BOUNDS ON THE N-TH POWER RESIDUES (MOD P)

S. Chowla and H. London

For p a prime $\equiv 1 \pmod{n}$, where n is an odd positive integer, let $k(p, n)$ denote the least integer k such that the numbers x^n and $(-x)^n$, where $x = 1, 2, \ldots, k$, yield all the non-zero n-th power residues (mod p) (possibly with repetitions). Clearly

$$k(p, n) < \tfrac{1}{2} p .$$

THEOREM. $k(p, n) < (\frac{1}{2} - \frac{1}{2n})\, p$.

Proof. Suppose x_0 is a solution of

(1) $x^n \equiv m \pmod{p}$.

Then $x_i = x_0 g^{i(p-1)/n}$, $i = 1, 2, \ldots, n-1$, where g is a primitive root (mod p), are also solutions of (1). Let $b = g^{(p-1)/n}$ so that $x_i = x_0 b^i$. Note that

$$x_0 + x_1 + \ldots + x_{n-1} = x_0 \frac{b^n - 1}{b - 1} \equiv 0 \pmod{p} .$$

Suppose that

$$x_0 + x_1 + \ldots + x_{n-1} = kp, \qquad 1 \le k \le (n-1)/2 .$$

Then there is at least one i such that $0 < x_i < kp/n$, for if $x_i > kp/n$ for all i we get a contradiction. Now suppose that

$$x_0 + x_1 + \ldots + x_{n-1} = kp, \qquad (n+1)/2 \le k \le n-1 .$$

Then there is at least one i such that $p > x_i > kp/n$, for if $x_i < kp/n$

https://doi.org/10.4153/CMB-1969-090-3 Published online by Cambridge University Press

for all i we get a contradiction. Thus

$$0 < p - x_i < (\frac{1}{2} - \frac{1}{2n})\, p .$$

Remark. Note that

$$\begin{aligned} 2k(p, n) &\geqq \text{number of non-zero residues of } x^n \pmod p \\ &= (p-1)/n , \end{aligned}$$

so

$$k(p, n) \geq (p-1)/2n .$$

Thus, for n fixed and small, p large in comparison with n,

$$p/2n + O(1) \leq k(p, n) < (\frac{1}{2} - \frac{1}{2n})\, p .$$

It would be interesting to know if

$$k(p \quad n) = 2(n)p + \text{error}$$

as $p \to \infty$.

Pennsylvania State University

McGill University

https://doi.org/10.4153/CMB-1969-090-3 Published online by Cambridge University Press