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.

Let W be the set of all nonzero elements of k^* of the form $\rho^3 - 1$. Then W contains exactly $(q - 4)/3$ distinct elements. Let W^{-1} be the set of multiplicative inverses of the elements of W, and let $V = k^3 \cup W \cup W^{-1}$. Then V contains at most $q - 3$ elements. Let δ be any nonzero element of k not in V. Clearly, δ and $1 + \delta$ are not in k^3. Furthermore, δ^{-1} is not in V, hence $1 + \delta^{-1}$ is not in k^3, and consequently $1 + \delta$ is not in δk^3. Since -1 is in k^3, $1 + \delta \neq 0$, and it follows that $1 + \delta$ is in $\delta^2 k^3$.

For many diagonalized forms of degree $d \neq 3$ over finite fields, $d + 1$ variables are necessary to guarantee that the form will have a nontrivial zero in the field of coefficients of the form. This is easily seen by observing that if p is a prime, the congruence $\Sigma_{i=i}^{p-1} x_i^{p-1} \equiv 0 \pmod p$ has only the trivial solution, modulo p. Also, since our proof relied heavily on the fact that the quotient group k^*/k^3 is of order three, one would not expect this proof to generalize to higher degrees. It should also be noted, in passing, that there exist homogeneous cubic polynomials over k in three variables, that have only the trivial zero in k; example: the norm form of $GF(q^3)$ to $GF(q)$.

3. DIAGONALIZED CUBICS OVER $\mathfrak{p}$-ADIC FIELDS, WHERE THE RESIDUE CLASS FIELD HAS CHARACTERISTIC 3

Let K be a complete field under a discrete nontrivial valuation whose residue class field k is isomorphic to $GF(3^f)$. If the characteristic of K is not zero, let $T = K$. If the characteristic of K is zero, let T be the inertial field of K relative to the minimal complete subfield of K. Then the residue class field of T is isomorphic to k. Let $\mathfrak{O}$ be the ring of integers of K, and $\mathfrak{P}$ the prime ideal in $\mathfrak{O}$. Then $\mathfrak{o} = T \cap \mathfrak{O}$ is the ring of integers of T, and $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$ is the prime ideal in $\mathfrak{o}$. Let R be a complete residue system of $\mathfrak{o}$, modulo $\mathfrak{p}$, containing 0, 1, -1. R will also serve as a complete residue system of $\mathfrak{O}$, modulo $\mathfrak{P}$. Let Π be a fixed prime of $\mathfrak{P}$, π a fixed prime of $\mathfrak{p}$. Then $\pi \equiv \varepsilon \Pi^e \pmod{\mathfrak{P}^{e+1}}$, where ε is in R and e is the ramification degree of K over T. Also, $3 \equiv u\Pi^e \pmod{\mathfrak{P}^{e+1}}$, where u is in R. If the characteristic of K is not zero, then R is a field, and $3 = u = 0$.

If a and α are elements of $\mathfrak{o}$ and $\mathfrak{O}$, respectively, there exist unique elements a_j and b_j in R such that

$$a = \sum_{j=0}^{\infty} a_j \pi^j \quad \text{and} \quad \alpha = \sum_{j=0}^{\infty} b_j \Pi^j .$$

The characteristic of the residue class field is 3, hence for each a in R there exists a unique $\tilde{a}$ in R such that $\tilde{a}^3 \equiv a \pmod{\mathfrak{p}}$. Hence, if b_k is the first nonzero element in the expression for α, then

$$\alpha = \tilde{b}_k{}^3 \Pi^k (1 + \sum_{j=0}^{\infty} c_j \Pi^j),$$

where $\tilde{b}_k$ and the c_j are in R and $\tilde{b}_k{}^3 \equiv b_k \pmod{\mathfrak{p}}$. Thus in determining the existence of a zero, in K, of

$$F(X) = \sum_{i=1}^{n} \alpha_i x_i^3 \qquad (\alpha_i \text{ in } K),$$

we may, without loss of generality, assume that $\alpha_1 = 1$ and that for $i > 1$,

$$\alpha_i = \Pi^{\nu_i}(1 + \sum_{i=0}^{\infty} a_{ij}\Pi^j),$$

where $0 \leq \nu_i \leq 2$, and where the a_{ij} are in R. If m(k) is the number of α_i for which $\nu_i = k$, we may also assume that $m = m(0) \geq m(k)$, for $k \geq 0$, and that $\alpha_1, \alpha_2, \cdots, \alpha_m$ are units.

Write $x_i = \Sigma_{j=0}^{\infty} x_{ij}\Pi^j$; then $F(X) = \Sigma_{k=0}^{\infty} f_k \Pi^k$, where f_k is a polynomial in the x_{ij} with $j \leq k$, and with coefficients from R. If the x_{ij} are from R, then the f_k are in K and hence F(X) is in K. However, if R is not a field, then the x_{ij} being in R need not imply that the f_k are in R. Hence in this case it would not be possible to show that $F(X) = 0$ by making $f_k \equiv 0 \pmod{\mathfrak{P}}$. If for some x_{ij} from R, $f_k \equiv 0$ $(\text{mod } \mathfrak{P})$, then, since the coefficients of f_k are in R and R is in $\mathfrak{o}$, it would follow that $f_k \equiv 0 \pmod{\mathfrak{p}}$, hence that $f_k \equiv 0 \pmod{\mathfrak{P}^e}$. Of course, if R is a field, then $f_k \equiv 0 \pmod{\mathfrak{P}}$ implies $f_k = 0$.

Define

$$f_s^* = 0 \quad \text{if } s < 0, \qquad f_s^* = f_s + \Pi^{-e} f_{s-e}^* \quad \text{if } s \geq 0.$$

If we can find x_{ij} in R such that, for each s, $f_s^* \equiv 0 \pmod{\mathfrak{p}}$, then $F(X) = 0$. To insure that X is nontrivial, we shall seek such x_{ij} for which at least one of $x_{10}, x_{20}, \cdots, x_{n0}$ is not zero.

We shall make use of the usual dot product of two vectors, as well as of a componentwise product; that is, if $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_n)$, then

$$AB = (a_1b_1, a_2b_2, \cdots, a_nb_n).$$

Define $L_k = (a_{1k}, a_{2k}, \cdots, a_{nk})$, where the a_{ik} come from the expression for α_i. Define $X_s = (x_{1s}, x_{2s}, \cdots, x_{ns})$, where the x_{is} come from the formal expression for x_i. Let

$$g_s = \sum_{j=0}^{[s/3]} L_{s-3j} \cdot X_j^3,$$

where [s/3] is the greatest integer not exceeding s/3. Then

$$f_s^* = g_s \quad \text{if } 0 \leq s < e,$$

$$f_e^* = g_e + \Pi^{-e} f_0 = g_e + h_e,$$

$$f_s^* = g_s + h_s \quad \text{if } s \geq e,$$

where

$$h_s = u \sum_{\substack{i+2j+t=s-e \\ j \neq t}} L_i \cdot X_j^2 X_t + \Pi^{-e} f_{s-e}^*$$

$$= uL_0X_0^2 \cdot X_{s-e} + k_s(X_0, X_1, \cdots, X_{s-e-1}).$$

[Recall that $3 \equiv u\Pi^e \pmod{\mathfrak{P}^{e+1}}$]. If R is a field, and $f_i^* = 0$ for $i = 1, 2, \cdots, s-1$, then $h_s = 0$ for $s \geq e$.

If we determine vectors X_j such that, for all $t \geq 0$, $g_t \equiv h_{t+e} \equiv 0 \pmod{\mathfrak{p}}$, then the associated vector X is clearly a solution of $F(X) = 0$.

If $V = (v_1, v_2, \cdots, v_n)$ is a vector with v_i in $\mathfrak{o}$, we define $\widetilde{V} = (\widetilde{v}_1, \widetilde{v}_2, \cdots, \widetilde{v}_n)$, where $\widetilde{v}_i$ is the unique solution in R of the congruence $z^3 \equiv v_i \pmod{\mathfrak{p}}$. Thus $V \cdot X^3 + a \equiv (\widetilde{V} \cdot X + \widetilde{a})^3 \pmod{\mathfrak{p}}$. Consequently, whenever we encounter a congruence of the type $V \cdot X^3 + a \equiv 0 \pmod{\mathfrak{p}}$, we shall speak of it and treat it as a linear congruence. If V and W are linearly dependent (independent), modulo $\mathfrak{p}$, so are $\widetilde{V}$ and $\widetilde{W}$. This is due to the fact that the map $b \to b^3$ is an automorphism of the residue class field. For the remainder of this section and the next two, whenever we speak of linear dependence (independence), we shall mean linear dependence (independence), modulo $\mathfrak{p}$. Likewise, dimension shall mean dimension modulo $\mathfrak{p}$.

Consider the congruences $g_s \equiv 0 \pmod{\mathfrak{p}}$. Suppose L_0, L_1 and L_2 are not zero. If we have previously determined vectors $X_0, X_1, \cdots, X_{r-1}$, we can view

$$g_{3r} \equiv g_{3r+1} \equiv g_{3r+2} \equiv 0 \pmod{\mathfrak{p}}$$

as linear congruences in $x_{1r}, x_{2r}, \cdots, x_{nr}$. If R is not a field, we also need to solve $h_{r+e} \equiv 0 \pmod{\mathfrak{p}}$. If X_0 is such that $L_0X_0^2 \not\equiv 0 \pmod{\mathfrak{p}}$, then h_{r+e}, for $r \geq 1$, is a linear polynomial in the x_{ir}. If, for all $r \geq 0$, we could determine X_r such that

$$g_{3r} \equiv g_{3r+1} \equiv g_{3r+2} \equiv h_{r+e} \equiv 0 \pmod{\mathfrak{p}},$$

then the associated vector X would be a solution of $F(X) = 0$. We can find such vectors X_r, provided the rank of the matrix of coefficients of these linear equations is the same as the rank of the augmented matrix. In case the rank of the coefficient matrix is less than 4, we must choose the vectors X_i $(0 \leq i < r)$ in such a way that these two matrices have the same rank. To simplify matters, we shall attempt to choose X_0 such that $L_0X_0^2$ is linearly independent of L_0, L_1 and L_2. Also, we shall need $f_0 \equiv 0 \pmod{\mathfrak{p}^2}$, so that $h_e \equiv 0 \pmod{\mathfrak{p}}$. If L_1 or L_2 should be zero, some modification is needed, but the approach remains essentially the same. We proceed with our problem, handling all such modifications at once.

Let E_i denote the vector with 1 in the ith coordinate and 0 elsewhere. Then $L_0 = \Sigma_{i=1}^{m} E_i$ and $L_k \cdot E_1 = 0$, if $k \geq 1$. If there exist integers j such that L_{3j+1} and L_{3j+2} are not both zero, let v denote the smallest such integer. From our assumptions on the α_i it follows that if $m \neq n$, then $v = 0$. Let d_v be the dimension of the space spanned by the vectors L_{3v+1} and L_{3v+2}; then $d_v \geq 1$. If $d_v = 2$, define $\rho_v = \lambda_v = 0$. If $d_v = 1$, choose ρ_v and λ_v from R, not both zero, such that $\rho_v L_{3v+1} + \lambda_v L_{3v+2} \equiv 0 \pmod{\mathfrak{p}}$. Define

$$T_r^{(v)} = \rho_v L_{3r+1} + \lambda_v L_{3r+2}, \quad S_{v+1} = T_{v+1}^{(v)}, \quad S_v = 0.$$

Then, if $r \leq v$, $T_r^{(v)} = 0$.

Let d_{v+1} be the dimension of the space spanned by the vectors L_{3v+1}, L_{3v+2} and S_{v+1}. If $d_{v+1} = 2$, set $\rho_{v+1} = \lambda_{v+1} = 0$. If $d_{v+1} = 1$, choose ρ_{v+1}, λ_{v+1} from R, not both zero, such that

$$\rho_{v+1} L_{3v+1} + \lambda_{v+1} L_{3v+2} + S_{v+1} \equiv 0 \pmod{\mathfrak{p}}.$$

Define

$$T_r^{(v+1)} = \rho_{v+1} L_{3r+1} + \lambda_{v+1} L_{3r+2}, \qquad S_{v+2} = \sum_{i=0}^{1} T_{v+2-i}^{(v+i)}.$$

We continue inductively: when $T_r^{(v+t)}$ and S_{v+t} are defined, let d_{v+t} be the dimension of the space spanned by the vectors $L_{3v+1}, L_{3v+2}, S_{v+1}, S_{v+2}, \cdots, S_{v+t}$. If $d_{v+t} = 2$, choose $\rho_{v+t} = 0 = \lambda_{v+t}$. If $d_{v+t} = 1$, choose $\rho_{v+t}, \lambda_{v+t}$ from R, not both zero, such that

$$\rho_{v+t} L_{3v+1} + \lambda_{v+t} L_{3v+2} + S_{v+t} \equiv 0 \pmod{\mathfrak{p}}$$

Define

$$T_r^{(v+t)} = \rho_{v+t} L_{3r+1} + \lambda_{v+t} L_{3r+2}, \qquad S_{v+t+1} = \sum_{i=0}^{t} T_{v+t+1-i}^{(v+i)}.$$

As a consequence, we have $S_{v+t} = -T_v^{(v+t)}$.

We observe that if $\rho_i = \lambda_i = 0$ and $j > i$, then ρ_j and λ_j are zero. Let w denote the smallest of the integers, if such exist, for which $\rho_{v+w} = \lambda_{v+w} = 0$. Then S_{v+w} is linearly independent of L_{3v+1} and L_{3v+2}.

Finally, we define

$$U_{v+r}^{(s)} = \sum_{i=0}^{s} T_{v+r-i}^{(v+i)} \text{ if } s \geq 0,\ r \geq 0; \qquad U_j^{(-1)} = 0.$$

Then $U_{v+r}^{(r-1)} = S_{v+r}$ and $U_{v+r}^{(s)} = T_{v+r-s}^{(v+s)} + U_{v+r}^{(s-1)}$. It follows that $U_{v+w}^{(w-1)}$ is linearly independent of L_{3v+1} and L_{3v+2}.

4. AN ALGORITHM

Consider the following algorithm, where, if v and (or) w do not exist, in the algorithm any vector [polynomial] involving v and (or) w shall be taken as the 0-vector [polynomial].

ALGORITHM. ($\mathfrak{A}$) *Determine* X_0 *with coordinates in* R *such that one of* I, II, *or* III *is satisfied.*

I (1) $g_0 = 0$, (2) $g_{3v+1} \equiv 0 \pmod{\mathfrak{p}}$, (3) $g_{3v+2} \equiv 0 \pmod{\mathfrak{p}}$,

(4) $U_{v+w}^{(w-1)} \cdot X_0^3 \equiv 0 \pmod{\mathfrak{p}}$,

(5) $L_0 X_0^2$ *is linearly independent, modulo* $\mathfrak{p}$, *of the nonzero vectors in the set* $\{\tilde{L}_0, \tilde{L}_{3v+1}, \tilde{L}_{3v+2}, \tilde{U}_{v+w}^{(w-1)}\}$.

II (1) $L_0 X_0 = 0$, (2) $g_1 = 0$, (3) $g_2 \equiv 0 \pmod{\mathfrak{p}}$,

(4) $U_w^{(w-1)} \cdot X_0^3 \equiv 0 \pmod{\mathfrak{p}}$.

(5) $L_1 X_0^2$ *is linearly independent, modulo* $\mathfrak{p}$, *of the nonzero vectors in the set* $\{\tilde{L}_0, \tilde{L}_1, \tilde{L}_2, \tilde{U}_w^{(w-1)}\}$.

III (1) $L_0X_0 = 0$, (2) $L_1X_0 = 0$, (3) $g_2 = 0$,

(4) $U_w^{(w-1)} \cdot X_0^3 \equiv 0 \pmod{\mathfrak{p}}$,

(5) $L_2X_0^2$ *is linearly independent, modulo* $\mathfrak{p}$, *of the nonzero vectors in the set* $\{\widetilde{L}_0, \widetilde{L}_1, \widetilde{L}_2, \widetilde{U}_w^{(w-1)}\}$.

($\mathfrak{B}$) *If* $r \geq 1$ *and if* $X_0, X_1, \cdots, X_{r-1}$ *have been determined, select* X_r *with coordinates in* R *such that*

(6) $g_{3r} \equiv g_{3(r+v)+1} \equiv g_{3(r+v)+2} \equiv 0 \pmod{\mathfrak{p}}$,

(7) $\sum_{j=0}^{r} U_{v+w+j}^{(w-1)} \cdot X_{r-j} \equiv 0 \pmod{\mathfrak{p}}$,

(8) *If* X_0 *is determined by* I, *then* $h_{r+e} \equiv 0 \pmod{\mathfrak{p}}$,

If X_0 *is determined by* II, *then* $h_{r+e+1} \equiv 0 \pmod{\mathfrak{p}}$,

If X_0 *is determined by* III, *then* $h_{r+e+2} \equiv \pmod{\mathfrak{p}}$.

We observe that if $j < v$, then g_{3j+1} and g_{3j+2} are the zero polynomial. If $g_0 = 0$, then

$$h_e = \Pi^{-e} f_0 = 0.$$

If $L_jX_0 = 0$ and j is either 0 or 1, then $g_j = L_j \cdot X_0^3 = 0$. If $L_0X_0 = 0$ and $g_1 = 0$, then

$$h_{e+1} = \Pi^{-e}\{3L_0X_0^2 \cdot X_1 + f_1\} = 0.$$

If $L_0X_0 = L_1X_0 = 0$ and $g_2 = 0$, then

$$h_{e+2} = \Pi^{-e}\{3L_0X_0^2 + 3L_1X_0^2 \cdot X_1 + f_2\} = 0.$$

Hence, if there exist vectors X_i satisfying the algorithm, then, for these X_i, $h_{s+e} \equiv g_s \equiv 0 \pmod{\mathfrak{p}}$ for $s \geq 0$. Thus the associated vector X would be a solution of $F(X) = 0$.

LEMMA 2. *If* $n \geq 7$, *there exist vectors* $X_i = (x_{1i}, x_{2i}, \cdots, x_{ni})$, *with* x_{ki} *in* R, *which satisfy the algorithm and such that* X_0 *is nontrivial, modulo* $\mathfrak{p}$.

The following is a consequence of Lemma 2.

LEMMA 3. *If* K *is a complete field under a discrete nontrivial valuation and if it has a finite residue class field of characteristic* 3, *then every equation of the form*

$$\alpha_1 x_1^3 + \alpha_2 x_2^3 + \cdots + \alpha_n x_n^3 = 0 \qquad (\alpha_i \text{ in } K,\ n \geq 7)$$

has a nontrivial solution in K.

Proof of Lemma 2. In the next section we shall show that we can select an X_0 satisfying conditions ($\mathfrak{A}$) of the algorithm. We now show that for $r \geq 1$ we can select a vector X_r satisfying ($\mathfrak{B}$), provided the preceding X_i fulfill the conditions specified in the algorithm.

As was previously noted, the congruences in (6) and (7) may be viewed as linear congruences in X_r. Since

$$h_{r+e+j} = u L_j X_0^2 \cdot X_r + \cdots \qquad (j = 0, 1, 2)$$

is also a linear polynomial in X_r, condition ($\mathfrak{B}$) requires X_r to be a simultaneous solution of a system of linear congruences.

The choice of w (or our assumption, if w does not exist) and condition 5) assure us that a simultaneous solution exists provided the system of congruences in 6) has a simultaneous solution. Since L_0 is linearly independent of the L_i $(i \geq 1)$, the system in 6) has a solution provided

$$(2) \qquad \rho_v g_{3(v+r)+1} + \lambda_v g_{3(v+r)+2} \equiv 0 \pmod{\mathfrak{p}}.$$

Trivially, (2) is true if v does not exist or if $\rho_v = 0 = \lambda_v$. We need to consider the other possibilities. Since

$$g_{3v+1} = L_{3v+1} \cdot X_0^3, \quad g_{3v+2} = L_{3v+2} \cdot X_0^3, \quad S_{v+t} = -T_v^{(v+t)} \quad \text{and} \quad S_{v+w} = U_{v+w}^{(w-1)},$$

the conditions ($\mathfrak{A}$) on the choice of X_0 assure us that

$$S_{v+t} \cdot X_0^3 \equiv 0 \pmod{\mathfrak{p}}$$

if $t \leq w$. Observe that

$$\rho_{v+s} g_{3(v+r-s)+1} + \lambda_{v+s} g_{3(v+r-s)+2} = \sum_{i=0}^{r-s} T_{v+i}^{(v+s)} \cdot X_{r-s-i}^3 .$$

If the vectors X_{r-s-i} satisfies 6), the left side of this relation is congruent to zero, modulo $\mathfrak{p}$. If in addition $1 \leq s < w$, we obtain

$$U_{v+s}^{(s-1)} \cdot X_{r-s}^3 \equiv S_{v+s} \cdot X_{r-s}^3 \equiv -T_v^{v+s} \cdot X_{r-s}^3 \equiv \sum_{i=1}^{r-s} T_{v+i}^{(v+s)} \cdot X_{r-s-i}^3 \pmod{\mathfrak{p}}.$$

Consequently, if $X_0, X_1, \cdots, X_{r-1}$ satisfy the algorithm and if $t \leq \min(r, w)$, then

$$\begin{aligned}
\rho_v g_{3(v+r)+1} + \lambda_v g_{3(v+r)+2} &= \sum_{i=0}^{r} T_{v+i}^{(v)} \cdot X_{r-i}^3 = \sum_{i=1}^{r} T_{v+i}^{(v)} \cdot X_{r-i}^3 \\
&= \sum_{i=0}^{r-1} U_{v+1+i}^{(0)} \cdot X_{r-1-i}^3 \\
&\equiv \sum_{i=0}^{r-2} U_{v+2+i}^{(1)} \cdot X_{r-2-i}^3 \pmod{\mathfrak{p}} \\
&\quad \cdots \\
&\equiv \sum_{i=0}^{r-t} U_{v+t+i}^{(t-1)} \cdot X_{r-t-i}^3 \pmod{\mathfrak{p}}.
\end{aligned}$$

Hence, if $r \leq w$, then

$$\rho_v g_{3(v+r)+1} + \lambda_v g_{3(v+r)+2} \equiv U_{v+r}^{(r-1)} \cdot X_0^3 \equiv S_{v+r} \cdot X_0^3 \equiv 0 \pmod{\mathfrak{p}}.$$

If $r > w$, then

$$\rho_v g_{3(v+r)+1} + \lambda_v g_{3(v+r)+2} \equiv \sum_{j=0}^{r-w} U_{v+w+j}^{(w-1)} \cdot X_{r-w-j}^3 \pmod{\mathfrak{p}}.$$

The choice of X_{r-w} (see condition 7)) assures us that the right side of this congruence is congruent to 0, modulo $\mathfrak{p}$.

We see, therefore, that if $X_0, X_1, \cdots, X_{r-1}$ satisfy the algorithm, then an X_r may be determined which also satisfies the algorithm.

To obtain X_r satisfying ($\mathfrak{B}$), we need to solve at most five linearly independent linear congruences. Consequently, at this juncture in the proof, we only need $n \geq 6$.

5. DETERMINATION OF X_0

We shall show that a nontrivial X_0 satisfying ($\mathfrak{A}$) can be found, provided $n \geq 7$. Throughout this section we assume that $n \geq 7$.

If v does not exist, neither does w, and condition ($\mathfrak{A}$ I) is trivially satisfied by taking $X_0 = E_1 - E_2$.

If v exists, set $A = L_0 = \Sigma_{i=1}^m E_i$, where $3 \leq m \leq n$. If $L_{3v+1} \neq 0$, set $B = L_{3v+1}$. If $L_{3v+1} = 0$, set $B = L_{3v+2}$; then $B \neq 0$. Choose a vector C such that i) $C \cdot E_1 = 0$, ii) C is linearly independent of B, iii) C and B span a space which contains L_{3v+1}, L_{3v+2}, and $U_{v+w}^{(w-1)}$.

For $m < n$, we have $v = 0$; hence either $B = L_1$, or $L_1 = 0$ and $B = L_2$. Keeping in mind these various changes of notation, we see readily that condition ($\mathfrak{A}$) of the algorithm is satisfied if we determine a vector X which is nontrivial, modulo $\mathfrak{p}$, and has coordinates in R, and which has either the property that condition I* (see below) is satisfied, or else the property that II* is satisfied and $m < n$.

I* i) $A \cdot X^3 = 0$,

ii) $B \cdot X^3 \equiv 0 \pmod{\mathfrak{p}}$,

iii) $C \cdot X^3 \equiv 0 \pmod{\mathfrak{p}}$,

iv) AX^2 is linearly independent, modulo $\mathfrak{p}$, of $\widetilde{A}$, $\widetilde{B}$ and $\widetilde{C}$.

II* i) $AX = 0$,

ii) $B \cdot X^3 = 0$,

iii) $C \cdot X^3 \equiv 0 \pmod{\mathfrak{p}}$,

iv) BX^2 is linearly independent, modulo $\mathfrak{p}$, of $\widetilde{A}$, $\widetilde{B}$ and $\widetilde{C}$.

For any vector $D = \Sigma_{i=1}^n d_i E_i$, define $D' = \Sigma_{i=1}^m d_i E_i$ and $D'' = D - D'$. For $m < n$, it follows from the assumption on the α_i that if B'' and C'' are linearly dependent, then $B'' = \Sigma_{i=m+1}^n E_i$.

If B'' and C'' are linearly independent, choose $X' = E_1 - E_2$ and X'' such that $\widetilde{B} \cdot X \equiv 0 \equiv \widetilde{C} \cdot X \pmod{\mathfrak{p}}$. Then X satisfies I*. We let $D_{ij} = b_i c_j - c_i b_j$. Whenever B'' and C'' are linearly dependent, we may assume that $D_{2n} \not\equiv 0 \pmod{\mathfrak{p}}$. For the remainder of this section we assume that B'' and C'' are linearly dependent.

If $n - m = 3$, take $X = E_n - E_{n-1}$; then X satisfies II*.

If $n - m = 2$, take $X = x_2(E_2 - E_1) + E_3 - E_4 + x_nE_n$. Since $n \geq 7$, we have $m \geq 5$, and clearly $A \cdot X^3 = 0$. The resulting system of congruences, $\widetilde{B} \cdot X \equiv 0 \equiv \widetilde{C} \cdot X \pmod{\mathfrak{p}}$ has a solution for (x_2, x_n). Suppose that

$$\sigma\widetilde{A} + \beta\widetilde{B} + \gamma\widetilde{C} + \delta AX^2 \equiv 0 \pmod{\mathfrak{p}}.$$

By looking at the first coordinate, we immediately obtain $\sigma + \delta x_2^2 \equiv 0 \pmod{\mathfrak{p}}$. Hence $\beta\widetilde{b}_2 + \gamma\widetilde{c}_2 \equiv 0 \pmod{\mathfrak{p}}$. But $\beta\widetilde{b}_n + \gamma\widetilde{c}_n \equiv 0 \pmod{\mathfrak{p}}$. Since $D_{2n} \not\equiv 0 \pmod{\mathfrak{p}}$, $\widetilde{D}_{2n} \not\equiv \pmod{\mathfrak{p}}$; it follows that $\beta \equiv \gamma \equiv 0 \pmod{\mathfrak{p}}$. Looking at the fifth coordinate, we see that $\sigma + \beta\widetilde{b}_5 + \gamma\widetilde{c}_5 \equiv 0 \pmod{\mathfrak{p}}$ and hence $\sigma \equiv 0 \pmod{\mathfrak{p}}$. Since $AX^2 \not\equiv 0 \pmod{\mathfrak{p}}$, $\delta \equiv 0 \pmod{\mathfrak{p}}$. Thus X satisfies iv) and hence I*.

If $n - m \leq 1$, we have several cases. If $D_{ij} \equiv D_{ik} \pmod{\mathfrak{p}}$ for $3 \leq i < j < k < n$, set $X = x_3(E_3 - E_4) + x_5(E_5 - E_6)$. Since $n \geq 7$, we have $m \geq 6$; hence $A \cdot X^3 = 0$. The system of congruences $\widetilde{B} \cdot X \equiv 0 \equiv \widetilde{C} \cdot X \pmod{\mathfrak{p}}$ has its determinant of coefficients congruent to zero, modulo p, hence there exists a solution which is nontrivial, modulo p. The resulting X clearly satisfies I*.

Suppose there exist integers i, j and k such that $3 \leq i < j < k < n$ and such that $D_{ij} \not\equiv D_{ik} \pmod{\mathfrak{p}}$. For $n - m = 1$, set

$$X = x_i(E_i - E_1) + x_k(E_k - E_j) + E_n;$$

for $n = m$, set

$$X = x_i(E_i - E_1) + x_k(E_k - E_j) + E_n - E_2.$$

In either case, the congruence $\widetilde{B} \cdot X \equiv 0 \equiv \widetilde{C} \cdot X \pmod{\mathfrak{p}}$ has a solution for (x_i, x_k) which is also a solution for the congruence $A \cdot X^3 \equiv 0 \pmod{\mathfrak{p}}$. In either case, suppose that $\sigma\widetilde{A} + \beta\widetilde{B} + \gamma\widetilde{C} + \delta AX^2 \equiv 0 \pmod{\mathfrak{p}}$. By looking at the first coordinate, we see that $\sigma + \delta x_i^2 \equiv 0 \pmod{\mathfrak{p}}$, hence that $\beta\widetilde{b}_i + \gamma\widetilde{c}_i \equiv 0 \pmod{\mathfrak{p}}$. At the jth coordinate we have

$$\sigma + \beta\widetilde{b}_j + \gamma\widetilde{c}_j + \delta x_k^2 \equiv 0 \pmod{\mathfrak{p}},$$

and at the kth coordinate we have

$$\sigma + \beta\widetilde{b}_k + \gamma\widetilde{c}_k + \delta x_k^2 \equiv 0 \pmod{\mathfrak{p}}.$$

Hence $\beta\widetilde{b}_j + \gamma\widetilde{c}_j \equiv \beta\widetilde{b}_k + \gamma\widetilde{c}_k \pmod{\mathfrak{p}}$. Thus

$$\beta\widetilde{b}_j\widetilde{b}_i + \gamma\widetilde{c}_j\widetilde{b}_i \equiv \beta\widetilde{b}_k\widetilde{b}_i + \gamma\widetilde{c}_k\widetilde{c}_i \pmod{\mathfrak{p}},$$

and consequently $\gamma\widetilde{D}_{ij} \equiv \gamma\widetilde{D}_{ik} \pmod{\mathfrak{p}}$. It follows that $\gamma \equiv 0 \pmod{\mathfrak{p}}$. Similarly we obtain $\beta \equiv 0 \pmod{p}$. Since $n \geq 7$, we have $m \geq 6$, and therefore in either case one of the first m coordinates of X is zero, and hence $\widetilde{A}$ and AX^2 are linearly independent, modulo $\mathfrak{p}$. It follows that X satisfies I*. This completes the proof of Lemma 2.

6. DIAGONALIZED CUBICS OVER ARBITRARY $\mathfrak{p}$-ACID FIELDS

THEOREM 2. *If* K *is a complete field under a non-archimedean valuation and has a finite residue class field, then every equation of the form*

$$F(X) = \alpha_1 x_1^3 + \alpha_2 x_2^3 + \cdots + \alpha_n x_n^3 = 0 \qquad (\alpha_i \textit{ in } K,\ n \geq 7)$$

has a nontrivial solution in K.

Let $\mathfrak{O}$ be the ring of integers of K, and $\mathfrak{P}$ the prime ideal in $\mathfrak{O}$. We may assume that the α_i are in $\mathfrak{O}$, and if $n \geq 7$, we may assume that at least three of the α_i are units in $\mathfrak{O}$.

If 3 is in $\mathfrak{P}$, then the characteristic of the residue class field of K is three, and Lemma 3 is applicable.

If 3 is not in $\mathfrak{P}$, then 3 is a unit in $\mathfrak{O}$. Applying Theorem 1, we conclude that there exists a vector $B = (\beta_1, \beta_2, \cdots, \beta_n)$ such that the β_i are in $\mathfrak{O}$, such that at least one of them, say β_k, is a unit in $\mathfrak{O}$, and such that $F(B) \equiv 0 \pmod{\mathfrak{P}}$. Furthermore, $\left.\frac{\partial F}{\partial x_k}\right|_B = 3\beta_k^2$, and $3\beta_k^2$ is a unit in $\mathfrak{O}$. Hence we may refine B to obtain a nontrivial zero in $\mathfrak{O}$ of F(X), (see Lemma I of [2].)

Since the equation $x_1^3 + 2y_1^3 + 7(x_2^3 + 2y_2^3) + 7^2(x_3^3 + 2y_3^3) = 0$ has only the trivial solution in the 7-adic field, we see that the theorem is false if $n < 7$.

7. DIAGONALIZED CUBIC CONGRUENCES OVER ALGEBRAIC NUMBER FIELDS

LEMMA 4. *Let* Γ *be a finite extension of the rational field, let* Δ *be the ring of algebraic integers in* Γ, *and let* $\mathfrak{p}$ *be a prime ideal in* Δ. *If* δ *is a positive rational integer, then every congruence of the form*

$$F(X) = \sum_{i=1}^{n} \alpha_i x_i^3 \equiv 0 \pmod{\mathfrak{p}^\delta} \qquad (n \geq 7,\ \alpha_i \textit{ in } \Delta)$$

has a solution in Δ *which is nontrivial, modulo* $\mathfrak{p}$.

Let K be the completion of Γ under the natural valuation given by $\mathfrak{p}$. Then K satisfies the hypothesis of Theorem 2. Hence, if $n \geq 7$, there exist integers b_i in the ring of integers of K, some of which are units in K, such that $\Sigma_{i=1}^n \alpha_i b_i^3 = 0$ in K. The congruences $\beta_i = b_i \pmod{\mathfrak{p}^\delta}$ have solutions for the β_i in Δ. If b_i is a unit in K, then $\beta_i \not\equiv 0 \pmod{\mathfrak{p}}$. Hence $\Sigma_{i=1}^n \alpha_i \beta_i^3 \equiv 0 \pmod{\mathfrak{p}^\delta}$.

Let $\mathfrak{m}$ be any ideal in Δ; then $\mathfrak{m}$ has a prime factorization, say $\mathfrak{m} = \mathfrak{p}^\delta \mathfrak{q}^\varepsilon \cdots \mathfrak{r}^\rho$, where $\mathfrak{p}, \mathfrak{q}, \cdots, \mathfrak{r}$ are distinct prime ideals in Δ. If $F(X) = \Sigma_{i=1}^n \alpha_i x_i^3$, then for each prime $\mathfrak{p}$ in $\mathfrak{m}$ there exists a vector $B_\mathfrak{p} = (b_{1\mathfrak{p}}, b_{2\mathfrak{p}}, \cdots, b_{n\mathfrak{p}})$ such that the $b_{i\mathfrak{p}}$ are in Δ, not all are in $\mathfrak{p}$, and $F(B_\mathfrak{p}) \equiv 0 \pmod{\mathfrak{p}^\delta}$.

By the approximation theorem in [1], there exists, for each i, a common solution in Δ of the system of congruences

$$z_i \equiv b_{i\mathfrak{p}} \pmod{\mathfrak{p}^\delta},$$
$$z_i \equiv b_{i\mathfrak{q}} \pmod{\mathfrak{q}^\varepsilon},$$
$$\cdots$$
$$z_i \equiv b_{i\mathfrak{r}} \pmod{\mathfrak{r}^\rho}.$$

But then $F(Z) \equiv 0 \pmod{\mathfrak{m}}$, and Z is nontrivial, modulo each prime factor in $\mathfrak{m}$.

THEOREM 3. *If* Γ *is a finite extention of the field of rational numbers, and if* $\triangle$ *is the ring of algebraic integers in* Γ, *and* $\mathfrak{m}$ *is an ideal in* $\triangle$, *then every congruence of the form*

$$\alpha_1 x_1^3 + \alpha_2 x_2^3 + \cdots + \alpha_n x_n^3 \equiv 0 \pmod{\mathfrak{m}} \qquad (n > 7,\ \alpha_i \textit{ in } \triangle)$$

has a solution in $\triangle$ *which is nontrivial, modulo each prime factor in* $\mathfrak{m}$.

REFERENCES

1. E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. 51 (1945), 469-492.

2. D. J. Lewis, *Cubic homogeneous polynomials over* $\mathfrak{p}$*-adic number fields*, Ann. of Math. (2) 56 (1952), 473-478.

University of Notre Dame