JOURNAL OF NUMBER THEORY **57**, 231–241 (1996)
ARTICLE NO. 0046

Quintic Forms over p-adic Fields

DAVID B. LEEP

Department of Mathematics, University of Kentucky, Lexington, Kentucky 40506-0027

AND

CHARLES C. YEOMANS

809 Cooper Drive, Lexington, Kentucky 40502

Communicated by P. Roquette

Received June 7, 1993; revised January 4, 1994

We prove that a quintic form in 26 variables defined over a p-adic field K always has a nontrivial zero over K if the residue class field of K has at least 47 elements. This is in agreement with the theorem of Ax–Kochen which states that a homogeneous form of degree d in d^2+1 variables defined over $\mathbf{Q}_p$ has a nontrivial $\mathbf{Q}_p$-rational zero if p is sufficiently large. The Ax–Kochen theorem gives no results on the bound for p. For $d=1, 2, 3$ it has been known for a long time that there is a nontrivial $\mathbf{Q}_p$-rational zero for all values of p. For $d=4$, Terjanian gave an example of a form in 18 variables over $\mathbf{Q}_2$ having no nontrivial $\mathbf{Q}_2$-rational zero. This is the first result which gives an effective bound for the case $d=5$.

1. INTRODUCTION

In the preface to Artin's collected works, the editors discuss several conjectures of Artin including the following: let K be a complete, discretely valued field with finite residue class field k. Then every homogeneous form defined over K of degree d in greater than d^2 variables has a nontrivial zero. When this is true, we say that K has the property $C_2(d)$.

Artin's conjecture is true when K is a power series field, as was shown by Lang in [La]. When K is a p-adic field (i.e. the unequal characteristic case), a counterexample of degree 4 in 18 variables over $\mathbf{Q}_2$ was given by Terjanian in [T]. Since then many other counterexamples, all of even degree, have been found. See [G] and [Lw] for a summary and further references.

It is still of interest to determine by precisely how much Artin's conjecture fails for p-adic fields. Ax and Kochen showed the following in [A-K]:

0022-314X/96 $18.00

(1) For a given integer $d \geqslant 1$, the set of primes for which $\mathbf{Q}_p$ is not $C_2(d)$ is finite.

(2) If $[K : \mathbf{Q}_p] = n$ is finite, there exists a constant $M(d, n)$, depending on d and n, such that K is $C_2(d)$ if $p > M(d, n)$.

It is known that all p-adic fields satisfy the properties $C_2(2)$ (Hasse) and $C_2(3)$ (Dem'anov, for $p \neq 3$, and Lewis). Thus we may take $M(2, n) = M(3, n) = 1$ for all $n \geqslant 1$. We give short proofs of these results in Section 4.

The Ax–Kochen theorem asserts the existence of a constant $M(d, 1)$ for all d. However, an upper bound for $M(d, 1)$ has never been computed for any $d \geqslant 4$. The only lower bound estimates known for $M(d, 1)$, $d \geqslant 4$, come from the known counterexamples to Artin's conjecture and these only occur (so far) for certain even values of d. In particular, Artin's conjecture is still open when d is a prime number. Our main result is the following.

THEOREM. *Let K be any p-adic field with residue class field k of cardinality $q \geqslant 47$. Then K satisfies the property $C_2(5)$.*[1]

The theorem holds for those fields K satisfying $[K : \mathbf{Q}_p] = n = ef$, where $q = p^f$ and $p > 43^{1/f}$. In particular, $M(5, n) \leqslant 43$ for all n.

Here is a rough outline of the proof of the theorem. Let F be a quintic form over K in 26 variables. We may assume that F is reduced, in the sense of [Lx-Lw] (see Section 4). By using an enhancement of a lemma of Laxton–Lewis we may assume that, upon passage to the residue class field k, F^* is a quintic form in at least seven variables defined over k. We can then reduce to the case where F^* can be specialized to a curve with at least three singular rational zeros which is either absolutely irreducible or which is reducible. In the former case we apply a version of the Weil estimate to get a nonsingular zero of F^*, if the residue class field has cardinality at least 47. In the latter case we are able to show that F^* has a nonsingular zero, if the residue class field has at least 7 elements. Once F^* is known to have a nonsingular zero, Hensel's lemma gives a nonsingular zero of F.

We thank A. Prestel for a helpful discussion of the Ax–Kochen theorem.

2. NOTATION AND CONVENTIONS

We now summarize various notation, facts, etc. By a form we mean a homogeneous polynomial. Note that a homogeneous polynomial has only homogeneous factors. The x_i-degree of a polynomial is the degree of the

[1] J.-P. Serre has informed the authors that he can lower the bound of the theorem to $q \geqslant 43$. He improves the result of our Lemma 3.6 by extending the methods of [S1, Section 2] and [S2, Section 3.2].

highest power of the variable x_i occurring in the polynomial. A polynomial over a field k is said to be absolutely irreducible if it is irreducible over the algebraic closure of k.

A point in some affine space is said to be defined over k, or is k-rational, if its coordinates are elements of k; in projective space, a point is said to be defined over k, or is k-rational, if all of the ratios of any set of homogeneous coordinates of the point are in k.

We say that an affine zero of a form is trivial if all of its coordinates are 0; otherwise, we say that the zero is nontrivial. A zero of a polynomial is said to be singular if all of the partial derivatives of the polynomial vanish there. Let f be a polynomial in n variables and let $\tilde{f}$ be the restriction of f to a linear subspace V. If $z \in V$ is a zero of f and a nonsingular zero of $\tilde{f}$, then z is a nonsingular zero of f.

Let f be a homogeneous polynomial in n variables over the finite field $\mathbf{F}_q$. By $Z(f)$ we mean the set of $\mathbf{F}_q$-rational zeros of f. $Z(f)$ may be interpreted as a subset of either $\mathbf{A}^n(\mathbf{F}_q)$ or $\mathbf{P}^n(\mathbf{F}_q)$. We define $N(f)$ to be the number of projective $\mathbf{F}_q$-rational zeros of f. Note that the number of affine zeros of f is equal to $(q-1)\,N(f)+1$. If X is a set, we write $|X|$ for the cardinality of X.

Let $f \in k[x_1, ..., x_n]$ be a polynomial and let $\gamma(f)$ be the number of variables occurring in the monomials in f with nonzero coefficient. Define the order of f to be $\min\{\gamma(f(Ax)) \mid A \in GL_n(k)\}$. This is the number of variables upon which f actually depends. A polynomial for which $\gamma(f) \neq \text{order}(f)$ is said to be degenerate; otherwise it is said to be nondegenerate. By definition every polynomial can be made nondegenerate by a linear change of variables. Many times we will refer to a "polynomial in n variables" in the statement of results; by this we will always mean that the polynomial is nondegenerate. Also we note that any absolutely irreducible homogeneous polynomial of degree greater than 1 has order at least 3.

Let R be a complete discrete valuation ring with quotient field K, local prime π and maximal ideal $M=(\pi)$. Let k denote the residue field R/M. When k is finite, K is said to be a local, or p-adic, field. We denote passage to the residue field by adding a superscript *. A primitive K-vector is one with integral (i.e. in R) coordinates, at least one of which is a unit.

3. Some General Facts

Lemma 3.1 [Wa]. *Let f be a homogeneous form of degree d in n variables over $\mathbf{F}_q$. If $n>d$, then f has at least q^{n-d} affine $\mathbf{F}_q$-rational zeros. The number of projective zeros of f satisfies $N(f) \geqslant (q^{n-d}-1)/(q-1)$. In particular, if $n>d$ then f has a nontrivial $\mathbf{F}_q$-rational zero.*

LEMMA 3.2. *Let Q be a quadratic form and C a cubic form, both defined over $\mathbf{F}_q$. Assume that Q does not divide C. If Q has order 3, C has order at most 3 and $q > 5$, then Q has a nonsingular $\mathbf{F}_q$-rational zero which is not a zero of C.*

Proof. Since Q has order 3, it is absolutely irreducible. Thus Q and C have no common factor. By Bezout's theorem ([Fu, p. 112]), we know that Q and C have at most 6 common projective zeros. It is easy to show that Q has exactly $q+1$ projective $\mathbf{F}_q$-rational zeros, all of which are nonsingular. Thus if $q+1 > 6$, then there is a nonsingular $\mathbf{F}_q$-rational zero of Q which is not a zero of C. ∎

LEMMA 3.3. *Let f be a nondegenerate form of prime degree defined over a perfect field K which has a nontrivial K-rational zero. If f is not absolutely irreducible, then f is reducible over K.*

Proof. Let $d = \deg(f)$. We may assume that $(1, 0, ..., 0)$ is a zero of f. Then, since f is assumed to be nondegenerate, $1 \leqslant \deg_{x_0}(f) \leqslant d-1$.

Let L be a finite Galois extension of K over which f factors into absolutely irreducible elements. Let σ be an element of $\mathrm{Gal}(L \mid K)$. Since $L[x_0, ..., x_n]$ is a UFD, σ induces a permutation on the set of primes dividing f. Let h be a prime properly dividing f such that $h(1, 0, ..., 0) = 0$. We note that $\deg h = \deg \sigma h$, $\deg_{x_i}(h) = \deg_{x_i}(\sigma h)$, for all i, and that $\deg h > \deg_{x_0}(h)$.

Let H equal the product of the K-conjugates of h and let r be the number of K-conjugates of h. Without loss of generality we may assume that $r > 1$. We have $d \geqslant \deg H = r \cdot \deg h$. If $\deg_{x_0}(h) = 0$ then $\deg_{x_0}(H) = 0$; since $\deg_{x_0}(f) \geqslant 1$, H must be a proper factor of f. Now we may assume that both r and $\deg h$ are greater than 1 (since $\deg h > \deg_{x_0}(h)$). Since d is prime and $d \geqslant r \cdot \deg(h)$ we must in fact have $d > r \cdot \deg(h) = \deg H$. Thus H is a proper factor of f defined over K; it's easy to show that the other factor is also defined over K. ∎

When K is not perfect, then Lemma 3.3 is not true. For example, let $K = \mathbf{F}_p(t)$, $L = K(t^{1/p})$ and $f = x_1^p + t x_2^p + (1+t) x_3^p$. Then $f(1, 1, -1) = 0$ and $f = (x_1 + t^{1/p} x_2 + (1+t)^{1/p} x_3)^p$, but f is irreducible over K.

Lemma 3.3 also fails for forms of composite degree. For example, let K be a field and L an extension of degree 2. Let Q be an isotropic quadratic form of order at least 3 which is defined over L but not K. Assume that $(1, 0, ..., 0)$ is a zero of Q. Then the product of the conjugates of Q is an isotropic form of degree 4 which is irreducible over K, but not absolutely irreducible. It has no K-rational nonsingular zeros. However, Lemma 3.3

extends to forms f of composite degree if we assume that f has a nonsingular K-rational zero. To see this, assume f is irreducible and let L be an extension of K of degree greater than 1 over which f splits into conjugate factors. A rational zero of f is a rational zero of some factor and hence of all of them. It then follows from the product rule for derivatives that this zero is singular.

LEMMA 3.4. *Let F be a polynomial over a p-adic field K with K-integral coefficients. Let F^* denote the reduction* mod π *of F. If F^* has a nontrivial nonsingular F^*-rational zero, then F has a nontrivial K-rational zero.*

This is one of the many versions of Hensel's lemma. [G] contains a thorough exposition of Hensel's lemma.

THEOREM 3.5 [L-Y] (See Also [Au, Théorème 3.3 and Section 4]). *Let N be the number of $\mathbf{F}_q$-rational points on an absolutely irreducible projective plane curve C of absolute genus g and degree d, defined over $\mathbf{F}_q$. Then N satisfies*

$$|N-(q+1)| \leqslant 2g\sqrt{q}+\tfrac{1}{2}(d-1)(d-2)-g.$$

Note that if C is nonsingular then $g=\frac{1}{2}(d-1)(d-2)$ and we recover the usual estimate.

LEMMA 3.6. *Let f be an absolutely irreducible homogeneous polynomial of degree 5 in three variables over $\mathbf{F}_q$. Assume that f has at least three singular zeros over the algebraic closure of $\mathbf{F}_q$. If $q \geqslant 47$, then f has a nonsingular $\mathbf{F}_q$-rational zero.*

Proof. Let S be the number of singular zeros defined over the algebraic closure of $\mathbf{F}_q$ on the projective plane curve defined by f. It follows from the genus formula [Fu, p. 201] that $g \leqslant 6-S$. Then $g \leqslant 3$ since $S \geqslant 3$. These inequalities imply

$$\begin{aligned}(2\sqrt{q}-1)\,g+S &\leqslant (2\sqrt{q}-1)\,g+(6-g)=(2\sqrt{q}-2)\,g+6\\ &\leqslant (2\sqrt{q}-2)3+6=6\sqrt{q}<q-5,\end{aligned}$$

for $q \geqslant 47$. Thus,

$$S<q-5-(2\sqrt{q}-1)\,g=q+1-2g\sqrt{q}+g-6 \leqslant N,$$

by Theorem 3.5. Therefore, f has a nonsingular $\mathbf{F}_q$-rational zero. ∎

4. Reduced Forms

Let F be a form of degree d in n variables and let K be a p-adic field with residue class field $\mathbf{F}_q$. Define $I(F)$ to be the resultant of the n partial derivatives of F. We summarize those facts concerning $I(F)$ which are needed here. For more information, the reader is referred to Section 4 of [Lx-Lw] and, for general information on resultants, to [W, Chap. 11].

Lemma 4.1 [Lx-Lw, Lemma 6]. *If F is a form over a p-adic field K such that $I(F)=0$ then there exists a sequence of forms $F_1, F_2, ...,$ defined over K, which converges to F and for which $I(F_j)\neq 0$.*

Corollary 4.2 [Lx-Lw, Cor. to Lemma 6]. *In order to prove that any form of degree d over a p-adic field K in $n>d^2$ variables has a nontrivial zero over K it is sufficient to prove this fact for forms F for which $I(F)\neq 0$.*

The condition $I(F)\neq 0$ says that the form F is nonsingular over the algebraic closure of K, since the resultant of n forms in n variables is 0 if and only if the polynomials have a common nontrivial zero. If F has K-integral coefficients, then $\operatorname{ord}(I(F))\geqslant 0$, where ord is the normalized valuation on K.

If F has K-integral coefficients, we say that F is reduced if

$$I(F)\neq 0$$

and

$$\operatorname{ord}(I(F))\leqslant \operatorname{ord}(I(G))$$

for all G which are equivalent to F (i.e. $G=aF(Tx)$ for $a\in K^\times$, $T\in GL_n(K)$) and have K-integral coefficients. It is obvious that every F with K-integral coefficients and $I(F)\neq 0$ is equivalent to a reduced form.

If F is a reduced form and T is a unimodular matrix (i.e., an integral matrix which remains an invertible matrix upon passage to the residue class field), then $F(Tx)$ is also a reduced form.

Let F be a reduced form over K and F^* its reduction mod π. Let k be the residue class field of K and m be the order of F^*. The next proposition extends Lemma 7 of [Lx-Lw].

Proposition 4.3. *Let F be a reduced form of degree $d\geqslant 2$ in n variables. Let $s\geqslant 0$ be an integer such that F^* vanishes on an affine s-dimensional* *linear plane V. If $s \geqslant 2$, assume that the cardinality of the residue class field is at least d. Then*

$$\text{order } F^* \geqslant \frac{n}{d} + s.$$

Proof. Write $F = F_0 + \pi F_1$, where F_0 has R-unit coefficients ($F \equiv F_0 \bmod \pi$). Let $p_1, ..., p_m$ be the standard basis vectors of $\mathbf{A}^m(k)$. By a unimodular change of variables over R, we may assume that F^* involves only $x_1, ..., x_m$ nontrivially and that F^* vanishes on $x_{s+1} = \cdots = x_m = 0$. It follows from the vanishing of F^* on V that every monomial occurring nontrivially in F^* is divisible by at least one of $x_{s+1}, ..., x_m$. When $s \geqslant 2$, we make use of the well-known fact that if $d \leqslant q$, then the only homogeneous polynomial of degree d over $\mathbf{F}_q$ which vanishes identically is the zero polynomial.

Let T be the K-integral change of variables given by

$$x_i \to x_i, \quad i = 1, ..., s, m+1, ..., n; \qquad x_i \to \pi x_i, \quad i = s+1, ..., m.$$

The form $G = \pi^{-1} F(Tx)$ has K-integral coefficients, so as in Lemma 7 of [Lx-Lw] we have

$$-n + d(m - s) \geqslant 0,$$

$$m \geqslant \frac{n}{d} + s. \quad \blacksquare$$

COROLLARY 4.4. *If $n > d^2$ and the cardinality of the residue class field is at least d when $s \geqslant 2$, then $N(F^*) \geqslant (q^{s+1} - 1)/(q - 1)$.*

Proof. By Proposition 4.3, we have

$$m - d \geqslant \frac{n}{d} + s - d \geqslant \frac{d^2 + 1}{d} + s - d > s.$$

Since $m - d$ is an integer, we have $m - d \geqslant s + 1$. Combining this with Lemma 3.1, we get

$$N(F^*) \geqslant \frac{q^{m-d} - 1}{q - 1} \geqslant \frac{q^{s+1} - 1}{q - 1}. \quad \blacksquare$$

Using the results of this section we can give a quick proof that quadratic forms in at least five variables and cubic forms in at least ten variables over p-adic fields are isotropic, as promised in the introduction.

The argument goes as follows. Let F be a form of degree $d = 2$ or 3 in at least $d^2 + 1$ variables over a p-adic field K, with residue class field of any cardinality. By Corollary 4.2 we may assume that F is reduced. Then by Proposition 4.3 with $s = 0$ we know that F^* has order at least

$d+1$, $d=2, 3$. By Lemma 3.1, F^* has a nontrivial rational zero. If F^* is a quadratic form of order at least 3, then it is easy to show that F^* has a nonsingular zero. If F^* is a cubic form, suppose it has a nontrivial singular zero. After changing variables we may write

$$F^* = x_0 A(x_1, ..., x_n) + B(x_1, ..., x_n),$$

where A is a nonzero quadratic form. Choose $z_1, ..., z_n$ such that $A(z_1, ..., z_n) \neq 0$ and set $z_0 = -B(z_1, ..., z_n)/A(z_1, ..., z_n)$. Then $(z_0, ..., z_n)$ is a nonsingular zero of F^*. Hensel's lemma then gives a nontrivial K-rational zero of F, in both cases.

5. The Proof of the Main Theorem

Lemma 5.1. *Let f be a quintic form in at least two variables over a field k. Assume that f has two singular projective k-rational zeros u and v. Let $\langle u, v\rangle \subset \mathbf{P}^n(k)$ denote the projective line through u and v. Then at least one of the following possibilities occurs*:

(1) *u and v are the only zeros of f in $\langle u, v\rangle$;*

(2) *The restriction of f to $\langle u, v\rangle$ is the zero polynomial;*

(3) *$\langle u, v\rangle$ contains a nonsingular k-rational zero of f.*

Proof. By a k-rational change of variables we may assume $u = (1, 0, ..., 0)$ and $v = (0, 1, 0, ..., 0)$. Then

$$f(x_0, x_1, 0, ..., 0) = ax_0^3x_1^2 + bx_0^2x_1^3 = x_0^2x_1^2(ax_0 + bx_1).$$

If either $a = 0$ or $b = 0$, but not both, we have case 1. If $a = b = 0$, we have case 2. If $ab \neq 0$, then f has a simple linear factor and $(-b, a, 0, ..., 0)$ is a nonsingular zero of f. ∎

Lemma 5.2. *Let f be a quintic form in at least three variables over $\mathbf{F}_q$. Assume that f has three singular $\mathbf{F}_q$-rational zeros v_1, v_2, v_3 which span a projective plane. Assume that $\langle v_i, v_j\rangle \cap Z(f) = \{v_i, v_j\}$, for all i, j.*

If the restriction of f to $\langle v_1, v_2, v_3\rangle$ is not absolutely irreducible and $q > 5$, then f has a nonsingular $\mathbf{F}_q$-rational zero.

Proof. By a change of variables we may assume that the v_i are the first three basis vectors. Define $g(x_1, x_2, x_3) = f(x_1, x_2, x_3, 0, ..., 0)$. Assume that g is not absolutely irreducible. Then by Lemma 3.3, g is reducible over $\mathbf{F}_q$.

Let K denote the algebraic closure of $\mathbf{F}_q$. Let $\langle v_i, v_j\rangle \subset \mathbf{P}^2(K)$ be the line spanned by v_i and v_j. From the proof of Lemma 5.1, one sees that v_i and v_j are the only zeros of f on $\langle v_i, v_j\rangle$ over K. Assume that g has a linear factor L defined over K. $\langle v_i, v_j\rangle \cap Z(L)$ consists of exactly one point, for each i, j. As any point on $Z(L)$ is a zero of g, we conclude that $\langle v_1, v_2\rangle \cap Z(L)$

equals, say, $\{v_1\}$. Then $\langle v_2, v_3\rangle \cap Z(L)$ equals, say, $\{v_2\}$, from which we conclude that $Z(L)=\langle v_1, v_2\rangle$. This contradicts the assumption that $\langle v_1, v_2\rangle$ contains but two zeros of f. Thus g has no linear factor over K.

Since g is reducible and has no linear factor, we conclude that $g=hk$, where $\deg h=2$, h is absolutely irreducible and h does not divide k. By Lemma 3.2, h has a nonsingular $\mathbf{F}_q$-rational zero which is not a zero of k. This gives a nonsingular $\mathbf{F}_q$-rational zero of g and thus a nonsingular $\mathbf{F}_q$-rational zero of f. ▮

LEMMA 5.3. *Let f be a quintic form in n variables over $\mathbf{F}_q$; assume $q\geqslant 4$. Let $m\geqslant 1$ and assume that $Z(f)$ contains an m-dimensional projective plane V and two points u, v not in V. Also assume that for every projective plane $W\subset V$ of codimension* 1, *we have either $\langle W, u\rangle \subset Z(f)$ or $\langle W, v\rangle \subset Z(f)$. If f does not have a nonsingular rational zero, either $\langle V, u\rangle \subset Z(f)$ or $\langle V, v\rangle \subset Z(f)$.*

Proof. Let $[x_0 : \cdots : x_m]$ be homogeneous coordinates for V. Let $W_1, ..., W_{q+1}$ be the collection of codimension 1 projective planes in V defined by the equations

$$ax_{m-1}+bx_m=0, \qquad \text{for} \quad [a:b]\in \mathbf{P}^1(\mathbf{F}_q).$$

Easily we see that $V=\bigcup_{i=1}^{q+1} W_i$ and $\operatorname{codim}(\bigcap_{i=1}^{q+1} W_i)=2$.

Since $q\geqslant 4$, there are at least five W_i. By a pigeonhole argument and appropriate relabeling, we may assume that $\langle W_i, u\rangle \subset Z(f)$, $i=1, 2, 3$.

Next we show that, for distinct i, j $(1\leqslant i, j\leqslant 3)$,

$$(*) \quad \langle W_i, u\rangle \cap \langle W_j, u\rangle = \langle W_i \cap W_j, u\rangle$$

$$(**) \quad \langle W_i, u\rangle \cap \langle W_j, u\rangle = \bigcap_{i=1}^{3} \langle W_i, u\rangle$$

Clearly, the inclusion "$\supseteq$" holds in both statements. Observe that each $\langle W_i, u\rangle$ is an m-dimensional projective plane and $\langle W_i \cap W_j, u\rangle$ is an $(m-1)$-dimensional projective plane. In addition, $\langle W_i, u\rangle \neq \langle W_j, u\rangle$ since $\langle W_i, u\rangle \cap V=W_i$. Now equality in $(*)$ follows easily by counting dimensions.

Since $W_i \cap W_j=\bigcap_{i=1}^{3} W_i$, we see

$$\langle W_i, u\rangle \cap \langle W_j, u\rangle = \langle W_i \cap W_j, u\rangle = \left\langle \bigcap_{i=1}^{3} W_i, u \right\rangle \subseteq \bigcap_{i=1}^{3} \langle W_i, u\rangle,$$

and this proves $(**)$.

Let $x\in \langle V, u\rangle$, $x\notin \bigcup_{i=1}^{3} \langle W_i, u\rangle$. Since $\operatorname{codim}(\bigcap_{i=1}^{3} W_i)=2$, it follows from $(*)$ and $(**)$ that $\bigcap_{i=1}^{3} \langle W_i, u\rangle$ has codimension 2 in $\langle V, u\rangle$. Thus there is a projective line L in $\langle V, u\rangle$ through x which does not intersect $\bigcap_{i=1}^{3}\langle W_i, u\rangle$. Since $x\notin\langle W_i, u\rangle$ and $\langle W_i, u\rangle$ has codimension 1 in $\langle V, u\rangle$, it follows that $L\cap\langle W_i, u\rangle$ consists of exactly one point u_i, for each i. The u_i are distinct, for if $u_i=u_j$, then from (**) we would have $u_i\in L\cap\langle W_i, u\rangle\cap\langle W_j, u\rangle=L\cap(\bigcap_{i=1}^{3}\langle W_i, u\rangle)=\emptyset$, a contradiction.

We have shown that $L\cap Z(f)$ contains at least three points. By Lemma 5.1, we know that either L contains a nonsingular point of f or f vanishes identically on L. If $\langle V, u\rangle$ contains no nonsingular zero of f, then $x\in Z(f)$ for each $x\in\langle V, u\rangle$ and hence $\langle V, u\rangle\subseteq Z(f)$. ∎

PROPOSITION 5.4. *Let F be a reduced quintic form in at least 26 variables over a p-adic field K. Assume that $q>5$. Then either F^* satisfies the hypotheses of Lemma 5.2 or F^* has a nonsingular zero over the residue class field of K.*

Proof. Assume that F^* has no nonsingular zero over the residue class field of K. Let s be the maximum of the affine dimensions of the linear subspaces of $Z(F^*)$. By Lemma 3.1 and Proposition 4.3, $s\geqslant 1$.

If $s=1$, then by Corollary 4.4, F^* has at least $q+1$ projective zeros. They cannot all lie on a projective line since $s=1$. Choose three, v_1, v_2, v_3, which span a projective plane. Since $s=1$, F^* does not vanish identically on any $\langle v_i, v_j\rangle$. By Lemma 5.1, v_1, v_2, v_3 satisfy the hypotheses of Lemma 5.2.

Assume now that $s\geqslant 2$. Let $V\subseteq Z(F^*)$ be a projective plane of maximal dimension $s-1$. It follows from Corollary 4.4 that $Z(F^*)$ contains at least two points not in V. Let $X=Z(F^*)-V$. We will show there exist $w\in V$ and $u, v\in X$ such that $\{u, v, w\}$ satisfies the hypotheses of Lemma 5.2. That is, $Z(F^*)\cap\langle u, v\rangle=\{u, v\}$, and similarly for $\{u, w\}$ and $\{v, w\}$.

Suppose there is no pair $u, v\in X$ such that $Z(F^*)\cap\langle u, v\rangle=\{u, v\}$. Then for all $x, y\in X$ with $x\neq y$, $\langle x, y\rangle\subseteq Z(F^*)$ by Lemma 5.1. Let W be a projective plane in $Z(F^*)$ of maximal dimension, not contained in V. Such a plane exists because $Z(F^*)$ contains $\langle x, y\rangle$, where $x, y\in X$. We will now show that $X\subseteq W$.

Suppose $w\in X$ and $w\notin W$. Then $W\cap V$ has positive codimension in W, since $W\not\subseteq V$. We have $W-(W\cap V)\subseteq X$ since $W\subseteq Z(F^*)$. Thus F^* vanishes on the complement of $\langle W\cap V, w\rangle$ in $\langle W, w\rangle$ because every element of this complement lies on a line joining two points of X, namely, a point of $W-(W\cap V)$ and w. Let H be a plane in $\langle W, w\rangle$ of codimension 1 containing $\langle W\cap V, w\rangle$ and let H be given by the equation $g=0$. Then $gF^*=0$ for every point of $\langle W, w\rangle$. Since $q>5$, we conclude that gF^* is the zero polynomial on $\langle W, w\rangle$. Since g is not the zero polynomial on $\langle W, w\rangle$, it follows F^* is the zero polynomial on $\langle W, w\rangle$. Thus $\langle W, w\rangle\subseteq Z(F^*)$, contradicting the maximality of dim W. Therefore, $X\subseteq W$.

We have $Z(F^*) = V \cup W$ and $\dim W \leqslant \dim V = s-1$. Corollary 4.4 implies

$$N(F^*) = |W \cup V| \leqslant |W| + |V| \leqslant \frac{2(q^s-1)}{q-1} < \frac{(q^{s+1}-1)}{q-1} \leqslant N(F^*),$$

a contradiction. Thus there must exist $u, v \in X$ such that $\langle u, v\rangle \cap Z(F^*) = \{u, v\}$.

Suppose now that for all $x \in V$, either $\langle u, x\rangle \subseteq Z(F^*)$ or $\langle v, x\rangle \subseteq Z(F^*)$. Then we may apply Lemma 5.3 inductively to conclude $\langle V, u\rangle \subseteq Z(F^*)$ or $\langle V, v\rangle \subseteq Z(F^*)$, each of which contradicts the maximality of dim V. Therefore, there exists $w \in V$ such that $\langle u, w\rangle \cap Z(F^*) = \{u, w\}$ and $\langle v, w\rangle \cap Z(F^*) = \{v, w\}$. We are done since $\{u, v, w\}$ satisfies the hypotheses of Lemma 5.2. ∎

Proof of Theorem. Let F be a quintic form over a p-adic field K in at least 26 variables. By Corollary 4.2, we may assume F is reduced. By Proposition 5.4 we know that either F^* has a nonsingular rational zero or it satisfies the hypotheses of Lemma 5.2, in which case we may assume the restriction of F^* is absolutely irreducible. Then we apply Lemma 3.6 to conclude that F^* has a nonsingular rational zero. It then follows from Lemma 3.4 (Hensel's lemma) that F has a nontrivial rational zero.

References

[Ar] E. Artin, "Collected Papers," Springer-Verlag, Berlin/New York, 1986.

[Au] Y. Aubry, Variétés sur un corps fini et codes géométriques algébriques, Dissertation, Université d'Aix-Marseille II. 1993.

[A-K] J. Ax and S. Kochen, Diophantine problems over local fields, I, *Am. J. Math.* **87** (1965), 605–630.

[Fu] William Fulton, "Algebraic Curves," Addison–Wesley, Reading, MA, 1989.

[G] M. J. Greenberg, "Lectures on Forms in Many Variables," Benjamin, New York, 1969.

[La] S. Lang, On quasi-algebraic closure, *Ann. Math.* **55** (1952), 373–390.

[Lx-Lw] R. R. Laxton and D. J. Lewis, Forms of degree 7 and 11 over p-adic fields, *in* "Proceedings of Symposia in Pure Mathematics," Vol. 7, pp. 16–21, Amer. Math. Soc., Providence, RI, 1965.

[L-Y] David B. Leep and Charles C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math.* **63** (1994), 420–426.

[Lw] D. J. Lewis, Diophantine problems: Solved and unsolved, *in* "Number Theory and Applications," pp. 103–121, Kluwer Academic, Dordrecht/Norwell, MA, 1989.

[S1] J.-P. Serre, Nombre de points des courbes algébriques sur $\mathbf{F}_q$, Séminaire de Théorie des Nombres de Bordeaux 1982/83, No. 22. ("Coll. Works," Vol. III, pp. 664–668).

[S2] J.-P. Serre, Résumé des cours de 1983–84, "Coll. Works," Vol. III, pp. 701–705.

[T] G. Terjanian, Un contre-exemple à une conjecture d'Artin, *C. R. Acad. Sci. Paris* **262** (1966), 612.

[W] B. F. van der Waerden, "Modern Algebra II" (3rd ed.), Ungar, New York, 1950.

[Wa] E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Hamburg* **11** (1935), 76–83.