SOME NEW RESIDUACITY CRITERIA

RICHARD HOWARD HUDSON AND KENNETH S. WILLIAMS
SOME NEW RESIDUACITY CRITERIA

Richard H. Hudson and Kenneth S. Williams

Let \( e \) and \( k \) be integers \( \geq 2 \) with \( e \) odd and \( k \) even. Set \( 2l = \text{L.C.M.} (e, k) \) 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 (mod \( p \)) and for 3 to be an eighth power (mod \( p \)).

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 \( 2l = \text{L.C.M.} (e, k) \). Let \( g \) be a fixed primitive root (mod \( p \)). If \( a \) is an integer not divisible by \( p \), the index of \( a \) with respect to \( g \) is denoted by \( \text{ind}(a) \) and is the least nonnegative integer \( b \) such that \( a = g^b \pmod{p} \). For \( 0 \leq h, \ k \leq l - 1 \), the cyclotomic number \((h, k)\), of order \( l \) is the number of integers \( n \) (\( 1 \leq n \leq p - 2 \)) such that \( \text{ind}(n) = h \pmod{l} \), \( \text{ind}(n + 1) = k \pmod{l} \).

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

**Theorem 1.**

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

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

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

\[
p = x^2 + 3y^2, \quad x \equiv 1 \pmod{3}.
\]

Then 3 is a fourth power (mod \( p \)) if and only if \( x \equiv 1 \pmod{4} \).

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

\[
\begin{align*}
&b \equiv 0 \pmod{3}, &\text{if } &p \equiv 1 \pmod{24}, \\
&a \equiv 0 \pmod{3}, &\text{if } &p \equiv 13 \pmod{24},
\end{align*}
\]

135
where
\[ p = a^2 + b^2, \quad a \equiv 1 \pmod{4}, \quad b \equiv 0 \pmod{2}, \]
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 \((\pmod{p})\).

**Theorem 3.** Let \( p \equiv 1 \pmod{20} \) be a prime, so that there are integers \( x, u, v, \) and \( w \) satisfying
\[
16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad xw = v^2 - 4uv - u^2,
\]
and
\[
x \equiv 1 \pmod{5}.
\]
Then 5 is a fourth power \((\pmod{p})\) 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 \((\pmod{p})\) 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 \((\pmod{p})\).

**Theorem 4.** Let \( p \equiv 1 \pmod{24} \) be a prime so that there are integers \( a, b, x \) and \( y \) satisfying
\[
p = a^2 + b^2 = x^2 + 3y^2,
\]
and
\[
a \equiv 1 \pmod{4}, \quad b \equiv 0 \pmod{4}, \quad x \equiv 1 \pmod{6}, \quad y \equiv 0 \pmod{2}.
\]
Assume 3 is a fourth power \((\pmod{p})\), so that
\[
b \equiv 0 \pmod{3}, \quad x \equiv 1 \pmod{4}.
\]
Then 3 is an eighth power \((\pmod{p})\) if and only if
\[
a \equiv 1 \pmod{3}, \quad y \equiv 0 \pmod{8},
\]
or
\[
a \equiv -1 \pmod{3}, \quad y \equiv 4 \pmod{8}.
\]
This criterion should be compared to that of von Lienen [3: p. 114], namely, if $3$ is a fourth power $\pmod{p}$ then $3$ is an eighth power $\pmod{p}$ if and only if

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

where

$$p = a^2 + 6^2 = c^2 + 2d^2$$

and

$$a \equiv 1 \pmod{4}, \quad b \equiv 0 \pmod{4}, \quad c \equiv 1 \pmod{4}, \quad d \equiv 0 \pmod{2}.$$ 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

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

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

$$
(2.1) \quad \frac{x^e - 1}{x - 1} = 0 \pmod{p}
$$

are

$$x \equiv g^{j\ell} \pmod{p}, \quad j = 1, 2, \ldots, e - 1,$$

where $p - 1 = ef$, so that

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

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

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

and so

$$
(2.4) \quad \text{ind} \ (e) \equiv \sum_{j=1}^{e-1} \text{ind} \ (1 - g^{j\ell}) \pmod{p - 1}.
$$

Next

$$
\sum_{j=\lceil (e-1)/2 \rceil}^{e-1} \text{ind} \ (1 - g^{j\ell})
= \sum_{j=1}^{\lceil (e-1)/2 \rceil} \text{ind} \ (1 - g^{(e-j-1)\ell})
$$
\[
\begin{align*}
\sum_{j=1}^{(e-1)/2} \text{ind} (1 - g^{-ij}) &= \sum_{j=1}^{(e-1)/2} \text{ind} (1 - g^{ij}) + \sum_{j=1}^{(e-1)/2} \text{ind} (-g^{-ij}) \pmod{p - 1} \\
&\equiv \sum_{j=1}^{(e-1)/2} \text{ind} (1 - g^{ij}) + \sum_{j=1}^{(e-1)/2} \left( \frac{p - 1}{2} - jf \right) \pmod{p - 1},
\end{align*}
\]

so
\[
(2.5) \quad \text{ind} (e) \equiv 2 \sum_{j=1}^{(e-1)/2} \text{ind} (1 - g^{ij}) + \frac{(p - 1)(e - 1)^2}{8e} \pmod{p - 1}.
\]

Next the roots of
\[
x^f - g^{ij} \equiv 0 \pmod{p}
\]
are
\[
x \equiv g^{e^{i+j}} \pmod{p} \quad (i = 1, 2, \ldots, f),
\]
so
\[
(2.6) \quad x^f - g^{ij} \equiv \prod_{i=1}^{f} (x - g^{e^{i+j}}) \pmod{p}.
\]

Taking \(x = 1\) in (2.6), we obtain
\[
1 - g^{ij} \equiv \prod_{i=1}^{f} (1 - g^{e^{i+j}}) \pmod{p},
\]
so
\[
(2.7) \quad \text{ind} (1 - g^{ij}) \equiv \sum_{i=1}^{f} \text{ind} (1 - g^{e^{i+j}}) \pmod{p - 1}.
\]

Further, working modulo \(k/2\), we have
\[
\sum_{i=1}^{f} \text{ind} (1 - g^{e^{i+j}})
\]
that is
\[
\sum_{i=1}^{p-1} \text{ind} (n) \pmod{p - 1}
\]
\[
\equiv \sum_{\text{ind}(n) \equiv f \pmod{k/2}} \text{ind} (n - 1) + \sum_{\text{ind}(n) \equiv f \pmod{k/2}} \text{ind} (-1)
\]
\[
\equiv \sum_{n=1}^{p-2} \text{ind} (n + 1) \pmod{p - 1}
\]
\[
\equiv \sum_{n=0}^{p-2} \text{ind} (n) - \sum_{n=1}^{p-2} \frac{p - 1}{2} \pmod{p - 1},
\]
that is
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 \( p \equiv 1 \pmod{12} \),

\[
(3.1) \quad \text{ind} (3) = 2 \sum_{r=0}^{2} \sum_{s=0}^{1} (1 + 2r, 1 + 3s) + \frac{p-1}{6} \pmod{4}.
\]

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

\[
x = 6(0, 3) - 6(1, 2) + 1
\]

and

\[
y = (0, 1) - (0, 5) - (1, 3) + (1, 4),
\]

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

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

Hence, from (3.1), we obtain

\[
\text{ind} (3) \equiv \frac{1}{3} (p - x) - y + \frac{p-1}{6} \pmod{4}.
\]

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

\[
\text{ind} (3) \equiv \frac{1}{3} (p - x) \equiv \frac{1}{3} (1 - x) \pmod{4},
\]

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 \( p \equiv 1 \pmod{20} \),
\[(4.1) \quad \text{ind} (5) = 2 \sum_{j=1}^{4} \sum_{r=0}^{4} \sum_{s=0}^{4} (1 + 2r, j + 5s)_{10} + \frac{2}{5}(p - 1) \pmod{4}.
\]

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

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

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 \((\pmod{p})\) or equivalently, \(x \equiv 0 \pmod{2}\) [1: p. 13]:

\[
\sum_{j=1}^{4} \sum_{r=0}^{4} \sum_{s=0}^{4} (1 + 2r, j + 5s)_{10}
= \frac{1}{20} \{4p + x - 15u + 15v - 30w\},
\]

so

\[
\text{ind} (5) \equiv \frac{1}{10} \{4p + x - 15u + 15v - 30w\} \pmod{4}
\equiv \frac{1}{10} (x + 4) - \frac{3}{2} (u - v) + w \pmod{4}.
\]

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

\[
x \equiv u \equiv v \equiv w \equiv 0 \pmod{4}, \quad u \equiv v \pmod{8},
\]

so that

\[
\text{ind} (5) \equiv \frac{1}{10} (x + 4) \equiv \frac{x}{2} + 2 \pmod{4},
\]

completing the proof of Theorem 3 in this case.

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

\[
\sum_{j=1}^{4} \sum_{r=0}^{4} \sum_{s=0}^{4} (1 + 2r, j + 5s)_{10}
= \frac{1}{40} \{8p - 3x + 10u + 20v - 25w\},
\]
so that
\[ 4 \text{ind} (5) = 8p - 3x + 10u + 20v - 25 \pmod{16}, \]
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
\[ \text{ind} (5) \equiv v + w \pmod{4}. \]

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
\[ u \equiv \frac{1}{2}(w - x) \pmod{4}, \quad v \equiv \frac{1}{2}(3w - x) \pmod{4}. \]

Hence we have
\[ (4.2) \quad \text{ind} (5) \equiv \frac{1}{2}(5w - x) \pmod{4}. \]

Since all solutions of (1.2) satisfying (1.3) are given by (see for example [1: p. 13])
\( (x, u, v, w), \ (x, v, -u, -w), \ (x, -u, -v, w), \ (x, -v, u, -w), \)
(4.2) gives
\[ \text{ind} (5) \equiv 0 \pmod{4} \iff x \equiv \pm 3w \pmod{8}, \]
and
\[ \text{ind} (5) \equiv 2 \pmod{4} \iff x \equiv \pm w \pmod{8}, \]
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 \( p \equiv 1 \pmod{24} \),

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

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 \( \pmod{p} \), 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

\[
(5.2) \quad \begin{cases} 
\{ c = +1 & \iff a \equiv 1 \pmod{3} , \\
\{ c = -1 & \iff a \equiv 2 \pmod{3} .
\end{cases}
\]

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

Next we set

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

so that

\[
(5.3) \quad \text{ind} (3) \equiv 2 \left( \sum_1 + 2 \sum_2 + 3 \sum_3 \right) + \frac{1}{6} (p - 1) \pmod{8}.
\]

From Whiteman’s tables, we obtain

\[
12 \sum_{1} = \begin{cases} 
(p - 2b - x - 3y) , & \text{if } a \equiv 1 \pmod{3} , \\
p + 2b - x - 3y , & \text{if } a \equiv -1 \pmod{3} ,
\end{cases}
\]
\[
12 \sum_{2} = \begin{cases} 
(p - 2a + x + 3y) , & \text{if } a \equiv 1 \pmod{3} , \\
p + 2a + x + 3y , & \text{if } a \equiv -1 \pmod{3} ,
\end{cases}
\]
\[
12 \sum_{3} = \begin{cases} 
p - 2b - x - 3y , & \text{if } a \equiv 1 \pmod{3} , \\
p + 2b - x - 3y , & \text{if } a \equiv -1 \pmod{3} .
\end{cases}
\]
\[ 12 \sum_{a} = \begin{cases} 
  p + 2b - x - 3y, & \text{if } a \equiv 1 \pmod{3}, \\
  p - 2b - x - 3y, & \text{if } a \equiv -1 \pmod{3}.
\end{cases} \]

From (5.3) and (5.4) we obtain

\[ (5.5) \quad \text{ind}(3) = \begin{cases} 
  1 - \frac{1}{3}(2a-2b+x)-y + \frac{1}{6}(p-1) \pmod{8}, & \text{if } a \equiv 1 \pmod{3}, \\
  1 + \frac{1}{3}(2a-2b-x)-y + \frac{1}{6}(p-1) \pmod{8}, & \text{if } a \equiv -1 \pmod{3}.
\end{cases} \]

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

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

so

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

which completes the proof of Theorem 4.

**References**


Received October 26, 1979. Research supported by the Natural Sciences and Engineering Research Council Canada Grant No. A-7233.
Harvey Leslie Abbott, *Extremal problems on nonaveraging and nondividing sets* ......................................................... 1
Marine Bruce Abrahamse and Stephen D. Fisher, *Mapping intervals to intervals* .............................................................. 13
William Wells Adams, *The best two-dimensional Diophantine approximation constant for cubic irrationals* ......................... 29
Marilyn Breen, *A quantitative version of Krasnosel’skiǐ’s theorem in \( \mathbb{R}^2 \) ................................................................. 31
Stephen LaVern Campbell, *Linear operators for which \( T^*T \) and \( TT^* \) commute. III* ..................................................... 39
Zvonko Cerin, *On cellular decompositions of Hilbert cube manifolds* ................................................................. 47
J. R. Choike, Ignacy I. Kotlarski and V. M. Smith, *On a characterization using random sums* ........................................... 71
Karl-Theodor Eisele, *Direct factorizations of measures* ............. 79
Douglas Harris, *Every space is a path component space* ............ 95
John P. Holmes and Arthur Argyle Sagle, *Analytic H-spaces, Campbell-Hausdorff formula, and alternative algebras* .................. 105
Richard Howard Hudson and Kenneth S. Williams, *Some new residuacity criteria* .......................................................... 135
V. Karunakaran and Michael Robert Ziegler, *The radius of starlikeness for a class of regular functions defined by an integral* .......... 145
Ka-Sing Lau, *On the Banach spaces of functions with bounded upper means* .............................................................. 153
Daniel Paul Maki, *On determining regular behavior from the recurrence formula for orthogonal polynomials* ........................ 173
Stephen Joseph McAdam, *Asymptotic prime divisors and going down* ................. 179
Kent Morrison, *The scheme of finite-dimensional representations of an algebra* ............................................................ 199
Donald P. Story, *A characterization of the local Radon-Nikodým property by tensor products* .......................................... 219
Arne Stray, *Two applications of the Schur-Nevanlinna algorithm* .... 223
N. B. Tinberg, *The Levi decomposition of a split \((B, N)\)-pair* .............. 233
Charles Irvin Vinsonhaler and William Jennings Wickless, *A theorem on quasi-pure-projective torsion free abelian groups of finite rank* . 239
Yitzhak Weit, *Spectral analysis in spaces of vector valued functions* .... 243