Journal de Théorie des Nombres
de Bordeaux **19** (2007), 205–219

On p-adic zeros of systems of diagonal forms restricted by a congruence condition

par Hemar GODINHO et Paulo H. A. RODRIGUES

Résumé. Cet article étudie l'existence de solutions non triviales en entiers p-adiques de systèmes d'équations pour des formes additives. En supposant que l'équation $ax^k + by^k + cz^k \equiv d \pmod p$ ait une solution telle que $xyz \not\equiv 0 \pmod p$, nous montrons qu'un système quelconque de formes additives de degré k et d'au moins $2 \cdot 3^{R-1} \cdot k + 1$ variables possède toujours des solutions p-adiques non-triviales, si $p \nmid k$. L'hypothèse ci-dessus pour l'existence de solutions non-triviales de l'équation est vérifiée si, par exemple, $p > k^4$.

Abstract. This paper is concerned with non-trivial solvability in p-adic integers of systems of additive forms. Assuming that the congruence equation $ax^k + by^k + cz^k \equiv d \pmod p$ has a solution with $xyz \not\equiv 0 \pmod p$ we have proved that any system of R additive forms of degree k with at least $2 \cdot 3^{R-1} \cdot k + 1$ variables, has always non-trivial p-adic solutions, provided $p \nmid k$. The assumption of the solubility of the above congruence equation is guaranteed, for example, if $p > k^4$.

1. Introduction

A classical problem concerning systems of diagonal forms over p-adic fields involves finding an explicit relation between the degree of the forms and the number of variables that will ensure non-trivial p-adic solubility. The guideline given by Artin's conjecture is that p-adic solubility is guaranteed once the number of variables exceeds the sum of the squares of the degrees of each one of the forms of the system. Although we still do not know if this conjecture is true or false for systems of additive forms of the same degree (see [4]), an extensive theory on the subject has been developed over the last decades (see for example [1],[2],[5]). Recently the authors have proved that for systems of three diagonal forms of odd degree k in N variables, p-adic solubility for all $p \nmid k$ is ensured, once $N > 14k + 1$ and

Manuscrit reçu le 21 octobre 2005.
The first author was partially supported by a grant of CNPq-Brasil, and the second author was partially supported by a grant of CAPES-PICDT.

a *mild* condition (at least in our view) is fulfilled. The condition is that the congruence equation $ax^k + by^k + cz^k \equiv d \pmod p$, with a, b, c nonzero modulo p, has a solution with $xyz \not\equiv 0 \pmod p$ (see [3]). In this paper we generalize this result proving, for any degree k and any number R of forms, that

Theorem 1.1. *Let p be a prime and k an integer such that $p \nmid k$. Let us suppose that the congruence equation $ax^k + by^k + cz^k \equiv d \,(mod\, p)$, with a, b, c nonzero modulo p, has a solution with $xyz \not\equiv 0 \,(mod\, p)$, for all d. Then, for any $R > 1$ the system*

$$F_i(x_1, \ldots, x_N) = a_{i1}x_1^k + \cdots + a_{iN}x_N^k = 0, \quad (i = 1, \ldots, R), \tag{1}$$

with coefficients $a_{ij} \in \mathbb{Z}$, has a non-trivial p-adic zero, provided $N \geq 2 \cdot 3^{R-1} \cdot k + 1$.

Corollary 1.2. *Let k be an integer and p be a prime such that $p > k^4$. Then, for any $R > 1$, the system (1) has a non-trivial p-adic zero, provided*

$$N \geq 2 \cdot 3^{R-1} \cdot k + 1.$$

Proof. This is a consequence of Meir [6] (Lemma 8), where it is proved that if $p > k^4$ then the congruence $ax^k + by^k + cz^k \equiv d \pmod p$ has a solution with $xyz \not\equiv 0 \pmod p$. □

It is important to mention that the hypothesis $p > k^4$ can be improved in many cases (and it is generally believed that it can be improved in all cases), for example, for $k = 5$, it is enough to consider $p > 101$ (see [3] for details).

We believe it is interesting to compare these results with the previous results of Atkinson, Brüdern and Cook [1] and I.D. Meir [6] in which they proved that:

Theorem 1.3 (Atkinson, Brüdern and Cook)**.** *Let R, k, N be positive integers, with $k > 1$ and $N \geq 2Rk + 1$. Then the system (1) has a p-adic zero, provided $p > k^{2R+2}$.*

Theorem 1.4 (Meir)**.** *Let k, N be positive integers, with $k > 1$ and $N \geq 4k + 1$. Then a system of two diagonal forms of degree k has a p-adic zero, provided $p > 3k^4$.*

Theorem 1.3 gives a better bound for N (comparing to Theorem 1.1), but the given bound for the values of p grows exponentially from R.

In this paper we are going to make use of the p-adic normalization introduced by Davenport and Lewis (see [2] for details). They associated a function ϑ to the coefficients of the forms F_j's

$$\vartheta(F_1, \ldots, F_R) = \prod_J \det(a_{ij}), \quad (1 \leq i \leq R \text{ and } j \in J)$$

where J runs over all subsets of $\{1, 2, \ldots, N\}$ with R elements. By an argument involving the compactness of the set of p-adic integers, it is proved in [2] that we can assume the additional hypothesis $\vartheta(F_1, \ldots, F_R) \neq 0$ in the proof of Theorem 1.1, with no loss of generality.

We are going to say that a system of R additive forms $F_1^* = \ldots = F_R^* = 0$ is p-equivalent to the system (1) if it is obtained from (1) by a combination of the operations (i) and (ii) below:

(i) $F_j^* = \sum_{i=1}^{R} \lambda_{ij} F_i, \quad \lambda_{ij} \in \mathbb{Q}, \quad$ and $\det(\lambda_{ij}) \neq 0$, or,
(ii) $F_j^*(x_1, \ldots, x_N) = F_j(p^{r_1} x_1, \ldots, p^{r_N} x_N), \quad r_i \in \mathbb{Z}$.

Since we are assuming that $\vartheta(F_1, \ldots, F_R) \neq 0$, and the p-adic fields have characteristic 0, we can choose in each p-equivalence class a system for which the power of p dividing $\vartheta(F_1, \ldots, F_R)$ is minimal. This system will be called a *p-normalized system*, and it is easy to see that if a p-normalized system has p-adic solutions, then any system in its class will also have p-adic solutions.

An important feature of the p-adic normalization is described in the next lemma (this is Lemma 11 of [2])

Lemma 1.5. *A p-normalized system of R additive forms of degree k can be written (after renumbering the variables) as*

$$F_i = f_i(x_1, \ldots, x_n) + p g_i(x_{n+1}, \ldots, x_N) = 0 \tag{2}$$

for $i = 1, \ldots, R$, where $n \geq N/k$ and each of the variables $x_1, \ldots, x_n$ occurs in at least one of the forms $f_1, \ldots, f_R$ with a coefficient not divisible by p. Moreover, if we form any S linear combinations of the forms f_j's, which are independent modulo p, and denote by $q_S = q_S(f_1, \cdots, f_R)$ the number of variables that occur in at least one of these combinations with a coefficient not divisible by p, then

$$q_S \geq SN/Rk \quad (S = 1, \ldots, R) \quad \textit{(in particular } q_R = n\textit{)}.$$

From this point on we assume that the system $F_1 = F_2 = \cdots = F_R = 0$ (see (1)) is p-normalized, with the properties stated on Lemma 1.5, which give rise to the congruence system (see (2))

$$f_i(x_1, \ldots, x_n) = a_{i1} x_1^k + \cdots + a_{in} x_{in}^k \equiv 0 \pmod{p} \quad (i = 1, \ldots, R). \tag{3}$$

Remark 1.6. Let $A = (a_{ij})$ be the $R \times n$ matrix of the coefficients of the congruence system (3). The definitions of q_S given by Lemma 1.5 can be translated to the matrix A in the following way: *after any finite sequence of row operations on A, any row of A will still have at least q_1 nonzero entries modulo p, any two rows will still have at least q_2 nonzero entries (i.e., 2×1 column vectors) modulo p, and so forth.* With that in mind, we are going to use, from now on, $q_s(A)$ instead of $q_S(f_1, \cdots, f_R)$.

Following the notation given in [1], let $\mu_d(A)$ $(1 \leq d \leq R)$ denote the maximum number of columns of A that are in the same d-dimensional linear subspace of $\mathbb{F}_p^R$. It is easy to see that

$$\mu_d(A) + q_{R-d}(A) = n, \quad (d = 1, \ldots, R-1). \tag{4}$$

The relation (4) is completely independent of the p-normalization, and in the same way, for any $R \times n$ matrix, we have

$$q_1(A) \leq q_2(A) \leq \ldots \leq q_R(A) \quad \text{and} \quad \mu_1(A) \leq \mu_2(A) \leq \ldots \leq \mu_R(A). \tag{5}$$

For the p-normalized case, and, as before, assuming A to be the $R \times n$ matrix of the coefficients of the congruence system (3), we cannot have $\mu_d(A) = n$ for any $d < R$, since it would imply that $q_{R-d}(A) = 0$ by (4), which is impossible according to Lemma 1.5. Hence, for p-normalized systems we have

$$1 \leq \mu_1(A) \leq \cdots \leq \mu_{R-1}(A) < \mu_R(A) = n. \tag{6}$$

Definition 1.7. A solution $\xi = (\xi_1, \cdots, \xi_n)$ for the congruences (3) will be called a rank ν solution if the matrix $(a_{ij}\xi_j)$ has rank ν modulo p.

The next lemma is a version of Hensel's lemma, and it was proved by Davenport and Lewis (a particular case of lemma 9 in [2]).

Lemma 1.8. *If $p \nmid k$ and the congruences (3) have a rank R solution modulo p, then the corresponding system (2) has non-trivial p-adic solutions.*

Based on Lemmas 1.5, 1.8, and the observations above, the proof of Theorem 1.1 is a consequence of the proof of the following result (taking $\alpha_1 = \ldots = \alpha_R = 0$).

Theorem 1.9. *Let p be a prime, k be an integer such that $p \nmid k$, and suppose that the congruence*

$$ax^k + by^k + cz^k \equiv d \,(mod p), \tag{7}$$

with a, b, c different from zero modulo p, has a solution with $xyz \not\equiv 0 \,(mod p)$, for any d. For any $\alpha_1, \ldots, \alpha_R \in \mathbb{Z}$, consider the system

$$\begin{cases} f_1 = a_{11}x_1^k + \cdots + a_{1n}x_n^k \equiv \alpha_1 \,(mod p) \\ \quad \vdots \\ f_R = a_{R1}x_1^k + \cdots + a_{Rn}x_n^k \equiv \alpha_R \,(mod p). \end{cases} \tag{8}$$

If for $s = 1, \ldots, R$ we have

$$q_s(A) > \frac{s}{R} \cdot 2 \cdot 3^{R-1} \quad \textit{(in particular } n = q_R \geq 2 \cdot 3^{R-1} + 1\textit{)}, \tag{9}$$

then the system (8) has a solution of rank R modulo p.

The proof of this theorem will be done by induction on the number R of forms f_i's, and will follow from a series of lemmas presented in the next section.

2. Proof of Theorem 1.9

We start this section with some simple remarks. Let $\ell = gcd(p-1, k)$. It is easy to see that the equation $x^\ell \equiv a \,(\mathrm{mod}\, p)$ has a solution if, and only if, $x^k \equiv a \,(\mathrm{mod}\, p)$ has a solution. This implies that the set of ℓ-th powers and the set of k-th powers in $\mathbb{F}_p$ are equal. Since we are assuming k to be any natural number, there is no loss of generality if we replace k by ℓ in the congruences (3). Hence, from now on, we will always assume that $p \equiv 1 \,(\mathrm{mod}\, k)$, whenever considering the congruence system (8).

Let $\mathbb{F}_p^*$ be the group of all non-zero elements of $\mathbb{F}_p$, and let K be the subgroup of $\mathbb{F}_p^*$ of all k-th powers. Since we are assuming $p \equiv 1 \pmod{k}$, there exists a $\delta \in (\mathbb{F}_p^* - K)$, such that

$$\mathbb{F}_p^* = K \cup \delta K \cup \delta^2 K \cup \cdots \cup \delta^{k-1} K \quad \text{(a disjoint union)}. \tag{10}$$

Let us denote by $\mathbb{S}$ the following set of representatives of the k cosets above

$$\mathbb{S} = \{1, \delta, \delta^2, \ldots, \delta^{k-1}\}. \tag{11}$$

It follows from these considerations that any $\alpha \in \mathbb{F}_p^*$ can be written in the form

$$\alpha = \delta^i a^k \tag{12}$$

for some $a \in \mathbb{F}_p^*$ and some $\delta^i \in \mathbb{S}$.

The next lemma gives the initial step of inductive argument used for the proof of Theorem 1.9.

Proposition 2.1. *The statement of Theorem 1.9 holds for $R = 2$.*

Proof. Let A be the $2 \times n$ matrix of coefficients of (8). It follows from (9) and (4) that

$$n = q_2 \geq 7, \qquad q_1(A) \geq 4 \qquad \text{and} \quad \mu_1(A) + q_1(A) = n.$$

Hence the system (8) (with $R = 2$) can be rewritten as

$$\begin{cases} a_1 x_1^k + \cdots + a_{\mu_1} x_{\mu_1}^k + b_1 y_1^k + \ldots + b_{q_1} y_{q_1}^k \equiv \alpha_1 (\mathrm{mod}\, p) \\ c_1 y_1^k + \cdots + c_{q_1} y_{q_1}^k \equiv \alpha_2 (\mathrm{mod}\, p) \end{cases}, \tag{13}$$

where $\mu_1 = \mu_1(A)$ and $q_1 = q_1(A)$.

Let $(\xi_1, \ldots, \xi_{q_1})$ be a solution for $c_1 y_1^k + \cdots + c_{q_1} y_{q_1}^k \equiv \alpha_2 \,(\mathrm{mod}\, p)$ with all entries nonzero modulo p, which is a consequence of the hypothesis (7) (one can take, for example, $y_4 = \cdots = y_{q_1} = 1$ and solve $c_1 y_1^k + c_2 y_2^k + c_3 y_3^k \equiv \alpha_2 - (c_4 + \cdots + c_{q_1}) \,(\mathrm{mod}\, p)$). Now write $b_1 \xi_1^k + \cdots + b_{q_1} \xi_{q_1}^k \equiv \tau \,(\mathrm{mod}\, p)$ and consider the congruence

$$a_1 x_1^k + \cdots + a_{\mu_1} x_{\mu_1}^k \equiv \alpha_1 - \tau \,(\mathrm{mod}\, p). \tag{14}$$

If $\mu_1 \geq 3$ then, by hypothesis, we can find a nontrivial solution $(\varepsilon_1, \ldots, \varepsilon_{\mu_1})$ for (14), and $(\varepsilon_1, \ldots, \varepsilon_{\mu_1}, \xi_1, \ldots, \xi_{q_1})$ is a rank two solution for (13). Let us

suppose that $\mu_1 = 2$. If $\tau \equiv \alpha_1 \,(\mathrm{mod}\, p)$ then $(0, 0, \xi_1, \ldots, \xi_{q_1})$ is a solution of rank 2 for (13) since this solution has at least three entries nonzero modulo p and $\mu_1 = 2$. Now suppose that $\alpha_1 - \tau \not\equiv 0 \,(\mathrm{mod}\, p)$. Let $(\varepsilon_1, \varepsilon_2, \varepsilon)$ be a solution for the congruence

$$a_1 x_1^k + a_2 x_2^k + (\tau - \alpha_1) z^k \equiv 0 \,(\mathrm{mod}\, p) \tag{15}$$

with $\varepsilon_1 \varepsilon_2 \varepsilon \not\equiv 0 \,(\mathrm{mod}\, p)$. Then, $(\varepsilon_1 \varepsilon^{-1}, \varepsilon_2 \varepsilon^{-1})$ is a solution for (14) (now $\mu_1 = 2$) and then $(\varepsilon_1 \varepsilon^{-1}, \varepsilon_2 \varepsilon^{-1}, \xi_1, \ldots, \xi_{q_1})$ is a rank 2 solution for (13).

Finally suppose that $\mu_1 = 1$ and $q_1 \geq 6$. After the change of variables $c_j y_j^k \longleftrightarrow \delta^r (c_j^* y_j)^k$ based upon (12), we can consider the coefficients $c_1, \ldots, c_{q_1} \in \mathbb{S}$ (see (11)), that is, they form a subset of the representatives of the equivalence classes modulo K (see (10)).

We are going to conclude this proof by considering the following two cases:

Case (i): Suppose that there are two equal coefficients among $c_1, \ldots, c_{q_1}$, say $c_1 = c_2$. Since $\mu_1 = 1$ we must have $b_1 \not\equiv b_2 \,(\mathrm{mod}\, p)$. Now, since $c_1 = c_2$, the congruences

$$c_1 y_1^k + c_3 y_3^k + c_4 y_4^k \equiv 0 \,(\mathrm{mod}\, p) \quad \text{and} \quad c_2 y_2^k + c_3 y_3^k + c_4 y_4^k \equiv 0 \,(\mathrm{mod}\, p)$$

have a common solution, say (ξ_1, ξ_3, ξ_4) with $\xi_1 \xi_3 \xi_4 \not\equiv 0 \,(\mathrm{mod}\, p)$. Let $b_1 \xi_1^k + b_3 \xi_3^k + b_4 \xi_4^k \equiv \omega \,(\mathrm{mod}\, p)$ and $b_2 \xi_1^k + b_3 \xi_3^k + b_4 \xi_4^k \equiv \gamma \,(\mathrm{mod}\, p)$ we must have that $\omega \not\equiv \gamma \,(\mathrm{mod}\, p)$, otherwise we would have $b_1 \equiv b_2 \,(\mathrm{mod}\, p)$, a contradiction. Thus, with no loss of generality, we may assume that $\omega \not\equiv 0 \,(\mathrm{mod}\, p)$. Next let $(\xi_2, \xi_5, \ldots, \xi_{q_1})$ be a solution with all entries nonzero modulo p for the congruence $c_2 y_2^k + c_5 y_5^k + \cdots + c_{q_1} y_{q_1}^k \equiv \alpha_2 \,(\mathrm{mod}\, p)$ (as done in the beginning of this proof). Now let $b_2 \xi_2^k + b_5 \xi_5^k + \cdots + b_{q_1} \xi_{q_1}^k \equiv \tau \,(\mathrm{mod}\, p)$. If $\tau \equiv \alpha_1 \,(\mathrm{mod}\, p)$ then $(0, 0, \xi_2, 0, 0, \xi_5, \ldots, \xi_{q_1})$ is a rank 2 solution for (13), since $\mu_1 = 1$. Otherwise we have the congruence

$$a_1 x_1^k + \omega T^k \equiv \alpha_1 - \tau \,(\mathrm{mod}\, p)$$

which has a solution $(\varepsilon_1, \varepsilon)$ (as done in the case $\mu_1 = 2$ of this proof). Hence,

$$(\varepsilon_1, \xi_1 \varepsilon, \xi_2, \xi_3 \varepsilon, \xi_4 \varepsilon, \xi_5, \ldots, \xi q_1)$$

is a rank 2 solution modulo p for (13) (by the construction of ω).

Case (ii): Suppose that $c_1, \ldots, c_{q_1} \in \mathbb{S}$ and they are all distincts. Since there are at least 6 of them, we may assume, after a renumbering if necessary, that $c_1 \not\equiv -c_2 \,(\mathrm{mod}\, p)$ (which also means that they do not belong to the same class modulo K (see (10))).

Rewriting the system (13) as

$$\begin{cases} a_1 x_1^k + b_1 y_1^k + \ldots + b_{q_1 - 1} y_{q_1 - 1}^k & \equiv \alpha_1 (\mathrm{mod}\, p) \\ c_1 y_1^k + \cdots + c_{q_1 - 1} y_{q_1 - 1}^k + c_{q_1} y_{q_1}^k & \equiv \alpha_2 (\mathrm{mod}\, p) \end{cases}, \tag{16}$$

with all b_i's and c_j's different from zero modulo p, with a possible change in the values of α_1 and α_2.

Follows from the hypothesis (7) (as done before in this proof) that we can find solutions $(\varepsilon_1, \xi_1, \xi_2)$ and $(\xi_3, \ldots, \xi_{q_1-1})$ for the congruences $a_1x_1^k + b_1y_1^k + b_2y_2^k \equiv 0 \pmod p$ and $b_3y_3^k + \cdots + b_{q_1-1}y_{q_1-1}^k \equiv \alpha_1 \pmod p$, with all entries nonzero modulo p. Now let $c_3\xi_3^k + \cdots + c_{q_1-1}\xi_{q_1-1}^k \equiv \tau \pmod p$. If $\tau \equiv \alpha_2 \pmod p$ then $(0, 0, 0, \xi_3, \ldots, \xi_{q_1-1}, 0)$ is a rank 2 solution for (16). Otherwise, let $c_1\xi_1^k + c_2\xi_2^k \equiv \omega \pmod p$ and observe that if $\omega \equiv 0 \pmod p$ we would have c_1 and $-c_2$ in the same class modulo K, a contradiction. Hence $\omega \not\equiv 0 \pmod p$. Since $\alpha_2 - \tau$ and ω are nonzero modulo p, we can find a solution (ρ, ξ_{q_1}), with all entries nonzero modulo p, for the congruence

$$\omega T^k + c_{q_1}y_{q_1}^k \equiv \alpha_2 - \tau \pmod p.$$

Then $(\varepsilon_1\rho, \xi_1\rho, \xi_2\rho, \xi_3, \ldots, \xi_{q_1})$ is a rank 2 solution for (16), by the construction of ω. □

Induction Hypothesis: Let us now assume, as the induction hypothesis, that, under the hypothesis (7) and for any $R' < R$, any congruence system $G_i \equiv \beta_i \pmod p$ of R' forms of degree k in at least $2 \cdot 3^{R'-1} + 1$ variables, and such that its coefficient matrix $\mathfrak{C}$ has $q_s(\mathfrak{C}) > (s/R') \cdot 2 \cdot 3^{R'-1}$ for $i = 1, \ldots, R'$, has always a rank R' solution modulo p.

One important comment before continuing the proof is that, if the matrix of coefficients A, of order $R \times n$, is written in the form

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$$

where A_1 has order $d \times n$ and A_2 has order $(R-d) \times n$, then $q_j(A_1) \geq q_j(A)$ for $j = 1, ..., d$ and $q_j(A_2) \geq q_j(A)$ for $j = 1, ..., R-d$. In particular, if the matrix A has the form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix} \tag{17}$$

where A_{22} has order $(R-d) \times (n-t)$ then we still have $q_j(A_{22}) \geq q_j(A)$ for $j = 1, ..., R-d$.

Lemma 2.2. *Let us suppose that there is d, $1 \leq d \leq R-1$, such that $\mu_d(A) > 2 \cdot 3^{d-1}$. Then (8) has a rank R solution, modulo p.*

Proof. Let d, $1 \leq d \leq R-1$, be the smallest number such that $\mu_d(A) > 2 \cdot 3^{d-1}$. After re-enumerating the variables (if necessary) and after performing row operations on the coefficients of the matrix A, we can rewrite the system (8) as

$$(18)\qquad \begin{cases} g_1(x_1,\dots,x_{\mu_d}) + & h_1(y_1,\dots,y_{q_{R-d}}) & \equiv \alpha_1 & (\mathrm{mod}\, p) \\ & \vdots & & \\ g_d(x_1,\dots,x_{\mu_d}) + & h_d(y_1,\dots,y_{q_{R-d}}) & \equiv \alpha_d & (\mathrm{mod}\, p) \\ & h_{d+1}(y_1,\dots,y_{q_{R-d}}) & \equiv \alpha_{d+1} & (\mathrm{mod}\, p) \\ & \vdots & & \\ & h_R(y_1,\dots,y_{q_{R-d}}) & \equiv \alpha_R & (\mathrm{mod}\, p) \end{cases},$$

where $g_1,\dots,g_d,h_1,\dots,h_R$ are diagonal forms of degree k, $\mu_d = \mu_d(A)$ and $q_{R-d} = q_{R-d}(A)$.

Now consider the subsystem of (18) given by

$$(19)\qquad h_i(y_1,\dots,y_{q_{R-d}}) \equiv \alpha_i \,(\mathrm{mod}\, p) \quad (i = d+1,\dots,R)$$

and let B be the coefficient matrix of the system (19), of order $(R-d)\times q_{R-d}$. From the above comments, we have, for $s = 1,\dots,R-d$,

$$q_s(B) \geq q_s(A) > \frac{s}{R} 2\cdot 3^{R-1} > \frac{s}{R-d} 2\cdot 3^{R-d-1}.$$

Hence, by the induction hypothesis, (19) has a rank $R-d$ solution $(\xi_1,\dots,\xi_{q_{R-d}})$ modulo p.

Next we can consider the following system

$$(20)\qquad g_j(x_1,\dots,x_{\mu_d}) \equiv \alpha_j - h_j(\xi_1,\dots,\xi_{q_{R-d}}) \,(\mathrm{mod}\, p) \quad (j = 1,\dots,d).$$

Let C be the coefficient matrix of this system of order $d\times\mu_d$. For $s = 1,\dots,d-1$, we have

$$\mu_{d-s}(C) + q_s(C) = \mu_d(A) > 2\cdot 3^{d-1}$$

and, by the minimality of d and since C is a sub-matrix of A, we have

$$\mu_s(C) \leq \mu_s(A) \leq 2\cdot 3^{s-1},$$

hence

$$\begin{aligned} q_s(C) &> 2\cdot 3^{d-1} - \mu_{d-s}(C) \\ &\geq 2\cdot 3^{d-1} - 2\cdot 3^{d-s-1} \\ &> \frac{s}{d} 2\cdot 3^{d-1}. \end{aligned}$$

Next we can apply the induction hypothesis for the system (20) to obtain a rank d solution $(\varepsilon_1,\dots,\varepsilon_{\mu_d})$ modulo p.

Let $(\omega_1,\cdots,\omega_n)$ be a solution for the system (18), given by $\omega_i = \varepsilon_i$ for $i = 1,\cdots,\mu_d$, and $\omega_{\mu_d+j} = \xi_j$ for $j = 1,\cdots,q_{R-d}$.

Now let $A = (a_{ij})$ be the coefficient matrix of (18). Together with the solution $(\omega_1,\cdots,\omega_n)$, we can have the matrix $M = (a_{ij}\omega_j)$ as in Definition 1.7. Next observe that M has order $R\times n$ and the form

$$M = \begin{pmatrix} M_1 & M_2 \\ 0 & M_3 \end{pmatrix}$$

where M_1 has order $d \times \mu_d$ and rank d, and M_3 has order $(R-d) \times q_{R-d}$ and rank $R-d$ (by the way, we obtained the above solutions $(\varepsilon_1, \ldots, \varepsilon_{\mu_d})$ and $(\xi_1, \ldots, \xi_{q_{R-d}})$). From a simple linear algebra argument, it follows that M has rank R, proving that $(\omega_1, \cdots, \omega_n)$ is a rank R solution for (18), as desired. □

Let us rewrite the system (8) of theorem 1.9 (with a possible change in the values of α_j's) modulo p as

$$(21) \qquad \begin{cases} g_1(x_1, \ldots, x_\mu) + & b_{11}y_1^k + \cdots + b_{1q}y_q^k & \equiv \alpha_1 \\ & \vdots & \vdots \\ g_{R-1}(x_1, \ldots, x_\mu) + & b_{(R-1)1}y_1^k + \cdots + b_{(R-1)q}y_q^k & \equiv \alpha_{R-1} \\ & b_{R1}y_1^k + \cdots + b_{Rq}y_q^k & \equiv \alpha_R \end{cases},$$

where $\mu = \mu_{R-1}(A)$, $q = q_1(A)$, and the coefficients $b_{R1}, \ldots, b_{Rq}$ are all nonzero modulo p. From this point on we are going to focus our attention on this system, observing that, from (4) and (9) follows that $n = q + \mu > 2 \cdot 3^{R-1}$, and since we can assume that $\mu \leq 2 \cdot 3^{R-2}$ (see Lemma (2.2)), then we have

$$(22) \qquad q > 4 \cdot 3^{R-2} > 2\mu.$$

Definition 2.3. Consider the sub-forms of the forms of the system (21)

$$\begin{gathered} b_{1r}y_r^k + b_{1s}y_s^k + b_{1t}y_t^k \\ \vdots \\ b_{Rr}y_r^k + b_{Rs}y_s^k + b_{Rt}y_t^k \end{gathered}$$

such that its $R \times 3$ matrix (b_{ij}) has rank 3 modulo p. From the hypothesis (see (7)) we can find a solution (ξ_r, ξ_s, ξ_t) for the congruence equation $b_{Rr}y_r^k + b_{Rs}y_s^k + b_{Rt}y_t^k \equiv 0 \pmod p$. The substitution of (ξ_r, ξ_s, ξ_t) by $(T\xi_r, T\xi_s, T\xi_t)$, where T is a new variable, in the remaining sub-forms will give

$$\begin{gathered} b_{1r}(T\xi_r)^k + b_{1s}(T\xi_s)^k + b_{1t}(T\xi_t)^k \equiv \gamma_1 T^k \pmod p \\ \vdots \qquad\qquad \vdots \\ b_{(R-1)r}(T\xi_r)^k + b_{(R-1)s}(T\xi_s)^k + b_{(R-1)t}(T\xi_t)^k \equiv \gamma_{R-1}T^k \pmod p \end{gathered}.$$

This substitution of the variables y_r, y_s, y_t by a new variable T will be called a rank 3 contraction to a new variable T. It is important to observe that we cannot have $\gamma_1 \equiv \cdots \equiv \gamma_{R-1} \equiv 0 \pmod p$ since the coefficient matrix (b_{ij}) has rank 3.

In order to set the stage for the proof of the remaining four lemmas, we will need the following remark.

Remark 2.4. It follows from the definition of $\mu_d(A)$ that any set of $\mu+1$ columns corresponding to the variables y_i's in (21) must have rank R. Since $q > 2\mu$ (see (22)), we can choose, in this set of columns, R columns forming a rank R matrix modulo p. Let us say that the R columns corresponding to the variables $y_1, \dots y_R$ are of rank R. From the hypothesis (7) follows that there is a solution $(\xi_1, \dots, \xi_R)$ for the congruence $b_{R1}y_1^k + \cdots + b_{RR}y_R^k \equiv \alpha_R \,(\mathrm{mod}\, p)$ with all $\xi_i \not\equiv 0 \,(\mathrm{mod}\, p)$. Now suppose that we can produce v rank 3 contractions with $3v$ variables among the remaining variables $y_{R+1}, \dots, y_q$ (see definition 2.3 above)

Writing

$$\beta_j = \alpha_j - (b_{j1}\xi_1^k + \cdots + b_{jR}\xi_R^k) \,(\mathrm{mod}\, p), \quad \text{for} \quad j = 1, \cdots, R-1,$$

and renumbering the variables (if necessary) of the system (21) we can form the following system modulo p (with $r = R-1$)

$$(23) \qquad \begin{cases} m_1(T_1, \dots, T_v) + g_1(x_1, \dots, x_\mu) + b_1(y_{R+3v+1}, \dots, y_q) \equiv \beta_1 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\ m_r(T_1, \dots, T_v) + g_r(x_1, \dots, x_\mu) + b_r(y_{R+3v+1}, \dots, y_q) \equiv \beta_r \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad b_R(y_{R+3v+1}, \dots, y_q) \equiv 0 \end{cases},$$

a system with $n - 2v - R$ variables, since

$$(24) \qquad v + \mu + (q - 3v - R) = (\mu + q) - 2v - R = n - 2v - R.$$

Observe that if we can find an nontrivial solution

$$(\alpha_1, \cdots, \alpha_v, \lambda_1, \dots, \lambda_\mu, \gamma_{R+3v+1}, \dots, \gamma_q)$$

modulo p for the system (23) above, then

$$(25) \qquad (\lambda_1, \dots, \lambda_\mu, \xi_1, \dots, \xi_R, \omega_{R+1}, \dots, \omega_{R+3v}, \gamma_{R+3v+1}, \dots, \gamma_q)$$

will be a rank R solution (guarantied by $(\xi_1, \dots, \xi_R)$, see above) for the system (21), where, for $i = 1, \dots, v$,

$$(\omega_{R+3i-2}, \omega_{R+3i-1}, \omega_{R+3i}) = (\alpha_i\delta_1^{(i)}, \alpha_i\delta_2^{(i)}, \alpha_i\delta_3^{(i)})$$

and the v triples $(\delta_1^{(i)}, \delta_2^{(i)}, \delta_3^{(i)})$, are the solutions necessary to perform the v rank 3 contractions produced above (see definition 2.3). And this would conclude the proof of theorem 1.9.

Let $\mathfrak{C}$ be the $R \times (n - R - 2v)$ coefficient matrix of the system (23), and $\mathfrak{M}$ its $R \times v$ sub-matrix composed by the coefficients of the variables T_i's.

By definition, $\mu = \mu_{R-1}(A)$ and $q = q_1(A)$, where A is the coefficient matrix of the system (21), and since the last line of the matrix $\mathfrak{M}$ has only zeros, then

$$(26) \qquad \mu_{R-1}(\mathfrak{C}) = \mu + v.$$

Since

$$\mu_{R-1}(\mathfrak{C}) + q_1(\mathfrak{C}) = n - R - 2v \quad \text{and} \quad \mu + q = n$$

it follows that

$$q_1(\mathfrak{C}) = q - 3v - R. \tag{27}$$

Lemma 2.5. *Let $R \geq 4$ and suppose that for the system (23) we can find $1 \leq d \leq R-2$, such that $v \geq 2 \cdot 3^{d-1} + 1$ and the matrix $\mathfrak{M}$ has rank d. Then there is an nontrivial solution for the system (23).*

Proof. Let $1 \leq d \leq R-2$ be the least integer with the property given in the lemma, and let us assume $v = 2 \cdot 3^{d-1} + 1$. Rewrite the system (23) as

$$\begin{cases} m_1(T_1, \ldots, T_v) + t_1(x_{3v+1}, \ldots, x_{n-R}) & \equiv \beta_1 \pmod p \\ \qquad\qquad\qquad\qquad \vdots & \\ m_d(T_1, \ldots, T_v) + t_d(x_{3v+1}, \ldots, x_{n-R}) & \equiv \beta_d \pmod p \\ \qquad\qquad\qquad\qquad \vdots & \\ t_{R-1}(x_{3v+1}, \ldots, x_{n-R}) & \equiv \beta_{R-1} \pmod p \\ t_R(x_{3v+1}, \ldots, x_{n-R}) & \equiv 0 \pmod p \end{cases}, \tag{28}$$

where $m_1, \ldots, m_d, t_1, \ldots, t_R$ are diagonal forms of degree k, and since the coefficient matrix $\mathfrak{M}$ of the new variables T_i's has rank d.

Now consider the subsystem

$$\begin{cases} t_{d+1}(x_{3v+1}, \ldots, x_{n-R}) \equiv \beta_{d+1} \pmod p \\ \qquad\qquad \vdots \\ t_{R-1}(x_{3v+1}, \ldots, x_{n-R}) \equiv \beta_{R-1} \pmod p \\ t_R(x_{3v+1}, \ldots, x_{n-R}) \equiv 0 \pmod p \end{cases}, \tag{29}$$

and let C be the coefficient matrix of this system (29), of order $(R-d) \times (n-R-3v)$. Note that follows from the comments made just before (17) and from (27)

$$q_1(C) \geq q_1(\mathfrak{C}) = q_1(A) - R - 3v, \tag{30}$$

hence, for $s = 1, \ldots, R-d$,

$$\begin{aligned} q_s(C) &\geq q_1(C) \geq q_1(A) - R - 3(2 \cdot 3^{d-1} + 1) \\ &\geq (2 \cdot 3^{R-1} + 1 - \mu_{R-1}(A)) - 2 \cdot 3^d - 3 - R \\ &\geq 2 \cdot 3^{R-1} - 2 \cdot 3^{R-2} - 2 \cdot 3^d - 2 - R \\ &= 4 \cdot 3^{R-2} - 2 \cdot 3^d - 2 - R \\ &\geq 2 \cdot 3^{R-d-1} \geq \tfrac{s}{R-d} 2 \cdot 3^{R-d-1}, \end{aligned} \tag{31}$$

for $R \geq 4$ and $1 \leq d \leq R-2$. Applying the induction hypothesis to system (29), we can obtain a solution $\overrightarrow{\xi} = (\xi_{v+1}, \ldots, \xi_{n-R})$. Replacing this solution in (28) we have the system

$$m_i(T_1, \ldots, T_v) = \beta_i - t_i(\overrightarrow{\xi}) \pmod p \quad (i = 1, \ldots, d). \tag{32}$$

Let D be the matrix of the coefficients of (32) of order $d \times v$. Since d is the least one with the property given in the lemma, we have $\mu_{d-s}(D) \leq 2 \cdot 3^{d-s-1}$ for $s = 1, \ldots, d-1$. Hence

$$\begin{aligned} q_s(D) &= v - \mu_{d-s}(D) \\ &> 2 \cdot 3^{d-1} - 2 \cdot 3^{d-s-1} \\ &\geq \frac{s}{d} 2 \cdot 3^{d-1} \end{aligned} \tag{33}$$

for $s = 1, \ldots, d-1$. Again by the induction hypothesis, there is a solution $(\tau_1, \ldots, \tau_v)$ for (32). Therefore $(\tau_1, \ldots, \tau_v, \xi_{v+1}, \ldots, \xi_{n-R})$ is a nontrivial solution modulo p for the system (28).

□

Lemma 2.6. *Let $R = 3$ and suppose that for the system (23) we can produce two new variables (i.e. $v = 2$), such that the rank of $\mathfrak{M}$ is equal to 1. Then we can find an nontrivial solution for the system (23) modulo p.*

Proof. Since $R = 3$, it follows that, (see (9) and (22))

$$n \geq 19 \quad \text{and} \quad q \geq 13.$$

As done in the previous lemma, rewrite the system (23) as

$$\begin{cases} \gamma_1 T_1^k + \gamma_2 T_2^k + t_1(x_7, \ldots, x_{n-3}) \equiv \beta_1 \pmod p \\ \qquad\qquad\quad t_2(x_7, \ldots, x_{n-3}) \equiv \beta_2 \pmod p \\ \qquad\qquad\quad t_3(x_7, \ldots, x_{n-3}) \equiv 0 \pmod p \end{cases}. \tag{34}$$

Then the subsystem (see (29))

$$\begin{cases} t_2(x_7, \ldots, x_{n-3}) \equiv \beta_2 \pmod p \\ t_3(x_7, \ldots, x_{n-3}) \equiv 0 \pmod p \end{cases}$$

has at least 10 variables and $q_1 \geq 4$, by (30). Therefore it satisfies all the conditions required in the Proposition 2.1, and hence it has a nontrivial solution $\overrightarrow{\xi} = (\xi_7, \ldots, \xi_{n-3})$ modulo p. Applying this solution in the first equation we would have

$$\gamma_1 T_1^k + \gamma_2 T_2^k \equiv \beta_1 - t_1(\overrightarrow{\xi}) \pmod p. \tag{35}$$

If $\beta_1 - t_1(\overrightarrow{\xi}) \equiv 0 \pmod p$ then $(0, 0, \xi_7, \ldots, \xi_{n-3})$ is a nontrivial solution for (23), otherwise we can apply the ideas given in the proof of Proposition 2.1 (see (15)) and find a solution (ω_1, ω_2) for (35), and then $(\omega_1, \omega_2, \xi_7, \ldots, \xi_{n-3})$ is an nontrivial solution for (23). □

Lemma 2.7. *The system (8) has a rank R solution modulo p provided $R \geq 4$.*

Proof. With no loss of generality, let us assume that the coefficient matrix A of the system (8) is written as in (21), with the same notations described there. We make use of the ideas presented in Remark 2.4, but forming a

system like in (23) in a very specific way. As done before (see Remark 2.4), in any set of $\mu+1$ columns of A corresponding to the variables $y_1,\dots,y_q$, we can find R columns of rank R, from where we can extract 3 linearly independent columns. But we want to repeat this process v times, as long as

$$q-3v\geq \mu+1.$$

This means that, after collecting the v sets of 3 linearly independent columns, we are still able to find, among the remaining $q-3v$ columns , R columns of rank R. As seen before,

$$q=n-\mu\geq 2\cdot 3^{R-1}+1-\mu$$

then, we have

$$q-3v\geq (2\cdot 3^{R-1}+1-\mu)-3v\geq \mu+1.$$

Hence we can take v to be

$$v=\left[\frac{2\cdot 3^{R-1}-2\mu}{3}\right]\geq 2\cdot 3^{R-2}-\frac{2\mu+2}{3}. \tag{36}$$

With these v triples of columns we can perform v rank 3 contractions (see definition 2.3), and still have R columns of rank R. Now we have all the necessary ingredients to produce a system in the form of system (23). But, at this time, let us put all the unused variables y_j's equal to zero. Thus the new system will look like

$$\begin{cases} g_1(x_1,\dots,x_\mu)+t_1(T_1,\dots,T_v) & \equiv \beta_1 \pmod p \\ \qquad\qquad\vdots & \\ g_{R-1}(x_1,\dots,x_\mu)+t_{R-1}(T_1,\dots,T_v) & \equiv \beta_{R-1} \pmod p \end{cases} \tag{37}$$

From (36) follows that

$$\mu+v\geq 2\cdot 3^{R-2}-\frac{2\mu+2}{3}+\mu=2\cdot 3^{R-2}+\frac{\mu-2}{3}>2\cdot 3^{R-2}, \tag{38}$$

since $\mu=\mu_{R-1}\geq R-1>2$.

Let us still write the coefficient matrix of (37) as $\mathfrak{C}$ and the coefficient matrix of the new variables T's as $\mathfrak{M}$ (see Remark 2.4). At this point one needs to observe that the first μ columns of the matrix A (see (21)) are equal to the first μ columns of the matrix $\mathfrak{C}$, but with a zero in the last coordinate.

Another important observation about the matrix $\mathfrak{C}$ is the following. Let D be the maximal set of the columns of $\mathfrak{C}$ belonging to the same d-dimensional linear subspace of $\mathbb{F}_p^{R-1}$ (since $\mathfrak{C}$ has order $(R-1)\times(\mu+v)$), and by definition the cardinality of D is equal to $\mu_d(\mathfrak{C})$. Now divide D into two subsets D_1 and D_2, where D_1 contains the columns taken among the first μ columns of $\mathfrak{C}$, and D_2 contains the columns taken among the last v of $\mathfrak{C}$. Hence, the dimension of the two linear subspaces generated by the

columns in D_1 and D_2 respectively is at most d. Therefore, it follows from (5) that, for $d = 1, \ldots, R-2$

$$\mu_d(\mathfrak{C}) \leq \mu_d(A) + \mu_d(\mathfrak{M}). \tag{39}$$

According to Lemmas 2.2 and 2.5 (since any nontrivial solution for (37) implies a rank R solution for (21))

$$\mu_d(A) \leq 2 \cdot 3^{d-1} \quad \text{and} \quad \mu_d(\mathfrak{M}) \leq 2 \cdot 3^{d-1},$$

hence for $d = 1, \ldots, R-2$

$$\mu_d(\mathfrak{C}) \leq 4 \cdot 3^{d-1}. \tag{40}$$

For the matrix $\mathfrak{C}$ one has (see (4)), for $d = 1, \ldots, R-2$

$$q_d(\mathfrak{C}) + \mu_{R-1-d}(\mathfrak{C}) = \mu + v.$$

Hence (see (38) and (40))

$$q_d(\mathfrak{C}) = (\mu + v) - \mu_{R-1-d}(\mathfrak{C}) > 2 \cdot 3^{R-2} - 4 \cdot 3^{(R-1-d)-1}.$$

Now

$$q_d(\mathfrak{C}) > 2 \cdot 3^{R-2} - 4 \cdot 3^{(R-d-1)-1} \geq \frac{d}{R-1} 2 \cdot 3^{R-2}$$

since

$$2 \cdot 3^{R-2} - \frac{d}{R-1} 2 \cdot 3^{R-2} = \frac{2(R-1-d)}{R-1} \cdot 3^{R-2} \geq 4 \cdot 3^{R-d-2}$$

and

$$\frac{(R-1-d)}{R-1} \geq \frac{2}{3^d}$$

for $d = 1, \ldots, R-2$, and $R \geq 4$. Now we can apply the induction hypothesis to the system (37), which guarantees a nontrivial solution for this system, and therefore a rank R solution modulo p (see (25)) for the system (8). □

Lemma 2.8. *The system (8) has a rank R solution modulo p.*

Proof. It remains only the case $R = 3$ to consider, and we are going to follow very closely the steps presented in the proof of Lemma 2.7. After performing the possible v contractions and still having left, among the remaining variables y_j's, 3 columns of rank 3, we can form the system, putting the unused variables equal to zero (see (37)),

$$\begin{cases} g_1(x_1, \ldots, x_\mu) + t_1(T_1, \ldots, T_v) \equiv \beta_1 \,(\mathrm{mod}\, p) \\ g_2(x_1, \ldots, x_\mu) + t_2(T_1, \ldots, T_v) \equiv \beta_2 \,(\mathrm{mod}\, p) \end{cases}. \tag{41}$$

According to (38) this system has at least $\mu + v \geq 7$ variables, and the matrix $\mathfrak{C}$ of this system has (see (39))

$$\mu_1(\mathfrak{C}) \leq \mu_1(A) + \mu_1(\mathfrak{M}).$$

It follows from lemmas 2.2 and 2.6 that

$$\mu_1(A) \leq 2 \quad \text{and} \quad \mu_1(\mathfrak{M}) = 1,$$

hence $\mu_1(\mathfrak{C}) \leq 3$. Since $n = q_1(\mathfrak{C}) + \mu_1(\mathfrak{C})$, we have

$$q_1(\mathfrak{C}) \geq 7 - 3 = 4.$$

It follows from Proposition 2.1 that there is a nontrivial solution of the system (41), and therefore (8) has a rank 3 solution modulo p, concluding the proof. □

References

[1] O.D. Atkinson, J. Brüdern, R.J. Cook, *Simultaneous additive congruences to a large prime modulus*. Mathematika **39 (1)** (1992), 1–9.

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

[3] H. Godinho, P. H. A. Rodrigues, *Conditions for the solvability of systems of two and three additive forms over p-adic fields*. Proc. of the London Math. Soc. **91** (2005), 545–572.

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

[5] L. Low, J. Pitman, A. Wolff, *Simultaneous Diagonal Congruences*. J. Number Theory **29** (1988), 31–59.

[6] I. D. Meir, *Pairs of Additive Congruences to a Large Prime Modulus*. J. Number Theory **63** (1997), 132–142.

Hemar Godinho
Departamento de Matemática
Universidade de Brasília
70.910-900, Brasília, DF, Brasil
E-mail : hemar@unb.br

Paulo H. A. Rodrigues
Instituto de Matemática e Estatística
Universidade Federal de Goiás
74.001-970, Goiânia, GO, Brasil
E-mail : paulo@mat.ufg.br