ACTA ARITHMETICA
124.1 (2006)

Local solvability of diagonal equations (again)

by

Christopher Skinner (Ann Arbor, MI)

1. Introduction. In this paper we return to the problem considered in [B] and [S], namely that of giving an upper bound on the integer $\Gamma(d)$, defined for each positive integer d as the least integer such that any diagonal equation

$$a_1x_1^d + \cdots + a_sx_s^d = 0 \tag{1}$$

with coefficients a_i in a p-adic field K (i.e., a finite extension of $\mathbb{Q}_p$) has a solution $0 \neq (x_1, \ldots, x_s) \in K^s$ whenever $s > \Gamma(d)$ (that is, (1) has a *non-trivial* solution in K). Here and throughout, p is taken to be a fixed prime. Of course, implicit in providing an upper bound on $\Gamma(d)$ is a proof of its existence!

Let $d = p^\tau m$ with $p \nmid m$. The main result of [B] asserts that

$$\Gamma(d) < (2\tau+3)^d(d_1^2d)^{d-1}, \qquad d_1 = (d, q-1)$$

with q the size of the residue field of K. In [S] we claimed that $\Gamma(d) \leq d((d+1)^{2\tau+1}-1)$. Unfortunately, there is a simple but serious error in the final step of the proof in [S]: an appeal is made to Hensel's lemma in a situation where it might not apply ([1]). As a consequence, the main result of that paper is only proved ([2]) for $d = p^\tau$. In this paper we present a modification of the arguments in [S], obtaining a bound for all d:

Theorem A. $\Gamma(d) \leq d(p^{3\tau}m^2)^{2\tau+1}$.

In particular, $\Gamma(d) \leq d^{6\tau+4}$.

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

Research supported in part by a fellowship from the David and Lucile Packard Foundation and a grant from the National Science Foundation.

([1]) The author discovered this error shortly after the publication of [S]. The error is cited in [K]. The author's interest in this problem was recently rekindled by a conversation with David Leep.

([2]) In [R] it is shown that the methods of [S] extend to the case $(d, q-1) = 1$ giving the same bound for $\Gamma(d)$ as claimed in [S].

We prove Theorem A by demonstrating that the existence of a non-trivial solution in K to an equation as in (1) can be deduced from the existence of a non-trivial solution in K to a certain system of additive equations of degree m. So we are naturally led to investigate the solvability of systems

$$a_{1j}x_1^m + \cdots + a_{sj}x_s^m = 0, \quad j = 1, \ldots, R, \tag{2}$$

with coefficients a_{ij} in K.

If we let $\Gamma(R,m)$ be the smallest integer such that any system as in (2) has a solution $0 \neq (x_1, \ldots, x_s) \in K^s$ whenever $s > \Gamma(R,m)$, then

THEOREM B ([BG, Theorem 3]). $\Gamma(R,m) \le R^2m^2$.

To be precise, Brüdern and Godinho only state and prove their theorem for the case $K = \mathbb{Q}_p$. However, it is easily checked that all the results used in that proof carry over to any K. For the interested reader as well as for a semblance of completeness, in Section 3 we indicate how to carry over these arguments.

The connection between Theorems A and B is the observation that $\Gamma(d) \le d(p^\tau \Gamma(p^\tau, m))^{2\tau+1}$ (compare Lemmas 1 and 2).

2. Reducing Theorem A to Theorem B. We let $\mathcal{O}$ denote the integer ring of the local field K, fix a uniformizer $\pi \in \mathcal{O}$, and let $k = \mathcal{O}/(\pi)$ be the residue field of K. We denote by $\Gamma_1(d)$ the smallest integer such that any additive equation as in (1) with each $a_i \in \mathcal{O}^\times$ has a non-trivial solution in K. For each positive integer r we denote by $\Phi(d,r)$ the smallest integer such that if $s > \Phi(d,r)$ then any congruence equation

$$a_1x_1^d + \cdots + a_sx_s^d \equiv 0 \pmod{p^r}, \quad a_i \in \mathcal{O}, \tag{3}$$

has a solution $(x_1, \ldots, x_s) \in \mathcal{O}^s$ with some $x_j \in \mathcal{O}^\times$. Of course, these notations only make sense provided the integers in question exist.

LEMMA 1. *Let $d = p^\tau m$ with $p \nmid m$. If $\Phi(d,1)$ exists then so do $\Gamma(d)$, $\Gamma_1(d)$, and $\Phi(d,r)$ (any $r > 0$). In particular,*

(i) $\Phi(d, r+1) \le \Phi(d,1)\Phi(d,r)$.
(ii) $\Gamma_1(d) \le \Phi(d, 2\tau+1)$.
(iii) $\Gamma(d) \le d\Gamma_1(d)$.
(iv) $\Gamma(d) \le d\Phi(d,1)^{2\tau+1}$.

This is just Lemma 1 of [S]. In any event, these reductions are elementary and involve only standard techniques. For example, (ii) is a simple consequence of a version of Hensel's lemma.

LEMMA 2. *Let $d = p^\tau m$ with $p \nmid m$. If $\Gamma(p^\tau, m)$ exists, then so does $\Phi(d,1)$ and*

$$\Phi(d,1) \le p^\tau \Gamma(p^\tau, m).$$

Proof. Assume that $\Gamma(p^\tau, m)$ exists. Suppose $a_1x_1^d + \dots + a_sx_s^d$ to be as in (3). Writing each a_i as $a_i = \pi^{r_i + p^\tau t_i} b_i$ with $0 \le r_i < p^\tau$ and $b_i \in \mathcal{O}^\times$, we see that if $s > p^\tau \Gamma(p^\tau, m)$, then at least $\Gamma(p^\tau, m) + 1$ of the r_i's are the same. Let $N = \Gamma(p^\tau, m) + 1$. Relabeling our variables if necessary, we can assume that $r_1 = \dots = r_N$. It follows that the congruence (3) with $r = 1$ has a solution $(x_1, \dots, x_s) \in \mathcal{O}^s$ with some $x_i \in \mathcal{O}^\times$ if the congruence

$$\pi^{p^\tau t_1} b_1 x_1^d + \dots + \pi^{p^\tau t_N} b_N x_N^d \equiv 0 \pmod p \tag{4}$$

has a solution $(x_1, \dots, x_N) \in \mathcal{O}^N$ with some $x_i \in \mathcal{O}^\times$.

For $\alpha \in k$ we define $u_\alpha \in \mathcal{O}$ as follows. If $\alpha = 0$ then $u_\alpha = 0$, but if $\alpha \ne 0$ then u_α is the unique element in $\mathcal{O}$ such that $u_\alpha^{q-1} = 1$ and $u_\alpha \bmod \pi = \alpha$, where q is the order of k. The existence and uniqueness of u_α is an easy consequence of Hensel's lemma. The association $\alpha \mapsto u_\alpha$ is multiplicative: $u_\alpha u_\beta = u_{\alpha\beta}$. We let $\mathbf{T} = \{u_\alpha : \alpha \in k\}$. Then for any $r \ge 0$ the map $\mathbf{T} \to \mathbf{T}$, $u \mapsto u^{p^r}$, is a bijection. Also, since $\mathbf{T}$ is a complete set of representatives for the residue field k, each $x \in \mathcal{O}$ can be uniquely written as $x = \sum_{n=0}^\infty v_n \pi^n$, $v_n \in \mathbf{T}$.

Writing $b_i = \sum_{n=0}^\infty v_{n,i}\pi^n$, $v_{n,i} \in \mathbf{T}$, we let $h_{n,i} \in \mathbf{T}$ be the unique element such that $h_{n,i}^{p^\tau} = v_{n,i}$. Putting $f = [e/p^\tau]$ where e is defined by $(p) = (\pi^e)$, we then let

$$c_{i,j} = \sum_{n=0}^{f} h_{p^\tau n + j, i} \pi^n, \qquad j = 0, \dots, p^\tau - 1.$$

Since

$$c_{i,j}^{p^\tau} \equiv \sum_{n=0}^{f} h_{p^\tau n + j, i}^{p^\tau} \pi^{p^\tau n} \equiv \sum_{n=0}^{f} v_{p^\tau n + j, i} \pi^{p^\tau n} \pmod p,$$

we have

$$b_i \equiv \sum_{j=0}^{p^\tau - 1} \pi^j c_{i,j}^{p^\tau} \pmod p.$$

From this we see that the congruence (4) has a solution of the desired type if the system of congruence equations

$$(\pi^{t_1} c_{1,j})^{p^\tau} x_1^d + \dots + (\pi^{t_N} c_{N,j})^{p^\tau} x_N^d \equiv 0 \pmod p, \qquad j = 0, \dots, p^\tau - 1, \tag{5}$$

has a solution $(x_1, \dots, x_N) \in \mathcal{O}^N$ with some $x_i \in \mathcal{O}^\times$. But, since $d = p^\tau m$,

$$\Big(\sum_{i=1}^{N} \pi^{t_i} c_{i,j} x_i^m\Big)^{p^\tau} \equiv \sum_{i=1}^{N} (\pi^{t_i} c_{i,j})^{p^\tau} x_i^d \pmod p.$$

Therefore, the system (5) has a solution of the sought-for type if the system

$$\pi^{t_1} c_{1,j} x_1^m + \dots + \pi^{t_N} c_{N,j} x_N^m \equiv 0 \pmod p, \qquad j = 0, \dots, p^\tau - 1, \tag{6}$$

has such a solution. And finally we note that (6) has such a solution if the system of equations

$$\pi^{t_1} c_{1,j} x_1^m + \cdots + \pi^{t_N} c_{N,j} x_N^m = 0, \quad j = 0, \ldots, p^\tau - 1, \tag{7}$$

has a non-trivial solution in K (for by homogeneity such a non-trivial solution $(x_1, \ldots, x_N)$ can always be scaled so that each x_i is in $\mathcal{O}$ and not all the x_i's are divisible by π). Since $N > \Gamma(p^\tau, m)$, (7) has a non-trivial solution in K. ∎

Assuming Theorem B, we obtain Theorem A by combining part (iv) of Lemma 1 with Lemma 2.

3. Remarks on the proof of Theorem B. We begin by noting that if $R = 1$ then the bound in Theorem B follows from part (i) of Lemma 1 together with the observation that since $p \nmid m$, the theorem of Chevalley–Warning together with Hensel's lemma implies that $\Gamma_1(m) \le m$.

Next we indicate how to obtain the same bound on $\Gamma(R, m)$ for a general K as that given in [BG, Theorem 3] for $K = \mathbb{Q}_p$ (when $R \ge 2$ this bound is slightly better than that stated in Theorem B). More precisely, we explain how to modify the statements of the results used in the proof in [BG] so that they apply to the general situation, that is, to the situation where "systems" are systems of equations or congruences with coefficients in $\mathcal{O}$ and "solutions" are solutions with entries in $\mathcal{O}$. We use without explanation some of the terminology and notation from [BG].

First we note that the notions of p-normalized systems of additive equations and p-equivalence have immediate generalizations to π-normalized systems and π-equivalence: one merely replaces p with π in the definition. Similarly, p must be replaced by π in the definition of the level of a variable. Then all the results from [DL] quoted in [BG] continue to hold for π-normalized systems; the proofs are exactly the same. In particular, [BG, Lemma 1] holds with p replaced by π and "integer coefficients" meaning coefficients in $\mathcal{O}$.

Next we note that the result from [LPW] quoted in [BG] also holds for π-normalized systems. In [LPW] this result is deduced by reducing the system modulo p and applying a combinatorial result about matrices over fields. Since this combinatorial result is proved in [LPW] for any field (and so for k) the same argument applies to the reduction modulo π of a π-normalized system. Thus [BG, Lemma 2] holds with p replaced by π.

We also note that the version of Hensel's lemma quoted in [BG, Lemma 3] also holds over K without change, but in the definition of a non-singular solution of a system of congruences such as [BG, (10)], p gets replaced by π (i.e., the condition is $x_{i_1} \cdots x_{i_R} \det(\mathbf{a}_{i_1} \ldots \mathbf{a}_{i_R}) \not\equiv 0 \pmod{\pi}$).

Similarly, [BG, Lemma 4] holds with the p in the congruence [BG, (12)] replaced by π, the $p - 1$ in the definition of δ replaced by $q - 1$ with q the order of the residue field k of K, and with the c_{ij}'s allowed to be in $\mathcal{O}$; this is still the theorem of Chevalley–Warning. It then follows that [BG, Lemma 5] holds with p replaced by π; the same proof works.

Combining the modified versions of [BG, Lemmas 1–5] then implies that $\Gamma(R,m) \le Rm(R(m,q-1)-R+2)$, where q is the order of the residue field of K.

A final remark. Finally, we note that an elementary argument of Leep and Schmidt (cf. [LS, (2.11)]) shows that a system of R equations as in (1) has a non-trivial solution in K provided $s > (\Gamma(d)+1)^R$, so in particular if $s > (d^{6\tau+4}+1)^R$. However, it should be possible to adapt the methods of this paper to prove that there is an integer c such that a non-trivial solution exists if $s > (Rd)^{c\tau}$.

References

[B] B. J. Birch, *Diagonal equations over $\mathfrak{p}$-adic fields*, Acta Arith. 9 (1964), 291–300.

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

[DL] H. Davenport and D. J. Lewis, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A 264 (1969), 557–595.

[K] M. Knapp, *Systems of diagonal equations over p-adic fields*, J. London Math. Soc. (2) 63 (2001), 257–267.

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

[LPW] L. Low, J. Pitman, and A. Wolff, *Simultaneous diagonal congruences*, J. Number Theory 29 (1988), 31–59.

[R] A. Rangachev, *On the solvability of $\mathfrak{p}$-adic diagonal equations*, preprint, 2004.

[S] C. Skinner, *Solvability of $\mathfrak{p}$-adic diagonal equations*, Acta Arith. 75 (1996), 251–258.

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1043, U.S.A.
E-mail: cskinner@umich.edu

Received on 18.7.2005 (5036)