ON THE NUMBER OF SOLUTIONS OF $u^k + D \equiv w^2 \pmod p$

EMMA LEHMER

Introduction. The number $N_k(D)$ of solutions (u, w) of the congruence

$$(1) \qquad u^k + D \equiv w^2 \pmod p$$

can be expressed in terms of the Gaussian cyclotomic numbers (i, j) of order LCM$(k, 2)$ as has been done by Vandiver [7], or in terms of the character sums introduced by Jacobsthal [4] and studied in special cases by von Schrutka [6], Chowla [1], and Whiteman [8]. In the special cases $k = 3, 4, 5, 6$, and 8, the answer can be expressed in terms of certain quadratic partitions of p, but unless D is a kth power residue there remained an ambiguity in sign, which we will be able to eliminate in some cases in the present paper. Theorems 2 and 4 were first conjectured from the numerical evidence provided by the SWAC and later proved by the use of cyclotomy. They improve Jacobsthal's results for all p for which 2 is not a quartic residue. Similarly Theorem 6 improves von Schrutka's and Chowla's results for those p's which do not have 2 for a cubic residue. Only in case $k = 2$ and in the cases where k is oddly even and D is a $(k/2)$th but not a kth power residue is $N_k(D)$ a function of p alone and is in fact $p - 1$. This result appears in Theorem 1. In case $k = 4$, Vandiver [7a] gives an unambiguous solution, which requires the determination of a primitive root.

1. Character sums. It is clear that the number of solutions $N_k(D)$ of (1) can be written

$$N_k(D) = \sum_{u=0}^{p-1} \left[1 + \left(\frac{u^k + D}{p}\right)\right] = p + \sum_{u=0}^{p-1} \left(\frac{u^k + D}{p}\right),$$

or

$$(2) \qquad N_k(D) = p + \left(\frac{D}{p}\right) + \psi_k(D),$$

Received July 10, 1953.
Pacific J. Math. 5 (1955), 103-118