

# On Artin's conjecture, I: Systems of diagonal forms

J. Brüdern and H. Godinho\*

**1. Introduction.** As a special case of a well-known conjecture of Artin, it is expected that a system of  $R$  additive forms of degree  $k$ , say

$$\sum_{i=1}^N a_{ij}x_i^k = 0 \quad (1 \leq j \leq R) \quad (1)$$

with integer coefficients  $a_{ij}$ , has a *non-trivial* solution in  $\mathbb{Q}_p$  for all primes  $p$  whenever

$$N > Rk^2. \quad (2)$$

Here we adopt the convention that a solution of (1) is non-trivial if not all the  $x_i$  are 0. To date, this has been verified only when  $R = 1$  by Davenport and Lewis [4], and for odd  $k$  when  $R = 2$  by Davenport and Lewis [5]. For larger values of  $R$ , and in particular when  $k$  is even, more severe conditions on  $N$  are required to assure the existence of  $p$ -adic solutions of (1) for all primes  $p$ . In another important contribution, Davenport and Lewis [6] showed that the conditions

$$N \geq 9R^2k \log(3Rk) \quad (k \text{ odd}), \quad N \geq 48R^2k^3 \log(3Rk^2) \quad (k > 2 \text{ even})$$

are sufficient. There have been a number of refinements of these results. Schmidt [13] obtained  $N \gg R^2k^3 \log k$ , and Low, Pitman and Wolff [10] improved the work of Davenport and Lewis by showing the weaker constraints

$$N \geq 2R^2k \log k \quad (k \gg 1 \text{ odd}), \quad N \geq 48Rk^3 \log(3Rk^2) \quad (k > 2)$$

to be sufficient for  $p$ -adic solubility of (1).

---

\*This paper was written while H.G. was visiting Universität Stuttgart, supported by grants of CNPQ and FAP/DF

A noticeable feature of these results is that for even  $k$  one always encounters a factor  $k^3 \log k$ , in spite of the expected  $k^2$  in (2). In this paper we show that one can reach the expected order of magnitude  $k^2$ .

**THEOREM 1.** *Let  $k \geq 3$  and  $R \geq 3$ . Then the system of equations (1) has a non-trivial solution in  $\mathbb{Q}_p$  for all primes  $p$  provided that*

$$N \geq R^3 k^2$$

*unless  $R = 3$  and  $k$  is a power of 2 in which case the condition on  $N$  has to be replaced by  $N \geq 36k^2$ .*

For small values of  $R$  or  $k$  our analysis can be considerably refined. We shall discuss in greater detail the case of pairs of equations  $R = 2$ . In the light of the aforementioned result of Davenport and Lewis, only even  $k$  deserve attention. Davenport and Lewis [5] showed that for even  $k$ , the pair of equations

$$\sum_{i=1}^N a_i x_i^k = \sum_{i=1}^N b_i x_i^k = 0 \quad (3)$$

with  $a_i, b_i \in \mathbb{Z}$  has a non-trivial  $p$ -adic solution for all primes  $p$  when  $N \geq 7k^3$ , and this remained unimproved until very recently when Godinho [9] obtained bounds on  $N$  which are dependent on the prime factorisation of the degree. However, it does not follow from the work of [9] that a condition like  $N \geq Ck^2$  with some constant  $C$  suffices to guarantee solubility of (3) in all  $\mathbb{Q}_p$ . Our second theorem provides such a bound with  $C = 16$ .

**THEOREM 2.** *If  $k$  is of the form*

$$k = 2 \cdot 5^\tau \quad \text{or} \quad k = (p-1)p^\tau \text{ for some prime } p > 2 \quad (4)$$

*then the pair (3) has a non-trivial solution in all  $p$ -adic fields whenever*

$$N \geq 6k(k-1).$$

*If  $k$  is not of the form (4) but*

$$k = k_0 2^\tau \quad \text{with } k_0 = 1 \text{ or } 3 \text{ or } 5 \text{ or } 7 \quad (5)$$

*then the same conclusion holds if  $N \geq 16k^2 k_0^{-1} - 4k$ .*

*If  $k$  is neither of the form (4) or (5) but takes the shape*

$$k = 2p^\tau(p-1), \quad (6)$$

then for  $N \geq 3k(k-2)$  the equations (3) have a non-trivial solution in all  $p$ -adic fields. When  $k$  is neither of the forms (4), (5) or (6), then the condition  $N \geq 2k^2 + 1$  suffices.

Godinho [8] considered pairs of degree  $k = 2^\tau$ , and obtained the slightly superior sufficient condition

$$N \geq 16k^2 - 26k + 1.$$

Our approach follows earlier work in all preparatory steps. We shall begin with the  $p$ -normalisation process. This amounts to finding a system of equations (1) which is equivalent to the given one but has additional properties to facilitate the later analysis. Then we reduce the problem to finding a non-singular solution to an auxiliary congruence. This part is standard and will be quoted from the literature in §2. We then dismiss primes not dividing the degree in §3 by a simple application of Chevalley's theorem. For primes dividing the degree, congruences to prime power modulus have to be considered, and in §4 we apply a result of Olson [12] in combinatorial group theory to solve them. Theorem 1 will then be immediate, and in the last section Theorem 2 will be deduced by a finer analysis, but based on the same ideas.

Olson's powerful theorem provides, in a certain sense, a suitable substitute for Chevalley's theorem when prime power moduli occur. This is our main source for improvement. Baker and Schmidt [2] have also used Olson's theorem in related problems, but its use for the present problem appears to be new.

We mention in passing that for very large primes  $p$  the number of variables required for the existence of  $p$ -adic solutions reduces to  $N > 2Rk$ . See Atkinson, Brüdern and Cook [1] and Meir [11] for work in this direction.

**2. Normalisation.** In this section we briefly recall the concept of  $p$ -normalisation introduced by Davenport and Lewis [6]. Let  $A = (a_{ij})$  be the matrix of coefficients of (1), and write  $\mathbf{a}_j = (a_{ij})_{1 \leq i \leq R}$  to denote the  $j$ -th column of  $A$ . Let

$$\theta(A) = \prod_{1 \leq i_1 < i_2 < \dots < i_R \leq N} \det(\mathbf{a}_{i_1} \mathbf{a}_{i_2} \dots \mathbf{a}_{i_R}).$$

For a fixed prime  $p$ , suppose we wish to investigate whether or not the system (1) admits a non-trivial  $p$ -adic solution. Then, in (1) we may replace the

original equations by any  $R$  independent linear combinations thereof (this corresponds to row operations applied to  $A$ ). Moreover, since  $\mathbb{Q}_p$  is a field of characteristic 0, we may replace a variable  $x_i$  with  $p^\nu x_i$ , for any  $\nu \in \mathbb{N}$ , and then divide the resulting equations by any power of  $p$  which divides all coefficients. Two systems of equations (1) are called  $p$ -equivalent if one can be obtained from the other by a finite succession of these processes. A system (1) is called  $p$ -normalised if  $\theta(A) \neq 0$  and the power of  $p$  dividing  $\theta(A)$  is minimal among all systems which are  $p$ -equivalent to the given one.

LEMMA 1. *Let  $k \geq 2$ ,  $N > R$  and suppose that (1) admits non-trivial  $p$ -adic solutions for all  $p$ -normalised systems. Then, (1) has non-trivial  $p$ -adic solutions for any choice of integer coefficients.*

*Proof.* See Davenport and Lewis [6], §4.

Following Davenport and Lewis [5] in spirit, we say that the variable  $x_i$  is at level  $l$  if  $p^l | \mathbf{a}_i$  but  $p^{l+1} \nmid \mathbf{a}_i$ . If a system is  $p$ -normalised, all variables are at a level less than  $k$ . To see this suppose that  $x_i$  is at level  $l \geq k$ . Then  $p^{-k} \mathbf{a}_i$  has integral components, and therefore the substitution  $x'_i = px_i$  changes the  $\theta$ -value of  $A$  by a factor  $p^{-Mk}$  for some  $M > 0$ .

Suppose that (1) is  $p$ -normalised, and let  $n$  denote the number of variables at level 0. By Lemma 11 of Davenport and Lewis [6], one has

$$n \geq N/k. \tag{7}$$

We may renumber the variables of (1) to arrange that  $x_1, x_2, \dots, x_n$  are the variables at level 0, and we denote the submatrix of  $A$ , consisting of the first  $n$  columns, by  $A_0$ . We consider  $A_0$  as a matrix with coefficients in the finite field  $\mathbb{F}_p$  of  $p$  elements. For  $1 \leq \nu \leq R$  the invariant  $q_\nu$  is defined as the minimum number of non-zero columns in any  $\nu$  linear combinations of the rows of  $A_0$  which are independent over  $\mathbb{F}_p$ . Again by Lemma 11 of Davenport and Lewis [6],

$$q_\nu \geq \nu N / (Rk) \quad (1 \leq \nu \leq R). \tag{8}$$

Now let  $\mu(d)$  be the maximal number of columns of  $A_0$  which lie in a  $d$ -dimensional linear subspace of  $\mathbb{F}_p^R$ . Then

$$q_\nu + \mu(R - \nu) = n \tag{9}$$

for  $1 \leq \nu \leq R$ . Low, Pitman and Wolff [10] observed that the invariants  $\mu(d)$  control non-singular  $R \times R$  submatrices of  $A_0$ . From a combinatorial result

on matroids they deduced that for any  $t \in \mathbb{N}$ , the matrix  $A_0$  will contain  $t$  disjoint  $R \times R$  submatrices with determinant not divisible by  $p$ , if and only if,

$$n - \mu(d) \geq t(R - d) \quad \text{for all } 0 \leq d \leq R$$

(this is Low, Pitman and Wolff [10], Lemma 1). By (9), this is equivalent with  $q_\nu \geq t\nu$  for  $1 \leq \nu \leq R$ , and by (8), we may conclude as follows.

LEMMA 2. *Suppose that (1) is  $p$ -normalised and has  $n$  variables at level 0. Then the  $n \times R$  matrix  $A_0$  contains at least  $\lfloor N/(Rk) \rfloor$  disjoint  $R \times R$  submatrices with determinant not divisible by  $p$ .*

As a final preparation for our approach to the theorems, we reduce the question of  $p$ -adic solubility to congruences. Let  $\gamma \geq 1$ . A solution of the system of congruences

$$\sum_{i=1}^N a_{ij} x_i^k \equiv 0 \pmod{p^\gamma} \quad (1 \leq j \leq R) \quad (10)$$

is called non-singular if there are  $i_1, \dots, i_R$  with

$$x_{i_1} x_{i_2} \dots x_{i_R} \det(\mathbf{a}_{i_1} \dots \mathbf{a}_{i_R}) \not\equiv 0 \pmod{p}.$$

For a given  $k$  we define  $\tau$  via  $p^\tau \parallel k$  and write

$$\gamma = \gamma(k; p) = \begin{cases} \tau + 2 & \text{if } p = 2, \tau > 0, \\ \tau + 1 & \text{otherwise.} \end{cases} \quad (11)$$

LEMMA 3. *Suppose that the congruences (10) have a non-singular solution when  $\gamma$  is given by (11). Then the equations (1) have a non-trivial solution in  $\mathbb{Q}_p$ .*

This is a version of Hensel's Lemma, see Davenport and Lewis [6], Lemma 9.

**3. Congruences modulo primes.** In this section we provide non-singular solutions to the system of congruences when  $\gamma = 1$ , and as a corollary obtain a version of Theorem 1 for all primes  $p \nmid k$ . We begin by recalling a classic result of Chevalley [3].

LEMMA 4. Let  $k \geq 1$  and  $p$  be a prime. Let  $\delta = (k, p - 1)$ . Let  $c_{ij}$  be any integers and  $m > R\delta$ . Then the system of congruences

$$\sum_{i=1}^m c_{ij} x_i^k \equiv 0 \pmod{p} \quad (1 \leq j \leq R) \quad (12)$$

admits a primitive solution.

Recall that a solution of congruences is called primitive if not all its coordinates are divisible by  $p$ .

Simple examples show that all solutions of (12) may be singular. However, the following corollary yields non-singular solutions.

LEMMA 5. Let  $k, p, \delta, c_{ij}$  be as in the previous Lemma. Suppose that

$$m \geq R^2(\delta - 1) + 2R, \quad (13)$$

and that the  $m \times R$  matrix  $(c_{ij})$  contains  $R(\delta - 1) + 2$  disjoint  $R \times R$  matrices with determinant not divisible by  $p$ . Then the system of congruences (12) admits a non-singular solution.

*Proof.* By renumbering the columns  $\mathbf{c}_i$  of  $(c_{ij})$  we may suppose that the  $R \times R$  matrices  $(\mathbf{c}_{lR+1} \dots \mathbf{c}_{(l+1)R})$  for  $0 \leq l \leq R(\delta - 1) + 1$  are all non-singular. We may now assume that  $m = R^2(\delta - 1) + 2R$  (take  $x_i = 0$  for  $i > R^2(\delta - 1) + 2R$  otherwise). Put

$$b_{lj} = \sum_{i=lR+1}^{(l+1)R} c_{ij} \quad (0 \leq l \leq R(\delta - 1)) \quad (14)$$

and consider the system of congruences

$$\sum_{l=0}^{R(\delta-1)} b_{lj} y_l^k + \sum_{i=m-R+1}^m c_{ij} x_i^k \equiv 0 \pmod{p} \quad (1 \leq j \leq R) \quad (15)$$

This involves  $R\delta + 1$  variables and therefore has a primitive solution by Lemma 4. Since the columns  $\mathbf{c}_{m-R+1}, \dots, \mathbf{c}_m$  are linearly independent (mod  $p$ ), any primitive solution of (15) must have at least one of the  $y_l$  not divisible by  $p$ . By taking

$$x_i = y_l \quad \text{for } lR < i \leq (l+1)R, \quad 0 \leq l \leq R(\delta - 1)$$

we obtain a solution of (12) which is non-singular.

It is now easy to deduce a result on  $p$ -adic solubility when  $p \nmid k$ . In this case Lemma 3 is applicable with  $\gamma = 1$ . By Lemmas 2 and 5 we may conclude as follows.

**THEOREM 3.** *Let  $p$  be a prime,  $p \nmid k$  and  $N \geq Rk(R(k, p-1) - R + 2)$ . Then the system of equations (1) admits a non-trivial solution in  $\mathbb{Q}_p$ .*

A result very similar to this occurs *inter alia* in Davenport and Lewis [6]. We have preferred to present the above approach which is somewhat different from previous techniques, and can serve as a model for the more original arguments in the next section. It would be very interesting to weaken the condition (13). When  $R = 2$ , Davenport and Lewis [5] established the following result.

**LEMMA 6.** *Let  $k \geq 2$ ,  $p$  be prime and  $\delta = (k, p-1)$ . Let  $a_i, b_i \in \mathbb{Z}$  ( $1 \leq i \leq m$ ) and suppose that  $m \geq 2\delta + 1$ . Further suppose that any linear combination of the rows  $(a_i), (b_i)$  with coefficients not both divisible by  $p$  contains at least  $\delta + 1$  entries not divisible by  $p$ . Then the pair of congruences*

$$\sum_{i=1}^m a_i x_i^k \equiv \sum_{i=1}^m b_i x_i^k \equiv 0 \pmod{p}$$

*has a non-singular solution.*

One may easily deduce that for  $R = 2$ , the equations (1) have a non-trivial solution in  $\mathbb{Q}_p$  when  $N \geq 2k^2 + 1$  and  $p \nmid k$ . However, when  $R = 3$ , the natural generalisation of Lemma 6, with  $m \geq 3\delta + 1$ ,  $q_\nu \geq \nu\delta + 1$  ( $\nu = 1, 2$ ), is false. See Davenport and Lewis [7], p. 344, for details and further comments.

**4. Primes dividing the degree.** We complete the proof of Theorem 1 in this section by considering primes  $p \mid k$ . In this case we shall solve the congruences (10) with the aid of combinatorial group theory. We begin with recalling a result of Olson [12]. Let  $G$  be a (additive) finite abelian  $p$ -group. Then  $G$  is isomorphic to

$$\mathbb{Z}/p^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{e_r}\mathbb{Z}$$

for suitable  $e_j \in \mathbb{N}$ . If  $g_1, \dots, g_s \in G$  and

$$s > \sum_{j=1}^r (p^{e_j} - 1)$$

then, by Olson's theorem, there are  $\epsilon_i \in \{0, 1\}$ , not all 0, with  $\epsilon_1 g_1 + \dots + \epsilon_s g_s = 0$ . We need this result only when all  $e_j$  are equal, and reformulate it in the language of congruences when  $G = (\mathbb{Z}/p^t \mathbb{Z})^R$ .

LEMMA 7. *Let  $b_{ij} \in \mathbb{Z}$  ( $1 \leq i \leq s, 1 \leq j \leq R$ ). Let  $p$  be a prime and  $t \geq 1$ . Then, provided that  $s > R(p^t - 1)$ , there are  $\epsilon_i \in \{0, 1\}$ , not all 0, such that*

$$\sum_{i=1}^s \epsilon_i b_{ij} \equiv 0 \pmod{p^t} \quad (1 \leq j \leq R).$$

It is now easy to modify the arguments of the previous section to establish the following result.

THEOREM 4. *Let  $p$  be a prime with  $p|k$  and define  $\gamma$  by (11). Then, provided that*

$$N \geq Rk(R(p^\gamma - 2) + 2) \tag{16}$$

*the equations (1) have a non-trivial solution in  $\mathbb{Q}_p$ .*

*Proof.* By Lemma 2, we may suppose that the variables  $x_i$  with  $1 \leq i \leq n$  are at level 0 where  $n \geq R^2(p^\gamma - 2) + 2R$ , and that the matrices

$$(\mathbf{a}_{lR+1} \dots \mathbf{a}_{(l+1)R}) \tag{17}$$

with  $0 \leq l \leq R(p^\gamma - 2) + 1$  are all non-singular (mod  $p$ ). We define  $b_{lj}$  by (14). The system of congruences

$$\sum_{l=0}^{R(p^\gamma-2)} b_{lj} y_l^k + \sum_{i=R^2(p^\gamma-2)+R+1}^{R^2(p^\gamma-2)+2R} a_{ij} x_i^k \equiv 0 \pmod{p^\gamma} \quad (1 \leq j \leq R)$$

involves  $R(p^\gamma - 1) + 1$  variables and therefore has, by Lemma 7, a solution with  $y_l \in \{0, 1\}$ ,  $x_i \in \{0, 1\}$ , not all 0. As in the previous section we see



that at least one  $y_l$  is non-zero, and this yields a non-singular solution of the system

$$\sum_{i=1}^{R^2(p^\gamma-2)+2R} a_{ij}x_i^k \equiv 0 \pmod{p^\gamma} \quad (1 \leq j \leq R),$$

as required in Lemma 3 to complete the proof of the theorem.

We have included Theorem 4 mainly for use with very small primes where it proves to be highly effective. It also has a certain interest on its own right. If the prime factorisation of  $k$  is “neat enough”, then one may deduce from (16) much better bounds than available from Theorem 1. For example, if  $p^\gamma \leq k$  holds for all  $p|k$  then (1) is soluble in all  $\mathbb{Q}_p$  whenever  $N \geq R^2k^2$ . However, one cannot expect to deduce Theorem 1 from Theorem 4. If  $k = 2p$  for some odd prime  $p$ , then  $\gamma = 2$  and in (16) about  $\frac{1}{2}R^2k^3$  variables are required. Fortunately there is an alternative approach through *contractions*, a term coined by Davenport and Lewis [4]. This will keep the bounds quadratic in  $k$ , but at the price of an extra factor  $R$ .

**THEOREM 5.** *Let  $p \neq 2$  and suppose that  $p^\tau \parallel k$ ,  $\delta = (k, p-1)$ . Then, provided that*

$$N \geq Rk(R(\delta-1)+2)(R(p^\tau-1)+1),$$

*the equations (1) have a non-trivial  $p$ -adic solution in  $\mathbb{Q}_p$ .*

We begin by describing the contraction argument. Suppose that the system (1) is  $p$ -normalised and that the matrix  $A_0$  of the columns at level 0 contains  $T$  disjoint blocks of  $R \times R$  submatrices which are non-singular (mod  $p$ ). Put  $H = R(\delta-1)+2$  and suppose that  $T = Ht$  with some  $t \in \mathbb{N}$ . We may then assume that the matrices (17) with  $0 \leq l \leq T-1$  are all non-singular (mod  $p$ ). By Lemma 5, the congruences

$$\sum_{hHR < i \leq (h+1)HR} a_{ij}u_i^k \equiv 0 \pmod{p} \quad (1 \leq j \leq R) \quad (18)$$

have a non-singular solution for any choice of  $0 \leq h \leq t-1$ . We then write

$$\sum_{hHR < i \leq (h+1)HR} a_{ij}u_i^k = pb_{hj} \quad (19)$$

with integers  $b_{hj}$ , and consider the congruences

$$\sum_{h=0}^{t-1} b_{hj} \epsilon_h \equiv 0 \pmod{p^\tau} \quad (1 \leq j \leq R), \quad (20)$$

to be solved with  $\epsilon_h \in \{0, 1\}$ . If  $t \geq R(p^\tau - 1) + 1$  such a solution exists with not all  $\epsilon_h = 0$ . By suitable renumbering, we may assume that (20) holds with  $\epsilon_h = 1$  for  $0 \leq h \leq H_1$  and  $\epsilon_h = 0$  for  $H_1 < h \leq t - 1$ , with some  $H_1 \geq 0$ . From (19) we now deduce that

$$\sum_{h=0}^{H_1} \sum_{hHR < i \leq (h+1)HR} a_{ij} u_i^k \equiv 0 \pmod{p^{\tau+1}},$$

and the solution is non-singular by construction. For  $p \neq 2$  we have  $\gamma = \tau + 1$ , and this establishes the non-singular solubility of (10).

Theorem 5 is now available. Take  $t = R(p^\tau - 1) + 1$  and  $T = Ht$  as above. If  $N \geq RkT$ , the matrix  $A_0$  will contain the required  $T$  disjoint non-singular blocks for any  $p$ -normalised system (1). Theorem 5 now follows from Lemmas 1 and 3.

When  $R = 2$ , the result can be refined by injecting Lemma 6 in place of Lemma 5 in the above argument. If  $m = 2\delta + 2$  and the matrix  $\begin{pmatrix} a_i \\ b_i \end{pmatrix}_{i < m}$  splits into  $\delta + 1$  disjoint  $2 \times 2$  matrices which are non-singular  $(\text{mod } p)$ , then for any  $\lambda, \mu$  not both divisible by  $p$ , the numbers  $\lambda a_i + \mu b_i$  will contain at least  $\delta + 1$  numbers not divisible by  $p$ . Hence, the congruences in Lemma 6 have a non-singular solution. Consequently, in the preceding argument, we may take  $H = \delta + 1$ , and then proceed as before to deduce the following.

**THEOREM 6.** *Let  $p, k$  and  $\delta$  be as in Theorem 5. Then the pair of equations (3) with integer coefficients admits a non-trivial  $p$ -adic solution provided that*

$$N \geq 2k(\delta + 1)(2p^\tau - 1).$$

Theorem 1 is now a simple corollary. For all primes  $p \nmid k$  the required conclusion is immediate from Theorem 3, and when  $p \mid k$ ,  $p \neq 2$ , Theorem 5 yields the required result. When  $p = 2$  and  $2 \mid k$ , we write  $k = 2^\tau k_0$  with odd  $k_0$ . By Theorem 4, the equations (1) have a non-trivial 2-adic solution whenever

$$N \geq 2Rk(R(2^{\tau+1} - 1) + 1),$$

which is more than required unless  $R = 3$  and  $k_0 = 1$  in which case the condition  $N \geq 36k^2$  certainly suffices.

**5. Pairs of equations.** We shall now deduce Theorem 2. We may suppose that  $k$  is even since otherwise  $N \geq 2k^2 + 1$  suffices by Theorem 1 of Davenport and Lewis [5]. When  $k$  is even, Davenport and Lewis [5] have shown the following.

LEMMA 8. *Let  $k$  be even and suppose that  $p^\tau \parallel k$ ,  $\delta = (k, p - 1)$ . If  $\tau = 0$  and  $N \geq 2k^2 + 1$ , the pair of equations (3) has a non-trivial  $p$ -adic solution. If  $\delta < \frac{1}{2}(p - 1)$ , or  $\delta = \frac{1}{2}(p - 1) \geq 3$ , then again the equations (3) have a non-trivial  $p$ -adic solution whenever  $N \geq 2k^2 + 1$ .*

*Proof.* The first statement follows from Lemma 6. For the second statement, see Davenport and Lewis [5], sections 6 and 7.

It now remains to discuss the following cases:

$$p|k, \quad \delta = p - 1 \tag{21}$$

and

$$p|k, \quad \delta = \frac{1}{2}(p - 1) < 3. \tag{22}$$

Note that (22) implies that  $p < 7$ , and since  $k$  is even, the cases  $p = 2$  and  $3$  cannot occur. Hence (22) occurs only for  $p = 5$ , when  $5|k$  and  $\delta = (4, k) = 2$ . This means  $2 \parallel k$ , and we may write  $k = 2 \cdot 5^\tau k_0$  with  $(10, k_0) = 1$ . In this particular case, Theorem 6 yields 5-adic solubility for

$$N \geq 6k(kk_0^{-1} - 1).$$

If  $k_0 = 1$ , this is one of the exceptional cases in Theorem 2, and  $k_0 > 1$  implies  $k_0 \geq 3$ . In this last case,  $N \geq 2k^2 + 1$  will suffice.

We can now concentrate on the case (21). We can then write  $k = p^\tau(p - 1)k_0$ . First suppose that  $p \neq 2$ . Then, by Theorem 6, we see that the equations (3) have a  $p$ -adic solution whenever

$$N \geq 2kp(2p^\tau - 1) = \frac{4p}{p - 1} \frac{k^2}{k_0} - 2kp. \tag{23}$$

Note that  $p/(p - 1) \leq 3/2$ . Hence, if  $k_0 \geq 3$ , then  $N \geq 2k^2 + 1$  will certainly suffice to guarantee  $p$ -adic solubility of (3). When  $k_0 = 2$ , we use  $p \geq 3$

in (23) to see that  $N \geq 3k(k-2)$  suffices. Finally, when  $k_0 = 1$ , the same reasoning shows that  $N \geq 6k(k-1)$  is enough to guarantee solubility of (3) in  $\mathbb{Q}_p$ .

Finally we discuss 2-adic solubility. Here we write  $k = 2^\tau k_0$  with odd  $k_0$  and apply Theorem 4 with  $R = p = 2$ . This shows that (3) admits non-trivial  $p$ -adic solutions whenever  $N \geq 16k^2 k_0^{-1} - 4k$ .

Theorem 2 is now immediate.

## References

- [1] O.D. Atkinson, J. Brüdern and R.J. Cook. Simultaneous additive congruences to a large prime modulus. *Mathematika* 39 (1992) 1–9.
- [2] R.C. Baker and W.M. Schmidt. Diophantine problems in variables restricted to the values 0 and 1. *J. Number Theory* 12 (1980) 460–486.
- [3] C. Chevalley. Démonstration d’une hypothèse de M. Artin. *Abh. Math. Sem. Hamburg* 11 (1935) 73–75.
- [4] H. Davenport and D.J. Lewis. Homogeneous additive equations. *Proc. Royal Soc. London A* 274 (1963) 443–460.
- [5] H. Davenport and D.J. Lewis. Two additive equations. *Proc. Symposia in Pure Maths.* (Houston, 1972) 12, pp. 74–98.
- [6] H. Davenport and D.J. Lewis. Simultaneous equations of additive type. *Philos. Trans. Royal Soc. A* 264 (1969) 557–595.
- [7] H. Davenport and D.J. Lewis. Notes on congruences III. *Quart. J. Math.* (2) 17 (1966) 339–344.
- [8] H. Godinho. Additive forms of degree  $K = 2^l$ . *J. Number Theory* 46 (1994) 391–408.
- [9] H. Godinho. On  $p$ -adic zeros of additive forms of even degree. *J. Number Theory* 68 (1998) 1–20.
- [10] L. Low, J. Pitman and A. Wolff. Simultaneous diagonal congruences. *J. Number Theory* 29 (1988) 31–59.

- [11] I.D. Meir, Pairs of additive congruences to a large prime modulus. *J. Number Theory* 63 (1997) 132–142.
- [12] J.E. Olson, A combinatorial problem on finite abelian groups I. *J. Number Theory* 1 (1969) 8–10.
- [13] W.M. Schmidt. The solubility of certain  $p$ -adic equations. *J. Number Theory* 19 (1984) 63–80.

Jörg Brüdern  
Mathematisches Institut A  
Universität Stuttgart  
D-70550 Stuttgart, Germany

Hemar Godinho  
Dept. de Matematica  
Universidade de Brasilia  
Brasilia, DF 70910-900, Brazil