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 $2l = \text{L. C. M.}\ (e, k)$ 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 $a \equiv g^b \pmod{p}$. 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 $\text{ind}\,(n) \equiv h \pmod{l}$, $\text{ind}\,(n + 1) \equiv k \pmod{l}$.

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

THEOREM 1.

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

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

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

$$p = x^2 + 3y^2\,, \qquad x \equiv 1 \pmod{3}\ . \tag{1.1}$$

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

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