PAIRS OF CONSECUTIVE PRIMITIVE ROOTS MODULO A PRIME

EMANUEL VEGH

A. Brauer [1] has shown that given an integer N, there are at least N consecutive quadratic nonresidues modulo p for all sufficiently large primes p. A similar result, if true, for the primitive roots modulo p appears to be difficult to prove. A. Brauer has asked (oral communication) if, for all sufficiently large primes, there is a pair of consecutive primitive roots. In this direction we prove the

THEOREM. *If p is a prime greater than 3 such that $\Phi(p-1)/(p-1) > 1/3$, where Φ is the Euler totient function, then p has consecutive primitive roots.*

First, we prove the

LEMMA. *If p is a prime greater than 3 then exactly half the primitive roots modulo p are followed by quadratic nonresidues.*

PROOF OF THE LEMMA. Let ξ be a primitive root modulo p. Now $p-1$ and $p-2$ are relatively prime and therefore ξ^{p-2} is also a primitive root modulo p. Furthermore $\xi \not\equiv \xi^{p-2} \bmod p$ since $p \neq 3$. Since ξ is also a quadratic nonresidue, it follows from the congruence

$$\xi(\xi^{p-2}+1) = \xi^{p-1} + \xi \equiv \xi + 1 \qquad \text{modulo } p$$

that $\xi+1$ is a quadratic nonresidue if and only if $\xi^{p-2}+1$ is a quadratic residue. Thus exactly one of the primitive roots ξ and ξ^{p-2} is followed by a quadratic nonresidue. It is easy to see that if η is a primitive root incongruent to ξ and ξ^{p-2} then η^{p-2} is also incongruent to ξ and ξ^{p-2}. The lemma then follows by considering all pairs of primitive roots ξ and ξ^{p-2}.

PROOF OF THE THEOREM. Let p be a prime greater than 3 such that $\Phi(p-1)/(p-1) > 1/3$. If we assume that there are no consecutive primitive roots modulo p, then using the Lemma, one half of the $\Phi(p-1)$ primitive roots are followed by quadratic nonresidues, no one of which is a primitive root. Since each of the primitive roots is a quadratic nonresidue it follows that there are then at least $(3/2)\Phi(p-1)$ quadratic nonresidues. Since there is a total $(p-1)/2$ quadratic nonresidues, $(3/2)\Phi(p-1) \leq (p-1)/2$, a contradiction. The theorem is thus proved.

Received by the editors June 13, 1967.

It might be noted that, as a consequence of the theorem cited in [1], for all sufficiently large primes of the form 2^n+1, there are arbitrarily long sequences of primitive roots, since here each quadratic nonresidue is also a primitive root.

Reference

1. A. Brauer, *Über Sequenzen von Potenzresten*, S.-B. Preuss. Akad. Wiss., 1928, pp. 9–16.

Naval Research Laboratory, Washington, D. C.