ACTA ARITHMETICA
132.4 (2008)

Simultaneous diagonal equations over $\mathfrak{p}$-adic fields

by

D. Brink (Brasília), H. Godinho (Brasília) and
P. H. A. Rodrigues (Goiânia)

Let K be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$. Let $\mathcal{O}$ be the ring of integers in K and let $\mathfrak{p}$ be $\mathcal{O}$'s unique maximal ideal. We say that K is a $\mathfrak{p}$-*adic field*.

Consider R simultaneous diagonal equations

$$(*)\qquad \begin{aligned} a_{11}X_1^k + \cdots + a_{1N}X_N^k &= 0,\\ \vdots \qquad\qquad \vdots \quad &\quad \vdots\\ a_{R1}X_1^k + \cdots + a_{RN}X_N^k &= 0 \end{aligned}$$

with coefficients a_{ij} in $\mathcal{O}$. Write the degree as $k = p^\tau m$ with $p \nmid m$. A solution $\mathbf{x} = (x_1, \ldots, x_N) \in K^N$ is called *non-trivial* if at least one x_j is non-zero. It is a special case of a conjecture of Emil Artin that $(*)$ has a non-trivial solution whenever $N > Rk^2$. This conjecture has been verified by Davenport and Lewis for a single diagonal equation over $\mathbb{Q}_p$ and for a pair of equations of odd degree over $\mathbb{Q}_p$ (see [3] and [4]), but the general case remains open.

The main results of the present paper are the following two theorems.

Theorem 1. *The system $(*)$ has a non-trivial solution if the number of variables N exceeds $(Rk)^{2\tau+5}$.*

Theorem 2. *Let n be the degree of the field extension $K/\mathbb{Q}_p$. Then $(*)$ has a non-trivial solution if N exceeds $4nR^2k^2$.*

Theorem 1 has the virtue of being independent of K and can be compared with Skinner [11] where the bound $N > k^{6\tau+4}$ is given for a single diagonal equation. Theorem 2 is a natural generalisation of Knapp [7, Theorem 1]

2000 *Mathematics Subject Classification*: 11D72, 11D79.
Key words and phrases: diagonal forms, Artin's conjecture, $\mathfrak{p}$-adic fields.
The first two authors were partially supported by a grant from CNPq-Brasil.

and improves Dodson [6, Theorem 1] and Knapp [7, Theorem 3]. See also Skinner [11] for other references.

Define the integer $\Gamma(R,k)$ as minimal with the property that any system $(*)$ with $N > \Gamma(R,k)$ has a non-trivial solution over K. Then Theorems 1 and 2 can be restated as $\Gamma(R,k) \le (Rk)^{2\tau+5}$ and $\Gamma(R,k) \le 4nR^2k^2$, respectively. The idea of the proof of the theorems is to first solve $(*)$ in the finite residue ring $\mathcal{O}/\mathfrak{p}^\gamma$ (for a suitable exponent γ), and then lift this solution to K via a version of Hensel's lemma.

A solution $\mathbf{x} \in \mathcal{O}^N$ is called *primitive* if at least one coordinate x_j is a unit in $\mathcal{O}$. Define the integer $\Phi(R,k,\nu)$ as minimal with the property that any system $(*)$ with $N > \Phi(R,k,\nu)$ has a primitive solution modulo $\mathfrak{p}^\nu$.

The Chevalley–Warning theorem (see [2, Lemma 4]) states that any system of homogeneous polynomials over a finite field has a non-trivial zero if the number of variables exceeds the sum of the polynomials' degrees. In the special case of systems of diagonal equations, the Chevalley–Warning theorem gives

$$\Phi(R,k,1) \le Rk. \tag{1}$$

For general moduli $a, b \ge 1$ one has the relation

$$\Phi(R,k,a+b) + 1 \le (\Phi(R,k,a)+1)\cdot(\Phi(R,k,b)+1). \tag{2}$$

This is shown using a well-known "contraction" argument (see examples in [4] and [11]). The idea is to construct a primitive solution modulo $\mathfrak{p}^{a+b}$ in $N = (\Phi(R,k,a)+1)\cdot(\Phi(R,k,b)+1)$ variables as follows: First divide the left hand side of $(*)$ into $\Phi(R,k,a)+1$ subsystems of diagonal forms, each in $\Phi(R,k,b)+1$ variables, and solve each system primitively modulo $\mathfrak{p}^b$. Then multiply each of these solutions by a new variable to form a system of diagonal forms in $\Phi(R,k,a)+1$ variables. Since every coefficient is a multiple of $\mathfrak{p}^b$, to solve this new system primitively modulo $\mathfrak{p}^{a+b}$ is *basically* to solve it modulo $\mathfrak{p}^a$. This results in a primitive solution modulo $\mathfrak{p}^{a+b}$ to $(*)$ which proves (2).

Let $A = (a_{ij})$ be the coefficient matrix of $(*)$. A solution $\mathbf{x} \in \mathcal{O}^N$ is called *non-singular* if the matrix $(a_{ij}x_j^k)$ has rank R modulo $\mathfrak{p}$, or equivalently, if the columns of A corresponding to the indices j with $x_j \not\equiv 0 \pmod{\mathfrak{p}}$ have rank R modulo $\mathfrak{p}$.

The following strong version of Hensel's lemma is a natural generalisation of [5, Lemma 9], from p-adic to $\mathfrak{p}$-adic fields. The definition of γ here is somewhat better than the value $2e\tau + 1$ often found in the literature (although Alemu [1] has a result for one equation similar to the lemma below).

LEMMA 1. *Let e be the ramification index of K over $\mathbb{Q}_p$ and define*

$$\gamma := \begin{cases} 1 & \text{for } \tau = 0, \\ e(\tau+1) & \text{for } \tau > 0 \text{ and } p \neq 2, \\ e(\tau+2) & \text{for } \tau > 0 \text{ and } p = 2. \end{cases}$$

The system $(*)$ then has a non-trivial solution in K if it has a non-singular solution modulo $\mathfrak{p}^\gamma$.

Proof. We first show that a unit $u \in \mathcal{O}^*$ is a kth power if $u \equiv \xi^k \pmod{\mathfrak{p}^\gamma}$ for some $\xi \in \mathcal{O}^*$. This is the standard Hensel's lemma for $\tau = 0$, so we may assume $\tau > 0$. Then multiplication $x \mapsto k \cdot x$ maps $\mathfrak{p}^e$ onto $k \cdot \mathfrak{p}^e = \mathfrak{p}^{e\tau+e} = \mathfrak{p}^\gamma$ for $p \neq 2$, and $\mathfrak{p}^{2e}$ onto $k \cdot \mathfrak{p}^{2e} = \mathfrak{p}^\gamma$ for $p = 2$. For any $n > e/(p-1)$, the $\mathfrak{p}$-adic exponential function and the $\mathfrak{p}$-adic logarithm are inverse isomorphisms between the additive group $\mathfrak{p}^n$ and the multiplicative group $1+\mathfrak{p}^n$ ([9, Kapitel II, Satz 5.5]). It follows that exponentiation $x \mapsto x^k$ maps $1 + \mathfrak{p}^e$ (for $p \neq 2$) and $1 + \mathfrak{p}^{2e}$ (for $p = 2$) onto $1 + \mathfrak{p}^\gamma$. The diagram shows the situation for $p \neq 2$:

$$\begin{array}{ccc} 1+\mathfrak{p}^e & \xrightarrow{x \mapsto x^k} & 1+\mathfrak{p}^\gamma \\ \downarrow{\scriptstyle \log} & & \uparrow{\scriptstyle \exp} \\ \mathfrak{p}^e & \xrightarrow{x \mapsto k \cdot x} & \mathfrak{p}^\gamma \end{array}$$

Therefore, the elements of the set $\xi^k \cdot (1+\mathfrak{p}^\gamma) = \xi^k + \mathfrak{p}^\gamma$, to which u belongs, are all kth powers.

Now let $\mathbf{x} = (x_1, \ldots, x_N)$ be a non-singular solution to $(*)$ modulo $\mathfrak{p}^\gamma$. We may assume $x_1, \ldots, x_R \not\equiv 0 \pmod{\mathfrak{p}}$ and that the first R columns of A have rank R modulo $\mathfrak{p}$, i.e. form a non-singular matrix modulo $\mathfrak{p}$. Row operations on A will not change the solution set, so we may assume

$$A = \begin{pmatrix} a_{11} & & 0 & a_{1,R+1} & \cdots & a_{1N} \\ & \ddots & & \vdots & & \vdots \\ 0 & & a_{RR} & a_{R,R+1} & \cdots & a_{RN} \end{pmatrix}$$

with $a_{11}, \ldots, a_{RR} \not\equiv 0 \pmod{\mathfrak{p}}$. For each $i = 1, \ldots, R$ we have $x_i^k \equiv u_i \pmod{\mathfrak{p}^\gamma}$ with $u_i = -(a_{i,R+1}x_{R+1}^k + \cdots + a_{iN}x_N^k)/a_{ii}$. By the above, the equation $X^k = u_i$ has a solution x_i' because it has the solution x_i modulo $\mathfrak{p}^\gamma$. We conclude that $(x_1', \ldots, x_R', x_{R+1}, \ldots, x_N)$ solves $(*)$. ∎

The notion of a *p-normalised* system of diagonal equations over $\mathbb{Q}_p$ was introduced in [5]. It is shown there that any system of the form $(*)$ over $\mathbb{Q}_p$ has a non-trivial solution provided that any p-normalised system has a non-trivial solution. All of this is easily generalised to *π-normalised* systems with $\mathfrak{p}$-adic coefficients (see [7] for details).

Let $\mu(d)$ be the maximal number of columns of the coefficient matrix A which, when considered modulo $\mathfrak{p}$, lie in a d-dimensional subspace of $\mathbb{F}_q^N$. The key property of π-normalised systems is the inequality

$$\mu(d) \le N - (R-d)N/Rk \quad \text{for } d = 0, \dots, R-1. \tag{3}$$

This is [5, Lemma 11] combined with [2, eq. (9)]. An equivalent statement of this inequality is that any matrix having $R-d$ rows which are linear combinations of the rows of A, independent modulo $\mathfrak{p}$, contains at least $(R-d)N/Rk$ columns which are non-zero modulo $\mathfrak{p}$.

The following slight strengthening of [2, Lemma 2] essentially gives one extra non-singular submatrix.

LEMMA 2. *Suppose* $(*)$ *is* π*-normalised and has more than* $k(tR-1)$ *variables, where* t *is arbitrary. Then the coefficient matrix* A *contains* t *disjoint* $R \times R$ *submatrices which are non-singular modulo* $\mathfrak{p}$.

Proof. For every $d = 0, \dots, R-1$, the assumption $N > k(tR-1)$ combined with (3) implies $\mu(d) \le N - (R-d)t$ since $\mu(d)$ is integral. Now the conclusion follows by a combinatorial result of Aigner (see [8, Lemma 1] or the comment before [2, Lemma 2]). ∎

Next, we extend and improve [2, Lemma 5] using the same idea of proof.

LEMMA 3. *Suppose* $(*)$ *is* π*-normalised and has more than* $Rk\cdot\Phi(R,k,\nu) - k(R-1)^2$ *variables, where* ν *is arbitrary. Then* $(*)$ *has a non-singular solution modulo* $\mathfrak{p}^\nu$.

Proof. Suppose first that $(*)$ has $N = k(tR-1)+1$ variables for some t to be defined later. Then, by Lemma 2, A has t disjoint $R \times R$ submatrices which are non-singular modulo $\mathfrak{p}$. Discard all variables not belonging to one of these t submatrices. Then we have tR variables left. In each of all but one of the t submatrices, replace all R variables by one new variable. Then we have a new system with $t-1+R$ variables. This system, by definition, has a primitive solution modulo $\mathfrak{p}^\nu$ if $t-1+R > \Phi(R,k,\nu)$, hence if $t = \Phi(R,k,\nu) - R + 2$. Not all the new variables of this solution can be zero modulo $\mathfrak{p}$ since the columns corresponding to the old variables form a non-singular submatrix modulo $\mathfrak{p}$ and so are linearly independent modulo $\mathfrak{p}$. Therefore, "inflating" the new variables again gives a non-singular solution to our original system $(*)$ in $N = Rk\cdot\Phi(R,k,\nu) - k(R-1)^2 + 1$ variables, and the lemma is proved. ∎

Recall that $\Gamma(R,k)$ is the minimal integer such that any system $(*)$ with $N > \Gamma(R,k)$ has a non-trivial solution. From Lemmas 1 and 3 it follows that

$$\Gamma(R,k) \le Rk\cdot\Phi(R,k,\gamma) - k(R-1)^2 \tag{4}$$

since any bound on $\Gamma(R,k)$ may be proved under the assumption that $(*)$ is π-normalised. For degree k not divisible by p, (4) and (1) give

$$\Gamma(R,k) \le (Rk)^2 - k(R-1)^2, \tag{5}$$

which extends [2, Theorem 3].

Now, Theorem 2 follows from (4) and the following lemma.

Lemma 4. *With γ defined as in Lemma 1, we have*

$$\Phi(R,k,\gamma) \le \begin{cases} p(p-1)^{-1}nRk & \text{for } p>2, \\ 4nRk & \text{for } p=2. \end{cases}$$

Proof. To bound $\Phi(R,k,\gamma)$, we must find a primitive solution modulo $\mathfrak{p}^\gamma$ to $(*)$. The additive group of the finite residue ring $\mathcal{O}/\mathfrak{p}^\gamma$ is equal to the direct sum of n cyclic subgroups of order $p^{\gamma/e}$,

$$\mathcal{O}/\mathfrak{p}^\gamma = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n.$$

This can be seen for example by counting the number of elements of any given order in both groups and noting that these numbers are the same (see also [1] for a different proof and a more general statement). Writing each coefficient a_{ij} of $(*)$ as a $\mathbb{Z}$-linear combination of the λ_i's, we see that it suffices to solve nR congruences

$$c_{i1}X_1^k + \cdots + c_{iN}X_N^k \equiv 0 \pmod{p^{\gamma/e}}, \qquad i=1,\ldots,nR, \tag{6}$$

with coefficients $c_{ij} \in \mathbb{Z}$. We shall only look for solutions $\mathbf{x} \in \mathbb{T}^N$ where $\mathbb{T} = \{x \in \mathbb{Q}_p \mid x^p = x\}$ is the set of *Teichmüller representatives.* Since $\{x^k \mid x \in \mathbb{T}\} = \{x^{(k,p-1)} \mid x \in \mathbb{T}\}$, we may in (6) replace the exponent k by $(k,p-1)$. Now, by a theorem of Schanuel [10], the system (6) has a non-trivial solution $\mathbf{x} \in \mathbb{T}^N$ if $N > nR(k,p-1)(p^{\gamma/e}-1)(p-1)^{-1}$. Recalling $k = p^\tau m$, we see that $(k,p-1)$ divides m and conclude that $\Phi(R,k,\gamma)$ is bounded by $nR(k,p-1)p^{\tau+1}(p-1)^{-1} \le p(p-1)^{-1}nRk$ for $p \ne 2$, and by $4nRk$ for $p=2$. ∎

The next two lemmas and the final proof of Theorem 1 are much inspired by the ideas presented in Skinner [11].

Lemma 5. *Any $a \in \mathcal{O}$ can be written as*

$$a \equiv c_0^{p^\tau} + \pi c_1^{p^\tau} + \pi^2 c_2^{p^\tau} + \cdots + \pi^{p^\tau-1} c_{p^\tau-1}^{p^\tau} \pmod{p}$$

with $c_j \in \mathcal{O}$ and π being a prime element of $\mathcal{O}$.

Proof. If $\mathcal{R} \subset \mathcal{O}$ is a set of representatives for $\mathcal{O}/\mathfrak{p}$, then so is $\{r^{p^\tau} \mid r \in \mathcal{R}\}$, because the map $x \mapsto x^{p^\tau}$ is a bijection $\mathbb{F}_q \to \mathbb{F}_q$. Hence, with suitable $r_n \in \mathcal{R}$, we can write

$$a=\sum_{n=0}^{\infty} r_n^{p^\tau}\pi^n=\sum_{j=0}^{p^\tau-1}\pi^j\sum_{i=0}^{\infty} r_{j+ip^\tau}^{p^\tau}\pi^{ip^\tau}\equiv\sum_{j=0}^{p^\tau-1}\pi^j\Big(\sum_{i=0}^{\infty} r_{j+ip^\tau}\pi^i\Big)^{p^\tau} \pmod p,$$

which proves the lemma. ∎

LEMMA 6. $\Phi(R,k,e)\le\Phi(Rp^\tau,m,e)$.

Proof. We have to find a primitive solution $\mathbf{x}\in\mathcal{O}^N$ to the R congruences

$$a_{i1}X_1^k+\cdots+a_{iN}X_N^k\equiv 0 \pmod p,\qquad i=1,\ldots,R.$$

Write each polynomial in this system as a sum of p^τ polynomials using the above lemma on each coefficient $a=a_{ij}$. Thus it suffices to find a primitive solution to Rp^τ congruences

$$c_{i1}^{p^\tau}X_1^k+\cdots+c_{iN}^{p^\tau}X_N^k\equiv 0 \pmod p,\qquad i=1,\ldots,Rp^\tau.$$

Since

$$c_{i1}^{p^\tau}X_1^k+\cdots+c_{iN}^{p^\tau}X_N^k\equiv (c_{i1}X_1^m+\cdots+c_{iN}X_N^m)^{p^\tau} \pmod p,$$

it suffices to find a primitive solution to the Rp^τ congruences

$$c_{i1}X_1^m+\cdots+c_{iN}X_N^m\equiv 0 \pmod p,\qquad i=1,\ldots,Rp^\tau.$$

Such a solution exists by definition for $N>\Phi(Rp^\tau,m,e)$. ∎

We can finally prove Theorem 1. Clearly, $\Phi(Rp^\tau,m,e)$ is bounded by $\Gamma(Rp^\tau,m)$, which is in turn bounded by $(Rk)^2-m(Rp^\tau-1)^2$ by (5) since m is not divisible by p. For $\tau=0$ we already have the bound (5) which is superior to the one given in Theorem 1. So assume $\tau>0$. Then Lemma 6 implies

$$\Phi(R,k,e)<(Rk)^2. \tag{7}$$

From (4), (2), and (7) it now follows that

$$\Gamma(R,k)\le Rk\cdot\Phi(R,k,\gamma)\le Rk\cdot(\Phi(R,k,e)+1)^{\gamma/e}\le(Rk)^{2\gamma/e+1}\le(Rk)^{2\tau+5}.$$

This concludes the proof of Theorem 1.

References

[1] Y. Alemu, *On zeros of diagonal forms over $\mathfrak{p}$-adic fields*, Acta Arith. 48 (1987), 261–273.

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

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

[4] —, —, *Two additive equations*, in: Number Theory, W. J. LeVeque and E. G. Strauss (eds.), Proc. Sympos. Pure Math. 12, Amer. Math. Soc., Providence, RI, 1969, 74–98.

[5] H. Davenport and D. J. Lewis, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A 264 (1969), 557–595.
[6] M. M. Dodson, *Some estimates for diagonal equations over $\mathfrak{p}$-adic fields*, Acta Arith. 40 (1982), 117–124.
[7] M. P. Knapp, *Systems of diagonal equations over $\mathfrak{p}$-adic fields*, J. London Math. Soc. (2) 63 (2001), 257–267.
[8] L. Low, J. Pitman and A. Wolff, *Simultaneous diagonal congruences*, J. Number Theory 29 (1988), 31–59.
[9] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.
[10] S. H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory 6 (1974), 284–290.
[11] C. Skinner, *Local solvability of diagonal equations* (*again*), Acta Arith. 124 (2006), 73–77.

Departamento de Matemática
Universidade de Brasília
Brasília, DF 70910-900, Brazil
E-mail: brink@math.ku.dk
hemar@unb.br

Instituto de Matemática e Estatística
Universidade Federal de Goiás
Goiânia, GO 74001-970, Brazil
E-mail: paulo@mat.ufg.br

Received on 17.10.2007 (5549)