PACIFIC JOURNAL OF MATHEMATICS
Vol. 16, No. 1, 1966

THE DISTRIBUTION OF CUBIC AND QUINTIC NON-RESIDUES

JAMES H. JORDAN

For a prime $p \equiv 1 \pmod 3$, the reduced residue system S_3, modulo p, has a proper multiplicative subgroup, C^0, called the cubic residues modulo p. The other two cosets formed with respect to C^0, say C^1 and C^2, are called classes of cubic non-residues. Similarly for a prime $p \equiv 1 \pmod 5$ the reduced residue system S_5, modulo p, has a proper multiplicative subgroup, Q^0, called the quintic residues modulo p. The other four cosets formed with respect to Q^0, say Q^1, Q^2, Q^3 and Q^4 are called classes of quintic non-residues. Two functions, $f_3(p)$ and $f_5(p)$, are sought so that (i) if $p \equiv 1 \pmod 3$ then there are positive integers $a_i \in C^i$, $i = 1, 2$, such that $a_i < f_3(p)$, and (ii) if $p \equiv 1 \pmod 5$ then there are positive integers $a_i \in Q^i$, $i = 1, 2, 3, 4$ such that $a_i < f_5(p)$. The results established in this paper are that for p sufficiently large, (i) $f_3(p) = p^{\alpha+\varepsilon}$, where α is approximately .191, and (ii) $f_5(p) = p^{\beta+\varepsilon}$, where $.27 < \beta < .2725$.

Davenport and Erdös [3] raised the general question about the size of the smallest element in any given class of kth power non-residues. The special cases $k = 3$ and $k = 5$ are of primary concern in this paper. They proved a quite general theorem of which two special cases are:

THEOREM A. *For sufficiently large primes $p \equiv 1 \pmod 3$ and $\varepsilon > 0$ each class of cubic non-residues possess a positive integer smaller than $p^{55/112+\varepsilon}$.*

THEOREM B. *For sufficiently large primes $p \equiv 1 \pmod 5$ and $\varepsilon > 0$ each class of quintic non-residues possess a positive integer smaller than $p^{197/396+\varepsilon}$.*

In the same paper Davenport and Erdös used a result of de Bruijn [2] to improve the constant of Theorem A to approximately .383.

Recently D. A. Burgess [1] succeeded in improving Polya's inequality concerning character sums. Burgess' result is

THEOREM C. *If p is a prime and if χ is a nonprincipal character, modulo p, and if H and r are arbitrary positive integers then*

Received April 8, 1963 and in revised form May 4, 1964.