Pacific Journal of Mathematics

EXTENSIONS OF THEOREMS OF CUNNINGHAM-AIGNER AND HASSE-EVANS

Richard Howard Hudson and Kenneth S. Williams

Vol. 104, No. 1 May 1983

PACIFIC JOURNAL OF MATHEMATICS
Vol. 104, No. 1, 1983

EXTENSIONS OF THEOREMS OF CUNNINGHAM-AIGNER AND HASSE-EVANS

RICHARD H. HUDSON AND KENNETH S. WILLIAMS

If k is a positive integer and p is a prime with $p \equiv 1 \pmod{2^k}$, then $2^{(p-1)/2^k}$ is a 2^kth root of unity modulo p. We consider the problem of determining $2^{(p-1)/2^k}$ modulo p. This has been done for $k = 1, 2, 3$ and the present paper treats $k = 4$ and 5, extending the work of Cunningham, Aigner, Hasse, and Evans.

1. Introduction. When $k = 1$, we have the familiar result

$$(1.1)\qquad 2^{(p-1)/2} \equiv \begin{cases} +1 \pmod p, & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 \pmod p, & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

When $k = 2$ and $p \equiv 1 \pmod 4$, there are integers $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 2$ such that $p = a^2 + b^2$, with a and $|b|$ unique. If $b \equiv 0 \pmod 4$ (so that $p \equiv 1 \pmod 8$), Gauss [**8**: p. 89] (see also [**4**], [**16**]) has shown that

$$(1.2)\qquad 2^{(p-1)/4} \equiv \begin{cases} +1 \pmod p, & \text{if } b \equiv 0 \pmod 8, \\ -1 \pmod p, & \text{if } b \equiv 4 \pmod 8. \end{cases}$$

If $b \equiv 2 \pmod 4$ (so that $p \equiv 5 \pmod 8$), we can choose $b \equiv -2 \pmod 8$, by changing the sign of b, if necessary, and Gauss [**8**: p. 89] (see also [**4**], [**11**: p. 66], [**16**]) has shown that

$$(1.3)\qquad 2^{(p-1)/4} \equiv -b/a \pmod p.$$

We note that $(-b/a)^2 \equiv -1 \pmod p$.

When $k = 3$ and $p \equiv 1 \pmod 8$, there are integers $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ such that $p = a^2 + b^2$, with a and $|b|$ unique. Now $\{2^{(p-1)/8}\}^4 = 2^{(p-1)/2} \equiv 1 \pmod p$, as $p \equiv 1 \pmod 8$, so $2^{(p-1)/8}$ is a 4th root of unity modulo p. If $b \equiv 0 \pmod 8$, Reuschle [**14**] conjectured and Western [**15**] (see also [**16**]) proved that

$$(1.4)\qquad 2^{(p-1)/8} \equiv \begin{cases} (-1)^{(p-1)/8} \pmod p, & \text{if } b \equiv 0 \pmod{16}, \\ (-1)^{(p+7)/8} \pmod p, & \text{if } b \equiv 8 \pmod{16}. \end{cases}$$

If $b \equiv 4 \pmod 8$, we can choose $b \equiv 4(-1)^{(p+7)/8} \pmod{16}$, by changing the sign of b, if necessary, and Lehmer [**11**: p. 70] has shown that

$$(1.5)\qquad 2^{(p-1)/8} \equiv -\frac{b}{a} \pmod p.$$

It is the purpose of this paper to treat the cases $k = 4$ and 5. For $k = 4$ and $p \equiv 1 \pmod{16}$, there are integers $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, $c \equiv 1 \pmod 4$, $d \equiv 0 \pmod 2$, such that $p = a^2 + b^2 = c^2 + 2d^2$, with a, $|b|$, c, $|d|$ unique. Now $\{2^{(p-1)/16}\}^8 = 2^{(p-1)/2} \equiv 1 \pmod p$, so $2^{(p-1)/16}$ is an 8th root of unity modulo p. Since

$$(1.6) \qquad \left\{\frac{-(a+b)d}{ac}\right\}^2 \equiv -b/a \pmod p,$$

the 8th roots of unity $\pmod p$ are given by $\{-(a+b)d/ac\}^n$, $n = 0, 1, \ldots, 7$. Making use of a congruence due to Hasse [**9**: p. 232] (see also [**5**: Theorem 3], [**17**: p. 411]), we prove in §2 the following extension of the criterion for 2 to be a 16th power $\pmod p$, which was conjectured by Cunningham [**3**: p. 88] and first proved by Aigner [**1**] (see also [**16**: p. 373]).

THEOREM 1. *Let $p \equiv 1 \pmod{16}$ be a prime. Let $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, $c \equiv 1 \pmod 4$, $d \equiv 0 \pmod 2$ be integers such that $p = a^2 + b^2 = c^2 + 2d^2$. It is well known that $b \equiv 0 \pmod 8 \Leftrightarrow d \equiv 0 \pmod 4$ (see for example* [**2**: p. 68]). *Then the values of $2^{(p-1)/16} \pmod p$ are given in Table* 1.

The case $b \equiv 0 \pmod{16}$ constitutes the criterion of Cunningham-Aigner.

For $k = 5$ and $p \equiv 1 \pmod{32}$, there are integers $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, $c \equiv 1 \pmod 4$, $d \equiv 0 \pmod 2$, $x \equiv -1 \pmod 8$, $u \equiv v \equiv w \equiv 0 \pmod 2$, such that $p = a^2 + b^2 = c^2 + 2d^2$ and

$$(1.7) \qquad \begin{cases} p = x^2 + 2u^2 + 2v^2 + 2w^2, \\ 2xv = u^2 - 2uw - w^2, \end{cases}$$

with a, $|b|$, c, $|d|$, x unique. If (x, u, v, w) is a solution of (1.7), then all solutions are given by $\pm(x, u, v, w)$, $\pm(x, -u, v, -w)$, $\pm(x, w, -v, -u)$, $\pm(x, -w, -v, u)$ (see for example [**12**: p. 366]). Now $\{2^{(p-1)/32}\}^{16} = 2^{(p-1)/2} \equiv +1 \pmod p$, so $2^{(p-1)/32}$ is a 16th root of unity modulo p. Since

$$(1.8) \qquad \left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^2 \equiv \frac{-(a+b)d}{ac} \pmod p,$$

the 16th roots of unity $\pmod p$ are given by

$$\left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^n, \qquad n = 0, 1, \ldots, 15.$$

Making use of another congruence due to Hasse [**9**: p. 233] (see also [**7**: eqn. (2)]), we prove in §3 the following extension of the criterion for 2 to be a 32nd power (mod p) due to Hasse [**9**: p. 232–238] and Evans [**6**: Theorem 7].

THEOREM 2. *Let* $p \equiv 1 \pmod{32}$ *be a prime. Let* $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, $c \equiv 1 \pmod 4$, $d \equiv 0 \pmod 2$, $x \equiv -1 \pmod 8$, $u \equiv v \equiv w \equiv 0 \pmod 2$, *be integers such that* $p = a^2 + b^2 = c^2 + 2d^2$ *and* $p = x^2 + 2u^2 + 2v^2 + 2w^2$, $2xv = u^2 - 2uw - w^2$. *Then the values* $2^{(p-1)/32} \pmod p$ *are given in Table* 2.

Justification of the choices in the left-hand column of Table 2 is made in the proof of Theorem 2, which appears in §3. The cases $2^{(p-1)/32} \equiv \pm 1 \pmod p$ constitute the criterion of Hasse-Evans.

2. Evaluation of $2^{(p-1)/16} \pmod p$.

Let p be a prime satisfying

(2.1) $$p \equiv 1 \pmod{16}.$$

Set

(2.2) $$p = 8f + 1,$$

so that

(2.3) $$f \equiv 0 \pmod 2.$$

Let

(2.4) $$\omega = \exp(2\pi i/8) = (1+i)/\sqrt{2}.$$

We note that the ring of integers of $Q(\omega) = Q(i, \sqrt{2})$ is a unique factorization domain (see for example [**13**]). In this ring p factors as a product of four primes. Denoting one of these by π, these four primes are $\pi_j = \sigma_j(\pi)$, $j = 1, 3, 5, 7$, where σ_j denotes the automorphism which maps ω to ω^j.

Let g be a primitive root (mod p). Then $g^{(p-1)/2} \equiv -1 \pmod p$, and so

$$(g^f - \omega)(g^f - \omega^3)(g^f - \omega^5)(g^f - \omega^7) \equiv 0 \pmod{\pi_1\pi_3\pi_5\pi_7}.$$

Hence

$$g^f - \omega^j \equiv 0 \pmod{\pi_1},$$

for some j, $j = 1, 3, 5, 7$, and by relabelling the π's we may assume without loss of generality that

(2.5) $$g^f \equiv \omega \pmod{\pi}.$$

Given g, π (apart from units) is uniquely determined by (2.5). Next we define a character $\chi \pmod p$ (depending upon g) of order 8 by setting

(2.6) $$\chi(g) = \omega.$$

For $r, s = 0, 1, 2, \ldots, 7$ the Jacobi sum $J(r, s)$ is defined by

(2.7) $$J(r, s) = \sum_{n \,(\mathrm{mod}\, p)} \chi^r(n)\chi^s(1-n).$$

It is known that (see for example [7: §1])

(2.8) $$J(2,2) = -a + bi,$$

where

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

and that

(2.10) $$J(1,3) = -c + di\sqrt{2},$$

where

(2.11) $$p = c^2 + 2d^2, \quad c \equiv 1 \pmod 4.$$

It is easy to check that replacing the primitive root g by the primitive root g^{8s+t}, where $t = 1, 3, 5, 7$ and $(8s+t, f) = 1$, has the effect in (2.8) of replacing b by $(-1/t)b$ and in (2.10) of replacing d by $(-2/t)d$.

Our proof depends upon the following important congruence due to Hasse [**9**: p. 232]

(2.12) $$b \equiv 4d + 2m \pmod{32},$$

where m is the least positive integer such that

(2.13) $$g^m \equiv 2 \pmod p,$$

and b and d are given by (2.8) and (2.10) respectively. From (2.12) and (2.13) we obtain

(2.14) $$2^{(p-1)/16} = 2^{f/2} \equiv g^{mf/2} \equiv g^{f(b/4-d)} \pmod p.$$

It follows from (2.5) and (2.6) that

(2.15) $$\chi(n) \equiv n^f \pmod \pi,$$

for any integer n not divisible by p. Hence, for non-negative integers r and s satisfying $0 \le r + s < 8$, we have

$$\begin{aligned} J(r,s) &\equiv \sum_{n=0}^{p-1} n^{rf}(1-n)^{sf} \pmod \pi \\ &\equiv \sum_{n=0}^{p-1} n^{rf} \sum_{j=0}^{sf} \binom{sf}{j} (-1)^j n^j \pmod \pi \\ &\equiv \sum_{j=0}^{sf} \binom{sf}{j} (-1)^j \sum_{n=0}^{p-1} n^{rf+j} \pmod \pi, \end{aligned}$$

that is

(2.16) $$J(r, s) \equiv 0 \pmod{\pi},$$

as

(2.17) $$\sum_{n=0}^{p-1} n^k \equiv 0 \pmod{p}, \text{ for } k = 0, 1, \ldots, p-2.$$

Taking $(r, s) = (2, 2)$ and $(1, 3)$ in (2.16), we have, by (2.8) and (2.10),

(2.18) $$i \equiv a/b \pmod{\pi}, \; i\sqrt{2} \equiv c/d \pmod{\pi},$$

so that

(2.19) $$\sqrt{2} \equiv -ac/bd \pmod{\pi}.$$

Hence we have, appealing to (2.5), (2.18) and (2.19),

$$g^f \equiv \omega = \frac{1+i}{\sqrt{2}} \equiv -\frac{(a+b)d}{ac} \pmod{\pi},$$

and, since g^f and $-(a+b)d/ac$ are integers $\pmod{p}$, we have

(2.20) $$g^f \equiv -\frac{(a+b)d}{ac} \pmod{p}.$$

Appealing to (2.14) we get

(2.21) $$2^{(p-1)/16} \equiv \left\{ \frac{-(a+b)d}{ac} \right\}^{(b/4)-d} \pmod{p}.$$

We consider three cases:

(i) $2^{(p-1)/4} \equiv -1 \pmod{p}$,
(ii) $2^{(p-1)/4} \equiv +1$, $2^{(p-1)/8} \equiv -1 \pmod{p}$,
(iii) $2^{(p-1)/8} \equiv +1 \pmod{p}$.

Case (i). From (1.2) we have $b \equiv 4 \pmod{8}$. Then, from $p = a^2 + b^2$, we obtain $a \equiv 1 \pmod{8}$ and $p \equiv 2a + 15 \pmod{32}$. The cyclotomic number $(0, 7)_8$ is given by (see for example [**10**: p. 116])

$$64(0,7)_8 = p - 7 + 2a + 4c,$$

so $c \equiv 5 \pmod{8}$. Then, from $p = c^2 + 2d^2$, we get $d \equiv 2 \pmod{4}$. Replacing g by an appropriate primitive root

$$g^{8s+t} \; (t = 1, 3, 5, 7; \; (8s + t, f) = 1)$$

we may take $b \equiv -4 \equiv 12 \pmod{16}$ and $d \equiv 2 \pmod 8$. Then, from (2.21), we obtain

$$2^{(p-1)/16} \equiv \begin{cases} -\dfrac{(a+b)d}{ac} \pmod p, & \text{if } b \equiv 12 \pmod{32}, \\ +\dfrac{(a+b)d}{ac} \pmod p, & \text{if } b \equiv 28 \pmod{32}. \end{cases}$$

Case (ii). From (1.2) and (1.4) we have $b \equiv 8 \pmod{16}$. Then, from $p = a^2 + b^2$, we obtain $a \equiv 1 \pmod 8$ and $p \equiv 2a - 1 \pmod{32}$. The cyclotomic number $(1,2)_8$ is given by (see for example [**10**: p. 116])

$$64\,(1,2)_8 = p + 1 + 2a - 4c,$$

so $c \equiv 1 \pmod 8$. Then, from $p = c^2 + 2d^2$, we get $d \equiv 0 \pmod 4$. Replacing g by an appropriate primitive root

$$g^{8s+t}\ (t = 1, 3;\ (8s + t, f) = 1)$$

we may take $b \equiv 8 \pmod{32}$. Then as

$$\left\{\frac{-(a+b)d}{ac}\right\}^2 \equiv \frac{-b}{a} \pmod p,$$

we have from (2.21)

$$2^{(p-1)/16} \equiv \begin{cases} -b/a \pmod p, & \text{if } d \equiv 0 \pmod 8, \\ +b/a \pmod p, & \text{if } d \equiv 4 \pmod 8. \end{cases}$$

Case (iii). From (1.4) we have $b \equiv 0 \pmod{16}$. Exactly as in Case (ii) we have $d \equiv 0 \pmod 4$. Considering four cases according as $b \equiv 0, 16 \pmod{32}$ and $d \equiv 0, 4 \pmod 8$ we obtain from (2.21)

$$2^{(p-1)/16} \equiv \begin{cases} +1 \pmod p, & \text{if } b \equiv 0 \pmod{32}, \quad d \equiv 0 \pmod 8 \\ & \text{or} \\ & \phantom{\text{if }} b \equiv 16 \pmod{32}, \quad d \equiv 4 \pmod 8, \\ -1 \pmod p, & \text{if } b \equiv 0 \pmod{32}, \quad d \equiv 4 \pmod 8 \\ & \text{or} \\ & \phantom{\text{if }} b \equiv 16 \pmod{32}, \quad d \equiv 0 \pmod 8. \end{cases}$$

This completes the proof of Theorem 1.

3. Evaluation of $2^{(p-1)/32} \pmod p$. Let p be a prime satisfying

(3.1) $$p \equiv 1 \pmod{32}.$$

Set

(3.2) $$p = 16f + 1,$$

so that

(3.3) $$f \equiv 0 \pmod 2.$$

Let

(3.4) $$\theta = \exp(2\pi i/16) = \tfrac{1}{2}\left\{\sqrt{2+\sqrt{2}} + i\sqrt{2-\sqrt{2}}\right\}.$$

Again, the ring of integers of $Q(\theta)$ is a unique factorization domain (see for example [**13**]). In this ring p factors as a product of eight primes. Denoting one of these by π, these eight primes are given by $\pi_i = \sigma_i(\pi)$, $i = 1, 3, 5, 7, 9, 11, 13, 15$, where σ_i denotes the automorphism which maps θ to θ^i.

Let g be a primitive root (mod p). Then

$$(g^f - \theta)(g^f - \theta^3) \cdots (g^f - \theta^{15}) \equiv 0 \pmod{\pi_1\pi_3 \cdots \pi_{15}},$$

and, as before, we can choose $\pi_1 = \pi$ (unique apart from units) so that

(3.5) $$g^f \equiv \theta \pmod{\pi}.$$

We define a character Ψ (mod p) of order 16 by setting

(3.6) $$\Psi(g) = \theta,$$

and for $r, s = 0, 1, 2, \ldots, 15$ we define the Jacobi sum $J(r, s)$ by

(3.7) $$J(r, s) = \sum_{n \pmod p} \psi^r(n)\psi^s(1-n).$$

It is known that (see for example [**7**: §1])

(3.8) $J(4,4) = -a + bi,$ where $p = a^2 + b^2,\quad a \equiv 1 \pmod 4,$

(3.9) $J(2,6) = -c + di\sqrt{2},$ where $p = c^2 + 2d^2,\quad c \equiv 1 \pmod 4,$

and

(3.10) $$\begin{aligned} J(1,7) &= x + ui\sqrt{2-\sqrt{2}} + v\sqrt{2} + wi\sqrt{2+\sqrt{2}} \\ &= x + u(\theta + \theta^7) + v(\theta^2 - \theta^6) + w(\theta^3 + \theta^5), \end{aligned}$$

where (see for example [**5**; eqn. (8)])

(3.11) $$\begin{cases} p = x^2 + 2u^2 + 2v^2 + 2w^2, & x \equiv -1 \pmod 8, \\ 2xv = u^2 - 2uw - w^2. \end{cases}$$

It is easy to check that u, v and w are all even. Applying the mapping $\theta \to \theta^3$ to (3.10), we obtain

$$(3.12)\qquad \begin{aligned} J(3,5) &= x - wi\sqrt{2-\sqrt{2}} - v\sqrt{2} + ui\sqrt{2+\sqrt{2}} \\ &= x - w(\theta+\theta^7) - v(\theta^2-\theta^6) + u(\theta^3+\theta^5). \end{aligned}$$

Further, it is known (see [**12**: p. 366] and [**6**: eqn. (48)]) that a, b, c, d, x, u, v, w are related by

$$(3.13)\qquad bd(x^2-2v^2) \equiv ac(u^2+2uw-w^2) \pmod{p}.$$

The effect on (3.8), (3.9), (3.10) of replacing the primitive root g by the primitive root g^{16s+t}, where $t = 1, 3, 5, \ldots, 15$ and $(16s+t, f) = 1$, is summarized below:

(3.14)

g	a	b	c	d	x	u	v	w
g^{16s+3}	a	$-b$	c	d	x	w	$-v$	$-u$
g^{16s+5}	a	b	c	$-d$	x	w	$-v$	$-u$
g^{16s+7}	a	$-b$	c	$-d$	x	u	v	w
g^{16s+9}	a	b	c	d	x	$-u$	v	$-w$
g^{16s+11}	a	$-b$	c	d	x	$-w$	$-v$	u
g^{16s+13}	a	b	c	$-d$	x	$-w$	$-v$	u
g^{16s+15}	a	$-b$	c	$-d$	x	$-u$	v	$-w$

The following important congruence relating b, d, u and w has been proved by Hasse [**9**: p. 233]

$$(3.15)\qquad b + 4d - 8(u+w) \equiv 2m \pmod{64},$$

where m satisfies (2.13). From (2.13) and (3.15), we obtain

$$(3.16)\qquad 2^{(p-1)/32} = 2^{f/2} \equiv g^{mf/2} \equiv g^{f((b/4)+d-2(u+w))} \pmod{p}.$$

As in §2, if r and s are non-negative integers satisfying $0 \le r+s < 16$, we have

$$(3.17)\qquad J(r,s) \equiv 0 \pmod{\pi}.$$

Thus, in particular, taking $(r,s) = (4,4), (2,6), (1,7)$, and $(3,5)$, in (3.17), we obtain

$$(3.18)\qquad -a + bi \equiv 0 \pmod{\pi},$$

$$(3.19)\qquad -c + di\sqrt{2} \equiv 0 \pmod{\pi},$$

$$(3.20)\qquad x + ui\sqrt{2-\sqrt{2}} + v\sqrt{2} + wi\sqrt{2+\sqrt{2}} \equiv 0 \pmod{\pi},$$

$$(3.21)\qquad x - wi\sqrt{2-\sqrt{2}} - v\sqrt{2} + ui\sqrt{2+\sqrt{2}} \equiv 0 \pmod{\pi}.$$

From (3.18) and (3.19) we get

$$(3.22) \qquad i \equiv a/b \pmod{\pi}, \quad i\sqrt{2} \equiv c/d \pmod{\pi},$$

$$\sqrt{2} \equiv -\frac{ac}{bd} \pmod{\pi}.$$

Solving (3.20) and (3.21) simultaneously for $\sqrt{2+\sqrt{2}}$ and $\sqrt{2-\sqrt{2}}$ $(\mathrm{mod}\ \pi)$, and making use of (3.22), we obtain

$$(3.23) \qquad \sqrt{2 \pm \sqrt{2}} \equiv \frac{x(u \pm w)ad \mp v(u \mp w)bc}{bd(u^2 + w^2)} \pmod{\pi}.$$

Then, from (3.4), (3.5), (3.22) and (3.23), we have

$$(3.24) \qquad g^f \equiv \theta \equiv \frac{(dx + cv)(a(u+w) - b(u-w))}{2bd(u^2 + w^2)} \pmod{\pi}.$$

Since both sides of (3.24) are integers $(\mathrm{mod}\ p)$, we deduce that

$$(3.25) \qquad g^f \equiv \frac{(dx + cv)(a(u+w) - b(u-w))}{2bd(u^2 + w^2)} \pmod{p}.$$

Appealing to (3.16) we get

$$(3.26) \quad 2^{(p-1)/32} \equiv \left\{ \frac{(dx + cv)(a(u+w) - b(u-w))}{2bd(u^2 + w^2)} \right\}^{(b/4)+d-2(u+w)} \pmod{p}.$$

We consider four cases:

(i) $2^{(p-1)/4} \equiv -1 \pmod{p}$,
(ii) $2^{(p-1)/4} \equiv +1$, $2^{(p-1)/8} \equiv -1 \pmod{p}$,
(iii) $2^{(p-1)/8} \equiv +1$, $2^{(p-1)/16} \equiv -1 \pmod{p}$,
(iv) $2^{(p-1)/16} \equiv +1 \pmod{p}$.

Case (i). From Case (i) of §2 we have $b \equiv 4 \pmod{8}$ and $d \equiv 2 \pmod{4}$. Next, from (2.12) and (3.15), we obtain

$$u + w \equiv d \equiv 2 \pmod{4},$$

so that

$$(u, w) \equiv (0, 2) \quad \text{or} \quad (2, 0) \pmod{4}.$$

Replacing g by an appropriate primitive root g^{16s+t} (where $t = 1, 3, 5, \ldots, 15$ and $(16s + t, f) = 1$), we can suppose that

$$(3.27) \qquad b \equiv -4 \pmod{16}, \quad u \equiv 0 \pmod{4}, \quad w \equiv 2 \pmod{8}.$$

Exactly one 5-tuple (b, d, u, v, w) satisfies (3.13) and (3.27). Then, from $2xv = u^2 - 2uw - w^2$, we obtain (recalling $x \equiv -1 \pmod 8$)

$$(3.28) \qquad v \equiv 2 \pmod 8.$$

From the work of Evans and Hill [7: Table 2a], we have

$$(3.29) \qquad 256\{(2,4)_{16} - (4,10)_{16}\} = 32(v - d),$$

so that, by (3.28),

$$(3.30) \qquad d \equiv v \equiv 2 \pmod 8.$$

The choice (3.27) makes the exponent $(b/4) + d - 2(u + w)$ in (3.26) congruent to 1 (mod 4). We now consider cases according as $b \equiv 12, 28, 44, 60 \pmod{64}$; $d \equiv 2, 10 \pmod{16}$; $u \equiv 0, 4 \pmod 8$. For example, if $b \equiv 12 \pmod{64}$, $d \equiv 2 \pmod{16}$, $u \equiv 0 \pmod 8$, then $(b/4) + d - 2(u + w) \equiv 1 \pmod{16}$, so that (3.26) gives

$$(3.31) \qquad 2^{(p-1)/32} \equiv \frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)} \pmod p,$$

in this case. The other cases can be treated similarly, see Table 2 (VII).

Case (ii). From Case (ii) of §2, we have $b \equiv 8 \pmod{16}$ and $d \equiv 0 \pmod 4$. Appealing to the work of Evans [5: Theorem 4 and its proof], we have

$$(3.32) \qquad u \equiv 2 \pmod 4, \quad v \equiv 4 \pmod 8, \quad w \equiv 2 \pmod 4, \quad \text{if } d \equiv 0 \pmod 8,$$

and

$$(3.33) \qquad u \equiv 0 \pmod 4, \quad v \equiv 0 \pmod 8, \quad w \equiv 0 \pmod 4, \quad \text{if } d \equiv 4 \pmod 8.$$

If $d \equiv 0 \pmod 8$, replacing g by g^{16s+t} (where $t = 1, 7, 9, 15$ and $(16s + t, f) = 1$), as necessary, we can suppose that

$$(3.34) \qquad b \equiv 8 \pmod{32}, \qquad w \equiv 2 \pmod 8.$$

There are exactly two 5-tuples (b, d, u, v, w), which satisfy (3.13) and (3.34). These are

$$(b, d, u, v, w) \quad \text{and} \quad (b, -d, -w, -v, u), \quad \text{if } u \equiv 2 \pmod 8,$$

and

$$(b, d, u, v, w) \quad \text{and} \quad (b, -d, w, -v, -u), \quad \text{if } u \equiv 6 \pmod 8.$$

We note that the 16th root of unity modulo p,

$$\left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^{b/4+d-2(u+w)},$$

is independent of which 5-tuple is used, since

$$\left\{\frac{((-d)x+c(-v))(a(\mp w\pm u)-b(\mp w\mp u))}{2b(-d)((\mp w)^2+(\pm u)^2)}\right\}^{(b/4)-d-2(\mp w\pm u)}$$
$$=\left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^{A},$$

where

$$A=\begin{cases}13\left(\dfrac{b}{4}-d-2u+2w\right), & \text{if } u\equiv 2 \pmod 8,\\ 5\left(\dfrac{b}{4}-d+2u-2w\right), & \text{if } u\equiv 6 \pmod 8;\end{cases}$$

moreover,

$$13\left(\frac{b}{4}-d-2u+2w\right)-\left(\frac{b}{4}+d-2u-2w\right)$$
$$=3b-14d-24u+28w\equiv 0 \pmod{16},$$
$$5\left(\frac{b}{4}-d+2u-2w\right)-\left(\frac{b}{4}+d-2u-2w\right)$$
$$=b-6d+12u-8w\equiv 0 \pmod{16},$$

so that

$$A\equiv\frac{b}{4}+d-2(u+w) \pmod{16}.$$

The choice (3.34) makes the exponent $(b/4)+d-2(u+w)$ in (3.26) congruent to 2 (mod 8). We now consider cases according as $b\equiv 8, 40 \pmod{64}$; $d\equiv 0, 8 \pmod{16}$; $u\equiv 2, 6 \pmod 8$. For example if $b\equiv 8 \pmod{64}$, $d\equiv 0 \pmod{16}$, $u\equiv 6 \pmod 8$, then $(b/4)+d-2(u+w)\equiv 2 \pmod{16}$, so (3.26) gives

$$\text{(3.35)}\quad 2^{(p-1)/32}\equiv\left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^2 \pmod p$$
$$\equiv\frac{-(a+b)d}{ac} \pmod p,$$

see Table 2(VI). We remark that in applying Theorem 2 in this case, d must be chosen to satisfy the congruence (3.13). We can do this as $x^2 - 2v^2 \not\equiv 0 \pmod p$, since

$$-p = -x^2 - 2u^2 - 2v^2 - 2w^2 < x^2 - 2v^2 \leq x^2 < p.$$

If $d \equiv 4 \pmod 8$, replacing g by g^{16s+t} (where $t = 1, 3, 5$ or 7 and $(16s + t, f) = 1$), as necessary, we can suppose that

$$\text{(3.36)} \qquad b \equiv -8 \equiv 24 \pmod{32}, \qquad d \equiv 4 \pmod{16}.$$

There are precisely two 5-tuples (b, d, u, v, w), which satisfy (3.13) and (3.36). These are

$$(b, d, u, v, w) \quad \text{and} \quad (b, d, -u, v, -w).$$

We note that the 16th root of unity modulo p,

$$\left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^{(b/4)+d-2(u+w)}$$

is independent of which 5-tuple is chosen, since

$$\left\{\frac{(dx + cv)(a(-u - w) - b(-u + w))}{2bd((-u)^2 + (-w)^2)}\right\}^{(b/4)+d-2(-u-w)}$$
$$= \left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^{B},$$

where

$$B = 9\left(\frac{b}{4} + d + 2u + 2w\right) \equiv \frac{b}{4} + d - 2(u + w) \pmod{16}.$$

The choice (3.36) makes the component $(b/4) + d - 2(u + w)$ in (3.26) congruent to 2 (mod 8). We now consider cases according as $b \equiv 24, 56 \pmod{64}$; $u + w \equiv 0, 4 \pmod 8$. For example, if $b \equiv 56 \pmod{64}$, $u + w \equiv 4 \pmod 8$, then $(b/4) + d - 2(u + w) \equiv 10 \pmod{16}$, so (3.26) gives

$$\text{(3.37)} \quad 2^{(p-1)/32} \equiv \left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^{10} \pmod p$$
$$\equiv \left\{\frac{-(a + b)d}{ac}\right\}^{5} \pmod p$$
$$\equiv \frac{+(a + b)d}{ac} \pmod p,$$

see Table 2(V). However, when applying Theorem 2 in this case, it is not necessary to use the congruence $bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$ to distinguish the solutions $(x, \pm u, v, \pm w)$ from the solutions $(x, \pm w, -v, \mp u)$. since $\pm w \mp u \equiv \pm(u + w) \pmod 8$, as $u \equiv w \equiv 0 \pmod 4$.

Case (iii) From Case (iii) of §2 we have

$$b \equiv 0 \pmod{32}, \qquad d \equiv 4 \pmod 8, \tag{3.38}$$

or

$$b \equiv 16 \pmod{32}, \qquad d \equiv 0 \pmod 8. \tag{3.39}$$

If $b \equiv 0 \pmod{32}$, $d \equiv 4 \pmod 8$, from the work of Evans [**5**: Theorem 4 and its proof], we have

$$u \equiv 2 \pmod 4, \quad v \equiv 4 \pmod 8, w \equiv 2 \pmod 4. \tag{3.40}$$

Replacing g by g^{16s+t}, where $t = 1, 7, 9$ or 15 and $(16s + t, f) = 1$, as necessary, we can suppose that

$$d \equiv 4 \pmod{16}, w \equiv 2 \pmod 8. \tag{3.41}$$

There are exactly two 5-tuples (b, d, u, v, w) which satisfy (3.13) and (3.41). These are

$$(b, d, u, v, w) \quad \text{and} \quad (-b, d, -w, -v, u), \quad \text{if } u \equiv 2 \pmod 8,$$

and

$$(b, d, u, v, w) \quad \text{and} \quad (-b, d, w, -v, -u), \quad \text{if } u \equiv 6 \pmod 8.$$

We note that the 16th root of unity modulo p,

$$\left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^{(b/4)+d-2(u+w)}$$

is independent of which 5-tuple is used, since

$$\left\{\frac{(dx + c(-v))(a(\mp w \pm u) + b(\mp w \mp u))}{2(-b)d((\mp w)^2 + (\mp u)^2))}\right\}^{(-b/4)+d-2(\mp w \pm u)}$$
$$= \left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^C,$$

where

$$C = \begin{cases} 11\left(-\dfrac{b}{4} + d - 2u + 2w\right), & \text{if } u \equiv 2 \pmod 8, \\ 3\left(-\dfrac{b}{4} + d + 2u - 2w\right), & \text{if } u \equiv 6 \pmod 8, \end{cases}$$

and it is easily checked that

$$C \equiv \frac{b}{4} + d - 2(u + w) \pmod{16}.$$

Clearly, from (3.38) and (3.40), we have $(b/4) + d - 2(u + w) \equiv 4 \pmod 8$, and we determine $(b/4) + d - 2(u + w) \pmod{16}$ by considering the cases $b \equiv 0, 32 \pmod{64}$ and $u \equiv 2, 6 \pmod 8$. For example, if $b \equiv 0 \pmod{64}$ and $u \equiv 6 \pmod 8$, we have $(b/4) + d - 2(u + w) \equiv 4 \pmod{16}$, so by (3.26), (1.6) and (1.8),

$$(3.42) \qquad 2^{(p-1)/32} \equiv \left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^4 \equiv -\frac{b}{a} \pmod p,$$

see Table 2 (III). In applying Theorem 2 in this case we must use the congruence $bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$ to distinguish the solutions $(x, \pm u, v, \pm w)$ from the solutions $(x, \mp w, -v, \pm u)$.

If $b \equiv 16 \pmod{32}$, $d \equiv 0 \pmod 8$, from the work of Evans [5: Theorem 4 and its proof], we have

$$(3.43) \qquad u \equiv 0 \pmod 4, \quad v \equiv 0 \pmod 8, \quad w \equiv 0 \pmod 4.$$

Replacing g by g^{16s+t}, where $t = 1$ or 7 and $(16s + t, f) = 1$, as necessary, we may suppose that

$$(3.44) \qquad b \equiv 16 \pmod{64}.$$

There are exactly four 5-tuples (b, d, u, v, w), which satisfy (3.13) and (3.44). These are

$$(b, d, \pm u, v, \pm w), \qquad (b, -d, \pm w, -v, \mp u).$$

We note as before that the 16th root of unity modulo p,

$$\left\{\frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)}\right\}^{(b/4)+d-2(u+w)}$$

is independent of which 5-tuple is used.

Clearly, from (3.39) and (3.43), we have $(b/4) + d - 2(u + w) \equiv 4 \pmod 8$, and we determine $(b/4) + d - 2(u + w) \pmod{16}$ by considering the cases $d \equiv 0, 8 \pmod{16}$ and $u + w \equiv 0, 4 \pmod 8$. For example, if $d \equiv 0 \pmod{16}$ and $u + w \equiv 4 \pmod 8$, then $(b/4) + d - 2(u + w) \equiv 12 \pmod{16}$, so by (3.26), (1.6) and (1.8),

$$(3.45) \qquad 2^{(p-1)/32} \equiv \left\{ \frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)} \right\}^{12}$$

$$\equiv +\frac{b}{a} \pmod p,$$

see Table 2(IV). When applying Theorem 2 in this case, we can use any one of the four solutions $(x, \pm u, v, \pm w)$, $(x, \pm w, -v, \mp u)$, as $\pm w \mp u \equiv \pm(u + w) \pmod 8$.

Case (iv). As $2^{(p-1)/16} \equiv 1 \pmod p$, from Table 1, we have

$$(3.46) \qquad b \equiv 0 \pmod{32}, \qquad d \equiv 0 \pmod 8,$$

or

$$(3.47) \qquad b \equiv 16 \pmod{32}, \qquad d \equiv 4 \pmod 8.$$

If $b \equiv 0 \pmod{32}$, $d \equiv 0 \pmod 8$, appealing to the work of Evans [**5**: Theorem 4 and its proof], we have

$$(3.48) \qquad u \equiv 0 \pmod 4, \quad v \equiv 0 \pmod 8, \quad w \equiv 0 \pmod 4.$$

There are exactly eight 5-tuples which satisfy (3.13) and (3.48), namely,

$$(b, d, \pm u, v, \pm w), \qquad (b, -d, \pm w, -v, \mp u),$$
$$(-b, d, \pm w, -v, \mp u), \qquad (-b, -d, \pm u, v, \pm w).$$

It is straightforward to check that

$$\left\{ \frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)} \right\}^{(b/4)+d-2(u+w)}$$

is the same for all of these. The exponent $(b/4) + d - 2(u + w)$ is congruent to $0 \pmod 8$. It is easily determined modulo 16 by considering the cases $b \equiv 0,\ 32 \pmod{64}$, $d \equiv 0,\ 8 \pmod{16}$, and $u + w \equiv 0,\ 4 \pmod 8$. For example, if $b \equiv 0 \pmod{64}$, $d \equiv 0 \pmod{16}$, $u + w \equiv 4 \pmod 8$, we have $b/4 + d - 2(u + w) \equiv 8 \pmod{16}$ so that, by (1.6), (1.8) and (3.26),

$$2^{(p-1)/32} \equiv \left\{ \frac{(dx + cv)(a(u + w) - b(u - w))}{2bd(u^2 + w^2)} \right\}^{8} \equiv -1 \pmod p,$$

see Table 2 (I). As noted by Evans [**6**: Comments following Theorem 7], it is unnecessary to use the congruence $bd(x^2-2v^2)\equiv ac(u^2+2uw-w^2) \pmod p$ when applying Theorem 2 in this case.

Finally if $b\equiv 16 \pmod{32}$, $d\equiv 4 \pmod 8$, appealing to the work of Evans [**5**: Theorem 4 and its proof], we have

$$u\equiv 2 \pmod 4, \quad v\equiv 4 \pmod 8, \quad w\equiv 2 \pmod 4.$$

Replacing g by g^{16s+t}, where $t=1$, 3, 5 or 7 and $(16s+t, f)=1$, as appropriate, we can choose

$$b\equiv 16 \pmod{64}, \qquad d\equiv 4 \pmod{16}. \tag{3.49}$$

There are two 5-tuples (b, d, u, v, w) satisfying (3.13) and (3.49), namely,

$$(b, d, \pm u, v, \pm w),$$

and again it is easy to check that

$$\left\{\frac{(dx+cv)(a(u+w)-b(u-w))}{2bd(u^2+w^2)}\right\}^{(b/4)+d-2(u+w)} = \left\{\frac{(dx+cv)(a(-u-w)-b(-u+w))}{2bd\left((-u)^2+(-w)^2\right)}\right\}^{(b/4)+d-2(-u-w)}.$$

Now

$$\frac{b}{4}+d-2(u+w)\equiv 8-2(u+w) \pmod{16}$$

so, by (3.26), we have

$$2^{(p-1)/32}\equiv\begin{cases}+1, & \text{if } u+w\equiv 4 \pmod 8,\\ -1, & \text{if } u+w\equiv 0 \pmod 8,\end{cases}$$

see Table 2 (II). In applying Theorem 2 in this case, as noted by Evans [**6**: Comments following Theorem 7], it is necessary to use the congruence $bd(x^2-2v^2)\equiv ac(u^2+2uw-w^2) \pmod p$. This completes the proof of Theorem 2.

4. Numerical examples. (a) $p=2113$ (see Table 2 (I)). We have

$$(a, b)=(33, \pm 32); \qquad a\equiv 1 \pmod 4;$$
$$(c, d)=(-31, \pm 24); \qquad c\equiv 1 \pmod 4;$$
$$(x, u, v, w)=(-17, \pm 28, -8, \pm 8) \quad\text{or}\quad (-17, \pm 8, +8, \mp 28);$$
$$x\equiv -1 \pmod 8.$$

For each choice we have

$$b \equiv 32 \pmod{64}, \quad d \equiv 8 \pmod{16}, \quad u + w \equiv 4 \pmod 8,$$

so by Theorem 2(I), we have

$$2^{(p-1)/32} = 2^{66} \equiv -1 \pmod{2113}.$$

(b) $p = 257$ (see Table 2 (II)). We have

$$(a, b) = (1, 16); \quad a \equiv 1 \pmod 4, \quad b \equiv 16 \pmod{64};$$
$$(c, d) = (-15, 4); \quad c \equiv 1 \pmod 4, \quad d \equiv 4 \pmod{16};$$
$$(x, u, v, w) = (-9, \pm 6, -4, \mp 6) \quad \text{or} \quad (-9, \pm 6, +4, \pm 6);$$
$$x \equiv -1 \pmod 8.$$

The congruence $bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$ is satisfied by $(x, u, v, w) = (-9, \pm 6, -4, \mp 6)$. As $u + w \equiv 0 \pmod 8$, by Theorem 2(II), we have

$$2^{(p-1)/32} = 2^8 \equiv -1 \pmod{257}.$$

(c) $p = 1249$ (see Table 2(III)). We have

$$(a, b) = (-15, 32) \quad \text{or} \quad (-15, -32);$$
$$a \equiv 1 \pmod 4, \quad b \equiv 0 \pmod{32};$$
$$(c, d) = (-31, -12); \quad c \equiv 1 \pmod 4, \quad d \equiv 4 \pmod{16};$$
$$(x, u, v, w) = (7, 10, 4, -22) \quad \text{or} \quad (7, 22, -4, 10);$$
$$x \equiv -1 \pmod 8, \quad w \equiv 2 \pmod 8.$$

The congruence $bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$ is satisfied by $(a, b) = (-15, 32)$ and $(x, u, v, w) = (7, 22, -4, 10)$ or by $(a, b) = (-15, -32)$ and $(x, u, v, w) = (7, 10, 4, -22)$. Hence, by Theorem 2, taking $b = 32$, $u = 22 \equiv 6 \pmod 8$, we have

$$2^{(p-1)/32} = 2^{39} \equiv +b/a \equiv 32/-15 \equiv 664 \pmod{1249};$$

taking $b = -32$, $u = 10 \equiv 2 \pmod 8$, we have

$$2^{(p-1)/32} = 2^{39} \equiv -b/a \equiv 32/-15 \equiv 664 \pmod{1249}.$$

(d) $p = 1217$ (see Table 2 (IV)). We have

$$(a, b) = (-31, 16); \quad a \equiv 1 \pmod 4, \quad b \equiv 16 \pmod{64};$$
$$(c, d) = (33, +8) \quad \text{or} \quad (33, -8); \quad c \equiv 1 \pmod 4;$$
$$(x, u, v, w) = (-17, \pm 12, -8, \mp 16), \quad (-17, \pm 16, +8, \pm 12),$$
$$x \equiv -1 \pmod 8.$$

As $d \equiv 8 \pmod{16}$ and $u + w \equiv 4 \pmod 8$ (for each possibility), we have, by Theorem 2,

$$2^{(p-1)/32} = 2^{38} \equiv -b/a \equiv 16/31 \equiv 1139 \pmod{1217}.$$

(e) $p = 577$ (see Table 2 (V)). We have

$$(a, b) = (1, 24); \quad a \equiv 1 \pmod 4, \quad b \equiv 24 \pmod{32};$$

$$(c, d) = (17, -12); \quad c \equiv 1 \pmod 4, \quad d \equiv 4 \pmod{16};$$

$$(x, u, v, w) = (-1, \pm 4, -16, \mp 4) \quad \text{or} \quad (-1, \pm 4, +16, \pm 4).$$

As $b \equiv 24 \pmod{64}$, $u + w \equiv 0 \pmod 8$, by Theorem 2(V), we have

$$2^{(p-1)/32} = 2^{18} \equiv +\frac{(a+b)d}{ac} \equiv \frac{-300}{17} \equiv 186 \pmod{577}.$$

(f) $p = 353$ (see Table 2 (VI)). We have

$$(a, b) = (17, 8); \quad a \equiv 1 \pmod 4, \quad b \equiv 8 \pmod{32};$$

$$(c, d) = (-15, 8) \quad \text{or} \quad (-15, -8); \quad c \equiv 1 \pmod 4;$$

$$(x, u, v, w) = (7, -10, -4, -6) \quad \text{or} \quad (7, -6, 4, 10);$$

$$x \equiv -1 \pmod 8, \quad w \equiv 2 \pmod 8.$$

The congruence $bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$ is satisfied by $(c, d) = (-15, 8)$ and $(x, u, v, w) = (7, -10, -4, -6)$, or by $(c, d) = (-15, -8)$ and $(x, u, v, w) = (7, -6, 4, 10)$. Hence, by Theorem 2, taking the first possibility, we have $b \equiv 8 \pmod{64}$, $d \equiv 8 \pmod{16}$, $u = -10 \equiv 6 \pmod 8$, so

$$2^{(p-1)/32} = 2^{11} \equiv \frac{(a+b)d}{ac} \equiv \frac{40}{-51} \equiv 283 \pmod{353}.$$

(g) $p = 97$ (see Table 2 (VIII)). We have

$$(a, b) = (9, -4); \quad a \equiv 1 \pmod 4, \quad b \equiv 12 \pmod{16};$$

$$(c, d) = (5, -6); \quad c \equiv 1 \pmod 4, \quad d \equiv 2 \pmod 8;$$

$$(x, u, v, w) = (7, -4, 2, 2); \quad x \equiv -1 \pmod 8, \quad w \equiv 2 \pmod 8.$$

As $b \equiv 60 \pmod{64}$, $d \equiv 10 \pmod{16}$, $u \equiv 4 \pmod 8$, by Theorem 2(VII), we have

$$2^{(p-1)/32} = 2^3 \equiv \frac{(-32)(-46)}{(48)(20)} \equiv \frac{23}{15} \equiv 8 \pmod{97}.$$

5. Acknowledgement. We wish to thank Mr. Lee-Jeff Bell for doing some calculations for us in connection with the preparation of this paper.

TABLE 1

b	d	Cases	$2^{(p-1)/16} \pmod p$	Examples
$b \equiv 0 \pmod{16}$	$d \equiv 0 \pmod 4$	$b \equiv 0 \pmod{32}$, $d \equiv 0 \pmod 8$ or $b \equiv 16 \pmod{32}$, $d \equiv 4 \pmod 8$	$+1$	$p = 2113$ $p = 257$
		$b \equiv 0 \pmod{32}$, $d \equiv 4 \pmod 8$ or $b \equiv 16 \pmod{32}$, $d \equiv 0 \pmod 8$	-1	$p = 1249$ $p = 1217$
$b \equiv 8 \pmod{16}$		$d \equiv 0 \pmod 8$	$-b/a$	$p = 353$
b chosen $\equiv 8 \pmod{32}$		$d \equiv 4 \pmod 8$	$+b/a$	$p = 113$
$b \equiv 4 \pmod 8$	$d \equiv 2 \pmod 4$	$b \equiv 12 \pmod{32}$	$\dfrac{-(a+b)d}{ac}$	$p = 193$
b chosen $\equiv 12 \pmod{16}$	d chosen $\equiv 2 \pmod 8$	$b \equiv 28 \pmod{32}$	$\dfrac{+(a+b)d}{ac}$	$p = 17$

TABLE 2

		$b \pmod{64}$, $d \pmod{16}$, $u \pmod 8$, $u+w \pmod 8$	$2^{(p-1)/32} \pmod p$
I	$b \equiv 0(32)$, $d \equiv 0(8)$	$(b, d, u+w) \equiv (0,0,0), (0,8,4), (32,0,4), (32,8,0)$	$+1$
		Examples $p = 47713, 10657, 31649, 50753$	
		$(b, d, u+w) \equiv (0,0,4), (0,8,0), (32,0,0), (32,8,4)$	-1
		Examples $p = 25121, 18593, 51137, 2113$	
II	$b \equiv 16(32)$, $d \equiv 4(8)$	$u+w \equiv 4$	$+1$
	Choose	Example $p = 2593$	
	$b \equiv 16(64)$, $d \equiv 4(16)$	$u+w \equiv 0$	-1
	$bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$	Example $p = 257$	
III	$b \equiv 0(32)$, $d \equiv 4(8)$	$(b, u) \equiv (0,6), (32,2)$	$-b/a$
	Choose	Examples $p = 10337, 1249$	
	$d \equiv 4(16)$, $w \equiv 2(8)$	$(b, u) \equiv (0,2), (32,6)$	$+b/a$
	$bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$	Examples $p = 10337, 1249$	
IV	$b \equiv 16(32)$, $d \equiv 0(8)$	$(d, u+w) \equiv (0,0), (8,4)$	$-b/a$
	Choose	Examples $p = 14753, 1217$	
	$b \equiv 16(64)$	$(d, u+w) \equiv (0,4), (8,0)$	$+b/a$
		Examples $p = 4481, 11329$	

V	Choose $b \equiv 8(16), d \equiv 4(8)$	$(b, u+w) \equiv (56,0), (24,4)$	$\frac{-(a+b)d}{ac}$
		Examples $p = 15361, 1889$	
	$b \equiv 24(32), d \equiv 4(16)$	$(b, u+w) \equiv (56,4), (24,0)$	$\frac{+(a+b)d}{ac}$
		Examples $p = 9377, 577$	
VI	Choose $b \equiv 8(16), d \equiv 0(8)$	$(b, d, u) \equiv (8,0,6), (8,8,2), (40,0,2), (40,8,6)$	$\frac{-(a+b)d}{ac}$
		Examples $p = 2273, 353, 1601, 13921$	
	$b \equiv 8(32), w \equiv 2(8)$	$(b, d, u) \equiv (8,0,2), (8,8,6), (40,0,6), (40,8,2)$	$\frac{+(a+b)d}{ac}$
	$bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p$	Examples $p = 2273, 353, 1601, 13921$	
VII	Choose $b \equiv 4(8), d \equiv 2(4)$	$(b, d, u) \equiv (12,2,0), (12,10,4), (44,2,4), (44,10,0)$	$\frac{(dx+cv)(a(u+w) - b(u-w))}{2bd(u^2+w^2)}$
		Examples $p = 673, 10273, 449, 2081$	
		$(b, d, u) \equiv (28,2,0), (28,10,4), (60,2,4), (60,10,0)$	$-\frac{(dx+cv)(b(u+w) + a(u-w))}{2bd(u^2+w^2)}$
		Examples $p = ?, 1409, 3041, 641$	
	$b \equiv 12(16), d \equiv 2(8), w \equiv 2(8)$	$(b, d, u) \equiv (12,2,4), (12,10,0), (44,2,0), (44,10,4)$	$-\frac{(dx+cv)(a(u+w) - b(u-w))}{2bd(u^2+w^2)}$
		Examples $p = 2753, 193, 5441, 929$	
		$(b, d, u) \equiv (28,2,4), (28,10,0), (60,2,0), (60,10,4)$	$\frac{(dx+cv)(b(u+w) + a(u-w))}{2bd(u^2+w)}$
		Examples $p = 15937, 11489, 4129, 97$	

References

1. A. Aigner, *Kriterien zum* 8. *und* 16. *Potenzcharakter der Reste* 2 *und* -2, Deutsche Math., **4** (1939), 44–52.
2. P. Barrucand and H. Cohn, *Note on primes of type* $x^2 + 32y^2$, *class number, and residuacity*, J. Reine Angew. Math., **238** (1969), 67–70.
3. A. Cunningham, *On* 2 *as a* 16-*ic residue*, Proc. London Math. Soc., (1) **27** (1895/6), 85–122.
4. G. L. Dirichlet, *Ueber den biquadratischen Charakter der Zahl "Zwei"*, J. Reine Angew. Math., **57** (1860), 187–188.
5. R. J. Evans, *Resolution of sign ambiguities in Jacobi and Jacobsthal sums*, Pacific J. Math., **81** (1979), 71–80.
6. _____, *The* 2^r*th power character of* 2, J. Reine Angew. Math., **315** (1980), 174–189.
7. R. J. Evans and J. R. Hill, *The cyclotomic numbers of order sixteen*, Math. Comp., **33** (1979), 827–835.
8. C. F. Gauss, *Theoria residuorum biquadraticorum. I*, Commentationes soc. reg. sc. Gotting. recentiores., **6** (1828), 27– . II. 7 (1832), 89– , (See Untersuchungen über Höhere Arithmetik, Chelsea Publ. Co. (N. Y.) (1965), 511–586.)
9. H. Hasse, *Der* 2^n*te Potenzcharakter von* 2 *im Körper der* 2^n*ten Einheitswurzeln*, Rend. Circ. Mat. Palermo, Serie II, **7** (1958), 185–244.
10. Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod p$, Pacific J. Math., **5** (1955), 103–118.
11. _____, *On Euler's criterion*, J. Austral. Math. Soc., **1** (1959), 64–70.
12. P. A. Leonard and K. S. Williams, *A rational sixteenth power reciprocity law*, Acta Arith., **33** (1977), 365–377.
13. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math., **286/287** (1976), 248–256.
14. C. G. Reuschle, *Mathematische Abhandlung, enthaltend neue Zahlentheoretische Tabellen*, Programm zum Schlusse des Schuljahrs 1855–56 am Königlichen Gymnasium zu Stuttgart (1856), 61 pp.
15. A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math., (2), **9** (1911), 244–272.
16. A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math., **6** (1954), 364–373.
17. _____, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc., **86** (1957), 401–413.

Received November 19, 1979 and in revised form August 18, 1981. Research supported by grant no. A-7233 of the Natural Sciences and Engineering Research Council Canada.

University of South Carolina
Columbia, SC U.S.A 29208
and
Carleton University
Ottawa, Ontario, Canada K1S 5B6

Pacific Journal of Mathematics

Vol. 104, No. 1 May, 1983