ISRAEL JOURNAL OF MATHEMATICS, Vol. 38, No. 3, 1981

A NEW CRITERION FOR 7 TO BE A FOURTH POWER (mod p)

BY

RICHARD H. HUDSON AND KENNETH S. WILLIAMS[†]

ABSTRACT

A new application is made of Muskat's evaluation of the cyclotomic numbers of order fourteen, to obtain a necessary and sufficient condition for seven to be a fourth power modulo a prime $\equiv 1 \pmod{28}$.

1. Introduction

Let p be a prime $\equiv 1 \pmod 4$. For small primes q with $(p/q) = +1$, necessary and sufficient criteria for q to be a fourth power modulo p have traditionally been given in terms of congruences modulo q involving the integers a and b defined by $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$ (see for example [2], [6], [8]).

Recently other parametric representations of p have been used to give similar criteria. For example, if $p \equiv 1 \pmod{16}$ then there are integers x_1, x_2, x_3, x_4 such that

$$\text{(1.1)} \qquad \begin{cases} p = x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2, & x_1 \equiv 1 \pmod 8, \\ 2x_1x_3 = x_2^2 - 2x_2x_4 - x_4^2, \end{cases}$$

(see for example [5, p. 338] and [12, p. 366]) and Evans [4] has shown that

$$\text{(1.2)} \qquad 2 \text{ is a fourth power} \pmod p \Leftrightarrow x_3 \equiv 0 \pmod 4.$$

We note that (1.1) has exactly four solutions, namely $(x_1, \pm x_2, x_3, \pm x_4)$ and $(x_1, \pm x_4, -x_3, \mp x_2)$, so that x_1 and $|x_3|$ are uniquely determined by (1.1). If

[†] Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

Received June 6, 1980

$p \equiv 1 \pmod{20}$ it follows from the work of Dickson [3, p. 402] that there are integers x_1, x_2, x_3, x_4 such that

$$(1.3) \qquad \begin{cases} 16p = x_1^2 + 50x_2^2 + 50x_3^2 + 125x_4^2, & x_1 \equiv 1 \pmod 5, \\ x_1x_4 = x_3^2 - 4x_2x_3 - x_2^2, \end{cases}$$

and the authors [7] have proved that

$$(1.4) \qquad 5 \text{ is a fourth power} \pmod p \iff \begin{cases} x_1 \equiv 4 \pmod 8, & \text{if } x_1 \equiv 0 \pmod 2, \\ x_1 \equiv \pm 3x_4 \pmod 8, & \text{if } x_1 \equiv 1 \pmod 2. \end{cases}$$

All four solutions of (1.3) are given by

$$(x_1, \pm x_2, \pm x_3, x_4), \ (x_1, \pm x_3, \mp x_2, -x_4),$$

so that x_1 and $|x_4|$ are uniquely determined by (1.3).

In this note, we obtain a result for 7 to be a fourth power $(\text{mod } p)$ analogous to (1.2) and (1.4). This is done using Muskat's formulae [13] for the cyclotomic numbers of order fourteen in conjunction with an index formula given by the authors in [7]. The details for $q = 7$ are considerably more complicated than those for $q = 2$ and $q = 5$, as the diophantine system corresponding to (1.1) and (1.3) in this case involves six parameters and the group of solutions is cyclic of order six. Our main result is given in Theorem 5.

2. Criteria for 2 to be a seventh power $(\text{mod } p)$

Let p be a prime $\equiv 1 \pmod 7$, so that $p = 14f + 1$. Let g be a fixed primitive root $(\text{mod } p)$. For integers h and k the number of solutions (s, t) with $0 \leqq s, t < (p-1)/7$ of the congruence

$$(2.1) \qquad g^{7s+h} + 1 \equiv g^{7t+k} \pmod p$$

is denoted by $(h, k)_7$. The number $(h, k)_7$ is called the cyclotomic number of order 7. The Dickson–Hurwitz sum of order 7 is defined by

$$B_7(i, j) = \sum_{h=0}^{6} (h, i - jh)_7.$$

As in [16, pp. 609–611], we can define integers $x_1, x_2, x_3, x_4, x_5, x_6$ (depending upon g) by

$$(2.2)\qquad \begin{cases} x_1 = 2 - p + 7(0,0)_7 + 14(1,2)_7 + 14(1,4)_7 + 14(2,4)_7, \\ x_2 = 2(0,1)_7 + (0,3)_7 - (0,4)_7 - 2(0,6)_7 + 2(1,3)_7 - 2(1,5)_7, \\ x_3 = -(0,1)_7 + 2(0,2)_7 - 2(0,5)_7 + (0,6)_7 + 2(1,3)_7 - 2(1,5)_7, \\ x_4 = (0,2)_7 + 2(0,3)_7 - 2(0,4)_7 - (0,5)_7 - 2(1,3)_7 + 2(1,5)_7, \\ x_5 = -2(1,2)_7 + (1,4)_7 + (2,4)_7, \\ x_6 = -(1,4)_7 + (2,4)_7. \end{cases}$$

It is known [10], [16, theorem 2] that $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution of the diophantine system

$$(2.3)\qquad \begin{cases} 72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \quad x_1 \equiv 1 \pmod 7, \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 \\ \quad + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0, \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 \\ \quad + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0. \end{cases}$$

The sums $B_7(i, 1)$ $(0 \leqq i \leqq 6)$ have been given in terms of $x_1, x_2, x_3, x_4, x_5, x_6$ (see [9], [11]):

$$(2.4)\qquad \begin{cases} 84B_7(0,1) = 12x_1 + 12p - 24, \\ 84B_7(1,1) = -2x_1 + 42x_2 + 49x_5 + 147x_6 + 12p - 24, \\ 84B_7(2,1) = -2x_1 + 42x_3 + 49x_5 + 147x_6 + 12p - 24, \\ 84B_7(3,1) = -2x_1 + 42x_4 - 98x_5 + 12p - 24, \\ 84B_7(4,1) = -2x_1 - 42x_4 - 98x_5 + 12p - 24, \\ 84B_7(5,1) = -2x_1 - 42x_3 + 49x_5 - 147x_6 + 12p - 24, \\ 84B_7(6,1) = -2x_1 - 42x_2 + 49x_5 + 147x_6 + 12p - 24. \end{cases}$$

We also define integers t and u by

$$(2.5)\qquad \begin{cases} 6t = p - 2 - 7(0,0)_7 - 21(1,3)_7 - 21(1,5)_7, \\ 2u = (0,1)_7 + (0,2)_7 - (0,3)_7 + (0,4)_7 - (0,5)_7 - (0,6)_7 - (1,3)_7 + (1,5)_7, \end{cases}$$

(see [11, p. 298], [14, p. 64]), so that (t, u) satisfies

$$p = t^2 + 7u^2, \qquad t \equiv 1 \pmod 7). \tag{2.6}$$

It is shown in [16, theorem 2] that $(x_1, x_2, x_3, x_4, x_5, x_6)$ is not equal to either of the two "trivial" solutions $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$ of the system (2.3). There are exactly six "non-trivial" solutions of (2.3). These are

$$\begin{cases} (x_1, x_2, x_3, x_4, x_5, x_6), \\ (x_1, x_3, -x_4, -x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)), \\ (x_1, x_4, -x_2, x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)), \\ (x_1, -x_4, x_2, -x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)), \\ (x_1, -x_3, x_4, x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)), \\ (x_1, -x_2, -x_3, -x_4, x_5, x_6), \end{cases} \tag{2.7}$$

see for example [9, p. 144].

Clearly from the first equation of (2.3), we have

LEMMA 1. $x_5 \equiv x_6 \pmod 2$.

Leonard and Williams [9] have shown

LEMMA 2. *2 is a seventh power* $\pmod p \Leftrightarrow x_1 \equiv 0 \pmod 2$.

The next lemma is a special case of a result of Alderson [1, theorem 1].

LEMMA 3. *2 is a seventh power* $\pmod p$

$$\Leftrightarrow (0,1)_7, (0,2)_7, \cdots, (0,6)_7 \textit{ are all even.}$$

From the evaluation of the cyclotomic numbers of order 7 given by Leonard and Williams [11], we have (with a minor misprint corrected in the first equation)

LEMMA 4.

$$588(0,1)_7 = 12p - 72 + 24t + 168u - 6x_1 + 84x_2 - 42x_3 + 147x_5 + 147x_6,$$

$$588(0,2)_7 = 12p - 72 + 24t + 168u - 6x_1 + 84x_3 + 42x_4 - 294x_6,$$

$$588(0,3)_7 = 12p - 72 + 24t - 168u - 6x_1 + 42x_2 + 84x_4 - 147x_5 + 147x_6,$$

$$588(0,4)_7 = 12p - 72 + 24t + 168u - 6x_1 - 42x_2 - 84x_4 - 147x_5 + 147x_6,$$

$$588(0,5)_7 = 12p - 72 + 24t - 168u - 6x_1 - 84x_3 - 42x_4 - 294x_6,$$

$$588(0,6)_7 = 12p - 72 + 24t - 168u - 6x_1 - 84x_2 + 42x_3 + 147x_5 + 147x_6.$$

From Lemmas 2, 3 and 4 we obtain

LEMMA 5. *If 2 is a seventh power* (mod p) *then* $x_2, \cdots, x_6$ *are all even and* $x_5 \equiv x_6$ (mod 4).

PROOF. By Lemmas 3 and 4, we have

$$\begin{aligned}
2x_1 + 4x_2 - 2x_3 + 3x_5 + 3x_6 &\equiv 4 \pmod 8,\\
2x_1 + 4x_3 + 2x_4 + 2x_6 &\equiv 4 \pmod 8,\\
2x_1 + 2x_2 + 4x_4 - 3x_5 + 3x_6 &\equiv 4 \pmod 8,\\
2x_1 - 2x_2 + 4x_4 - 3x_5 + 3x_6 &\equiv 4 \pmod 8,\\
2x_1 + 4x_3 - 2x_4 + 2x_6 &\equiv 4 \pmod 8,\\
2x_1 + 4x_2 + 2x_3 + 3x_5 + 3x_6 &\equiv 4 \pmod 8,
\end{aligned}$$

from which it follows easily that

$$x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 2.$$

Moreover, by Lemma 2, we have $x_1 \equiv 0$ (mod 2). The first two congruences now give $x_5 \equiv x_6 \equiv 0$ (mod 2) and the third gives $x_5 \equiv x_6$ (mod 4).

Hence by Lemmas 1 and 5 we have

LEMMA 6. *If* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *is such that*

$$x_5 \equiv x_6 \equiv 1 \pmod 2$$

or

$$x_5 \equiv x_6 \equiv 0 \pmod 2, \qquad x_5 \not\equiv x_6 \pmod 4,$$

then 2 is not a seventh power (mod p).

Next we prove

LEMMA 7. *If f is even and* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *is such that*

$$x_5 \equiv x_6 \equiv 0 \pmod 2, \qquad x_5 \equiv x_6 \pmod 4,$$

then

(i) $x_1 \equiv 2$ (mod 4),
(ii) $x_2 \equiv x_3 \equiv x_4 \equiv x_5 \equiv x_6 \equiv 0$ (mod 4),
(iii) $x_5 \equiv x_6$ (mod 8),
(iv) $x_2 + x_3 + x_4 \equiv 2f$ (mod 8).

PROOF. As $x_5 \equiv x_6 \equiv 0 \pmod 2$, $x_5 \equiv x_6 \pmod 4$, we can define integers y_6 and z by

$$x_5 = 2y_6 + 4z, \qquad x_6 = 2y_6.$$

Taking each of the three equations in (2.3) modulo 64, we obtain

$$x_1^2 + 21(x_2^2 + x_3^2 + x_4^2) + 24(y_6^2 + y_6 z + z^2) \equiv 4 - 8f \pmod{32}, \tag{2.8}$$

$$3x_2^2 - 3x_4^2 - 4y_6^2 - 4z^2 - 4x_1y_6 + 6x_2x_3 - 6x_2x_4 + 12x_3x_4 \equiv 0 \pmod{16}, \tag{2.9}$$

$$\begin{aligned} &3x_3^2 - 3x_4^2 + 8y_6^2 + 8y_6z + 4z^2 + 28x_1y_6 \\ &\qquad + 28x_1z + 12x_2x_3 + 6x_2x_4 + 6x_3x_4 \equiv 0 \pmod{16}. \end{aligned} \tag{2.10}$$

Clearly from (2.9) and (2.10) we have

$$x_2 \equiv x_3 \equiv x_4 \pmod 2.$$

Taking (2.8) modulo 8, and supposing that $x_2 \equiv x_3 \equiv x_4 \equiv 1 \pmod 2$, we obtain

$$x_1^2 + 7 \equiv 4 \pmod 8,$$

which is impossible. Hence we must have

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 2.$$

Thus we can define integers y_i ($i = 1, 2, 3, 4$) by $x_i = 2y_i$. Using these in (2.8), (2.9), (2.10), we obtain

$$y_1^2 + 5(y_2^2 + y_3^2 + y_4^2) - 2(y_6^2 + y_6z + z^2) \equiv 1 - 2f \pmod 8, \tag{2.11}$$

$$-y_2^2 + y_4^2 - y_6^2 - z^2 + 2y_1y_6 + 2y_2y_3 + 2y_2y_4 \equiv 0 \pmod 4, \tag{2.12}$$

$$-y_3^2 + y_4^2 + 2y_6^2 + 2y_6z + z^2 + 2y_1y_6 + 2y_1z + 2y_2y_4 + 2y_3y_4 \equiv 0 \pmod 4. \tag{2.13}$$

From (2.11), (2.12), (2.13) we obtain, as f is even,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 + 2(y_6^2 + y_6z + z^2) \equiv 1 \pmod 4,$$

$$y_2 + y_4 + y_6 + z \equiv 0 \pmod 2,$$

$$y_3 + y_4 + z \equiv 0 \pmod 2.$$

These congruences give the following possible residues (mod 2) for y_1, y_2, y_3, y_4, y_6, z.

y_1	y_2	y_3	y_4	y_6	z
1	0	0	0	0	0
1	1	1	0	0	1
1	0	1	1	1	0
1	1	0	1	1	1

The second of these possibilities cannot occur in view of (2.13) and the third and fourth in view of (2.12). Hence we have

$$x_1 \equiv 2 \pmod 4, \quad x_2 \equiv x_3 \equiv x_4 \equiv x_5 \equiv x_6 \equiv 0 \pmod 4, \quad x_5 \equiv x_6 \pmod 8,$$

proving (i), (ii) and (iii). Finally, from (2.11), we have, with $y_2 = 2z_2$, $y_3 = 2z_3$, $y_4 = 2z_4$,

$$1 + 4(z_2^2 + z_3^2 + z_4^2) \equiv 1 - 2f \pmod 8,$$

that is

$$z_2 + z_3 + z_4 \equiv f/2 \pmod 2,$$

giving

$$x_2 + x_3 + x_4 \equiv 2f \pmod 8,$$

which is (iv).

Putting Lemmas 1, 2, 6 and 7 together we obtain

THEOREM 1. *If f is even then*

$$2 \text{ is a seventh power} \pmod p \Leftrightarrow x_5 \equiv x_6 \equiv 0 \pmod 2, \quad x_5 \equiv x_6 \pmod 4,$$

or, equivalently,

$$2 \text{ is not a seventh power} \pmod p$$

$$\Leftrightarrow x_5 \equiv x_6 \equiv 1 \pmod 2 \quad \text{or} \quad x_5 \equiv x_6 \equiv 0 \pmod 2, \quad x_5 \not\equiv x_6 \pmod 4.$$

3. Congruences for $\mathrm{ind}_g(2)$ and $\mathrm{ind}_g(7)$

If n is an integer not divisible by p, the index of n with respect to g, written $\mathrm{ind}_g(n)$, is that integer b such that $n \equiv g^b \pmod p$, $0 \leqq b \leqq p-2$. We prove the following more precise form of Theorem 1.

THEOREM 2. *If f is even, then*

$$\operatorname{ind}_g(2) \equiv \begin{cases} 0 \pmod 7, \text{ if } x_5 \equiv x_6 \equiv 0 \pmod 2, & x_5 \equiv x_6 \pmod 4, \\ \pm 1 \pmod 7, \text{ if } x_5 \equiv x_6 \equiv 1 \pmod 2, & x_5 \not\equiv x_6 \pmod 4, \\ \pm 2 \pmod 7, \text{ if } x_5 \equiv x_6 \equiv 0 \pmod 2, & x_5 \not\equiv x_6 \pmod 4, \\ \pm 3 \pmod 7, \text{ if } x_5 \equiv x_6 \equiv 1 \pmod 2, & x_5 \equiv x_6 \pmod 4. \end{cases}$$

PROOF. In view of Theorem 1 we need only treat the cases when $\operatorname{ind}_g(2) \not\equiv 0 \pmod 7$. As 2 is not a seventh power (mod p), by Theorem 1, we have

$$x_5 \equiv x_6 \equiv 1 \pmod 2 \quad \text{or} \quad x_5 \equiv x_6 \equiv 0 \pmod 2, \quad x_5 + x_6 \equiv 2 \pmod 4.$$

From Muskat's table 3 [13, p. 277] for the cyclotomic numbers of order 14 and the expressions for $B_7(i, 1)$ $(1 \leqq i \leqq 6)$ given in (2.4), we obtain

$$\begin{aligned} 4\{(4,8)_{14} - (1,11)_{14}\} &= x_5 + x_6, && \text{if } \operatorname{ind}_g(2) \equiv 1 \pmod 7, \\ 2\{(1,9)_{14} - (2,8)_{14}\} &= x_6, && \text{if } \operatorname{ind}_g(2) \equiv 2 \pmod 7, \\ 4\{(2,11)_{14} - (2,4)_{14}\} &= x_5 - x_6, && \text{if } \operatorname{ind}_g(2) \equiv 3 \pmod 7, \\ 4\{(2,5)_{14} - (2,4)_{14}\} &= x_5 - x_6, && \text{if } \operatorname{ind}_g(2) \equiv 4 \pmod 7, \\ 2\{(1,6)_{14} - (2,8)_{14}\} &= x_6, && \text{if } \operatorname{ind}_g(2) \equiv 5 \pmod 7, \\ 4\{(4,8)_{14} - (1,4)_{14}\} &= x_5 + x_6, && \text{if } \operatorname{ind}_g(2) \equiv 6 \pmod 7. \end{aligned}$$

If $\operatorname{ind}_g(2) \equiv \pm 1 \pmod 7$, we have $x_5 + x_6 \equiv 0 \pmod 4$, and thus by Theorem 1, we have $x_5 \equiv x_6 \equiv 1 \pmod 2$, $x_5 \not\equiv x_6 \pmod 4$.

If $\operatorname{ind}_g(2) \equiv \pm 2 \pmod 7$, we have $x_6 \equiv 0 \pmod 2$, and thus by Theorem 1, we obtain $x_5 \equiv x_6 \equiv 0 \pmod 2$, $x_5 \not\equiv x_6 \pmod 4$.

If $\operatorname{ind}_g(2) \equiv \pm 3 \pmod 7$, we have $x_5 \equiv x_6 \pmod 4$, and so by Theorem 1, we deduce that $x_5 \equiv x_6 \equiv 1 \pmod 2$.

This completes the proof of Theorem 2.

An immediate application of theorem 1 of [7] (with $e = 7$, $k = 4$, $l = 14$) gives

LEMMA 8. *If f is even, then*

$$\operatorname{ind}_g(7) \equiv 2 \sum_{i=0}^{6} \sum_{j=0}^{1} \sum_{k=1}^{3} (2i+1, 7j+k)_{14} + f \pmod 4.$$

Applying Muskat's formulae [13, tables 1 and 3] for the cyclotomic numbers of order 14 in Lemma 8, we obtain, using (2.4) and Lemma 7 (iv), the following theorem.

THEOREM 3. *If f is even, then*

$$\operatorname{ind}_g(7) \equiv \begin{cases} 1-\frac{1}{2}x_1 \pmod 4, & \text{if } \operatorname{ind}_g(2) \equiv 0 \pmod 7, \\ f-1-\frac{1}{2}(x_5+3x_6) \pmod 4, & \text{if } \operatorname{ind}_g(2) \equiv \pm 1 \pmod 7, \\ f-1-\frac{1}{2}(x_5-3x_6) \pmod 4, & \text{if } \operatorname{ind}_g(2) \equiv \pm 2 \pmod 7, \\ f-1+x_5 \pmod 4, & \text{if } \operatorname{ind}_g(2) \equiv \pm 3 \pmod 7. \end{cases}$$

Putting Theorems 2 and 3 together we obtain

THEOREM 4. *If f is even, then*

$$\operatorname{ind}_g(7) \equiv \begin{cases} 1-\frac{1}{2}x_1 \pmod 4, \text{ if } x_5 \equiv x_6 \equiv 0 \pmod 2,\ x_5 \equiv x_6 \pmod 4, \\ f-1-\frac{1}{2}(x_5+3x_6) \pmod 4, \text{ if } x_5 \equiv x_6 \equiv 1 \pmod 2,\ x_5 \not\equiv x_6 \pmod 4, \\ f-1-\frac{1}{2}(x_5-3x_6) \pmod 4, \text{ if } x_5 \equiv x_6 \equiv 0 \pmod 2,\ x_5 \not\equiv x_6 \pmod 4, \\ f-1+x_5 \pmod 4, \text{ if } x_5 \equiv x_6 \equiv 1 \pmod 2,\ x_5 \equiv x_6 \pmod 4. \end{cases}$$

Clearly, from (2.7), if $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution of (2.3) satisfying $x_5 \equiv x_6 \equiv 0 \pmod 2$, $x_5 \equiv x_6 \pmod 4$, all six solutions satisfy the same congruences. If not, then two of the six solutions of (2.3) satisfy $x_5 \equiv x_6 \equiv 1 \pmod 2$, $x_5 \not\equiv x_6 \pmod 4$; two satisfy $x_5 \equiv x_6 \equiv 0 \pmod 2$, $x_5 \not\equiv x_6 \pmod 4$; two satisfy $x_5 \equiv x_6 \equiv 1 \pmod 2$, $x_5 \equiv x_6 \pmod 4$. Hence, in this case, we can always choose a non-trivial solution of (2.3) satisfying $x_5 \equiv x_6 \equiv 1 \pmod 2$, $x_5 \equiv x_6 \pmod 4$. Thus Theorem 4 yields our main result.

THEOREM 5. *Suppose f is even and $(x_1, x_2, x_3, x_4, x_5, x_6)$ denotes a non-trivial solution of* (2.3). *If $x_1 \equiv 0 \pmod 2$, then*

$$7 \textit{ is a fourth power} \pmod p \Leftrightarrow x_1 \equiv 2 \pmod 8.$$

If $x_1 \not\equiv 0 \pmod 2$, we can choose the solution so that $x_5 \equiv x_6 \equiv 1 \pmod 2$, $x_5 \equiv x_6 \pmod 4$. Then

$$7 \textit{ is a fourth power} \pmod p \Leftrightarrow x_5 \equiv 1 - f \pmod 4.$$

4. Four numerical examples (see table 2 of [15])

EXAMPLE 1. $p = 29$, $f = 2$
$(x_1, x_2, x_3, x_4, x_5, x_6) = (1, 3, -2, -2, -1, -1)$,
$x_5 = -1 \equiv 1 - f \pmod 4$,
$7 \equiv 8^4 \pmod{29}$.

EXAMPLE 2. $p = 197$, $f = 14$
$(x_1, x_2, x_3, x_4, x_5, x_6) = (-13, 1, 8, 6, 1, -3)$,

$x_5 = 1 \not\equiv 1 - f \pmod 4$,
$7 \equiv 106^2 \pmod{197}$, $(106/197) = -1$.

EXAMPLE 3. $p = 673$, $f = 48$
$(x_1, x_2, x_3, x_4, x_5, x_6) = (22, 20, 8, -12, -4, -4)$,
$x_1 = 22 \equiv -2 \pmod 8$,
$7 \equiv 396^2 \pmod{673}$, $(396/673) = -1$.

EXAMPLE 4. $p = 953$, $f = 68$
$(x_1, x_2, x_3, x_4, x_5, x_6) = (50, 12, 8, -28, 4, 4)$,
$x_1 = 50 \equiv 2 \pmod 8$,
$7 \equiv 160^4 \pmod{953}$.

REFERENCES

1. Helen Popova Alderson, *On the septimic character of* 2 *and* 3, Proc. Camb. Phil. Soc. **74** (1973), 421–433.

2. Allan Cunningham and Thorold Gosset, 4-*tic &* 3-*bic residuacity-tables*, Mess. Math. **50** (1920), 1–30.

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

4. Ronald J. Evans, *Resolution of sign ambiguities in Jacobi and Jacobsthal sums*, Pacific J. Math. (to appear).

5. Reinaldo E. Giudici, Joseph B. Muskat, and Stanley F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. **171** (1972), 317–347.

6. Thorold Gosset, *On the law of quartic reciprocity*, Mess. Math. **41** (1911), 65–90.

7. Richard H. Hudson and Kenneth S. Williams, *Some new residuacity criteria*, Pacific J. Math. (to appear).

8. Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

9. Philip A. Leonard and Kenneth S. Williams, *The septic character of* 2, 3, 5 *and* 7, Pacific J. Math. **52** (1974), 143–147.

10. Philip A. Leonard and Kenneth S. Williams, *A diophantine system of Dickson*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56** (1974), 145–150.

11. Philip A. Leonard and Kenneth S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. **51** (1975), 295–300.

12. Philip A. Leonard and Kenneth S. Williams, *A rational sixteenth power reciprocity law*, Acta Arith. **33** (1977), 365–377.

13. J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. **11** (1965/66), 263–279.

14. Albert Leon Whiteman, *Theorems on quadratic partitions*, Proc. Nat. Acad. Sci. U.S.A. **36** (1950), 60–65.

15. Kenneth S. Williams, *A quadratic partition of primes* $\equiv 1 \pmod 7$, Math. Comp. **28** (1974), 1133–1136.

16. Kenneth S. Williams, *Elementary treatment of a quadratic partition of primes* $p \equiv 1 \pmod 7$, Illinois J. Math. **18** (1974), 608–621.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SC 29208 USA

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA K1S, 5B6