ARTIN'S CONJECTURE FOR FORMS OF DEGREE 7 AND 11

MICHAEL P. KNAPP

1. *Introduction*

A fundamental aspect of the study of Diophantine equations is that of determining when an equation has a local solution. Artin once conjectured (see the preface to [**1**]) that if k is a complete, discretely valued field with finite residue class field, then every homogeneous form of degree d in greater than d^2 variables whose coefficients are integers of k has a nontrivial zero. In this paper, we consider the case of this conjecture in which k is a p-adic field. Although a counterexample due to Terjanian [**16**] proved Artin's conjecture false in this situation, Ax and Kochen [**2**] have shown when $[k:\mathbf{Q}_p] = n$ is finite, that given d, there exists a number $p(d,n)$ such that Artin's conjecture is true provided that p is larger than $p(d,n)$. Unfortunately, the methods of Ax and Kochen do not lead to explicit estimates for $p(d,n)$. Cohen [**5**] found a method which determines the possible cardinalities of the residue class fields of all p-adic fields for which Artin's conjecture is false, and Brown [**3**] has used this to bound $p(d,1)$, but this bound is so large that one feels that it must be possible to do better. Hence, it is still an interesting problem to obtain estimates on the size of $p(d,n)$.

Previous to Ax and Kochen's proof, several results of this kind were already known. Hasse [**9**] showed that $p(2,n) = 1$ for all n, and Demyanov [**6**] (when the characteristic of the residue field is not 3) and Lewis [**13**] proved that $p(3,n) = 1$. That is, Artin's conjecture is true for $d = 2$ and $d = 3$. Furthermore, Birch and Lewis [**4**] and Laxton and Lewis [**11**] showed the existence of $p(5,n)$, $p(7,n)$ and $p(11,n)$, but were unable to estimate their values. More recently, Leep and Yeomans [**12**] obtained the bound $p(5,n) \leqslant 43$.

In this note, we will show how a theorem due to Schmidt can be combined with the method of Laxton and Lewis to obtain upper bounds for $p(7,n)$ and $p(11,n)$. In particular, in Section 3 we prove the following theorem.

THEOREM 1. *Let k be a p-adic field with residue class field of cardinality q. Let d be a positive integer and let m be an integer exceeding d^2. Let F be a homogeneous polynomial of degree d in m variables whose coefficients are integers of k.*

(i) *When $d = 7$, the polynomial F has a nontrivial k-rational zero provided that* $q > 2^7 5^{10} 7^5 17^3$.

(ii) *When $d = 11$, the polynomial F has a nontrivial k-rational solution provided that* $q > 2^7 5^4 11^5 23^3 61^3$.

This provides the bounds $p(7,n) \leqslant 2^7 5^{10} 7^5 17^3$ and $p(11,n) \leqslant 2^7 5^4 11^5 23^3 61^3$. Hence, if k is restricted to the fields $\mathbf{Q}_p$, one needs in principle only to check a finite number of cases to determine whether Artin's conjecture is true when $d = 7$ or 11.

Received 23 October 1998; revised 1 May 2000.

2000 *Mathematics Subject Classification* 11D72, 11G25, 11E76.

Work partially supported through a fellowship from the David and Lucile Packard Foundation.

J. London Math. Soc. (2) 63 (2001) 268–274.

Our method will closely follow the method of Laxton and Lewis [**11**]. We start by showing that it is sufficient to prove the theorem for certain 'reduced' forms, which are explicit in a relatively large number of variables after reducing modulo the maximal ideal of k. Working in the residue class field k^* of k, we are able to estimate the number of singular solutions of F in k^*. Then if the cardinality of the residue class field is large enough, a theorem due to Schmidt may be used to show that F must contain a nonsingular zero in k^*. Finally, Hensel's lemma is used to lift this nonsingular zero to a nontrivial zero of F in k.

The reader may care to compare the upper bounds for $p(7,n)$ and $p(11,n)$ in the above theorem with the bound $p(5,n) \leqslant 43$ given by Leep and Yeomans [**12**]. The major reason for the disparity between these bounds and Leep and Yeomans' bound for $p(5,n)$ is the large value of q needed in order to apply Schmidt's theorem. It is interesting to note that the conclusion of Schmidt's theorem gives a bound on q smaller than the bound needed to apply the theorem. Leep and Yeomans obtain their better result by slicing to an absolutely irreducible curve, and then using a version of the Weil estimate for points on curves over finite fields. Unfortunately, it seems to be difficult to extend their slicing argument to equations of higher degrees.

2. *Preliminaries*

Our notation will be consistent with that of Laxton and Lewis [**11**]. Let k be a p-adic field with maximal ideal $\hat{p}$. The residue class field of k will be denoted k^*, and will have cardinality q and characteristic p. A form will mean a homogeneous polynomial. A point will mean a point in projective space, and dimension will mean projective dimension. If the coefficients of a form $F = F(\underline{x})$ are integers of k, then the image of F under the natural map from $k[\underline{x}]$ to $k^*[\underline{x}]$ will be denoted by F^*. The algebraic closure of the residue class field k^* will be written as $\tilde{k}$. When F is defined over k and has integral coefficients, then $\tilde{V}$ will represent the variety defined by $F^*(\underline{x}) = 0$. A point of $\tilde{V}$ is said to be nonsingular if some partial derivative of F^* does not vanish there. Finally, if Z is a variety or collection of varieties defined over a finite field k^*, then N_z will represent the number of points of Z defined over k^*.

We begin with a brief discussion of reduced forms. Let F be a form of degree d whose coefficients are integers of k. Define $\mathrm{var}(F)$ to be the number of variables explicit in F. We call two forms F and G equivalent if one can be obtained from the other by a nonsingular linear change of variables. Note that if F and G are equivalent, then the change of variables yields a bijection between the zeros of F and the zeros of G, under which nonsingular zeros correspond to nonsingular zeros. Define $\mathrm{ord}(F) = \min \mathrm{var}(G)$, where the minimum is taken over all forms G equivalent to F. A form F is said to be nondegenerate if $\mathrm{ord}(F) = \mathrm{var}(F)$. Clearly, any degenerate form has a nontrivial integral zero. Hence we may always assume that F is nondegenerate.

Now define $I(F)$ to be the resultant of the partial derivatives of F. The following lemma permits us to suppose that $I(F) \neq 0$. This means that the partial derivatives of F have no common zeros, and hence that all of the zeros of F are nonsingular. More information about resultants may be found in [**14**].

LEMMA 1. *In order to prove that any form of degree d in $n > d^2$ variables whose coefficients are integers of k has a nontrivial zero in k, it is sufficient to prove this fact for forms F for which $I(F) \neq 0$.*

This is a corollary to [**11**, Lemma 6].

Next, we call F a reduced form if the power of p dividing $I(F)$ is less than or equal to the power of p dividing $I(G)$ for all forms G equivalent to F. Since any nondegenerate form F with $I(F) \neq 0$ is equivalent to a reduced form, it suffices to prove the theorem for such forms. We now state two lemmas about reduced forms which we will need later.

LEMMA 2. *Suppose that $F(\underline{x})$ is a reduced form of degree d in $n > d^2$ variables. Then $F^*(\underline{x})$ has no linear factor in $\tilde{k}[\underline{x}]$.*

LEMMA 3. *With the same hypotheses on F as in the statement of Lemma 2, if $d =$ 2, 3, 5, 7 or 11 then among the absolutely irreducible factors of F^* is one whose degree is different from all the others. This factor has coefficients in k^* and is a simple factor of F^*.*

These are [**11**, Lemmas 9 and 10]. Note that Lemma 3 is false in general when d is larger than 11.

Our plan is to find a nonsingular zero of the distinguished factor from Lemma 3 which is not a zero of any other factor of F^*, and then 'lift' this zero to a zero of F. In order to accomplish this, we need a lemma that tells us we can 'lift' this zero.

LEMMA 4. *Suppose that $F(\underline{x})$ is a polynomial in n variables whose coefficients are integers of k, and $\underline{a}$ is a nonsingular nontrivial solution in k^* to the equation $F^*(\underline{x}) = 0$. Then there exists $\underline{b} \in k^n$ such that $F(\underline{b}) = 0$, all the coordinates of $\underline{b}$ are integers of k, and each coordinate b_i of $\underline{b}$ maps to a_i under the natural homomorphism from the ring of integers of k to k^*.*

This is one version of Hensel's lemma. A good discussion of Hensel's lemma can be found in [**7**, Chapter 5].

Next, we need information about the number of rational points on varieties. In our next lemma, we use the notation and terminology of [**10**], which makes use of that in [**17**].

LEMMA 5. *Let Z be a positive cycle in $\mathbf{P}^n$ of degree d, dimension r, and rational over the finite field $\mathbf{F}_q$ containing q elements. Then we have $N_Z \leqslant d^2(q+1)^r$. In particular, if $q \geqslant 10$, then we have $N_Z \leqslant 1.1^r d^2 q^r$.*

Proof. This is a trivial elaboration of [**10**, Lemma 1]. Since an algebraic variety is a positive cycle, we can use this lemma to obtain information about the number of rational points on varieties.

The proof proceeds by induction on r. If $r = 0$, then $N_Z \leqslant d$, and so we are done. For $r \geqslant 1$, the cycle Z can be expressed as a sum of at most d prime rational cycles, which have dimension r and degree at most d. Assume now that P is a prime rational cycle. Lang and Weil prove that if $B(n, d, r)$ is a function such that $N_P \leqslant B(n, d, r)$ whenever P is a prime rational cycle, then we can take $B(n, d, r) = (q+1)\, B(n, d, r-1)$. Since we may take $B(n, d, 0) = d$, an easy induction shows that we can take $B(n, d, r) = d(q+1)^r$. Since Z is a sum of at most d prime rational cycles, we therefore have $N_Z \leqslant d^2(q+1)^r$.

The second statement of the lemma follows trivially. □

Our next lemma is the main theorem of [**15**]. This gives us a lower bound on the number of zeros of an absolutely irreducible polynomial over a finite field, assuming that the number of elements in the field is large enough.

LEMMA 6 (Schmidt). *Suppose that $f(X_1, \dots, X_m)$ is an absolutely irreducible polynomial of total degree $d > 0$, with coefficients in the finite field $\mathbf{F}_q$ with q elements. Let A be the number of solutions $(x_1, \dots, x_m)$ with components in $\mathbf{F}_q$ of the equation $f(X_1, \dots, X_m) = 0$. Suppose that $q > 10^4 m^3 d^5 P^3([4 \log d])$, where [ ] is the greatest integer function and $P(1) = 2$, $P(2) = 3, \dots$ is the sequence of primes. Then*

$$A > q^{m-1} - (d-1)(d-2) q^{m-3/2} - 6d^2 q^{m-2}.$$

This lemma gives information about the number of affine zeros of a polynomial. If f happens to be homogeneous, and N is the number of projective zeros of f, then Schmidt's result implies that we have

$$N \geqslant q^{m-2} - (d-1)(d-2) q^{m-5/2} - 6d^2 q^{m-3}.$$

Our final lemma is Bezout's theorem (see for example [**8**, p. 53]). This will allow us to do computations involving the degrees of intersections of varieties.

LEMMA 7. *Let Y be a variety of dimension greater than 1 in $\mathbf{P}^n$, and let H be a hypersurface not containing Y. Suppose that $Z_1, \dots, Z_n$ are the irreducible components of $Y \cap H$, and let $i(Y, H; Z_j)$ be the intersection multiplicity of Y and H along Z_j. Then*

$$\sum_{j=1}^{n} i(Y, H; Z_j) \deg Z_j = (\deg Y)(\deg H).$$

3. *Proof of Theorem* 1

Now we can essentially follow Laxton and Lewis' argument, using these results, to obtain upper bounds for $p(7, n)$ and $p(11, n)$. We suppose that F is a form of degree d in m variables. If $m > d^2 + 1$, we may set $m - d^2 - 1$ of the variables equal to zero to obtain a form G in $d^2 + 1$ variables. Since any nontrivial solution of G gives a nontrivial solution of F, we may assume at the beginning that F is a form in $d^2 + 1$ variables. That is, we may assume that $m = d^2 + 1$. Finally, assume that q is larger than the bounds given in the statement of the theorem, and note that this is large enough to satisfy the hypothesis of Lemma 6.

Suppose that $F^* = H_1 \dots H_n$ is a factorization of F^* over $\tilde{k}$ into absolutely irreducible factors. By Lemma 3, at least one of the H_i is the only factor with its degree, and this factor has coefficients in k^*. Suppose that H_1 is such a factor, and let $g = \deg H_1$. We aim to find a nonsingular zero of H_1 which is not a zero of $H_2 \dots H_n$. Since H_1 is absolutely irreducible, it follows that $U_J = \partial H_1 / \partial x_J$ is not identically zero for some J. Let $\tilde{V}_i$ denote the hypersurface defined by the equation $H_i = 0$, and let $\tilde{U}_j$ be the hypersurface defined by $U_j = 0$. We have $\deg U_J = g - 1$, and $\dim \tilde{U}_J = m - 2$. Now, we cannot have $\dim(\tilde{U}_J \cap \tilde{V}_1) = m - 2$, as this would imply that $\tilde{U}_J$ and $\tilde{V}_1$ share a component, which is impossible since each component of $\tilde{U}_J$ has degree strictly less than $\deg \tilde{V}_1$. Hence, $\dim(\tilde{U}_J \cap \tilde{V}_1) \leqslant m - 3$.

Now, set $\tilde{W} = \tilde{V}_1 \cap \tilde{U}_1 \cap \ldots \cap \tilde{U}_m$. We wish to find an upper bound for $N_{\tilde{W}}$, which is the number of singular rational zeros of H_1. Trivially, we have $N_{\tilde{W}} \leqslant N_{\tilde{U}_J \cap \tilde{V}_1}$. Let $Z_1, \ldots, Z_k$ be the irreducible components of $\tilde{U}_J \cap \tilde{V}_1$. By Lemma 5, and since $\deg Z_i$ is always positive, we have

$$\begin{aligned} N_{\tilde{W}} &\leqslant N_{\tilde{U}_J \cap \tilde{V}_1} \leqslant \sum_{i=1}^{k} N_{Z_i} \\ &\leqslant \sum_{i=1}^{k} 1.1^{\dim Z_i} (\deg Z_i)^2 \, q^{\dim Z_i} \\ &\leqslant (1.1q)^{\max_i \dim Z_i} \sum_{i=1}^{k} (\deg Z_i)^2 \\ &\leqslant (1.1q)^{m-3} \left(\sum_{i=1}^{k} \deg Z_i \right)^2. \end{aligned}$$

Next, noting that $\deg \tilde{V}_1 = g$ and $\deg \tilde{U}_J = g-1$, Bezout's theorem implies that

$$g(g-1) = \sum_{i=1}^{k} i(\tilde{U}_J, \tilde{V}_1; Z_i) \deg Z_i \geqslant \sum_{i=1}^{k} \deg Z_i.$$

Inserting this inequality into the previous inequality, we have

$$N_{\tilde{W}} \leqslant (1.1q)^{m-3} g^2 (g-1)^2.$$

Next, we find an upper bound for the number of zeros of H_1 which are also zeros of $H_2 \ldots H_n$. Since H_1 is a simple factor of F^*, it follows that for each i with $2 \leqslant i \leqslant n$, we have $\dim(\tilde{V}_1 \cap \tilde{V}_i) \leqslant m-3$. By successively using Lemmas 5 and 7, and again the fact that $\deg \tilde{V}_i$ is positive, we obtain

$$\begin{aligned} N_{\tilde{V}_1 \cap (\tilde{V}_2 \cup \ldots \cup \tilde{V}_n)} &\leqslant \sum_{i=2}^{n} N_{\tilde{V}_1 \cap \tilde{V}_i} \\ &\leqslant \sum_{i=2}^{n} (1.1q)^{m-3} (\deg \tilde{V}_1)^2 (\deg \tilde{V}_i)^2 \\ &= (1.1q)^{m-3} g^2 \sum_{i=2}^{n} (\deg \tilde{V}_i)^2 \\ &\leqslant (1.1q)^{m-3} g^2 \left(\sum_{i=2}^{n} \deg \tilde{V}_i \right)^2. \end{aligned}$$

Since it is clear that $\sum_{i=2}^{n} \deg \tilde{V}_i = d-g$, the above inequality becomes

$$N_{\tilde{V}_1 \cap (\tilde{V}_2 \cup \ldots \cup \tilde{V}_n)} \leqslant (1.1q)^{m-3} g^2 (d-g)^2.$$

Therefore, an upper bound on the number of zeros of H_1 which are singular points of F^* is

$$(1.1q)^{m-3} g^2 ((g-1)^2 + (d-g)^2).$$

Now, since we have assumed that q is large enough so that Lemma 6 may be applied, the number N of rational points of $\tilde{V}_1$ satisfies

$$N \geqslant q^{m-2} - (g-1)(g-2) q^{m-5/2} - 6g^2 q^{m-3}.$$

Therefore, to ensure that $\tilde{V}_1$ has a nonsingular rational point, it suffices to have

$$q^{m-2}-(g-1)(g-2)q^{m-5/2}-6g^2q^{m-3} > (1.1q)^{m-3}g^2((g-1)^2+(d-g)^2).$$

That is,

$$q-(g-1)(g-2)q^{1/2}-g^2(6+1.1^{m-3}((g-1)^2+(d-g)^2)) > 0.$$

Considering this as a quadratic equation in $q^{1/2}$, we find that we need to have

$$q^{1/2} > \frac{s+\sqrt{s^2+4g^2(6+1.1^{m-3}((g-1)^2+(d-g)^2))}}{2},$$

where we have set $s = (g-1)(g-2)$.

Now we must find the value of g which gives the largest bound for $q^{1/2}$. A 'brute force' calculation shows that for $d = 7$ and $d = 11$, the bound on $q^{1/2}$ is largest when we have $g = d$. When $d = 7$, we obtain the bound $q \geqslant 168\,178$. However, in order to apply Lemma 6, we need to assume that q is larger than $2^7 5^{10} 7^5 17^3$. Hence, when $d = 7$, the equation $F^*(\underline{x}) = 0$ has a nonsingular solution in k^* provided that $q > 2^7 5^{10} 7^5 17^3$. This situation occurs again when $d = 11$. In this case, our equation gives an upper bound on q of approximately 10^9. In order to apply Lemma 6, however, we need to assume that $q > 2^7 5^4 11^5 23^3 61^3$, which is larger than 10^{19}. Hence, when $d = 11$, the equation $F^*(\underline{x}) = 0$ has a nonsingular solution in k^* provided that q is larger than $2^7 5^4 11^5 23^3 61^3$.

Therefore, whether $d = 7$ or $d = 11$, whenever q is larger than the bound in the statement of the theorem, the equation $F^*(\underline{x}) = 0$ has a nonsingular rational solution in k^*. Then Lemma 4 implies that $F(\underline{x})$ has a nontrivial solution over k. □

Acknowledgements. The author wishes to thank Professor Trevor Wooley for suggesting this problem, and also for his guidance and encouragement.

References

1. E. Artin, *Collected papers* (Addison–Wesley, Reading, MA, 1965).
2. J. Ax and S. Kochen, 'Diophantine problems over local fields I', *Amer. J. Math.* 87 (1965) 605–630.
3. S. S. Brown, 'Bounds on transfer principles for algebraically closed and complete discretely valued fields', *Mem. Amer. Math. Soc.* 15 (1978).
4. B. J. Birch and D. J. Lewis, 'p-adic forms', *J. Indian Math. Soc.* 23 (1959) 11–31.
5. P. J. Cohen, 'Decision procedures for real and p-adic fields', *Comm. Pure Appl. Math.* 22 (1969) 131–151.
6. V. B. Demyanov, 'On cubic forms in discretely normed fields', *Dokl. Akad. Nauk SSSR* 74 (1950) 889–891 (Russian).
7. M. J. Greenberg, *Lectures on forms in many variables* (W. A. Benjamin, New York, 1969).
8. R. Hartshorne, *Algebraic geometry* (Springer, New York, 1977).
9. H. Hasse, 'Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper', *J. Reine Angew. Math.* 153 (1924) 113–130.
10. S. Lang and A. Weil, 'Number of points of varieties in finite fields', *Amer. J. Math.* 76 (1954) 819–827.
11. R. R. Laxton and D. J. Lewis, 'Forms of degree 7 and 11 over p-adic fields', *Proc. Sympos. Pure Math.* 7 (1965) 16–21.
12. D. B. Leep and C. C. Yeomans, 'Quintic forms over p-adic fields', *J. Number Theory* 57 (1996) 231–241.
13. D. J. Lewis, 'Cubic homogeneous polynomials over p-adic fields', *Ann. of Math.* (2) 56 (1952) 473–478.
14. F. S. Macaulay, *The algebraic theory of modular systems* (Cambridge University Press, Cambridge, 1916).
15. W. M. Schmidt, 'A lower bound for the number of solutions of equations over finite fields', *J. Number Theory* 6 (1974) 448–480.

16. G. TERJANIAN, 'Un contre-example à une conjecture d'Artin', *C. R. Acad. Sci. Paris Ser.* AB 262 (1966) A612.
17. A. WEIL, 'Foundations of algebraic geometry', American Mathematical Society Colloquium Publications 29 (1946).

Department of Mathematics
University of Michigan
Ann Arbor
MI 48109-1109
USA