МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2005
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2005
Proceedings of the Thirty Fourth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 6–9, 2005

SOME SUFFICIENT CONDITIONS FOR THE SOLVABILITY OF $\mathfrak{p}$-ADIC POLYNOMIAL EQUATIONS*

Vesselin At. Dimitrov, Antoni Kr. Rangachev

This paper presents some new conditions which ensure that certain special polynomials in a large number of variables have a non-trivial zero over a $\mathfrak{p}$-adic field. In particular, it is shown that if $\mathbb{K}$ is an extension of $\mathbb{Q}_p$ of finite degree n, then every diagonal equation $a_1x_1^k + \cdots + a_sx_s^k = 0$ over $\mathbb{K}$ in at least nk^5 variables is solvable non-trivially.

1. Introduction. Let $\mathbb{Q}_p$ be the field of p-adic numbers, $\mathbb{K}$ an extension of $\mathbb{Q}_p$ of degree $n = [\mathbb{K} : \mathbb{Q}_p] < \infty$, and $\mathfrak{O}$ the ring of integers of $\mathbb{K}$. The present note is addressed to the solvability of equations of the form $f(x_1, \ldots, x_s) = 0$ in elements $x_1, \ldots, x_s \in \mathbb{K}$, not all zero, for certain polynomials $f \in \mathfrak{O}[x_1, \ldots, x_s]$ with a zero free term and in a large number s of variables.

Our main result is the following:

Theorem 1. *Let $F \in \mathfrak{O}[x_1, \ldots, x_s]$ be a polynomial with zero free term, and let $k, t, w \in \mathbb{N}$ be positive integers such that:*

(i) $s \geq 1 + nkw\big(p^{2t+2} - 1\big)$;

(ii) *The degree of F in each variable x_j is at most k;*

(iii) *No monomial of F consists of more than w variables;*

(iv) *If for each $i = 1, \ldots, s$, if $x_1^{l_{11}} \cdots x_i^{l_{i1}} \cdots x_s^{l_{s1}}, \ldots, x_1^{l_{1v}} \cdots x_i^{l_{iv}} \cdots x_s^{l_{sv}}$ are the monomials of F which are divisible by x_i (in other words, which appear with $l_{i1}, \ldots, l_{iv} \geq 1$), then $\operatorname{ord}_p l_{i1}, \ldots, \operatorname{ord}_p l_{iv}$ are pairwise different, and $\max_{j=1}^{v} \operatorname{ord}_p l_{ij} = t$. Here, $\operatorname{ord}_p l$ is the exact exponent of p dividing $l \in \mathbb{N}$;*

(v) *For every monomial N of F, either the coefficient of N is a $\mathfrak{p}$-adic unit, or there exist a variable $x_j \,|\, N$ which does not appear in any other monomial.*

Then, the equation $F(x_1, \ldots, x_s) = 0$ has a solution $(x_1, \ldots, x_s) \in \mathbb{K}^s$, different from the trivial solution $(0, \ldots, 0)$.

The special case when $F(x_1, \ldots, x_s) = a_1x_1^k + \cdots + a_sx_s^k$ is a diagonal form has been long the subject of intensive research. Let $\Gamma(\mathbb{K}, k)$ denote the smallest integer s for which any equation of the form

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k = 0, \quad a_1, \ldots, a_s \in \mathfrak{O} \setminus \{0\}$$

*2000 Mathematics Subject Classification: 11D72, 11P05, 11E76, 11S05

has a solution $(x_1, \dots, x_s) \in \mathbb{K}^s$ different from the trivial solution $(0, \dots, 0)$. In 1964 Davenport and Lewis [3] showed that $\Gamma(\mathbb{Q}_p, k) \le k^2+1$. In the case of arbitrary extensions $\mathbb{K}$, however, the following conjecture remains wide open.

Conjecture 2. *There exists a polynomial $P \in \mathbb{R}[x]$, independent of the prime p and of the field $\mathbb{K}$, such that*

$$\Gamma(\mathbb{K}, k) < P(k)$$

for all $\mathbb{K}/\mathbb{Q}_p$ and $k \in \mathbb{N}$.

In fact, the only field-independent bound in the literature is the one recorded by Birch [2] in 1964. Birch's bound implies that Conjecture 2 holds if the hypothesis that P is a polynomial is weakened to $P(x) = x^{3x-2}$.

Dodson [4] was the first to establish the following weaker version of Conjecture 2:

There exists a polynomial $P \in \mathbb{R}[x, y]$, independent of p, such that $\Gamma(\mathbb{K}, k) < P(n, k)$. More precisely,

$$\Gamma(\mathbb{K}, k) < 16n^2k^2(\log k)^2. \tag{1}$$

As an immediate corollary of Theorem 1 we establish an estimate of the form $\Gamma(\mathbb{K}, k) < P(n, k)$ which is linear in n (while Dodson's bound (1) is quadratic in n).

Theorem 3. *Let $k = p^t m$ with $(p, m) = 1$. Then,*

$$\Gamma(\mathbb{K}, k) \le 1 + nk\big(p^{2t+2} - 1\big).$$

In particular, we have the polynomial bound $\Gamma(\mathbb{K}, k) < nk^5$.

Finally, we deduce the following corollary of Theorem 1.

Corollary 4. *If d is the total degree of F, then Condition (i) in Theorem 1 may be replaced by the simpler condition $s \ge nd^6$.*

2. Preliminaries. In this section we set up the machinery that will enable us to establish our bounds. The main idea is to use Hensel's lemma to reduce the equations to systems of modular congruences, and then to restrict the variables of these congruences to the set $\{0, 1\}$ and apply a theorem of Baker and Schmidt [1].

Throughout the paper, $\mathbb{K}$ is a fixed field extension of $\mathbb{Q}_p$ with $[\mathbb{K} : \mathbb{Q}_p] = n < \infty$; $\mathfrak{O}$ is the ring of integers of $\mathbb{K}$; $\mathfrak{p} = (\pi)$ is the unique maximal ideal of the (local) field $\mathbb{K}$; e is the ramification index of $\mathbb{K}$; f is the residue class degree of $\mathbb{K}$ (so that $ef = n$ and $|\mathfrak{O}/\mathfrak{p}| = p^f$).

Definition 2.1. *For our purposes, a polynomial $F \in \mathfrak{O}[x_1, \dots, x_s]$ which is non-constant in each x_i and has a zero free term will be called* admissible *if it has the following properties:* 1. *If $x_1^{l_{11}} \cdots x_i^{l_{i1}} \cdots x_s^{l_{s1}}, \dots, x_1^{l_{1v}} \cdots x_i^{l_{iv}} \cdots x_s^{l_{sv}}$ are the monomials of F which are divisible by x_i (in other words, which appear with $l_{i1}, \dots, l_{iv} \ge 1$), then $\operatorname{ord}_p l_{i1}, \dots, \operatorname{ord}_p l_{iv}$ are pairwise different. (Here, $\operatorname{ord}_p l$ is the exact power of p dividing $l \in \mathbb{N}$); and* 2. *If N is any monomial of F whose coefficient is divisible by π, then N does not divide the product of the other monomials of F.*

In other words, an admissible polynomial is a polynomial that satisfies conditions (iv) and (v) of Theorem 1.

Let $\mathcal{P}(k, t, w)$ be the set of all *admissible* polynomials $F \in \mathfrak{O}[x_1, \dots, x_s]$ satisfying conditions (ii), (iii), (iv) and (v) from Theorem 1, and let $\mathcal{P}_1(k, t, w) \subset \mathcal{P}(k, t, w)$ be the subset consisting of those polynomials in $F_1 \in \mathcal{P}(k, t, w)$ all of whose non-zero coefficients

are indivisible by π. Define $G(k,t,w) = G(\mathbb{K};k,t,w)$ to be the minimal integer s such that every polynomial in $\mathcal{P}(k,t,w)$ on s variables has a non-trivial zero (i.e. a zero different from $(0,\dots,0)$). Finally, define $H(k,t,w,r) = H(\mathbb{K};k,t,w,r)$ to be the minimal integer s such that, for every polynomial $F \in \mathcal{P}(k,t,w)$ on s variables, the congruence

$$F(\varepsilon_1,\dots,\varepsilon_s) \equiv 0 \pmod{\pi^r}.$$

has a solution $(\varepsilon_1,\dots,\varepsilon_s) \in \{0,1\}^s$ different from $(0,\dots,0)$.

It is not difficult to see (for instance, by a classical theorem of Olson [5]) that $H(k,t,w,r)$ is always finite. The following lemma shows that $G(k,t,w)$ is finite, and reduces the problem of bounding $G(k,t,w)$ to that of bounding $H(k,t,w,r)$.

Lemma 2.2. *For all $k,t,w \in \mathbb{N}$, we have*

$$G(k,t,w) \le 1 + k\big(H(k,t,w,2te+1) - 1\big). \tag{2}$$

Proof. Let $h = H(k,t,w,2te+1)$. Consider an arbitrary polynomial $F \in \mathcal{P}(k,t,w)$ of $s > k(h-1)$ variables. Label by $M_1, M_2, \dots$ the monomials of F in such a way that the coefficients of $M_1,\dots,M_u$ are divisible by π, while the coefficients of $M_{u+1}, M_{u+2},\dots$ are $\mathfrak{p}$-adic units. By condition (v), $M_i \not| \prod_{j\ne i} M_j$ for each $i = 1,2,\dots,u$. By enumeration the variables $x_1,x_2,\dots,x_s$, we may assume that $x_i | M_j$ for $i = 1,\dots,u$, if and only if $j = i$. For $1 \le i \le u$, let $k_i > 0$ be the exact exponent of x_i in M_i, and let $\alpha_i = \pi^{\gamma_i}\beta_i$ be the coefficient of M_i, where β_i is a $\mathfrak{p}$-adic unit. Write $\gamma_i = q_i k_i + r_i$ with $q_i, r_i \in \mathbb{Z}$ and $0 \le r_i < k_i$. Since $k_i \le k$ for each i, we have that $0 \le r_1, r_2, \dots, r_u < k$. By the pigeonhole principle, at least $\lceil u/k \rceil$ of the numbers $r_1,\dots,r_u$ are equal; without loss of generality, assume that $r_1 = \cdots = r_\ell = \delta$, where $\ell = \lceil u/k \rceil$. Let F^* be the polynomial $\pi^{-\delta}F(\pi^{-q_1}x_1,\dots,\pi^{-q_\ell}x_\ell,0,\dots,0,x_{u+1},\dots,x_s)$. It is sufficient to show that F^* has a non-trivial zero.

Since, for $i \le u$, x_i does not appear in monomials other than M_i, and since the coefficients of $M_{u+1}, M_{u+2},\dots$ are $\mathfrak{p}$-adic units, it follows easily that $F^* \in \mathcal{P}_1(k,t,w)$ is a polynomial whose non-zero coefficients are all indivisible by π. By the definition of h and the fact that F^* is a polynomial on $s' := \lceil u/k \rceil + s - u \ge \lceil s/k \rceil > h-1$ variables, the congruence

$$F^*(\varepsilon_1,\dots,\varepsilon_{s'}) \equiv 0 \pmod{\pi^{2te+1}} \tag{3}$$

has a solution $(\varepsilon_1,\dots,\varepsilon_{s'}) \in \{0,1\}^{s'}$ with $\varepsilon_{j_0} = 1$ for at least one j_0.

We will show that the polynomial $f(x) := F^*(\varepsilon_1,\dots,\varepsilon_{j_0-1},x,\varepsilon_{j_0+1},\dots,\varepsilon_{s'})$ has a $\mathfrak{p}$-adic root $\alpha \equiv 1 \pmod{\pi}$, which will complete the proof of the lemma. Write $f(x) = \sum_i a_i x^{t_i}$ with $0 < t_1 < t_2 < \cdots$. By condition (iv), the powers of p in $t_1, t_2, \dots$ are pairwise different, and $\max_i \operatorname{ord}_p t_i = t$. Hence, the coefficients a_i are all indivisible by π (because those of F^* are all $\mathfrak{p}$-adic units), so the powers of π in $a_1k_1, a_2k_2, \dots$ are pairwise different, implying in particular that

$$\operatorname{ord}_\pi\{f'(1)\} = \operatorname{ord}_\pi\Big\{\sum_i a_i k_i\Big\} = \min_i\{\operatorname{ord}_\pi a_i k_i\} = e\min_i\{\operatorname{ord}_p k_i\} \le et.$$

On the other hand, (3) implies that $\operatorname{ord}_\pi\{f(1)\} = \operatorname{ord}_\pi\{f(\varepsilon_{j_0})\} \ge 2et+1$. By Hensel's lemma, there exists a unique $\alpha \in \mathbb{K}, \alpha \equiv 1 \pmod{\pi^{2te+1}}$ such that $f(\alpha) = 0$. The proof of the lemma is completed. $\square$

We will also need the following result of Baker and Schmidt [1] concerning the solv-

ability of modular polynomial equations with variables restricted to the set $\{0,1\}$. A short and elementary proof, due to Zhi-Wei Sun, can be found in [8].

Lemma 2.3 (Baker-Schmidt [1]). *Let $e_i \in \mathbb{N}$ and $f_i \in \mathbb{Z}[x_1,\dots,x_k]$, $1 \le i \le m$. If p is a prime and $k > \sum_{i=1}^{m}(p^{e_i}-1)\deg f_i$, then*

$$\sum_{\substack{I\subset[k]\\ p^{e_i}\mid f_i([1\in I],\dots,[k\in I])\\ \text{for all } i\in[m]}} (-1)^{|I|} \equiv 0 \pmod p.$$

Here, $[j \in I]$ is 1 or 0, according to whether $j \in I$ or $j \notin I$, and $[m] := \{1,\dots,m\}$. In particular, if each of the polynomials f_i has zero free term, then the system

$$f_i(x_1,\dots,x_k) \equiv 0 \pmod{p^{e_i}}, \quad 1 \le i \le m$$

has a solution $(x_1,\dots,x_k) \in \{0,1\}^k$, different from the trivial solution $(0,\dots,0)$.

With $e_1 = \cdots = e_m = \ell$, we have the following important corollary:

Corollary 2.4. *Let p be a prime and R be a finite ring whose additive group is isomorphic to $\mathbb{Z}_{p^\ell}^h$ (the direct sum of h copies of $\mathbb{Z}_{p^\ell}$). Let $f_1,\dots,f_m \in R[x_1,\dots,x_s]$ be polynomials with zero free terms, each of which has degree at most d. If $s \ge 1 + mhd(p^\ell - 1)$, then the system $f_1 = \cdots = f_m = 0$ is solvable non-trivially in the set $\{0,1\}^s$.*

Proofs of the main results. In this section we present proofs of Theorem 1, Theorem 3 and Corollary 4.

Proof of Theorem 1. In view of Lemma 2.2, it is sufficient to show that $H\big(k,t,w,(2te+1)\big) \le 1 + nw\big(p^{2t+2}-1\big)$. This follows by taking $r = 2te+1$ in the following lemma; recall that $f = n/e$ is the residue class degree of $\mathbb{K}$.

Lemma 3.1. *For all $k,t,w,r \in \mathbb{N}$, we have the inequality*

$$H(k,w,t,r) \le 1 + nw\big(p^{\lceil r/e\rceil}-1\big).$$

Proof. In what follows, L is the maximal unramified subfield of $\mathbb{K}$ and $\mathfrak{o}$ is the ring of integers of L. Let $F \in \mathcal{P}_1(k,w,t)$ be an arbitrary polynomial, and let $\overline{F}$ be the multilinear polynomial obtained from F modulo the relations $x_i^2 = x_i$. By condition (iii), we have $\deg\overline{F} \le w$. We shall seek a non-trivial solution to the congruence $\overline{F}(x_1,\dots,x_s) \equiv 0 \pmod{\pi^r}$ in the set $\{0,1\}^s$.

Because $\{1,\pi,\pi^2,\dots,\pi^{e-1}\}$ is an $\mathfrak{o}$-basis for $\mathfrak{O}$, we have

$$\overline{F}(x_1,\dots,x_s) \equiv \sum_{j=0}^{e-1}\pi^j F_j(x_1,\dots,x_s) \pmod{\pi^r}$$

for some polynomials $F_0,\dots,F_{e-1} \in \mathfrak{o}[x_1,\dots,x_s]$. Note that $\deg F_i \le \deg\overline{F} \le w$ for each $i \in \{0,1,\dots,e-1\}$.

Let $\ell = \lceil r/e\rceil$. Then, $\ell e \ge r$, so each solution $(y_1,\dots,y_s)$ of the system $F_j(y_1,\dots,y_s) \equiv 0 \pmod{p^\ell}, 0 \le i < e$, satisfies $F(y_1,\dots,y_s) \equiv 0 \pmod{\pi^r}$. Therefore, it will be sufficient to show that every such system is solvable non-trivially. Since the additive group of the ring $\mathfrak{o}/(p^\ell)$ is isomorphic to $\mathbb{Z}_{p^\ell}^f$, Corollary 2.4 guarantees the existence of a non-trivial solution to $F_0 \equiv \cdots \equiv F_{e-1} \equiv 0 \pmod{p^\ell}$ provided that

$s \geq 1 + fwe\big(p^{\ell} - 1\big) = 1 + nw\big(p^{\lceil r/e \rceil} - 1\big)$. This completes the proof of the lemma. $\square$

Proof of Theorem 3. Let $t = \mathrm{ord}_p k$. Then, each diagonal form $F(x_1, \ldots, x_s) = a_1 x_1^k + \cdots + a_s x_s^k$ belongs to the set $\mathcal{P}(k, t, 1)$ of *admissible* polynomials with $w = 1$. Therefore, $\Gamma(\mathbb{K}, k) \leq G(k, t, 1)$ which, by Theorem 1, gives the bound

$$\Gamma(\mathbb{K}, k) \leq 1 + nk\big(p^{2t+2} - 1\big).$$

If $t \geq 1$, then the right-hand side is less than $nkp^{2+2t} \leq nkp^{4t} \leq nk^5$. If $t = 0$, then $(k, p) = 1$. In this case, Lemma 2.2 gives that $\Gamma(\mathbb{K}, k) \leq 1 + k\big(H(k, 0, 1, 1) - 1\big) \leq k^2 + 1 < nk^4$ because, by the Chevalley-Warning theorem, we have the inequality $H(k, 0, 1, 1) \leq k + 1$. Therefore, the polynomial bound $\Gamma(\mathbb{K}, k) < nk^5$ holds in all cases. $\square$

Proof of Corollary 4. Theorem 1, together with the obvious fact that $w, k \leq d$, gives the bound

$$G(k, t, w) < nkwp^{2+2t} \leq nd^2 p^{2+2t},$$

due to $kw \leq d^2$. Now, if $t \geq 1$, from $d \geq k \geq p^t$ it follows immediately that $G(k, t, w) < nd^2 p^{4t} \leq nd^6$. In the case $t = 0$, the assertion follows from

$$G(k, 0, w) \leq 1 + k\big(H(k, 0, w, 1) - 1\big) \leq 1 + kd \leq 1 + d^2 < nd^6,$$

where the second inequality is an immediate corollary of the Chevalley-Warning theorem. This proves the assertion in all cases. $\square$

4. Acknowledgements. This project is inspired by the work conducted by the second author during the 2004 Research Science Institute (RSI) at the Massachusetts Institute of Technology under the supervision of Mr. Mohsen Bahramgiri. We express our deepest gratitude to Mr. Bahramgiri for his ongoing support and inspiring discussions. We are also greatly indebted to: Prof. Hartley Rogers of MIT for providing such a mentor; Prof. Christopher Skinner of the Michigan University for suggesting this topic; Dr. Michael Knapp of the Rochester University for his numerous helpful comments; Dr. Jenny Sendova of the Bulgarian Academy of Sciences for her constant encouragement. We, being both RSI alumni, are extremely grateful to the Center for Excellence in Education and to the High School Institute of Mathematics and Informatics for making this research possible.

REFERENCES

[1] R. Baker, W. M. Schmidt. Diophantine problems in variables restricted to the values 0 and 1. *Journal of Number Theory*, **12** (1980), 460–486.

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

[3] H. Davenport, D. J. Lewis. Homogeneous additive equations. *Proc. Royal Soc. London Ser.*, **274** (1964), 443–460.

[4] M. M. Dodson. Some estimates for diagonal equations over $\mathfrak{p}$-adic fields. *Acta Arithmetica*, **40** (1982), 117–124.

[5] J. E. Olson. A combinatorial problem in finite abelian groups I. *Journal of Number Theory*, **1** (1969), 8–10.

[6] A. Rangachev. Solvability of $\mathfrak{p}$-adic diagonal equations. 2004 Research Science Institute Compendium, 71–75.

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

[8] Z. W. Sun. A unified theory of zero-sum problems, subset sums and covers of $\mathbb{Z}$. Preprint, Nanjing University, March 1, 2003. arXiv:math.NT/0305369.

Vesselin Dimitrov
National High School
of Mathematics and Science
52, Bigla Str.
1164 Sofia, Bulgaria
e-mail: avding@hotmail.com

Antoni Rangachev
Sofia Mathematics High School
61, Iskar Str.
1000 Sofia, Bulgaria
e-mail: anthony_rangachev@yahoo.co.uk

НЯКОИ ДОСТАТЪЧНИ УСЛОВИЯ ЗА РАЗРЕШИМОСТТА НА $\mathfrak{p}$-АДИЧНИ ПОЛИНОМНИ УРАВНЕНИЯ

Веселин Ат. Димитров, Антони Кр. Рангачев

В настоящата статия са представени някои условия, които гарантират нетривиалната разрешимост на някои полиномни уравнения над $\mathfrak{p}$-адични полета. В частност е доказано, че ако $\mathbb{K}$ е разширение на $\mathbb{Q}_p$ с $[\mathbb{K} : \mathbb{Q}_p] = n < \infty$, то всяко диагонално уравнение $a_1x_1^k + \cdots + a_sx_s^k = 0$ на поне nk^4 променливи има нетривиално решение над $\mathbb{K}$.