Indian J. pure appl. Math., **17** (6) : 786-799, June 1986

PAIRS OF ADDITIVE CONGRUENCES : QUINTIC CONGRUENCES

R. J. COOK

Department of Pure Mathematics, University of Sheffield, Hicks Building Hounsfield Road, Sheffield S3 7RH

(*Received* 3 *September* 1985)

We consider two additive quintic equations

$$a_1 x_1^5 + \cdots + a_n x_n^5 = 0$$

$$b_1 x_1^5 + \cdots + b_n x_n^5 = 0$$

in p-adic fields. Davenport and Lewis showed that the equations have a non-trivial solution in every p-adic field if $n \geqslant 51$. Here we prove that the equations have a non-trivial solution in all but a finite number of p-adic fields, with an explicit list of possible exceptional fields, if $n \geqslant 31$.

1. INTRODUCTION

Davenport and Lewis[1] considered two additive equations

$$\left.\begin{aligned} a_1 x_1^k + \cdots + a_n x_n^k &= 0 \\ b_1 x_1^k + \cdots + b_n x_n^k &= 0 \end{aligned}\right\} \qquad \ldots(1)$$

where the coefficients a_i, b_i are integers and k is a positive integer. They proved that if k is odd and $n \geqslant 2k^2 + 1$ then the equations (1) have a non-trivial solution in every p-adic field.

In the case $k = 5$ Cook[2] proved that if $N \geqslant 51$ then eqns. (1) have a non-trivial solution in $\mathbb{Z}$. In fact the Hardy-Littlewood method, showing that non-trivial solutions in p-adic integers imply non-trivial solutions in rational integers, will work for "most" pairs of additive quintics in 47 variables. Specifically, the method works if

$$\left.\begin{aligned} f(\mathbf{x}) = a_1 x_1^5 + \cdots + a_n x_n^5 &= 0 \\ g(\mathbf{x}) = b_1 x_1^5 + \cdots + b_n x_n^5 &= 0 \end{aligned}\right\} \qquad \ldots(2)$$

are such that

(i) $n \geqq 47$;

(ii) the equations have a non-trivial solution in every p-adic field; and

(iii) the ratios a_i/b_i can be partitioned into two sets $\mathscr{S}$ and $\mathscr{T}$ with $|\mathscr{S}| = 15$, $|\mathscr{T}| = 32$ such that no ratio a_i/b_i occurs more than twice in $\mathscr{S}$ or more than 16 times in $\mathscr{T}$.

It seems reasonable then to investigate whether the equations (2) have p-adic solutions when $n < 51$.

Theorem 1—If $n \geqslant 46$ the equations (2) have a non-trivial solution in p-adic integers except (possibly) when $p = 5$, 11, 31 or 41.

The proof of Theorem 1 can be adapted to the case of fewer variables, but the set of exceptional primes becomes larger. Essentially the same proof gives the following two results.

Theorem 2—If $n \geqslant 41$ eqns. (2) have a non-trivial solution in p-adic integers except (possibly) when $p = 5$, 11, 31, 41 or 71.

Theorem 3—If $n \geqslant 36$ eqns. (2) have a non-trivial solution in p-adic integers except (possibly) when

$$p = 5 \quad \text{or} \quad p \equiv 1 \pmod{10} \text{ and } p \leqslant 101. \qquad \ldots(3)$$

In the case of a singie additive quintic, Gray[3] proved that 16 variables are sufficient in every p-adic field and the example

$$\sum_{i=0}^{4} 11^i \left(x_i^5 + 2y_i^5 + 4z_i^5 \right) \qquad \ldots(4)$$

shows that 15 variables are not sufficient in the 11-adic field. Taking two disjoint copies of this form we obtain two additive quintics in 30 variables which do not have a non-trivial simultaneous zero in the 11-adic field. A refinement of the method used for Theorems 1,2 and gives the following result.

Theorem 4—If $N \geqslant 31$ the equations have a non-trivial solution in p-adic integers except (possibly) when

$$p = 5 \text{ or } p = 191 \text{ or } p \equiv 1 \pmod{10} \text{ and } p \leqslant 131. \qquad \ldots(5)$$

Theorems 1 to 4 all depend on calculations involving exponential sums. However, in the case $N \geqslant 46$ it is possible to improve on Theorem 1 by a combination of ad hoc elementary arguments.

Theorem 1A—If $N \geqslant 46$ the equations have a non-trivial solution in p-adic integers except (possibly) when $p = 5$ or 11.

2. Preliminary Lemmata

We begin by recalling lemmata of Davenport and Lewis[1,4] in a form applicable to the more general problem

$$\left.\begin{aligned} f(\mathbf{x}) &= a_1 x_1^k + \ldots + a_n x_n^k = 0 \\ g(\mathbf{x}) &= b_1 x_1^k + \ldots + b_n x_n^k = 0. \end{aligned}\right\} \qquad \ldots(6)$$

In this section p is a fixed prime which does not divide k. With f and g we associate the parameter

$$\theta = \theta(f, g) = \prod_{i \neq j} (a_i b_j - a_j b_i) \qquad \ldots(7)$$

and it is sufficient to prove the theorems under the additional assumption that $\theta \neq 0$ (see section 5 of Davenport and Lewis[4]).

Lemma 1—Any pair of forms f, g with $\theta(f, g) \not\equiv 0$ is equivalent to (i. e. has the same p-adic solutions as) a p-normalized pair of forms f^*, g^* with

$$\left.\begin{aligned} f^* &= f_0 + pf_1 + \ldots + p^{k-1} f_{k-1} \\ g^* &= g_0 + pg_1 + \ldots + p^{k-1} g_{k-1} \end{aligned}\right\} \qquad \ldots(8)$$

where f_i, g_i, forms in m_i variables, each of which occurs in one at least of f_i, g_i with a coefficient not divisible by p, and

$$m_0 + m_1 + \ldots + m_{j-1} \geqslant jn/k, \; j = 1, 2, \ldots, k. \qquad \ldots(9)$$

Further if q_j denotes the minimum number of variables occurring explicity in any form $\lambda f_j + \mu q_j$ (λ, μ not both divisible by p) with a coefficient not divisible by p, then

$$m_0 + \ldots + m_{j-1} + q_j \leqslant (2j + 1)\, n/2k, \; j = 0, 1, \ldots, k - 1. \qquad \ldots(10)$$

This is Lemma 2 of Davenport and Lewis[4].

We consider the section f_0, g_0 of f^*, g^* and put

$$m = m_0 \geqslant n/k, \; q = q_0 \geqslant n/2k. \qquad \ldots(11)$$

Lemma 2—If $p + k$ and the congruences

$$f_0 \equiv 0 \quad g_0 \equiv 0 \bmod p \qquad \ldots(12)$$

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

$$\begin{bmatrix} a_1 \xi_1 \ldots a_m \xi_m \\ b_1 \xi_1 \ldots b_m \xi_m \end{bmatrix} \qquad \ldots(13)$$

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

This version of Hensel's Lemma is Lemma 7 of Davenport and Lewis[1].

We now take $\delta = (k, p - 1)$.

Lemma 3—If $m > 2\delta + 1$ and $q \geqslant \delta + 1$ then the congruences (12) have a solution of rank 2 (mod p).

This is Lemma 3 of Davenport and Lewis[1].

We now observe that if k is a prime, and $p \equiv 1 \pmod{k}$, then $\delta = 1$. Combining the results of this section we obtain

Lemma 4—Let k and p be primes, $p \neq k$ and $p \not\equiv 1 \bmod k$. If $n \geqslant 2k + 1$ then the equations (6) have a non-trivial solution in p-adic integers.

We shall also need a result of Chowla *et al.*[5] which holds for any positive integer k.

Lemma 5—Let $p > 2\delta + 1$ and $\alpha_1 \ldots, \alpha_n \not\equiv 0 \pmod{p}$. Then

$$\alpha_1 x_1^k + \ldots + \alpha_n x_n^k$$

either represents all residues (mod p) or represents at least $1 + (2n - 1)(p - 1)/\delta$ residues (mod p).

Corollary —Let $p > 11$ and $\alpha_1 \alpha_2 \alpha_3 \not\equiv 0 \bmod p$. Then $\alpha_1 x_1^5 + \alpha_2 x_2^5 + \alpha_3 x_3^5$ represents all residues mod p.

3. Quintic Congruences

We now return to the original problem of two quintic equations. After a considerable (but obvious) change in notation we may write

$$f_0 = a_1 x_1^5 + \ldots + a_r x_r^5 + b_1 y_1^5 + \ldots + b_s y_s^5 \equiv 0 \pmod{p} \quad \ldots(14)$$

$$g_0 = c_1 y_1^5 + \ldots + c_s y_s^5 + d_1 z_1^5 + \ldots + d_t z_t^5 \equiv 0 \pmod{p} \quad \ldots(15)$$

where none of the coefficients appearing in (14) and (15) are divisible by p and

$$m = r + s + t \geqslant n/5, \quad \ldots(16)$$

$$q = s + t \geqslant n/10. \quad \ldots(17)$$

Taking suitable multiples of f_0 and g_0 we may also suppose that

$$a_1 = d_1 = 1. \quad \ldots(18)$$

We also have r as the length of the longest block of common ratios "a_i/b_i" (mod p) and t is the length of the second longest block. Thus

$$r \geqslant t \geqslant 1. \quad \ldots(19)$$

After Lemma 4 we need only consider the case

$$p \equiv 1 \pmod{5}, \; p > 11 \quad \ldots(20)$$

and, using Lemma 2, it is now sufficient to prove that the congruences (14) and (15) have a simultaneous solution of rank 2 (mod p).

Lemma 6—Let $N \geqslant 31$ and $p > 11$. If $r \geqslant 3$ then the congruences (14) and (15) have a simultaneous solution of rank 2 (mod p).

PROOF : We have $m \geqslant 7$ and $q \geqslant 4$.

(i) If $s = 0$ then $r \geqslant t \geqslant 4$. We take $x_1 = z_1 = 1$ and solve the congruences

$$a_2 x_2^5 + \ldots + a_r x_r^5 \equiv -1, \; d_2 z_2^5 + \ldots + d_t z_t^5 \equiv -1 \pmod{p}$$

independently, using the Corollary to Lemma 5.

(ii) If $s = 1$ then $r \geqslant t \geqslant 3$. We take $y_1 = 1$ and solve the congruences

$$x_1^5 + \ldots + a_r x_r^5 \equiv -b_1, \; z_1^5 + \ldots + d_t z_t^5 \equiv -c_1 \pmod{p}$$

independently.

(iii) If $s \geqslant 3$ we take $z_1 = 1$ and solve the congruence

$$c_1 y_1^5 + \ldots + c_s y_s^5 \equiv -1 \pmod{p}$$

so that $y_1, \ldots, y_s$ are not all divisible by p. Then we solve

$$x_1^5 + \ldots + a_r x_r^5 \equiv -b_1 y_1^5 - \ldots - b_s y_s^5 \pmod{p}.$$

(iv) If $s = 2$ and $t \geqslant 3$ we repeat the argument used in case (ii), so finally we may suppose that $s = t = 2$, since $q > 4$.

We take $z_1 = 1$ and solve (15), substitute these values for y_1, y_2 into (14) and solve it. This provides a solution of rank 2 unless $y_1 \equiv y_2 \equiv 0$ in which case

$$z_1^5 + d_2 z_2^5 \equiv 0 \pmod{p}.$$

Then d_2 is a fifth power (mod p) and using a substitution $z_2 \to \alpha z_2$ we may take $d_2 = 1$.

If $b_1/c_1 \not\equiv b_2/c_2 \pmod{p}$ we take $y_1 = 1$ and solve (15), substitute these values for y_1, y_2 into (14) and solve it. Since the solution of (15) involves two linearly independent columns we have a simultaneous solution of rank 2 (mod p).

Now we may suppose that $b_1/c_1 \equiv b_2/c_2 \equiv q \pmod{p}$ and replace the congruences (14) and (15) with

$$x_1^5 + \ldots + a_r x_r^5 + q c_1 y_1^5 + q c_2 y_2^5 \equiv 0 \pmod{p}, \qquad \ldots(21)$$

$$c_1 y_1^5 + c_2 y_2^5 + z_2^5 \equiv 0 \pmod{p}. \qquad \ldots(22)$$

The fifth powers (mod p) form a subgroup of the multiplicative group of non-zero residues, and there are five cosets. If c_1 and c_2 are in the same coset then c_1/c_2 is a fifth power and the congruence

$$c_1 y_1^5 + c_2 y_2^5 \equiv 0 \pmod{p} \qquad \ldots(23)$$

has a non-trivial solution. We then take $x_1 = x_2 = \ldots = x_r = 0$, $z_1 = -z_2 = 1$ to give a simultaneous solution of rank 2 (mod p).

If c_1 and c_2 are not in the same coset then (23) has no non-trivial solutions. We take $y_1 = 1$ and solve (22), and this solution must have either z_1 or z_2 non-zero, then

substitute these values of y_1, y_2 into (21) and solve for $x_1,\ldots, x_r$ to give a solution of rank 2 (mod p.).

4. Exponential Sums

We now have $r \leqslant 2$ and rewrite the congruences (14) and (15) as

$$\left.\begin{aligned} f_0 &= a_1 x_1^5 + \ldots + a_m x_m^5 \equiv 0 \pmod p. \\ g_0 &= b_1 x_1^5 + \ldots + b_m x_m^5 \equiv 0 \pmod p. \end{aligned}\right\} \quad \ldots(24)$$

Using exponential sums we can count the number of simultaneous solutions of (24) as

$$N = p^{-2} \sum_{u_1,u_2 \bmod p} T(\Lambda_1) \ldots T(\Lambda_m) \quad \ldots(25)$$

where

$$\Lambda_j = u_1 a_j + u_2 b_j \quad \ldots(26)$$

and

$$T(\Lambda) = \sum_{x \bmod p} e(\Lambda x^5/p). \quad \ldots(27)$$

Further,

$$T(\Lambda) = p \text{ if } \Lambda \equiv 0 \pmod p \quad \ldots(28)$$

$$|T(\Lambda)| \leqslant 4\sqrt{p} \text{ if } \Lambda \not\equiv 0 \pmod p \quad \ldots(29)$$

and

$$|N - p^{m-2}| \leqslant p^{-2} \sum'_{u_1,u_2 \bmod p} |T(\Lambda_1) \ldots T(\Lambda_m)|, \quad \ldots(30)$$

where Σ' denotes the omission of the term $u_1 = u_2 = 0$.

We consider the contribution made to the sum on the right of (30) by those points (u_1, u_2) for which exactly ν of the linear forms $\Lambda_j \equiv 0 \pmod p$. Since $(u_1, u_2) \not\equiv (0,0)$ and $r \leqslant 2$ we have $\nu = 0$, 1 or 2. When $\nu = 2$ the columns are linearly dependent, since otherwise $u_1 \equiv u_2 \equiv 0$. so there are at most $[m/2]$ choices for the two columns and for each pair of columns there are p-1 points (u_1, u_2). Thus the contribution of these terms is at most

$$[m/2]\, p^2\, (4\sqrt{p})^{m-2}\, (p-1) < [m/2]\, 4^{m-2}\, p^{(m+4)/2} \quad \ldots(31)$$

When $\nu = 1$ there are m possible choices for Λ_j so these terms contribute at most

$$m\,p\,(4\sqrt{p})^{m-1}\ (p-1) < m\,4^{m-1}\ p^{(m+3)/2}. \qquad \ldots(32)$$

The final contribution from the points with $\nu = 0$ is at most

$$(4\sqrt{p})^m\,(p-1)^2 < 4^m\,p^{(m+4)/2}. \qquad \ldots(33)$$

Thus the number N of solutions of (24) satisfies

$$N > p^{m-2} - 4^{m-2}\,p^{m/2}\,\{[m/2] + 16 + 4m/\sqrt{p}\}. \qquad \ldots(34)$$

The congruences (24) have one solution of rank 0 and solutions of rank 1 must occur in a pair of linearly dependent columns. There are at most $[m/2]$ choices for the pair of columns and if these columns correspond to x_1 and x_2 we then have

$$a_1\,x_1^5 + a_2\,x_2^5 \equiv 0 \pmod{p} \text{ or } (x_1\,x_2^{-1})^5 \equiv -a_2a_1^{-1} \pmod{p}$$

so there are at most $p-1$ choices for x_1, x_2. Thus there are at most $1 + [m/2]\,(p-1)$ solutions of rank < 2 so the desired solution of rank 2 exists provided that

$$p^{m-2} - 4^{m-2}\,p^{m/2}\,\{[m/2] + 16 + 4\,m/\sqrt{p}\} - [m/2]\,(p-1) > 1. \qquad \ldots(35)$$

5. Small Primes

For $N \geqslant 31$ we have $m \geqq 7$ and (35) is clearly satisfied for all large primes. For each prime $p \equiv 1 \mod 10$ which does not satisfy (35) we calculate the least the quintic non-residue $q \pmod{p}$. Now $1, q, \ldots, q^4$ are elements from the 5 cosets of quintic residues $(\mod p)$ and the exponential sum $T(\Lambda)$ depends only on the coset in which Λ lies. We calculate, on a computer, the absolute values of the exponential sums.

$$T_i = \Big|\sum_{x \bmod p} e\,(q^{i-1}\,x^5/p)\Big|\ ,\ i = 1, \ldots, 5, \qquad \ldots(36)$$

(see Table I, the values can be checked using the identity)

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

By taking suitable linear combinations of f_0 and g_0 in the congruences (24) we may suppose that $a_1 = b_2 = 1$, $a_2 = b_1 = 0$. Then $\Lambda_1 = u_1$ and $\Lambda_2 = u_2$. We consider the values of $T(\Lambda_1)\ T(\Lambda_2)$ as (u_1, u_2) runs through the $p^2 - 1$ points other than (0,0).

TABLE I

p	q	T_1	T_2	T_3	T_4	T_5
31	2	19.5579	1.8019	3.2828	11.5544	9.4845
41	2	16.3126	3.2305	7.0814	4.9793	21.6453
61	2	3.3036	8.4734	24.0641	4.3315	23.2259
71	2	30.4420	17.9536	12.9876	1.2852	0.7860
101	2	4.4471	17.6931	37.7501	0.3695	16.1793
131	2	31.8572	8.4292	7.4627	37.8199	6.9292
151	3	25.9535	0.1840	27.8929	19.6428	34.3878
181	2	14.3050	2.3206	5.5245	44.2091	37.7493
191	2	52.2529	20.4851	3.9026	25.4764	2.3887
211	2	37.2624	29.7819	0.1937	34.7811	27.1067
241	3	49.6037	16.0750	34.1447	0.9684	30.5656
251	3	43.1517	24.6018	18.2038	2.4847	47.0650
271	2	11.5078	58.2510	13.1179	7.2391	40.8644
281	2	22.5665	35.9711	35.8279	50.3190	1.0866

There are $(p-1)$ points $(0, u_2)$ and then

$$| T(\Lambda_1)\, T(\Lambda_2) | = p\, T_i,\ i = 1, \ldots, 5 \qquad \ldots(37)$$

for exactly $(p-1)/5$ values of (u_1, u_2). Similarly the $p-1$ points $(u_1, 0)$ fall into 5 subsets of size $(p-1)/5$ on each of which (37) holds. Let $T = \max T_i$. Since $r \leqslant 2$ at most one of the other linear forms $\Lambda_j \equiv 0 \pmod p$ so the total contribution of these terms to the sum on the right of (30) is at most

$$2(p-1)\, p^2\, (T_1 + \ldots + T_5)\, T^{m-3}/5. \qquad \ldots(38)$$

When neither u_1 nor u_2 is zero the $(p-1)^2$ points (u_1, u_2) fall into 25 subsets of size $(p-1)^2/25$ on each of which

$$| T(\Lambda_1)\ T(\Lambda_2) | = T_i\, T_j,\ 1 \leqslant i, j \leqslant 5. \qquad \ldots(39)$$

If the other linear forms Λ_j are non-zero (mod p) then the contribution of these terms would be at most

$$(p-1)^2\, T^{m-2} \sum_{i=1}^{5} \sum_{j=1}^{5} T_i\, T_j/25. \qquad \ldots(40)$$

However, there may be at most $(m-2)(p-1)$ points (u_1, u_2) where some $\Lambda_j \equiv 0 \pmod p$ and then at most two of the $\Lambda_j \equiv 0 \pmod p$. Therefore the estimate (40) must be increased by

$$(m-2)(p-1)(p^2 T^{m-2} - T^m). \qquad \ldots(41)$$

Thus we may replace the bound on the right of (34) by

$$p^{m-2} - p^{-2}(p-1) T^{m-3} \{2p^2 \Sigma_1/5 + (p-1) T \Sigma_2/25 + (m-2) \times (p^2 T - T^3)\} \qquad \ldots(42)$$

where

$$\Sigma_1 = \sum_{i=1}^{5} T_i \text{ and } \Sigma_2 = \sum_{i=1}^{5} \sum_{j=1}^{5} T_i T_j \qquad \ldots(43)$$

with corresponding changes in (35).

Proof of Theorem 1— When $n \geqslant 46$ we have $m \geqslant 10$ and (35) is satisfied when $p > 130$. For the remaining primes $p \equiv 1 \pmod{10}$, $p > 11$, we calculate q and the values T_i, see Table I. From (42) and the estimate $1 + [m/2](p-1)$ for the number of singular solutions it follows that solutions of rank 2 exist when $p = 61$, 71 or 101.

Proof of Theorem 2—When $n > 41$ we have $m \geqslant 9$ and (35) is satisfied when $p > 180$. Inserting the values for T_i into (42) it follows that solutions of rank 2 exist when $p = 61$, 101, 131 and 151.

Proof of Theorem 3—When $n > 36$ we have $m \geqslant 8$ and (35) is satisfied when $p > 300$. Inserting the values for T_i into (42) it follows that solutions of rank 2 exist when $p > 101$.

6. Proof of Theorem 4

When $n \geqslant 31$ we have $m \geqslant 7$ and (35) is satisfied for $p > 750$. Inserting the values of T_i into (42) and repeating the previous argument shows that solutions of rank 2 (mod p) exist whenever $p > 331$. This bound may be improved by refining the method of section 5 to consider three separate cases.

(i) $r = t = 2$. In this case we replace the estimate (41) with

$$(m-4)(p-1)(p^2 T^{m-2} - T^m) \qquad \ldots(44)$$

and make the corresponding changes in (42).

(ii) $r = 2$, $t = 1$. We replace the estimate (41) with

$$(m - 3)\ (p - 1\ (pT^{m-1} - T^m) \qquad \ldots(45)$$

(38) with

$$(p - 1)\ \Sigma_1\ pT^{m-4}\ (pT + T^2)/5 \qquad \ldots(46)$$

and make the corresponding changes in (42).

(iii) $r = t = 1$. We replace the estimate (41) with

$$(m - 2)\ (p - 1)\ (pT^{m-1} - T^m) \qquad \ldots(47)$$

(38) with

$$2\ (p - 1)\ \Sigma_1\ pT^{m-2}/5 \qquad \ldots(48)$$

and make the corresponding changes in (42).

With these revised estimates in (42) straightforward calculations show that the desired solutions of rank 2 exist if $p > 200$, $p = 151$ or 181.

7. The Case $N \geqslant 46$

In the notation of §3 we may suppose that $m = 2$ and, after Lemma 6, that $r = 1$ or 2. Throughout this section p is a fixed prime $\equiv 1 \bmod 10$, $p > 11$. Unless otherwise indicated, congruences should be interpreted modulo p. From the Corollary to Lemma 5 it is easy to see that if $\alpha_1 \ldots \alpha_4 \not\equiv 0$ then there is a non-trivial solution of

$$\alpha_1 x_1^5 + \ldots + \alpha_4 x_4^5 \equiv 0. \qquad \ldots(49)$$

Returning to the congruences (24) we may take $a_1 = 1$ and $b_1 = 0$. Let $1, q, \ldots, q^4$ be representatives of the five cosets of fifth powers (mod p). After a suitable change of variable we may suppose that each non-zero b_l lies in this set of representatives.

Case 1, $r = t = 1$. Two of the values $b_2, \ldots, b_{10}$ are equal, say $b_2 = b_{10}$. Multiplying by b_2^{-1} and then replacing f_0 by $f_0 - a_{10} g_0$ the congruences become

$$\left.\begin{aligned} f_0 &= x_1^5 + a_2 x_2^5 + \ldots + a_9 x_9^5 \equiv 0 \\ g_0 &= x_2^5 + b_3 x_3^5 + \ldots + b_9 x_9^5 + x_{10}^5 \equiv 0. \end{aligned}\right\} \qquad \ldots(50)$$

Now two of $b_3, \ldots, b_8$ are equal so we may also suppose that $b_3 = b_4 = b$, say.

We choose $x_5, \ldots, x_8$, not all zero, with

$$b_5 x_5^5 + \ldots + b_8 x_8^5 \equiv 0. \qquad \ldots(51)$$

If

$$a_5 x_5^5 + \ldots + a_8 x_8^5 \equiv 0 \qquad \ldots(52)$$

then we have the required solution of rank 2 (mod p), since $t = 1$. If (52) is not satisfied let $x_2 = -x_{10} = x$, $x_3 = -x_4 = y$. Then $g_0 \equiv 0$ and, as $a_3 \not\equiv a_4$, we may choose u, x, y to satisfy

$$u^5 + a_2 x^5 + (a_3 - a_4) y^5 \equiv -\left(a_5 x_5^5 + \ldots + a_8 x_8^5\right) \qquad \ldots(53)$$

giving the required solution of rank 2 (mod p).

Case 2, $r = 2$ and $t = 1$. We observe that the solution in Case 1 did not use the variable x_9. We take x_9 to be the second variable with $b_l = 0$ and repeat the previous argument.

Case 3, $r = t = 2$. Since two of $b_3, \ldots, b_8$ are equal we may write the congruences as

$$f_0 = x_1^5 + a_2 x_2^5 + a_3 x_3^5 + \ldots + a_8 x_8^5 \equiv 0$$

$$g_0 = b x_3^5 + b x_4^5 + \ldots + b_8 x_8^5 + b_9 x_9^5 + x_{10}^5 \equiv 0.$$

Assume first that two of $b_5, \ldots b_8$, are equal, say $b_5 = b_6 = c$. We choose $x_7, \ldots, x_{10}$, not all zero, such that

$$b_7 x_7^5 + b_8 x_8^5 + b_9 x_9^5 + x_{10}^5 \equiv 0. \qquad \ldots(54)$$

We then take $x_3 = -x_4 = u$, $x_5 = x_6 = v$ and consider the congruence

$$x_1^5 + a_2 x_2^5 + (a_3 - a_4) u^5 + (a_5 - a_6) v^5 \equiv -\left(a_7 x_7^5 + a_8 x_8^5\right) \ldots(55)$$

If $a_7 x_7^5 + a_8 x_8^5 \equiv 0$ then (55) has a non-trivial solution for x_1, x_2, u, v unless

$a_3 \equiv a_4$ or $a_5 \equiv a_6$. If, say, $a_3 \equiv a_4$ we take $x_3 = -x_4 = 1$ with $x_7, \ldots, x_{10}$ to give a solution of rank 2. On the other hand, if $a_7 x_7^5 + a_8 x_8^5 \not\equiv 0$ then (55) has a non-trivial solutions unless $a_3 \equiv a_4$ and $a_5 \equiv a_6$, in which case we take $x_3 = -x_4 = 1$, $x_5 = -x_6 = 1$. The non-trival solutions of (55), together with the variables $x_7, \ldots, x_{10}$, clearly give solutions of rank 2 (mod p).

Now we may suppose that $b_5, \ldots, b_8$ take four distinct values. Since $r = 2$ we may renumber the variables so that $a_7/b_7 \not\equiv a_8/b_8$. We begin by choosing $x_7, \ldots, x_{10}$, not all zero, to satisfy (54).

We assume first that $a_7 x_7^5 + a_8 x_8^5 \equiv 0$, which will give the required solution of rank 2 (mod p) unless $x_7 = x_8 = 0$. In that case we have a non-trivial solution of $b_9 x_9^5 + x_{10}^5 \equiv 0$ and so $b_9 = 1$. We now start choosing the variables $x_1, \ldots, x_{10}$ afresh, taking $x_9 = -x_{10} = 1$. We choose $x_5, \ldots, x_8$, not all zero, so that (51) is satisfied. If (52) is also satisfied then $x_5, \ldots x_{10}$ give a solution of rank 2. Otherwise we take $x_3 = -x_4 = y$ and, if $a_3 \not\equiv a_4$, choose u, x and y to satisfy (53). Finally, if $a_3 \equiv a_4$ we take $x_3 = -x_4 = 1$, $x_9 = -x_{10} = 1$ and all the other variables to be 0.

Now we may suppose that $a_7 x_7^5 + a_8 x_8^5 \not\equiv 0$ in our solution of (54). We take $x_3 = -x_4 = x$ and consider the congruence

$$x_1^5 + a_2 x_2^5 + (a_3 - a_4) x^5 \equiv -\left(a_7 x_7^5 + a_8 x_8^5\right). \qquad \ldots(56)$$

If $a_3 \not\equiv a_4$ this is soluble and, since $r = 2$, the solution has rank 2. Now $a_3 \equiv a_4$ and $f\, b_9 \equiv 1$ then a suitable solution is $x_3 = -x_4 = 1$, $x_9 = -x_{10} = 1$. Thus we may now suppose the congruences are

$$\left.\begin{aligned} x_1^5 + a_2 x_2^5 + a\ x_3^5 + a\ x_4^5 + \ldots + a_8 x_8^5 &\equiv 0 \\ b\, x_3^5 + b\ x_4^5 + \ldots + b_8 x_8^5 + b_9 x_9^5 + x_{10}^5 &\equiv 0, \end{aligned}\right\} \qquad \ldots(57)$$

where $b_9 \not\equiv 1$. Since the values of $b_5, \ldots, b_8$ are distinct one of them must equal 1 or b_9 and there is no loss of generality in assuming that $b_5 = 1$. We choose $x_6, \ldots x_9$, not all zero, so that

$$b_6 x_6^5 + \ldots + b_9 x_9^5 \equiv 0.$$

If

$$a_6 x_6^5 + \ldots + a_9 x_9^5 \equiv 0$$

we take $x_3 = -x_4 = 1$ and have a non-singular solution of the congruences (57). Otherwise we take $x_5 = -x_{10} = x$ and complete the proof by solving

$$x_1^5 + a_2 x_2^5 + a_5 x^5 \equiv -\left(a_6 x_6^5 + \ldots + a_9 x_9^5\right).$$

References

1. H. Davenport, and D. J. Lewis, *Proc. Symp. in Pure Math.* **12**, 74–98.
2. R. J. Cook, *Proc. Edinburgh Math. Soc.* 26 (1983), 191–211.
3. J. F. Gray, Ph. D. thesis University of Notre Dame, 1958.
4. H. Davenport, and D. J. Lewis, *Phil. Trans. R. Soc. Lond.* 261 A (1966), 97–136.
5. S. Chowla, H. B. Mann, and E. G. Straus, *Kon Norske Vidensk. Forh.* 32 (1959) 74–80.