ACTA ARITHMETICA
126.2 (2007)

Diagonal equations of different degrees over p-adic fields

by

Michael P. Knapp (Baltimore, MD)

1. Introduction. Let a_i and b_i $(1 \le i \le s)$ be rational integers, and let k and n be natural numbers with $k \ge n$. Consider the system of diagonal equations

$$a_1x_1^k + \cdots + a_sx_s^k = 0, \qquad b_1x_1^n + \cdots + b_sx_s^n = 0. \tag{1}$$

We are interested in determining conditions on s which will guarantee that the system (1) has nontrivial integral solutions over the fields $\mathbb{Q}_p$, where a solution is considered to be nontrivial provided that at least one of the x_i is nonzero. A special case of a conjecture attributed to Artin states that the system (1) should have a nontrivial $\mathbb{Q}_p$-integral solution for each prime p provided only that $s \ge k^2 + n^2 + 1$.

To describe the known results about this conjecture, we introduce a small amount of notation. For a given prime p and positive integers k, n, we write $\Gamma_p^*(k,n)$ to denote the least number such that the system (1) has a nontrivial $\mathbb{Q}_p$-integral solution whenever $s \ge \Gamma_p^*(k,n)$. Further, we define

$$\Gamma^*(k,n) = \max_p \Gamma_p^*(k,n).$$

A result due to Brauer [1] shows that this maximum exists for all pairs (k,n). Note that if $s \ge \Gamma^*(k,n)$, then the system (1) has a nontrivial $\mathbb{Q}_p$-integral solution for every prime p. Therefore Artin's conjecture may be restated as claiming that one should have $\Gamma^*(k,n) \le k^2 + n^2 + 1$ for all pairs (k,n).

Much is known about this problem in the situation where $k = n$. Davenport & Lewis [7] have shown that

$$\Gamma^*(k,k) \le \begin{cases} 2k^2+1, & k \text{ odd}, \\ 7k^3, & k \text{ even}. \end{cases} \tag{2}$$

2000 *Mathematics Subject Classification*: Primary 11D72; Secondary 11E76, 11E95.

Key words and phrases: Artin's conjecture, diagonal forms in many variables, local solubility.

The completion of this paper was partially supported by NSF grant DMS-0344082.

Hence this case of Artin's conjecture is true in the situation where $k = n$ and k is odd. Moreover, Davenport & Lewis show in their paper that one has $\Gamma_p^*(k,k) \le 2k^2 + 1$ except possibly when both $p \mid k$ and we have either $(k,p-1) = p-1$ or $(k,p-1) = (p-1)/2 < 3$.

We note here that if $k+1$ is a prime p, then one also has the lower bound $\Gamma^*(k,k) \ge 2k^2 + 1$. This follows from the observation of Davenport & Lewis [6] that in this situation there exists a single diagonal form in k^2 variables having no p-adic solutions. Taking two such forms with no variables in common leads to a system of two forms in $2k^2$ variables having no p-adic solution. Thus the work of Davenport & Lewis shows that $\Gamma^*(k,k) = 2k^2+1$ for these values of k.

Recently, Brüdern & Godinho ([2], [3]) have proven this case of Artin's conjecture for most even values of k. In particular, they have shown that $\Gamma_p^*(k,k) \le 2k^2 + 1$ except possibly when either $k = p^\tau(p-1)$ with p prime and $\tau \ge 1$, or $k = 3 \cdot 2^\tau$. Even in these situations, however, they have shown that $\Gamma_p^*(k,k) \le 8k^2$.

When $k \ne n$, much less is known about this problem. Leep & Schmidt [8] have shown that $\Gamma^*(k,n) \le (k^2+1)(n^2+1)$. Also, their work in [8] shows that $\Gamma^*(k,1) \le k^2 + 2$, although this latter fact is not explicitly stated. Hence, this case of Artin's conjecture is true when one of the degrees is equal to 1.

While the bound due to Leep & Schmidt for general degrees k and n is larger than that conjectured by Artin, Wooley [10] has shown that if the prime p is large, then the Artin bound is too big. In particular, he has shown that if $p > k^4 n^2$, then

$$\Gamma_p^*(k,n) \le \begin{cases} 2k+2n+1 & \text{if } k \ge n > 1, \\ 2k+2 & \text{if } k > n = 1, \\ 3 & \text{if } k = n = 1. \end{cases}$$

Hence, for each pair (k,n), it is only for relatively small primes that bounds as large or larger than those conjectured by Artin are needed.

The purpose of this paper is to develop new bounds on $\Gamma^*(k,n)$ in the case where $k \ne n$. First, we have the following theorem.

THEOREM 1. *Let $k > n > 1$ be integers. Then*

$$\Gamma^*(k,n) \le 64(k+2n)(k+n)(k-n)^2 - 2k - 3n + 1.$$

The reader can see that the conclusion of Theorem 1 is better than that of Leep & Schmidt [8] when the degrees k and n are large and close together, but worse when k is significantly larger than n. Unfortunately, even in the best possible scenario, when $k = n+1$, the bound of Theorem 1 is worse than the bound conjectured by Artin.

Theorem 1 is actually an easy corollary of the following theorem, which is more precise but somewhat more complicated to state.

THEOREM 2. *Let $k > n > 1$ be integers. Let p be a prime, and write $k = p^{\tau_k} k_0$ and $n = p^{\tau_n} n_0$, with $(p, k_0 n_0) = 1$.*

(i) *If p is odd, then*

$$\Gamma_p^*(k,n) \le (k+2n)\left(k_0\,\frac{p^{2h+\tau_k-1}-1}{p-1} + n_0\,\frac{p^{2h+\tau_n-1}-1}{p-1}\right) + n + 1,$$

where $h = [\log_p((k-n)/(p-1))]+2$, with $[\cdot]$ being the greatest integer function.

(ii) *If $p = 2$, then*

$$\Gamma_2^*(k,n) \le (k+2n)(k+n)(2^{2h}) - 2k - 3n + 1,$$

where we define

$$h = \begin{cases} 2 & \text{if } k-n \text{ is odd,} \\ [\log_2(k-n)] + 3 & \text{if } k-n \text{ is even.} \end{cases}$$

The basic idea behind the proof of Theorem 2 is to lift solutions of congruences to p-adic solutions. We begin by utilizing a normalization procedure due to Wooley [10], which shows that we may restrict our attention to systems which have the property that many of the variables are explicit modulo p (i.e. the variable still occurs with a nonzero coefficient when the system is reduced modulo p). By setting some of these variables equal to multiples of others, we then show that there exists a nontrivial nonsingular solution of a system similar to (1), but with the equalities replaced by congruences modulo suitable powers of p. Finally, we use a version of Hensel's Lemma to lift this solution to a nontrivial $\mathbb{Q}_p$-integral solution of (1).

If it happens that $(p-1) \nmid (k-n)$, then it turns out that our methods allow us to look modulo smaller powers of p than in the main argument. Thus we obtain the following corollary.

COROLLARY 1. *Let $k > n > 1$ be integers and p be a prime. If $(p-1) \nmid (k-n)$, then*

$$\Gamma_p^*(k,n) \le \frac{3}{2}\,(k+2n)(k+n) + n + 1.$$

If we restrict the parities of k and n, then we can use a different, simpler method to obtain smaller bounds, even when k is large compared to n. In this vein, we will also prove the following theorem.

THEOREM 3. *Let k and n be positive integers with k odd. Then $\Gamma^*(k,n) \le 2n^2 + k^2 + 1$.*

We will prove this theorem by finding a linear space on which the form of odd degree is identically zero and then finding a zero of the other form in this space.

2. Preliminaries. Before we begin the proof of Theorems 1 and 2, we must discuss the concept of a normalized system of forms. To do this, we will follow the normalization procedure used by Wooley in [10]. Consider a system $\mathbf{F} = (F, G)$ of two forms as in (1), with $\deg F = k$ and $\deg G = n$. We assume that $k > n$. Fix a prime p and write $k = p^{\tau_k} k_0$ and $n = p^{\tau_n} n_0$, where $(p, k_0 n_0) = 1$. We write $\mathbf{F}^* = (F^*, G^*)$ for the image of the system $\mathbf{F}$ modulo p. Two systems $\mathbf{F}$ and $\mathbf{F}'$ whose coefficients are p-adic integers are called *equivalent* if we can write

$$\mathbf{F}' = (F', G') = (aF(p^{v_1}x_1, \ldots, p^{v_s}x_s), bG(p^{v_1}x_1, \ldots, p^{v_s}x_s)),$$

where $v_1, \ldots, v_s$ are all rational integers and a and b are any nonzero rational numbers. Now, for a fixed number r (to be chosen later) with $1 \le r \le s$, we define $R = \{1, \ldots, r\}$, $T = \{r+1, \ldots, s\}$, $t = |T|$, and $N = 2(r-1)n$. Finally, we define

$$\partial(\mathbf{F}) = \partial(F, G) = \prod_{\substack{i \neq j \\ i,j \in R}} (a_i^n b_j^k - a_j^n b_i^k) \prod_{h \in T} a_h^N,$$

and call a system $\mathbf{F}$ *p-normalized* if $\partial(\mathbf{F}) \neq 0$ and the power of p dividing $\partial(\mathbf{F})$ is less than or equal to the power of p dividing $\partial(\mathbf{F}')$ for all systems $\mathbf{F}'$ equivalent to $\mathbf{F}$. By a standard argument (see for example page 33 of [11]) based on the compactness of the p-adic integers, it is sufficient to prove Theorem 2 for p-normalized systems.

We now give a lemma showing that p-normalized systems are explicit in a large number of variables when considered modulo p. First, however, we need to establish some more notation. If $\mathbf{F}$ is a p-normalized system, let U be the set of variables explicit in F^* and let V be the set of variables explicit in G^*. Then we have the following lemma.

Lemma 1. *Suppose that $\mathbf{F} = (F, G)$ is a p-normalized system of the form* (1). *Then*

$$|U| \ge \frac{r}{2k} + \frac{t}{k}, \qquad |V| \ge \frac{r}{2n}.$$

This lemma is immediate from Lemma 2 of [10]. While Lemma 1 is all that we need for our purposes, Wooley in fact shows in [10] that more can be said about systems which have been normalized by this procedure.

As mentioned in the introduction, our plan is to solve the system (1) modulo powers of p and then lift this solution to a solution of (1) in p-adic integers. Our next lemma, due to Schanuel [9], will help us with the first part of our plan. This is a version of Chevalley's Theorem (see [4]) for congruences modulo prime powers. However, rather than allowing the variables to take on any values as in Chevalley's Theorem, the variables are restricted to lie in the Teichmüller set $T_{\mathbb{Q}_p} = \{x \in \mathbb{Q}_p : x^p = x\}$.

LEMMA 2. *Let $f_1, \dots, f_R \in \mathbb{Z}_p[x_1, \dots, x_N]$ be polynomials with no constant terms, and for each i let d_i be the (total) degree of f_i. Finally, let $v_1, \dots, v_R$ be positive integers. If*

$$N > \sum_{i=1}^{R} d_i(p^{v_i} - 1)/(p-1),$$

then the system

$$f_i(x_1, \dots, x_N) \equiv 0 \pmod{p^{v_i}}, \qquad i = 1, \dots, R,$$

has a nontrivial solution with each variable belonging to the Teichmüller set $T_{\mathbb{Q}_p}$.

The final lemma of this section will be needed in order to deal with the prime $p = 2$.

LEMMA 3. *Let d be a positive integer and write $d = 2^r \ell$, with ℓ odd. Set $h \ge 2$ if $r = 0$, and set $h \ge r + 3$ if $r > 0$. Then the expression x^d takes on more than one value modulo 2^h for odd values of x. Moreover, if h is any smaller integer, then $x^d \equiv 1 \pmod{2^h}$ for all odd values of x.*

Proof. If $h = 1$, then the lemma is trivially true. For $h \ge 2$, the lemma is an easy consequence of the fact that the number of reduced dth power residues modulo 2^h is given by

$$\frac{2^{h-1}}{(d,2)(d,2^{h-2})}.$$

To see that this formula is true, we note that modulo 2^h, all reduced dth power residues have the same number of dth roots, so that the number of such residues is given by $\phi(2^h)/N = 2^{h-1}/N$, where N is the number of dth roots of unity. Recalling that for $h \ge 2$, any reduced residue modulo 2^h may be written uniquely in the form $(-1)^\alpha 5^\beta$ with $\alpha \in \{0, 1\}$ and $\beta \in \{0, \dots, 2^{h-2} - 1\}$, we see that the number of dth roots of unity is equal to the number of pairs (α, β) such that $(-1)^{\alpha d} 5^{\beta d} \equiv 1 \pmod{2^h}$. It is then necessary and sufficient that the pair (α, β) satisfy the equations

$$\alpha d \equiv 0 \pmod 2, \qquad \beta d \equiv 0 \pmod{2^{h-2}}.$$

It is easy to see that there are exactly $(d, 2)(d, 2^{h-2})$ such pairs. This completes the proof of the lemma. ■

3. A version of Hensel's Lemma. The final result which we will need in order to prove Theorems 1 and 2 is a version of Hensel's Lemma. This will allow us to lift solutions of congruences to solutions of equations in p-adic integers. Since it is no more difficult to prove this version of Hensel's Lemma for a system of arbitrarily many additive forms than for a system of two forms, we will prove a slightly stronger statement than we actually need. Our proof does, however, require a fair amount of notation, and so for this section only we will depart from the notation used in the remainder of this paper.

Lemma 4. *Consider a system*

$$\begin{aligned} F_1(\mathbf{x}) &= a_{11}x_1^{k_1} + \cdots + a_{1s}x_s^{k_1} = 0, \\ &\vdots \\ F_R(\mathbf{x}) &= a_{R1}x_1^{k_R} + \cdots + a_{Rs}x_s^{k_R} = 0, \end{aligned} \tag{3}$$

where $k_1, \ldots, k_R$ are positive integers and all of the coefficients are integers. Let p be a prime number and for $1 \le j \le R$ define numbers τ_j and $\widetilde{k}_j$ such that $k_j = p^{\tau_j}\widetilde{k}_j$ with $(p, \widetilde{k}_j) = 1$. Further, for $1 \le j \le R$, define

$$\gamma_j = \begin{cases} \tau_j & \text{if } p \text{ is odd}, \\ \tau_j + 1 & \text{if } p = 2. \end{cases}$$

Let h be a positive integer, and suppose that $\mathbf{z}$ is a nontrivial solution of the system of congruences

$$F_j(\mathbf{x}) \equiv 0 \pmod{p^{2h+\gamma_j-1}} \qquad (1 \le j \le R) \tag{4}$$

such that the matrix

$$\begin{bmatrix} a_{11}z_1^{k_1-1} & \cdots & a_{1s}z_s^{k_1-1} \\ \vdots & & \vdots \\ a_{R1}z_1^{k_R-1} & \cdots & a_{Rs}z_s^{k_R-1} \end{bmatrix} \tag{5}$$

has an $R \times R$ submatrix M such that

$$\det M \not\equiv 0 \pmod{p^h}. \tag{6}$$

Then the system (3) *has a $\mathbb{Q}_p$-integral solution $\mathbf{y}$ such that $\mathbf{y} \equiv \mathbf{z} \pmod{p^h}$.*

An immediate corollary of Lemma 4 is that if $R = 2$ and $\mathbf{z}$ is a nontrivial solution of (4) such that

$$a_{1m}a_{2n}z_m^{k_1-1}z_n^{k_2-1} - a_{1n}a_{2m}z_n^{k_1-1}z_m^{k_2-1} \not\equiv 0 \pmod{p^h} \tag{7}$$

for some m and n, then the system (3) has a nontrivial $\mathbb{Q}_p$-integral solution.

Proof. We first note that we may assume without loss of generality that $\tau_1 \ge \cdots \ge \tau_R$. For each j, we now define $q_j = \tau_j - \tau_R$, so that $\tau_j = \tau_R + q_j$

and $\gamma_j = \gamma_R + q_j$ for each j with $1 \leq j \leq R$. Finally, define $\mu_0 = 2h + \gamma_R - 1$, and suppose that for some $\mu \geq \mu_0$ there is a point $\mathbf{z} = (z_1, \ldots, z_s)$ such that

$$\begin{gathered} F_1(\mathbf{z}) \equiv 0 \pmod{p^{\mu+q_1}}, \\ \vdots \\ F_R(\mathbf{z}) \equiv 0 \pmod{p^{\mu+q_R}}, \end{gathered}$$

and such that there exists an $R \times R$ submatrix M of (5) for which the relation (6) holds. For $1 \leq i \leq s$, we set

$$y_i = z_i + p^{\mu-h-\tau_R+1} d_i,$$

where we wish to choose the d_i to satisfy

$$\begin{gathered} F_1(\mathbf{y}) \equiv 0 \pmod{p^{\mu+q_1+1}}, \\ \vdots \\ F_R(\mathbf{y}) \equiv 0 \pmod{p^{\mu+q_R+1}}. \end{gathered} \tag{8}$$

Suppose for the moment that this can be done for all values of μ with $\mu \geq \mu_0$. Noting that $\mathbf{y} \equiv \mathbf{z} \pmod{p^h}$, we see that the condition (6) also holds for $\mathbf{y}$. Hence we may proceed inductively to show that for all positive integers r, the system

$$\begin{gathered} F_1(\mathbf{x}) \equiv 0 \pmod{p^{\mu_0+q_1+r}}, \\ \vdots \\ F_R(\mathbf{x}) \equiv 0 \pmod{p^{\mu_0+q_R+r}} \end{gathered}$$

has a solution $\mathbf{y}_r$ with $\mathbf{y}_r \equiv \mathbf{z} \pmod{p^h}$. Therefore the solution to (4) can be lifted to a solution of (3), as desired.

To show that we may always choose the d_i appropriately, note that for each i and j we have

$$y_i^{k_j} = (z_i + p^{\mu-h-\tau_R+1} d_i)^{k_j} = z_i^{k_j} + k_j p^{\mu-h-\tau_R+1} d_i z_i^{k_j-1} + \cdots .$$

Considering this as a polynomial in the z_i and d_i, we claim that only the first two terms of this expansion can be explicit modulo $p^{\mu+q_j+1}$. Before proving this, we will show how it implies the truth of the lemma. The claim implies that we have

$$y_i^{k_j} \equiv z_i^{k_j} + k_j p^{\mu-h-\tau_R+1} d_i z_i^{k_j-1} \pmod{p^{\mu+q_j+1}}.$$

Therefore, if we write $F_j(\mathbf{z}) = p^{\mu+q_j} C_j$ for each j and recall that $k_j = p^{\tau_j} \widetilde{k}_j$ and $\tau_j = \tau_R + q_j$, then

$$F_1(\mathbf{y}) \equiv p^{\mu+q_1}C_1 + p^{\mu+q_1-h+1}\widetilde{k}_1(a_{11}z_1^{k_1-1}d_1 + \cdots + a_{1s}z_s^{k_1-1}d_s) \pmod{p^{\mu+q_1+1}},$$

$$\vdots$$

$$F_R(\mathbf{y}) \equiv p^{\mu+q_R}C_R + p^{\mu+q_R-h+1}\widetilde{k}_R(a_{R1}z_1^{k_R-1}d_1 + \cdots + a_{Rs}z_s^{k_R-1}d_s) \pmod{p^{\mu+q_R+1}}.$$

Hence we can choose $d_1, \ldots, d_s$ as desired if we can solve the system

$$p^{h-1}C_1 + \widetilde{k}_1(a_{11}z_1^{k_1-1}d_1 + \cdots + a_{1s}z_s^{k_1-1}d_s) \equiv 0 \pmod{p^h},$$

$$\vdots$$

$$p^{h-1}C_R + \widetilde{k}_R(a_{R1}z_1^{k_R-1}d_1 + \cdots + a_{Rs}z_s^{k_R-1}d_s) \equiv 0 \pmod{p^h}.$$

However, since there is a submatrix M of (5) such that $\det M \not\equiv 0 \pmod{p^h}$, we can solve this system for $d_1, \ldots, d_s$. Therefore we can solve (8) for all $\mu \ge \mu_0$, as needed.

It remains to prove the claim that only the first two terms in the expansion of $y_i^{k_j}$ may be explicit modulo $p^{\mu+q_j+1}$. When we consider the expansion as a polynomial in the z_i and d_i, the coefficient of the lth term after the first is

$$\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l.$$

Note that

$$\mathrm{ord}_p\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right) = \mathrm{ord}_p\left(\binom{k_j}{l}\right) + l\mu - lh - l\tau_R + l,$$

where $\mathrm{ord}_p(x)$ is the maximal power of p dividing x.

For $l > 1$, write $l = p^r\widetilde{l}$ with $(p, \widetilde{l}) = 1$. Since

$$\binom{k_j}{l} = \frac{k_j}{l}\binom{k_j-1}{l-1},$$

we obtain

$$\begin{aligned}\mathrm{ord}_p&\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right)\\ &= \mathrm{ord}_p\left(\frac{k_j}{l}\binom{k_j-1}{l-1}\right) + l\mu - lh - l\tau_R + l\\ &= \tau_j - r + \mathrm{ord}_p\left(\binom{k_j-1}{l-1}\right) + l\mu - lh - l\tau_R + l\\ &\ge \tau_j - r + l\mu - lh - l\tau_R + l.\end{aligned}$$

Thus, if $l > 1$ and $r = 0$, then

$$\begin{aligned}\operatorname{ord}_p\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right) &\geq \tau_j + l\mu - lh - l\tau_R + l\\ &\geq \tau_j + (\mu - h - \tau_R + 1) + (\mu - h - \tau_R + 1)\\ &= \mu + q_j + 1 + (\mu - 2h - \tau_R + 1)\\ &\geq \mu + q_j + 1,\end{aligned}$$

where the last inequality is true since we assumed that $\mu \geq 2h + \gamma_R - 1 \geq 2h + \tau_R - 1$. Hence these terms are not explicit modulo $p^{\mu+q_j+1}$.

Finally, we must deal with the situation where $l > 1$ and $r > 0$. We have

$$\begin{aligned}(9)\quad \operatorname{ord}_p&\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right)\\ &\geq \tau_j - r + l(\mu - h - \tau_R + 1)\\ &= \tau_j - r + \mu - h - \tau_R + 1 + (l-1)(\mu - h - \tau_R + 1)\\ &\geq \tau_j - r + \mu - h - \tau_R + 1 + (p^r - 1)(\mu - h - \tau_R + 1).\end{aligned}$$

Our assumption is that $\mu \geq 2h + \tau_R - 1 + \delta$, where $\delta = 0$ if p is odd and $\delta = 1$ if $p = 2$. This implies that

$$(10)\quad \operatorname{ord}_p\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right) \geq \mu + q_j + 1 - r - h + (p^r - 1)(h + \delta).$$

To see that these terms are not explicit modulo $p^{\mu+q_j+1}$, we need to show that $-r - h + (p^r - 1)(h + \delta) \geq 0$. We have

$$\begin{aligned}-r - h + (p^r - 1)(h + \delta) &= (p^r - 2)h + (p^r - 1)\delta - r\\ &\geq p^r - 2 + (p^r - 1)\delta - r\\ &= \begin{cases} p^r - r - 2, & p > 2,\\ 2^{r+1} - r - 3, & p = 2.\end{cases}\end{aligned}$$

To see that this last expression is nonnegative when $p > 2$, let $f(x) = p^x - x - 2$. Then

$$f(1) = p - 3 \geq 0.$$

Moreover, when $x \geq 1$, we have

$$f'(x) = p^x \ln(p) - 1 \geq 3^1 \ln(3) - 1 > 0.$$

Hence, when $p > 2$, the function $f(x)$ starts out nonnegative at $x = 1$ and is increasing for $x \geq 1$. Thus $f(r)$ is nonnegative for all positive integers r, and so

$$\operatorname{ord}_p\left(\binom{k_j}{l}(p^{\mu-h-\tau_R+1})^l\right) \geq \mu + q_j + 1.$$

Therefore these terms are not explicit modulo $p^{\mu+q_j+1}$, as claimed. When $p = 2$, an essentially identical proof shows that $2^{r+1} - r - 3 \geq 0$ for all positive integers r. This completes the proof of the lemma. ■

4. The proofs of Theorems 1 and 2 and Corollary 1. We now return to the notation used in Sections 1 and 2. As mentioned in Section 2, it suffices to prove our results in the case where the system (1) is p-normalized, and so we will make that assumption throughout this section. Let h be a positive integer such that the expression x^{k-n} takes on at least two nonzero values modulo p^h when x is relatively prime to p, and define the numbers γ_k and γ_n as in the statement of Lemma 4. Our plan is to find a nontrivial nonsingular solution of the system

$$\begin{aligned} F(\mathbf{x}) &= a_1x_1^k+\cdots+a_sx_s^k \equiv 0 \pmod{p^{2h+\gamma_k-1}},\\ G(\mathbf{x}) &= b_1x_1^n+\cdots+b_sx_s^n \equiv 0 \pmod{p^{2h+\gamma_n-1}}, \end{aligned} \tag{11}$$

which will lift to a nontrivial solution of (1) by Lemma 4.

In order to accomplish this, suppose that for some number N we can choose a set $\mathfrak{U}$ of N variables in the set U defined in Section 2 and a set $\mathfrak{V}$, disjoint from $\mathfrak{U}$, of N variables in the set V. We then pick N disjoint pairs of variables consisting of one variable from $\mathfrak{U}$ and one from $\mathfrak{V}$. Now, if a pair x_i, x_j of variables is such that both are in both sets U and V, then we set $x_i = tx_j$, where t is nonzero modulo p and chosen such that

$$a_ib_jt^{k-n} - a_jb_i \not\equiv 0 \pmod{p^h}.$$

By our assumption on h, such a choice of t is possible. Otherwise, we set $x_i = x_j$. If a variable x_i is not a member of any of our pairs, we set $x_i = 0$. Making these assignments yields a new system

$$c_1y_1^k+\cdots+c_Ny_N^k = 0, \qquad d_1y_1^n+\cdots+d_Ny_N^n = 0. \tag{12}$$

We now seek a nontrivial solution of the system

$$\begin{aligned} c_1y_1^k+\cdots+c_Ny_N^k &\equiv 0 \pmod{p^{2h+\gamma_k-1}},\\ d_1y_1^n+\cdots+d_Ny_N^n &\equiv 0 \pmod{p^{2h+\gamma_n-1}}. \end{aligned} \tag{13}$$

Although we could use Lemma 2 immediately to obtain a bound on N which will guarantee that we can solve (13) nontrivially, we can obtain a smaller bound by solving instead the equations

$$\begin{aligned} c_1y_1^{k_0}+\cdots+c_Ny_N^{k_0} &\equiv 0 \pmod{p^{2h+\gamma_k-1}},\\ d_1y_1^{n_0}+\cdots+d_Ny_N^{n_0} &\equiv 0 \pmod{p^{2h+\gamma_n-1}}, \end{aligned} \tag{14}$$

with all of the variables restricted to lie in the Teichmüller set $T_{\mathbb{Q}_p}$. Because of the property that $x^p = x$ for any $x \in T_{\mathbb{Q}_p}$, any nontrivial solution of (14) is also a nontrivial solution of (13).

By Lemma 2, a solution of (14) exists with each variable in $T_{\mathbb{Q}_p}$ and at least one variable nonzero modulo p provided that

$$N \ge k_0\,\frac{p^{2h+\gamma_k-1}-1}{p-1} + n_0\,\frac{p^{2h+\gamma_n-1}-1}{p-1} + 1. \tag{15}$$

Suppose that this condition holds. Then the solution of (14) is also a solution of (13), and upon converting the variables $y_1, \ldots, y_N$ back into $x_1, \ldots, x_s$, we obtain a nontrivial solution of the system (11). Moreover, since at least one of $y_1, \ldots, y_N$ is nonzero modulo p, there exist i, j such that x_i and x_j are nonzero modulo p and were paired together to obtain a variable y_l. The way in which we set either $x_i = tx_j$ or $x_i = x_j$ above ensures that

$$\begin{aligned}(16)\qquad a_ib_jx_i^{k-1}x_j^{n-1} - a_jb_ix_j^{k-1}x_i^{n-1} &= (x_ix_j)^{n-1}(a_ib_jx_i^{k-n} - a_jb_ix_j^{k-n}) \\ &\not\equiv 0 \pmod{p^h}.\end{aligned}$$

Therefore, since we have a solution of (11) for which the condition (16) holds, Lemma 4 allows us to lift this solution to a nontrivial solution of (1).

To complete the proof, we need to first find an appropriate value for h, and then obtain a bound on s which will guarantee that we can satisfy the condition given in (15). Recall that our criterion for choosing h was that the expression x^{k-n} should attain at least two distinct values modulo p^h when x is relatively prime to p. If p is odd, then this can only fail to occur if $k-n$ is divisible by $\phi(p^h) = p^{h-1}(p-1)$. If we set $h = [\log_p((k-n)/(p-1))]+2$, then h is a positive integer such that $p^{h-1}(p-1) > k-n$, and so our condition on h is satisfied. Now, for convenience, write M for the right-hand side of the inequality (15). Note that we can definitely choose M pairs of variables in the above manner if we know that there are at least M variables explicit when F is reduced modulo p and there are at least $2M$ variables explicit when G is reduced modulo p. That is, we can satisfy the condition on N given in (15) if we can ensure that

$$(17)\qquad |U| \geq M, \qquad |V| \geq 2M.$$

Since $|U|$ and $|V|$ are both integers, it is sufficient to show that

$$|U| > M-1, \qquad |V| > 2M-1.$$

By Lemma 1, these inequalities will hold provided that we have

$$\frac{r}{2k} + \frac{t}{k} > M-1, \qquad \frac{r}{2n} > 2M-1,$$

where $r+t = s$. Noting that M is an integer, we can satisfy these inequalities by setting $r = 4nM - 2n + 1$ and $s \geq (k+2n)M - (k+n) + 1$. Hence, when p is odd, we can satisfy all of our conditions, and hence find a nontrivial p-adic solution to the system (1), whenever we have

$$(18)\qquad s \geq (k+2n)\left(k_0\,\frac{p^{2h+\gamma_k-1}-1}{p-1} + n_0\,\frac{p^{2h+\gamma_n-1}-1}{p-1} + 1\right) - (k+n) + 1.$$

Upon noting that $\gamma_k = \tau_k$ and $\gamma_n = \tau_n$ when p is odd, we see that this is equal to the estimate in Theorem 2.

Since $h = [\log_p((k-n)/(p-1))] + 2$, one can see that this bound on s is less than

$$\begin{aligned}(k+2n)\biggl(k_0\,\frac{p^{2h+\tau_k-1}}{p-1} + n_0\,\frac{p^{2h+\tau_n-1}}{p-1} + 1\biggr) - (k+n) + 1 \\ &= (k+2n)(k+n)\biggl(\frac{p^{2h-1}}{p-1}\biggr) + (k+2n) - (k+n) + 1 \\ &\le (k+2n)(k+n)(k-n)^2\biggl(\frac{p}{p-1}\biggr)^3 + n + 1 \\ &\le \frac{27}{8}\,(k+2n)(k+n)(k-n)^2 + n + 1,\end{aligned}$$

where the first inequality follows from the definition of h and the second follows from the fact that $p \ge 3$. Note that this estimate is clearly smaller than the estimate given in Theorem 1.

Finally, we need to deal with the case when $p = 2$. In this situation we make use of Lemma 3, defining

$$h = \begin{cases} 2 & \text{if } k-n \text{ is odd,} \\ [\log_2(k-n)] + 3 & \text{if } k-n \text{ is even.} \end{cases}$$

This definition ensures that the hypotheses of Lemma 3 are satisfied with $d = k - n$, and hence that the expression x^{k-n} takes on at least two distinct values modulo 2^h for odd values of x.

Now, with this value of h we need once again to satisfy the condition on N given in (15). The same reasoning as above shows that this can be done if we again set $r = 4nM - 2n + 1$ and $s \ge (k+2n)M - (k+n) + 1$. Recalling that $\gamma_k = \tau_k + 1$ and $\gamma_n = \tau_n + 1$ when $p = 2$, this means that we can find a 2-adic solution to the system (1) provided that

$$\begin{aligned} s &\ge (k+2n)(k_0 \cdot 2^{2h+\tau_k} + n_0 \cdot 2^{2h+\tau_n} - 1) - (k+n) + 1 \\ &= (k+2n)(k+n)(2^{2h}) - 2k - 3n + 1,\end{aligned}$$

as desired. If our definition of h yields $h = [\log_2(k-n)] + 3$, then this bound is at most

$$\begin{aligned}(k+2n)(k+n)(2^{2\log_2(k-n)+6}) - 2k - 3n + 1 \\ &\le 64(k+2n)(k+n)(k-n)^2 - 2k - 3n + 1,\end{aligned}$$

which is the estimate in Theorem 1. If we have $h = 2$, then our bound on s is

$$s \ge 16(k+2n)(k+n) - 2k - 3n + 1,$$

which is clearly smaller than the estimate for $\Gamma^*(k,n)$ given in Theorem 1. This completes the proof of Theorems 1 and 2. ∎

In order to prove Corollary 1, we simply note that if p is a prime and $(p-1) \nmid (k-n)$, then we clearly cannot have $\phi(p^h) \mid (k-n)$ for any h. Therefore we may take $h = 1$ in the proof of Theorem 2. Then the bound on s which we obtain in (18) becomes

$$\begin{aligned} s &\geq (k+2n)\left(k_0 \frac{p^{\tau_k+1}-1}{p-1} + n_0 \frac{p^{\tau_n+1}-1}{p-1} + 1\right) - (k+n) + 1 \\ &= (k+2n)\left(\frac{kp}{p-1} - \frac{k_0}{p-1} + \frac{np}{p-1} - \frac{n_0}{p-1} + 1\right) - (k+n) + 1. \end{aligned}$$

Since p must be at least 3 in order for the hypothesis of the corollary to hold, it is easy to see that this bound is at most $\frac{3}{2}(k+2n)(k+n)+n+1$, as desired. ∎

One can of course prove many other corollaries in a similar manner. We point out here for the record that for specific values of p, k and n, one can typically obtain better bounds on $\Gamma_p^*(k,n)$ by adapting the methods here to the particular numbers involved than by merely quoting Theorems 1 and 2.

5. The proof of Theorem 3. As mentioned in the introduction, we prove Theorem 3 via an argument based on finding linear spaces of zeros of a form of odd degree. Since this argument will not require the normalization procedure described in Section 2, we will drop the assumption that the system (1) is p-normalized. Before we begin the proof, we state a few lemmata. Our first lemma, which gives a bound on how many variables are needed to ensure that a single additive form has a nontrivial zero, is due to Davenport & Lewis. This is Theorem 1 of [6].

Lemma 5. *The equation*

$$a_1 x_1^n + \cdots + a_s x_s^n = 0,$$

where the a_i are rational integers, has a $\mathbb{Q}_p$-integral solution for each p provided that $s \geq n^2 + 1$. Moreover, if $n+1$ is prime, then this bound cannot be reduced.

Our second lemma is another version of Hensel's Lemma, this version being a consequence of the theory of kth power residues of rational integers.

Lemma 6. *Suppose that $p^\tau \parallel k$, and define $\gamma = \gamma(k,p)$ by*

$$\gamma = \begin{cases} 1 & \text{if } \tau = 0, \\ \tau + 1 & \text{if } \tau > 0 \text{ and } p > 2, \\ \tau + 2 & \text{if } \tau > 0 \text{ and } p = 2. \end{cases}$$

Then if the congruence

$$ax^k + b \equiv 0 \pmod{p^\gamma}$$

with $ab \not\equiv 0 \pmod{p}$ *is soluble*, *then the equation*

$$ax^k + b = 0$$

has a nonzero solution in $\mathbb{Q}_p$.

A proof of this result can be found on page 36 of [5]. We point out that this definition of γ differs from the one given in Section 3. Note that a consequence of this lemma is that any number which is both relatively prime to p and a kth power modulo p^γ is also a kth power in $\mathbb{Q}_p$.

Our final lemma will be used in the proof of Theorem 3 to help produce a linear space of zeros of the form of odd degree.

LEMMA 7. *Suppose that* p *is an odd prime*, k *is a rational integer*, *and* $c_1, \ldots, c_s$ *are* p*-adic integers which are not divisible by* p. *If* $s \geq k+1$, *then there exist distinct numbers* i *and* j *such that* c_i/c_j *is a* k*th power in* $\mathbb{Q}_p$.

Proof. Suppose that $p^\tau \parallel k$. Since p is odd, Lemma 6 shows that it suffices to prove that we can find i and j such that c_i/c_j is a kth power modulo $p^{\tau+1}$. We write $(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times$ for the group of (multiplicative) units modulo $p^{\tau+1}$, write $(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^{\times k}$ for the subgroup of kth powers, and we note the well-known fact that when p is odd, one has $|(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^{\times k}| = \phi(p^{\tau+1})/(\phi(p^{\tau+1}), k)$. Then the number of cosets of the subgroup of kth powers is

$$\begin{aligned}[(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times : (\mathbb{Z}/p^{\tau+1}\mathbb{Z})^{\times k}] &= |(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times| \,/\, |(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^{\times k}| \\ &= \phi(p^{\tau+1}) \Big/ \left(\frac{\phi(p^{\tau+1})}{(\phi(p^{\tau+1}), k)} \right) \\ &= (\phi(p^{\tau+1}), k) \leq k.\end{aligned}$$

Therefore, if we have $k+1$ reduced residues modulo $p^{\tau+1}$, then two must lie in the same coset of $(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^{\times k}$, and so their ratio is a kth power modulo $p^{\tau+1}$. This completes the proof of the lemma. ∎

Now we begin the proof of Theorem 3. Consider the system (1), where we assume that k is odd, and do not make any assumptions about the parity of n. Note that since both equations are homogeneous, it suffices to find a $\mathbb{Q}_p$-rational solution of the system. By a linear change of variables of the form $x_i \mapsto p^\nu x_i$, we may assume that if $a_i \neq 0$ and $p^\alpha \parallel a_i$, then $0 \leq \alpha < k$. We set $V = \{i : a_i = 0\}$, and for $g \in \{0, \ldots, k-1\}$, set $U_g = \{i : p^g \parallel a_i\}$. Note that if $i \in V$, then the equation $a_i y_i^k = 0$ has $y_i = 1$ as a solution.

Next, for a fixed $g \in \{0, \ldots, k-1\}$, suppose that U_g has at least $k+1$ elements. For each $i \in U_g$, write $a_i = p^g c_i$, so that $p \nmid c_i$. Suppose for now that p is odd. Then by Lemma 7, there exist distinct integers i and j and an element $\zeta \in \mathbb{Q}_p$ such that $c_i/c_j = \zeta^k$. Hence the equation

$$a_i y_i^k + a_j y_j^k = 0 \tag{19}$$

can be solved by setting $y_i = -1$ and $y_j = \zeta$. After picking i and j, if there are still at least $k+1$ elements left in U_g, then we may repeat the process until fewer than $k+1$ elements remain. Therefore we can choose from each U_g at least $(|U_g| - k)/2$ disjoint pairs of indices i, j such that there exist y_i and y_j satisfying (19). Note that this statement is still true if U_g contains fewer than $k+1$ elements, for then our bound is at most zero. Therefore, after possibly relabeling variables, we can write the degree k equation in (1) as

$$\begin{aligned} a_1x_1^k + a_2x_2^k + \cdots + a_{2N-1}x_{2N-1}^k + a_{2N}x_{2N}^k \\ + a_{2N+1}x_{2N+1}^k + \cdots + a_{2N+|V|}x_{2N+|V|}^k \\ + a_{2N+|V|+1}x_{2N+|V|+1}^k + \cdots + a_sx_s^k = 0, \end{aligned}$$

where for $i = 1, \ldots, N$ there exist y_{2i-1} and y_{2i} such that

$$a_{2i-1}y_{2i-1}^k + a_{2i}y_{2i}^k = 0, \tag{20}$$

and for $i = 2N+1, \ldots, 2N+|V|$ we have $a_i = 0$.

Next, for $i = 1, \ldots, N$, we set $x_{2i-1} = y_{2i-1}Y_i$ and $x_{2i} = y_{2i}Y_i$. We also set $x_i = Y_{i-N}$ when $i = 2N+1, \ldots, 2N+|V|$, and $x_i = 0$ when $i > 2N+|V|$. Note that the degree k equation will be satisfied for any choice of the Y_i, and that if at least one of the Y_i is nonzero then at least one of the x_i is also nonzero. After this assignment of variables, the degree n equation in (1) becomes

$$d_1Y_1^n + \cdots + d_{N+|V|}Y_{N+|V|}^n = 0 \tag{21}$$

for some $d_1, \ldots, d_{N+|V|}$. By Lemma 5, we can solve this nontrivially provided that $N + |V| > n^2$. However, we have

$$N + |V| \geq |V| + \sum_{g=0}^{k-1} \frac{|U_g| - k}{2} \geq \frac{|V|}{2} + \sum_{g=0}^{k-1} \frac{|U_g| - k}{2} = \frac{1}{2}\,s - \frac{1}{2}\,k^2.$$

Therefore we can always solve the equation (21) nontrivially if we have

$$\frac{1}{2}\,s - \frac{1}{2}\,k^2 > n^2,$$

which occurs whenever

$$s > 2n^2 + k^2,$$

as desired. Therefore, when p and k are both odd, we have the bound $\Gamma_p^*(k,n) \leq 2n^2 + k^2 + 1$.

If we have $p = 2$, then we can even do a little better. We define the sets V and U_g as before, and follow the same line of reasoning as above. However, if we fix g then for any choice of $i, j \in U_g$, the quotient a_i/a_j will be a 2-adic integer which is not divisible by 2. A simple application of Lemma 6 shows that any such number is a kth power in $\mathbb{Q}_2$ for any odd k. Therefore, we are able to choose at least $(|U_g| - 1)/2$ disjoint pairs of elements from U_g

for which we can satisfy the equation (19). We can then proceed exactly as above, except that our bound on $N+|V|$ now becomes

$$N+|V| \geq |V| + \sum_{g=0}^{k-1} \frac{|U_g|-1}{2} \geq \frac{|V|}{2} + \sum_{g=0}^{k-1} \frac{|U_g|-1}{2} = \frac{s}{2} - \frac{k}{2}.$$

Hence we will be able to solve the equation (21) provided that

$$\frac{s}{2} - \frac{k}{2} > n^2,$$

which occurs when $s > 2n^2+k$. This yields the bound $\Gamma_2^*(k,n) \leq 2n^2+k+1$ whenever k is odd. These two bounds together show that if k is odd, then we have the bound $\Gamma^*(k,n) \leq 2n^2+k^2+1$. This completes the proof of Theorem 3. ∎

References

[1] R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. 51 (1945), 749–755.

[2] J. Brüdern and H. Godinho, *On Artin's conjecture*, *I*: *systems of diagonal forms*, Bull. London Math. Soc. 31 (1999), 305–313.

[3] —, —, *On Artin's conjecture*, *II*: *pairs of additive forms*, Proc. London Math. Soc. 84 (2002), 513–538.

[4] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Hamburg Univ. 11 (1935), 73–75.

[5] H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Ann Arbor Publ., Ann Arbor, MI, 1963.

[6] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. London Ser. A 274 (1963), 443–460.

[7] —, —, *Two additive equations*, in: Number Theory, Proc. Sympos. Pure Math. 12, Amer. Math. Soc., Providence, RI, 1969, 74–98.

[8] D. B. Leep and W. M. Schmidt, *Systems of homogeneous equations*, Invent. Math. 71 (1983), 539–549.

[9] S. H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory 6 (1974), 284–290.

[10] T. D. Wooley, *On simultaneous additive equations III*, Mathematika 37 (1990), 85–96.

[11] —, *On simultaneous additive equations I*, Proc. London Math. Soc. 63 (1991), 1–34.

Mathematical Sciences Department
Loyola College
4501 N. Charles Street
Baltimore, MD 21210-2699, U.S.A.
E-mail: mpknapp@loyola.edu

Received on 3.4.2006
and in revised form on 8.8.2006 (5177)