THE NUMBER OF SOLUTIONS OF CERTAIN QUINTIC CONGRUENCES

By H. S. Hayashi

1. Introduction. In the first of a series of three memoirs, Dickson [3] showed that if p is a prime $\equiv 1 \pmod 5$, then there are exactly four integral simultaneous solutions of the pair of diophantine equations

$$(1.1)\qquad \begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - 4uv - u^2, \end{aligned}$$

with x uniquely determined by the condition $x \equiv 1 \pmod 5$. The four solutions are given by

$$(1.2)\qquad \begin{aligned} &(1)\quad (x, u, v, w), &&(3)\quad (x, v, -u, -w), \\ &(2)\quad (x, -v, u, -w), &&(4)\quad (x, -u, -v, w). \end{aligned}$$

Let n be an arbitrary integer and let a_i, $(i = 1, 2, \cdots, m)$, be integers relatively prime to p for $p \equiv 1 \pmod 5$. In this paper, formulas expressing the number of solutions, N_m^5, of the quintic congruence

$$(1.3)\qquad n \equiv \sum_{i=1}^{m} a_i y_i^5 \pmod{p^L}$$

are obtained in terms of x, u, v and w. The technique employed utilizes elementary properties of finite trigonometric sums and cyclotomic numbers. We consider the cases $m = 1$ to $m = 5$, but the method serves for arbitrary values of m. Indeed for sums of arbitrary e-th powers with $p \equiv 1 \pmod e$, the method can be used whenever explicit formulas for cyclotomic numbers of order e exist.

It is shown in article 5 that (1.3) with $m \geq 5$ is always solvable. For $m < 5$, the insolvable cases are determined. For the homogeneous case, where $n \equiv 0 \pmod{p^L}$, there always exist non-trivial solutions if $m \geq 4$. For $m < 4$, the conditions under which only trivial solutions exist are established.

Regarding previous research on congruences of this type, we note that Dickson [2] determined N_m^e for e arbitrary, $L = 1$, and $a_i = 1$ for all i. More recently, Cohen [1] determined N_m^3 for $p \equiv 1 \pmod 3$.

2. Some aspects of cyclotomy. Let e be a fixed integer. Consider a prime p of the form $p = ef + 1$ and let g be a primitive root of p. For each pair of integers

Received February 17, 1966. This paper is part of a doctoral dissertation written at the University of Southern California. The author wishes to thank Professor A. L. Whiteman for his advice and helpful suggestions.