CRITERION FOR rTH POWER RESIDUACITY

N. C. ANKENY

The Law of Quadratic Reciprocity in the rational integers states: If p, q are two distinct odd primes, then q is a square $(\bmod p)$ if and only if $(-1)^{(p-1)/2}p$ is a square $(\bmod q)$.

One of the classical generalizations of the law of reciprocity is of the following type. Let r be a fixed positive integer, $\phi(r)$ denotes the number of positive integers $\leq r$ which are relatively prime to r; p, q are two distinct primes and $p \equiv 1 \pmod r$. Then can we find rational integers $a_1(p), a_2(p), \cdots, a_h(p)$ determined by p, such that q is an rth power $(\bmod p)$ if and only if $a_1(p), \cdots, a_h(p)$ satisfy certain conditions $(\bmod q)$.

The Law of Quadratic Reciprocity states that for $r = 2$, we may take $a_1(p) = (-1)^{(p-1)/2}p$.

Jacobi and Gauss solved this problem for $r = 3$ and $r = 4$, respectively. Mrs. E. Lehmer gave another solution recently [2].

In this paper I would like to develop the theory when r is a prime and $q \equiv 1 \pmod r$. I then show that q is an rth power $(\bmod p)$ if and only if a certain linear combination of $a_1(p), \cdots, a_{r-1}(p)$ is an rth power $(\bmod q)$. $a_1(p), \cdots, a_{r-1}(p)$ are determined by solving several simultaneous Diophantine equations. This determination appears mildly formidable and to make the actual numerical computations would certainly be so for a large r. (See Theorem B below.) Also given is a criterion for when r is an rth power $(\bmod p)$ in terms of a linear combination of $a_1(p), \cdots, a_{r-1}(p) \pmod{r^2}$. (See Theorem A below.)

It is possible by the methods developed in this paper to eliminate the conditions that r is a prime and $q \equiv 1 \pmod r$. This would complicate the paper a great deal, and the cases given clearly indicate the underlying theory.

Consider the following Diophantine equations in the rational integers:

$$(1) \qquad r\sum_{j=1}^{r-1} X_j^2 - \left(\sum_{j=1}^{r-1} X_j\right)^2 = (r-1)p^{r-2}$$

$$(2) \qquad \sum\nolimits_1^{(1)} X_{j_1}X_{j_2} = \sum\nolimits_i^{(1)} X_{j_1}X_{j_2} \qquad i = 2, \cdots, \frac{r-1}{2},$$

where $\sum_i^{(k)}$ denotes the sum over all $j_1, \cdots, j_{k+1} = 1, 2, \cdots, r-1$, with the condition $j_1 + \cdots + j_k - kj_{k+1} \equiv i \pmod r$.

Received April 24, 1959; in revised form January, 1960. This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract No. AF 18 (603)-90. Reproduction in whole or in part is permitted for any purpose of the United States Government.