J. Austral. Math. Soc. (*Series A*) **46** (1989), 438–455

PAIRS OF ADDITIVE CONGRUENCES TO A LARGE PRIME MODULUS

O. D. ATKINSON AND R. J. COOK

(Received 13 October 1987; revised 11 May 1988)

Communicated by J. H. Loxton

Abstract

This paper is concerned with non-trivial solvability in p-adic integers, for relatively large primes p, of a pair of additive equations of degree $k > 1$:

$$f(\mathbf{x}) = a_1x_1^k + \cdots + a_nx_n^k = 0,$$
$$g(\mathbf{x}) = b_1x_1^k + \cdots + b_nx_n^k = 0,$$

where the coefficients $a_1, \ldots, a_n, b_1, \ldots, b_n$ are rational integers.

Our first theorem shows that the above equations have a non-trivial solution in p-adic integers if $n > 4k$ and $p > k^6$. The condition on n is best possible.

The later part of the paper obtains further information for the particular case $k = 5$. Specifically we show that when $k = 5$ the above equations have a non-trivial solution in p-adic integers (a) for all $p > 3061$ if $n \geq 21$; (b) for all p except $p = 5, 11$ if $n \geq 26$.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 D 88.

1. Introduction

It is well known (see, for example, Chapter 1 of Borevich and Shafarevich [3]) that the number of solutions of a polynomial congruence

$$F(x_1, \ldots, x_n) \equiv 0 \quad \mod p$$

may be estimated using exponential sums. For an additive form

$$(1) \qquad a_1x_1^k + \cdots + a_nx_n^k \equiv 0 \quad \mod p,$$

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

where $p \nmid a_1 \cdots a_n$, it follows from Theorem B of Borevich and Shafarevich [3, page 15] that the number N of solutions of (1) satisfies

$$|N - p^{n-1}| \leq Cp^{(n/2)-1}, \tag{2}$$

with $C = (k-1)^n$. Therefore a congruence

$$ax^k + by^k + cz^k \equiv 0 \quad \bmod p,\ p \nmid abc, \tag{3}$$

has a non-trivial solution for all $p > k^6$. The condition on p may be improved to $p > k^4$ (see Theorem 1 of Chowla [4] or Lemma 2.4.1 of Dodson [17]).

Before considering pairs of additive equations we recall some of the results on the p-adic solvability of a single additive equation

$$f(\mathbf{x}) = a_1 x_1^k + \cdots + a_n x_n^k = 0, \tag{4}$$

with coefficients in $\mathbf{Z}$. For quadratic forms ($k = 2$) the equation has a non-trivial solution in p-adic integers for every prime p provided that $n \geq 5 = 2.2 + 1$. This result is best possible since when $n = 4$ and $p \equiv 3 \bmod 4$ the equation

$$x_1^2 + x_2^2 + p(x_3^2 + x_4^2) = 0 \tag{5}$$

has no non-trivial solution in p-adic integers.

For $k = 3$ Lewis [20] showed that (4) has a non-trivial solution in p-adic integers for every prime provided that $n \geq 7 = 2.3 + 1$. In order to see that the condition $n \geq 7$ is best possible, let p be any prime with $p \equiv 1 \bmod 3$ and let q be a cubic non-residue $\bmod p$. Then the equation

$$(x_1^3 - qy_1^3) + p(x_2^3 - qy_2^3) + p^2(x_3^3 - qy_3^3) = 0 \tag{6}$$

has no non-trivial solution in p-adic integers.

For $k = 5$, Gray [19] showed that (4) has a solution in every p-adic field provided that $n \geq 16 = 3.5 + 1$. This is best possible since the equation

$$\sum_{i=1}^{5} 11^{i-1}(x_i^5 + 2y_i^5 + 4z_i^5) = 0 \tag{7}$$

has no non-trivial solution in 11-adic integers.

Davenport and Lewis [11] showed that for any $k > 1$ the equation (4) has a non-trivial solution in p-adic integers provided that $n \geq k^2 + 1$. This is best possible for any exponent k such that $k = p - 1$ for some prime p, as can be seen from a generalization of the example (5); see [11, page 454].

The next theorem is a "folklore" result, which does not seem to appear explicitly in the literature. It follows on combining the arguments of Davenport and Lewis [11] with the result for congruence (3), and the proof is left to the reader.

THEOREM A. *Let $n \geq 2k+1$. A single additive equation* (4) *has a non-trivial solution in p-adic integers for all $p > k^4$.*

A generalization of the example (6) shows that the condition $n \geq 2k+1$ is best possible. The interest of the result is that the problem of p-adic solvability is reduced to a finite, and explicit, question; for a given equation the remaining primes can be dealt with by a computer.

Our aim here is to produce an analogue of Theorem A for pairs of additive equations and to exploit this further in the case $k = 5$. To gain some idea of what may be feasible for given k and large primes p we consider a generalization of the example (6). For any exponent k and any prime $p \equiv 1 \bmod k$, let q be a kth power non-residue mod p. Then the equation

$$\sum_{i=1}^{k} p^{i-1}(x_i^k - qy_i^k) = 0 \tag{8}$$

has no non-trivial solution in p-adic integers. We consider (8) together with a "disjoint copy" of (8) (the equation obtained by replacing x_i, y_i with new variables x_i', y_i' for $i = 1, \dots, k$). This gives a pair of equations in $4k$ variables which have no non-trivial solution in p-adic integers, no matter how large p is. Thus in order to generalize Theorem A to a pair of additive equations we must at least assume that $n \geq 4k+1$.

For $k = 2$, two quadratic equations (not necessarily additive) have a non-trivial solution in p-adic integers for all primes p provided that $n \geq 9$ (see Demyanov [16]), and this result is best possible. For $k = 3$, Davenport and Lewis [12] showed that two additive equations

$$\begin{aligned} f(\mathbf{x}) &= a_1x_1^k + \cdots + a_nx_n^k = 0, \qquad a_i \in \mathbf{Z}, \\ g(\mathbf{x}) &= b_1x_1^k + \cdots + b_nx_n^k = 0, \qquad b_i \in \mathbf{Z}, \end{aligned} \tag{9}$$

have a non-trivial solution in p-adic integers for every prime p provided that $n \geq 16$. They also gave a counterexample with $n = 15$ and $p = 7$ showing that this is best possible. More recently, Cook [7] has shown that for all $p \neq 7$ a sufficient condition is $n \geq 13 = 4.3+1$. In view of the example (8), and the remarks following it, this result is best possible; if we reduce n to 12 there are infinitely many primes p ($p \equiv 1 \bmod 3$) for which we have counterexamples.

Davenport and Lewis [14] studied the case of two additive equations (9) with an exponent $k > 1$, obtaining sufficient conditions for the equations to have a non-trivial solution in p-adic integers for every prime p. For odd k they showed that $n \geq 2k^2+1$ variables are sufficient, but for even k they were only able to prove that $n \geq 7k^3$ variables would suffice.

THEOREM 1. *Let $n > 4k$. Any two additive equations* (9) *of degree k with integer coefficients a_i, b_i have a non-trivial solution in p-adic integers for all* *primes $p > k^6$. Further this result is best possible in the sense that it fails to hold when $n = 4k$.*

The last sentence of Theorem 1 follows from the remarks following the example (8). We also note that Theorem 1 follows from the results of Demyanov [16] when $k = 2$ and Cook [7] when $k = 3$, so we may suppose that $k > 3$. The case $k = 5$ has already been investigated in some detail by Cook [8,9] who showed that $n \geq 31$ variables will suffice expect possibly when $p = 11$. Moreover, consideration of two disjoint copies of the equation (7), in a total of 30 variables, shows that the best possible condition for such a result covering all primes p would be $n \geq 31$. However, for $p = 11$ Cook [9] was only able to show that $n \geq 41$ variables will suffice.

We investigate those primes p for which the condition $n \geq 21 = 4.5 + 1$ is sufficient. Theorem 1 deals with those primes $p > 5^6 = 15625$. Some primes $p < 5^6$ may be dealt with by explicitly calculating exponential sums, and appropriate computer investigation deals with other cases. The primes p for which $n \geq 26 = 5.5 + 1$ is sufficient were also investigated by similar methods. The results are summarized in the following theorem.

THEOREM 2. *In the case $k = 5$ the equations* (9) *have a non-trivial solution in p-adic integers*

(a) *for all $p > 3061$ when $n \geq 21$;*

(b) *for all p except $p = 5, 11$ if $n \geq 26$.*

When $p = 11$ we have already constructed an example in 30 variables having no non-trivial solutions. Computer searches have revealed examples which may be used to construct similar counterexamples in 25 variables for $p = 31$ and 41. These are listed at the end of this paper.

Apart from their intrinsic interest, p-adic solutions are an essential preliminary to any application of the Hardy-Littlewood method. In the case $k = 3$, Davenport and Lewis [12] showed that two additive cubic equations have a non-trivial simultaneous solution in rational integers provided that $n \geq 18$. Subsequently '18' was reduced to '17' by Cook [6] and '16' by Vaughan [24]. In view of the counterexample of Davenport and Lewis [12] with $n = 15$ and $p = 7$ this is the best that could be done without making some 7-adic assumption. More recently, Baker and Brüdern [2] have shown, using the p-adic results of Cook [7], that 15 variables are sufficient if we assume the existence of non-singular 7-adic solutions. Atkinson [1] has classified those pairs of additive cubic equations in $n = 13, 14$ or 15 variables which do not have 7-adic solutions.

The Hardy-Littlewood method requires the existence of non-singular (not just non-trivial) p-adic solutions. In view of the recent advances in this method, see for example Vaughan [25], we state (without proof) an appropriate version of Theorem 1. The point here being that this reduces any p-adic assumptions to a finite (and explicit) set of primes.

THEOREM 3. *Let $p > k^4$ and suppose that the equations* (10) *have a non-trivial p-adic solution. If every form $\lambda f + \mu g, (\lambda, \mu \neq 0, 0)$ in the pencil of f and g has at least $2k+1$ variables with non-zero coefficients then the equations have a non-singular p-adic solution.*

The proof mimics the proofs of Theorem 2 of Davenport and Lewis [14] except that we appeal to Theorem A instead of their result [11] on additive forms in $k^2 + 1$ variables.

One question which naturally arises is how these results generalize to $R > 2$ simultaneous equations. An example given by Davenport and Lewis [13, Section 4] shows that the generalization is not straightforward. The p-adic results obtained by Davenport and Lewis [15] for R simultaneous equations required $[9R^2k \log 3Rk]$ variables when k is odd, and $[48R^2k^3 \log 3Rk^2]$ variables when k is even. These results have recently been improved upon by Schmidt [22] and Low, Pitman and Wolff [21].

When $R = 3$ the "Artin question" is whether $3k^2+1$ variables are sufficient to ensure non-trivial p-adic solutions for every prime p. In the case $k = 2$ this was proved by Ellison [19]. When $k = 3$ Stevenson [23] showed that, except possibly for $p = 3$ or 7, $n \geq 28$ variables are sufficient. More recently Atkinson [1] has shown that 25 variables are sufficient to ensure non trivial p-adic solutions of three additive cubics in every p-adic field, except possibly $p = 3$ or 7.

We are indebted to the referee for many useful comments which have improved the exposition of our results.

2. Preliminaries to Theorem 1

We begin by recalling a normalisation procedure introduced by Davenport and Lewis [12, 14, 15]. With a pair (9) of additive forms f, g we associate the parameter

$$\theta = \theta(f, g) = \prod_{i \neq j}(a_i b_j - a_j b_i). \tag{10}$$

For a given pair of forms with $\theta(f, g) \neq 0$ and a fixed prime p, there is a related p-normalized pair of forms (f^*, g^*). Further the equations $f = g = 0$

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

have a non-trivial p-adic solution if and only if the equations $f^* = g^* = 0$ do. Also, by the p-adic compactness argument in Davenport and Lewis [14, Section 5], it is sufficient to prove Theorem 1 with the additional assumption that $\theta \neq 0$. We may now suppose that the forms f, g are p-normalized, with $\theta \neq 0$, and use the following property which is essentially Lemma 2 of Davenport and Lewis [12].

LEMMA 1. *Let f and g be a p-normalized pair of forms. Then we may write*

$$f = f_0 + pf_1, \qquad g = g_0 + pg_1. \tag{11}$$

Here f_0, g_0 are forms in $m \geq n/k$ variables, each of which occurs in one at least of f_0, g_0 with a coefficient not divisible by p. Further, if q denotes the minimum number of variables occuring explicitly in any form $\lambda f_0 + \mu g_0$ (λ, μ not both divisible by p) with a coefficient not divisible by p, then $q \geq n/2k$.

Our next lemma is a version of Hensel's Lemma; it is Lemma 7 of Davenport and Lewis [14].

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

$$\begin{aligned} f_0 &= a_1 x_1^k + \cdots + a_m x_m^k \equiv 0 \mod p, \\ g_0 &= b_1 x_1^k + \cdots + b_m x_m^k \equiv 0 \mod p \end{aligned} \tag{12}$$

have a solution $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ for which the matrix

$$\begin{pmatrix} a_1\xi_1 \cdots a_m\xi_m \\ b_1\xi_1 \cdots b_m\xi_m \end{pmatrix} \tag{13}$$

has rank 2 (mod p) *then the equations $f_0 = g_0 = 0$ have a non-trivial solution in p-adic integers.*

In the proof of Theorem 1 we have $p > k^6$ so $p \nmid k$. It is therefore sufficient to show that the congruences (12) have a solution of rank 2 (mod p). We may also suppose that $p \equiv 1 \mod k$, see Lemma 3 of Davenport and Lewis [9]; similarly we may suppose that $p \equiv 1 \mod 5$ for Theorem 2.

Since $n > 4k$, Lemma 1 gives the bounds $m \geq 5, q \geq 3$. We partition the variables $x_1, \ldots, x_m$ into blocks such that in each block the ratios a_i/b_i are equal (mod p). Let r be the length of the longest block of common ratios a_i/b_i. We note that replacing f_0, g_0 by suitable linear combinations we may take $a_i/b_i =$ "1/0" for these r variables. Further, let t be the length of the second longest block of common ratios. We may take the ratios in this block to be "0/1".

We assert that if $t \geq 3$ then the congruences (12) have a common solution of rank 2. This follows from our remarks on the single congruence (3) since the congruences (12) contain two disjoint congruences in 3 variables. Now we assume that $t \leq 2$ and reduce m from its initial value to 5 by discarding variables from the longest block of common ratios. We end up with a pair of congruences (12) satisfying

$$m = 5, \qquad q \geq 3 \quad \text{and} \quad r \leq 2 \tag{14}$$

since $r = m - q$.

3. Exponential sums

Since $r \leq 2$ we may renumber the variables in (12) so that $\{a_1/b_1, a_2/b_2\}$ and $\{a_3/b_3, a_4/b_4, a_5/b_5\}$ are sets of unequal ratios mod p. We count the number N of solutions of the congruences (12) using exponential sums:

$$N = p^{-2} \sum_{u_1, u_2 \bmod p}\sum T(\Lambda_1) \cdots T(\Lambda_5) \tag{15}$$

where

$$\Lambda_j = u_1 a_j + u_2 b_j, \qquad j = 1, \dots, 5, \tag{16}$$

$$T(\Lambda) = \sum_{x \bmod p} e(\Lambda x^5/p), \tag{17}$$

and $e(\theta) = \exp(2\pi i\theta)$.

Separating out the term $u_1 = u_2 = 0$ in (15) we find that

$$N - p^3 = p^{-2} \sum{}' T(\Lambda_1) \cdots T(\Lambda_5) \tag{18}$$

$$= p^{-2} \left(\sum\nolimits_1 + \sum\nolimits_2\right) \tag{19}$$

where $\sum'$ denotes the omission of the term $u_1 = u_2 = 0$, $\sum_1$ is the sum over those terms for which no $\Lambda_i \equiv 0$ and $\sum_2$ is the sum over those terms $(u_1, u_2) \neq (0, 0)$ for which some $\Lambda_i \equiv 0$.

Now

$$\left|\sum\nolimits_1\right|^2 \leq \sum\nolimits_1 |T(\Lambda_1)T(\Lambda_2)|^2 \cdot \sum\nolimits_1 |T(\Lambda_3)T(\Lambda_4)T(\Lambda_5)|^2. \tag{20}$$

We put

$$S_r = \sum_{u=1}^{p-1} |T(u)|^r. \tag{21}$$

Since Λ_1, Λ_2 are independent linear forms the mapping $(\Lambda_1, \Lambda_2) \to (u_1, u_2)$ is a bijection and therefore

$$(22)\quad \sum\nolimits_1 |T(\Lambda_1)T(\Lambda_2)|^2 \le \sum_{\Lambda_1\Lambda_2\not\equiv 0} |T(\Lambda_1)T(\Lambda_2)|^2 = \sum\nolimits_1 |T(u_1)T(u_2)|^2 = S_2^2.$$

Similarly, using Hölder's inequality, we have

$$(23)\quad \begin{aligned} \sum\nolimits_1 |T(\Lambda_3)T(\Lambda_4)T(\Lambda_5)|^2 &\le \max_{\Lambda_i\not\equiv\Lambda_j} \sum\nolimits_1 |T(\Lambda_i)T^2(\Lambda_j)|^2 \\ &= \sum_{u_1} |T(u_1)|^2 \cdot \sum_{u_2} |T(u_2)|^4 = S_2 S_4. \end{aligned}$$

Thus

$$(24)\quad \left|\sum\nolimits_1\right| \le S_2^{3/2} S_4^{1/2}.$$

In order to estimate $\sum_2$ suppose first that the ratio $a_5/b_5 \bmod p$ occurs only once amongst the a_i/b_i. Then the contribution of the points (u_1, u_2) with $\Lambda_5 \equiv 0$ to $\sum_2$ is at most

$$(25)\quad \begin{aligned} p \sum_{\Lambda_5\equiv 0} |T(\Lambda_1)\cdots T(\Lambda_4)| &\le p \max_{i\ne 5} \sum_{\Lambda_5\equiv 0} |T(\Lambda_i)|^4 \\ &= p\sum_{u=1}^{p-1} |T(u)|^4 = pS_4, \end{aligned}$$

since the mapping $(\Lambda_i, \Lambda_5) \to (u_1, u_2)$ is a bijection. If the ratio a_5/b_5 occurs twice amongst the a_i/b_i a similar argument shows that the contribution is at most $p^2 S_3$. Thus

$$(26)\quad \left|\sum\nolimits_2\right| \le \max(5pS_4, 3pS_4 + p^2S_3, pS_4 + 2p^2S_3).$$

Now (see Dodson [17, Lemma 2.5.1]),

$$(27)\quad S_2 = (k-1)p(p-1)$$

and (see Davenport [10, Lemma 12])

$$(28)\quad |T(u)| \le (k-1)\sqrt{p}, \quad u \not\equiv 0 \mod p$$

so that

$$(29)\quad |S_3| < (k-1)^2 p^{5/2}$$

and

$$(30)\quad |S_4| < (k-1)^3 p^3.$$

Hence

$$(31)\quad \begin{aligned} p^{-2}\left|\sum\nolimits_1 + \sum\nolimits_2\right| &< p^{-2}\{(k-1)^3p^{9/2} + 2(k-1)^2p^{9/2} + (k-1)^3p^4\} \\ &< k^3p^{5/2}, \end{aligned}$$

since $p > k^6$.

Any solution of rank 1 occurs in a pair of linearly dependent columns and since $r \leq 2$ there are at most 2 such pairs of columns, each pair giving $5(p-1)$ solutions. Further there is one solution of rank 0 and so at most $10p-9$ solutions of rank < 2. Thus we obtain the required solution of rank 2 provided that $p^3 - k^3 p^{5/2} \geq 10p$.

This is equivalent to

$$h(p,k) = p^2 - k^3 p^{3/2} - 10 \geq 0, \tag{32}$$

and, for fixed k, $h(p,k)$ is an increasing function of p so it is enough to verify (32) when $p = k^6 + 1$:

$$k^{12} + 2k^6 - 9 - k^{12}(1+k^{-6})^{3/2} \geq 0$$

or

$$(1 + 2k^{-6} - 9k^{-12})^2 \geq (1+k^{-6})^3.$$

Writing y for k^6, we obtain $H(y) = y^3 - 17y^2 - 37y + 81 \geq 0$. Now $H' \geq 0$ for $y \geq 37/3$ and the inequality is easily verified for $y \geq 2^6 = 64$, which completes the proof of Theorem 1.

4. Preliminary remarks for Theorem 2

After Theorem 1, we only need to consider those primes $p < 5^6 = 15625$. The quintic residues mod p form a cyclic subgroup of the non-zero residue classes, and the value of the exponential sum $T(u)$ depends only on the coset in which u lies. For each prime $p \equiv 1 \bmod 5$ with $p \leq 15625$ we find the least quintic non-residue q mod p, using a computer. Then $S = \{1, q, q^2, q^3, q^4\}$ is a set of representatives from the 5 cosets. Using double precision Fortran we calculate the absolute values of the exponential sums

$$T_i = \left| \sum_{x \bmod p} e(q^{i-1}x^5/p) \right|, \qquad i = 1, \ldots, 5, \tag{33}$$

and these values are checked using the identity

$$\sum_{i=1}^{5} T_i^2 = 20p. \tag{34}$$

As u runs through $1, 2, \ldots, p-1$ it falls into each coset exactly $(p-1)/5$ times and so

$$S_r = \left(\frac{p-1}{5}\right) \sum_{i=1}^{5} T_i^r. \tag{35}$$

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

In this way we calculate $S_2(= 4p(p-1)), S_3$ and S_4 exactly, and compute the bound

$$B = S_2^{3/4} S_4^{1/2} + \max(5pS_4, 3pS_4 + p^2 S_3, pS_4 + 2p^2 S_3) \tag{36}$$

for $\sum_1 + \sum_2$. Then, checking the primes up to 15625 we obtain

$$p^3 - p^{-2} B \geq 10p \quad \text{for } 6800 < p \leq 15625 \tag{37}$$

which leads to the required solution of rank 2.

We now take $p \equiv 1 \bmod 5$ to be a fixed prime in the range

$$11 < p \leq 6800. \tag{38}$$

We find the least quintic non-residue q mod p and put

$$S = \{1, q, \ldots, q^4\}. \tag{39}$$

LEMMA 3. *Let* $p \equiv 1 \bmod 5$, $p > 11$. *If* $abc \not\equiv 0 \bmod p$ *then*

$$ax^5 + by^5 + cz^5 \equiv d \qquad \bmod p \tag{40}$$

has a solution, which is non-trivial if $d \equiv 0 \bmod p$.

PROOF. For $d \not\equiv 0 \bmod p$ this follows from Theorem 3 of Chowla, Mann and Straus [5]. Now $d \equiv 0 \bmod p$ and for $p > 625$ the result follows from Theorem 1 of I Chowla [3] (or Lemma 2.4.1 of Dodson [17]).

For $11 < p \leq 625$, using substitutions $x \to \alpha x$, we may assume that $a, b, c \in S$. This result is obvious unless a, b, c are unequal and we may suppose that

$$1 = a < b < c. \tag{41}$$

Thus for each prime p there are only 6 cases to consider and the result is easily verified by computer.

5. Proof of Theorem 2(a)

The normalization process described in Section 2 results in a pair of forms with $m = 5, q \leq 3$ and $r \leq 2$, which we can write in the form

$$\begin{aligned} f_0 &= x_1^5 + a_2 x_2^5 + \cdots + a_4 x_4^5 && \equiv 0 \quad \bmod p, \\ g_0 &= \qquad\qquad b_3 x_3^5 + \cdots + x_5^5 && \equiv 0 \quad \bmod p \end{aligned} \tag{42}$$

where possibly $a_4 \equiv 0 \bmod p$ but $a_3 \not\equiv 0 \bmod p$, and $a_2, b_3, b_4 \in S$. In this section we consider the case $r = 2$.

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

LEMMA 4. *Let* $p \equiv 1 \bmod 5$, $p \geq 101$. *If* $abc \not\equiv 0 \bmod p$ *then the congruence*

$$ax^5 + by^5 + cz^5 \equiv d \mod p \tag{43}$$

has a solution with $xyz \not\equiv 0 \bmod p$.

PROOF. We count the number N_1 of solutions of (43) using exponential sums:

$$|N_1 - p^2| \leq p^{-1} S_3 \leq 16(p-1)\sqrt{p}, \tag{44}$$

using (27) and (28).

When $x \equiv 0$ the congruence (43) becomes

$$by^5 + cz^5 \equiv d \mod p. \tag{45}$$

For any given value y there are at most 5 solutions for z, so the number of solutions of (43) with $xyz \equiv 0 \bmod p$ is at most $15p$. We have

$$N_1 \geq p^2 - 16p^{3/2} > 15p \tag{46}$$

for $p \geq 291$.

For $101 \leq p < 291$ we take $a, b, c \in S$ with

$$1 = a \leq b \leq c \tag{47}$$

(after substitutions $x \to \alpha x$). The result is now easily verified by computer.

LEMMA 5. *Let* $p \equiv 1 \bmod 5, p \geq 101$. *If* $r = 2$ *then the congruences* (42) *have a solution of rank* 2 $\bmod p$.

PROOF. We begin by solving

$$b_3 x_3^5 + b_4 x_4^5 + x_5^5 \equiv 0 \mod p \tag{48}$$

with $x_3 x_4 x_5 \not\equiv 0 \bmod p$. This solution involves 2 linearly independent columns of coefficients.

Let

$$A = a_3 x_3^5 + a_4 x_4^5. \tag{49}$$

If $A \equiv 0$ we take $x_1 = x_2 = 0$ to give the required solution. Otherwise we multiply x_3, x_4, x_5 by ξ and solve

$$x_1^5 + a_2 x_2^5 + A\xi^5 \equiv 0 \mod p \tag{50}$$

with $x_1 x_2 \xi \not\equiv 0 \bmod p$ to give the required solution.

We now take t to be the length of the second longest block of common ratios $a_i/b_i \bmod p$.

Lemma 6. *Let* $p \equiv 1 \bmod 5, p > 11$. *If* $r = 2, t = 1$ *and* a_2 *is a quintic non-residue* mod p *then the congruences* (42) *have a solution of rank* 2 mod p.

Proof. This is a repetition of Lemma 5 except that the solution of (48) is non-trivial, but still involves two linearly independent columns, and the solution of (50) has $\xi \not\equiv 0$ since a_2 is a quintic non-residue.

We are now left with the cases

$$p = 31, 41, 61 \quad \text{or} \quad 71; \tag{51}$$

either $r = 2, t = 2$, and then

$$f_0 = x_1^5 + a_2x_2^5 + a_3x_3^5, \tag{52}$$

$$g_0 = \qquad b_3x_3^5 + b_4x_4^5 + x_5^5 \tag{53}$$

where $a_2, b_3, b_4 \in S, a_3 \not\equiv 0 \bmod p$;

or $r = 2, t = 1, a_2 = 1$, and then

$$f_0 = x_1^5 + x_2^5 + a_3x_3^5 + a_4x_4^5 \tag{54}$$

$$g_0 = \qquad b_3x_3^5 + b_4x_4^5 + x_5^5, \tag{55}$$

where $b_3, b_4 \in S, a_3a_4 \not\equiv 0 \bmod p$.

For a fixed prime p there 25 forms g_0 to consider. For each g_0 we begin by forming a list of all solutions of $g_0 \equiv 0 \bmod p$. We then run through $5(p-1)$ forms f_0 of the first type (52) and $(p-1)^2$ forms f_0 of the second type (54). The computer then runs through the list of solutions of $g_0 \equiv 0 \bmod p$ until it finds one which is also a solution of $f_0 \equiv 0 \bmod p$ and which has rank 2. In this way a computer search revealed the counterexample listed in Section 8.

6. Theorem 2(a): the case $r = 1$

In this case any non-trivial solution has rank 2 mod p. We begin by writing the congruences as

$$\begin{aligned} f_0 &= x_1^5 + a_2x_2^5 + \cdots + a_5x_5^5 \equiv 0 \mod p, \\ g_0 &= \qquad b_2x_2^5 + \cdots + b_5x_5^5 \equiv 0 \mod p, \end{aligned} \tag{56}$$

where $b_2, \ldots, b_5 \in S$.

Suppose first that $b_2, \ldots, b_5$ consist of two pairs of equal values, say $b_2 = b_3$ and $b_4 = b_5$. We take $x_2 = -x_3 = u, x_4 = -x_5 = v$ and the non-trivial solution of

$$x_1^5 + (a_2 - a_3)u^5 + (a_4 - a_5)v^5 \equiv 0 \mod p \tag{57}$$

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

gives the required solution of rank 2. (The coefficients are non-zero since $r = 1$.) Now we may assume that for any form g^* in the pencil generated by f_0, g_0 and having one zero coefficient, the 4 non-zero coefficients do not all lie in the same coset.

We count the number N_2 of solutions of (56) using exponential sums. Since the ratios a_i/b_i are distinct mod p we have, as in Section 3,

$$N_2 - p^3 = p^{-2} \sum_{u_1, u_2}{}' T(\Lambda_1) \cdots T(\Lambda_5) = p^{-2}\left(\sum\nolimits_1 + \sum\nolimits_2\right). \tag{58}$$

Here $\sum_1$ is the contribution coming from those points (u_1, u_2) for which no $\Lambda_i \equiv 0 \bmod p$. Now

$$\left|\sum\nolimits_1\right|^2 \leq \sum\nolimits_1 |T(\Lambda_1)T(\Lambda_2)|^2 \cdot \sum\nolimits_1 |T(\Lambda_3)T(\Lambda_4)T(\Lambda_5)|^2. \tag{59}$$

Since Λ_1 and Λ_2 are linearly independent the first sum on the right factorizes to give S_2^2. The second sum is majorized by

$$\max_{i \neq j} \sum\nolimits_1 |T(\Lambda_i)T(\Lambda_j)|^3 = S_3^2. \tag{60}$$

Hence

$$\left|\sum\nolimits_1\right| \leq S_2 S_3. \tag{61}$$

The term $\sum_2$ in (58) is the contribution coming from those points (u_1, u_2) for which some $\Lambda_i \equiv 0 \bmod p$.

LEMMA 7. *We have*

$$\left|\sum\nolimits_2\right| \leq 5pS_4. \tag{62}$$

PROOF. Since $\Lambda_1 = u_1$ the contribution to $\sum_2$ coming from the terms with $\Lambda_1 \equiv 0 \bmod p$ is at most

$$\left| p \sum_{u=1}^{p-1} T(b_2 u) \cdots T(b_5 u) \right| \leq p \prod_{i=2}^{5} \left\{ \sum_{u=1}^{p-1} |T(b_i u)|^4 \right\}^{1/4}. \tag{63}$$

As u runs through $1, 2, \ldots, p-1$ so does $b_i u$. Thus each of these sums

$$\sum_{u=1}^{p-1} |T(b_i u)|^4 = \sum_{u=1}^{p-1} |T(u)|^4 = S_4 \tag{64}$$

so this contribution to $\sum_2$ is majorized by

$$pS_4. \tag{65}$$

We assert that the same bound applies to the contribution arising from the points (u_1, u_2) with $\Lambda_j \equiv 0 \bmod p$ for each $j = 2, \dots, 5$. If $\Lambda_j \equiv 0 \bmod p$ then, interpreting $b_j^{-1} \bmod p$, $u_2 \equiv -a_j u_1/b_j \bmod p$ and so for $i \neq j$

$$\begin{aligned} \Lambda_i &\equiv u_1(a_i b_j - a_j b_i)/b_j \mod p \\ &= c_i u_i \end{aligned} \tag{66}$$

say. Thus the contribution of these terms is

$$p \sum_{u=1}^{p-1} \prod_{i \neq j} T(c_i u_i). \tag{67}$$

Now we can replace f_0, g_0 in (56) by any 2 independent forms in the pencil, for example by $f^* = f_0$ and

$$g^* \equiv (b_j f_0 - a_j g_0)/b_j \mod p. \tag{68}$$

The coefficients c_i are just the coefficients of g^* and therefore (67) is also bounded by (65), which gives the lemma.

The estimates (58), (61) and (63) give

$$N_2 \geq p^3 - S_2 S_3 - 5pS_4. \tag{69}$$

For $11 < p < 6800$ we calculate the bound on the right of (69) and find that $N_2 > 1$ (implying a non-trivial solution, which will have rank 2) for $p > 3061$.

7. Proof of Theorem 2(b)

Now $n \geq 26$ so

$$m \geq 6, \qquad q \geq 3. \tag{70}$$

Discarding excess variables we may take $m = 6$ and still have $q \geq 3$, so $r \leq 3$. We suppose first that $r = 1$, and therefore any non-trivial solution of the congruences (14) has rank 2. We begin by rewriting the congruences in the form

$$\begin{aligned} f_0 &= x_1^5 + a_2 x_2^5 + \cdots + a_6 x_6^5 \equiv 0 \mod p, \\ g_0 &= \qquad\;\; b_2 x_2^5 + \cdots + b_6 x_6^5 \equiv 0 \mod p \end{aligned} \tag{71}$$

where $b_2, \dots, b_6 \in S$.

Suppose first that some value is repeated amongst $b_2, \dots, b_6$; then we may take $b_2 = b_6 = 1$. Replacing f_0 by $b_6 f_0 - a_6 g_0$ we may also take $a_6 = 0$. Consider any non-trivial solution of the congruence

$$b_3 x_3^5 + b_4 x_4^5 + b_5 x_5^5 \equiv 0 \mod p. \tag{72}$$

If

$$A = a_3x_3^5 + a_4x_4^5 + a_5x_5^5 \equiv 0 \mod p \tag{73}$$

then we have the required solution. Otherwise we multiply x_3, x_4, x_5 by ξ, take $x_2 = -x_6 = u$ and solve

$$x_1^5 + a_2^5 u + A\xi^5 \equiv 0 \mod p \tag{74}$$

to give the required solution.

We may now suppose that $b_2, \dots, b_6$ lie one in each of the distinct cosets. Similarly, for any form g^* in the pencil generated by f_0 and g_0 which has one zero coefficient, the other 5 coefficients must lie one in each coset. Counting the number N_2 of solutions of (71) using exponential sums we have

$$\begin{aligned} N_2 - p^4 &= p^{-2} \sum{}' T(\Lambda_1) \cdots T(\Lambda_6) \\ &= p^{-2} \left(\sum\nolimits_1 + \sum\nolimits_2 \right), \end{aligned} \tag{75}$$

where $\sum_1$ is the sum over those (u_1, u_2) for which no $\Lambda_i \equiv 0 \bmod p$ and $\sum_2$ is the sum over those (u_1, u_2) for which some $\Lambda_i \equiv 0 \bmod p$.

Since $r = 1$ we have

$$\left| \sum\nolimits_1 \right| \le S_3^2. \tag{76}$$

The contribution to $\sum_2$ coming from the points (u_1, u_2) with $\Lambda_1 = u_1 \equiv 0 \bmod p$ is at most

$$\left| p \sum_{u=1}^{p-1} T(b_2 u) \cdots T(b_6 u) \right| \le p(p-1) T_1 \cdots T_5. \tag{77}$$

As in Section 6 the same estimate holds on each line $\Lambda_j \equiv 0 \bmod p$ so

$$\left| \sum\nolimits_2 \right| \le 6p(p-1) T_1 \cdots T_5. \tag{78}$$

For $131 < p \le 3061$ we find that

$$p^4 - S_3^3 - 6p(p-1) T_1 \cdots T_5 > 1 \tag{79}$$

so $N_2 > 1$, and we have the required solution.

Each of the remaining primes has $q = 2$ so we may take

$$g_0 = x_2^5 + 2x_3^5 + 4x_4^5 + 8x_5^5 + 16x_6^5, \tag{80}$$

and we begin by forming a list of non-trivial solutions of $g_0 \equiv 0 \bmod p$. We may take f_0 to be form with $a_6 = 0, a_1 = 1$ and the other coefficients lying one in each coset. If A, B, C, D are representatives of the cosets then $a_2, \dots, a_5$ is of type A, B, C, D in some order, giving 24 different cases for f_0. For each of these cases there are $((p-1)/5)^4$ individual forms f_0 to

https://doi.org/10.1017/S1446788700030925 Published online by Cambridge University Press

consider. The computer runs through each of these and then runs down the list of non-trivial solutions of $g_0 \equiv 0 \bmod p$ until it finds a common solution (since $r = 1$ this solution must have rank 2).

If $r = 3$ the congruences become

$$(81) \qquad f_0 = a_1x_1^5 + a_2x_2^5 + a_3x_3^5 + \cdots + a_6x_6^5 \equiv 0 \mod p,$$

$$(82) \qquad g_0 = b_4x_4^5 + \cdots + b_6x_6^5 \equiv 0 \mod p$$

where $a_1, a_2, a_3, b_4, b_5, b_6 \not\equiv 0 \bmod p$. We solve $g_0 \equiv 0$ with x_4, x_5, x_6 not all zero, and then solve $f_0 \equiv 0$ with x_1, x_2, x_3 not all zero. This solution has rank 2.

Now we are left with the case $r = 2$. We discard one of $x_3, \dots, x_6$ to reduce the problem to the case

$$(83) \qquad m = 5, \qquad r = 2, \qquad q = 3$$

already contained in Section 5. The results of Section 5 provide the required solution when $p \geq 101$ and we are now left with the primes 31, 41, 61 and 71.

We repeat the argument used at the end of Section 5; either

(i) $r = t = 2$ and then

$$(84) \qquad f_0 = x_1^5 + a_2x_2^5 + a_3x_3^5 + a_4x_4^5,$$

$$(85) \qquad g_0 = b_3x_3^5 + b_4x_4^5 + b_5x_5^5 + x_6^5$$

where $a_2, b_3, b_4, b_5 \in S_1, a_3a_4 \not\equiv 0 \bmod p$; or

(ii) $r = 2, t = 1, a_2 = 1$ and then

$$(86) \qquad f_0 = x_1^5 + x_2^5 + a_3x_3^5 + a_4x_4^5 + a_5x_5^5,$$

$$(87) \qquad g_0 = b_3x_3^5 + b_4x_4^5 + b_5x_5^5 + x_6^5$$

where $b_3, b_4, b_5 \in S, a_3a_4a_5 \not\equiv 0 \bmod p$.

For a fixed prime p there are 125 forms g_0 to consider. For each g_0 we begin by forming a list of solutions of $g_0 \equiv 0 \bmod p$. We then run through $5(p-1)^2$ forms of the first type (84) and $(p-1)^3$ forms of the second type (86). The computer then runs through the list of solutions of $g_0 \equiv 0 \bmod p$ until it finds one which is also a solution of $f_0 \equiv 0 \bmod p$ and which has rank 2 mod p. In this way a compter (the IBM 3083 at Sheffield University) completed the proof of Theorem 2.

8. Some counterexamples

The computer search described in Sections 5 and 6 produced the following counterexamples with $m = 5$:

(i) $p = 31$,

$$f_0 = x_1^5 + x_2^5 + x_3^5 + 3x_4^5, \tag{88}$$

$$g_0 = \quad 2x_2^5 + 4x_3^5 + 2x_4^5 + x_5^5; \tag{89}$$

(ii) $p = 41$,

$$f_0 = x_1^5 + x_2^5 + x_3^5 + \quad 2x_4^5, \tag{90}$$

$$g_0 = \quad 2x_2^5 + 4x_3^5 + 22x_4^5 + x_5^5; \tag{91}$$

(iii) $p = 61$, when there are only singular solutions,

$$f_0 = x_1^5 + x_2^5 + 4x_3^5 \tag{92}$$

$$g_0 = \qquad 4x_3^5 + 2x_4^5 + x_5^5. \tag{93}$$

It is well known that the p-adic fields with $p = 5, 11$ are exceptional for quintic equations. However the counterexamples above are of a different character. The problem here is simply that the prime p is too small rather than it being of any generic type ($p = k$ or $2k + 1$).

References

[1] O. D. Atkinson (PhD Dissertation, University of Sheffield, 1989).

[2] R. C. Baker and J. Brüden, 'On pairs of additive cubic equations', *J. Reine Angew. Math.* **391** (1988), 157–180.

[3] Z. I. Borevich and I. R. Shafarevich, *Number theory* (Academic Press, New York, 1966).

[4] I. Chowla, 'On the number of solutions of some congruences in two variables', *Proc. Nat. Acad. Sci. India Ser. A* **5** (1937), 40–44.

[5] S. Chowla, H. B. Mann and E. G. Straus, 'Some applications of the Cauchy-Davenport theorem', *Norske Vid. Selsk. Forh.* **32** (1959), 74–80.

[6] R. J. Cook, 'Pairs of additive equations', *Michigan Math. J.* **19** (1972), 325–331.

[7] R. J. Cook, 'Pairs of additive congruences: cubic congruences', *Mathematika* **32** (1985), 286–300.

[8] R. J. Cook, 'Pairs of additive congruences: quintic congruences', *Indian J. Pure Appl. Math.* **17** (1986), 786–799.

[9] R. J. Cook, 'Computations for additive Diophantine equations: quintic congruences II', *Computers in Mathematical Research*, edited by N. M. Stephens and M. P. Thorne, pp. 93–117 (Clarendon Press, Oxford, 1988).

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

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

[12] H. Davenport and D. J. Lewis, 'Cubic equations of additive type', *Philos. Trans. Roy. Soc. London Ser. A* **261** (1966), 97–136.

[13] H. Davenport and D. J. Lewis, 'Notes on congruences III', *Quart. J. Math. Oxford Ser* (2), **17** (1966), 339–344.

[14] H. Davenport and D. J. Lewis, 'Two additive equations', *Proc. Sympos. Pure Math.* **12** (1967), 74–98.
[15] H. Davenport and D. J. Lewis, 'Simultaneous equations of additive type', *Philos. Trans. Roy. Soc. London Ser. A* **264** (1969), 557–595.
[16] V. B. Demyanov, 'Pairs of quadratic forms over a complete field with discrete norm with finite residue class field', *Izv. Akad. Nauk SSSR* **20** (1956), 307–324.
[17] M. M. Dodson, 'Homogeneous additive congruences', *Philos. Trans. Roy. Soc. London Ser A* **261** (1966), 163–210.
[18] F. Ellison, 'Three diagonal quadratic forms', *Acta Arith.* **23** (1973), 137–151.
[19] J. F. Gray, *Diagonal forms of prime degree* (PhD thesis, University of Notre Dame, 1958).
[20] D. J. Lewis, 'Cubic congruences', *Michigan Math. J.* **4** (1957), 85–95.
[21] L. Low, J. Pitman and A. Wolff, 'Simultaneous diagonal congruences', *J. Number Theory* **29** (1988), 31–59.
[22] W. M. Schmidt, 'The solubility of certain p-adic equations', *J. Number Theory* **19** (1984), 63–80.
[23] E. Stevenson, 'The Artin conjecture for three diagonal cubic forms', *J. Number Theory* **14** (1982), 374–390.
[24] R. C. Vaughan, 'On pairs of additive cubic equations', *Proc. London Math. Soc.* **34** (1977), 354–364.
[25] R. C. Vaughan, 'On Waring's problem for smaller exponents', *Proc. London Math. Soc.* **52** (1986), 445–463.

Department of Pure Mathematics
University of Sheffield
Sheffield S3 7RH
England