J. Austral. Math. Soc. (Series A) **55** (1993), 355–368

THREE ADDITIVE CONGRUENCES TO A LARGE PRIME MODULUS

O. D. ATKINSON, J. BRÜDERN and R. J. COOK

(Received 15 January 1991)

Communicated by J. H. Loxton

Abstract

Let $k \geq 3$ and $n > 6k$ be positive integers. The equations

$$\begin{aligned} f(\mathbf{x}) &= a_1x_1^k + \cdots + a_nx_n^k = 0, \\ g(\mathbf{x}) &= b_1x_1^k + \cdots + b_nx_n^k = 0, \\ h(\mathbf{x}) &= c_1x_1^k + \cdots + c_nx_n^k = 0, \end{aligned}$$

with integer coefficients, have nontrivial p-adic solutions for all $p > Ck^8$, where C is some positive constant. Further, for values $k \geq K$ we can take $C = 1 + O(K^{-\frac{1}{2}})$.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11 D 88.

1. Introduction

Before considering systems of 3 equations we recall the analogous results for smaller systems of equations.

THEOREM A. *Let $n > 2k$. A single additive equation*

$$a_1x_1^k + \cdots + a_nx_n^k = 0, \tag{1}$$

with integer coefficients, has a non-trivial p-adic solution for all $p > k^4$.

This is Theorem A of Atkinson and Cook (1989). The condition $n > 2k$ is best possible, since the equation

$$\sum_{i=1}^{k} p^{i-1}(x_i^k - qy_i^k) = 0 \tag{2}$$

where $p \equiv 1 \bmod k$ and q is a k-th power non-residue $\bmod p$, has no non-trivial solutions.

THEOREM B. *Let $n > 4k$. Any two additive equations*

$$\left.\begin{array}{rcl} a_1x_1^k + \cdots + a_nx_n^k & = & 0, \\ b_1x_1^k + \cdots + b_nx_n^k & = & 0, \end{array}\right\} \tag{3}$$

with integer coefficients, have a non-trivial p-adic solution for all $p > k^6$.

This is Theorem 1 of Atkinson and Cook (1989). The condition $n > 4k$ is best possible, as can be seen by taking two disjoint copies of the example (2). Similarly, if we consider a system of r simultaneous additive forms

$$f_i(\mathbf{x}) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0 \tag{4}$$

then the corresponding condition $n > 2rk$ is best possible. Recently Dörner (1990) has proved a result for forms over algebraic number fields which we restate in our more specific setting.

THEOREM C. (Dörner) *Let r, k, n be positive integers with $n > 2rk$. There exists a bound $p_0 = p_0(r, k)$ such that every system of equations* (4), *with integer coefficients, has a non-trivial p-adic solution for all $p > p_0(r, k)$.*

Dörner's approach is based on techniques of Schmidt (1984) and does not lead to particularly good bounds for p_0. Dörner made no attempt to estimate p_0 but rough calculations based on his paper appear to lead to a value

$$p_0(r, k) \gg r^{2rk}k^{4r^2k^2}. \tag{5}$$

Wooley (1990) has generalized Theorem B to the case when the two equations have different degrees, and made a conjecture (in this more general setting) that we can take

$$p_0(r, k) = k^{2r+2}. \tag{6}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

As a first step towards obtaining better bounds for $p_0(r, k)$ we consider here the particular case of 3 additive equations. Fern Ellison (1973) showed that 3 additive quadratic equations in $n > 12$ variables have non-trivial p-adic solutions for all $p \neq 2$, so we restrict our attention to the case $k \geq 3$.

The major problem encountered lies in the combinatorial structure of subspaces generated by columns of coefficients. It was recognized by Low, Pitman and Wolff (1988) that such difficulties can be tackled using a combinatorial result of Aigner (1979). These techniques are again useful in this context.

THEOREM 1. *Let $k \geq 3$ and $n > 6k$. Any three additive equations*

$$\left.\begin{aligned} f(\mathbf{x}) = a_1x_1^k + \cdots + a_nx_n^k &= 0, \\ g(\mathbf{x}) = b_1x_1^k + \cdots + b_nx_n^k &= 0, \\ h(\mathbf{x}) = c_1x_1^k + \cdots + c_nx_n^k &= 0, \end{aligned}\right\} \tag{7}$$

with integer coefficients, have a non-trivial p-adic solution for all $p > Ck^8$ where C is some positive constant. Further, we may take $C = 38.39\ldots$

Wooley's conjecture implies that Theorem 1 should hold with $C = 1$. In this context the following variation on Theorem 1 may be of interest.

THEOREM 2. *Let $K \geq 3$. For $k \geq K$ and $n > 6k$ the equations* (7) *have a non-trivial p-adic solution for all $p \geq C_K k^8$ where $C_K \downarrow 1$ in such a way that $C_K = 1 + O(K^{-\frac{1}{2}})$.*

This paper was written whilst the third author (R. J. Cook) was a visitor in the mathematics department at the University of British Columbia. He is grateful to the department at the University of British Columbia for their kind hospitality.

2. Preliminary normalization

We begin by recalling the normalization procedure introduced by Davenport and Lewis (1969). With the forms f, g, h we associate the parameter

$$\theta = \theta(f, g, h) = \prod_{i,j,k} \Delta_{ijk} \tag{8}$$

where Δ_{ijk} denotes the determinant obtained from columns i, j, k of the matrix of coefficients, and (i, j, k) runs through all 3 element subsets of $\{1, 2, 3, \ldots, R\}$.

For a given system of forms with $\theta(f, g, h) \neq 0$ and a fixed prime p, there is a related p-normalized system of forms (f^*, g^*, h^*). Further the equations (7) have a non-trivial p-adic solution if and only if the equations $f^* = g^* = h^* = 0$ do. Also, by the p-adic compactness argument in section 4 of Davenport and Lewis (1969), it is sufficient to prove the theorem with the additional assumption that $\theta \neq 0$. We may now suppose that the forms f, g, h are p-normalized, with $\theta \neq 0$, and use the following property which is essentially Lemma 11 of Davenport and Lewis (1969).

LEMMA 1. *Let f, g, h be a p-normalized system of forms, with $\theta \neq 0$. Then we may write* (*after renumbering the variables*)

$$\left.\begin{aligned} f &= f_0 + pf_1, \\ g &= g_0 + pg_1, \\ h &= h_0 + ph_1. \end{aligned}\right\} \tag{9}$$

Here f_0, g_0, h_0, are forms in variables $x_1, \dots, x_m$ where

$$m \geq n/k. \tag{10}$$

Moreover, each of $x_1, \dots, x_m$ occurs in at least one of f_0, g_0, h_0 with a coefficient not divisible by p.

Further, if we form any ν linear combinations of f_0, g_0, h_0 (*these combinations being independent* mod p), *and denote by q_ν the number of variables that occur in one at least of these combinations with a coefficient not divisible by p, then*

$$q_\nu \geq \nu n/3k \tag{11}$$

for $\nu = 1, 2$.

Our next lemma is a version of Hensel's Lemma; it is essentially Lemma 9 of Davenport and Lewis (1969). (Since we have $p \geq k^8$, $p \nmid k$ and so we may take the parameter γ of Davenport and Lewis to be 1.)

LEMMA 2. *If $p \nmid k$ and the congruences*

$$\left.\begin{aligned} f_0 &= a_1x_1^k + \cdots + a_mx_m^k &\equiv 0 \mod p \\ g_0 &= b_1x_1^k + \cdots + b_mx_m^k &\equiv 0 \mod p \\ h_0 &= c_1x_1^k + \cdots + c_mx_m^k &\equiv 0 \mod p \end{aligned}\right\} \tag{12}$$

have a solution $\xi = (\xi_1, \dots, \xi_m)$ *for which the matrix*

$$\begin{pmatrix} a_1\xi_1 \dots a_m\xi_m \\ b_1\xi_1 \dots b_m\xi_m \\ c_1\xi_1 \dots c_m\xi_m \end{pmatrix} \tag{13}$$

has rank 3 mod p *then the equations* $f_0 = g_0 = h_0$ *have a non-trivial* p*-adic solution.*

3. Choosing a submatrix

For $n > 6k$ the inequalities (11) become

$$m > 6, \qquad q_1 > 2, \qquad q_2 > 4. \tag{14}$$

Let $\mu(d)$ denote the maximum number of columns of coefficients from (12) which lie in a d-dimensional subspace of $\mathbf{Z}_p^3$. Then

$$q_i = m - \mu(3-i) \tag{15}$$

and the inequalities (14) are equivalent to

$$m \geq 7, \qquad \mu(1) \leq m-5, \qquad \mu(2) \leq m-3, \tag{16}$$

so that in particular the congruences have rank 3.

Let A denote the matrix of coefficients in (13). For any subset J of $\{1, 2, \dots, m\}$ we denote by A_J the submatrix of A consisting of the columns c_j with $j \in A_J$. We write

$$\rho(A_J) = \text{rank of } A_J = \dim \operatorname{lin}\{\mathbf{c}_j : j \in J\} \tag{17}$$

Our next lemma is Lemma 1 of Low, Pitman and Wolff (1988).

LEMMA 3. *Let* A *be an* $r \times m$ *matrix over a field* K *and let* t *be a positive integer. Then* A *includes* t *disjoint* $r \times r$ *submatrices which are non-singular over* K *if and only if*

$$m - |J| \geq t(r - \rho(A_J)) \tag{18}$$

for all subsets J *of* $\{1, 2, \dots, m\}$.

In our context $r = 3$ and we take $t = 2$. Writing d for $\rho(A_J)$, (18) becomes

$$|J| \le m - 2(3 - d) \tag{19}$$

and from (16) we see that the matrix A contains two disjoint 3×3 non-singular matrices.

LEMMA 4. *If $p \not\equiv 1 \bmod k$ then the congruences* (13) *have a solution of rank* 3 mod p.

PROOF. In this case every residue mod$p$ is a k-th power residue and, after a substitution $y_i = x_i^k$, we may treat the congruences as linear equations in $\mathbb{Z}_p$. Relabelling the variables and using row operations we may take the matrix of coefficients as [IC] where I is the 3×3 identity and C is a $3 \times (m - 3)$ matrix of rank 3 mod p. We take $y_1 = y_2 = y_3 = 1$ and solve $C'_{\mathbf{y}} = -\mathbf{1}$ to give the required solution of rank 3.

Since the inequalities (16) are stronger than (19) we can do better than merely choosing two non-singular matrices from the coefficient matrix.

LEMMA 5. *Suppose that $m > 7$. Then either*

(i) *we can choose a subset of* 7 *columns which still have $q_1 \ge 3$ and $q_2 \ge 5$; or*

(ii) *we have $m = 8$, $\mu(1) = 3$ and $\mu(2) = 5$ in disjoint blocks; or*

(iii) *we can choose a subset of* 9 *columns which can be partitioned into* 3 *independent* 1*-dimensional subsets, each containing* 3 *columns.*

PROOF. The inequalities $q_1 \ge 3$ and $q_2 \ge 5$ are equivalent to $\mu(1) \le m - 5$ and $\mu(2) \le m - 3$. While $m > 7$ we reduce m to $m - 1$ using the following rule, which preserves these inequalities:

(i) If $\mu(1) < m - 5$ and $\mu(2) < m - 3$ we discard any column.

(ii) If $\mu(1) = m - 5$ and $\mu(2) < m - 3$ then there can be at most one 1-dimensional block of columns of length $m - 5$, for otherwise

$$\mu(2) \ge 2(m - 5) > m - 3$$

for $m > 7$. We discard a column from this longest 1-dimensional block of columns.

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

(iii) If $\mu(1) = m - 5$ and $\mu(2) = m - 3$ then, as before, there is a unique 1-dimensional block of length $m - 5$. Suppose that the 1-dimensional block and any 2-dimensional block of length $m - 3$ are disjoint, then

$$m \geq (m - 5) + (m - 3) = 2m - 8$$

so $m \leq 8$. Thus for $m > 8$ the 1-dimensional block of length $m - 5$ must sit inside any 2-dimensional block of length $m - 3$ and we discard a column from this longest 1-dimensional block. If $m = 8$ and the blocks are not disjoint then we still discard a column from this block, otherwise we arrive at part (ii) in the statement of the lemma.

(iv) Finally we have $\mu(1) < m - 5$ and $\mu(2) = m - 3$. If there were two disjoint 2-dimensional blocks of length $m - 3$ then $m \geq 2(m - 3)$ or $m \leq 6$. Thus any two 2-dimensional blocks must intersect in a 1-dimensional block. If there are only two blocks we discard a column from their intersection.

Now suppose that there are k such blocks B_i, $i = 1, \dots, k$, $k \geq 3$. Let B_1 and B_2 intersect in the 1-dimensional block B_0. If each of $B_3, \dots, B_k$ contains B_0 then we discard a column from this intersection B_0. Otherwise we may suppose that B_3 does not contain B_0. Let $|B_0| = \ell$, we choose a column $\mathbf{c}_0$ which generates B_0. We obtain B_i, $i = 1, 2$ by adjoining a column $\mathbf{c}_i$ and including an extra $m - 3 - \ell$ columns. Thus $B_1 \cup B_2$ contains

$$\ell + 2(m - 3 - \ell) = 2m - 6 - \ell \leq m$$

columns, so $\ell \geq m - 6$. Since $\mu(1) < m - 5$ we have $\ell = m - 6$ and $m - 3 - \ell = 3$. Further $B_1 \cup B_2$ contains all the m columns so we see that B_3 contains 6 columns, consisting of 3 multiples of $\mathbf{c}_1$ and 3 multiples of $\mathbf{c}_2$. Therefore $m - 5 > 3$, that is, $m \geq 9$ and we discard excess columns from B_0 to give 3 multiples of $\mathbf{c}_0$. Thus we arrive at case (iii) in the statement of the lemma.

LEMMA 6. *Let $p \equiv 1 \bmod k$, $p > k^4$. If $a_1a_2a_3 \not\equiv 0 \bmod p$ then*

$$a_1x_1^k + a_2x_2^k + a_3x_3^k \equiv 0 \bmod p \tag{20}$$

has a non-trivial solution (mod p).

This is essentially Lemma 2.4.1 of Dodson (1966).

LEMMA 7. *Let $p \equiv 1 \bmod k$, $p > k^6$. Suppose that for the congruences*

$$\left.\begin{aligned} a_1x_1^k + \cdots + a_5x_5^k &\equiv 0 \mod p \\ b_1x_1^k + \cdots + b_5x_5^k &\equiv 0 \mod p \end{aligned}\right\} \tag{21}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

at most 2 *columns of coefficients take any particular value for* $a_i/b_i \bmod p$, *and each column contains at least one non-zero entry. Then the congruences have a simultaneous solution of rank* 2 mod p.

This is proved in Section 3 of Atkinson and Cook (1989).

We now consider the cases (ii) and (iii) arising from Lemma 5. In case (ii) the system of congruences is equivalent to a system with coefficient matrix

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & 0 & 0 & 0 \\ b_1 & b_2 & b_3 & b_4 & b_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c_6 & c_7 & c_8 \end{bmatrix}.$$

There is a unique 1-dimensional subspace of length 3 so at most two of the ratios a_i/b_i take any particular value $\bmod p$. The system of congruences can then be solved using Lemmas 6 and 7, and the solution obtained has rank 3 $\bmod p$.

In case (iii) the system is equivalent to one with coefficient matrix

$$\begin{bmatrix} a_1 & a_2 & a_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b_4 & b_5 & b_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & c_7 & c_8 & c_9 \end{bmatrix}.$$

Solving three separate congruences, using Lemma 6, we obtain a simultaneous solution of rank 3 mod p.

Now we can choose a subset of 7 columns to give a system with

$$m = 7, \qquad q_1 \geq 3, \qquad q_2 \geq 5. \tag{22}$$

If we remove any column we have a set of 6 columns with $q_1' \geq 2$, $q_2' \geq 4$. From Lemma 3 we see that any 6 columns can be partitioned into 2 non-singular matrices $\bmod p$.

4. Exponential sums

We now count the number of solutions to a system of 3 congruences (12), satisfying (22), using exponential sums. The number N of solutions $\pmod p$ to the congruences (13) is given by

$$p^3 N = \sum_{u_1,u_2,u_3} \sum \sum_{(\bmod\ p)} T(\Lambda_1) \dots T(\Lambda_7) \tag{23}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

where

$$\Lambda_j = u_1 a_j + u_2 b_j + u_3 c_j \tag{24}$$

for $j = 1, \ldots, 7$ and

$$T(\Lambda) = \sum_{x \pmod p} e(\Lambda x^k / p). \tag{25}$$

Separating out the term $u_1 = u_2 = u_3 = 0$ in (23) we see that

$$p^3 N - p^7 = \sum \sum_{u \neq 0} \sum T(\Lambda_1) \ldots T(\Lambda_7) \tag{26}$$

We classify the points $u \not\equiv 0$ according to the number τ of linear forms Λ_j which are $0 \pmod p$. Since any six columns of coefficients contain two non-singular matrices, any 5 forms Λ_j must contain 3 independent forms. Therefore $\tau \leq 4$.

For $u \not\equiv 0 \pmod p$ we have, from Lemma 12 of Davenport (1963),

$$|T(u)| \leq (k-1)\sqrt{p}. \tag{27}$$

Let

$$S_2 = \sum_{u \neq 0} |T(u)|^2 \tag{28}$$

then, from Lemma 2.5.1 of Dodson (1966),

$$S_2 = (k-1)p(p-1). \tag{29}$$

Let $\sum_\tau$ denote the contribution to the right hand side of (26) coming from those points $\mathbf{u} \not\equiv \mathbf{0}$ with exactly τ forms $\Lambda_j \equiv 0$. Since $\mathbf{u} \not\equiv \mathbf{0}$ we have $\tau \leq 4$. Now

$$\left|\sum_0\right| \leq (k-1)\sqrt{p} \sum \sum \sum_0 |T(\Lambda_1) \ldots T(\Lambda_6)|. \tag{30}$$

The forms $\Lambda_1, \ldots, \Lambda_6$ can be partitioned into 2 sets, $\{\Lambda_1, \Lambda_2, \Lambda_3\}$, $\{\Lambda_4, \Lambda_5, \Lambda_6\}$ say, of 3 independent forms. Then

$$\begin{aligned} \left|\sum_0\right| &\leq (k-1)\sqrt{p} \left\{ \sum_{\mathbf{u} \neq \mathbf{0}} \sum \sum_0 |T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)|^2 \right\}^{1/2} \\ &\quad \times \left\{ \sum_{\mathbf{u} \neq \mathbf{0}} \sum \sum_0 |T(\Lambda_4)T(\Lambda_5)T(\Lambda_6)|^2 \right\}^{1/2}. \end{aligned} \tag{31}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

Now the mappings $(\Lambda_1, \Lambda_2, \Lambda_3) \to (u_1, u_2, u_3)$ and $(\Lambda_4, \Lambda_5, \Lambda_6) \to (u_1, u_2, u_3)$ are both bijections so both bracketed terms on the right are

$$\sum\sum\sum_{u_1, u_2, u_3 \neq 0} |T(u_1)T(u_2)T(u_3)|^2 = S_2^3. \tag{32}$$

Hence

$$\left|\sum_0\right| \leq (k-1)\sqrt{p}\{(k-1)p(p-1)\}^3 < k^4 p^{13/2}. \tag{33}$$

To estimate $\sum_\tau$, $\tau \geq 1$, we choose a form $\Lambda_k \not\equiv 0$ on the subset, say Λ_7. The remaining 6 forms can be partitioned into 2 subsets of 3 independent forms, say $\{\Lambda_1, \Lambda_2, \Lambda_3\}$ and $\{\Lambda_4, \Lambda_5, \Lambda_6\}$. Then the contribution of this set of τ forms $\Lambda_i \equiv 0$ to $\sum_\tau$ is bounded by

$$\begin{aligned}(k-1)\sqrt{p}&\left\{\sum\sum\sum_s |T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)|^2\right\}^{1/2} \\ &\times\left\{\sum\sum\sum_t |T(\Lambda_4)T(\Lambda_5)T(\Lambda_6)|^2\right\}^{1/2},\end{aligned} \tag{34}$$

where $s + t = \tau$ and s forms of the first set and t forms from the second set are $0 \bmod p$.

To estimate the first bracketed term we map the s forms $\Lambda_i \equiv 0$ onto $u_1, \ldots, u_s$ and the remaining forms in $\{\Lambda_1, \Lambda_2, \Lambda_3\}$ onto $u_{s+1}, \ldots, u_3$. Then the first bracketed term is

$$p^{2s}\sum_{u_s=1}^{p} \cdots \sum_{u_3=1}^{p} |T(u_{s+1}) \cdots T(u_3)|^2 = p^{2s} S_2^{3-s} < k^{3-s}p^6. \tag{35}$$

Hence the terms (34) are bounded by $k^{4-\tau/2}p^{13/2}$.

We now have to consider geometric properties of the seven columns of coefficients $\mathbf{c}_j$ (or forms Λ_j). Since any 6 columns can be partitioned into two non-singular matrices, no more than 4 columns can lie in a plane. Suppose that there are a pairs of linearly dependent columns, b sets of just 3 coplanar columns and c sets of 4 coplanar columns. Then, from (35),

$$\left|\sum_1 + \sum_2 + \sum_3 + \sum_4\right| \leq ((7-2a)k^{3/2} + ak + bk^{1/2} + c)k^2 p^{13/2}. \tag{36}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

With the geometric configuration of columns we associate the polynomial $ax^2 + bx + c$, and call two systems equivalent if they are associated with the same polynomial. We need to determine the dominant (largest) polynomial for each value $x \geq \sqrt{3}$. Let $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ denote the usual orthonormal basis for $\mathbb{R}^3$.

(i) $a = 3$. In this case the system is equivalent to $\mathbf{e}_1, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_3, \mathbf{c}_7 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$. Then $b = 3$, on taking $\mathbf{c}_7$ with any axis, and $c = 3$, on taking any pair of axes. Thus we obtain the polynomial

$$x^3 + 3x^2 + 3x + 3. \tag{37}$$

(ii) $a = 2$. In this case we can take $\mathbf{c}_1, \ldots, \mathbf{c}_5$ as $\mathbf{e}_1, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_2, \mathbf{e}_3$. If $c > 1$ then one or both of the remaining columns $\mathbf{c}_6$ and $\mathbf{c}_7$ must lie in the planes $x = 0$ or $y = 0$, or $\mathbf{c}_6$ and $\mathbf{c}_7$ are coplanar with $\mathbf{e}_1$ or $\mathbf{e}_2$. If both columns lie in these planes we obtain the polynomial $2x^2 + 2x + 3$. If just one column, $\mathbf{c}_6$ say, lies in a plane, $x = 0$ say, then we have the polynomials $2x^2 + 4x + 2$, when $\mathbf{c}_7$ is not in the $\mathbf{e}_1 - \mathbf{c}_6$ plane, or $2x^2 + 2x + 3$ if $\mathbf{c}_7$ is in the $\mathbf{e}_1 - \mathbf{c}_6$ plane. If $\mathbf{c}_6$ and $\mathbf{c}_7$ are coplanar with $\mathbf{e}_1$ we obtain the polynomials $2x^2 + 4x + 2$ if neither $\mathbf{c}_6$ nor $\mathbf{c}_7$ lies in the plane $x = 0$, $2x^2 + 2x + 3$ otherwise.

If neither $\mathbf{c}_6$ nor $\mathbf{c}_7$ lies in the planes $x = 0$ or $y = 0$ then $c = 1$ and b is maximized when $\mathbf{e}_3$, $\mathbf{c}_6$ and $\mathbf{c}_7$ are coplanar. This gives $b = 7$ by taking $\mathbf{c}_6$ or $\mathbf{c}_7$ with $\mathbf{e}_1$ or $\mathbf{e}_2$, $\mathbf{e}_1$ or $\mathbf{e}_2$ with $\mathbf{e}_3$ and the $\mathbf{e}_3, \mathbf{c}_6, \mathbf{c}_7$ plane; for example $\mathbf{c}_6, \mathbf{c}_7 = (1, 1, \pm 1)$. Thus the dominant polynomial in case (iii) is

$$3x^3 + 2x^2 + 7x + 1. \tag{38}$$

(iii) $a = 1$. We can take $\mathbf{c}_1, \ldots, \mathbf{c}_4$ as $\mathbf{e}_3, \mathbf{e}_3, \mathbf{e}_1, \mathbf{e}_2$. We have 3 coplanar columns either by taking $\mathbf{e}_3$ with one of $\mathbf{c}_3, \ldots, \mathbf{c}_7$, or if 3 of $\mathbf{c}_3, \ldots, \mathbf{c}_7$ are coplanar: say $\mathbf{c}_3, \mathbf{c}_5, \mathbf{c}_6$ and $\mathbf{c}_4, \mathbf{c}_6, \mathbf{c}_7$. Thus $b \leq 7$ and an example of this configuration is $\mathbf{c}_5 = (1, 1, 1)^T$, $\mathbf{c}_6 = (0, 1, 1)^T$ and $\mathbf{c}_7 = (1, 0, 1)^T$. When $b = 7$ no 4 columns are coplanar so $c = 0$.

If $c > 0$ then either 4 of $\mathbf{c}_3, \ldots, \mathbf{c}_7$ are coplanar, and we can take that plane as $z = 0$, or one of $\mathbf{c}_5, \ldots, \mathbf{c}_7$ lies in the planes $x = 0$ or $y = 0$. In the first case suppose $\mathbf{c}_5$ and $\mathbf{c}_6$ lie in the plane $z = 0$, depending on the position of $\mathbf{c}_7$ the polynomial is $x^2 + 5x + 1$ or $x^2 + 3x + 2$. If two columns, $\mathbf{c}_5$ and $\mathbf{c}_6$ lie respectively in the planes $x = 0$ and $y = 0$ then $c = 2$, taking $\mathbf{c}_7$ to be the intersection of the $\mathbf{e}_1 - \mathbf{c}_6$ and $\mathbf{e}_2 - \mathbf{c}_5$ planes we obtain $b = 3$ and the polynomial $x^2 + 3x + 2$. If just one column, $\mathbf{c}_6$ say, lies in a plane, $x = 0$ say, then $c \leq 3$ and also $b \leq 5$. Since $x \geq \sqrt{3}$ the dominant polynomial for case (iii) is

$$5x^3 + x^2 + 7x. \tag{39}$$

(iv) $a = 0$. If any coplanar sets exist we can take the first plane as $x = 0$ and, if any other plane exists we take it as $y = 0$. We can then take $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$ as $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. If at most one plane exists then the polynomial is $0, 1$, or x. Otherwise we can take $\mathbf{c}_4, \mathbf{c}_5$ as $\mathbf{e}_1 + \mathbf{e}_3$, $\mathbf{e}_2 + \mathbf{e}_3$ respectively, and position $\mathbf{c}_6$ and $\mathbf{c}_7$ to maximize b and c.

If $\mathbf{c}_6$ and $\mathbf{c}_7$ lie in the planes $x = 0$, $y = 0$ respectively then $b = 0$ and $c = 2$. If just one of them, $\mathbf{c}_5$ say, lies in the plane $x = 0$ then $c = 1$ and we maximize b, at $b = 2$, to lie on the intersection of two planes determined by the other columns, say the $\mathbf{e}_1 - \mathbf{c}_5$ and $\mathbf{e}_2 - \mathbf{c}_4$ planes. Now suppose that neither $\mathbf{c}_6$ nor $\mathbf{c}_7$ lies in the planes $x = 0$, $y = 0$. If $\mathbf{c}_6$ and $\mathbf{c}_7$ lie in a set of 4 coplanar vectors then, reversing the roles of $\mathbf{e}_1, \mathbf{c}_4$ and $\mathbf{e}_2, \mathbf{c}_5$ if necessary, both $\mathbf{c}_6$ and $\mathbf{c}_7$ lie in the plane $z = 0$. Thus $c = 1$ and $b \leq 3$ (when $\mathbf{c}_6$ lies in the $\mathbf{c}_4 - \mathbf{c}_5$ plane).

Finally, no 4 vectors are coplanar, so $c = 0$. We maximize b when each of $\mathbf{c}_6$ and $\mathbf{c}_7$ lies in a plane formed by the other columns and the plane determined by $\mathbf{c}_6$ and $\mathbf{c}_7$ also contains one of the other columns; for example $\mathbf{c}_6$ in $\mathbf{e}_2 - \mathbf{c}_4$ planes, $\mathbf{c}_7$ in the $\mathbf{e}_3 - \mathbf{c}_6$ and $\mathbf{e}_1 - \mathbf{e}_2$ planes. Thus $b \leq 6$ and the dominant polynomial of this case is

$$7x^3 + 6x. \tag{40}$$

The dominant polynomial, in the region $x \geq 1$ is (40). We take $k = x^2$ and see, from (36), that

$$\left| \sum_1 + \sum_2 + \sum_3 + \sum_4 \right| \leq (7k^{3/2} + 6k^{1/2})k^2 p^{13/2}. \tag{41}$$

5. Singular solutions

Finally, we estimate the number of solutions to the congruences (12) which do not have rank 3. Suppose that we have a solution of rank $\nu > 0$ with t variables non-zero, then $\nu + 1 \leq t \leq 2\nu$. We can transform the section of coefficients on these t columns into the shape [IB] where I is the $\nu \times \nu$ identity matrix and B is a $\nu \times (t - \nu)$ matrix, using row operations and relabelling the variables. The variables corresponding to the columns in B can be chosen freely, $(p-1)^{t-\nu}$ choices, and this determines the variables corresponding to I up to the kth powers, k^ν choices. Thus the total number of solutions with these parameters t, ν is at most

$$\binom{7}{t} k^\nu (p-1)^{t-\nu}. \tag{42}$$

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

Summing over the possible values of $\nu < 3$ and t, the total number of singular solutions is bounded by

$$1+\sum_{\nu=1}^{2}\sum_{t=\nu+1}^{2\nu}\binom{7}{t}k^{\nu}(p-1)^{t-\nu} < 1+21kp+35kp^2+35k^2p+35k^2p^2$$

$$(43) \qquad < 48k^2p^2$$

provided that $k \geq 3$ and $p \geq k^8$.

Thus the congruences (12) will have the required solution of rank 3 if

$$p^4-(k^2+7k^{3/2}+6k^{1/2})k^2p^{13/2} > 48k^2p^2$$

or

$$(44) \qquad p-(k^2+7k^{3/2}+6k^{1/2})k^2p^{1/2} > 48k^2p^{-1}.$$

For $p \geq k^8$ the right side is bounded above by $48k^{-6} < 0.066$ as $k \geq 3$. For $p \geq Ck^8$ the left side is bounded below by

$$(45) \qquad C^{1/2}k^8(C^{1/2}-(1+7k^{-1/2}+6k^{-3/2}))$$

so we have the required solution if C is chosen suitably large. For $k \geq 3$ we take $C > (1+3\sqrt{3})^2 \simeq 38.39$. For $k \geq K$ we choose

$$(46) \qquad C_K = (1+7K^{-1/2}+6K^{-3/2})^2+K^{-2} = 1+O(K^{-\frac{1}{2}}).$$

to complete the proof of the theorems.

References

Aigner, M. (1979), *Combinatorial Theory*, (Springer, Berlin).

Atkinson, O. D. and Cook, R. J. (1989), 'Pairs of additive congruences to a large prime modulus', *J. Austral. Math. Soc. Series A* **46**, 438–455.

Davenport, H. (1963), *Analytic methods for Diophantine equations and Diophantine inequalities*, (Campus Publishers, Ann Arbor).

Davenport, H. and Lewis, D. J. (1969), 'Simultaneous equations of additive type', *Philos. Trans. Roy. Soc. London Ser. A* **264**, 577–595.

Dodson, M. M. (1966), 'Homogeneous additive congruences', *Philos. Trans. Roy. Soc. London Ser. A* **261**, 163–210.

Dörner, E. (1990), 'Simultaneous diagonal equations over certain p-adic fields', *J. Number Theory* **36**, 1–11.

Ellison, F. (1973), 'Three diagonal quadratic forms', *Acta Arith.* **23**, 137–151.

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press

Low, L., Pitman, J. and Wolff, A. (1988), 'Simultaneous diagonal congruences', *J. Number Theory* **29**, 31–59.
Schmidt, W. M. (1984), 'The solubility of certain p-adic equations', *J. Number Theory* **19**, 63–80.
Wooley, T. D. (1990), 'On simultaneous additive equations III', *Mathematika* **37**, 85–96.

https://doi.org/10.1017/S1446788700034091 Published online by Cambridge University Press