ACTA ARITHMETICA
133.1 (2008)

Artin's conjecture for septic and unidecic forms

by

Trevor D. Wooley (Bristol)

In honorem Wolfgang M. Schmidt annos LXXV nati

1. Introduction. A theorem of Ax and Kochen [3] provides conditional confirmation of Artin's conjecture. Let n, t and $d_1, \ldots, d_t$ be natural numbers. Then Ax and Kochen show that there is a positive integer p_0 with the following property. Let K be a p-adic field with $[K : \mathbb{Q}_p] = n$, and suppose that $f_1, \ldots, f_t \in K[\mathbf{x}]$ are homogeneous with respective degrees $d_1, \ldots, d_t$, and possess $s > d_1^2 + \cdots + d_t^2$ variables. Then whenever $p > p_0$, these polynomials have a common non-trivial K-rational zero. Familiar examples, involving suitable linear combinations of norm forms, demonstrate that no such conclusion is available when the hypothesis on s is relaxed. Investigations have consequently focused on bounding the least permissible value of p_0, an integer that we denote by $M(\mathbf{d}; n)$. Artin's conjecture, formulated around 1936 (see the preface to [2]), implies that for all choices of $\mathbf{d}$ and n, one may take $M(\mathbf{d}; n) = 1$. An example of Terjanian [30] shows that $M(4; 1) \geq 2$, thereby disproving this conjecture, and more recently Chakri and Hanine [11] have established that $M(d; 1) \geq (1 + o(1))\sqrt{d}$ for infinitely many even exponents d (see also [1], [9] and [26] for earlier work). Reasonable upper bounds for $M(\mathbf{d}; n)$ are known only in a handful of cases.

The object of this paper is to obtain improvements in two cases, namely for forms of degree 7 and 11, sufficient to place them in the latter select category. In §3 of this paper we establish the following theorem.

Theorem 1. *Let K be a field extension of $\mathbb{Q}_p$ with residue class field of cardinality q. Put $q_0(7) = 883$ and $q_0(11) = 8053$, and suppose that $f \in K[\mathbf{x}]$ is homogeneous of degree $d = 7$ or 11 in more than d^2 variables. Then f has a non-trivial K-rational zero provided only that $q > q_0(d)$.*

2000 *Mathematics Subject Classification*: 11D72, 11D88, 11E76, 11G25.

Key words and phrases: equations in many variables, p-adic equations, Artin's conjecture.

Research supported in part by NSF grant DMS-0601367.

It follows from Theorem 1 that for every natural number n, one has $M(7;n) \leq 883$ and $M(11;n) \leq 8053$. For comparison, we note that Knapp [20] has obtained bounds slightly sharper than $M(7;n) < 1.04 \cdot 10^{17}$ and $M(11;n) < 3.56 \cdot 10^{19}$. While the conclusions of Ax and Kochen do not yield explicit estimates for $M(\mathbf{d};n)$, by developing an argument stemming from work of Cohen [12], an explicit bound for $M(d;1)$ has been obtained by S. Brown [8]. Writing $a \uparrow b$ for a^b, and $a \uparrow b \uparrow c$ for $a \uparrow (b \uparrow c)$, the estimate of Brown takes the shape $M(d;1) \leq 2 \uparrow 2 \uparrow 2 \uparrow 2 \uparrow 2 \uparrow d \uparrow 11 \uparrow (4d)$. Bounds of more terrestrial magnitude are scarce. Hasse [18] had shown already in 1924 that $M(2;n) = 1$, and a quarter of a century later, Lewis [25] proved that $M(3;n) = 1$ (see also [13] when the underlying residue class field has characteristic different from 3). Shortly afterwards, Dem'yanov [14] established that $M(2,2;n) = 1$ (see also [7]), and then Schuur [29], building on earlier work of Birch and Lewis [6], proved that $M(2,2,2;n) \leq 47$, and described how to obtain $M(2,2,2;n) \leq 9$. The only other distinct case for which a reasonable bound has been obtained is that of a single quintic form. Leep and Yeomans [24] obtained the estimate $M(5;n) \leq 43$, and have noted also that an improvement due to Serre yields $M(5;n) \leq 41$.

Shortly before the advent of the Ax–Kochen theorem, Laxton and Lewis [22] (building on work of Birch and Lewis [4, 5]) presented a method that, in principle, yields an explicitly computable bound for $M(d;n)$ when $d = 5$, 7 and 11. These ideas motivate both the work of Knapp [20] on forms of degree 7 and 11, and the earlier work of Leep and Yeomans [24]. In order to sketch this approach, consider a form $\mathcal{F}$ of degree $d > 1$ in $K[\mathbf{x}]$ having more than d^2 variables. Laxton and Lewis develop a p-normalisation procedure that utilises an invariant associated with the form. By exploiting the compactness of K, they show that a non-trivial K-rational zero of $\mathcal{F}$ exists whenever an associated form F, with coefficients in the residue class field k of K, and having more than d variables, possesses a non-singular k-rational zero. Consider the factorisation of F over the algebraic closure of k. One may ensure that F possesses no linear factor, and so whenever d fails to be represented as the sum of two non-negative composite numbers (whence $d = 2$, 3, 5, 7 or 11), then amongst the factors of F there is an absolutely irreducible one whose degree is unique. This factor G is essentially fixed under conjugation, and hence is a constant multiple of a k-rational polynomial. One now seeks a non-singular k-rational zero of G that is not simultaneously a zero of the quotient polynomial H defined via the relation $F = GH$. Such a zero may be lifted via Hensel's lemma to the non-trivial K-rational zero of $\mathcal{F}$ that we seek.

Laxton and Lewis [22] obtain the non-singular zero of the above polynomial G by means of the Lang–Weil theorem (see [21]). Available versions of the latter theorem remained inexplicit until the work of Schmidt [28], who combined Bertini's first theorem with his version of Stepanov's method. It is this result that Knapp employs in his work on forms of degree 7 and 11. The versions of Bertini's theorem available to Schmidt were relatively crude, and only recently have substantially sharper versions become available (see [19]). Cafure and Matera [10] employed these advances to improve substantially the available estimates of Lang–Weil type, and such already permits improvements to be made in the conclusions of Knapp. We obtain further advantage by exploiting a flexible variant of Bertini's theorem (see Corollary 3.4 of Cafure and Matera [10]) that, rather than ensuring absolute irreducibility, instead provides control of the degrees of the absolutely irreducible factors of the polynomial resulting from a slicing process.

Leep and Yeomans [24] bound $M(5;n)$ following the strategy of Laxton and Lewis [22], at least in the initial phases of their argument. Rather than wrestle with explicit versions of the Lang–Weil theorem, however, Leep and Yeomans exploit problematic singular solutions so as to isolate useful structures that simultaneously ease the construction of a concrete slicing process, and reduce the genus of the resulting curve. Such is possible owing to the relatively low degree of a quintic form, and the rigidity this imposes on the anatomy of the associated polynomial. Such features would appear to be absent from septic and unidecic forms. A direct application of the arguments of this paper, meanwhile, would yield the bound $M(5;n) \leq 137$. We note also that in common with the work of Laxton and Lewis, our methods are inapplicable to any exponents save 2, 3, 5, 7 and 11. In all other circumstances, the reduced k-rational form arising in the above sketch could factor in the shape $F_1^2F_2^3$, for some k-rational polynomials F_1 and F_2, an eventuality that precludes the existence of a non-singular k-rational zero to which to apply Hensel's lemma.

It transpires that the methods employed in our proof of Theorem 1 may be applied to address the solubility of congruences modulo p^2, for prime numbers p, thereby improving a theorem of Chakri and Hanine (see Theorem 3.1 of [11]) that makes explicit an earlier conclusion of Ax and Kochen [3]. In §4 we prove the following theorem.

Theorem 2. *Let p be a prime number, and suppose that the polynomial $f \in \mathbb{Z}_p[x_1,\dots,x_s]$ is homogeneous of degree d. Then the congruence $f(x_1,\dots,x_s) \equiv 0 \pmod{p^2}$ possesses a primitive zero provided only that $s > 2d$ and $p > \frac{1}{2}(3d^4 - 4d^3 + 5d^2)$.*

The above-cited work of Chakri and Hanine provides a conclusion of the same shape as that of Theorem 2, but with the hypothesis on p replaced by the more stringent condition that $p > 250d^5$ and $d(d-1)^2 + (2pd^5)^{1/2} + 2d\phi \leq p$, with $\phi = 2dk^{2^k}$, wherein $k = d(d+1)/2$. For large values of d, the latter requires that p be rather larger than $\exp(\exp(d^2/3))$, whereas Theorem 2 above is applicable whenever $p > 3d^4/2$.

We summarise in §2 the preliminary simplifications inherent in the argument of Laxton and Lewis, and also such details of the slicing argument of Cafure and Matera as are required in our subsequent deliberations. The proof of Theorem 1 is then dispatched in §3, with that of Theorem 2 following in §4 by a similar argument, on incorporating a variant of the argument of Chakri and Hanine.

2. Preliminary manoeuvres. We begin by introducing some notation. Let $\mathfrak{K}$ be a field, and consider a *form* (that is, a homogeneous polynomial) $F \in \mathfrak{K}[\mathbf{x}]$. Write $\mathrm{var}(F)$ for the number of variables explicit in F. Two forms F and G in $\mathfrak{K}[x_1, \ldots, x_n]$ are said to be *equivalent* when there exist $a \in \mathfrak{K}^\times$ and $T \in \mathrm{GL}_n(\mathfrak{K})$ for which $F(\mathbf{x}) = aG(T\mathbf{x})$. When F and G are equivalent forms, there is a bijection between their zeros, and also their non-singular zeros, provided by the latter implicit change of variables. We define $\mathrm{ord}(F)$ to be the minimum value assumed by $\mathrm{var}(G)$ as we consider all forms G equivalent to F. A form F is said to be *non-degenerate* if $\mathrm{ord}(F) = \mathrm{var}(F)$, and otherwise is said to be *degenerate*. Plainly, any degenerate form in $\mathfrak{K}[\mathbf{x}]$ possesses a non-trivial $\mathfrak{K}$-rational zero.

Our initial manoeuvres follow the path laid by Laxton and Lewis [22]. Suppose that K is a field extension of $\mathbb{Q}_p$, let $\mathfrak{o}$ be its ring of integers, and write $\mathfrak{p} = (\pi)$ for the prime ideal of $\mathfrak{o}$. Let q denote the cardinality of the residue class field $k \simeq \mathfrak{o}/\mathfrak{p}$, and write $\overline{k}$ for the algebraic closure of k. We define the valuation $|\cdot|_{\mathfrak{p}}$ for $\alpha \in K^\times$ by putting $|\alpha|_{\mathfrak{p}} = p^{-h}$, where h is the unique rational integer for which $\pi^{-h}\alpha$ is a unit of K. When $F \in \mathfrak{o}[\mathbf{x}]$, the image of F under the natural map from $\mathfrak{o}[\mathbf{x}]$ to $k[\mathbf{x}]$ will be denoted by F^*. Next, given a form F in $K[x_1, \ldots, x_n]$, define $\mathcal{I}(F)$ to be the resultant of the partial derivatives $\partial F/\partial x_i$ $(1 \le i \le n)$. The element $\mathcal{I}(F)$ of K is an invariant amongst the forms equivalent to F under the action of $\mathrm{SL}_n(K)$. We say that a form $F \in \mathfrak{o}[\mathbf{x}]$ is *reduced* when $\mathcal{I}(F) \ne 0$, and if, in addition, whenever $G \in \mathfrak{o}[\mathbf{x}]$ is equivalent to F, one has $|\mathcal{I}(F)|_{\mathfrak{p}} \ge |\mathcal{I}(G)|_{\mathfrak{p}}$. We next recall a consequence of Hensel's lemma. In this context, we say that a zero $\mathbf{y}$ of a form F is *non-singular* when some partial derivative of F is non-zero at $\mathbf{y}$.

Lemma 3. *Suppose that $F \in \mathfrak{o}[\mathbf{x}]$, and that F^* has a non-singular k-rational zero. Then F has a non-singular zero with coefficients in $\mathfrak{o}$.*

Proof. This is a standard application of Hensel's lemma (see, for example, Greenberg [16]).

We restrict attention in §3 to the set $\mathcal{F}_d$ of forms $F \in \mathfrak{o}[\mathbf{x}]$ of degree $d = 7$ or 11, satisfying the property that $\mathrm{ord}(F^*) > d$ and F^* has no $\overline{k}$-rational linear factor. The following lemma summarises the conclusions of Laxton and Lewis relevant to our discussion.

Lemma 4. *Suppose that every form F lying in $\mathcal{F}_d$ possesses a non-singular K-rational zero. Then every form $G \in K[\mathbf{x}]$ of degree d, with* $\mathrm{var}(G) > d^2$, *possesses a non-trivial K-rational zero.*

Proof. Consider a form $G \in K[\mathbf{x}]$ of degree d with $\mathrm{var}(G) > d^2$. We have already noted that the existence of a non-trivial K-rational zero of G is self-evident whenever G is degenerate. We may therefore suppose that G is non-degenerate, and then it follows from the Corollary to Lemma 6 of [22] that in order to establish that G has a non-trivial K-rational zero, it suffices to establish such for non-degenerate forms H with $\mathrm{var}(H) > d^2$ and $\mathcal{I}(H) \neq 0$. Any such form H is equivalent to a reduced form $F \in \mathfrak{o}[\mathbf{x}]$ with $\mathrm{ord}(F) > d^2$. It follows from Lemma 7 of [22] that $\mathrm{ord}(F^*) \geq \mathrm{ord}(F)/d > d$ (see also Lemma 1 of [27]). In addition, Lemma 9 of [22] shows that F^* has no $\overline{k}$-rational linear factor. Thus we find that $F \in \mathcal{F}_d$, so by hypothesis we may assume that F possesses a non-singular K-rational zero. This completes the proof of the lemma.

We approach Theorem 1 via a modified Bertini theorem. We record next both the latter result and such additional estimates as are required in order to dispose of residual cases. The first lemma concerns the properties of certain polynomials following a slicing process. Let L be a field, and consider a polynomial $f \in L[x_0, x_1, \dots, x_n]$. When $\boldsymbol{\xi} = (\xi_0, \xi_1, \dots, \xi_{3n}) \in L^{3n+1}$, we write $f|_{\boldsymbol{\xi}} = f|_{\boldsymbol{\xi}}(X, Y)$ for the sliced polynomial

$$f(\xi_0 + X, \xi_1 + \xi_{n+1}X + \xi_{2n+1}Y, \dots, \xi_n + \xi_{2n}X + \xi_{3n}Y).$$

Lemma 5. *Let $f \in k[x_0, \dots, x_n]$ be an absolutely irreducible polynomial of degree $\delta \geq 2$.*

(i) *The number of slices $\boldsymbol{\xi} \in k^{3n+1}$ for which the polynomial $f|_{\boldsymbol{\xi}}$ is not absolutely irreducible is at most $\frac{1}{2}(3\delta^4 - 4\delta^3 + 5\delta^2)q^{3n}$.*

(ii) *Let D be an integer satisfying $1 \leq D \leq \delta - 1$. Then the number of slices $\boldsymbol{\xi} \in k^{3n+1}$ for which the polynomial $f|_{\boldsymbol{\xi}}$ possesses a $\overline{k}$-rational factor of positive degree at most D does not exceed*

$$\tfrac{1}{8}(\delta D(D+1)(D+2)(8\delta - D - 3) + 16\delta^2)q^{3n}.$$

Proof. The conclusions of the lemma are immediate from Corollaries 3.2 and 3.4 of [10].

Next we recall a version of Weil's estimate valid for singular curves. Here we make use of the familiar notation $[\beta]$ for the largest integer not exceeding β.

LEMMA 6. *Let $F, G \in k[x,y]$ be non-zero polynomials of respective degrees $d_1 \ge 1$ and $d_2 \ge 0$. Suppose that F is absolutely irreducible, and that the absolutely irreducible factors of G each have degree distinct from d_1. Then the number, N, of non-singular k-rational zeros of FG satisfies*

$$N \ge q + 1 - \tfrac{1}{2}(d_1 - 1)(d_1 - 2)[2\sqrt{q}] - d_1 d_2.$$

Proof. Let F and G satisfy the hypotheses of the statement of the lemma. We consider first the situation in which G is a non-zero constant polynomial. Write S for the number of k-rational singular zeros of F. Then if the curve defined by the equation $F(x,y) = 0$ has genus g, it follows from Corollary 1 to Theorem 1 of Leep and Yeomans [23] that

$$|N + S - (q+1)| \le g[2\sqrt{q}] + \tfrac{1}{2}(d_1 - 1)(d_1 - 2) - g.$$

On applying the latter estimate together with the bound $g \le \frac{1}{2}(d_1-1)(d_1-2) - S$ supplied by the genus formula (see p. 201 of [15]), we obtain the lower bound

$$N \ge q + 1 - \tfrac{1}{2}(d_1 - 1)(d_1 - 2)[2\sqrt{q}]. \tag{1}$$

Suppose next that G is not a constant polynomial, so that G takes the shape $G_1 \dots G_t$, with each factor G_i absolutely irreducible of positive degree $e_i \ne d_1$. Since F is absolutely irreducible, and the degree of each factor G_i is distinct from that of F, the polynomials F and G possess no common factor in $\overline{k}[x,y]$. The equation $F(x,y) = 0$ defines an irreducible curve, moreover, and so it follows from Bézout's theorem (see Corollary 7.8 of Chapter I of [17]) that the number of common $\overline{k}$-rational zeros of F and G is at most $d_1 d_2$. The lower bound on the number of non-singular k-rational zeros of FG asserted in the statement of the lemma now follows on applying (1) to estimate the number of non-singular k-rational zeros of F, and accounting for those that are simultaneously zeros of G.

3. The proof of Theorem 1. We now apply the slicing procedure implicit in §2 within a modification of the argument developed by Laxton and Lewis, treating the cases with degree 7 and with degree 11 separately. It is convenient in our discussion to adopt the following convention. We say that a polynomial $G \in k[\mathbf{x}]$ has *type* $\mathbf{d} = (d_1, \dots, d_t)$ when (i) one has $d_1 \ge \dots \ge d_t \ge 1$, and (ii) the polynomial G factors over $\overline{k}[\mathbf{x}]$ in the shape $G = G_1 \dots G_t$, where for $1 \le i \le t$, each factor G_i is absolutely irreducible of degree d_i. Plainly, the type of a polynomial is uniquely defined. In addition we refer to a polynomial $\mathfrak{f} \in k[X,Y]$ as being *amenable* with profile $(\mathfrak{g}, \mathfrak{h})$ when $\mathfrak{f}$ factors in the shape $\mathfrak{f} = \mathfrak{g}\mathfrak{h}$, in which (i) the polynomials $\mathfrak{g}$ and $\mathfrak{h}$ are k-rational, (ii) $\mathfrak{g}$ is absolutely irreducible of degree at least 2, and (iii) the absolutely irreducible factors of $\mathfrak{h}$ over $\overline{k}[X,Y]$ each have degree distinct from that of $\mathfrak{g}$.

The proof of Theorem 1 for septic forms. Suppose that $q > 883$, and consider a form $F \in \mathfrak{o}[x_0, x_1, \dots, x_n]$ lying in the set $\mathcal{F}_7$, so that F^* satisfies $\mathrm{ord}(F^*) > 7$ and possesses no $\overline{k}$-rational linear factor. Suppose that F^* has type $\mathbf{d}$. A modicum of computation reveals that $\mathbf{d}$ must be one of (7), $(5,2)$, $(4,3)$ or $(3,2,2)$. We consider these cases in turn.

(a) $\mathbf{d} = (5,2)$, $(4,3)$ or $(3,2,2)$. In these situations the polynomial F^* factors in the shape $F^* = G_1 \dots G_t$, where G_i is absolutely irreducible of degree d_i $(1 \le i \le t)$. Note that in each case, the polynomial G_1 is the only absolutely irreducible factor of F^* of its degree, and so by conjugation, there is no loss in supposing that G_1 is k-rational. Since $q > 750$, we may apply Lemma 5(i) to G_1 with $\delta = d_1$ to deduce that a slice $\boldsymbol{\xi} \in k^{3n+1}$ exists for which $G_1|_{\boldsymbol{\xi}}$ is absolutely irreducible. Fix any one such slice, and fix any choice of $\boldsymbol{\Xi} \in \mathfrak{o}^{3n+1}$ with $\boldsymbol{\Xi} \equiv \boldsymbol{\xi} \pmod{\mathfrak{p}}$. Write $\mathfrak{f} = F|^*_{\boldsymbol{\Xi}}$ and $\mathfrak{g}_i = G_i|_{\boldsymbol{\xi}}$ $(1 \le i \le t)$. Then it follows that $\mathfrak{f} = \mathfrak{g}\mathfrak{h}$, where $\mathfrak{g} = \mathfrak{g}_1$ is absolutely irreducible of degree d_1, and $\mathfrak{h} = \mathfrak{g}_2 \dots \mathfrak{g}_t$ is a product of polynomials whose absolutely irreducible factors each have degree smaller than d_1. We may conclude, therefore, that $\mathfrak{f}$ is amenable with profile $(\mathfrak{g}, \mathfrak{h})$.

Suppose now that $\mathfrak{f} \in k[X,Y]$ is any amenable polynomial of degree 7, whether or not it is associated with a polynomial F^* of type $\mathbf{d} = (5,2)$, $(4,3)$ or $(3,2,2)$. Writing N for the number of non-singular k-rational zeros of $\mathfrak{f}$, it follows from Lemma 6 that $N \ge q + 1 - 15[2\sqrt{q}]$. Since q is a prime power, our hypothesis on its value ensures that $q > 884$, and so $\mathfrak{f}$ possesses a non-singular k-rational zero. We therefore deduce from Lemma 3 that $F|_{\boldsymbol{\Xi}}$, whence also F, possesses a non-singular K-rational zero.

(b) $\mathbf{d} = (7)$. Since $q > 371$, we may apply Lemma 5(ii) to F^*, with $\delta = 7$ and $D = 1$, to deduce that a slice $\boldsymbol{\xi} \in k^{3n+1}$ exists with the property that $F^*|_{\boldsymbol{\xi}}$ has no $\overline{k}$-rational linear factor. Fix any such slice, and a choice of $\boldsymbol{\Xi} \in \mathfrak{o}^{3n+1}$ with $\boldsymbol{\Xi} \equiv \boldsymbol{\xi} \pmod{\mathfrak{p}}$. It follows that the polynomial $\mathfrak{f} = F|^*_{\boldsymbol{\Xi}}$ does not possess a $\overline{k}$-rational linear factor, and so has type (7), $(5,2)$, $(4,3)$ or $(3,2,2)$. In each case, the absolutely irreducible factor of $\mathfrak{f}$ over $\overline{k}[X,Y]$ of highest degree is the only one of that degree, hence may be supposed to be k-rational. One consequently finds that $\mathfrak{f}$ is amenable with some profile $(\mathfrak{g}, \mathfrak{h})$, and so it follows as in the final paragraph of part (a) above that F possesses a non-singular K-rational zero.

We have demonstrated that whenever $q > 883$, then every polynomial F in $\mathcal{F}_7$ necessarily possesses a non-singular K-rational zero. Under the same hypothesis on q, we infer from Lemma 4 that every septic form $G \in K[\mathbf{x}]$, with $\mathrm{var}(G) > 49$, possesses a non-trivial K-rational zero. This completes the proof of Theorem 1 for septic forms.

The proof of Theorem 1 for unidecic forms. Suppose now that $q > 8053$, and consider a form $F \in \mathfrak{o}[x_0, x_1, \dots, x_n]$ lying in the set $\mathcal{F}_{11}$, so that F^*

satisfies $\operatorname{ord}(F^*) > 11$ and possesses no $\overline{k}$-rational linear factor. A smidgen of computation in this instance reveals that the type $\mathbf{d}$ of F^* is one of (11), $(9,2)$, $(4,4,3)$, $(3,3,3,2)$, or else lies in the set $\mathcal{D}$ consisting of the elements $(8,3)$, $(7,4)$, $(7,2,2)$, $(6,5)$, $(6,3,2)$, $(5,4,2)$, $(5,3,3)$, $(5,2,2,2)$, $(4,3,2,2)$, $(3,2,2,2,2)$. We examine these cases in turn.

(c) $\mathbf{d} \in \mathcal{D}$. Since $q > 5280$, in these cases the argument of part (a) may be applied, mutatis mutandis, to show that a slice $\mathbf{\Xi} \in \mathfrak{o}^{3n+1}$ exists for which the polynomial $\mathfrak{f} = F|^*_{\mathbf{\Xi}}$ is amenable with some profile $(\mathfrak{g}, \mathfrak{h})$. Suppose that $\mathfrak{f} \in k[X,Y]$ is any amenable polynomial of degree 11, whether or not it derives from a polynomial F^* of type $\mathbf{d} \in \mathcal{D}$. Writing N for the number of non-singular k-rational zeros of $\mathfrak{f}$, it follows from Lemma 6 that $N \ge q + 1 - 45[2\sqrt{q}]$. Since q is a prime power, our hypothesis on its value ensures that $q > 8054$, and so $\mathfrak{f}$ possesses a non-singular k-rational zero. We thus conclude from Lemma 3 that $F|_{\mathbf{\Xi}}$, whence also F, possesses a non-singular K-rational zero.

(d) $\mathbf{d} = (9,2)$. In this situation F^* factors in the shape $F^* = G_1G_2$, where G_1 has degree 9 and G_2 has degree 2. The polynomial G_1 is the only absolutely irreducible factor of its degree, and so by conjugation there is no loss in supposing that it is k-rational. Since $q > 4617$, we may apply Lemma 5(ii) to G_1, with $\delta = 9$ and $D = 3$, to show that a slice $\boldsymbol{\xi} \in k^{3n+1}$ exists for which $G_1|_{\boldsymbol{\xi}}$ has no absolutely irreducible factor over $\overline{k}[X,Y]$ of degree 3 or less. Fix any one such slice, and observe that $G_1|_{\boldsymbol{\xi}}$ must have type (9) or $(5,4)$. A choice of $\mathbf{\Xi} \in \mathfrak{o}^{3n+1}$ therefore exists, with $\mathbf{\Xi} \equiv \boldsymbol{\xi}$ (mod $\mathfrak{p}$), for which the polynomial $\mathfrak{f} = F|^*_{\mathbf{\Xi}}$ is of type $(9,2)$, $(9,1,1)$, $(5,4,2)$ or $(5,4,1,1)$. In each case, the absolutely irreducible factor of $\mathfrak{f}$ over $\overline{k}[X,Y]$ of highest degree is the only one of that degree, hence may be supposed to be k-rational. Thus we find that $\mathfrak{f}$ is amenable with some profile $(\mathfrak{g}, \mathfrak{h})$, and hence as in case (c) above we conclude that F possesses a non-singular K-rational zero.

(e) $\mathbf{d} = (11)$. Since $q > 7007$, we may apply Lemma 5(ii) to F^*, with $\delta = 11$ and $D = 3$, to deduce that a slice $\boldsymbol{\xi} \in k^{3n+1}$ exists for which $F^*|_{\boldsymbol{\xi}}$ has no absolutely irreducible factor over $\overline{k}[X,Y]$ of degree 3 or less. We may therefore suppose that there is a choice of $\mathbf{\Xi} \in \mathfrak{o}^{3n+1}$ for which the polynomial $\mathfrak{f} = F|^*_{\mathbf{\Xi}}$ is of type (11), $(7,4)$ or $(6,5)$. In each of these cases we deduce as in case (d) that $\mathfrak{f}$ is amenable with some profile $(\mathfrak{g}, \mathfrak{h})$. Thus, as in case (c), we conclude that F possesses a non-singular K-rational zero.

(f) $\mathbf{d} = (4,4,3)$ or $(3,3,3,2)$. In these cases the polynomial F^* factors in the shape $F^* = G_1 \dots G_t$, where G_i has degree d_i $(1 \le i \le t)$, and G_t is the only absolutely irreducible factor of its degree. By conjugation, therefore, there is no loss in supposing that G_t is k-rational. Since G_t has lowest degree amongst the absolutely irreducible factors of F^*, a slicing argument of the type previously employed might decompose one or more of the remaining factors so that no isolated factor remains. Such would obstruct the existence of a non-singular k-rational point. We instead proceed without slicing. Let the number of k-rational zeros of the polynomial G_t be M_0. Then according to Theorem 5.2 of [10], one has

$$(2)\qquad |M_0-q^{n-1}| \le (d_t-1)(d_t-2)q^{n-3/2}+5d_t^{13/3}q^{n-2} \le 2q^{n-3/2}+585q^{n-2}.$$

Since we are analysing quadratic and cubic polynomials, rather sharper estimates are achievable with greater effort, of course, but it transpires that such is unnecessary.

Write $f_1 = G_t$ and $f_2 = G_1 \dots G_{t-1}$. Since each factor G_i is absolutely irreducible, it follows that f_1 and f_2 are non-zero polynomials of degree at most 9 without a common factor in $\overline{k}[\mathbf{x}]$. Lemma 2.2 of [10] therefore ensures that the number of common k-rational zeros of f_1 and f_2 is at most $81q^{n-2}$. Next we bound the number of singular zeros of G_t. The latter polynomial is absolutely irreducible of degree $d_t \le 3$, and at least one of the partial derivatives of G_t, say $\partial G_t/\partial x_i$, is not identically zero and has degree $d_t - 1 \le 2$. Thus, again by Lemma 2.2 of [10], we see that the number of common k-rational zeros of G_t and $\partial G_t/\partial x_i$ is at most $9q^{n-2}$, whence G_t has at most $9q^{n-2}$ singular k-rational zeros. Write M_1 for the number of non-singular k-rational zeros of F^*. Then in view of the above discussion, one has $M_1 \ge M_0 - 90q^{n-2}$, and thus it follows from (2) that $M_1 \ge q^{n-1}-2q^{n-3/2}-675q^{n-2}$. Since $q > 729$, we conclude that F^* possesses a non-singular k-rational zero, and so Lemma 3 delivers a non-singular K-rational zero of F.

We have demonstrated that whenever $q > 8053$, then every polynomial F in $\mathcal{F}_{11}$ necessarily possesses a non-singular K-rational zero. Under the same hypothesis on q, we infer from Lemma 4 that every unidecic form $G \in K[\mathbf{x}]$, with $\mathrm{var}(G) > 121$, possesses a non-trivial K-rational zero. This completes the proof of Theorem 1 for unidecic forms.

4. The proof of Theorem 2. We now turn our attention to the refinement of Theorem 3.1 of Chakri and Hanine [11] embodied in Theorem 2 above. Let $f \in \mathbb{Z}_p[x_0,\dots,x_n]$ be homogeneous of degree d, and suppose that $n \ge 2d$ and $p > \frac{1}{2}(3d^4 - 4d^3 + 5d^2)$. An inspection of the proof of [11, Theorem 3.1] reveals that the conclusion of Theorem 2 follows at once whenever f^* fails to be absolutely irreducible, even in the absence of the hypothesis on p. Henceforth, therefore, we may suppose that f^* is absolutely irreducible. Given our hypothesis on p, we may apply Lemma 5(i) to f^* with $\delta = d$ to deduce that a slice $\boldsymbol{\xi} \in \mathbb{F}_p^{3n+1}$ exists for which $f^*|_{\boldsymbol{\xi}}$ is absolutely irreducible. It follows that there is a slice $\boldsymbol{\Xi} \in \mathbb{Z}_p^{3n+1}$ for which $f|_{\boldsymbol{\Xi}}^*$ is absolutely irreducible. Next let N denote the number of non-singular zeros of $f|_{\boldsymbol{\Xi}}^*$. Then as a consequence of Lemma 6, one has $N \geq p+1-(d-1)(d-2)\sqrt{p}$. Since $p > (d-1)^2(d-2)^2$, we conclude that $f|_{\boldsymbol{\Xi}}^*$ possesses a non-singular $\mathbb{F}_p$-rational zero. An application of Lemma 3 now shows that $f|_{\boldsymbol{\Xi}}$, and hence also f, possesses a non-trivial p-adic zero, whence, in particular, the congruence $f(x_0, \dots, x_n) \equiv 0 \pmod{p^2}$ has a primitive zero. This completes the proof of Theorem 2.

The condition $p > \frac{1}{2}(3d^4 - 4d^3 + 5d^2)$ in the statement of Theorem 2 can be improved, for certain smaller values of d, by employing a strategy similar to that underlying the proof of Theorem 1 in §3. The cases $d = 2$, 3, 5, 7 or 11 having already been dispatched by Theorem 1, we illustrate ideas with the case $d = 13$. As in our proof of Theorem 2, we consider a polynomial $f \in \mathbb{Z}_p[x_0, \dots, x_n]$ homogeneous of degree $d = 13$, and we suppose that $n \geq 2d$ and $p > 17357$. We may again suppose that f^* is absolutely irreducible, but now we apply Lemma 5(ii) with $\delta = d$ and $D = 3$. Since $p > 9893$, there is a slice $\boldsymbol{\xi} \in \mathbb{Z}_p^{3n+1}$ for which $f|_{\boldsymbol{\xi}}^*$ has no absolutely irreducible factor over $\overline{\mathbb{F}}_p[X, Y]$ of degree 3 or less. We may therefore suppose that $f|_{\boldsymbol{\xi}}^*$ is of type $\mathbf{d}$, where $\mathbf{d}$ is one of (13), $(9, 4)$, $(8, 5)$, $(7, 6)$ or $(5, 4, 4)$. In each case, the polynomial $f|_{\boldsymbol{\xi}}^*$ factorises over $\overline{\mathbb{F}}_p[X, Y]$ in such a manner that there is an absolutely irreducible factor that is the only factor of its degree. There is no loss, therefore, in supposing that this factor is $\mathbb{F}_p$-rational. The argument deployed to prove Theorem 1 in §3 above may consequently be applied to establish that whenever $p+1 > \frac{1}{2}(d-1)(d-2)[2\sqrt{p}]$, then $f|_{\boldsymbol{\xi}}^*$ possesses a non-singular $\mathbb{F}_p$-rational zero. The existence of a non-singular zero of f lying in $\mathbb{Z}_p^{n+1}$ now follows from Lemma 3. We conclude that the condition $p > \frac{1}{2}(3d^4 - 4d^3 + 5d^2)$ may be replaced when $d = 13$ by the sharper condition $p > 17357$. Similar observations hold for further smaller values of d.

References

[1] G. I. Arkhipov and A. A. Karatsuba, *Local representation of zero by a form*, Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), 948–961 (in Russian).

[2] E. Artin, *The Collected Papers of Emil Artin*, S. Lang and J. T. Tate (eds.), Addison-Wesley, Reading, 1965.

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

[4] B. J. Birch and D. J. Lewis, *$\mathfrak{p}$-adic forms*, J. Indian Math. Soc. (N.S.) 23 (1959), 11–32.

[5] —, —, *On $\mathfrak{p}$-adic forms*, Michigan Math. J. 9 (1962), 53–57.

[6] —, —, *Systems of three quadratic forms*, Acta Arith. 10 (1964/1965), 423–442.

[7] B. J. Birch, D. J. Lewis and T. G. Murphy, *Simultaneous quadratic forms*, Amer. J. Math. 84 (1962), 110–115.

[8] S. S. Brown, *Bounds on transfer principles for algebraically closed and complete discretely valued fields*, Mem. Amer. Math. Soc. 15 (1978), no. 204.

[9] W. D. Brownawell, *On p-adic zeros of forms*, J. Number Theory 18 (1984), 342–349.

[10] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. 12 (2006), 155–185.

[11] L. Chakri and E. M. Hanine, *Anisotropic forms modulo p^2*, Acta Arith. 108 (2003), 147–151.

[12] P. J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. 22 (1969), 131–151.

[13] V. B. Dem'yanov, *On cubic forms in discretely normed fields*, Dokl. Akad. Nauk SSSR (N.S.) 74 (1950), 889–891 (in Russian).

[14] —, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes*, Izv. Akad. Nauk SSSR Ser. Mat. 20 (1956), 307–324 (in Russian).

[15] W. Fulton, *Algebraic Curves*, Addison-Wesley, Reading, MA, 1989.

[16] M. J. Greenberg, *Lectures on Forms in Many Variables*, W. A. Benjamin, New York, 1969.

[17] R. Hartshorne, *Algebraic Geometry*, Springer, Berlin, 1977.

[18] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. 153 (1924), 113–130.

[19] E. Kaltofen, *Effective Noether irreducibility forms and applications*, J. Comput. System Sci. 50 (1995), 274–295.

[20] M. P. Knapp, *Artin's conjecture for forms of degree* 7 *and* 11, J. London Math. Soc. (2) 63 (2001), 268–274.

[21] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. 76 (1954), 819–827.

[22] R. R. Laxton and D. J. Lewis, *Forms of degrees* 7 *and* 11 *over $\mathfrak{p}$-adic fields*, in: Proc. Sympos. Pure Math. 8, Amer. Math. Soc., Providence, RI, 1965, 16–21.

[23] D. B. Leep and C. C. Yeomans, *The number of points on a singular curve over a finite field*, Arch. Math. (Basel) 63 (1994), 420–426.

[24] —, —, *Quintic forms over p-adic fields*, J. Number Theory 57 (1996), 231–241.

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

[26] D. J. Lewis and H. L. Montgomery, *On zeros of p-adic forms*, Michigan Math. J. 30 (1983), 83–87.

[27] P. A. B. Pleasants, *Forms over $\mathfrak{p}$-adic fields*, Acta Arith. 18 (1971), 289–296.

[28] W. M. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, J. Number Theory 6 (1974), 448–480.

[29] S. E. Schuur, *On systems of three quadratic forms*, Acta Arith. 36 (1980), 315–322.

[30] G. Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A612.

School of Mathematics
University of Bristol
University Walk, Clifton
Bristol BS8 1TW, United Kingdom
E-mail: matdw@bristol.ac.uk

Received on 23.2.2007 (5396)