ACTA ARITHMETICA
XXIII (1973)

Three diagonal quadratic forms

by

F. Ellison (Talence)

1. Introduction. A well known conjecture attributed to E. Artin is as follows:

Let K denote a p-adic number field. If $f_1(X), \ldots, f_r(X)$ are r homogeneous forms of degrees $d_1, \ldots, d_r$ in $n > \sum d_i^2$ variables $X_1, \ldots, X_n$ with coefficients in K, then the system of equations:

$$f_1(X) = \ldots = f_r(X) = 0 \tag{1.1}$$

has a non-trivial solution with $X_1, \ldots, X_n$ all in K.

In 1943 R. Brauer [5], showed the existence of a function $\lambda(d_1, \ldots, d_r)$ such that if $n > \lambda$, then the system (1.1) has a non-trivial solution in K. The most general result on Artin's conjecture is due to Ax and Kochen [1], who used techniques from model theory to prove the following result.

THEOREM. *If $d_1, \ldots, d_r$ are given positive integers then there exists an integer $A(d_1, \ldots, d_r)$ such that every system of equations* (1.1) *with integral coefficients has a non-trivial solution in each Q_p for all $p > A(d_1, \ldots, d_r)$ provided that $n > \sum d_i^2$.*

Unfortunately a major defect in their proof is that the function $A(d_1, \ldots, d_r)$ is non-constructive. This blemish was removed, in principle at any rate, by P. J. Cohen [7], who gave a "constructive" proof of the above theorem. However it does not seem to be possible to actually compute, say $A(4)$ by Cohen's method in a reasonably short period of time.

Interest in the Ax–Kochen theorem was increased when counter-examples to Artin's conjecture were found by Terjanian [16] and later by Browkin [6], which imply that $A(d)$ is greater than any given integer for a suitable value of d. Hence it is of some interest to know when the Artin conjecture is true. Prior to the Ax–Kochen theorem there were several special cases known.

There was the old result of Meyer [15], which asserts that a single quadratic form in $n > 4$ variables with integral coefficients has a non-trivial zero in each Q_p. Later, Demyanov [12] proved that a pair of quadratic forms in $n > 8$ variables with coefficients in Q_p has a non-trivial zero in Q_p. Demyanov's proof was later simplified by Birch, Lewis and Murphy [2].

For a system of three quadratic forms in $n > 12$ variables Birch and Lewis [3] essentially showed that if the residue class field of K_p has odd characteristic and is of order greater than 49, then the system of equations has a non-trivial zero in K_p. Their proof was ammended by Schur and the "49" was reduced to "17" in an unpublished University of Michigan Ph. D. dissertation.

For a single cubic form, Demyanov [11] and Lewis [14] independently verified Artin's conjecture. For single forms of degree 5, 7 and 11, Birch and Lewis [4] and Laxton and Lewis [13] verified Artin's conjecture, provided that the residue class field of K_p was sufficiently large.

In recent years much effort has been expended by Davenport and Lewis in studying "additive" or "diagonal" equations of the form $\sum a_i X_i^k = 0$. Their first main result [8] is that Artin's conjecture is true for a single diagonal form of degree k with integral coefficients.

Later Davenport and Lewis [9] proved that Artin's conjecture is true for a pair of diagonal forms of odd degree k and with integral coefficients.

For a pair of diagonal forms of even degree only a weak form of Artin's conjecture could be proved, namely:

If $n \geqslant 7d^3$ then the system has a non-trivial zero in each Q_p.

On extending their work to systems of r diagonal forms each of degree k in n variables with integral coefficients Davenport and Lewis [10] prove that if n is greater than $9r^2k\cdot\log(3rk)$, if k is odd or if n is even, greater than $48r^2k^3\cdot\log(3rk^2)$, then the system has a non-trivial solution in each Q_p. This is, of course, weaker than Artin's conjecture.

In this, paper we study a system of three diagonal quadratic forms in 13 variables with integral coefficients and verify Artin's conjecture for the case p odd.

The author has verified Artin's conjecture for the case $p = 2$ as well, but the proof is prohibitively long for inclusion here.

2. Congruences and p-adic solubility. In this section we collect together several results which will be needed in later sections. We will be concerned with finding non-trivial solutions to the following system of congruences

$$\begin{aligned} a_1X_1^2+a_2X_2^2+\ldots+a_{13}X_{13}^2 &\equiv 0\,(\operatorname{mod} p^\nu),\\ b_1X_1^2+b_2X_2^2+\ldots+b_{13}X_{13}^2 &\equiv 0\,(\operatorname{mod} p^\nu),\\ c_1X_1^2+c_2X_2^2+\ldots+c_{13}X_{13}^2 &\equiv 0\,(\operatorname{mod} p^\nu),\end{aligned} \tag{2.1}$$

where $\nu\in Z^+$ and $a_i, b_i, c_i\in Z$ for $1\leqslant i\leqslant 13$.

DEFINITION. *A solution $X = \xi$ of the congruences (2.1) is of p-rank S if the matrix*

$$\begin{pmatrix} a_1\xi_1 & a_2\xi_2 & \ldots & a_{13}\xi_{13}\\ b_1\xi_1 & b_2\xi_2 & \ldots & b_{13}\xi_{13}\\ c_1\xi_1 & c_2\xi_2 & \ldots & c_{13}\xi_{13}\end{pmatrix}$$

looked at modulo p, has rank S.

If we let M be the matrix consisting of those column vectors (a_j, b_j, c_j) from the coefficient matrix

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{13}\\ b_1 & b_2 & \ldots & b_{13}\\ c_1 & c_2 & \ldots & c_{13}\end{pmatrix}$$

for which $\xi_j \not\equiv 0\,(\operatorname{mod} p)$, then ξ is of p-rank S exactly when rank $(M) = S$.

LEMMA 2.1. *In* (2.1) *set $\nu = 1$ if $p \neq 2$ and $\nu = 3$ if $p = 2$. If the congruences have a solution of p-rank 3 then there is a non-trivial p-adic integer solution to the equations* (1.1).

Proof. Let $X = \xi$ be a p-rank 3 solution to the congruences (2.1). We may take the ξ_i to be integers in the range $0\leqslant \xi_i\leqslant p^\nu-1$ and write the congruences as

$$\begin{aligned} a_1\xi_1^2+a_2\xi_2^2+\ldots+a_{13}\xi_{13}^2 &= p^\nu A,\\ b_1\xi_1^2+b_2\xi_2^2+\ldots+b_{13}\xi_{13}^2 &= p^\nu B,\\ c_1\xi_1^2+c_2\xi_2^2+\ldots+c_{13}\xi_{13}^2 &= p^\nu C,\end{aligned}$$

where A, B, C are integers.

Since the solution has p-rank 3 there is a (3×3) submatrix of the coefficient matrix, consisting of say the first three columns, whose determinant and ξ_1, ξ_2, ξ_3 are p-adic units. We now solve the equations

$$\begin{aligned} a_1Y_1+a_2Y_2+a_3Y_3 &= -A,\\ b_1Y_1+b_2Y_2+b_3Y_3 &= -B,\\ c_1Y_1+c_2Y_2+c_3Y_3 &= -C,\end{aligned}$$

in the ring of p-adic integers.

Setting $\eta = (Y_1, Y_2, Y_3, 0, 0, \ldots, 0)$ we obtain the following equations

$$\begin{aligned} \sum a_i(\xi_i^2+\eta_i p^\nu) &= 0,\\ \sum b_i(\xi_i^2+\eta_i p^\nu) &= 0,\\ \sum c_i(\xi_i^2+\eta_i p^\nu) &= 0,\end{aligned}$$

where the summations are over those i in the interval $1\leqslant i\leqslant 13$.

The following observation gives a non-trivial p-adic solution to the system of equations (1.1).

LEMMA. *If $r, s \in Z_p$ and r is a p-adic unit, then (r^2+sp^ν) is a square in Z_p provided that $\nu \geqslant 1$ if $p \neq 2$ and $\nu \geqslant 3$ if $p = 2$.*

Proof. The ith term in the formal binomial expansion of $(1+p^\nu s/r^2)^{1/2}$ is

$$\frac{1(1-2)\dots(1-2(i-1))s^i p^{\nu i}}{r^{2i}2^i i!}.$$

We see that if p is odd and $\nu \geqslant 1$, or if $p = 2$ and $\nu \geqslant 3$, the ith term tends to zero p-adically as $i \to \infty$ and hence (r^2+sp^ν) is a square in Z_p.

3. A normalization. In this chapter we describe a normalization on the system (1.1) which is used by Davenport and Lewis [8]. For the sake of completeness and convenience for the reader, we include the details of this Davenport and Lewis normalization as applied to our situation.

We begin by defining a_j to be the column vector (a_j, b_j, c_j) where a_j, b_j, c_j are the coefficients in (1.1) and $j = 1, 2, \dots, 13$. We then define

$$\theta(f_1, f_2, f_3) = \left|\prod \det(a_{j_1}, a_{j_2}, a_{j_3})\right|$$

where the product is extended over all subsets of 3 distinct suffixes j_1, j_2, j_3 from $1, 2, \dots, 13$, two subsets being considered the same only if they are identical. The number of these subsets is $13\times 12\times 11 = N$.

LEMMA 3.1. (i) *If*

$$f_i'(X_1, X_2, \dots, X_{13}) = f_i(p^{\nu_1}X_1, p^{\nu_2}X_2, \dots, p^{\nu_{13}}X_{13})$$

for $i = 1, 2, 3$, then

$$\theta(f_1', f_2', f_3') = p^{6N\nu/13}\theta(f_1, f_2, f_3)$$

where $\nu = \nu_1+\nu_2+\dots+\nu_{13}$.

(ii) *If*

$$f''(X_1, X_2, \dots, X_{13}) = d_{i1}f_1+d_{i2}f_2+d_{i3}f_3$$

where $i = 1, 2, 3$ and $\det(d_{ij}) = D \neq 0$, then

$$\theta(f_1'', f_2'', f_3'') = D^N\theta(f_1, f_2, f_3).$$

Proof. (i) We have $a_j' = p^{2\nu_j}a_j$ and so

$$\det(a_{j_1}', a_{j_2}', a_{j_3}') = p^{2\mu}\det(a_{j_1}, a_{j_2}, a_{j_3})$$

where $\mu = \nu_{j_1}+\nu_{j_2}+\nu_{j_3}$.

When we sum μ over all N subsets of 3 distinct suffixes j_1, j_2, j_3 we get $3N\nu/13$, whence the result.

(ii) We have $a_j'' = (d_{ij})a_j$ and so

$$\det(a_{j_1}'', a_{j_2}'', a_{j_3}'') = D\det(a_{j_1}, a_{j_2}, a_{j_3}),$$

whence the result.

We define two sets of forms f_1, f_2, f_3, with rational integral coefficients to be *p-equivalent* if one set can be obtained from the other by a combination of the operations (i) and (ii) of Lemma 3.1. Here ν_1, ν_2, ν_3, are integers (positive, negative, or zero) and the d_{ij} are rational numbers with $D \neq 0$. The operations (i) and (ii) are commutative. If the equations

$$f_1 = 0, \quad f_2 = 0, \quad f_3 = 0$$

have a simultaneous non-trivial solution in the p-adic field, then so do the equations of any p-equivalent system.

We shall suppose initially that

$$\theta(f_1, f_2, f_3) = 0.$$

It is obvious that for any μ there exist forms $f_i^{(\mu)}$ with rational integral coefficients such that $a_j^{(\mu)}-a_j$, $b_j^{(\mu)}-b_j$, $c_j^{(\mu)}-c_j$ are divisible by p^μ and such that $\theta(f_1^{(\mu)}, f_2^{(\mu)}, f_3^{(\mu)}) \neq 0$, for $i = 1, 2, 3$ and $j = 1, \dots, 13$. Suppose that the equations

$$f_i^{(\mu)} = 0 \quad (i = 1, 2, 3)$$

have a non-trivial p-adic integral solution $\boldsymbol{X} = \boldsymbol{X}^{(\mu)}$. Since the equations are homogeneous, we can suppose that one coordinate at least of $\boldsymbol{X}^{(\mu)}$ is not divisible by p. Thus the point $\boldsymbol{X}^{(\mu)}$ lies on the surface of the cube $|X_j|_p \leqslant 1$ in the space of points with p-adic coordinates. Here $|\cdot|_p$ denotes the p-adic valuation. If μ goes to infinity through a suitable sequence, then

$$\lim_{\mu\to\infty}\boldsymbol{X}^{(\mu)} = \boldsymbol{X}$$

exists in the p-adic sense and is not the origin. We have

$$\lim_{\mu\to\infty}f_i(\boldsymbol{X}^{(\mu)}) = f_i(\boldsymbol{X})$$

and

$$|f_i(\boldsymbol{X}^{(\mu)})|_p = |f_i(\boldsymbol{X}^{(\mu)})-f_i^{(\mu)}(\boldsymbol{X}^{(\mu)})|_p \leqslant p^{-\mu}.$$

Thus

$$f_i(\boldsymbol{X}) = 0.$$

It follows that we may, without loss of generality, assume that θ is not zero.

From all systems of forms that are p-equivalent to the given system, subject to the limitation of having integral coefficients, we select one for which the power of p dividing θ is least. This is possible since we are assuming that θ is non-zero. Such a system of forms will be said to be *p-normalized*. The following lemma gives some properties of a system which is p-normalized.

LEMMA 3.2. *Let f_1, f_2, f_3, be a p-normalized system of additive quadratic forms in thirteen variables. Then*

(i) *They can be written (after renumbering the variables) as*

$$f_i = F_i(X_1, \ldots, X_t) + pG_i(X_{t+1}, \ldots, X_{13}) \tag{3.1}$$

for $i = 1, 2, 3$, where $t \geqslant 7$. Each of $X_1, \ldots, X_t$ occurs in one at least of F_1, F_2, F_3 with a coefficient not divisible by p.

(ii) *Each of $X_{t+1}, \ldots, X_{13}$ occurs in at least one of G_1, G_2, G_3 with a coefficient not divisible by p.*

(iii) *For $S \leqslant 3$, if we form S linear combinations of f_1, f_2, f_3 (these combinations being linearly independent modulo p) and denote by t_S the number of variables that occur in one at least of these combinations with a coefficient not divisible by p, then*

$$t_S > 2S \quad (S = 1, 2, 3). \tag{3.2}$$

If q_S is the number of variables that occur in one at least of these combinations with a coefficient not divisible by p^2, then

$$q_S > 4S \quad (S = 1, 2, 3). \tag{3.3}$$

(iv) *If G is the $3 \times (13-t)$ matrix whose i-th row consists of the coefficients of G_i $(i = 1, 2, 3)$, then the largest $3 \times j$ submatrix of G whose rank is r, has at most $j = 2r$ columns, where $r = 1, 2, 3$.*

Proof. Although, for the sake of clarity, we have stated (i) first, it is readily seen to be a special case of (iii).

We obtain (3.1) simply by including in the forms F_i all those variables that occur in one at least of the f_i with a coefficient not divisible by p, and then renumbering these variables as $X_1, \ldots, X_t$.

Consider the forms

$$p^{-1}f_i(pX_1, \ldots, pX_t, X_{t+1}, \ldots, X_{13}) = pF_i(X_1, \ldots, X_t) + G_i(X_{t+1}, \ldots, X_{13}),$$

for $i = 1, 2, 3$. These are derived from the forms $f_i(X_1, \ldots, X_{13})$ by a combination of the two operations of Lemma 3.1. The first operation is used with $\nu = t$ and the second with $D = p^{-3}$. Hence the value of θ for the new forms is obtained from that for the old forms by multiplying by $p^{6Nt/13-3N}$. Since the new forms have integral coefficients, it follows from the minimal choice made in the definition of a p-normalized system that we have $6Nt/13 - 3N \geqslant 0$, whence $t \geqslant 7$. This proves (i).

We observe that (ii) is in fact a special case of (iv) with $r = 0$. We include the proof of (ii) in the proof of (iv).

We next consider (iii). Let $f_1', \ldots, f_S'$ be any S linear combinations of f_1, f_2, f_3. This set can be completed to give a set of 3 linear combinations

which are independent modulo p. Then f_1', f_2', f_3' are derived using the second operation of Lemma 3.1 with D not divisible by p. As above, we have F_i' associated with f_i' and F_i' is in fact derived from F_i. Let t_S be the number of variables occurring in one at least of $F_1', \ldots, F_S'$ with a coefficient not divisible by p, and take these variables to be $X_1, \ldots, X_{t_S}$. The forms

$$p^{-1}f_i'(pX_1, \ldots, pX_{t_S}, X_{t_S+1}, \ldots, X_{13}) \quad (i = 1, \ldots, S),$$
$$f_i'(pX_1, \ldots, pX_{t_S}, X_{t_S+1}, \ldots, X_{13}) \quad (i = S+1, 3)$$

have integral coefficients and are derived from f_1, f_2, f_3 by the operations of Lemma 3.1 with $\nu = t_S$ and $D = p^{-S}D_0$ where p does not divide D_0. We now easily see $t_S > 2S$.

Similarly, if q_S is the number of variables which occur in $f_1', \ldots, f_S'$ with a coefficient not divisible by p^2, then take these variables to be $X_1, \ldots, X_{q_S}$. The forms

$$p^{-2}f_i'(pX_1, \ldots, pX_{q_S}, X_{q_S+1}, \ldots, X_{13}) \quad (i = 1, \ldots, S),$$
$$f_i'(pX_1, \ldots, pX_{q_S}, X_{q_S+1}, \ldots, X_{13}) \quad (i = S+1, 3)$$

have integral coefficients and are derived from f_1, f_2, f_3 by the operations of Lemma 3.1 with $\nu = q_S$ and $D = p^{-2S}D_1$ where p does not divide D_1. It follows that $q_S > 4S$.

Finally we prove (iv). Setting $S = 3 - r$ we see that from f_1, f_2, f_3 we derive a system f_1', f_2', f_3' such that the forms

$$p^{-2}f_i'(pX_1, \ldots, pX_{q_S}, X_{q_S+1}, \ldots, X_{13}) \quad (i = 1, \ldots, S),$$
$$p^{-1}f'(pX_1, \ldots, pX_{q_S}, X_{q_S+1}, \ldots, X_{13}) \quad (i = S+1, 3)$$

are integral. Here $\nu = q_S = 13 - j$ and $D = p^{-2S-(3-S)}D_2$ where p does not divide D_2. From this it follows that $q_S > 2(3+S)$ whence $j < 2r+1$.

In part (iv) of the statement of Lemma 3.2, we defined a matrix G whose rows are made up of the coefficients of the G_i. Similarly, we define a matrix F whose rows are made up of the coefficients of the F_i. In subsequent sections we will frequently use this notation.

Furthermore we will often renumber variables in order to assume that the first three columns of F are independent. We then apply operations of the second type in Lemma 3.1 to achieve a p-equivalent system which has the property that the first three columns of the coefficient matrix are $\varepsilon_1, \varepsilon_2, \varepsilon_3$. The d_{ij} in this case may certainly be assumed to have unit determinant modulo p, so that the p-normalization is not changed.

We shall often have occasion to refer to the number of columns in a given matrix. If M is a matrix, we shall denote the number of columns in M by $J(M)$.

4. The case $p \neq 2$. Throughout this section we will be assuming that p is an odd prime. We will prove the following result.

THEOREM 4.1. *Let p be an odd prime. Then a system of three diagonal quadratic forms with integer coefficients in $n \geqslant 13$ variables always has a non-trivial p-adic zero.*

The following two general lemmas will often be used in proving this theorem.

LEMMA 4.2 (Chevalley's Theorem). *Let $g_1(X_1, X_2, \ldots, X_n)$, $g_2(X_1, X_2, \ldots, X_n), \ldots, g_r(X_1, X_2, \ldots, X_n)$ be homogeneous forms of degree k in $Z[X_1, X_2, \ldots, X_n]$. Then if $n > kr$ the congruences*

$$(4.1)\qquad \begin{aligned} g_1(X_1, X_2, \ldots, X_n) &\equiv 0 \pmod{p},\\ g_2(X_1, X_2, \ldots, X_n) &\equiv 0 \pmod{p},\\ &\ldots\ldots\ldots\ldots\\ g_r(X_1, X_2, \ldots, X_n) &\equiv 0 \pmod{p} \end{aligned}$$

always have a common non-trivial zero (mod$p$).

LEMMA 4.3. *Let $g_1(X_1, X_2, \ldots, X_n), g_2(X_1, X_2, \ldots, X_n), \ldots, g_r(X_1, X_2, \ldots, X_n)$ be as in Lemma 4.2 with $n = kr$. If the congruences* (4.1) *have no common non-trivial solution, then the system*

$$(4.2)\qquad \begin{aligned} g_1(X_1, X_2, \ldots, X_n) &\equiv a_1 \pmod{p},\\ g_2(X_1, X_2, \ldots, X_n) &\equiv a_2 \pmod{p},\\ &\ldots\ldots\ldots\ldots\\ g_r(X_1, X_2, \ldots, X_n) &\equiv a_r \pmod{p}, \end{aligned}$$

where the a_i are any integers, always has a solution.

Proof. The system of congruences

$$(4.3)\qquad \begin{aligned} g_1(\boldsymbol{X}) - a_1 X_{n+1}^k &\equiv 0 \pmod{p},\\ g_2(\boldsymbol{X}) - a_2 X_{n+1}^k &\equiv 0 \pmod{p},\\ &\ldots\ldots\ldots\ldots\\ g_r(\boldsymbol{X}) - a_r X_{n+1}^k &\equiv 0 \pmod{p} \end{aligned}$$

satisfies the conditions of Lemma 4.2 and so has a non-trivial zero, say $\boldsymbol{X} = \xi$. Since $g_1, g_2, \ldots, g_r$ looked at modulo p have only the trivial zero in common, it follows that, unless all the a_i's are zero, $\xi_{n+1} \not\equiv 0 \pmod{p}$ and then $\xi_{n+1}^{-1}\xi$ is a solution of (4.2). If all the a_i's are zero, the lemma is trivially true.

Remark. For convenience, we note here the useful fact that if $ab \not\equiv 0 \pmod{p}$, one may always find a solution to $X^2 + aY^2 \equiv b \pmod{p}$.

LEMMA 4.4. *Suppose that modulo p*

$$f_1(\boldsymbol{X}) = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2,$$
$$f_2(\boldsymbol{X}) = b_1 X_1^2 + b_2 X_2^2 + b_3 X_3^2$$

have a common zero of p-rank 2. Then there is an integer m such that at least one of the pairs $\{f_1(\boldsymbol{X}), f_2(\boldsymbol{X})\}$ or $\{f_2(\boldsymbol{X}), f_1(\boldsymbol{X})\}$ represents every pair (Y, mY) in $Z/p \times Z/p$.

Proof. Applying the matrix transformation

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & \hat{a}_3 \\ 0 & 1 & \hat{b}_3 \end{pmatrix}$$

we may suppose that $f_1(\boldsymbol{X}) = X_1^2 + \hat{a}_3 X_3^2$ and $f_2(\boldsymbol{X}) = X_2^2 + \hat{b}_3 X_3^2$, where $\hat{a}$ and $\hat{b}_3$ are p-adic units. Also, $-\hat{a}_3$ and $-\hat{b}_3$ are squares modulo p and so there is a t_0 such that we have $\hat{a}_3 t_0^2 \equiv \hat{b}_3 \pmod{p}$.

Clearly, everything of the form (X_1^2, X_2^2) can be represented without the use of the third variable. In particular, for each $X_1 \in Z/p$, $X_1^2(1, t_0^2)$ can be represented. Independently of the first two variables, everything of the form

$$(\hat{a}_3 X_3^2, \hat{b}_3 X_3^2) \equiv (\hat{a}_3 X_3^2, \hat{a}_3 t_0^2 X_3^2) \equiv \hat{a}_3 X_3^2 (1, t_0^2) \pmod{p}$$

is represented. Adding a representation of the first form, obtained by using the first two variables, to one of the second, which uses only the third variable, we see that $(X_1^2 + \hat{a}_3 X_3^2)(1, t_0^2)$ is always represented. Since $X_1^2 + \hat{a}_3 X_3^2$ represents every $X \in Z/p$, we have the result with $m = t_0^2$ for forms of the given shape. In the general case, we can not be sure that m is a non-zero square because of the transformation.

LEMMA 4.5. *Let $f_1(\boldsymbol{X}) = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2 + a_4 X_4^2 + a_5 X_5^2$ and $f_2(\boldsymbol{X}) = b_1 X_1^2 + b_2 X_2^2 + b_3 X_3^2 + b_4 X_4^2 + b_5 X_5^2$. If the associated coefficient matrix has two disjoint submatrices of p-rank 2 and if no pair $(a_i, b_i) \equiv (0, 0) \pmod{p}$ then the pair $\{f_1(\boldsymbol{X}), f_2(\boldsymbol{X})\}$ looked at modulo p represents all $(a, b) \in Z/p \times Z/p$.*

Proof. Without essential loss of generality, we may suppose that $(a_1, a_2) \equiv (1, 0) \pmod{p}$ and $(b_1, b_2) \equiv (0, 1) \pmod{p}$ and that the matrix

$$\begin{pmatrix} a_3 & a_4 & a_5 \\ b_3 & b_4 & b_5 \end{pmatrix}$$

has p-rank 2.

Suppose first that the congruences

$$(4.4)\qquad \begin{aligned} a_3 X_3^2 + a_4 X_4^2 + a_5 X_5^2 &\equiv 0 \pmod{p},\\ b_3 X_3^2 + b_4 X_4^2 + b_5 X_5^2 &\equiv 0 \pmod{p} \end{aligned}$$

have a common non-trivial solution of p-rank 2. It follows from Lemma 4.4 that there is an m such that all (Y, mY) are represented by $\{f_1(\boldsymbol{X}), f_2(\boldsymbol{X})\}$, reversing the order and renumbering f_1 and f_2 if necessary. This representation does not use the first two variables.

If $m \not\equiv 0 \pmod p$ we can always solve the system $X_1^2 + Y \equiv a \pmod p$ and $X_2^2 + mY \equiv b \pmod p$ by solving $mX_1^2 - X_2^2 \equiv ma - b \pmod p$ and setting $Y \equiv a - X_1^2 \pmod p$. This gives a representation of (a, b).

If $m \equiv 0 \pmod p$, then we will show that $b_5 \equiv 0 \pmod p$. We may take $a_3 b_3 \not\equiv 0 \pmod p$, then the system with matrix

$$\begin{pmatrix} a_3 & a_4 & a_5 \\ b_3 & b_4 & b_5 \end{pmatrix}$$

represents all pairs $(Y, 0)$ if and only if the system with coefficient matrix

$$\begin{pmatrix} 1 & a_4' & a_5' \\ 1 & b_4' & b_5' \end{pmatrix}$$

where a_i' and b_i' are $a_i a_3^{-1}$ and $b_i b_3^{-1} \pmod p$, represents all $(Y, 0)$.

Recall that in constructing m we implicitly assumed that we applied the inverse to the transformation

$$\begin{pmatrix} 1 & a_4' & a_5' \\ 1 & b_4' & b_5' \end{pmatrix} \to \begin{pmatrix} 1 & 0 & a_5'' \\ 0 & 1 & b_5'' \end{pmatrix} \pmod p.$$

Let t_0 be as in the previous lemma and apply the inverse transformation to see that if the system with coefficient matrix

$$\begin{pmatrix} 1 & 0 & a_5'' \\ 0 & 1 & b_5'' \end{pmatrix}$$

represents all $(Y, t_0^2 Y)$, then the system with matrix

$$\begin{pmatrix} 1 & a_4' & a_5' \\ 1 & b_4' & b_5' \end{pmatrix}$$

represents all pairs $Y(1 + a_4' t_0^2, 1 + b_4' t_0^2)$. Since $m \equiv 0$, we must have $1 + b_4' t_0^2 \equiv 0 \pmod p$. Also, $b_5' \equiv a_5''(t_0^2 b_4' + 1) \equiv 0 \pmod p$, and so $b_5 \equiv 0 \pmod p$. In this case, the lemma is clearly true.

Suppose next that (4.4) has no non-trivial solution. If the pair $(a_3 X_3^2 + a_4 X_4^2 + a_5 X_5^2,\ b_3 X_3^2 + b_4 X_4^2 + b_5 X_5^2)$ represents all pairs of the form $(-w^2, -z^2)$, then we can always solve the system $X_1^2 - w^2 \equiv a$, and $X_2^2 - z^2 \equiv b \pmod p$ and we have the lemma. So suppose this pair does not represent $(-1, -c^2)$. Then the system

$$X^2 + a_3 X_3^2 + a_4 X_4^2 + a_5 X_5^2 \equiv 0 \pmod p,$$
$$c^2 X^2 + b_3 X_3^2 + b_4 X_4^2 + b_5 X_5^2 \equiv 0 \pmod p$$

has no zero and by Lemma 4.3, represents every pair $(a, b) \pmod p$. The lemma follows on taking $X_1 = X$, $X_2 = cX$.

Finally, if (4.4) has only a p-rank 1 zero, then it is equivalent to a system with coefficient matrix

$$\begin{pmatrix} 1 & a_4' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

in which case the lemma holds easily.

Remark. Since we will be dealing with p-normalized systems, the only systems of the type described in Lemma 4.5 which do not have two disjoint rank 2 submatrices are equivalent to a system having matrix

$$\begin{pmatrix} 1 & a_2 & a_3 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

LEMMA 4.6. *Suppose that the system* (1.1) *is p-normalized. Then the system of congruences* (2.1) *with* $\nu = 1$ *has a zero of p-rank greater than* 1.

Proof. By Chevalley's Theorem, there is at least a p-rank 1 zero, say $\boldsymbol{X} = \xi$. If there is a rank 2 or 3 zero we are done, so suppose ξ has rank exactly 1. We will show how to construct a zero of at least rank 2 starting from ξ.

Since there is a rank 1 zero, we will show that the system may be taken to be equivalent, without loss of the normalization, to one of the form

$$f_1 = F_1 + F_1' + pG_1,$$
$$f_2 = pF_2 + F_2' + pG_2,$$
$$f_3 = pF_3 + F_3' + pG_3$$

as follows. Into the F portion we put all columns which are dependent upon those involved in the zero and apply the obvious transformation. By Lemma 3.2, part (iii) with $S = 2$ applied to f_2 and f_3, we see that $J(F') \geq 5$. Also, since the zero is non-trivial, $J(F) \geq 2$, while $F_1(\xi) \equiv 0 \pmod p$.

By Chevalley's Theorem, $F_2'(\boldsymbol{X})$ and $F_3'(\boldsymbol{X})$ have, modulo p, a common non-trivial zero, say $\boldsymbol{X} = \boldsymbol{\eta}$. We can always solve $F_1(\boldsymbol{Y}) \equiv F_1'(\boldsymbol{\eta}) \pmod p$ and this gives at least a rank 2 zero.

Remark. Suppose the system is normalized and there is a rank 2 solution to (21) with $\nu = 1$, but no rank 3 solution. As above, the system of forms is seen to be unimodularly equivalent to a normalized system of the shape

$$
(4.5)\qquad \begin{aligned} f_1 &= F_1+F_1'+pG_1,\\ f_2 &= F_2+F_2'+pG_2,\\ f_3 &= pF_3+F_3'+pG_3, \end{aligned}
$$

where the following conditions are satisfied:

(i) $F_1(Y)$ and $F_2(Y)$ have a common rank 2 zero modulo p.

(ii) By the normalization, f_3 has at least 3 non-zero coefficients, also p does not divide any coefficient of F_3'. Thus $J(F')\geqslant 3$.

(iii) If F_1', F_2', F_3' have a common non-trivial zero modulo p, then addition would give a rank 3 zero. So F_1', F_2', F_3', have no common non-trivial zero modulo p.

In the following, we will always assume that the systems we are handling are normalized, at least initially, and have a p-rank 2 zero.

Lemma 4.7. *If $J(G)=6$, the system has a p-adic zero.*

Proof. By Lemma 3.2, part (iv), we know that the longest p-rank 2 subset of G has length at most 4. Since $J(G)=6$, this gives us at least two units in each row of G. If, in fact, 3 or more units occur in G_3, then multiplying the variables of F' (in (4.5)) by p and multiplying the "new" f_3 by p^{-i} we get the equivalent system

$$
\begin{aligned} f_1' &= F_1+p^2F_1'+pG_1,\\ f_2' &= F_2+p^2F_2'+pG_2,\\ f_3' &= F_3+pF_3'+G_3. \end{aligned}
$$

Since G_3 must represent every element of Z/p non-trivially, this system has a rank 3 zero modulo p and hence a p-adic zero.

If there are only two unit coefficients in each G_i suppose that the common zero of $F_1(X)$ and $F_2(X)$ in (4.5) is $X=\xi$. If $F_3(\xi)\not\equiv 0 \pmod p$ or if G_3 represents 0 non-trivially we may proceed as in the previous paragraph, and get the result. On the other hand, if $F_3(\xi)\equiv 0\pmod p$ but after a transformation as in the above paragraph we still have only a p-rank 2 zero, we continue as follows. Rewrite the F part of (4.5) as $F+F''$ where the new F includes all the columns for which $\xi_i\not\equiv 0\pmod p$ and all those which are dependent on them. The F'' part includes any remaining columns. A p-adic unimodular transformation then gives a system equivalent to (4.5) of the shape

$$
\begin{aligned} \hat f_1 &= F_1+F_1''+p^2F_1'+pG_1,\\ \hat f_2 &= F_2+F_2''+p^2F_2'+pG_2,\\ \hat f_3 &= pF_3+F_3''+pF_3'+G_3. \end{aligned}
$$

Multiply all variables of $F+F''$ and G by p. Then multiplying $\hat f_1, \hat f_2$ by p^{-2} and $\hat f_3$ by p^{-1} gives a system, equivalent to (4.5), of the shape

$$
(4.6)\qquad \begin{aligned} \tilde f_1 &= F_1+F_1''+F_1'+pG_1,\\ \tilde f_2 &= F_2+F_2''+F_2'+pG_2,\\ \tilde f_3 &= p^2F_3+pF_3''+F_3'+pG_3. \end{aligned}
$$

Here F' is as in (4.5) and so $J(F')\geqslant 3$. Now we have that $F_1(\xi)\equiv F_2(\xi)\equiv 0\pmod p$ is a p-rank 2 zero. Next set all variables of G, F'' and F' in (4.6) to pX_i, and multiplying the resulting last form by p^{-2} gives the equivalent system of the shape

$$
\begin{aligned} \ddot f_1 &= F_1+p^2F_1''+p^2F_1'+p^3G_1,\\ \ddot f_2 &= F_2+p^2F_2''+p^2F_2'+p^3G_2,\\ \ddot f_3 &= F_3+pF_3''+F_3'+pG_3. \end{aligned}
$$

As observed above, $J(F')\geqslant 3$ so there is clearly a p-rank 3 zero, and hence a p-adic zero, to this system.

We may now suppose that $J(G)\geqslant 5$ and hence $J(F+F')\geqslant 8$.

Lemma 4.8. *If in* (4.5), $J(F)\geqslant 5$, *then the system has a p-adic zero.*

Proof. If $F_1(X)$ and $F_2(X)$ do not satisfy the conditions of Lemma 4.5, by the remark following that lemma they could not have a p-rank 2 zero in common. Also, since $J(F')\geqslant 3$, we know that $F_3'(X)$ has a non-trivial zero, say $X=\eta \pmod p$. Then solving $\{F_1(X), F_2(X)\}\equiv\{-F_1'(\eta), -F_2'(\eta)\}$ modulo p, and adding, we get a zero with non-zero coordinate in both F' variables and in F variables, and so is of rank at least 2. If indeed this zero is only rank 2, we have (4.5) unimodularly equivalent to a system of the shape

$$
\begin{aligned} f_1 &= F_1+pF_1'+pG_1,\\ f_2 &= F_2+F_2'+pG_2,\\ f_3 &= pF_3+F_3'+pG_3. \end{aligned}
$$

Since the above is unimodularly equivalent to (4.5), it is still normalized and so each form must have at least 3 unit coefficients. Thus F_1 has at least 3 unit coefficients. Since we are assuming only a p-rank 2 zero if any of these unit coefficients were included in the above constructed zero, we would have to have p-rank 3 and so be done. Call these three unit coefficients a_1, a_2, a_3. We may further suppose that b_4 is a unit and we may always solve

$$
a_1X_1^2+a_2X_2^2+a_3X_3^2\equiv 0\pmod p
$$

non-trivially. Call a zero $X = \gamma$. Then either

$$b_1\gamma_1 + b_2\gamma_2 + b_3\gamma_3 \equiv 0 \pmod{p},$$

in which case we clearly get a p-rank 3 zero, or

$$b_1\gamma_1 + b_2\gamma_2 + b_3\gamma_3 \not\equiv 0 \pmod{p},$$

in which case the pair $\{a_1X_1^2 + a_2X_2^2 + a_3X_3^2,\ b_1X_1^2 + b_2X_2^2 + b_3X_3^2\}$ represents $(0, b)$ and hence, multiplying through by Y_1^2, every pair $(0, bY_1^2)$. Since b_4 is a unit, (F_1, F_2) also represents $(0, \hat{b}Y_2^2)$ for some b, without the use of X_1, X_2, X_3. From F' we get all $(0, b'Y_3^2)$ represented for some $b' \not\equiv 0 \pmod{p}$ and $F_3'(X) \equiv 0 \pmod{p}$ for each representation. Solving $bY_1^2 + \hat{b}Y_2^2 + b'Y_3^2 \equiv 0 \pmod{p}$ with $Y_1Y_2Y_3 \not\equiv 0 \pmod{p}$ gives the result.

Again referring to (4.5) we see that we may, by the above two lemmas and the normalization, assume that $J(F') \geqslant 4$. In order to complete the proof of Theorem 4.1, it remains only to consider the situation $J(F') \geqslant 4$.

LEMMA 4.9. *If in* (4.5) $J(F') \geqslant 4$ *there is a p-adic zero for the system.*

Proof. As usual suppose that $X = \xi$ is a common p-rank 2 zero of $F_1(X)$ and $F_2(X)$. Renumbering if necessary, we may suppose that $\xi_1\xi_2 \not\equiv 0 \pmod{p}$. Also, by a unimodular transformation we may assume the first column of F is $\varepsilon_1 \pmod{p}$ and the second is $\varepsilon_2 \pmod{p}$. Then ξ will still be a zero of the transformed system.

If $J(F') \geqslant 5$, Chevalley's Theorem tells us that F_1' and F_3' have a common non-trivial zero modulo p. Then multiplying through by a square we see that F' represents every triple $(0, aZ_3^2, 0) \pmod{p}$ for some a.

Also, because we have a p-rank 2 zero involving ε_2 F represents $(0, -\xi_2^2Z_1^2, 0)$ for every Z_1^2, without the use of X_2. We patch together a rank 3 zero by solving $-\xi_2^2Z_1^2 + Z_2^2 + aZ_3^2 \equiv 0 \pmod{p}$ with the Z_i units, and adding.

Finally take $J(F') = J(F) = 4$. If F' represents $(-X^2, 0, 0)$, or $(0, -Y^2, 0)$, we may proceed as in the above paragrah. If F' represents $(-X^2, -Y^2, 0)$ we would have η, say so that $F_3'(\eta) \equiv 0 \pmod{p}$ and considering $X_1^2 + (-X^2)$ and $X_2^2 + (-Y^2)$ we see there is a p-rank 3 zero. Thus, F' augmented by the first two columns of F does not have a zero, and by Lemma 4.3 must then represent every non-zero triple (d_1, d_2, d_3) modulo p.

Consider next the remaining two columns of F. If these are $a\varepsilon_1$ and $b\varepsilon_2$ in form, a p-rank 3 zero is easily constructed. So assume this is not the case. We may then assume that either $a_3a_4 \not\equiv 0$ or $b_3b_4 \not\equiv 0 \bmod p)$. Assume the latter. Then $b_3X_3^2 + b_4X_4^2$ represents every non-zero element of Z/p, and in particular, it represents $-d_2$ where d_2 is not a square. Say $b_3\delta_3^2 + b_4\delta_4^2 \equiv -d \pmod{p}$ with δ_3 and δ_4 both units. Then set $-d_1 \equiv a_3\delta_3^2 + a_4\delta_4^2$ and $d_3 \equiv 0 \pmod{p}$. Now F' augmented by the first two columns

of F represents (d_1, d_2, d_3). However, since d_2 is not a square, columns of F' must be used in the representation. Also, we observe by the remark following Lemma 4.5, that (a_3, b_3) is independent of (a_4, b_4) so patching together must give a rank 3 zero.

This completes the proof of Theorem 4.1.

Bibliography

[1] J. Ax and S. Kochen, *Diophantine problems over local fields*, Amer. J. Math. 87 (1965), pp. 605–630.
[2] B. J. Birch, D. J. Lewis, and T. G. Murphy, *Simultaneous quadratic forms*, Amer. J. Math. 84 (1962), pp. 110–116.
[3] — and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. 10 (1965), pp. 423–442.
[4] — — *On p-adic forms*, J. Indian Math. Soc. 23 (1959), pp. 11–32.
[5] R. Brauer, *A note on systems algebraic equations*, Bull. Amer. Math. Soc. 51 (1945), pp. 749–755.
[6] J. Browkin, *On forms over p-adic fields*, Bull. Acad. Polon. Sci. Ser. A, 14 (1966), pp. 489–492.
[7] P. J. Cohen, *Decision procedures in real and p-adic fields*, Comm. Pure Appl. Math. 22 (1969), pp. 131–151.
[8] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A, 274 (1963), pp. 443–460.
[9] — — *Two additive equations*, Number Theory, Proc. Sympos. Pure Math. 12, Houston, Tex. (1967), pp. 74–98.
[10] — — *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. Ser. A, 264 (1969), pp. 557–595.
[11] V. B. Demyanov, *On cubic forms in discretely normed fields*, C. R. Doklady 74 (1950), pp. 889–891.
[12] — *Pairs of quadratic forms over a complete field with a finite residue class field*, Izv. Acad. Nauk U.S.S.R. 20 (1956), pp. 307–324.
[13] D. J. Laxton and D. J. Lewis, *Forms of degree 7 and 11 over p-adic fields*, A. M. S. Symposium in Pure Math. 8 (1965), pp. 16–21.
[14] D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields*, Ann. of Math. 56 (1952), pp. 473–478.
[15] A. Meyer, *Über quadratischen Formen*, Vierteljschr. Naturforsch. Ges. Zürich 29 (1884), pp. 209–222.
[16] G. Terjanian, *Une contre exemple du conjecture d'Artin*, C. R. Acad. Sci. (Paris) 269 (1966), pp. 1040–1041.

UNIVERSITÉ DE BORDEAUX
33 – Talence, France

Reçu le 22. 4. 1972 (269)