CUBIC CONGRUENCES

D. J. Lewis

1. INTRODUCTION

It has been conjectured that there exists a positive integer N such that every homogeneous cubic polynomial equation over an algebraic number field in at least N variables has a nontrivial solution in that field. It is known [2] that if such an N exists, then $N \geq 10$. In an attempt to determine an upper bound on N we were led to the problem of determining the smallest integer M such that if $\mathfrak{m}$ is an ideal in a ring Δ of algebraic integers, then every congruence of the form

$$\sum_{i=1}^{n} \alpha_i x_i^3 \equiv 0 \pmod{\mathfrak{m}} \qquad (\alpha_i \text{ in } \Delta,\ n \geq M)$$

has a solution in Δ which is nontrivial, modulo each prime factor of $\mathfrak{m}$. The results of [2] can be used to show that M need not exceed ten. It is our purpose here to show that $M = 7$ will suffice, and that no smaller value will do. In showing this fact, we consider diagonalized cubic forms over finite fields and over $\mathfrak{p}$-adic fields.

2. DIAGONALIZED CUBICS OVER FINITE FIELDS

THEOREM 1. *If* k *is a finite field and* a, b *and* c *are in* k, *then the equation*

$$ax^3 + by^3 + cz^3 = 0 \tag{1}$$

has a nontrivial solution in k.

Assume that k has characteristic p; then k has $q = p^f$ elements. Let k^* be the group of nonzero elements of k, and let k^3 be the group of cubes of k^*. If a is in k^3, so are (a^{-1}) and $(-a)$. If $q \not\equiv 1 \pmod 3$, there exist integers s and t such that $1 = (q - 1)s + 3t$, hence $a = (a^t)^3$, and we have $k^* = k^3$. If $q \equiv 1 \pmod 3$, then $k^3 \neq k^*$. In fact, k^3 contains exactly $(q - 1)/3$ elements, and if δ is not in k^3, then $k^* = k^3 \cup \delta k^3 \cup \delta^2 k^3$.

We may assume that $abc \neq 0$; otherwise the result is trivially true. If ab^{-1} is in k^3, say $e^3 = ab^{-1}$, then $(1, -e, 0)$ is a solution of (1). We obtain similar solutions if ac^{-1} or bc^{-1} are in k^3. Thus we are left with the case where a, b and c lie in different cosets of k, modulo k^3, a situation which can only occur if $q \equiv 1 \pmod 3$. The following lemma completes the proof of Theorem 1.

LEMMA 1. *If* $q \equiv 1 \pmod 3$ *and* k *is a field of* q *elements, then there exists a nonzero element* δ *of* k *which is not in* k^3 *and such that the equation*

$$1 + \delta = \delta^2 z^3$$

has a solution in k.

Received January 5, 1956.