PACIFIC JOURNAL OF MATHEMATICS
Vol. 91, No. 1, 1980

SOME NEW RESIDUACITY CRITERIA

RICHARD H. HUDSON AND KENNETH S. WILLIAMS

Let e and k be integers ≥ 2 with e odd and k even. Set $2l = \mathrm{L.C.M.}(e, k)$ and let p be a prime with $p \equiv 1 \pmod{2l}$ having g as a primitive root. It is shown that the index of e (with respect to g) modulo k can be computed in terms of the cyclotomic numbers of order l. By applying this result with $e = 3$, $k = 4$; $e = 5$, $k = 4$; $e = 3$, $k = 8$; new criteria are obtained for 3 and 5 to be fourth powers $\pmod p$ and for 3 to be an eighth power $\pmod p$.

1. **Introduction.** Let e and k be integers greater than or equal to 2 with e odd and k even. Let p be a prime congruent to 1 modulo $2l$, where $2l = \mathrm{L.C.M.}(e, k)$. Let g be a fixed primitive root $\pmod p$. If a is an integer not divisible by p, the index of a with respect to g is denoted by $\operatorname{ind}(a)$ and is the least nonnegative integer b such that $a \equiv g^b \pmod p$. For $0 \leqq h, k \leqq l-1$, the cyclotomic number $(h, k)_l$ of order l is the number of integers n $(1 \leqq n \leqq p-2)$ such that $\operatorname{ind}(n) \equiv h \pmod l$, $\operatorname{ind}(n+1) \equiv k \pmod l$.

Using an idea due to Muskat [4: 257-258], we prove the following congruence for the index of e modulo k.

THEOREM 1.

$$\operatorname{ind}(e) \equiv 2 \sum_{i=1}^{k/2-1} i \sum_{j=1}^{(e-1)/2} \sum_{r=0}^{2l/k-1} \sum_{s=0}^{l/e-1} \left(i + r\frac{k}{2}, j + se\right)_l + \frac{(p-1)(e-1)^2}{8e} \pmod k .$$

Applying Theorem 1 with $e = 3$, $k = 4$, we obtain the following criterion for 3 to be a fourth power $\pmod p$.

THEOREM 2. *Let $p \equiv 1 \pmod{12}$ be a prime, so that there are integers x and y satisfying*

$$(1.1) \qquad p = x^2 + 3y^2 , \qquad x \equiv 1 \pmod 3 .$$

Then 3 is a fourth power $\pmod p$ if and only if $x \equiv 1 \pmod 4$.

This criterion should be compared with the classical result: 3 is a fourth power $\pmod p$ if and only if

$$\begin{cases} b \equiv 0 \pmod 3 , & \text{if } p \equiv 1 \pmod{24} , \\ a \equiv 0 \pmod 3 , & \text{if } p \equiv 13 \pmod{24} , \end{cases}$$

where

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

see for example [2: p. 24].

Next taking $e = 5$, $k = 4$, in Theorem 1 we obtain the following new criterion for 5 to be a fourth power $(\bmod p)$.

THEOREM 3. *Let* $p \equiv 1 \pmod{20}$ *be a prime, so that there are integers* x, u, v, *and* w *satisfying*

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 , \qquad xw = v^2 - 4uv - u^2 , \tag{1.2}$$

and

$$x \equiv 1 \pmod 5 . \tag{1.3}$$

Then 5 *is a fourth power* $(\bmod p)$ *if and only if*

$$\begin{cases} x \equiv 4 \pmod 8 , & \text{if } x \equiv 0 \pmod 2 , \\ x \equiv \pm 3w \pmod 8 , & \text{if } x \equiv 1 \pmod 2 . \end{cases}$$

This criterion should be compared with the well-known result (see for example [2: p. 24]):

5 is a fourth power $(\bmod p)$ if and only if

$$b \equiv 0 \pmod 5 , \quad \text{where} \quad p = a^2 + b^2 , \quad a \equiv 1 \pmod 4 , \quad b \equiv 0 \pmod 2 .$$

Finally, applying Theorem 1 with $e = 3$, $k = 8$, we obtain the following new criterion for 3 to be an eighth power $(\bmod p)$.

THEOREM 4. *Let* $p \equiv 1 \pmod{24}$ *be a prime so that there are integers* a, b, x *and* y *satisfying*

$$p = a^2 + b^2 = x^2 + 3y^2 , \tag{1.4}$$

and

$$a \equiv 1 \pmod 4 , \quad b \equiv 0 \pmod 4 , \quad x \equiv 1 \pmod 6 , \quad y \equiv 0 \pmod 2 . \tag{1.5}$$

Assume 3 *is a fourth power* $(\bmod p)$, *so that*

$$b \equiv 0 \pmod 3 , \qquad x \equiv 1 \pmod 4 .$$

Then 3 *is an eighth power* $(\bmod p)$ *if and only if*

$$a \equiv 1 \pmod 3 , \qquad y \equiv 0 \pmod 8 ,$$

or

$$a \equiv -1 \pmod 3 , \qquad y \equiv 4 \pmod 8 .$$

This criterion should be compared to that of von Lienen [3: p. 114], namely, if 3 is a fourth power $(\bmod p)$ then 3 is an eighth power $(\bmod p)$ if and only if

$$\begin{cases} a \equiv c \pmod 3 , & \text{if} \quad p \equiv 1 \pmod{48} , \\ a \equiv -c \pmod 3 , & \text{if} \quad p \equiv 25 \pmod{48} , \end{cases}$$

where

$$p = a^2 + b^2 = c^2 + 2d^2$$

and

$$a \equiv 1 \pmod 4 , \qquad b \equiv 0 \pmod 4 , \qquad c \equiv 1 \pmod 4 , \qquad d \equiv 0 \pmod 2 .$$

Combining these results, we see that if $(3/p)_4 = +1$ (equivalently $b \equiv 0 \pmod 3$ or $x \equiv 1 \pmod 4$), we have

$$\begin{cases} y \equiv 0 \pmod 8 \Longleftrightarrow c \equiv 1 \pmod 3 , & \text{if} \quad p \equiv 1 \pmod{48} , \\ y \equiv 0 \pmod 8 \Longleftrightarrow c \equiv -1 \pmod 3 , & \text{if} \quad p \equiv 25 \pmod{48} . \end{cases}$$

2. **Proof of Theorem 1.** The roots of the congruence

$$\frac{x^e - 1}{x - 1} \equiv 0 \pmod p \tag{2.1}$$

are

$$x \equiv g^{jf} \pmod p , \qquad j = 1, 2, \cdots, e - 1 ,$$

where $p - 1 = ef$, so that

$$x^{e-1} + x^{e-2} + \cdots + x + 1 \equiv \prod_{j=1}^{e-1} (x - g^{jf}) \pmod p . \tag{2.2}$$

Taking $x = 1$ in (2.2), we obtain

$$e \equiv \prod_{j=1}^{e-1} (1 - g^{jf}) \pmod p , \tag{2.3}$$

and so

$$\operatorname{ind}(e) \equiv \sum_{j=1}^{e-1} \operatorname{ind}(1 - g^{jf}) \pmod{p - 1} . \tag{2.4}$$

Next

$$\begin{aligned} &\sum_{j=(e+1)/2}^{e-1} \operatorname{ind}(1 - g^{jf}) \\ &\quad = \sum_{j=1}^{(e-1)/2} \operatorname{ind}(1 - g^{(e-j)f}) \end{aligned}$$

$$= \sum_{j=1}^{(e-1)/2} \operatorname{ind}(1 - g^{-jf})$$
$$\equiv \sum_{j=1}^{(e-1)/2} \operatorname{ind}(1 - g^{jf}) + \sum_{j=1}^{(e-1)/2} \operatorname{ind}(-g^{-jf}) \pmod{p-1}$$
$$\equiv \sum_{j=1}^{(e-1)/2} \operatorname{ind}(1 - g^{jf}) + \sum_{j=1}^{(e-1)/2} \left(\frac{p-1}{2} - jf\right) \pmod{p-1},$$

so

$$\operatorname{ind}(e) \equiv 2 \sum_{j=1}^{(e-1)/2} \operatorname{ind}(1 - g^{jf}) + \frac{(p-1)(e-1)^2}{8e} \pmod{p-1}. \tag{2.5}$$

Next the roots of

$$x^f - g^{jf} \equiv 0 \pmod{p}$$

are

$$x \equiv g^{ei+j} \pmod{p} \qquad (i = 1, 2, \cdots, f),$$

so

$$x^f - g^{jf} \equiv \prod_{i=1}^{f} (x - g^{ei+j}) \pmod{p}. \tag{2.6}$$

Taking $x = 1$ in (2.6), we obtain

$$1 - g^{jf} \equiv \prod_{i=1}^{f} (1 - g^{ei+j}) \pmod{p},$$

so

$$\operatorname{ind}(1 - g^{jf}) \equiv \sum_{i=1}^{f} \operatorname{ind}(1 - g^{ei+j}) \pmod{p-1}. \tag{2.7}$$

Further, working modulo $k/2$, we have

$$\sum_{i=1}^{f} \operatorname{ind}(1 - g^{ei+j})$$
$$= \sum_{\substack{n=2 \\ \operatorname{ind}(n) \equiv j \pmod{e}}}^{p-1} \operatorname{ind}(1 - n)$$
$$\equiv \sum_{\substack{n=2 \\ \operatorname{ind}(n) \equiv j \pmod{e}}}^{p-1} \operatorname{ind}(n - 1) + \sum_{\substack{n=2 \\ \operatorname{ind}(n) \equiv j \pmod{e}}}^{p-1} \operatorname{ind}(-1)$$
$$\equiv \sum_{\substack{n=1 \\ \operatorname{ind}(n+1) \equiv j \pmod{e}}}^{p-2} \operatorname{ind}(n) + \frac{p-1}{2} \sum_{\substack{n=1 \\ \operatorname{ind} n \equiv j \pmod{e}}}^{p-1} 1$$
$$\equiv \sum_{i=0}^{k/2-1} \sum_{\substack{n=1 \\ \operatorname{ind}(n) \equiv i \pmod{k/2} \\ \operatorname{ind}(n+1) \equiv j \pmod{e}}}^{p-2} i,$$

that is

$$(2.8)\qquad \sum_{i=1}^{f} \operatorname{ind}(1 - g^{ei+j}) \equiv \sum_{i=1}^{k/2-1} i \sum_{r=0}^{2l/k-1} \sum_{s=0}^{l/e-1} (i + rk/2, j + se)_l .$$

The result now follows from (2.5), (2.7) and (2.8).

3. Proof of Theorem 2. Taking $e = 3$, $k = 4$, so that $l = 6$, in Theorem 1, we obtain, for $p \equiv 1 \pmod{12}$,

$$(3.1)\qquad \operatorname{ind}(3) \equiv 2 \sum_{r=0}^{2} \sum_{s=0}^{1} (1 + 2r, 1 + 3s)_6 + \frac{p-1}{6} \pmod 4 .$$

Defining x and y, as in [6: p. 68], by

$$x = 6(0, 3)_6 - 6(1, 2)_6 + 1$$

and

$$y = (0, 1)_6 - (0, 5)_6 - (1, 3)_6 + (1, 4)_6 ,$$

so that x and y satisfy (1.1), from the tables for the cyclotomic numbers of order 6, we obtain

$$\sum_{r=0}^{2} \sum_{s=0}^{1} (1 + 2r, 1 + 3s)_6 = \frac{1}{6}(p - x - 3y) .$$

Hence, from (3.1), we obtain

$$\operatorname{ind}(3) \equiv \frac{1}{3}(p - x) - y + \frac{p-1}{6} \pmod 4 .$$

Now

$$y \equiv \begin{cases} 0 \pmod 4 , & \text{if } p \equiv 1 \pmod{24} , \\ 2 \pmod 4 , & \text{if } p \equiv 13 \pmod{24} , \end{cases}$$

that is

$$y \equiv \frac{1}{6}(p - 1) \pmod 4 ,$$

giving

$$\operatorname{ind}(3) \equiv \frac{1}{3}(p - x) \equiv \frac{1}{3}(1 - x) \pmod 4 ,$$

which completes the proof of Theorem 2.

4. Proof of Theorem 3. Taking $e = 5$, $k = 4$, so that $l = 10$, in Theorem 1, we obtain for $p \equiv 1 \pmod{20}$,

$$\text{(4.1)} \qquad \operatorname{ind}(5) \equiv 2\sum_{j=1}^{2}\sum_{r=0}^{4}\sum_{s=0}^{1}(1+2r,\, j+5s)_{10} + \frac{2}{5}(p-1) \pmod 4 .$$

Define m by $2 \equiv g^m \pmod p$. Replacing g by an appropriate power of g, we may suppose that $m \equiv 0$ or $1 \pmod 5$. Next we define x, u, v, w by

$$\begin{aligned} 3x &= -p + 14 + 25(0,0)_5 , \\ u &= (0,2)_5 - (0,3)_5 , \\ v &= (0,1)_5 - (0,4)_5 , \\ w &= (1,3)_5 - (1,2)_5 , \end{aligned}$$

so that x, u, v, w is a solution of (1.2) satisfying (1.3) (see for example [5: p. 100]). From the tables of Whiteman [5: pp. 107-109] for the cyclotomic numbers of order 10, we obtain in the case $m \equiv 0 \pmod 5$, that is, 2 is a fifth power $(\operatorname{mod} p)$ or equivalently, $x \equiv 0 \pmod 2$ [1: p. 13]:

$$\begin{aligned} &\sum_{j=1}^{2}\sum_{r=0}^{4}\sum_{s=0}^{1}(1+2r,\, j+5s)_{10} \\ &\qquad = \frac{1}{20}\{4p + x - 15u + 15v - 30w\} , \end{aligned}$$

so

$$\begin{aligned} \operatorname{ind}(5) &\equiv \frac{1}{10}\{4p + x - 15u + 15v - 30w\} \pmod 4 \\ &\equiv \frac{1}{10}(x+4) - \frac{3}{2}(u-v) + w \pmod 4 . \end{aligned}$$

Emma Lehmer [1: p. 13] has shown in this case that

$$x \equiv u \equiv v \equiv w \equiv 0 \pmod 4 , \qquad u \equiv v \pmod 8 ,$$

so that

$$\operatorname{ind}(5) \equiv \frac{1}{10}(x+4) \equiv \frac{x}{2} + 2 \pmod 4 ,$$

completing the proof of Theorem 3 in this case.

When $m \equiv 1 \pmod 5$, 2 is not a fifth power $(\operatorname{mod} p)$ and $x \equiv 1 \pmod 2$. From the tables of Whiteman [5: pp. 107-109], in this case, we obtain

$$\begin{aligned} &\sum_{j=1}^{2}\sum_{r=0}^{4}\sum_{s=0}^{1}(1+2r,\, j+5s)_{10} \\ &\qquad = \frac{1}{40}\{8p - 3x + 10u + 20v - 25w\} , \end{aligned}$$

so that

$$4 \operatorname{ind}(5) \equiv 8p - 3x + 10u + 20v - 25 \pmod{16},$$

which shows that $w \equiv 1 \pmod 2$.

Since

$$400(0, 2)_{10} = 4p - 36 + 17x + 50u - 25w,$$

we have (as $x \equiv w \equiv 1 \pmod 2$)

$$10u \equiv 3x + 5w \pmod{16},$$

so that

$$\operatorname{ind}(5) \equiv v + w \pmod 4.$$

As

$$200(0, 9)_{10} = 2p - 18 - 4x + 25u - 25v + 25w$$

and

$$200(1, 2)_{10} = 2p + 2 + x + 25u + 25v - 50w$$

we have

$$\begin{cases} u - v \equiv 4 - w \pmod 8, \\ u + v \equiv 4 + 2w - x \pmod 8, \end{cases}$$

so

$$u \equiv \frac{1}{2}(w - x) \pmod 4, \qquad v \equiv \frac{1}{2}(3w - x) \pmod 4.$$

Hence we have

$$\operatorname{ind}(5) \equiv \frac{1}{2}(5w - x) \pmod 4. \tag{4.2}$$

Since all solutions of (1.2) satisfying (1.3) are given by (see for example [1: p. 13])

$$(x, u, v, w), \quad (x, v, -u, -w), \quad (x, -u, -v, w), \quad (x, -v, u, -w),$$

(4.2) gives

$$\operatorname{ind}(5) \equiv 0 \pmod 4 \Longleftrightarrow x \equiv \pm 3w \pmod 8,$$

and

$$\operatorname{ind}(5) \equiv 2 \pmod 4 \Longleftrightarrow x \equiv \pm w \pmod 8,$$

which completes the proof of Theorem 3.

5. Proof of Theorem 4. Taking $e = 3$, $k = 8$ so that $l = 12$, in Theorem 1, we obtain, for $p \equiv 1 \pmod{24}$,

$$\text{ind}\,(3) \equiv 2\sum_{i=1}^{3} i \sum_{r=0}^{2}\sum_{s=0}^{3} (i + 4r, 1 + 3s)_{12} + \frac{1}{6}(p-1) \pmod 8 . \tag{5.1}$$

Following Whiteman [6: p. 64], we define m and m' by $2 \equiv g^m \pmod p$ and $3 \equiv g^{m'} \pmod p$ respectively. As $p \equiv 1 \pmod 8$ we have $m \equiv 0 \pmod 2$. Replacing g by an appropriate power of g we may suppose that $m \equiv 0$ or $2 \pmod 3$, so that $m \equiv 0$ or $2 \pmod 6$. Further, as we are assuming 3 is a fourth power $(\text{mod}\, p)$, we have $m' \equiv 0 \pmod 4$. Next we define x and y (as in [6: p. 68]) by

$$x = 6(0, 3)_6 - 6(1, 2)_6 + 1 ,$$
$$y = (0, 1)_6 - (0, 5)_6 - (1, 3)_6 + (1, 4)_6 ,$$

and a and b by equations (4.4) and (4.5) in [6] (a replaces Whiteman's x, b replaces Whiteman's $2y$). Then x, y, a, b satisfy (1.4) and (1.5). Whiteman [6: pp. 69–73] gives the cyclotomic numbers of order 12 in terms of x, y, a and b, as defined above. When $m \equiv 0 \pmod 6$, we must use Tables 9 and 10 of [6] and, when $m \equiv 2 \pmod 6$, we must use Tables 3 and 4. By considering the cyclotomic numbers $(3, 6)_{12}$ in Table 9; $(2.4)_{12}$ in Table 10; $(1, 2)_{12}$ in Table 3; $(2, 8)_{12}$ in Table 4; it is easy to check that Whiteman's quantity $c = \pm 1$ (see [6: pp. 64–65]) satisfies

$$\begin{cases} c = +1 \Longleftrightarrow a \equiv 1 \pmod 3 , \\ c = -1 \Longleftrightarrow a \equiv 2 \pmod 3 . \end{cases} \tag{5.2}$$

We remark that $a \not\equiv 0 \pmod 3$ as 3 is assumed to be a fourth power $(\text{mod}\, p)$.

Next we set

$$\sum_i = \sum_{r=0}^{2}\sum_{s=0}^{3} (i + 4r, 1 + 3s)_{12} \qquad (i = 1, 2, 3) ,$$

so that

$$\text{ind}\,(3) \equiv 2\Big(\sum_1 + 2\sum_2 + 3\sum_3\Big) + \frac{1}{6}(p-1) \pmod 8 . \tag{5.3}$$

From Whiteman's tables, we obtain

$$12\sum_1 = \begin{cases} p - 2b - x - 3y , & \text{if } a \equiv 1 \pmod 3 , \\ p + 2b - x - 3y , & \text{if } a \equiv -1 \pmod 3 , \end{cases}$$
$$12\sum_2 = \begin{cases} p - 2a + x + 3y , & \text{if } a \equiv 1 \pmod 3 , \\ p + 2a + x + 3y , & \text{if } a \equiv -1 \pmod 3 , \end{cases}$$

$$12 \sum_3 = \begin{cases} p + 2b - x - 3y, & \text{if } a \equiv 1 \pmod 3, \\ p - 2b - x - 3y, & \text{if } a \equiv -1 \pmod 3. \end{cases}$$

From (5.3) and (5.4) we obtain

(5.5) $\operatorname{ind}(3)$

$$\equiv \begin{cases} 1 - \frac{1}{3}(2a-2b+x) - y + \frac{1}{6}(p-1) \pmod 8, & \text{if } a \equiv 1 \pmod 3, \\ 1 + \frac{1}{3}(2a-2b-x) - y + \frac{1}{6}(p-1) \pmod 8, & \text{if } a \equiv -1 \pmod 3. \end{cases}$$

Also, from Whiteman's tables, we have in every case,

$$p + 1 - 8a + 6x \equiv 0 \pmod{16},$$

so

$\operatorname{ind}(3)$

$$\equiv \begin{cases} 1+2a-2b+\frac{p+1}{2}-4a-y+\frac{1}{6}(p-1) \pmod 8, & \text{if } a \equiv 1 \pmod 3, \\ 1-2a+2b+\frac{p+1}{2}-4a-y+\frac{1}{6}(p-1) \pmod 8, & \text{if } a \equiv -1 \pmod 3, \end{cases}$$

$$\equiv \begin{cases} -y \pmod 8, & \text{if } a \equiv 1 \pmod 3, \\ 4 - y \pmod 8, & \text{if } a \equiv -1 \pmod 3, \end{cases}$$

which completes the proof of Theorem 4.

References

1. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J., **18** (1951), 11-18.
2. ———, *Criteria for cubic and quartic residuacity*, Mathematika, **5** (1958), 20-29.
3. H. von Lienen, *Primzahlen als achte Potenzreste*, J. Reine Angew. Math., **266** (1974), 107-117.
4 J. B. Muskat, *On the solvability of* $x^e \equiv e \pmod p$, Pacific J. Math., **14** (1964), 257-260.
5. A. L. Whiteman, *The cyclotomic number of order ten*, Proceedings of the Symposia in Applied Mathematics **10**, pp. 95-111, Amer. Math. Soc., Providence, Rhode Island, 1960.
6. ———, *The cyclotomic numbers of order twelve*, Acta Arith., **6** (1960), 53-76.

Received October 26, 1979. Research supported by the Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

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