ON THE DISTRIBUTION OF k-TH POWER NONRESIDUES

BY RICHARD H. HUDSON

1. Introduction. Let k be a positive integer. Throughout this paper p will denote a prime congruent to 1 modulo k. Let $C(p)$ denote the multiplicative group consisting of the residue classes modulo p and let $g(p, k)$ be the smallest k-th power nonresidue. Finally, let l denote the maximum number of consecutive integers in any given residue class.

Using deep analytic methods, Burgess [2] has shown that for $k = 2, l = O(p^{1/4+\delta})$ for every positive δ. Estimates for l employing elementary methods are less exact but are valid for every prime p and consequently are of interest. In 1932 Brauer [1], using elementary methods, showed that for each p

$$l < (2p)^{1/2} + 2. \tag{1.1}$$

Let l_n denote the maximum number of consecutive integers in any of the $k - 1$ nonresidue classes. In 1971 the author [3] showed that for $k = 2$ and each prime p

$$l_n < p^{1/2} + 3/4\ \sqrt{2}\ p^{1/4} + 2. \tag{1.2}$$

This bound was previously shown by Brauer [1] to hold for all primes p with $g(p, k) < \sqrt{2}p^{1/4}$. In this paper a bound comparable to (1.2), namely,

$$l_n < p^{1/2} + 2^{2/3}p^{1/3} + 2^{1/3}p^{1/6} + 1, \tag{1.3}$$

will be shown to hold for all k and all $p \equiv 1 \pmod{k}$. The method of proof is purely elementary and furthermore illustrates an interesting connection between large values of l_n and upper bounds for $g(p, k)$.

2. A preliminary theorem.

THEOREM 1. *For* $1/3 \leq \alpha \leq 1/2$, $g(p, k) \geq 2^{2/3}p^{\alpha} + 2^{1/3}p^{\alpha/2} + 1 \Rightarrow l_n < p^{1-3\alpha/2} + 2^{4/3}p^{\alpha/2} + 2^{-1/3}p^{1-2\alpha} + 1$.

Proof. Designate the longest sequence of k-th power nonresidues by

$$\bar{Q} = \{Q, Q + 1, \cdots, Q + l_n - 1\}. \tag{2.1}$$

Let r be a residue with $1 \leq r < g(p, k)$, $(g(p, k) - 1)^2 > p/r$, and $r \leq l_n$. Consider all multiples of r contained in $\bar{Q}$, say

$$br, (b + 1)r, \cdots, (b + c - 1)r \tag{2.2}$$

where $c \geq 1$. This yields a sequence of c nonresidues, namely,

$$\bar{B} = \{b, b + 1, \cdots, b + c - 1\}. \tag{2.3}$$

Received October 15, 1971.