THE NUMBER OF SOLUTIONS OF CERTAIN CUBIC CONGRUENCES

ECKFORD COHEN

1. Introduction. In this paper we shall be concerned with cubic congruences of the form

$$n \equiv a_1x_1^3 + \cdots + a_sx_s^3 \pmod{m}, \tag{1.1}$$

where n is arbitrary, $m > 1$, and the a_i are integers prime to m. The number of sets of solutions $(x_1, \cdots, x_s)$ of (1.1), distinct modulo m, will be denoted by $N_s(n, m)$. Our discussion of $N_s(n, m)$ is limited to the cases $s=2$ and $s=3$; however, we emphasize that the method involved can be extended to arbitrary s.

Suppose that m has the factorization $m = p_1^{\lambda_1}, \cdots, p_l^{\lambda_l}$ as a product of powers of distinct primes $p_1, \cdots, p_l$. Then it follows easily that

$$N_s(n, m) = N_s(n, p_1^{\lambda_1}) \cdots N_s(n, p_l^{\lambda_l}) . \tag{1.2}$$

Thus the determination of $N_s(n, m)$ reduces to the problem of determining $N_s(n, p^\lambda)$ where p is a prime. We accordingly limit ourselves to the case of a prime-power modulus p^λ.

If we denote by t the largest integer $\leq \lambda$ such that $n \equiv 0 \pmod{p^t}$, then one may write

$$n = p^t\xi , \qquad (\xi, p) = 1 , \qquad 0 \leq t \leq \lambda . \tag{1.3}$$

We observe, in case $\lambda > t$, that ξ is uniquely determined $\pmod{p}$. Our main goal will be to obtain exact formulas for the number of solutions $N_2(n, p^\lambda, t) = N_2$ of

$$n \equiv ax^3 + by^3 \qquad \pmod{p^\lambda} , \tag{1.4}$$

and the number of solutions $N_3(n, p^\lambda, t) = N_3$ of

$$n \equiv ax^3 + by^3 + cz^3 \qquad \pmod{p^\lambda} , \tag{1.5}$$

where n is arbitrary of the form (1.3), and the following conditions are satisfied:

$$p \equiv 1 \pmod{3}, \qquad abc \not\equiv 0 \pmod{p} . \tag{1.6}$$

The restriction $p \equiv 1 \pmod 3$ is natural, since other primes are special in the case of cubic congruences.

The method of the paper is based on elementary properties of

Received March 5, 1954. This paper is based on research completed when the author was a member of the Institute for Advanced Study.