ON SIMULTANEOUS ADDITIVE EQUATIONS, III

T. D. WOOLEY

1. Introduction

Let c_i and d_i $(1 \leqslant i \leqslant s)$ be rational integers, and k and n be natural numbers. We shall consider the solubility over the p-adic integers $\mathbb{Z}_p$ of the pair of additive equations

$$\left.\begin{aligned} f(\mathbf{x}) &= c_1 x_1^k + \ldots + c_s x_s^k = 0 \\ g(\mathbf{x}) &= d_1 x_1^n + \ldots + d_s x_s^n = 0 \end{aligned}\right\}. \tag{1}$$

We say that the equations (1) satisfy the *p-adic solubility condition* if they have a non-trivial solution in p-adic integers (i.e., a solution with not all the x_i zero). If the equations satisfy the p-adic solubility condition for every rational prime p, then we say that they satisfy the *congruence condition*. We then define $\Gamma_p^*(k,n)$ to be the least integer r such that for all $s \geqslant r$, and all c_i and d_i $(1 \leqslant i \leqslant s)$, the equations (1) satisfy the p-adic solubility condition. Also, we define $\Gamma^*(k,n)$ to be $\max_{p \text{ prime}} \Gamma_p^*(k,n)$. (We generalise this notation to t simultaneous homogeneous diagonal equations in the obvious fashion.)

Let $k \geqslant n > 1$, and let $p \equiv 1 \pmod{k}$ and $p \equiv 1 \pmod{n}$. Suppose that q is a k-th power non-residue (mod p), and q' is an n-th power non-residue (mod p). Then the equations

$$\left.\begin{aligned} \sum_{i=1}^{k} p^{i-1}(x_i^k - q y_i^k) &= 0 \\ \sum_{i=1}^{n} p^{i-1}(x_i'^n - q' y_i'^n) &= 0 \end{aligned}\right\} \tag{2}$$

have no simultaneous non–trivial solution over $\mathbb{Z}_p$. Thus for infinitely many primes p, we have $\Gamma_p^*(k,n) > 2(k+n)$. When $k = n$, Atkinson and Cook [1] have made progress in the opposite direction.

Theorem 1. *Suppose that $k \geqslant 2$, and p is a rational prime with $p > k^6$. Then $\Gamma_p^*(k,k) \leqslant 4k+1$. This result is essentially best possible in that it fails when $4k+1$ is replaced by $4k$.*

This result may be compared with the result for a single equation.

Theorem 2 (see Dodson [6], Lemma 2.4.1)**.** *Suppose that $k \geqslant 2$, and p is a rational prime with $p > k^4$. Then $\Gamma_p^*(k) \leqslant 2k+1$. This result is essentially best possible in that it fails when $2k+1$ is replaced by $2k$.*

1990 *Mathematics Subject Classification.* 10B15.

Key words and phrases. Diophantine equations, p-adic fields.

The last lines of both theorems follow by considering examples of the form (2).

Thus the situation in which the exponents in equation (1) are equal has been resolved rather satisfactorily for all but a small set of primes. However, when $k \neq n$, little is known. In Wooley [9], we gave methods which are of use in considering the p-adic solubility of general systems of homogeneous additive equations, and we demonstrated that $\Gamma^*(3,2) = 11$. Here we shall refine the methods given in that paper to establish the following result.

Theorem 3. *Suppose that $k \geqslant n \geqslant 1$, and that p is a rational prime with $p > k^4n^2$. Then*

$$\Gamma_p^*(k,n) \leqslant \begin{cases} 2(k+n)+1, & \text{when } k \geqslant n > 1, \\ 2k+2, & \text{when } k > n = 1, \\ 3, & \text{when } k = n = 1. \end{cases}$$

This result is essentially best possible in that it fails to hold when the right-hand side is reduced.

Thus the conclusion of Theorem 3 rather neatly bridges the gap between Theorems 1 and 2. It would seem likely that the following generalisation holds.

Conjecture. *Let $k_i' = k_i$ when $k_i > 1$ and $k_i' = \frac{1}{2}$ when $k_i = 1$. Then, for all rational primes p satisfying*

$$p > \big(\max\{k_1, k_2, \dots, k_t\}\big)^2 (k_1 \cdots k_t)^2,$$

we have

$$\Gamma_p^*(k_1, \dots, k_t) \leqslant 2(k_1' + k_2' + \dots + k_t') + 1. \tag{3}$$

If true, this result would be best possible, in that the bound (3) could not be reduced, by virtue of examples analogous to (2).

In principle, one could use a computer to establish the p-adic solubility of the equations (1) for the small primes excluded by the conditions of Theorem 3, although it should be emphasised that much preparation may be necessary (see, for example, Wooley [9, Section 3], where the prime 7 causes problems). Since knowledge of the p-adic solubility of the equations (1) is an essential prerequisite to an application of the Hardy-Littlewood method (the standard method for establishing the non-trivial rational solubility of the equations (1)), such questions are not without importance.

Finally, we note that there would appear to be no fundamental difficulty in extending the methods contained herein to systems of more than two simultaneous equations.

The author thanks Professor R. C. Vaughan for much useful advice, and the Science and Engineering Research Council, for a grant. This work forms part of my PhD thesis for the University of London.

We adopt the notation of writing $e(\alpha)$ for $e^{2\pi i\alpha}$, and write the usual p-adic valuation $|\cdot|_p$, normalised with $|p|_p = p^{-1}$.

2. A refined p-adic normalisation procedure

First note that Theorem 3 follows at once when $k = n = 1$, and by Theorem 1, it also follows when $k = n$. We may therefore suppose that $k > n \geqslant 1$. The case with $n = 1$ follows by a slight alteration of the proof for the case $n > 1$, so we shall not give the details here.

Suppose then that $k > n > 1$, and consider the equations (1). We now refine the p-normalisation procedure adopted in Wooley [9] so as to more readily extract information about the coefficients of f. For $1 \leqslant r \leqslant s$, write $R = \{1, 2, \ldots, r\}$, $T = \{r+1, \ldots, s\}$, and $t = |T|$, so that $r + t = s$. Now write $M = r(r-1)$, and $N = 2(r-1)n$. Define

$$\partial(f,g) = \prod_{\substack{i \neq j \\ i,j \in R}} (c_i^n d_j^k - c_j^n d_i^k) \cdot \prod_{h \in T} c_h^N. \tag{4}$$

Write $\mathbf{f}$ for (f, g).

Lemma 1. *Given a system of the form* (1), *the quantity* $\partial(\mathbf{f})$ *satisfies the following.*

(i) *If* $\nu_1, \ldots, \nu_s$ *are integers, and*

$$\mathbf{f}' = \mathbf{f}(p^{\nu_1} x_1, \ldots, p^{\nu_s} x_s),$$

then

$$\partial(\mathbf{f}') = p^{2knM\nu/r} \partial(\mathbf{f}),$$

where $\nu = \nu_1 + \ldots + \nu_s$.

(ii) *If* λ *and* μ *are rational numbers, and the system* $\mathbf{f}''$ *is defined by*

$$f''(\mathbf{x}) = \lambda f(\mathbf{x}), \quad g''(\mathbf{x}) = \mu g(\mathbf{x}),$$

then we have

$$\partial(\mathbf{f}'') = (\lambda^n \mu^k)^M \lambda^{Nt} \partial(\mathbf{f}).$$

Proof. (i) Writing c_i' and d_i' respectively for the coefficients of x_i^k in $f'(\mathbf{x})$ and x_i^n in $g'(\mathbf{x})$, we have

$$c_i'^n d_j'^k - c_j'^n d_i'^k = p^{kn(\nu_i + \nu_j)} (c_i^n d_j^k - c_j^n d_i^k),$$

and

$$c_h'^N = p^{2knM\nu_h/r} c_h^N.$$

Then by (4), we have

$$\partial(\mathbf{f}') = p^{2knM(\nu_1 + \ldots + \nu_r)/r} p^{2knM(\nu_{r+1} + \ldots + \nu_s)/r} \partial(\mathbf{f}),$$

and the result follows.

(ii) This follows simply from the definition of $\partial(f,g)$.

This completes the proof of the lemma. □

We shall follow Davenport and Lewis [3, 4, 5], and call two systems of the form (1), with integral coefficients, *equivalent* if one system can be obtained from the other by a combination of the operations (i) and (ii) of Lemma 1; here we shall always demand that the operation (ii) is non-trivial, so that $\lambda\mu \neq 0$. Notice that the operations (i) and (ii) are commutative. Also, if the system $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ has a non-trivial solution over $\mathbb{Q}_p$, then so does any system equivalent to $\mathbf{f}$.

As in Wooley [9, Section 7] (following from Davenport and Lewis [4]), we are able to use a p-adic compactness argument to permit us to assume that $\partial(\mathbf{f}) \neq 0$. This property is plainly preserved under equivalence. We shall call a system $\mathbf{f}$ *p-normalised* if the power of the rational prime p dividing $\partial(\mathbf{f})$ is minimal amongst the set of all forms equivalent to $\mathbf{f}$. That this is possible follows because this power is non-negative.

To any system $\mathbf{f}$ with integral coefficients there corresponds a system $\mathbf{f}^*$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$, these coefficients being congruent (mod p) to the corresponding coefficients of $\mathbf{f}$. Plainly, there may be variables explicit in $\mathbf{f}$ but not in $\mathbf{f}^*$.

Lemma 2. *A p-normalised system $\mathbf{f}$ can be written in the form*

$$\left.\begin{aligned} f &= f_0 + pf_1 + \ldots + p^{k-1} f_{k-1} \\ g &= g_0 + pg_1 + \ldots + p^{k-1} g_{k-1} \end{aligned}\right\},$$

where the f_j and g_j are each forms in m_j variables, and these sets are disjoint for $j = 0, \ldots, k-1$. Moreover, each of the m_j variables occurs in one at least of f_j and g_j with a coefficient not divisible by p.

The following inequalities hold for all $1 \leqslant r, t \leqslant s$ with $r + t = s$.

(i) *We have*

$$m_0 + \ldots + m_{j-1} \geqslant \frac{jr}{\mathscr{k}} + \frac{jt}{k} \quad \textit{for} \quad j = 1, \ldots, n,$$

where $\mathscr{k} = 2kn/(k+n)$ is the harmonic mean of k and n.

(ii) *With $h = f$ or g, denote by $q_{h,j}$ the number of variables occurring explicitly in the form h_j^*. We have*

$$m_0 + m_1 + \ldots + m_{j-1} + q_{f,j} \geqslant \frac{jr}{\mathscr{k}} + \frac{jt}{k} + \frac{r}{2k} + \frac{t}{k} \quad \textit{for} \quad j = 0, \ldots, n,$$

and

$$m_0 + m_1 + \ldots + m_{j-1} + q_{g,j} \geqslant \frac{jr}{\mathscr{k}} + \frac{jt}{k} + \frac{r}{2n} \quad \textit{for} \quad j = 0, \ldots, n-1.$$

Proof. All the results except for (i) and (ii) follow as in Wooley [9, Lemma 2.2].

(i) Let $x_1, \ldots, x_m$, where $m = m_1 + \ldots + m_{j-1}$, denote the variables in $\mathbf{f}_0, \ldots, \mathbf{f}_{j-1}$ $(1 \leqslant j \leqslant n)$. Then the system

$$\mathbf{f}'(\mathbf{x}) = p^{-j}\mathbf{f}(px_1, \ldots, px_m, x_{m+1}, \ldots, x_s),$$

has integral coefficients and is equivalent to the system $\mathbf{f}$. By Lemma 1, we have

$$\partial(\mathbf{f}') = p^{-jM(k+n) - jNt + (2knMm/r)}\partial(\mathbf{f}).$$

Then by the definition of a p-normalised system,

$$m \geqslant \frac{jr(k+n)}{2kn} + \frac{jrNt}{2knM} = \frac{jr}{\mathscr{k}} + \frac{jt}{k}.$$

(ii) Suppose that the number of variables occurring in f_j^* is q. Let these variables be $x_{m+1}, \ldots, x_{m+q}$, where $m = m_0 + \ldots + m_{j-1}$, and let $x_1, \ldots, x_m$ be the variables occurring in $\mathbf{f}_0, \ldots, \mathbf{f}_{j-1}$. Then for $0 \leqslant j \leqslant n$, the system

$$\left.\begin{aligned} f''(\mathbf{x}) &= p^{-j-1} f(px_1, \ldots, px_{m+q}, x_{m+q+1}, \ldots, x_s) \\ g''(\mathbf{x}) &= p^{-j} g(px_1, \ldots, px_{m+q}, x_{m+q+1}, \ldots, x_s) \end{aligned}\right\}$$

has integral coefficients, and is equivalent to $\mathbf{f}$. But by Lemma 1, we have

$$\partial(\mathbf{f}'') = p^{(2knM(m+q)/r) - (j(k+n)+n)M - (j+1)Nt}\partial(\mathbf{f}),$$

and hence, by the definition of a p-normalised system,

$$2knM(m+q)/r \geqslant M(j(k+n)+n+(2tn(j+1)/r)).$$

Then

$$m+q \geqslant \frac{rj}{\cancel{k}} + \frac{r}{2k} + \frac{(j+1)t}{k}.$$

The result follows similarly for $q_{g,j}$.

This completes the proof of the lemma. □

Lemma 3. *Suppose that $s \geqslant 2(k+n)+1$, and that the system* (1) *is p-normalised. Then we may rearrange variables and change notation to write*

$$\left.\begin{array}{ll} f^* = a_1x_1^k + \ldots + a_ux_u^k + b_1y_1^k + \ldots + b_vy_v^k & \\ g^* = \qquad\qquad\qquad\qquad c_1y_1^n + \ldots + c_vy_v^n + d_1z_1^n + \ldots + d_wz_w^n & \end{array}\right\}, \tag{5}$$

where none of the a_i, b_i, c_i, d_i are divisible by p, and

$$u+v+w \geqslant 5, \quad v+w \geqslant 3, \quad u+v \geqslant 3.$$

Proof. We put $r = 4n+1$, $t = s-r \geqslant 2(k-n)$, and apply Lemma 2. We obtain by part (i) of that lemma,

$$m_0 \geqslant (4n+1)\frac{k+n}{2kn} + 2 - \frac{2n}{k} > 2 + \frac{2n}{k} + 2 - \frac{2n}{k}$$

and so $m_0 \geqslant 5$. Also, by Lemma 2(ii), we have

$$q_{f,0} \geqslant \frac{4n+1}{2k} + 2 - \frac{2n}{k} > 2,$$

and

$$q_{g,0} \geqslant \frac{4n+1}{2n} > 2,$$

and so $q_{f,0} \geqslant 3$ and $q_{g,0} \geqslant 3$.

This completes the proof of the lemma. □

We now state two lemmata which will permit us to eliminate certain cases of (5).

Lemma 4. *Suppose that $p \nmid abc$ and $p > k^4$. Then the congruence*

$$ax^k + by^k + cz^k \equiv d \pmod{p} \tag{6}$$

has a non-trivial solution (x, y, z).

Proof. For $d \equiv 0 \pmod{p}$ this follows easily from Dodson [6, Lemma 2.4.1]. Meanwhile, for $d \not\equiv 0 \pmod{p}$, the result follows from the proof of that lemma. This completes the proof of the lemma. □

Lemma 5 (Hensel's Lemma, see Greenberg [7], Proposition (5.20))**.** *Suppose that*

$$F(X,Y), G(X,Y) \in \mathbb{Z}_p[X,Y],$$

and that $a_0, b_0 \in \mathbb{Z}_p$ satisfy

$$\max\{|F(a_0,b_0)|_p, |G(a_0,b_0)|_p\} < |\Delta_0|_p^2,$$

where

$$\Delta_0 = \Delta(F,G)|_{(a_0,b_0)} = \Big(\frac{\partial F}{\partial X}\frac{\partial G}{\partial Y} - \frac{\partial G}{\partial X}\frac{\partial F}{\partial Y}\Big)_{(a_0,b_0)}$$

is non-zero, $\partial F/\partial X$ etc. being formal derivatives. Then there is a unique $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $F(a,b) = G(a,b) = 0$ and

$$\max\{|a-a_0|_p, |b-b_0|_p\} \leqslant p^{-1}|\Delta_0|_p.$$

Given f and g of the form (1), and $\mathbf{x} \in \mathbb{Z}_p^s$, we shall define

$$\Delta(i,j) = \Delta(f,g;i,j) = knx_i^{n-1}x_j^{n-1}(c_id_jx_i^{k-n} - c_jd_ix_j^{k-n}),$$

and

$$\Delta^*(f,g) = \max_{1\leqslant i<j\leqslant s}\{|\Delta(i,j)|_p\}.$$

Thus if $\mathbf{x}$ is a solution to the congruences $f \equiv g \equiv 0 \pmod{p}$, it is non-singular (mod p) when $\Delta^*(f,g) = 1$.

Lemma 6. *All p-normalised systems of the form (1), satisfying $s \geqslant 2(k+n)+1$, $p > k^4$, and either $u > 2$ or $w > 2$, have a non-trivial solution over $\mathbb{Z}_p$.*

Proof. By setting certain of the variables to zero, we may assume from Lemma 3 that $u+v+w = 6$, $u+v \geqslant 3$, $v+w \geqslant 3$, and either $u = 3$ or $w = 3$. We shall assume that $u = 3$, the case with $w = 3$ following in a similar manner.

Since $v + w \geqslant 3$, by Lemma 4 we can solve the congruence

$$c_1y_1^n + \ldots + c_vy_v^n + d_1z_1^n + \ldots + d_wz_w^n \equiv 0 \pmod{p} \tag{7}$$

with one at least of the variables non-zero, without loss of generality either y_1 or z_1. Also by Lemma 4, fixing the y_i and z_i so as to solve the congruence (7), we have a non-trivial solution to the congruence

$$a_1x_1^k + \ldots + a_ux_u^k \equiv -(b_1y_1^k + \ldots + b_vy_v^k) \pmod{p},$$

since $u = 3$. Without loss of generality, x_1 is non-zero. Then the system is soluble (mod p) with

$$\Delta^*(f,g) \geqslant \max\{|knx_1^{n-1}z_1^{n-1}(a_1d_1x_1^{k-n})|_p, |knx_1^{n-1}y_1^{n-1}(a_1c_1y_1^{k-n})|_p\} = 1.$$

An application of Hensel's Lemma completes the proof of the lemma. □

3. Use of exponential sums

After Lemmata 3 and 6, we may assume, by setting certain of the variables to zero, that the equations (1) are of the form (5), with

$$u+v+w = 5, \quad u+v \geqslant 3, \quad v+w \geqslant 3, \quad u \leqslant 2 \quad \text{and} \quad w \leqslant 2. \tag{8}$$

Let us write the equations in the form

$$\left.\begin{array}{l} A_1x_1^k + \ldots + A_5x_5^k \\ B_1x_1^n + \ldots + B_5x_5^n \end{array}\right\} \equiv 0 \pmod{p}, \tag{9}$$

where the A_i and B_i are not simultaneously zero, and these coefficients satisfy condition (8). The number, N, of solutions (mod p) to the congruences (9) is given by the exponential sum

$$N = p^{-2} \sum_{\alpha,\beta \pmod p} T_1(\boldsymbol{\alpha}) \cdots T_5(\boldsymbol{\alpha}), \tag{10}$$

where

$$T_j(\boldsymbol{\alpha}) = T_j(\alpha,\beta) = \sum_{x \bmod p} e\big((A_j \alpha x^k + B_j \beta x^n)/p\big), \quad \text{for} \quad j = 1, \ldots, 5.$$

Lemma 7. *Suppose that $p > k$, and $A_i B_i \not\equiv 0 \pmod p$. Then we have*

$$p^{-2} \sum_{\boldsymbol{\alpha} \pmod p} |T_i(\boldsymbol{\alpha})|^4 \leqslant knp^2.$$

Proof. We have that

$$p^{-2} \sum_{\boldsymbol{\alpha} \bmod p} |T_i(\boldsymbol{\alpha})|^4$$

is the number of solutions over $\mathbb{F}_p$ to the simultaneous equations

$$\left.\begin{aligned} x_1^k + x_2^k &= y_1^k + y_2^k \\ x_1^n + x_2^n &= y_1^n + y_2^n \end{aligned}\right\}. \tag{11}$$

Suppose that $(\mathbf{x}, \mathbf{y})$ is any solution of (11). Write $d = (k, n)$. Then by eliminating y_2 from the equations (11) we obtain

$$(x_1^k + x_2^k - y_1^k)^{n/d} = (x_1^n + x_2^n - y_1^n)^{k/d}. \tag{12}$$

On noting that k/d and n/d cannot both be even, there are two possibilities.

(i) *k/d and n/d are not both odd.* Then for each of the p^2 possible choices for x_1 and x_2, there are at most kn/d solutions in y_1 to the equation (12). This is because y_1 satisfies some non-trivial polynomial of degree kn/d, and hence there are at most kn/d solutions in y_1 to (12). The integer y_2 is then determined from the equations

$$\left.\begin{aligned} y_2^k &= x_1^k + x_2^k - y_1^k \\ y_2^n &= x_1^n + x_2^n - y_1^n \end{aligned}\right\}.$$

Thus, for some z, we have that y_2 satisfies

$$y_2^d = z,$$

to which there are at most d solutions. So in this case the total number of solutions to (11) is

$$\leqslant (kn/d)p^2 d = knp^2.$$

(ii) *k/d and n/d are both odd.* Suppose first that

$$\left.\begin{aligned} x_1^k + x_2^k &= 0 \\ x_1^n + x_2^n &= 0 \end{aligned}\right\}. \tag{13}$$

There are at most dp solutions to the equations (13), since for each of the p possible choices for x_2, we can eliminate to obtain an equation of the form $x_1^d = z$ for x_1. Repeating the same argument for y_1 and y_2, we deduce that the total number of solutions of this type is at most $(dp)^2$.

Suppose now that (13) does not hold. Then picking any of the remaining $\leqslant p^2$ possible choices for x_1 and x_2, the non-trivial polynomial in y_1 in (12) has degree at most $n(k/d-1)$. So in this case there are at most $n(k/d-1)p^2d$ solutions to (11).

Then the total number of solutions in the second case is

$$\leqslant knp^2 - ndp^2 + d^2p^2 \leqslant knp^2.$$

This completes the proof of the lemma. □

Lemma 8. *Write*

$$f_i(\boldsymbol{\alpha}) = T_i(\boldsymbol{\alpha}), \quad g_j(\alpha) = T_j(\alpha, 0), \quad \textit{and} \quad h_m(\beta) = T_m(0, \beta). \tag{14}$$

Suppose also that A_i, B_i, A_j and B_m are each non-zero. Then we have

(i) $p^{-2} \displaystyle\sum_{\boldsymbol{\alpha} \bmod p} |f_i(\boldsymbol{\alpha})|^2 |g_j(\alpha)|^2 \leqslant knp^2$,

(ii) $p^{-2} \displaystyle\sum_{\boldsymbol{\alpha} \bmod p} |f_i(\boldsymbol{\alpha})|^2 |h_m(\beta)|^2 \leqslant knp^2$,

(iii) $p^{-2} \displaystyle\sum_{\boldsymbol{\alpha} \bmod p} |g_j(\alpha)|^2 |h_m(\beta)|^2 \leqslant knp^2$.

Proof. The method of proof is typified by the proof of (i). The quantity

$$p^{-2} \sum_{\boldsymbol{\alpha} \bmod p} |f_i(\boldsymbol{\alpha})|^2 |g_j(\alpha)|^2$$

is the number of solutions over $\mathbb{F}_p$ to the simultaneous equations

$$\left.\begin{aligned} A_i x^k + A_j y^k &= A_i {x'}^k + A_j {y'}^k \\ B_i x^n \qquad\quad &= B_i {x'}^n \end{aligned}\right\}. \tag{15}$$

The number of solutions to the n-th power equation in (15) is at most $n(p-1)+1$. Given any such solution, the number of solutions to the k-th power equation

$$A_j(y^k - {y'}^k) = -A_i(x^k - {x'}^k)$$

is at most kp, since for each of the p possible choices for y', there are at most k possible solutions in y.

Then the total number of solutions to the equations (15) is

$$\leqslant \big(n(p-1)+1\big)kp \leqslant knp^2.$$

This completes the proof of the lemma. □

Lemma 9. *If $p > k$, then we have*

$$|N - p^3| \leqslant (kn-1)(k-1)p^{5/2}.$$

Proof. Write

$$\sum_{\boldsymbol{\alpha}}{}^{*} \quad \text{for} \quad \sum_{\substack{\boldsymbol{\alpha} \bmod p \\ \boldsymbol{\alpha} \neq \mathbf{0}}}.$$

Then defining f, g and h as in (14), we have by (5) that

$$\sum_{\boldsymbol{\alpha}}^{*}\prod_{i=1}^{5}T_i(\boldsymbol{\alpha})=\sum_{\boldsymbol{\alpha}}^{*}\Bigl(\prod_{i=1}^{u}g_i(\alpha)\prod_{j=u+1}^{u+v}f_j(\alpha,\beta)\prod_{m=u+v+1}^{5}h_m(\beta)\Bigr).$$

Then by Hölder's inequality,

$$\begin{aligned}\Bigl|\sum_{\boldsymbol{\alpha}}^{*}\prod_{i=1}^{5}T_i(\boldsymbol{\alpha})\Bigr| &\leqslant \prod_{i=1}^{u}\prod_{j=u+1}^{u+v}\prod_{m=u+v+1}^{5}\Bigl(\sum_{\boldsymbol{\alpha}}^{*}|g_i(\alpha)|^u|f_j(\alpha,\beta)|^v|h_m(\beta)|^w\Bigr)^{1/(uvw)}\\ &\leqslant \sum_{\boldsymbol{\alpha}}^{*}|g_I(\alpha)|^u|f_J(\alpha,\beta)|^v|h_M(\beta)|^w\end{aligned}$$

for some indices I, J and M corresponding to the maximum of the sums in the second expression. For the moment, write f, g, h respectively for $f_J(\alpha,\beta)$, $g_I(\alpha)$, and $h_M(\beta)$. Then by (8), we can find positive real numbers λ, μ, ν, ρ, such that $\lambda+\mu+\nu+\rho=1$, and

$$g^uf^{v-1}h^w=(f^2g^2)^\lambda\cdot(g^2h^2)^\mu\cdot(f^2h^2)^\nu\cdot(f^4)^\rho,$$

by repeated subdivision. So by Hölder's inequality,

$$\sum_{\boldsymbol{\alpha}}^{*}|g_I(\alpha)|^u|f_J(\alpha,\beta)|^{v-1}|h_M(\beta)|^w\leqslant S_\lambda S_\mu S_\nu S_\rho,$$

where

$$S_\lambda=\Bigl(\sum_{\boldsymbol{\alpha}}^{*}|g_I(\alpha)|^2|f_J(\alpha,\beta)|^2\Bigr)^\lambda,$$

and S_μ, S_ν, S_ρ are sums over g^2h^2, f^2h^2 and f^4, in obvious notation. But

$$p^{-2}\sum_{\boldsymbol{\alpha}}^{*}|g_I(\alpha)|^2|f_J(\alpha,\beta)|^2+p^2=p^{-2}\sum_{\boldsymbol{\alpha}}|g_I(\alpha)|^2|f_J(\alpha,\beta)|^2\leqslant knp^2,$$

by Lemma 8, so that

$$S_\lambda\leqslant((kn-1)p^4)^\lambda.$$

Similarly for S_μ, S_ν and S_ρ. Hence

$$\Bigl|\sum_{\boldsymbol{\alpha}}^{*}\prod_{i=1}^{5}T_i(\boldsymbol{\alpha})\Bigr|\leqslant\Bigl(\sup_{\substack{\boldsymbol{\alpha}\bmod p\\ \boldsymbol{\alpha}\neq\mathbf{0}}}|f_J(\boldsymbol{\alpha})|\Bigr)(kn-1)p^4.$$

But by the Riemann Hypothesis for finite fields (see for example, Schmidt [8]), we have $|f_J(\boldsymbol{\alpha})|\leqslant(k-1)p^{1/2}$ for all $\boldsymbol{\alpha}\neq\mathbf{0}$. The result now follows from (10).

This completes the proof of the lemma. □

In order to estimate the number of singular solutions to the congruences (9), we require the following result (see Wooley [9, Lemma 4.5] (due to Vaughan), and its corollary).

Lemma 10. *Let $\pi_1,\dots,\pi_g$ be reduced residues* (mod q)*, and let $N(q;\boldsymbol{\pi})$ denote the number of choices of $\epsilon_1,\dots,\epsilon_g$, with $\epsilon_i=0$ or 1, such that*

$$\sum_{i=1}^{g}\epsilon_i\pi_i\equiv 0 \pmod q.$$

Write g' for the integer part of $g/2$. Suppose that $(q,\pi_i)=1$ for every i, and $q>(g+1)/2$. Then we have

$$N(q;\boldsymbol{\pi})\leqslant\begin{cases}\binom{g}{g'}, & \text{for } g \text{ even,}\\ (1+1/g)^{1/2}\binom{g}{g'}, & \text{for } g \text{ odd.}\end{cases}$$

Lemma 11. *Suppose that $p\nmid kn$. Then the number of distinct solutions to the congruences* (9) *which are singular* (mod p) *is at most*

$$(9(k-n)^4+2k)p.$$

Proof. Suppose that $\alpha_1,\dots,\alpha_5$ is any solution of the congruences (9) singular (mod p). Suppose that precisely q of the α_i are non-zero, and rearrange variables so that one has $\alpha_i\not\equiv 0 \pmod p$ for $i=1,\dots,q$. Plainly, as A_i and B_i are not simultaneously zero, we have $q=0$ or $q\geqslant 2$. Since $\boldsymbol{\alpha}$ is a singular solution and $p\nmid kn$, we must have

$$A_iB_j\alpha_i^{k-n}\equiv A_jB_i\alpha_j^{k-n} \pmod p \tag{16}$$

for all i and j in $\{1,\dots,q\}$.

Suppose that $q\geqslant 2$; there are three cases.

(i) *There is an $i\in\{1,\dots,q\}$ with $A_i\equiv 0$* (mod p). Then for all $j\neq i$ with $j\in\{1,\dots,q\}$ we have from (16) that

$$A_jB_i\alpha_j^{k-n}\equiv 0 \pmod p,$$

and hence, as $B_i\alpha_j^{k-n}\not\equiv 0 \pmod p$, we obtain $A_j\equiv 0 \pmod p$ for $j=1,\dots,q$. But then by (8) we have $q\leqslant 2$, and hence $q=2$. So $\boldsymbol{\alpha}$ is a non-trivial solution to the congruence $B_1\alpha_1^n+B_2\alpha_2^n\equiv 0 \pmod p$, to which there are at most $n(p-1)$ non-trivial solutions. So there are at most $n(p-1)$ solutions in this case.

(ii) *There is an $i\in\{1,\dots,q\}$ with $B_i\equiv 0$* (mod p). A similar argument reveals that there are at most $k(p-1)$ solutions possible in this case.

(iii) *There is no $i\in\{1,\dots,q\}$ for which either $A_i\equiv 0$ or $B_i\equiv 0$* (mod p). Then from (16),

$$(\alpha_j/\alpha_i)^{k-n}\equiv (A_iB_j)/(B_iA_j) \pmod p \quad \text{for all} \quad i\neq j \quad \text{in} \quad \{1,\dots,q\}. \tag{17}$$

The congruences (17) must be soluble (mod p) for all $i\neq j$ with $i,j\in\{1,\dots,q\}$, for otherwise there could be no singular solutions of this type. But the congruence

$$x^{k-n}\equiv (A_1B_j)/(B_1A_j) \pmod p \tag{18}$$

has at most $k-n$ solutions $\xi_1^{(j)},\dots,\xi_{k-n}^{(j)}$, so there are at most $(k-n)^{q-1}$ possible choices for $(\xi^{(2)},\dots,\xi^{(q)})$ satisfying the congruences

$$\left.\begin{aligned}A_1+A_2(\xi^{(2)})^k+\ldots+A_q(\xi^{(q)})^k\equiv 0\\ B_1+B_2(\xi^{(2)})^n+\ldots+B_q(\xi^{(q)})^n\equiv 0\end{aligned}\right\} \pmod p.$$

Hence

$$\beta_1+\ldots+\beta_q\equiv 0 \pmod p,$$

where

$$\beta_i\equiv (\omega B_i^k/A_i^n)^{1/(k-n)} \pmod p \quad \text{for} \quad i=1,\dots,q, \tag{19}$$

and ω may be taken to be any (fixed) factor required to guarantee the existence of the $(k-n)$-th root. Note that our choice of the $\xi^{(j)}$ effectively forces a particular choice of roots in (19).

Rearrange variables so that $A_i \not\equiv 0$ and $B_i \not\equiv 0 \pmod p$ for $i = 1, \ldots, g$, and either $A_i \equiv 0$ or $B_i \equiv 0 \pmod p$ for $g < i \leqslant 5$. Using the notation of Lemma 10, for each set of choices of the root in (18), there are at most $N(p; \boldsymbol{\beta})$ distinct congruences of the form

$$\beta_{i_1} + \ldots + \beta_{i_t} \equiv 0 \pmod p,$$

with $1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant g$ and $0 \leqslant t \leqslant g$, including the empty congruence. For each such non-empty congruence, we have at most $(k-n)^4(p-1)$ non-trivial solutions to the congruences (9) (given by the $p-1$ non-zero values of α_1, and the $(k-n)^4$ possible choices of the roots in (18)). Thus, by Lemma 10, on noting that $N(p; \boldsymbol{\beta})$ is an integer, we find that the number of singular solutions of type (iii) to the congruences (9) is at most

$$(10-1)(k-n)^4(p-1).$$

Then taking all possible solutions into account, the total number of singular solutions to the equations (9) is at most

$$(k+n)(p-1) + 9(k-n)^4(p-1) + 1 < \big(9(k-n)^4 + 2k\big)p.$$

This completes the proof of the lemma. □

Lemma 12. *Suppose that $p > k^4n^2$ is a rational prime, and the congruences* (9) *satisfy the conditions implicit in* (8)*. Then the congruences admit a non-singular solution* $\pmod p$*.*

Proof. By Lemmata 9 and 11, the number, N^*, of non-singular solutions to the congruences (9) satisfies

$$|N^* - p^3| \leqslant (kn-1)(k-1)p^{5/2} + \big(9(k-n)^4 + 2k\big)p.$$

Since $p > k^4n^2$, we have

$$(kn-1)(k-1)+p^{-3/2}\big(9(k-n)^4+2k\big)-k^2n < -(n+1)k+1+(k^6n^3)^{-1}\big(9(k-n)^4+2k\big). \quad (20)$$

Recall that we are assuming that $k > n > 1$. Then $n \geqslant 2$, and $k \geqslant 3$, so that the right hand side of (20) is

$$\leqslant -3k + 1 + 11/k^2 < 0. \quad (21)$$

Then by (20) and (21), we have $|N^* - p^3| < k^2np^{5/2}$, and hence

$$N^* > p^3 - k^2np^{5/2} > 0.$$

Thus there is at least one non-singular solution $\pmod p$ to the congruences (9), as required. This completes the proof of the lemma. □

We may now use Hensel's Lemma to deduce that the equations (1) have a non-trivial p-adic solution whenever $p > k^4n^2$. This completes the proof of Theorem 3.

References

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

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

[3] H. Davenport and D. J. Lewis, *Cubic equations of additive type*, Phil. Trans. Roy. Soc. Lond. **261A** (1966), 97–136.

[4] H. Davenport and D. J. Lewis, *Two additive equations*, Proc. Symp. in Pure Math., Vol. XII (Houston, Tex., 1967), 74–98.

[5] H. Davenport and D. J. Lewis, *Simultaneous equations of additive type*, Phil. Trans. Roy. Soc. Lond. **264A** (1969), 557–595.

[6] M. M. Dodson, *Homogeneous additive congruences*, Phil. Trans. Roy. Soc. Lond. **261A** (1966), 163–210.

[7] M. J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin, Inc., New York, Amsterdam, 1969.

[8] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics **536**, Springer-Verlag, Berlin, 1976.

[9] T. D. Wooley, *On simultaneous additive equations, I*, Submitted for publication.

Imperial College of Science and Technology, Department of Mathematics, Huxley Building, 180 Queen's Gate, London SW7 2BZ