases} a_{20} + ib_{20}\sqrt{5}, & \text{if } 5 \nmid a_4, \\ ia_{20} - b_{20}\sqrt{5}, & \text{if } 5 \mid a_4, \end{cases} \tag{9}$$

where

$$p = a_{20}^2 + 5b_{20}^2 \quad \text{and} \quad a_{20} \equiv \begin{cases} a_4 \pmod 5, & \text{if } 5 \nmid a_4, \\ b_4 \pmod 5, & \text{if } 5 \mid a_4, \end{cases}$$

with $K(\chi_{20}^5) = a_4 + ib_4$ as in (4).

3. Congruence conditions (mod p). This section is to be read in conjunction with [**1**, §4]. We consider only those values of a for which the evaluations of $F_e(a)$ in [**1**, §4] have sign ambiguities, and we resolve these ambiguities with congruence conditions (mod p), for $e = 4, 6, 8, 12, 20, 24$.

Case 1. $e = 4$, $(a/p) = -1$.

The proof in [**1**, Theorem 4.4] shows that

$$F_4(a) = 2\,\mathrm{Re}(\bar{\chi}(a)K(\chi)) = -2b_4 i\chi(a) = \pm 2b_4. \tag{10}$$

To determine the correct sign, it remains to find $F_4(a)$ (mod p). By (3) and (4), $-ib_4 \equiv a_4$ (mod P). Thus by (10) and (2), $F_4(a) \equiv 2a_4a^f$ (mod P), so

$$F_4(a) \equiv 2a_4a^f \pmod{p}. \tag{11}$$

Remark. While it takes the computer $O(p)$ operations to compute $F_4(a)$ directly from the definition (1), it requires at most $O(\sqrt{p})$ operations to compute $F_4(a)$ from (10) and (11), since a^f (mod p) can be computed in $O(\log p)$ steps.

Case 2. $e = 6$, a is noncubic (mod p).

Write $\lambda = \chi_6^2$. Note that $\lambda(a) = (-1 \pm i\sqrt{3})/2$. The proof in [**1**, Theorem 4.2] shows that

$$\begin{aligned} F_6(a) &= -1 + 2\,\mathrm{Re}(\bar{\lambda}(a)K(\lambda)) \\ &= -1 - a_3 + 2b_3\sqrt{3}\,\mathrm{Im}\,\lambda(a) = -1 - a_3 \pm 3b_3. \end{aligned} \tag{12}$$

It remains to determine $F_6(a)$ (mod p). By (3) and (5), $a_3 \equiv -ib_3\sqrt{3}$ (mod P), so by (12) and (2),

$$F_6(a) \equiv a_3(a^{2f} - a^{4f}) - 1 - a_3 \equiv 2a_3a^{2f} - 1 \pmod{p}.$$

Case 3. $e = 8$, $(a/p) = -1$.

From the proof in [**1**, Theorem 4.6],

$$\begin{aligned} F_8(a) &= -2\,\mathrm{Re}\big(K(\chi)(\chi(a) + \chi^3(a))\big) \\ &= -2ib_8\sqrt{2}\,(\chi(a) + \chi^3(a)) = \pm 4b_8. \end{aligned} \tag{13}$$

Thus,

$$F_8(a) \equiv 2a_8(a^f + a^{3f}) \pmod{p}.$$

Case 4. $e = 12, (a/p) = -1$.

Subcase 4A. $3 \mid a_4$, a is cubic (mod p).

By [**1**, (4.3)],

$$(14) \qquad F_{12}(a) = 6\,\mathrm{Re}(\chi(a)(a_4 + ib_4)) = 6\chi(a)ib_4 = \pm 6b_4.$$

By (3) and (7), $a_4 \equiv -ib_4 \pmod P$, so

$$F_{12}(a) \equiv -6a_4 a^f \pmod p.$$

Subcase 4B. $3 \nmid a_4$.

By [**1**, (4.5)],

$$(15) \quad F_{12}(a) = 2b_4/\mathrm{Im}\,\chi(a)$$

$$= 4ib_4/(\chi(a) + \chi^5(a)) = \begin{cases} \pm 4b_4, & \text{if } a \text{ is noncubic} \pmod p \\ \pm 2b_4, & \text{if } a \text{ is cubic} \pmod p. \end{cases}$$

Thus,

$$F_{12}(a) \equiv -4a_4/(a^f + a^{5f}) \pmod p.$$

Case 5. $e = 24, (a/p) = -1$.

This case is slightly different than those above in that *two* congruence conditions are required to determine $F_{24}(a)$. From the proof in [**1**, Theorem 4.10],

$$F_{24}(a) = A_{24} + B_{24},$$

where

$$A_{24} = -2\,\mathrm{Re}\left(\left(a_8 + ib_8\sqrt{2}\right)(\chi^3(a) + \chi^9(a))\right)$$
$$= -2ib_8\sqrt{2}\,(\chi^3(a) + \chi^9(a)) = \pm 4b_8$$

and

$$B_{24} = -2\,\mathrm{Re}\left(\left(a_{24} + ib_{24}\sqrt{6}\right)(\chi(a) + \chi^5(a) + \chi^7(a) + \chi^{11}(a))\right)$$
$$= -2ib_{24}\sqrt{6}\,(\chi(a) + \chi^5(a) + \chi^7(a) + \chi^{11}(a))$$
$$= \begin{cases} \pm 12b_{24}, & \text{if } a \text{ is noncubic} \pmod p \\ 0, & \text{if } a \text{ is cubic} \pmod p. \end{cases}$$

It remains to determine A_{24} and B_{24} (mod p). Since $a_8 \equiv -ib_8\sqrt{2}$ and $a_{24} \equiv -ib_{24}\sqrt{6} \pmod P$, we have

$$A_{24} \equiv 2a_8(a^{3f} + a^{9f}) \pmod p$$

and

$$B_{24} \equiv 2a_{24}(a^f + a^{5f} + a^{7f} + a^{11f}) \pmod{p}.$$

Case 6. $e = 20$.

This case is similar to Case 5, so we omit some details. From the proof in [**1**, Theorem 4.13],

$$F_{20}(a) = A_{20} + B_{20},$$

where

$$A_{20} = 2\,\mathrm{Re}\{\chi^5(a)(a_4 - ib_4)\}$$

and

$$B_{20} = \begin{cases} 2\,\mathrm{Re}\left\{\left(\chi(a) - \chi^3(a) - \chi^7(a) + \chi^9(a)\right)\left(-ia_{20} - b_{20}\sqrt{5}\right)\right\}, & \text{if } 5 \mid a_4, \\ 2\,\mathrm{Re}\left\{\left(\chi(a) + \chi^3(a) + \chi^7(a) + \chi^9(a)\right)\left(a_{20} - ib_{20}\sqrt{5}\right)\right\}, & \text{if } 5 \nmid a_4. \end{cases}$$

It remains to determine A_{20} and B_{20} in each of the subcases below.

Subcase 6A. $5 \mid a_4$, $(a/p) = 1$, a nonquintic (mod p).

Here $A_{20} = \pm 2a_4$ and $B_{20} = \pm 10b_{20}$, with

$$A_{20} \equiv 2a_4 a^{5f} \pmod{p} \tag{16}$$

and

$$B_{20} \equiv 2(a^f - a^{3f} - a^{7f} + a^{9f})a_4 a_{20}/b_4 \pmod{p}. \tag{17}$$

Observe that there is no sign ambiguity in the right member of (17), since $a_{20}/b_4 \equiv 1 \pmod{5}$, as is noted after (9).

Subcase 6B. $5 \mid a_4$, $(a/p) = -1$.

Here,

$$A_{20} = \pm 2b_4 \quad \text{and} \quad B_{20} = \begin{cases} \pm 8a_{20}, & \text{if } a \text{ is quintic} \pmod{p} \\ \pm 2a_{20}, & \text{if } a \text{ is nonquintic} \pmod{p}, \end{cases}$$

with the congruences (16) and (17) again holding.

Subcase 6C. $5 \nmid a_4$, $(a/p) = -1$.
Here

$$A_{20} = \pm 2b_4 \quad \text{and} \quad B_{20} = \begin{cases} \pm 10b_{20}, & \text{if } a \text{ is nonquintic } (\text{mod } p) \\ 0, & \text{if } a \text{ is quintic } (\text{mod } p), \end{cases}$$

with (16) holding and

$$B_{20} \equiv 2a_{20}(a^f + a^{3f} + a^{7f} + a^{9f}) \pmod p.$$

4. Congruence conditions (mod a). Throughout this section, $e = 12$, $p = 12f + 1$, χ is a character (mod p) of order 12, $(a/p) = -1$, and a is prime. From (14) and (15),

$$F_{12}(a) = t \operatorname{Im} K(\chi^3)/\operatorname{Im} \chi(a) = tb_4/\operatorname{Im} \chi(a) = \pm hb_4 \tag{18}$$

where

$$K(\chi^3) = a_4 + ib_4 \tag{19}$$

and

$$\begin{aligned} h = t = -6, &\quad \text{if } 3 \mid a_4 \text{ and } a \text{ is cubic } (\text{mod } p), \\ h = t = 2, &\quad \text{if } 3 \nmid a_4 \text{ and } a \text{ is cubic } (\text{mod } p), \\ h = 4, t = 2, &\quad \text{if } 3 \nmid a_4 \text{ and } a \text{ is noncubic } (\text{mod } p). \end{aligned}$$

If the prime a is odd, then $a \nmid b_4$, otherwise we would have

$$p = a_4^2 + b_4^2 \equiv a_4^2 \pmod a,$$

which contradicts $(a/p) = -1$. Thus we can resolve the ambiguity in (18) by determining $F_{12}(a)$ (mod a), if $a > 3$. (Note $a \neq 3$, as $(a/p) = -1$.) For $a = 2$, we will resolve the ambiguity by determining $F_{12}(2)$ modulo an appropriate power of 2, in (20) and (21) below.

Case 1. $a = 2$.
It is classical [**4**, p. 107] that

$$b_4 \equiv -2i\chi^3(2) \pmod 8.$$

If 2 is a cubic residue (mod p), then

$$\frac{b_4}{\operatorname{Im} \chi(2)} = \frac{ib_4}{\chi(2)} \equiv \frac{2\chi^3(2)}{\chi(2)} = -2 \pmod 8,$$

so by (18),

$$F_{12}(2) \equiv -2t \equiv -4 \pmod{16}, \quad \text{if 2 is cubic } (\text{mod } p). \tag{20}$$

If $3 \nmid a_4$ and 2 is noncubic (mod p), then

$$F_{12}(2) = \frac{2b_4}{\operatorname{Im} \chi(2)} = \frac{4ib_4}{\chi(2) - \bar{\chi}(2)} \equiv \frac{8\chi^3(2)}{\chi(2) - \bar{\chi}(2)}$$
$$= \frac{8}{\chi^{10}(2) - \chi^8(2)} \pmod{32}.$$

Since $\chi^8(2) = (-1 \pm i\sqrt{3})/2$ and $\chi^{10}(2) = (1 \pm i\sqrt{3})/2$,

(21) $\quad F_{12}(2) \equiv 8 \pmod{32}, \quad$ if $3 \nmid a_4$ and 2 is noncubic (mod p).

Case 2. a is a prime > 3.

To determine $F_{12}(a)$ (mod a), it suffices, by (18), to determine

$$S(\chi) = \operatorname{Im} \chi(a)/b_4$$

modulo a. To do this, we need some formulas for Gauss sums $G(\psi)$, defined for characters ψ (mod p) by

$$G(\psi) = \sum_{n=1}^{p} \psi(n)\exp(2\pi in/p).$$

From [**1**, Theorems 2.2 and 3.1],

$$G(\chi)^{12} = pJ^4(\chi^4)K^6(\chi)$$

so by [**1**, Theorem 3.19],

(22) $$G(\chi)^{12} = pJ^4(\chi^4)K^6(\chi^3).$$

From [**1**, (3.28) and Theorems 2.2 and 3.1],

$$G^5(\chi)/G(\chi^5) = J^2(\chi^4)K^2(\chi),$$

so by [**1**, Theorem 3.19],

(23) $$G^5(\chi)/G(\chi^5) = J^2(\chi^4)K^2(\chi^3).$$

Here, as in [**1**, Theorem 3.4],

(24) $\quad 2J(\chi^4) = r_3 + 3it_3\sqrt{3}, \quad$ where $4p = r_3^2 + 27t_3^2$, $r_3 \equiv 1 \pmod 3$.

It is clear from the definition of $G(\chi)$ that, in the ring of algebraic integers,

(25) $$G^a(\chi) \equiv \bar{\chi}^a(a)G(\chi^a) \pmod a.$$

We will complete the proof by determining $S(\chi)$ (mod a) in (27)–(30) in terms of the parameters p, r_3, and a_4 unambiguously defined in (4) and (24).

Subcase 2A. $a \equiv 5 \pmod{12}$.

By (25) and (23),

$$\chi^7(a) \equiv G^{a-5}(\chi)G^5(\chi)/G(\chi^5) = G^{a-5}(\chi)J^2(\chi^4)K^2(\chi^3) \pmod{a}.$$

Thus, by (22),

$$\chi^7(a) \equiv p^{(a-5)/12}J^{(a+1)/3}(\chi^4)K^{(a-1)/2}(\chi^3) \pmod{a}.$$

Replacing χ by χ^7, we obtain

$$\chi(a) \equiv p^{(a-5)/12}J^{(a+1)/3}(\chi^4)K^{(a-1)/2}(\bar{\chi}^3) \pmod{a}. \tag{26}$$

Each member of (26) is a rational linear combination of 1, i, $\sqrt{3}$, $i\sqrt{3}$ by (19) and (24). The respective coefficients of i must be congruent (mod a). Since $\operatorname{Im}\chi(a)$ is rational, it follows that

$$\operatorname{Im}\chi(a) \equiv -p^{(a-5)/12}\operatorname{Re}J^{(a+1)/3}(\chi^4)\operatorname{Im}K^{(a-1)/2}(\chi^3) \pmod{a}$$

so

$$S(\chi) \equiv -p^{(a-5)/12}b_4^{-1}\operatorname{Re}J^{(a+1)/3}(\chi^4)\operatorname{Im}K^{(a-1)/2}(\chi^3) \pmod{a}. \tag{27}$$

For example, when $a = 5$, (27) yields

$$\begin{aligned} S(\chi) &\equiv (-4b_4)^{-1}\operatorname{Re}\left(r_3 + 3it_3\sqrt{3}\right)^2\operatorname{Im}(a_4 + ib_4)^2 \\ &\equiv 2a_4\left(r_3^2 - 27t_3^2\right) \pmod{5}. \end{aligned}$$

Subcase 2B. $a \equiv 7 \pmod{12}$.

By (25) and (23),

$$\begin{aligned} \chi^5(a) &\equiv G^{a+5}(\chi)\chi(-1)p^{-1}G(\chi^5)/G^5(\chi) \\ &\equiv G^{a+5}(\chi)\chi(-1)p^{-1}/\left(J^2(\chi^4)K^2(\chi^3)\right) \pmod{a}. \end{aligned}$$

Thus, by (22),

$$\chi^5(a) \equiv p^{(a-7)/12}\chi(-1)J^{(a-1)/3}(\chi^4)K^{(a+1)/2}(\chi^3) \pmod{a}.$$

Replacing χ by χ^5, we obtain

$$\chi(a) \equiv p^{(a-7)/12}(-1)^f J^{(a-1)/3}(\bar{\chi}^4)K^{(a+1)/2}(\chi^3) \pmod{a},$$

so

$$\begin{aligned} S(\chi) \equiv p^{(a-7)/12}(-1)^f &\operatorname{Re}J^{(a-1)/3}(\chi^4) \\ &\times\operatorname{Im}K^{(a+1)/2}(\chi^3)/b_4 \pmod{a}. \end{aligned} \tag{28}$$

For example, when $a = 7$, (28) yields

$$S(\chi) \equiv (-1)^f (4b_4)^{-1} \operatorname{Re}\left(r_3 + 3it_3\sqrt{3}\right)^2 \operatorname{Im}(a_4 + ib_4)^4$$
$$\equiv (-1)^f a_4 (r_3^2 - 27t_3^2)(2a_4^2 - p) \pmod 7.$$

Subcase 2C. $a \equiv 11 \pmod{12}$.
By (25) and (22),

$$\chi(a) \equiv p^{-1}\chi(-1)G^{a+1}(\chi)$$
$$\equiv p^{(a-11)/12}\chi(-1)J^{(a+1)/3}(\chi^4)K^{(a+1)/2}(\chi^3) \pmod a.$$

Thus,

$$S(\chi) \equiv p^{(a-11)/12}(-1)^f \operatorname{Re} J^{(a+1)/3}(\chi^4) \times \operatorname{Im} K^{(a+1)/2}(\chi^3)/b_4 \pmod a. \tag{29}$$

For example, when $a = 11$, (29) yields

$$S(\chi) = (-1)^f (16b_4)^{-1} \operatorname{Re}\left(r_3 + 3it_3\sqrt{3}\right)^4 \operatorname{Im}(a_4 + ib_4)^6$$
$$\equiv (-1)^f a_4 (3b_4^4 - 10a_4^2b_4^2 + 3a_4^4)(r_3^4 - 162r_3^2t_3^2 + 729t_3^4)/8$$
$$\equiv 7a_4(-1)^f (3b_4^4 + a_4^2b_4^2 + 3a_4^4)(r_3^4 + 3r_3^2t_3^2 + 3t_3^4) \pmod{11}.$$

Subcase 2D. $a \equiv 1 \pmod{12}$.
By (25) and (22),

$$\chi(a) \equiv G^{a-1}(\bar\chi) \equiv p^{(a-1)/12}J^{(a-1)/3}(\bar\chi^4)K^{(a-1)/2}(\bar\chi^3) \pmod a.$$

Thus,

$$S(\chi) \equiv -p^{(a-1)/12} \operatorname{Re} J^{(a-1)/3}(\chi^4) \operatorname{Im} K^{(a-1)/2}(\chi^3)/b_4 \pmod a. \tag{30}$$

For example, when $a = 13$, (30) yields

$$S(\chi) \equiv -p(16b_4)^{-1} \operatorname{Re}\left(r_3 + 3it_3\sqrt{3}\right)^4 \operatorname{Im}(a_4 + ib_4)^6$$
$$\equiv -pa_4(3b_4^4 - 10a_4^2b_4^2 + 3a_4^4)(r_3^4 - 162r_3^2t_3^2 + 729t_3^4)/8$$
$$\equiv -2pa_4(b_4^4 + a_4^2b_4^2 + a_4^4)(r_3^4 + 7r_3^2t_3^2 + t_3^4) \pmod{13}.$$

Numerical examples.

a	5	5	5	7	7	7	11	11	11	13	13	13
p	13	37	157	61	73	157	61	193	337	37	193	229
$F_{12}(a)$	12	24	-24	-24	48	-12	-12	24	-96	24	-24	12

References

[1] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory, **11** (1979), 349–398.

[2] R. H. Hudson and K. S. Williams, *Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums*, Pacific J. Math., **99** (1982), 379–386.

[3] ——, *An application of a formula of Western to the evaluation of certain Jacobsthal sums*, Acta Arith., (to appear).

[4] E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacific J. Math., **5** (1955), 103–118.

Received March 3, 1982 and in revised form June 7, 1982. Supported by NSF grant MCS 81-01860.

UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CA 92093