PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A
MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Simultaneous Equations of Additive Type

H. Davenport and D. J. Lewis

Phil. Trans. R. Soc. Lond. A 1969 **264**, 557-595
doi: 10.1098/rsta.1969.0035

SIMULTANEOUS EQUATIONS OF ADDITIVE TYPE*

By H. DAVENPORT, F.R.S.†
Trinity College, Cambridge

and D. J. LEWIS
University of Michigan

(*Received* 23 *September* 1968)

CONTENTS

The paper contains an investigation of conditions under which R simultaneous equations of additive type in N unknowns have a solution in integers, not all 0. If the degree k of the equations is odd, it suffices if N is greater than an explicit function of R and k. If k is even, two further conditions are imposed, and neither can be entirely avoided. It is also proved that the equations have a solution in p-adic integers, not all 0, if N is greater than an explicit function of R and k.

1. Introduction

In this paper we investigate the solubility of a system of R simultaneous equations of the type

$$\left.\begin{array}{c} a_{11}x_1^k+\ldots+a_{1N}x_N^k=0, \\ \ldots \quad \ldots \quad \ldots \\ a_{R1}x_1^k+\ldots+a_{RN}x_N^k=0, \end{array}\right\} \tag{1}$$

in integers $x_1, \ldots, x_N$, not all 0. The coefficients a_{ij} are arbitrary integers. For brevity we describe equations of this type as *additive*. We denote the forms on the left of (1) by $f_1, \ldots, f_R$.

When k is odd we shall establish the following result.

Theorem 1. *Let k be an odd positive integer. The equations* (1) *have a solution in integers* $x_1, \ldots, x_N$, *not all* 0, *if*

$$N \geqslant [9R^2k\log 3Rk]. \tag{2}$$

When k is even we need to impose further conditions. We exclude the case $k=2$, partly to avoid some minor complications and partly because there may well be more effective methods for this case. We prove:

* This paper was written with the assistance of a research contract from the National Science Foundation of the U.S.A.

† Professor Davenport died on 9 June 1969.

THEOREM 2. *Let k be an even positive integer greater than 2. Suppose that*

(i) *the equations* (1) *have a real non-singular solution;*

(ii) *every set of S independent linear combinations of $f_1, \ldots, f_R$, with integral multipliers not all 0, contains explicitly at least*

$$[48RSk^3 \log 3Rk^2]$$

variables, and this holds for $S = 1, 2, \ldots, R$.

Then the equations (1) *have a solution in integers $x_1, \ldots, x_N$, not all 0.*

By a non-singular solution we mean one such that the matrix $(\partial f_i/\partial x_j)$, evaluated at the solution, has rank R.

The condition (ii) implies in particular, on taking $S = R$, that

$$N \geqslant [48R^2k^3 \log 3Rk^2].$$

There are good reasons for both the additional hypotheses in theorem 2, though it may be that they can be somewhat relaxed. Certainly the existence of a real solution, with $x_1, \ldots, x_N$ not all 0, must be postulated when k is even. But even then, neither of the conditions (i) and (ii) is by itself sufficient, as is shown by the following examples with $R = 2$.

Consider two additive equations of the form

$$a_1 x_1^k + \ldots + a_m x_m^k + a_{m+1} x_{m+1}^k + \ldots + a_N x_N^k = 0,$$

$$b_{m+1} x_{m+1}^k + \ldots + b_N x_N^k = 0,$$

where $b_{m+1}, \ldots, b_N$ are all positive and $a_1, \ldots, a_m$ are not all of the same sign. These two equations have a real solution with not all of $x_1, \ldots, x_N$ zero (though with $x_{m+1}, \ldots, x_N$ zero). If m is small in relation to k they may have no non-trivial integral solution. The equations may be chosen so as to satisfy (ii), but do not satisfy (i).

Or again, consider the same two equations but suppose now that $a_1, \ldots, a_m$ are all positive and $b_{m+1}, \ldots, b_N$ are not all of the same sign. If $N-m$ is small in relation to k the equations may have no non-trivial integral solution. The coefficients may be chosen so that (i) is satisfied, but (ii) will not be satisfied because of the smallness of $N-m$.

In principle the proof of theorems 1 and 2 follows the lines of the Hardy–Littlewood method for Waring's problem, as improved by Vinogradov. An essential preliminary is the determination of conditions which will ensure the solubility of the equations (1) in every p-adic field. This forms the subject-matter of §§ 2 to 4, and results in the following conclusion.

THEOREM 3. *The equations* (1) *have a solution in p-adic integers $x_1, \ldots, x_N$, not all 0, for every prime p, if*

$$N \geqslant \begin{cases} [9R^2k \log 3Rk] & \text{for } k \text{ odd,} \\ [48R^2k^3 \log 3Rk^2] & \text{for } k \text{ even.} \end{cases} \tag{3}$$

For the proof of theorems 1 and 2 we need not merely a p-adic solution but a non-singular p-adic solution. This cannot be ensured by any condition of the above kind, asserting only that N is greater than some function of R and k. On this question we prove theorem 4 in § 5; this incorporates conditions of a similar general nature to (ii) in theorem 2 above. As regards the application of this in the proof of theorem 1, we show in § 13, by induction on R, that the condition can be deemed to be satisfied. As regards the application in the proof of theorem 2, the condition is covered by (ii) in the hypothesis of that theorem.

We have not exercised great economy in the analytical work of §§ 6 to 12, since the final answer is dominated by that in theorem 3 for the p-adic problem. More precise results in the special case when $R = 2$ and $k = 3$ were obtained in an earlier paper (Davenport & Lewis 1966).

The principal results hitherto known that are relevant to our problem are those of Birch (1957) and Birch (1962). Both these papers are of much wider scope, in that they apply to homogeneous forms in general (not necessarily additive). The result of Birch (1957) relates to forms of odd degree, and implies our theorem 1, but with an unspecified function of R and k on the right of (2). The paper of 1962 (which does not restrict k to be odd) postulates the existence of a non-singular p-adic solution for every p, and of course the existence of a real non-singular solution if k is even, and contains also a condition which involves the dimension of the singular locus of the algebraic set (in complex space) defined by (1). The latter condition, in the case of additive equations, has some affinity with condition (ii) in theorem 2.

2. The solubility of congruences

In this section we prove various results concerning the solubility of R simultaneous congruences in n unknowns of the type

$$\left.\begin{array}{c} a_{11}x_1^k+\ldots+a_{1n}x_n^k \equiv 0 \pmod{p^\gamma}, \\ \ldots \qquad \ldots \qquad \ldots \\ a_{R1}x_1^k+\ldots+a_{Rn}x_n^k \equiv 0 \pmod{p^\gamma}. \end{array}\right\} \tag{4}$$

Here the a_{ij} are any integers (or residue classes to the modulus p^γ), and γ is any positive integer, though some of the results relate only to the case $\gamma = 1$. It will be convenient, in the present section only, to restrict the words *solution* and *solubility* to refer to solutions with at least one x_j not divisible by p.

We should emphasize that the results of this section are by no means exhaustive; they have been selected to cover our requirements, as will become apparent in the next section.

Lemma 1 (Chevalley). *Let $\gamma = 1$. The congruences* (4) *are soluble if*

$$n > Rk. \tag{5}$$

Proof. See Chevalley (1935). (The result holds more generally for any R homogeneous congruences modulo p of degree k.)

Lemma 2. *Let k be odd. The congruences* (4) *are soluble with each $x_j = 0$ or 1 or -1 if*

$$2^n > p^{\gamma R}. \tag{6}$$

Proof. We use a straightforward extension of an argument of Chowla & Shimura (1963). Define the linear forms $L_1, \ldots, L_R$ in $y_1, \ldots, y_n$ by

$$L_i(y_1, \ldots, y_n) = a_{i1}y_1+\ldots+a_{in}y_n.$$

Giving each y_j the values 0 and 1, we obtain 2^n sets of values for $L_1, \ldots, L_R$. The number of distinct possibilities for $L_1, \ldots, L_R$ to the modulus p^γ is $p^{\gamma R}$. The hypothesis (6) implies that the same set of values (mod p^γ) must arise from two different sets of $y_1, \ldots, y_n$, say $y'_1, \ldots, y'_n$ and $y''_1, \ldots, y''_n$. Then

$$L_i(y'_1-y''_1, \ldots, y'_n-y''_n) \equiv 0 \pmod{p^\gamma}.$$

The numbers $y'_j - y''_j$ are all 0 or 1 or -1, and not all 0. They satisfy

$$(y'_j - y''_j)^k = y'_j - y''_j.$$

Hence they provide a solution of (4), in the sense defined earlier.

LEMMA 3. *Let $\gamma = 1$ and let $n = 3R$. Suppose that the number of columns of the matrix (a_{ij}) in any set of columns of rank S (mod p) does not exceed $3S-2$, for $S = 1, 2, \ldots, R-1$. Then the congruences (4) with $\gamma = 1$ have a solution if*

$$p > (3Rk)^6. \tag{7}$$

Proof. We recall first that the values assumed by x^k modulo p as x varies are the same as the values assumed by x^δ, where $\delta = (k, p-1)$. Hence we may replace k by δ in (4).

We may suppose that for every j there is some i for which $a_{ij} \not\equiv 0 \pmod p$. For in the contrary case the congruences have an obvious solution with one x_j equal to 1 and the rest 0.

We follow a classical line of argument which expresses the number of solutions in terms of exponential sums. Let $\mathcal{N}$ denote the number of solutions of the congruences (4), with $\gamma = 1$, including the trivial solution in which all x_j are 0. We wish to prove that $\mathcal{N} > 1$. We have

$$\mathcal{N} = p^{-R} \sum_{u_1, \ldots, u_R} \sum_{x_1, \ldots, x_n} e_p(u_1 \Phi_1 + \ldots + u_R \Phi_R),$$

where all the variables run over complete sets of residues (mod p), and $e_p(m) = \mathrm{e}^{2\pi i m/p}$, and $\Phi_1, \ldots, \Phi_R$ denote the forms on the left of (4), with δ in place of k. We isolate the term p^{n-R} on the right coming from $u_1 = \ldots = u_R = 0$. In the other terms we note that

$$u_1 \Phi_1 + \ldots + u_R \Phi_R = \Lambda_1 x_1^\delta + \ldots + \Lambda_n x_n^\delta,$$

where
$$\Lambda_j = \Lambda_j(u_1, \ldots, u_R) = \sum_{i=1}^{R} a_{ij} u_i \quad (j = 1, \ldots, n).$$

Hence
$$\mathcal{N} - p^{n-R} = p^{-R} \sum_{u_1, \ldots, u_R}{}' \; T(\Lambda_1) \ldots T(\Lambda_n), \tag{8}$$

where the prime denotes that not all u_i are 0, and where

$$T(\Lambda) = \sum_x e_p(\Lambda x^\delta). \tag{9}$$

Let χ be a character (mod p) of exact order δ; such a character exists since δ divides $p-1$. The number of solutions of

$$x^\delta \equiv y \pmod p$$

is
$$1 + \chi(y) + \chi^2(y) + \ldots + \chi^{\delta-1}(y).$$

Hence
$$T(\Lambda) = \sum_y \{1 + \chi(y) + \ldots + \chi^{\delta-1}(y)\} e_p(\Lambda y).$$

If $\Lambda \not\equiv 0 \pmod p$, the sum arising from the term 1 vanishes, and each of the other sums is a Gaussian sum having absolute value $p^{\frac{1}{2}}$ (see, for example, Davenport 1962, pp. 42–43). Hence

$$|T(\Lambda)| \leqslant (\delta - 1) p^{\frac{1}{2}} \quad \text{if} \quad \Lambda \not\equiv 0 \pmod p; \tag{10}$$

and of course
$$T(\Lambda) = p \quad \text{if} \quad \Lambda \equiv 0 \pmod p. \tag{11}$$

Suppose $R = 1$. In this case the rank condition is of course void. There is only one congruence, and its coefficients a_j, say, are not divisible by p, by an earlier remark. We have

$\Lambda_j = a_j u$, and consequently $\Lambda_j \not\equiv 0 \pmod{p}$ when $u \not\equiv 0 \pmod{p}$. It follows from (8) and (10) that

$$|\mathcal{N} - p^{n-1}| \leqslant p^{-1} \sum_u{}' \, |T(\Lambda_1) \ldots T(\Lambda_n)|$$
$$\leqslant p^{-1}(p-1)\{(\delta-1)p^{\frac{1}{2}}\}^n.$$

We have $n = 3R = 3$. To get $\mathcal{N} > 1$ it suffices to have

$$p^{-1}(p-1)\{(\delta-1)p^{\frac{1}{2}}\}^3 < p^2 - 1.$$

This holds† if $(\delta-1)^3 < p^{\frac{1}{2}}$, which is true by (7) since $\delta - 1 < k$.

Suppose $R > 1$. We consider the sum on the right of (8). For any $u_1, \ldots, u_R$ we have

$$|T(\Lambda_1) \ldots T(\Lambda_n)| \leqslant p^{\nu}\{(\delta-1)p^{\frac{1}{2}}\}^{n-\nu},$$

where ν is the number of $\Lambda_1, \ldots, \Lambda_n$ that are congruent to $0 \pmod{p}$.

The linear forms $\Lambda_1, \ldots, \Lambda_n$ are constructed from the columns of the coefficient matrix (a_{ij}) in (4). If, for some $u_1, \ldots, u_R$, there are ν of the Λ_j that are $\equiv 0 \pmod{p}$, the rank of the matrix formed by the corresponding ν columns must be less than R. If this rank is S, the hypothesis of the lemma implies that

$$\nu \leqslant 3S - 2 \leqslant 3R - 5.$$

This bound for ν is valid for all $u_1, \ldots, u_R$ on the right of (8).

Consider the contribution made to the sum on the right of (8) by those $u_1, \ldots, u_R$ for which exactly ν of $\Lambda_1, \ldots, \Lambda_n$ are $\equiv 0 \pmod{p}$, where ν is $3R-5$ or $3R-6$ or $3R-7$. The rank of the ν corresponding columns must be exactly $R-1$, for by hypothesis any set of columns of rank $S \leqslant R-2$ can number at most $3(R-2)-2 = 3R-8$. The number of possible choices for ν columns out of $3R$ columns is $\binom{3R}{\nu}$, and when these are assigned, $u_1, \ldots, u_R$ have to satisfy a system of ν linear congruences of rank $R-1$. The number of possibilities for $u_1, \ldots, u_R$, not all 0, is $p-1$. Hence the contribution in question is

$$\leqslant \binom{3R}{3R-5} p^{3R-5}((\delta-1)p^{\frac{1}{2}})^5(p-1) + \binom{3R}{3R-6} p^{3R-6}((\delta-1)p^{\frac{1}{2}})^6(p-1)$$
$$+ \binom{3R}{3R-7} p^{3R-7}((\delta-1)p^{\frac{1}{2}})^7(p-1)$$
$$< (p-1)p^{3R}\left(\frac{(3R)^5}{5!}\alpha^5 + \frac{(3R)^6}{6!}\alpha^6 + \frac{(3R)^7}{7!}\alpha^7\right),$$

where $$\alpha = \frac{\delta-1}{p^{\frac{1}{2}}} < \frac{k}{p^{\frac{1}{2}}} < \frac{1}{3R} \tag{12}$$

by (7). Hence the contribution is less than

$$2(p-1)p^{3R}\frac{(3R\alpha)^5}{5!}.$$

Next consider the contribution made by those terms for which ν is $3R-8$ or $3R-9$ or $3R-10$. By similar reasoning, the rank of the ν corresponding columns is $R-2$. When these columns are assigned, the number of possibilities for $u_1, \ldots, u_R$ (satisfying a system of ν

† It is easily proved that in this particular case a weaker condition suffices.

congruences of rank $R-2$) is certainly at most p^2-1. It is, however, at most p^2-p. For we can find some further column to supplement the ν columns to give a set of rank $R-1$, and $u_1, \ldots, u_R$ must not make the additional linear form vanish. Hence from p^2-1 we can subtract $p-1$ sets $u_1, \ldots, u_R$ as being ineligible. Proceeding as before, we see that the contribution under consideration is less than

$$2(p^2-p)\,p^{3R}\,\frac{(3R\alpha)^8}{8!}.$$

We continue with groups of 3 consecutive values of ν, the last being $\nu = 4$ or 3 or 2. The terms with $\nu = 1$, treated in the same way, give a contribution less than

$$(p^{R-1}-p^{R-2})\,p^{3R}\,\frac{(3R\alpha)^{3R-1}}{(3R-1)!}.$$

Finally there is the contribution of all $u_1, \ldots, u_R$ for which none of the Λ_i vanish. The number of possibilities for $u_1, \ldots, u_R$ is at most $(p-1)^R$, since the columns of the matrix contain some subset of rank R, and none of the linear forms Λ_j corresponding to this subset can vanish. Thus the contribution is at most

$$(p-1)^R\,((\delta-1)\,p^{\frac{1}{2}})^{3R} = (p-1)^R p^{3R} \alpha^{3R}.$$

Collecting the estimates and substituting in (8), and recalling that $n = 3R$, we obtain

$$|\mathcal{N}-p^{2R}| < (p-1)\,p^{2R}\,V,$$

where

$$V = 2\frac{(3R\alpha)^5}{5!}+2p\,\frac{(3R\alpha)^8}{8!}+\ldots+2p^{R-3}\,\frac{(3R\alpha)^{3R-4}}{(3R-4)!}+p^{R-2}\,\frac{(3R\alpha)^{3R-1}}{(3R-1)!}+(p-1)^{R-1}\,\alpha^{3R}.$$

To prove that $\mathcal{N} > 1$ it will suffice to prove that

$$(p-1)\,p^{2R}\,V < p^{2R}-1,$$

and this will be satisfied if

$$V \leqslant p^{-1}.$$

By the hypothesis (7), together with (12),

$$p > (3Rk)^6 > (3R\alpha)^6 p^3.$$

Hence $3R\alpha < p^{-\frac{1}{3}}$. It follows that

$$V < 2p^{-\frac{5}{3}}\left(\frac{1}{5!}+\frac{1}{8!}+\ldots\right)+p^{R-1}\,(\tfrac{1}{3}p^{-\frac{1}{3}})^{3R}$$
$$< p^{-1}.$$

This completes the proof of lemma 3.

Lemma 4. *Let* $\gamma = 1$ *and let* $n = 3R$. *Then the congruences* (4) *have a solution if* (7) *holds.*

Proof. The result holds when $R = 1$, since (as noted in the proof of lemma 3) the rank condition in the hypothesis of lemma 3 is void in this case. We prove the result by induction on R. The inductive hypothesis is that the result holds when R is replaced by S throughout, for any $S < R$.

If the rank hypothesis of lemma 3 is satisfied, there is nothing to prove. If it is not, there is some set of $3S-1$ columns in the matrix (a_{ij}) with rank $S \pmod{p}$, for some $S < R$. Without loss of generality we can take these to be the first $3S-1$ columns. As far as these columns alone are concerned, there must be $R-S$ linear relations, independent $(\bmod p)$, between the rows. Hence, without affecting the solubility of the congruences, we can replace some $R-S$ of them by others in which the coefficients of the first $3S-1$ variables are divisible by p. Without loss of generality we can write the congruences as

$$\begin{array}{llll} a_{11}x_1^k+\dots & \dots & & +a_{1n}x_n^k \equiv 0 \pmod p, \\ \dots & & & \\ a_{S1}x_1^k+\dots & \dots & & +a_{Sn}x_n^k \equiv 0 \pmod p, \\ & & a_{S+1\,3S}x_{3S}^k+\dots & +a_{S+1\,n}x_n^k \equiv 0 \pmod p, \\ & & \dots & \\ & & a_{R\,3S}x_{3S}^k+\dots & +a_{Rn}x_n^k \equiv 0 \pmod p. \end{array}$$

By the inductive hypothesis, and the fact that $p > (3(R-S)\,k)^6$, there is a solution of the last $R-S$ congruences in the $n-3S+1 = 3(R-S)+1$ unknowns. (In fact $3(R-S)$ unknowns would suffice.) Denote the solution by $\xi_{3S}, \dots, \xi_n$. Put $x_j = t\xi_j$ for $j \geq 3S$. The first S congruences are now congruences of the type (4) in the $3S$ unknowns

$$x_1, \dots, x_{3S-1}, t.$$

By the inductive hypothesis, and the fact that $p > (3Sk)^6$, these have a solution. In this solution, one at least of the variables is not divisible by p, and so one at least of

$$x_1, \dots, x_{3S-1}, t\xi_{3S}, \dots, t\xi_n$$

is not divisible by p. We therefore have a solution of (4) in the sense defined, and this proves the lemma.

The results of lemmas 1, 2, 4 give conditions for the solubility of a system of additive congruences when k is odd and γ is arbitrary, and when k is even and γ is 1. There remains the case when k is even and $\gamma > 1$. For this we provide the following lemma, which is of a somewhat different character from those that precede. In the lemma itself no restrictions are imposed on k and γ.

LEMMA 5. *Suppose the $R \times n$ matrix (a_{ij}) includes m disjoint $R \times R$ matrices, each of which is non-singular* $(\bmod p)$. *Let*

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

Then the congruences (4) *have a solution provided that*

$$m-1 > \frac{3p^{2\gamma}\delta^2}{(p-1)^2}\log 2Rp^\gamma; \tag{13}$$

and this solution can be chosen to have $x_j = 1$ for all the R values of j corresponding to the columns of a particular one of the $R \times R$ matrices.

Proof. It is easily verified that the number of distinct values (not divisible by p) assumed by x^k to the modulus p is exactly $d = (p-1)/\delta$. Let $x_1^k, \dots, x_d^k$ be congruent $(\bmod p)$ to these d values. Take $\xi_1 = x_1^k, \dots, \xi_d = x_d^k$. Then $\xi_1, \dots, \xi_d$ are kth power residues modulo p^γ, and are distinct modulo p.

We can suppose that the columns $j = 1, \dots, R$ of the matrix (a_{ij}) have rank R, and similarly for the columns $R+1, \dots, 2R$, up to $(m-1)R+1, \dots, mR$. We put $x_j = 0$ for $j > mR$, and we put $x_j = 1$ for $(m-1)R < j \leqslant mR$ so as to satisfy the last clause of the lemma. It will suffice to solve the congruences

$$\sum_{j=1}^{(m-1)R} a_{ij} x_j \equiv b_i (\operatorname{mod} p^\gamma) \quad (i = 1, \dots, R)$$

for arbitrary $b_1, \dots, b_R$, subject to the condition that the values of each x_j are limited to the set $0, \xi_1, \dots, \xi_d$.

The number of solutions, say $\mathcal{N}$, is given by

$$p^{R\gamma}\mathcal{N} = \sum_{u_1, \dots, u_R} \sum_{x_1, \dots, x_{(m-1)R}} e_{p^\gamma}(u_1(a_{11}x_1 + \dots - b_1) + \dots),$$

where $u_1, \dots, u_R$ run mod p^γ, and each x_j runs through the set of values specified above. The contribution of $u_1 = \dots = u_R = 0$ is $(d+1)^{(m-1)R}$. Our aim is to prove that $\mathcal{N} > 0$.

We introduce the linear forms

$$\Lambda_j = \sum_{i=1}^{R} a_{ij} u_i \quad (1 \leqslant j \leqslant (m-1)R),$$

and define
$$U(\Lambda) = 1 + \sum_{\xi} e_{p^\gamma}(\Lambda\xi),$$

where ξ takes the values $\xi_1, \dots, \xi_d$. We have

$$|p^{R\gamma}\mathcal{N} - (d+1)^{(m-1)R}| \leqslant \sum_{u_1, \dots, u_R}{}' |U(\Lambda_1) \dots U(\Lambda_{(m-1)R})|,$$

where Σ' means that $u_1 = \dots = u_R = 0$ is excluded. It will suffice if

$$\sum_{u_1, \dots, u_R}{}' |U(\Lambda_1) \dots U(\Lambda_{(m-1)R})| < (d+1)^{(m-1)R}.$$

By Hölder's inequality, this will be true if

$$\sum_{u_1, \dots, u_R}{}' |U(\Lambda_1) \dots U(\Lambda_R)|^{m-1} < (d+1)^{(m-1)R},$$

since $\Lambda_1, \dots, \Lambda_R$ are typical of any one of the $m-1$ sets of R linearly independent forms corresponding to one of the $R \times R$ submatrices of coefficients.

Since $\Lambda_1, \dots, \Lambda_R$ are linear forms in $u_1, \dots, u_R$ with determinant not divisible by p, we can take them as independent variables mod p^γ, and replace them by $u_1, \dots, u_R$. Thus it suffices if

$$\sum_{u_1, \dots, u_R}{}' |U(u_1) \dots U(u_R)|^{m-1} < (d+1)^{(m-1)R}.$$

We add back the term $(d+1)^{(m-1)R}$ corresponding to $u_1 = \dots = u_R = 0$. Then the sum on the left factorizes, and the condition becomes

$$\sum_{u} |U(u)|^{m-1} < 2^{1/R}(d+1)^{m-1}, \tag{14}$$

where u runs through a complete set of residues $(\operatorname{mod} p^\gamma)$.

We have, for $u \not\equiv 0 \ (\operatorname{mod} p^\gamma)$,

$$|U(u)|^2 = \left|1 + \sum_{r=1}^{d} e_{p^\gamma}(u\xi_r)\right|^2$$
$$= d + 1 + 2\sum_{r=1}^{d} \cos\frac{2\pi u\xi_r}{p^\gamma} + \sum_{s \neq r} \cos\frac{2\pi u(\xi_r - \xi_s)}{p^\gamma}.$$

We have $$\cos\theta = 1-2\sin^2\tfrac{1}{2}\theta \leqslant 1-2\pi^{-2}\theta^2$$
for $|\theta| \leqslant \pi$. Put $u\xi_r \equiv \eta_r \pmod{p^\gamma}$, where $|\eta_r| \leqslant \frac{1}{2}p^\gamma$. Then $\eta_1, \ldots, \eta_d$ are distinct since $\xi_1, \ldots, \xi_d$ are incongruent $(\operatorname{mod} p)$, and they are non-zero. We have

$$\sum_{r=1}^{d} \cos\frac{2\pi u\xi_r}{p^\gamma} = \sum_{r=1}^{d} \cos\frac{2\pi\eta_r}{p^\gamma} \leqslant \sum_{r=1}^{d}\left\{1-8\left(\frac{\eta_r}{p^\gamma}\right)^2\right\}.$$

Plainly $\Sigma\eta_r^2$ is minimal when the η_r consist of $1, 2, \ldots, d'$ and $-1, -2, \ldots, -d''$, where $d'+d''=d$, and its value then is at least $\frac{1}{12}d(d+1)(d+2)$. A similar argument applies to the double sum over r and s, in so far as we sum over s for fixed r. Hence

$$|U(u)|^2 \leqslant (d+1)^2 - \frac{8}{12}\frac{1}{p^{2\gamma}}d(d+1)(d+2) - \frac{8}{12}\frac{1}{p^{2\gamma}}\sum_{r=1}^{d} d(d+1)(d+2)$$
$$= (d+1)^2\left\{1-\frac{2}{3}\frac{d(d+2)}{p^{2\gamma}}\right\}.$$

We see that (14) will be satisfied if

$$1+(p^\gamma-1)\left\{1-\frac{2}{3}\frac{d(d+2)}{p^{2\gamma}}\right\}^{\frac{1}{2}(m-1)} < 2^{1/R}.$$

Since $$2^{1/R} = \exp\,(R^{-1}\log 2) > 1+\tfrac{1}{2}R^{-1},$$

this will hold if $$p^\gamma\left\{1-\frac{2}{3}\frac{d(d+2)}{p^{2\gamma}}\right\}^{\frac{1}{2}(m-1)} < (2R)^{-1},$$

and so if $$\tfrac{1}{2}(m-1)\log\left\{1-\frac{2}{3}\frac{d(d+2)}{p^{2\gamma}}\right\} < \log\frac{1}{2Rp^\gamma}.$$

Thus it will suffice if $$m-1 > 3\frac{p^{2\gamma}}{d^2}\log 2Rp^\gamma.$$

This is the condition (13).

We add some minor remarks on the results that precede.

(i) In the inequalities (5) and (7) of lemmas 1 and 3 one could replace k by $\delta = (k, p-1)$.

(ii) Lemma 2 is sometimes applicable when k is even. The essential condition is that -1 should be a kth power residue modulo p^γ.

(iii) Lemma 3, like lemma 5, applies in principle to non-homogeneous congruences.

3. Solutions of rank R

We continue to be concerned with the congruences (4) of § 2, which we rewrite here for convenience of reference:

$$\left.\begin{aligned} \Phi_1 &= a_{11}x_1^k+\ldots+a_{1n}x_n^k \equiv 0 \pmod{p^\gamma},\\ &\ldots \qquad \ldots \qquad \ldots\\ \Phi_R &= a_{R1}x_1^k+\ldots+a_{Rn}x_n^k \equiv 0 \pmod{p^\gamma}.\end{aligned}\right\} \tag{15}$$

But from now on we fix the value of γ as a function of p and k as follows: let p^τ be the exact power of p dividing k, and let

$$\gamma = \gamma(k,p) = \begin{cases} 1 & \text{if } \tau = 0,\\ \tau+1 & \text{if } \tau > 0 \text{ and } p > 2,\\ \tau+2 & \text{if } \tau > 0 \text{ and } p = 2.\end{cases} \tag{16}$$

Thus $\gamma > 1$ if and only if p divides k. This choice of γ is designed to ensure that solubility (mod p^γ), subject to a supplementary condition (rank R, defined later), will ensure p-adic solubility (see lemma 9). We record for future reference the fact that

$$k \geqslant \gamma. \tag{17}$$

This is trivial if p does not divide k, since then $\gamma = 1$. If p divides k, and p^τ divides k exactly, then

$$k \geqslant p^\tau \geqslant 2^\tau \geqslant \tau+1.$$

This proves (17) if $p > 2$. And if $p = 2$ we get strict inequality, giving $k \geqslant \tau+2$, unless $\tau = 1$ and $k = 2$, a case which was excluded in § 1.

LEMMA 6. *Suppose that either k is odd, or k is even and p does not divide k. Define $n_0 = n_0(k, R)$ by*

$$n_0 = \begin{cases} [9R\log 3Rk] & \text{if } k \text{ is odd,} \\ Rk+1 & \text{if } k \text{ is even and } p \nmid k. \end{cases} \tag{18}$$

Then if $n \geqslant n_0$ the congruences (15) *have a solution with not all of $x_1, \ldots, x_n$ divisible by p.*

Proof. We appeal to the results of § 2 with γ as defined in (16).

If k is odd and $p \nmid k$, so that $\gamma = 1$, we apply lemma 2, provided that

$$p < (3Rk)^6. \tag{19}$$

The desired solution exists if

$$n > \frac{R\log p}{\log 2}.$$

Since
$$\frac{R\log p}{\log 2} < \frac{R\log (3Rk)^6}{0\cdot 69} < 8\cdot 7R\log 3Rk < 9R\log 3Rk - 1,$$

the solution exists if $n \geqslant [9R\log 3Rk]$. If (19) is not satisfied we can use lemma 4, which gives solubility if $n \geqslant 3R$.

If k is odd and $p|k$ we have $\gamma = \tau+1$, where p^τ divides k exactly. We appeal to lemma 2, which assures solubility if

$$n > \frac{R\log p^\gamma}{\log 2}.$$

Now
$$\frac{R\log p^\gamma}{\log 2} = \frac{R\log p^{\tau+1}}{\log 2} < \frac{2R\log p^\tau}{0\cdot 69} < 3R\log k.$$

The last number is plainly less than $9R\log 3Rk - 1$, and the result follows.

If k is even and $p \nmid k$ we have $\gamma = 1$, and we appeal to lemma 1, which gives solubility if $n > Rk$. This completes the proof.

DEFINITION. *A solution* $\mathbf{x} = \boldsymbol{\xi}$ *of the congruences* (15) *will be said to be of rank S if the matrix*

$$(a_{ij}\xi_j^{k-1}) \tag{20}$$

has rank S (mod p). This is the same as saying that the matrix

$$(a_{ij}\xi_j) \tag{21}$$

has rank S (mod p), and this in turn is the same as saying that the rank of the matrix formed from (a_{ij}) by taking only those j for which $\xi_j \not\equiv 0 \pmod p$ is S.

Our aim is to find conditions, expressed in terms of k and R only, which will ensure that the congruences (15) have a solution of rank R. As we shall see in lemma 9 below, this implies that the corresponding equations have a non-trivial solution in the p-adic field. We follow two different lines of argument, one based on lemma 6 above (when it is applicable), and the other based on lemma 5.

LEMMA 7. *Suppose that either k is odd, or k is even and p does not divide k. Suppose that for every j there is at least one i for which $a_{ij} \not\equiv 0 \pmod{p}$. Suppose that any form*

$$g_1\Phi_1+\ldots+g_R\Phi_R, \tag{22}$$

where $g_1, \ldots, g_R$ are not all divisible by p, contains at least n_0 coefficients not divisible by p, where n_0 is defined by (18). *Then the congruences* (15) *have a solution of rank R.*

Proof. The hypothesis concerning the form (22) implies, in particular, that $n \geqslant n_0$. Hence the congruences (15) have a solution $\mathbf{x} = \boldsymbol{\xi}$ with not all of $\xi_1, \ldots, \xi_n$ divisible by p. This solution has rank at least 1, since some $\xi_j \not\equiv 0 \pmod{p}$ and for this j some $a_{ij} \not\equiv 0 \pmod{p}$.

We choose a solution $\mathbf{x} = \boldsymbol{\xi}$ of maximal rank $\pmod{p}$. If this rank is R there is no more to prove. So we may suppose that this rank is S, where $1 \leqslant S < R$.

We define $\mathscr{J}$ to be the set of all those suffixes j for which $\xi_j \not\equiv 0 \pmod{p}$. The rank of those columns a_{ij} for which $j \in \mathscr{J}$ is S.

We select all those columns of coefficients which are linearly dependent $\pmod{p}$ on those of $\mathscr{J}$. Without loss of generality we can take these to be the columns $j = 1, 2, \ldots, \nu$; these columns have rank S. Any column with $j > \nu$ is linearly independent $\pmod{p}$ of the columns with $j \leqslant \nu$.

Since the rank $\pmod{p}$ of the columns $j = 1, \ldots, \nu$ is $S < R$, there is some linear combination of $\Phi_1, \ldots, \Phi_R$ in which the variables $x_1, \ldots, x_\nu$ occur only with coefficients divisible by p. The number of coefficients not divisible by p is at most $n-\nu$. The hypothesis of the lemma implies that

$$n-\nu \geqslant n_0. \tag{23}$$

From the fact that $\mathbf{x} = \boldsymbol{\xi}$ is a solution of the congruences (15), we have

$$\sum_{j=1}^{n} a_{ij}\xi_j^k \equiv 0 \pmod{p^\gamma} \quad \text{for} \quad 1 \leqslant i \leqslant R. \tag{24}$$

Now $\xi_j \equiv 0 \pmod{p}$ for $j > \nu$, since all suffixes with $j > \nu$ are outside the set $\mathscr{J}$. By (17) we have $k \geqslant \gamma$, and this enables us to replace (24) by

$$\sum_{j=1}^{\nu} a_{ij}\xi_j^k \equiv 0 \pmod{p^\gamma} \quad \text{for} \quad 1 \leqslant i \leqslant R. \tag{25}$$

We turn our attention to the congruences

$$\sum_{j=\nu+1}^{n} a_{ij}x_j^k \equiv 0 \pmod{p^\gamma} \quad \text{for} \quad 1 \leqslant i \leqslant R. \tag{26}$$

Since $n-\nu \geqslant n_0$ by (23), lemma 6 applies, and these have a solution $\mathbf{x} = \boldsymbol{\eta}$ with not all of $\eta_{\nu+1}, \ldots, \eta_n$ divisible by p, say $\eta_{\nu+1} \not\equiv 0 \pmod{p}$.

It follows from (25) and (26) that

$$\xi_1, \ldots, \xi_\nu, \eta_{\nu+1}, \ldots, \eta_n$$

is a solution of the congruences (15). Moreover, it is a solution of rank at least $S+1$. For we have $\xi_j \not\equiv 0 \pmod{p}$ for $j \in \mathscr{J}$, and $\eta_{\nu+1} \not\equiv 0 \pmod{p}$, and the rank of the columns of $\mathscr{J}$ together with the column $j = \nu+1$ is $S+1$, since the latter column is independent of the former set, which themselves have rank S.

This solution of rank at least $S+1$ gives a contradiction to the maximal choice of S, and so the proof is complete.

LEMMA 8. *Suppose that k is even and that p divides k. Suppose that any form* (22), *where $g_1, \ldots, g_R$ are not all divisible by p, contains more than $(m-1)R$ coefficients not divisible by p, where m satisfies*

$$m \geqslant [48k^2 \log 3Rk^2]. \tag{27}$$

Then the congruences (15) *have a solution of rank R.*

Proof. We observe first that the hypothesis (27) ensures that m satisfies the condition (13) of lemma 5. For we have

$$m-1 \geqslant [48k^2 \log 3Rk^2]-1 > 48k^2 \log 2Rk^2.$$

If $p > 2$,

$$\frac{3p^{2\gamma}\delta^2}{(p-1)^2}\log 2Rp^{\gamma} = \frac{3p^{2\tau+2}\delta^2}{(p-1)^2}\log(2Rp^{\tau+1}) \leqslant 3k^2\left(\frac{p}{p-1}\right)^2 \log(2Rk^2) \leqslant \tfrac{27}{4}k^2 \log 2Rk^2,$$

since $k \geqslant p^{\tau}\delta$. If $p = 2$, so that $\delta = p-1 = 1$,

$$\frac{3p^{2\gamma}\delta^2}{(p-1)^2}\log(2Rp^{\gamma}) = 3\times 2^{2\tau+4}\log(2^{\tau+3}R).$$

If $\tau = 1$ this is $\qquad 192\log 16R < 48k^2 \log(2Rk^2),$

since $k \geqslant 4$. If $\tau \geqslant 2$ it is $\qquad \leqslant 48k^2\log(2Rk^2).$

This proves the statement made initially.

It suffices now to prove that the hypothesis concerning any form (22) implies that the matrix (a_{ij}) includes m disjoint $R\times R$ matrices, each non-singular $\pmod{p}$. For then lemma 5 ensures that the congruences (15) have a solution in which some R of the x_j, corresponding to the columns of one of these matrices, are all 1. This is a solution of rank R.

The proof of the existence of the disjoint matrices does not require the condition on m in (27). We note first that the hypothesis concerning any form (22) implies that $n \geqslant mR$; for it is always possible to construct a linear combination (22) of $\Phi_1, \ldots, \Phi_R$ in which the coefficients of any specified $R-1$ variables are $\equiv 0 \pmod{p}$, and the hypothesis implies that $n-(R-1) > (m-1)R$, whence $n \geqslant mR$.

The rank $\pmod{p}$ of the whole matrix (a_{ij}) is R, for otherwise it would be possible to form a linear combination of the rows in which all entries were divisible by p, and this would give a form (22) in which all the coefficients would be divisible by p, contrary to hypothesis. Hence it is possible to select R columns of rank $R \pmod{p}$, and we may take these to be the first R.

If we disregard these R columns, the rank of the remaining columns is still R, provided that $m \geqslant 2$. For if it were less than R we could construct a form (22) in which all the coefficients other than the first R would be divisible by p. This would imply that $R > (m-1)R$, which is false. Hence it is possible to select a second set of R columns, of rank R (mod p), disjoint from the first.

It is plain that the argument is general; if $m \geq 3$ we can select a third set of R columns, and so on. This proves the lemma.

Lemma 9. *Let the coefficients a_{ij} in (15) be rational integers. If the congruences (15) have a solution of rank R, then the equations corresponding to (15) have a non-trivial p-adic solution.*

Proof. The definition of γ adopted in (16) ensures that the solubility of $x^k \equiv m \pmod{p^\gamma}$, where $m \not\equiv 0 \pmod{p}$, implies the solubility of $y^k \equiv m \pmod{p^\nu}$ for every ν with $y \equiv x \pmod{p^\gamma}$. For a proof of this classical result, see, for example, Davenport (1962, lemma 9 of § 5).

Let $\mathbf{x} = \boldsymbol{\xi}$ be a solution of the congruences (15) of rank R, as postulated. Then there exist R values of j such that $\xi_j \not\equiv 0 \pmod{p}$ and such that the corresponding columns of the matrix (a_{ij}) have rank R (mod p). Without loss of generality we can take these to be $j = 1, \ldots, R$.

Let $\nu > \gamma$ be a positive integer. Since the determinant of the first R columns of coefficients is not divisible by p, there exist R linear combinations of $\Phi_1, \ldots, \Phi_R$ which, considered modulo p^ν, are of the following form:

$$\left.\begin{aligned} \Phi_1' &= c_1 x_1^k + \Psi_1(x_{R+1}, \ldots, x_n), \\ &\cdots \quad \cdots \quad \cdots \\ \Phi_R' &= c_R x_R^k + \Psi_R(x_{R+1}, \ldots, x_n), \end{aligned}\right\} \tag{28}$$

where $c_1 c_2 \ldots c_R \not\equiv 0 \pmod{p}$. These linear combinations are formed with rational integral multipliers, the determinant of which is not divisible by p.

We have $$\Phi_1'(\boldsymbol{\xi}) \equiv 0 \pmod{p^\gamma}, \ldots, \Phi_R'(\boldsymbol{\xi}) \equiv 0 \pmod{p^\gamma}$$

and since none of $\xi_1, \ldots, \xi_R$ are divisible by p it follows that

$$\Psi_i(\xi_{R+1}, \ldots, \xi_n) \not\equiv 0 \pmod{p} \quad \text{for} \quad i = 1, \ldots, R.$$

By the principle mentioned at the beginning of the proof, there exist $\eta_1, \ldots, \eta_R$ such that

$$c_i \eta_i^k + \Psi_i(\xi_{R+1}, \ldots, \xi_n) \equiv 0 \pmod{p^\nu}$$

for $i = 1, \ldots, R$, and $\eta_i \equiv \xi_i \pmod{p^\gamma}$. Thus

$$\eta_1, \ldots, \eta_R, \xi_{R+1}, \ldots, \xi_n$$

constitutes a solution of $$\Phi_1 \equiv 0 \pmod{p^\nu}, \ldots, \Phi_R \equiv 0 \pmod{p^\nu} \tag{29}$$

with none of $x_1, \ldots, x_R$ divisible by p.

The existence of such a solution of (29) for every $\nu > \gamma$ implies, by a familiar p-adic compactness argument, the non-trivial solubility of the equations

$$\Phi_1 = 0, \ldots, \Phi_R = 0$$

in the p-adic field. Hence the result. We would add that an alternative proof of the present lemma could be given on the lines of the proof of Hensel's lemma.

Remark. In view of lemma 9, lemmas 7 and 8 give sufficient conditions for a system of R equations of additive type to have a non-trivial p-adic solution. The resulting p-adic solution is in fact non-singular. But even though our ultimate aim is to obtain a non-singular p-adic solution, we can make no use of the fact that the solution provided by lemma 9 is non-singular. The reason for this is that we are unable to derive, from a given set of equations, a set which satisfies the hypotheses of lemmas 7 and 8 without employing a variational procedure, as will be seen in the proof of theorem 3 below. In the course of this process the non-singularity of a solution is lost, and it has to be restored (at a price) by the arguments of § 5.

4. p-ADIC SOLUBILITY

We are concerned with R additive forms of degree k:

$$\left.\begin{aligned} f_1 &= a_{11}x_1^k+\ldots+a_{1N}x_N^k, \\ &\ldots \quad \ldots \quad \ldots \\ f_R &= a_{R1}x_1^k+\ldots+a_{RN}x_N^k, \end{aligned}\right\} \tag{30}$$

with integral coefficients a_{ij}. Our aim in the present section is to prove theorem 3, which we restate for the convenience of the reader.

THEOREM 3. *Let*

$$N_0 = N_0(R) = \begin{cases} [9R^2k\log 3Rk] & \text{for } k \text{ odd,} \\ [48R^2k^3\log 3Rk^2] & \text{for } k \text{ even.} \end{cases} \tag{31}$$

Then, provided $N \geqslant N_0$, *the equations* $f_1 = 0, \ldots, f_R = 0$ *have a solution in each p-adic field, with not all the* x_j *zero.*

It will be apparent from the form of the theorem that for any particular prime p the result remains true if the coefficients a_{ij} are allowed to be p-adic numbers.

We begin by defining

$$\vartheta(f_1, \ldots, f_R) = \prod_{j_1, \ldots, j_R} \det(a_{ij_i}) \quad (i = 1, \ldots, R), \tag{32}$$

where the product is extended over all subsets of R distinct suffixes $j_1, \ldots, j_R$ from $1, 2, \ldots, N$, two subsets being considered the same only if they are identical. The number of these subsets is

$$M = N(N-1)\ldots(N-R+1).$$

The invariance properties of ϑ are given in the following lemma.

LEMMA 10. (i) *If*

$$f_i'(x_1, \ldots, x_N) = f_i(p^{\nu_1}x_1, \ldots, p^{\nu_N}x_N)$$

for $i = 1, \ldots, R$, *then*

$$\vartheta(f_1', \ldots, f_R') = p^{kRM\nu/N}\vartheta(f_1, \ldots, f_R),$$

where

$$\nu = \nu_1+\ldots+\nu_N.$$

(ii) *If*

$$f_i''(x_1, \ldots, x_N) = \sum_{j=1}^{R} d_{ij}f_j \quad (i = 1, \ldots, R),$$

where

$$\det d_{ij} = D \neq 0,$$

then

$$\vartheta(f_1'', \ldots, f_R'') = D^M\vartheta(f_1, \ldots, f_R).$$

Proof. (i) We have $a_{ij}' = p^{k\nu_j}a_{ij}$, and therefore

$$\det(a_{ij_i}') = p^{k\mu}\det(a_{ij_i}),$$

where
$$\mu = \nu_{j_1} + \ldots + \nu_{j_R}.$$

When we sum μ over all the M subsets of R distinct suffixes $j_1, \ldots, j_R$, we get $MR\nu/N$, whence the result.

(ii) We have
$$a''_{ij} = \sum_{h=1}^{R} d_{ih} a_{hj},$$
and therefore
$$\det(a''_{ij_i}) = D \det(a_{ij_i}),$$
whence the result.

As in Davenport & Lewis (1966), we define two sets of forms $f_1, \ldots, f_R$, with rational integral coefficients, to be *p-equivalent* if one set can be obtained from the other by a combination of the operations (i) and (ii) of lemma 10. Here $\nu_1, \ldots, \nu_N$ are integers (positive, negative or zero) and the d_{ij} are rational numbers with $D \neq 0$. The operations (i) and (ii) are commutative. If the equations
$$f_1 = 0, \ldots, f_R = 0$$
have a simultaneous non-trivial solution in the p-adic field, then so do the equations of any p-equivalent system.

We shall suppose initially that
$$\vartheta(f_1, \ldots, f_R) \neq 0, \tag{33}$$
and shall then show later how this limitation can be removed.

From all systems of forms that are p-equivalent to the given system, subject to the limitation of having integral coefficients, we select one for which the power of p dividing $\vartheta(f_1, \ldots, f_R)$ is least. This is possible because (33) holds for each such system. Such a system of forms will be said to be *p-normalized*. The following lemma, which gives some of the properties of a p-normalized system of forms, is similar in principle to lemma 2 of Davenport & Lewis (1966). It is simpler in that it contains no assertion about the parts of the forms that are divisible by p, but since R is now arbitrary (instead of being 2), the assertions about the forms F_i are more detailed.

LEMMA 11. *A p-normalized system of additive forms can be written (after renumbering the variables) as*
$$f_i = F_i(x_1, \ldots, x_n) + pG_i(x_{n+1}, \ldots, x_N) \tag{34}$$
for $i = 1, \ldots, R$, *where*
$$n \geq N/k \tag{35}$$
and each of $x_1, \ldots, x_n$ *occurs in one at least of* $F_1, \ldots, F_R$ *with a coefficient not divisible by* p.

Moreover, if we form any S linear combinations of $F_1, \ldots, F_R$ *(these combinations being independent* mod p), *and denote by* q_S *the number of variables that occur in one at least of these combinations with a coefficient not divisible by p, then*
$$q_S \geq SN/Rk \quad (S = 1, \ldots, R-1). \tag{36}$$

Proof. We have stated (35) first, for the sake of clarity, but it can also be regarded as the case $S = R$ of (36).

We obtain (34) simply by including in the forms F_i all those variables that occur in one at least of the f_i with a coefficient not divisible by p, and then renumbering these variables as $x_1, \ldots, x_n$. We have to prove (35) and (36).

Consider the forms

$$p^{-1}f_i(px_1, \ldots, px_n, x_{n+1}, \ldots, x_N) = p^{k-1}F_i(x_1, \ldots, x_n) + G_i(x_{n+1}, \ldots, x_N).$$

These are derived from the forms $f_i(x_1, \ldots, x_N)$ by a combination of the operations (i) and (ii) of lemma 10. Operation (i) is used with $\nu = n$, and operation (ii) with $D = p^{-R}$. Hence the value of ϑ for the new forms is obtained from that for the old forms by multiplying by

$$p^{kRMn/N-RM}.$$

Since the new forms have integral coefficients, it follows from the minimal choice made in the definition of a p-normalized system that $n \geqslant N/k$. This proves (35).

Let $F'_1, \ldots, F'_S$, be any S linear combinations of $F_1, \ldots, F_R$, independent $(\text{mod}\, p)$, and let $f'_1, \ldots, f'_S$ be the same linear combinations of $f_1, \ldots, f_R$. Each set can be completed (by taking the same $R-S$ of $F_1, \ldots, F_R$ or $f_1, \ldots, f_R$) to give a set of R linear combinations, independent $(\text{mod}\, p)$. Then $f'_1, \ldots, f'_R$ are derived from $f_1, \ldots, f_R$ by operation (ii) with D not divisible by p. Let $q\ (= q_S)$ be the number of variables that occur in one at least of $F'_1, \ldots, F'_S$ with a coefficient not divisible by p, and take these variables to be $x_1, \ldots, x_q$. The forms

$$p^{-1}f'_i(px_1, \ldots, px_q, x_{q+1}, \ldots, x_N) \quad (i = 1, \ldots, S),$$
$$f'_i(px_1, \ldots, px_q, x_{q+1}, \ldots, x_N) \quad (i = S+1, \ldots, R),$$

have integral coefficients. They are derived from $f_1, \ldots, f_R$ by a combination of operation (i) with $\nu = q$ and operation (ii) with $D = p^{-S}D_0$, where D_0 is not divisible by p. The same argument as before gives

$$kRMq/N - SM \geqslant 0$$

whence (36).

Proof of theorem 3. Suppose first that (33) holds. We can then take $f_1, \ldots, f_R$ to be a p-normalized system.

If k is odd, or if k is even and p does not divide k, we appeal to lemmas 7, 9, and 11. The definition of q_1 in lemma 11 means that any form (22) has at least q_1 coefficients not divisible by p. Hence the hypothesis of lemma 7 will be satisfied if $q_1 \geqslant n_0$, which will be so if $N \geqslant Rkn_0$. In view of the definition of n_0 in (18), this is ensured by the hypothesis $N \geqslant N_0$, where N_0 is defined in (31).

If k is even and p divides k, we appeal to lemma 8 instead of to lemma 7. The condition of that lemma will be satisfied if $q_1 \geqslant (m-1)R$, where $m \geqslant [48k^2 \log 3Rk^2]$. This will be so if

$$N/Rk \geqslant R[48k^2 \log 3Rk^2]$$

and this is ensured by the hypothesis $N \geqslant N_0$, where N_0 is defined in (31).

Now suppose that $\vartheta(f_1, \ldots, f_R) = 0$. It is obvious that for any μ there exist forms

$$f_i^{(\mu)} = \sum_{j=1}^{N} a_{ij}^{(\mu)} x_j^k \quad (i = 1, \ldots, R),$$

with rational integral coefficients, such that

$$\vartheta(f_1^{(\mu)}, \ldots, f_R^{(\mu)}) \neq 0$$

and such that $a_{ij}^{(\mu)} - a_{ij}$ is divisible by p^μ for every i and j. By what has been proved above, the equations

$$f_i^{(\mu)}(\mathbf{x}) = 0 \quad (i = 1, \ldots, R)$$

have a non-trivial p-adic integral solution $\mathbf{x} = \mathbf{x}^{(\mu)}$; and since the equations are homogeneous we can suppose that one coordinate at least of $\mathbf{x}^{(\mu)}$ is not divisible by p. Thus the point $\mathbf{x}^{(\mu)}$ lies on the surface of the cube $|x_j|_p \leqslant 1$ in the space of points with p-adic coordinates. Here $|\dots|_p$ denotes the p-adic valuation. If μ goes to infinity through a suitable sequence, then

$$\lim_{\mu\to\infty} \mathbf{x}^{(\mu)} = \mathbf{x}$$

exists in the p-adic sense and is not the origin. We have

$$f_i(\mathbf{x}) = \lim_{\mu\to\infty} f_i(\mathbf{x}^{(\mu)}),$$

and

$$\begin{aligned} |f_i(\mathbf{x}^{(\mu)})|_p &= |f_i(\mathbf{x}^{(\mu)}) - f_i^{(\mu)}(\mathbf{x}^{(\mu)})|_p \\ &= \left|\sum_{j=1}^{N} (a_{ij} - a_{ij}^{(\mu)})\,(x_j^{(\mu)})^k\right|_p \\ &\leqslant p^{-\mu}. \end{aligned}$$

It follows that

$$f_i(\mathbf{x}) = 0.$$

This completes the proof of theorem 3.

5. Non-singular p-adic solubility

Let $f_1, \dots, f_R$ be additive forms with rational integral coefficients, as in (30). Our object is to establish, under certain conditions, the existence of a non-singular solution of the equations

$$f_1 = 0, \dots, f_R = 0 \tag{37}$$

in every p-adic field. We prove:

Theorem 4. *Let*

$$N_0(R) = \begin{cases} [9R^2k \log 3Rk] & \text{if} \quad k \text{ is odd,} \\ [48R^2k^3 \log 3Rk^2] & \text{if} \quad k \text{ is even.} \end{cases} \tag{38}$$

For $S = 1, \dots, R$, let Q_S denote the minimum number of terms that occur, with at least one non-zero coefficient, in any S independent linear combinations of $f_1, \dots, f_R$. Suppose that

$$Q_S \geqslant N_0(S) \quad \text{for} \quad S = 1, \dots, R. \tag{39}$$

Then for every p the equations (37) *have a non-singular p-adic solution.*

Proof. We can suppose that every column contains some non-zero entry, since columns of zeros can be removed without affecting the hypothesis (39).

We follow initially the argument of lemma 7, but in the p-adic field instead of in the mod p field. Let $J = (\partial f_i/\partial x_j)$ denote the Jacobian matrix, of order $R \times N$, of the forms (30). For any prime p the equations (37) have a non-trivial p-adic integral solution by theorem 3, since (39) implies that $N \geqslant N_0(R)$. Clearly the rank of J at any such solution is positive. We choose a p-adic integral solution $\mathbf{x} = \boldsymbol{\xi}$ for which J has greatest rank, and denote this rank by S. If $S = R$ the solution is non-singular, so we may suppose that $S < R$.

If we replace $f_1, \dots, f_R$ by any R independent linear combinations of them, with rational integral multipliers, we do not change the solutions of (37), nor do we change the rank of the Jacobian at a solution.

We can form R such linear combinations $f'_1, \ldots, f'_R$, so that, after renumbering the variables, they have the form

$$f'_i = c_i x_i^k + \sum_{j=S+1}^{N} a_{ij} x_j^k \quad (1 \leqslant i \leqslant S),$$

$$f'_i = \sum_{j=S+1}^{N} a_{ij} x_j^k \quad (S < i \leqslant R),$$

where $c_i \neq 0$ and $\xi_1 \neq 0, \ldots, \xi_S \neq 0$. If $\xi_j \neq 0$ for some $j > S$ we must have $a_{ij} = 0$ for $i > S$, since otherwise the solution $\boldsymbol{\xi}$ would have rank greater than S. Selecting all those later columns that are linearly dependent on the first S, and numbering them $S+1, \ldots, \nu$, we can rewrite $f'_1, \ldots, f'_R$ in the form

$$\left.\begin{aligned} f'_i &= c_i x_i^k + \sum_{j=S+1}^{\nu} a_{ij} x_j^k + \sum_{j=\nu+1}^{N} a_{ij} x_j^k \quad (1 \leqslant i \leqslant S),\\ f'_i &= \sum_{j=\nu+1}^{N} a_{ij} x_j^k \quad (S < i \leqslant R), \end{aligned}\right\} \tag{40}$$

where, for $j > \nu$, $a_{ij} \neq 0$ for some $i > S$. We have $\xi_j = 0$ for $j > \nu$. By hypothesis,

$$c_i \xi_i^k + \sum_{j=S+1}^{\nu} a_{ij} \xi_j^k = 0 \quad (1 \leqslant i \leqslant S). \tag{41}$$

The forms $f'_{S+1}, \ldots, f'_R$ are $R-S$ independent linear combinations of $f_1, \ldots, f_R$ and contain only $N-\nu$ variables. The hypothesis of the present theorem tells us that

$$N-\nu \geqslant N_0(R-S).$$

It follows from theorem 3 that the equations

$$f'_{S+1} = 0, \ldots, f'_N = 0$$

have a non-trivial p-adic solution in $x_{\nu+1}, \ldots, x_N$, say $x_j = \eta_j$ $(\nu < j \leqslant N)$. Put

$$A_i = \sum_{j=\nu+1}^{N} a_{ij} \eta_j^k \quad (1 \leqslant i \leqslant S).$$

In the equations $f'_1 = 0, \ldots, f'_S = 0$ we put

$$\begin{aligned} x_j &= \xi_j + t_j \quad &&\text{for} \quad j \leqslant S,\\ x_j &= \xi_j &&\text{for} \quad S < j \leqslant \nu,\\ x_j &= z\eta_j &&\text{for} \quad \nu < j \leqslant R. \end{aligned}$$

By virtue of (41), the equations become

$$k c_i \xi_i^{k-1} t_i + \binom{k}{2} c_i \xi_i^{k-2} t_i^2 + \ldots + c_i t_i^k + A_i z^k = 0 \quad \text{for} \quad 1 \leqslant i \leqslant S.$$

Take z to be divisible by a large power of p. Then, since $c_i \xi_i^{k-1} \neq 0$, each separate equation is soluble for t_i in the p-adic field, the solution being of the form

$$t_i = \left(-\frac{A_i}{k c_i \xi_i^{k-1}}\right) z^k + \lambda_{2k} z^{2k} + \lambda_{3k} z^{3k} + \ldots,$$

where the series is convergent in the p-adic sense (that is, the power of p dividing $\lambda_{mk} z^{mk}$ tends to infinity with m). Moreover, if the power of p dividing z is sufficiently large, we have

$$\xi_i + t_i \neq 0 \quad (1 \leqslant i \leqslant S). \tag{42}$$

We now have a p-adic solution of all R equations, namely

$$\xi_1 + t_1, \ldots, \xi_S + t_S, \xi_{S+1}, \ldots, \xi_\nu, z\eta_{\nu+1}, \ldots, z\eta_N.$$

This solution satisfies (42). It also has $z\eta_j \neq 0$ for some $j > \nu$, and for this j we have $a_{ij} \neq 0$ for some $i > S$. The rank of the Jacobian at this solution is at least $S+1$, and this contradicts the maximal choice of S. Thus the theorem is proved.

6. Preliminaries to the analytical investigation

In the rest of the paper we shall be concerned with the solubility, in rational integers not all zero, of R additive equations in N unknowns, which we again write as

$$\left.\begin{aligned} f_1 &= a_{11} x_1^k + \ldots + a_{1N} x_N^k = 0, \\ &\cdots \quad \cdots \quad \cdots \\ f_R &= a_{R1} x_1^k + \ldots + a_{RN} x_N^k = 0. \end{aligned}\right\} \tag{43}$$

We may assume that the forms $f_1, \ldots, f_R$ are linearly independent, since if they are not it suffices to solve $R-1$ equations. In particular, the rank of the matrix (a_{ij}) is R. We may also assume that no column consists entirely of zeros, since then there is an obvious solution.

The natural approach to the problem, by means of the Hardy–Littlewood method, would be to attempt to prove an asymptotic formula for the number of integral solutions of (43) when the unknowns are confined to ranges of the type

$$c_j P < x_j < d_j P \quad (j = 1, \ldots, N), \tag{44}$$

and $P \to \infty$. Here c_j, d_j are fixed numbers which must be chosen in relation to a real non-singular solution of the equations (43). The existence of such a real solution is almost immediate if k is odd, and is postulated if k is even.

The number of solutions of (43), subject to (44), is given by an R-fold integral:

$$\int_{\mathscr{U}} \sum_{x_1, \ldots, x_N} e(\alpha_1(a_{11} x_1^k + \ldots) + \ldots + \alpha_R(a_{R1} x_1^k + \ldots))\, \mathrm{d}\boldsymbol{\alpha}$$

where $\mathscr{U}$ denotes the unit cube

$$0 < \alpha_1 < 1, \ldots, 0 < \alpha_R < 1, \tag{45}$$

and $e(\theta) = \mathrm{e}^{2\pi i\theta}$. The integrand factorizes into a product of sums in one variable, and the integral becomes

$$\int_{\mathscr{U}} T_1(\Lambda_1) \ldots T_N(\Lambda_N)\, \mathrm{d}\boldsymbol{\alpha}, \tag{46}$$

where $\Lambda_1, \ldots, \Lambda_N$ are the linear forms

$$\Lambda_j = \sum_{i=1}^{R} a_{ij} \alpha_i \quad (1 \leqslant j \leqslant N), \tag{47}$$

and
$$T_j(\Lambda) = \sum_{c_j P < x < d_j P} e(\Lambda x^k).$$

If we divide the integration over $\mathscr{U}$ into two parts, that over 'major arcs' and that over 'minor arcs', on the lines of Birch (1962), for instance, it is the latter that present the main difficulty. For each $\boldsymbol{\alpha}$ on the minor arcs one can apply Weyl's inequality (if k is small) or Vinogradov's inequality (if k is large) to some of the exponential sums $T_j(\Lambda_j)$. We need to know that the inequality is applicable for many values of j, and this raises problems concerning the rank of various subsets of columns in the coefficient matrix (a_{ij}). It appears to us that these problems can only be resolved by an inductive argument relative to R if k is odd, and by an additional hypothesis if k is even.

We shall adopt a modification of the above approach, which is more effective in relation to the final number of variables required for success. This is based on the technique of diminishing ranges for some of the variables, a technique introduced with great effect in Waring's problem by Vinogradov. We employed such a technique in our paper of 1963 on the case $R = 1$, and in our paper of 1966 on the case $R = 2$, $k = 3$.

The allocation of the variables to different ranges will be made on the basis of (i) a dissection of part of the coefficient matrix into disjoint $R \times R$ non-singular matrices, and (ii) a particular real non-singular solution which has a special relation to these matrices. In the next section, on a hypothesis to be stated there (see lemma 12), we establish the possibility of the dissection, and then the existence of the special real non-singular solution. The hypothesis will ultimately be shown (in § 13) to be unnecessary when k is odd, as far as a proof of integral solubility is concerned. When k is even the hypothesis will be covered by that of theorem 2.

The dissection of part of the coefficient matrix, mentioned above, will result in a division of the variables into $2H+3k$ sets of R, where

$$H = [3k \log Rk], \tag{48}$$

together with a residue of $N-(2H+3k)R$ variables. Each set of R variables will correspond to the columns of one of the $R \times R$ non-singular matrices.

We shall denote the $2H$ sets by

$$\mathscr{B}_1, \ldots, \mathscr{B}_H, \mathscr{B}'_1, \ldots, \mathscr{B}'_H,$$

and the $3k$ sets by

$$\mathscr{C}_1, \ldots, \mathscr{C}_{3k},$$

and the residue by $\mathscr{D}$. The non-singular solution, say $\xi_1, \ldots, \xi_N$, will be such that $\xi_j > 0$ for all j in the sets

$$\mathscr{C}_1, \ldots, \mathscr{C}_{3k}, \mathscr{B}_1, \mathscr{B}'_1, \mathscr{D},$$

and $\xi_j = 0$ for all j in the sets $\mathscr{B}_2, \ldots, \mathscr{B}_H, \mathscr{B}'_2, \ldots, \mathscr{B}'_H$.

For the former variables, we choose ranges

$$\kappa_j P < x_j < \kappa'_j P, \tag{49}$$

where $0 < \kappa_j < \xi_j < \kappa'_j$ and $\kappa'_j - \kappa_j$ is sufficiently small.

Let $\theta = 1-1/k$. The variables in the sets $\mathscr{B}_\nu, \mathscr{B}'_\nu$, where $\nu = 2, \ldots, H$, will be given ranges of the form

$$\kappa_j P^{\theta^{\nu-1}} < x_j < \kappa'_j P^{\theta^{\nu-1}}, \tag{50}$$

where $0 < \kappa_j < \kappa'_j$ and κ'_j is sufficiently small.

For each of the variables x_j we introduce the exponential sum

$$T_j(\Lambda) = \sum_{x_j} e(\Lambda x_j^k), \tag{51}$$

where x_j runs through the appropriate range.

The number $\mathcal{N}(P)$ of integral solutions of the equations (43), subject to the specified ranges for the variables, is again given by the integral (46), where the linear forms Λ_j are given by (47). But now the exponential sums are those defined in (51), and the ranges for the variables in

$$\mathcal{B}_2, \ldots, \mathcal{B}_H, \mathcal{B}'_2, \ldots, \mathcal{B}'_H$$

are of lower order than P.

7. The allocation of variables

As was indicated in general terms in the last section, there are two important considerations in allocating the N variables $x_1, \ldots, x_N$ among the various sets which were described there. We first need to establish the existence of a sufficient number of disjoint $R \times R$ submatrices of rank R in the coefficient matrix (a_{ij}). We shall deal with this question first, and here there is no distinction as to whether k is even or odd. Secondly, we need to find a special real non-singular solution of the equations (43) which is related to the disjoint submatrices in the special way indicated at the end of the last section. This offers no difficulty if k is odd, but if k is even some reasoning is needed to derive the special real non-singular solution from the one which was postulated in theorem 2.

Lemma 12. *Suppose that any linear combination of the forms $f_1, \ldots, f_R$ in* (43) *contains more than*

$$(2H+3k-1)R \tag{52}$$

variables with coefficients not all zero. Then it is possible to select $2H+3k$ disjoint $R \times R$ submatrices, each of rank R, from the coefficient matrix (a_{ij}). Moreover, two of them can be taken to be any two specified disjoint submatrices of rank R.

Proof. We know that the whole matrix (a_{ij}) has rank R, so there is some $R \times R$ submatrix of rank R. We choose one, and this can be any specified one.

The rank of the remaining $N-R$ columns is still R. For if it were less than R we could form a linear combination of $f_1, \ldots, f_R$ which contained at most the R variables corresponding to the R columns already selected. This would imply that $R \geqslant (2H+3k-1)R$, which is false. Thus there is a second $R \times R$ submatrix of rank R, disjoint from the first, and it can be taken to be any specified one.

If we already have $m-1$ disjoint matrices of rank R, the same argument shows that the rank of the remaining $N-(m-1)R$ columns is still R, provided that

$$(m-1)R \leqslant (2H+3k-1)R.$$

This is true for $m \leqslant 2H+3k$, and gives a further submatrix, making m in all. Thus we get the desired $2H+3k$ disjoint submatrices.

From now on, until § 13, we assume the hypothesis of lemma 12 to hold.

We now turn to the choice of a special real non-singular solution. In considering real solutions, we can put $x_j^k = y_j$, where y_j must be positive or zero if k is even. The equations (43) become the linear equations

$$\left.\begin{array}{c} a_{11}y_1 + \ldots + a_{1N}y_N = 0, \\ \ldots \quad \ldots \quad \ldots \\ a_{R1}y_1 + \ldots + a_{RN}y_N = 0. \end{array}\right\} \tag{53}$$

Suppose first that k is odd. We take the $2H+3k$ sets of R columns, found in lemma 12, to be

$$\mathscr{C}_1, \ldots, \mathscr{C}_{3k}, \mathscr{B}_1, \ldots, \mathscr{B}_H, \mathscr{B}'_1, \ldots, \mathscr{B}'_H$$

in any order, with a residue of columns $\mathscr{D}$, as in § 6. Using only the columns in $\mathscr{C}_1$ and $\mathscr{C}_2$, we can solve the equations (53) with none of these unknowns zero. By making a small variation, we can obtain a real solution of the full equations (53) in which all the unknowns except those in

$$\mathscr{B}_2, \ldots, \mathscr{B}_H, \mathscr{B}'_2, \ldots, \mathscr{B}'_H$$

are not zero, and those in these sets are zero. By changing the signs of the coefficient a_{ij} in some of the columns (if necessary) we can suppose that the non-zero unknowns are positive. We have now obtained a real solution $\xi_1, \ldots, \xi_N$ of (43) with the properties asserted in § 6.

Suppose now that k is even. We are concerned in this case with solutions of (53) in which those of the y_j that are not zero must be positive.

Lemma 13. *Suppose that the linear equations* (53) *have a real solution with all $y_j \geq 0$ and with $y_j > 0$ for some R values of j for which the corresponding columns of coefficients have rank R. Then there exist R columns of rank R, and a further $S \leq R$ columns of rank S such that the equations* (53) *have a real solution with the unknowns corresponding to these columns positive and the other unknowns zero.*

Proof. We represent each column of (a_{ij}) by a point in R dimensional Euclidean space with the entries in the column as coordinates. Thus we have N points $A_1, \ldots, A_N$, not necessarily distinct, none of which is the origin O. The hypothesis asserts that

$$u_1 A_1 + \ldots + u_N A_N = O,$$

where each $u_j \geq 0$ and some R of the u_j are strictly positive, the corresponding columns being of rank R. By a slight variation of the u_i we can represent in the same way any point sufficiently near to O. Hence O is in the interior of the polyhedron Π which constitutes the convex closure of the points $A_1, \ldots, A_N$.

Consider an arbitrary line through O. This meets the boundary of Π at two points P, P' on opposite sides of O. We can choose the line so that P, which is necessarily on some $R-1$ dimensional face $\mathscr{F}$ of Π, is not on any $R-2$ dimensional linear space defined by $R-1$ of the points $A_1, \ldots, A_N$, and similarly for P'.

By a well-known result (see Bonnesen & Fenchel 1934, p. 9), the point P is in or on the boundary of an $R-1$ dimensional polyhedron whose vertices are R of the points A_i in $\mathscr{F}$. By construction, P cannot be on the boundary of this $R-1$ dimensional polyhedron, and therefore it is in its interior.

We now have
$$P = v_1 A_1 + \ldots + v_R A_R, \quad \Sigma v_i = 1,$$

where each $v_i > 0$ and $A_1, \ldots, A_R$ are the R points mentioned above. The columns represented by the points $A_1, \ldots, A_R$ are necessarily independent, since these points are the vertices of an $R-1$ dimensional polyhedron. Similarly, we have

$$P' = w_1 A'_1 + \ldots + w_R A'_R, \quad \Sigma w_i = 1,$$

where each $w_i > 0$ and the columns represented by $A'_1, \ldots, A'_R$ are independent. The points $A'_1, \ldots, A'_R$ may coincide in part with the points $A_1, \ldots, A_R$, and indeed it is plain that there may be only $R+1$ distinct points among $A_1, \ldots, A_R, A'_1, \ldots, A'_R$.

Since O is between P and P' on the line joining them, we have

$$O = u_1 A_1 + \ldots + u_{2R} A'_R,$$

where each $u_i > 0$. Let $A'_1, \ldots, A'_S$ be those points of $A'_1, \ldots, A'_R$ that are distinct from $A_1, \ldots, A_R$. Then

$$t_1 A_1 + \ldots + t_R A_R + t'_1 A'_1 + \ldots + t'_S A'_S = O, \tag{54}$$

where all the coefficients are positive.

We can now return to the original formulation. The columns corresponding to $A_1, \ldots, A_R$ are of rank R, and the further columns corresponding to $A'_1, \ldots, A'_S$ are of rank S, and (54) implies that the linear equations have a solution as asserted. This proves the lemma.

It is evident from earlier remarks that the postulate that the equations (43) have a real non-singular solution implies the hypothesis of lemma 13. This lemma then gives us R columns of rank R, and a further S columns of rank S, and a real solution of (53) in positive variables corresponding to these columns.

We now apply lemma 12. We take the first of the $R \times R$ matrices of that lemma to be that provided by the R columns just mentioned, and call this $\mathscr{C}_1$. We take the second of the $R \times R$ matrices of that lemma so that it includes the S columns just mentioned. This is possible since the rank of the $N-R$ available columns is R. We call this $\mathscr{C}_2$. We call the remaining $R \times R$ submatrices

$$\mathscr{C}_3, \ldots, \mathscr{C}_{3k}, \mathscr{B}_1, \ldots, \mathscr{B}_H, \mathscr{B}'_1, \ldots, \mathscr{B}'_H$$

in an arbitrary order, and as before there is a residue of columns $\mathscr{D}$.

Finally, we modify the real solution of (53) found in lemma 13. We assign to the variables in

$$\mathscr{C}_2, \mathscr{C}_3, \ldots, \mathscr{C}_{3k}, \mathscr{B}_1, \mathscr{B}'_1, \mathscr{D},$$

other than those variables in $\mathscr{C}_2$ which already have positive values, small positive values in place of their previous zero values. This leads to a new solution of (53) in which the variables corresponding to $\mathscr{C}_1$ receive values differing slightly from their previous values. It is clear that if the variations are sufficiently small, we obtain a solution in which all the variables corresponding to

$$\mathscr{C}_1, \ldots, \mathscr{C}_{3k}, \mathscr{B}_1, \mathscr{B}'_1, \mathscr{D}$$

are positive. Those corresponding to $\mathscr{B}_2, \ldots, \mathscr{B}'_H$ are zero, as before.

On taking the positive kth roots of the variables, we obtain a real solution $\xi_1, \ldots, \xi_N$ of (43) which has the properties asserted in § 6.

8. A system of auxiliary equations

It will be convenient to define

$$P_\nu = P^{\theta^{\nu-1}} \quad \text{for} \quad \nu = 1, \ldots, H, \quad \text{where} \quad \theta = 1 - 1/k. \tag{55}$$

Then the ranges for the variables x_j in $\mathscr{B}_\nu$ or $\mathscr{B}'_\nu$, given in (50), are of the form

$$\kappa_j P_\nu < x_j < \kappa'_j P_\nu, \quad \text{where} \quad 0 < \kappa_j < \kappa'_j. \tag{56}$$

We denote by $\mathscr{B}$ the union of all the values of j in

$$\mathscr{B}_1, \ldots, \mathscr{B}_H, \mathscr{B}'_1, \ldots, \mathscr{B}'_H.$$

The object of the present section is to prove:

LEMMA 14. *We have*

$$\int_{\mathscr{U}} \prod_{j \in \mathscr{B}} |T_j(\Lambda_j)| \, d\boldsymbol{\alpha} \ll (P_1 P_2 \ldots P_H)^R. \tag{57}$$

Proof. By Cauchy's inequality, it will suffice to prove that

$$\int_{\mathscr{U}} \prod_{j \in \mathscr{B}_1, \ldots, \mathscr{B}_H} |T_j(\Lambda_j)|^2 \, d\boldsymbol{\alpha} \ll (P_1 P_2 \ldots P_H)^R, \tag{58}$$

together with the corresponding result for $\mathscr{B}'_1, \ldots, \mathscr{B}'_H$, which however is equally covered by the proof of (58).

The integral on the left of (58) can be interpreted as the number of solutions of a certain system of R equations of additive type in $2RH$ variables, subject to appropriate ranges for these variables. We can write this system of equations, in an abbreviated notation, as

$$\mathscr{X}_1 + \ldots + \mathscr{X}_H = \mathscr{Y}_1 + \ldots + \mathscr{Y}_H, \tag{59}$$

where $\mathscr{X}_\nu$ stands for R expressions of the form

$$\begin{array}{c} b_{11} x_1^k + \ldots + b_{1R} x_R^k, \\ \ldots \quad \ldots \quad \ldots \\ b_{R1} x_1^k + \ldots + b_{RR} x_R^k, \end{array}$$

and $\mathscr{Y}_\nu$ for R expressions with the same coefficients but with variables $y_1, \ldots, y_R$. The columns of coefficients here are those in the set $\mathscr{B}_\nu$ of columns of coefficients in the original matrix (a_{ij}), and so have a non-zero determinant.

The variables x, y in $\mathscr{X}_\nu, \mathscr{Y}_\nu$ run through ranges of the form

$$c_\nu P_\nu < x < c'_\nu P_\nu, \quad c_\nu P_\nu < y < c'_\nu P_\nu. \tag{60}$$

Here we have tacitly taken the ranges to be the same for all the variables in the same $\mathscr{B}_\nu$, as is permissible in the choice made in § 6. We shall also suppose, as we may, that c'_2 is sufficiently small in relation to c_1, and so on.

It suffices to prove that the number of solutions of the system of equations (59), in integer variables restricted to the ranges (60), satisfies the estimate in (58).

Since the coefficients in the R columns represented by $\mathscr{X}_1$ are linearly independent, and are the same for $\mathscr{X}_1$ and $\mathscr{Y}_1$, we can combine the R equations linearly to get an equivalent system of the form

$$\left.\begin{array}{c} b_1 x_1^k \\ \ldots \\ b_R x_R^k \end{array}\right\} + \mathscr{X}_2 + \ldots + \mathscr{X}_H = \left.\begin{array}{c} b_1 y_1^k \\ \ldots \\ b_R y_R^k \end{array}\right\} + \mathscr{Y}_2 + \ldots + \mathscr{Y}_H,$$

where each $b_i \neq 0$ and where $\mathscr{X}_2, \ldots, \mathscr{Y}_2, \ldots$ are expressions like those above but with altered coefficients. The coefficients in each $\mathscr{X}_\nu$ or $\mathscr{Y}_\nu$ are the same and have non-zero determinant.

The variables in all of $\mathscr{X}_2, \ldots, \mathscr{Y}_H$ are in the ranges (60), and since $c'_2, \ldots, c'_H$ are small in relation to c_1, the sum of all the terms in any row of $\mathscr{X}_2 + \ldots + \mathscr{X}_H$ or $\mathscr{Y}_2 + \ldots + \mathscr{Y}_H$ will have absolute value less than

$$c_1^{k-1} P_2^k = c_1^{k-1} P_1^{k-1}.$$

On the other hand, we have

$$\begin{aligned}|b_1 x_1^k - b_1 y_1^k| &\geqslant |x_1^k - y_1^k| \\ &\geqslant k|x_1 - y_1| \{\min(x_1, y_1)\}^{k-1} \\ &\geqslant 2|x_1 - y_1| (c_1 P_1)^{k-1}.\end{aligned}$$

It follows that $|x_1 - y_1| < 1$, whence $x_1 = y_1$. Similarly, $x_i = y_i$ for $i = 1, \ldots, R$.

The equations (59) reduce to

$$\mathscr{X}_2 + \ldots + \mathscr{X}_H = \mathscr{Y}_2 + \ldots + \mathscr{Y}_H,$$

and we can repeat the argument. We find that each variable on the left is equal to the corresponding variable on the right.

The number of choices for all the variables in $\mathscr{X}_1, \ldots, \mathscr{X}_H$ is

$$\ll P_1^R P_2^R \ldots P_H^R,$$

and this proves the result.

9. Inequalities for $T(\Lambda)$

In this section we prove some upper bounds for the sum

$$T(\Lambda) = \sum_{\kappa P < x < \kappa' P} e(\Lambda x^k) \tag{61}$$

and for a product of such sums. The sums $T_j(\Lambda)$ in (51) are of this form when j belongs to any of the sets

$$\mathscr{B}_1, \mathscr{B}_1', \mathscr{C}_1, \ldots, \mathscr{C}_{3k}, \mathscr{D},$$

but we shall only use the results of this section for j in $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$. The principal application will be made in the next section.

We begin by quoting Weyl's inequality and Vinogradov's inequality in the forms most useful to us. We denote by δ a sufficiently small positive constant.

Lemma 15. *Suppose that*

$$|q\Lambda - a| < P^{-k+1-\delta} \quad \text{and} \quad P^{1-\delta} < q \leqslant P^{k-1+\delta}, \tag{62}$$

where q and a are relatively prime integers. Then

$$|T(\Lambda)| \ll P^{1-\kappa+\delta}, \tag{63}$$

where $\kappa = (\frac{1}{2})^{k-1}$.

Proof. This follows immediately from lemma 1 of Davenport (1962).

Lemma 16. *Suppose that $k \geqslant 12$. With the hypotheses of lemma 15, we have*

$$|T(\Lambda)| \ll P^{1-\rho+\delta'}, \tag{64}$$

where

$$\rho = \frac{1}{2k^2(2\log k + \log\log k + 3)} \tag{65}$$

and where δ' is small with δ.

Proof. See lemma 9 of Davenport & Lewis (1963).

We combine these inequalities in:

Lemma 17. *With the hypotheses of lemma 15 we have*

$$|T(\Lambda)| \ll P^{1-\sigma}, \tag{66}$$

where
$$\sigma = \frac{1}{8k^2 \log k}. \tag{67}$$

Proof. If $k \geqslant 12$,

$$2k^2(2\log k + \log\log k + 3) < 2k^2(2\log k + \tfrac{1}{2}\log k + \tfrac{3}{2}\log k) = 8k^2 \log k.$$

If $k \leqslant 11$ then $2^{k-1} < 8k^2 \log k$. This proves the result, since we can obviously omit δ' and δ.

We also need an estimate for $|T(\Lambda)|$ when the first inequality in (62) holds, but $q \leqslant P^{1-\delta}$.

Lemma 18. *Suppose that*

$$|q\Lambda - a| < P^{-k+1-\delta} \quad \textit{and} \quad 1 \leqslant q \leqslant P^{1-\delta}. \tag{68}$$

Let
$$\Lambda = a/q + \gamma. \tag{69}$$

Then
$$|T(\Lambda)| \ll q^{-1/k} \min(P, P^{1-k}|\gamma|^{-1}). \tag{70}$$

Proof. For $k = 3$ the result follows from lemma 9 of Davenport (1939*a*), and for $k \geqslant 4$ from lemma 9 of Davenport (1939*b*).

We now use lemmas 17 and 18 to get an estimate for a product of R sums $T_j(\Lambda_j)$, where the Λ_j are linear forms in R real variables $\alpha_1, \ldots, \alpha_R$.

Lemma 19. *Let $\Lambda_1, \ldots, \Lambda_R$ be independent linear forms in $\alpha_1, \ldots, \alpha_R$ with integral coefficients. Let the $T_j(\Lambda_j)$ be sums of the form (61), where κ, κ' may depend on j. Then either*

$$\prod_{j=1}^{R} |T_j(\Lambda_j)| \ll P^{R-\sigma} \tag{71}$$

or $\alpha_1, \ldots, \alpha_R$ have simultaneous rational approximations $A_1/Q, \ldots, A_R/Q$ satisfying

$$\alpha_i = \frac{A_i}{Q} + \beta_i, \quad (Q, A_1, \ldots, A_R) = 1, \tag{72}$$

$$1 \leqslant Q \leqslant P^{k\sigma}, \quad Q|\beta_i| < P^{-k+k\sigma}. \tag{73}$$

Proof. If, for any j, Λ_j satisfies the hypotheses of lemma 15, the result follows from lemma 17, since for every other j there is the obvious estimate $|T_j(\Lambda_j)| \ll P$. Hence we can suppose that for no j do there exist integers a_j, q_j such that

$$|q_j \Lambda_j - a_j| < P^{-k+1-\delta}, \quad P^{1-\delta} < q_j \leqslant P^{k-1+\delta}$$

and $(a_j, q_j) = 1$.

On the other hand there always exist integers a_j, q_j satisfying

$$|q_j \Lambda_j - a_j| < P^{-k+1-\delta}, \quad 1 \leqslant q_j \leqslant P^{k-1+\delta}.$$

Hence, for each j, we must have $\quad 1 \leqslant q_j \leqslant P^{1-\delta}$.

Thus lemma 18 is applicable for each j, and gives

$$|T_j(\Lambda_j)| \ll q_j^{-1/k} \min(P, P^{1-k}|\gamma_j|^{-1}),$$

where $\Lambda_j = \gamma_j + a_j/q_j$. Denote the expression on the right-hand side above by $CP^{1-\phi_j}$, where C is a (large) constant to be determined. If

$$\phi_1 + \ldots + \phi_R \geqslant \sigma$$

we get the estimate (71). Hence we may suppose (for large P) that

$$\phi_1 + \ldots + \phi_R < \sigma. \tag{74}$$

It follows from the definition of ϕ_j that

$$q_j \leqslant C^{-k} P^{k\phi_j}, \tag{75}$$

and

$$|\gamma_j| \leqslant C^{-1} q_j^{-1/k} P^{-k+\phi_j}. \tag{76}$$

We have

$$\Lambda_j = \sum_{i=1}^{R} c_{ij} \alpha_i \quad (j = 1, \ldots, R),$$

where the c_{ij} are integers with $\det c_{ij} = \Delta \neq 0$. Hence

$$\Delta \alpha_i = \sum_{j=0}^{R} d_{ij} \Lambda_j \quad (i = 1, \ldots, R),$$

where the d_{ij} are fixed integers (cofactors of the c_{ij}). It follows that

$$\Delta \alpha_i = \sum_{j=1}^{R} d_{ij} \left(\frac{a_j}{q_j} + \gamma_j\right) \quad (i = 1, \ldots, R).$$

Hence

$$\alpha_i = A_i/Q + \beta_i,$$

where Q and the A_i are integers with $(Q, A_1, \ldots, A_R) = 1$, and

$$\beta_i = \Delta^{-1} \sum_{j=1}^{R} d_{ij} \gamma_j.$$

Plainly Q divides $\Delta q_1 \ldots q_R$, and therefore by (75) and (74)

$$Q \leqslant |\Delta| \, C^{-kR} P^{k(\phi_1 + \ldots + \phi_R)} < P^{k\sigma}, \tag{77}$$

if C is suitably chosen. Also by (76)

$$\begin{aligned} Q|\beta_i| &\leqslant q_1 \ldots q_R \sum_{j=1}^{R} |d_{ij}| \, |\gamma_j| \\ &\leqslant DC^{-1} P^{-k} \sum_{j=1}^{R} q_1 \ldots q_R q_j^{-1/k} P^{\phi_j}, \end{aligned}$$

where $D = \max |d_{ij}|$. Hence, by (75),

$$\begin{aligned} Q\,|\beta_i| &\leqslant DC^{-1} P^{-k} R C^{1-Rk} P^{k\phi_1 + \ldots + k\phi_R} \\ &< P^{-k+k\sigma}, \end{aligned}$$

on using (74) and taking C sufficiently large. This, together with (77), gives (73).

10. The contribution of the minor arcs

We divide the unit cube of integration $\mathscr{U}$ in (46) into parts called *major arcs* and *minor arcs*. For any integers $Q, A_1, \ldots, A_R$ satisfying

$$1 \leqslant Q < P^{k\sigma} \quad 0 \leqslant A_i < Q \quad (Q, A_1, \ldots, A_R) = 1, \tag{78}$$

we define the major arc $\mathfrak{M}_{Q,\mathbf{A}}$ to consist of all $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_R)$ given by

$$\alpha_i = A_i/Q + \beta_i, \quad |\beta_i| < Q^{-1} P^{-k+k\sigma}, \tag{79}$$

σ being defined in (67). There is the usual convention that any parts outside $\mathscr{U}$ are deemed to be translated modulo 1 to come in $\mathscr{U}$. Two major arcs do not overlap unless they are identical, since an overlap would imply that

$$\left|\frac{A_i}{Q}-\frac{A_i'}{Q'}\right| < P^{-k+k\sigma}\left(\frac{1}{Q}+\frac{1}{Q'}\right) < \frac{1}{QQ'}.$$

Let $\mathfrak{M}$ denote the union of all $\mathfrak{M}_{Q,\mathbf{A}}$, and let $\mathfrak{m}$ denote the rest of $\mathscr{U}$, called the minor arcs.

As shown in § 6, the number $\mathscr{N}(P)$ is given by the integral in (46). Thus

$$\mathscr{N}(P) = \sum_{Q,\mathbf{A}} \int_{\mathfrak{M}_{Q,\mathbf{A}}} \prod_{j=1}^{N} T_j(\Lambda_j)\, d\boldsymbol{\alpha} + \int_{\mathfrak{m}} \prod_{j=1}^{N} T_j(\Lambda_j)\, d\boldsymbol{\alpha}. \tag{80}$$

We now estimate the last integral on the right.

Lemma 20. *We have*

$$\int_{\mathfrak{m}} \prod_{j=1}^{N} |T_j(\Lambda_j)|\, d\boldsymbol{\alpha} = o(P^{\Omega}),$$

where $$\Omega = N-2HR+kR-2kR\theta^H, \tag{81}$$

provided H satisfies $$R\theta^H < 3\sigma. \tag{82}$$

Proof. The N values of j were divided in §§ 6 and 7 into the sets

$$\mathscr{B}_1, \ldots, \mathscr{B}_H, \mathscr{B}_1', \ldots, \mathscr{B}_H', \mathscr{C}_1, \ldots, \mathscr{C}_{3k}, \mathscr{D}.$$

For the j in $\mathscr{D}$ we use merely the trivial estimate P, which gives

$$\prod_{j\in\mathscr{D}} |T_j(\Lambda_j)| \ll P^{N-(2H+3k)R}. \tag{83}$$

For the j in any one of the sets $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$ we can appeal to lemma 19, since for the R values of j in any one set, the Λ_j are independent linear forms in $\alpha_1, \ldots, \alpha_R$. The second alternative conclusion of lemma 19 would imply that $\boldsymbol{\alpha}$ was in $\mathfrak{M}_{Q,\mathbf{A}}$, and this is excluded if $\boldsymbol{\alpha}$ is in $\mathfrak{m}$. Hence, for $\boldsymbol{\alpha}$ in $\mathfrak{m}$, we have (71), and on multiplying together $3k$ such inequalities we get

$$\prod_{j\in\mathscr{C}} |T_j(\Lambda_j)| \ll P^{3kR-3k\sigma}, \tag{84}$$

where $\mathscr{C}$ denotes the union of $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$.

There remain the values of j in the set $\mathscr{B}$. Here lemma 14 tells us that

$$\int_{\mathscr{U}} \prod_{j\in\mathscr{B}} |T_j(\Lambda_j)|\, d\boldsymbol{\alpha} \ll (P_1 P_2 \ldots P_H)^R.$$

By (55), the number on the right is P^{λ}, where

$$\lambda = R(1+\theta+\theta^2+\ldots+\theta^{H-1})$$
$$= Rk(1-\theta^H).$$

Combining this result with (83) and (84), we see that the integral under consideration is

$$\ll P^{N-2HR+kR-kR\theta^H-3k\sigma}.$$

This gives the result provided that (82) holds, since the numbers in (82) are independent of P as $P\to\infty$.

LEMMA 21. *The condition* (82) *of lemma* 20 *is satisfied if* H *is defined by* (48).

Proof. We have
$$\theta^H = (1-1/k)^H < e^{-H/k}.$$

It suffices for (82) if
$$e^{H/k} > \frac{R}{3\sigma} = \tfrac{8}{3}Rk^2 \log k.$$

It is easily verified that for $R \geqslant 2$ and $k \geqslant 3$ we have
$$\log\{\tfrac{8}{3}Rk^2\log k\} < k^{-1}[3k\log Rk],$$
so the condition is satisfied if $H = [3k\log Rk]$.

11. Pruning the major arcs

We turn to the contribution of the major arcs $\mathfrak{M}_{Q,\mathbf{A}}$ to the right-hand side of (80). The summation over Q and $\mathbf{A}$ is subject to
$$1 \leqslant Q < P^{k\sigma}, \quad 0 \leqslant A_i < Q, \quad (Q, A_1, \ldots, A_R) = 1, \tag{85}$$
and each $\mathfrak{M}_{Q,\mathbf{A}}$ is given by $\alpha_i = A_i/Q + \beta_i, \quad |\beta_i| < Q^{-1}P^{-k+k\sigma}.$ (86)

In the present section we shall first reduce the range for Q to $1 \leqslant Q \leqslant P^{\omega}$, where ω is arbitrarily small but fixed, and then contract $\mathfrak{M}_{Q,\mathbf{A}}$ to $|\beta_i| < P^{-k+\tau}$, where τ is also arbitrarily small but fixed.

The approximations A_i/Q to $\alpha_1, \ldots, \alpha_R$ imply approximations to the linear forms Λ_j. We have
$$\Lambda_j = \sum_{i=1}^{R} a_{ij}\alpha_i = \sum_{i=1}^{R} a_{ij}\left(\frac{A_i}{Q}+\beta_i\right).$$

We put
$$\frac{a_j}{q_j} = \frac{1}{Q}\sum_{i=1}^{R} a_{ij}A_i, \quad \text{where} \quad (a_j, q_j) = 1, \tag{87}$$
and
$$\gamma_j = \sum_{i=1}^{R} a_{ij}\beta_i, \tag{88}$$
and have
$$\Lambda_j = \frac{a_j}{q_j} + \gamma_j \quad (j = 1, \ldots, N). \tag{89}$$

LEMMA 22. *If* $\mathscr{W}$ *denotes the whole of* R *dimensional space then*
$$\int_{\mathscr{W}} \prod_{j\in\mathscr{C}} \min(P, P^{1-k}|\gamma_j|^{-1})\, d\boldsymbol{\beta} \ll P^{2kR}, \tag{90}$$
and if $\mathscr{T}$ *denotes the region* $\max|\beta_i| > P^{-k+\tau}$ *then*
$$\int_{\mathscr{T}} \prod_{j\in\mathscr{C}} \min(P, P^{1-k}|\gamma_j|^{-1})\, d\boldsymbol{\beta} \ll P^{2kR-(3k-1)\tau R}. \tag{91}$$

Proof. The set $\mathscr{C}$ is the union of the disjoint sets $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$. By Hölder's inequality, it suffices to prove that
$$\int_{\mathscr{W}} \prod_{j=1}^{R} \{\min(P, P^{1-k}|\gamma_j|^{-1})\}^{3k}\, d\boldsymbol{\beta} \ll P^{2kR},$$
and an analogous result for the integral over $\mathscr{T}$, where $\gamma_1, \ldots, \gamma_R$ typify a set of R independent linear forms (88) in $\beta_1, \ldots, \beta_R$, corresponding to any one of the sets $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$.

We can take $\gamma_1, \ldots, \gamma_R$ instead of $\beta_1, \ldots, \beta_R$ as the variables of integration. The integral over $\mathscr{W}$ factorizes, and it suffices to prove that

$$\int_{-\infty}^{\infty} \{\min(P, P^{1-k}|\gamma|^{-1})\}^{3k} \, d\gamma \ll P^{2k},$$

which is immediately verified. As regards the integral over $\mathscr{T}$, the region $\mathscr{T}$ corresponds to a region in $\boldsymbol{\gamma}$ space contained in

$$\max|\gamma_i| > CP^{-k+\tau},$$

for some positive constant C. The integral extended over the latter region again factorizes, and it suffices to prove that

$$\int_{CP^{-k+\tau}}^{\infty} \{\min(P, P^{1-k}\gamma^{-1})\}^{3k} \, d\gamma \ll P^{2k-(3k-1)\tau}.$$

This again is easily verified.

Lemma 23. *For any Q, we have*

$$\sum_{\mathbf{A}} \prod_{j \in \mathscr{C}} q_j^{-1/k} \ll Q^{-\frac{3}{2}}, \tag{92}$$

where the summation is subject to (85) *and the q_j are defined by* (87).

Proof. By Hölder's inequality it suffices to prove that

$$\sum_{\mathbf{A}} (q_1 q_2 \ldots q_R)^{-3} \ll Q^{-\frac{3}{2}}, \tag{93}$$

where $q_1, \ldots, q_R$ typify those q_j which correspond to any one of the sets $\mathscr{C}_1, \ldots, \mathscr{C}_{3k}$ of values of j. Thus we can take $q_1, \ldots, q_R$ to be determined as functions of $Q, A_1, \ldots, A_R$ by (87), where the a_{ij} are fixed integers with $\det a_{ij} \neq 0$. We have

$$q_j = Q/u_j,$$

where

$$u_j = \left(Q, \sum_{i=1}^{R} a_{ij} A_i\right). \tag{94}$$

Thus

$$\sum_{i=1}^{R} a_{ij} A_i \equiv 0 \pmod{u_j} \quad (j = 1, \ldots, R).$$

Let $d = (u_1, \ldots, u_R)$. Then the last congruences show that d divides $\det a_{ij}$, since

$$(A_1, \ldots, A_R, d) = 1;$$

and therefore d is bounded.

The sum on the left of (93) is

$$\sum_{\mathbf{A}} Q^{-3R}(u_1 u_2 \ldots u_R)^3. \tag{95}$$

Let

$$B_j = \sum_{i=1}^{R} a_{ij} A_i \quad (j = 1, \ldots, R). \tag{96}$$

Then $|B_j| \ll Q$, since $0 \leqslant A_i \leqslant Q$. We have $u_j = (Q, B_j)$ by (94). Thus B_j is a multiple of u_j and is $\ll Q$.

For given values of $u_1, \ldots, u_R$, all divisors of Q, the number of possibilities for $B_1, \ldots, B_R$ is

$$\ll \frac{Q}{u_1} \frac{Q}{u_2} \cdots \frac{Q}{u_R}.$$

Also there is at most one set $A_1, \ldots, A_R$ for given $B_1, \ldots, B_R$, by (96). Hence the sum in (95) is

$$\begin{aligned} &\ll \sum_{\substack{u_1|Q \\ (u_1, \ldots, u_R) \ll 1}} \cdots \sum_{u_R|Q} Q^{-3R}(u_1 \ldots u_R)^3 \, Q^R (u_1 \ldots u_R)^{-1} \\ &= \sum_{\substack{u_1|Q \\ (u_1, \ldots, u_R) \ll 1}} \cdots \sum_{u_R|Q} Q^{-2R}(u_1 \ldots u_R)^2 \\ &= Q^{-2R} S_R(Q), \end{aligned}$$

say.

We put $u_1 = dv_1, \ldots, u_R = dv_R$, where $(v_1, \ldots, v_R) = 1$. Then

$$S_R(Q) = \sum_{\substack{d|Q \\ d \ll 1}} \sum_{\substack{v_1|Q/d, \ldots, v_R|Q/d \\ (v_1, \ldots, v_R) = 1}} (d^R v_1 \ldots v_R)^2.$$

The conditions of summation imply that

$$v_1 v_2 \ldots v_R \,|\, (Q/d)^{R-1},$$

for if p^α is a prime power component of Q/d, then at most $R-1$ of $v_1, \ldots, v_R$ can be divisible by p. We put $v_1 v_2 \ldots v_R = w$, and recall that the number of times any particular w can occur is $\ll w^\epsilon$, for any fixed $\epsilon > 0$. Hence

$$\begin{aligned} S_R(Q) &\ll \sum_{\substack{d|Q \\ d \ll 1}} d^{2R} \sum_{w|(Q/d)^{R-1}} w^{2+\epsilon} \\ &\ll \sum_{\substack{d|Q \\ d \ll 1}} d^{2R} (Q/d)^{(2+\epsilon)(R-1)} \\ &\ll Q^{(2+\epsilon)(R-1)}. \end{aligned}$$

It follows that the sum in (95) is

$$\ll Q^{-2R+(2+\epsilon)(R-1)} \ll Q^{-\frac{3}{2}}.$$

This proves the lemma.

LEMMA 24. *The contribution made to the right-hand side of* (80) *by the* $\mathfrak{M}_{Q,\mathbf{A}}$ *with* $Q > P^\omega$ *is*

$$\ll P^{\Omega - \frac{1}{2}\omega}, \tag{97}$$

where Ω *is defined in* (81).

Proof. We estimate the product of the $|T_j(\Lambda_j)|$ trivially except when $j \in \mathscr{C}$. This gives

$$\prod_{j=1}^{N} |T_j(\Lambda_j)| \ll P^{N-2HR-kR-2kR\theta^H} \prod_{j \in \mathscr{C}} |T_j(\Lambda_j)|.$$

Since q_j is a divisor of Q by (87), we have

$$q_j \leqslant Q < P^{k\sigma} < P^{1-\delta}.$$

Also, by (88) and (86) $$|\gamma_j| \ll \sum_{i=1}^{R} |\beta_i| \ll Q^{-1} P^{-k+k\sigma}.$$

The hypotheses of lemma 18 are satisfied, and therefore

$$|T_j(\Lambda_j)| \ll q_j^{-1/k} \min(P, P^{1-k} |\gamma_j|^{-1}).$$

Hence $$\prod_{j \in \mathscr{C}} |T_j(\Lambda_j)| \ll \{\prod_{j \in \mathscr{C}} q_j^{-1/k}\} \{\prod_{j \in \mathscr{C}} \min(P, P^{1-k}|\gamma_j|^{-1})\}. \tag{98}$$

To estimate the contribution made by all $\mathfrak{M}_{Q,\mathbf{A}}$ with $Q > P^{\omega}$ we have first to integrate this over $\mathfrak{M}_{Q,\mathbf{A}}$. Instead we integrate over the whole of space and use (90). We have then to sum over $\mathbf{A}$ and over $Q > P^{\omega}$, and here we use (92). The resulting estimate for the contribution under consideration is

$$P^{N-2HR-kR-2kR\theta^H} \,.\, P^{2kR} \,.\, P^{-\frac{1}{2}\omega},$$

which is as stated.

We denote by $\mathfrak{M}'_{Q,\mathbf{A}}$ the contracted major arc obtained by replacing the second inequality in (86) by

$$|\beta_i| < P^{-k+\tau} \quad (i = 1, \dots, R). \tag{99}$$

The number on the right is less than that in (86) since now $Q \leqslant P^{\omega}$ and ω, τ are small.

LEMMA 25. *The difference between the contributions made by the* $\mathfrak{M}_{Q,\mathbf{A}}$ *and the* $\mathfrak{M}'_{Q,\mathbf{A}}$, *with* $Q \leqslant P^{\omega}$ *in both cases, is*

$$\ll P^{\Omega-\tau}. \tag{100}$$

Proof. It suffices to estimate

$$\sum_{Q \leqslant P^{\omega}} \sum_{\mathbf{A}} \int \prod_{j=1}^{N} |T_j(\Lambda_j)| \, d\boldsymbol{\alpha},$$

where the integration is over $\mathfrak{M}_{Q,\mathbf{A}} - \mathfrak{M}'_{Q,\mathbf{A}}$ that is, over

$$P^{-k+\tau} < \max |\beta_i| < Q^{-1}P^{-k+k\sigma}.$$

Again we take the trivial upper bound for all $T_j(\Lambda_j)$ except for j in $\mathscr{C}$, and for the product over j in $\mathscr{C}$ we have the estimate (98). We integrate the right-hand side of (98) over the region $\mathscr{T}$ of lemma 22 and use (91). We have then to sum over $\mathbf{A}$ and Q (where we can allow Q to go from 1 to ∞), and here we use lemma 23. The resulting estimate is

$$P^{N-2HR-kR-2kR\theta^H} P^{2kR-(3k-1)\tau R},$$

and this implies the result stated.

We have now reached the following situation:

$$\mathscr{N}(P) = \sum_{Q \leqslant P^{\omega}} \sum_{\mathbf{A}} \int_{\mathfrak{M}'_{Q,\mathbf{A}}} \prod_{j=1}^{N} T_j(\Lambda_j) \, d\boldsymbol{\alpha} + o(P^{\Omega}). \tag{101}$$

This follows from (80) and lemmas 20, 24, 25.

12. The asymptotic formula

We now proceed to evaluate (asymptotically, as $P \to \infty$) the sum of integrals on the right of (101).

Each exponential sum $T_j(\Lambda_j)$ is of the form

$$T(\Lambda) = \sum_{\kappa X < x < \kappa' X} e(\Lambda x^k). \tag{102}$$

If j is in any of the sets

$$\mathscr{C}_1, \dots, \mathscr{C}_{3k}, \mathscr{B}_1, \mathscr{B}'_1, \mathscr{D} \tag{103}$$

the appropriate value of X is P; if j is in $\mathscr{B}_\nu$ or $\mathscr{B}'_\nu$ (where $\nu = 2, \dots, H$) the appropriate value of X is P_ν. We denote by $\mathscr{E}$ the union of the (disjoint) sets (103).

We give first an approximation for sums of the general type (102).

Lemma 26. *Suppose that*

$$\Lambda = (a/q) + \gamma \tag{104}$$

where $$(a, q) = 1, \quad q \leqslant X^{\delta}, \quad |\gamma| < q^{-1}X^{-k+\delta}, \tag{105}$$

δ being a small positive constant. Then

$$T(\Lambda) = q^{-1}S(a, q)\, I(\gamma) + O(X^{2\delta}), \tag{106}$$

where $$S(a, q) = \sum_{x=1}^{q} e_q\,(ax^k), \tag{107}$$

and $$I(\gamma) = \int_{\kappa X}^{\kappa' X} e(\gamma x^k)\,\mathrm{d}x. \tag{108}$$

Proof. See lemma 4, Davenport (1962). Note that the conditions imposed there on α, a, q are the same as in (104) and (105). The proof is simple and elementary.

Lemma 27. *Suppose* $\boldsymbol{\alpha}$ *is in* $\mathfrak{M}'_{Q,\mathbf{A}}$. *If j is in the set $\mathscr{E}$ we have*

$$T_j(\Lambda_j) = q_j^{-1}S(a_j, q_j)\, I_j(\gamma_j) + O(P^{2\delta}), \tag{109}$$

where $S(a_j, q_j)$ is as defined in (107) and

$$I_j(\gamma_j) = \int_{\kappa_j P}^{\kappa'_j P} e(\gamma_j x^k)\,\mathrm{d}x, \tag{110}$$

and where δ is small if ω and τ are small. If j is in $\mathscr{B}_\nu$ or $\mathscr{B}'_\nu$, where $\nu = 2, \ldots, H$, we have

$$T_j(\Lambda_j) = (\kappa'_j - \kappa_j)\, P_\nu q_j^{-1} S(a_j, q_j) + O(P_\nu^{2\delta}). \tag{111}$$

Proof. For $\boldsymbol{\alpha}$ in $\mathfrak{M}'_{Q,\mathbf{A}}$ we have

$$\alpha_i = A_i/Q + \beta_i, \tag{112}$$

$$1 \leqslant Q \leqslant P^{\omega}, \quad |\beta_i| < P^{-k+\tau}. \tag{113}$$

Hence, for each j, by (87), $$q_j \leqslant Q \leqslant P^{\omega}, \tag{114}$$

and by (88) $$|\gamma_j| \ll P^{-k+\tau}. \tag{115}$$

Suppose first that j is in $\mathscr{E}$. Then (114) and (115) imply that the conditions (105) with X replaced by P are satisfied, provided we choose δ to be greater than $\tau + \omega$. Thus (109) follows from (106).

Suppose next that j is in $\mathscr{B}_\nu$ or $\mathscr{B}'_\nu$, where $2 \leqslant \nu \leqslant H$. We have to apply lemma 26 with X replaced by P_ν. Since P_ν is greater than a fixed positive power of P, the conditions (105) with X replaced by P_ν are still satisfied, provided we choose δ to be greater than some constant multiple of $\tau + \omega$. Hence we have (106), where now $I(\gamma)$ is replaced by

$$\int_{\kappa_j P_\nu}^{\kappa'_j P_\nu} e(\gamma_j x^k)\,\mathrm{d}x.$$

Here, however, by (115)

$$|\gamma_j|\, x^k \ll P^{-k+\tau} P_\nu^k \ll P^{-k+\tau} P^{k-1} \ll P^{-1+\tau}.$$

Thus the above integral is $$(\kappa'_j - \kappa_j)\, P_\nu + O(P_\nu P^{-1+\tau}),$$

and the error term is $O(1)$ if $\tau < 1/k$. On substituting this in (106), and noting that $|q^{-1}S(a, q)| \leqslant 1$, we obtain (111).

LEMMA 28. *We have*

$$\sum_{Q\leqslant P^\omega}\sum_{\mathbf{A}}\int_{\mathfrak{M}'_{Q,\mathbf{A}}}\prod_{j=1}^{N}T_j(\Lambda_j)\,d\boldsymbol{\alpha}=\mathfrak{S}(P^\omega)\,\mathscr{I}(P^{-k+\tau})+o(P^\Omega),\tag{116}$$

where
$$\mathfrak{S}(P^\omega)=\sum_{Q\leqslant P^\omega}\sum_{\mathbf{A}}\prod_{j=1}^{N}q_j^{-1}S(a_j,q_j),\tag{117}$$

and
$$\mathscr{I}(P^{-k+\tau})=C(P_2\dots P_H)^{2R}\int\prod_{j\in\mathscr{E}}I_j(\gamma_j)\,d\boldsymbol{\beta},\tag{118}$$

and C is a positive constant, and the integration is over

$$|\beta_i|<P^{-k+\tau}\quad(i=1,\dots,R).\tag{119}$$

Proof. In order to approximate to $\prod_j T_j(\Lambda_j)$ we have to multiply together the approximations (109) for j in $\mathscr{E}$ and the approximations (111) for j in $\mathscr{B}_\nu$ and $\mathscr{B}'_\nu$, for $\nu=2,\dots,H$. We can estimate the error by multiplying together estimates for any set of main terms and for the complementary set of error terms. Any main term is obviously majorized by P or P_ν (as the case may be) and any error term by $P^{2\delta}$ or $P_\nu^{2\delta}$. The largest estimate arises when we take P or P_ν in all but one case, and the omitted case is P_H. Thus the error is

$$\ll P^{N-2(H-1)R}P_2^{2R}\dots P_H^{2R-1}P_H^{2\delta}$$
$$=P^{N-2HR}(P_1\dots P_H)^{2R}P_H^{-1+2\delta}.$$

This has to be integrated over (119) and summed over $\mathbf{A}$ and over $Q\leqslant P^\omega$. The result is

$$\ll P^{N-2HR+2kR(1-\theta^H)}P_H^{-1+2\delta}P^{R(-k+\tau)}\sum_{Q\leqslant P^\omega}Q^R,$$

and when this is expressed as a power of P the exponent is

$$N-2HR+kR-2kR\theta^H-(1-2\delta)\,\theta^{H-1}+R\tau+(R+1)\,\omega.$$

This is a permissible term in accordance with (116) provided τ and ω are sufficiently small.

The product of main terms is

$$C(P_2\dots P_H)^{2R}\prod_{j=1}^{N}\{q_j^{-1}S(a_j,q_j)\}\prod_{j\in\mathscr{E}}I_j(\gamma_j),$$

where
$$C=\prod_{j\notin\mathscr{E}}(\kappa'_j-\kappa_j).\tag{120}$$

This gives the first term on the right of (116).

LEMMA 29. *We have*

$$\mathfrak{S}(P^\omega)=\mathfrak{S}+o(1),\tag{121}$$

where
$$\mathfrak{S}=\sum_{Q=1}^{\infty}\sum_{\mathbf{A}}Q^{-N}S_0(\mathbf{A},Q),\tag{122}$$

and
$$S_0(\mathbf{A},Q)=\sum_{x_1=1}^{Q}\dots\sum_{x_N=1}^{Q}e_Q(A_1f_1+\dots+A_Rf_R).\tag{123}$$

Proof. It follows from Lemma 15 of Davenport (1962) and lemma 23 that

$$\mathfrak{S}(P^\omega)=\mathfrak{S}+O(P^{-\frac{1}{2}\omega}),$$

where $$\mathfrak{S} = \sum_{Q=1}^{\infty} \sum_{\mathbf{A}} \prod_{j=1}^{N} q_j^{-1} S(a_j, q_j).$$

We have, by (87),
$$S(a_j, q_j) = \sum_{x=1}^{q_j} e(a_j x^k / q_j)$$
$$= \sum_{x=1}^{q_j} e\left(\frac{1}{Q} \sum_{i=1}^{R} a_{ij} A_i x^k\right)$$
$$= \frac{q_j}{Q} \sum_{x=1}^{Q} e_Q\left(\sum_{i=1}^{R} a_{ij} A_i x^k\right),$$

since Q is a multiple of q_j. Hence
$$\prod_{j=1}^{N} q_j^{-1} S(a_j, q_j) = Q^{-N} \sum_{x_1=1}^{Q} \dots \sum_{x_N=1}^{Q} e_Q\left(\sum_{i=1}^{R} \sum_{j=1}^{N} a_{ij} A_i x_j^k\right).$$

Since $f_i = \sum_{j=1}^{N} a_{ij} x_j^k$, this gives $\mathfrak{S}$ as in (122).

Lemma 30. *We have*
$$\mathscr{I}(P^{-k+\tau}) = C_0 P^{\Omega}(1+o(1)) \tag{124}$$
as $P \to \infty$, where C_0 is positive and independent of P.

Proof. The R-fold integral in the expression (118) for $\mathscr{I}(P^{-k+\tau})$

is $$\int \prod_{j \in \mathscr{E}} I_j(\gamma_j)\, d\boldsymbol{\beta}, \tag{125}$$

extended over (119). The first step is to extend the integral to the whole of $\boldsymbol{\beta}$ space. In the integral over the remainder of space, that is, over
$$\max |\beta_i| > P^{-k+\tau},$$
we use (91) for j in $\mathscr{C}$ and the trivial estimate $O(P)$ for other j. Note that (91) is applicable because
$$|I_j(\gamma_j)| \ll \min(P, P^{1-k} |\gamma_j|^{-1}).$$
Thus the difference between the integral over (119) and that over the whole space is
$$\ll P^{2kR-(3k-1)\tau R} P^{N-3kR-2(H-1)R}.$$
When this is multiplied by $(P_2 \dots P_H)^{2R}$ it gives an error which is permissible in (124).

Thus we can replace (125) by
$$\lim_{\phi \to \infty} \int_{-\phi}^{\phi} \dots \int_{-\phi}^{\phi} \prod_{j \in \mathscr{E}} I_j(\gamma_j)\, d\beta_1 \dots d\beta_R. \tag{126}$$
We put $\beta_i = P^{-k}\zeta_i$ $(i = 1, \dots, R)$, and in the definition of $I_j(\gamma_j)$ in (110) we put $x = Py^{1/k}$. Thus
$$I_j(\gamma_j) = P \int_{\kappa_j}^{\kappa_j'} k^{-1} y^{-1+1/k} e(\gamma_j P^k y)\, dy.$$

This applies for j in $\mathscr{E}$, that is, for $N-2(H-1)R$ values of j. The γ_j are linear forms in $\beta_1, \dots, \beta_R$, given in (88), and therefore
$$\gamma_j(\boldsymbol{\beta}) = \gamma_j(P^{-k}\boldsymbol{\zeta}) = P^{-k}\gamma_j(\boldsymbol{\zeta}).$$

Hence (126) becomes

$$P^{N-2(H-1)R-kR} \lim_{\psi\to\infty} \int_{-\psi}^{\psi} \dots \int_{-\psi}^{\psi} \prod_{j\in\mathscr{E}} J_j(\gamma_j)\, d\zeta_1 \dots d\zeta_R, \tag{127}$$

where $$J_j(\gamma_j) = k^{-1} \int_{\lambda_j}^{\lambda_j'} y^{-1+1/k} e(\gamma_j y)\, dy$$

and $$\lambda_j = \kappa_j^{1/k}, \quad \lambda_j' = (\kappa_j')^{1/k}.$$

The power of P in (127), when multiplied by the factor $(P_2 \dots P_H)^{2R}$ in (118), gives P^{Ω}, as in (124). Hence it remains only to prove that

$$\lim_{\psi\to\infty} \int_{-\psi}^{\psi} \dots \int_{-\psi}^{\psi} \prod_{j\in\mathscr{E}} J_j(\gamma_j)\, d\zeta_1 \dots d\zeta_R$$

is a positive number independent of P.

For convenience we take temporarily the values of j in $\mathscr{E}$ to be $j = 1, \dots, M$, where $M = N-2(H-1)R$. We may suppose that the columns for $j = 1, \dots, R$ are linearly independent (for instance we may take them to be the columns of $\mathscr{C}_1$). Apart from a factor k^{-M}, the last expression is

$$\lim_{\psi\to\infty} \int_{-\psi}^{\psi} \dots \int_{-\psi}^{\psi} d\boldsymbol{\zeta} \int_{\mathscr{K}} (y_1 \dots y_M)^{-1+1/k} e(\gamma_1 y_1 + \dots + \gamma_M y_M)\, d\mathbf{y},$$

where $\mathscr{K}$ is the fixed M dimensional region given by $\lambda_j < y_j < \lambda_j'$. Now

$$\sum_{j=1}^{M} \gamma_j y_j = \sum_{j=1}^{M} y_j \sum_{i=1}^{R} a_{ij} \zeta_i = \sum_{i=1}^{R} \zeta_i z_i(\mathbf{y}),$$

where the $z_i(\mathbf{y})$ are the linear forms

$$z_i(\mathbf{y}) = \sum_{j=1}^{M} a_{ij} y_j \quad (i = 1, \dots, R).$$

Hence we can rewrite the previous expression as

$$\lim_{\psi\to\infty} \int_{\mathscr{K}} (y_1 \dots y_M)^{-1+1/k} \prod_{i=1}^{R} \frac{\sin 2\pi\psi z_i}{\pi z_i}\, d\mathbf{y}. \tag{128}$$

The equations $$z_1(\mathbf{y}) = 0, \dots, z_R(\mathbf{y}) = 0$$

have the real solution $y_j = \xi_j^k = \eta_j$ (say), where $\boldsymbol{\xi}$, with all M coordinates positive, is the special real non-singular solution of §§ 6 and 7. By the choice of κ_j, κ_j' in (49) we have

$$\lambda_j < \eta_j < \lambda_j' \quad (j = 1, \dots, M).$$

We were also allowed to take $\lambda_j' - \lambda_j$ arbitrarily small.

In the integral (128) we make a change of variable from

$$y_1, \dots, y_R, y_{R+1}, \dots, y_M$$

to $$z_1, \dots, z_R, y_{R+1}, \dots, y_M,$$

as is permissible since the determinant of the linear forms $z_1, \dots, z_R$ relative to $y_1, \dots, y_R$ is not 0. We can write the result (apart from a positive constant factor) as

$$\lim_{\psi\to\infty} \int_{\mathscr{Z}} \prod_{i=1}^{R} \frac{\sin 2\pi\psi z_i}{\pi z_i} V(z_1, \dots, z_R)\, dz_1 \dots dz_R,$$

where $\mathscr{Z}$ is an R dimensional region which contains the origin as an inner point, and where

$$V(z_1, \ldots, z_R) = \int_{\mathscr{K}(\mathbf{z})} (y_1 \ldots y_M)^{-1+1/k} \,\mathrm{d}y_{R+1} \ldots \mathrm{d}y_M.$$

Here $\mathscr{K}(\mathbf{z})$ is the $M-R$ dimensional section of the M dimensional box $\mathscr{K}$ by the linear space for which $z_1, \ldots, z_R$ have assigned values. The integrand has a positive lower bound, assuming that the numbers $\lambda_j' - \lambda_j$ are sufficiently small.

By Fourier's integral theorem, the last limit has the value $V(0, \ldots, 0)$, and this is a positive constant. Hence the conclusion of the lemma.

Lemma 31. *Suppose the equations* (43) *have a non-singular p-adic solution for every prime p. Then* $\mathfrak{S} > 0$.

Proof. By (122),

$$\mathfrak{S} = \sum_{Q=1}^{\infty} \sum_{\mathbf{A}} Q^{-N} S_0(\mathbf{A}, Q),$$

where the series is absolutely convergent. It follows by standard arguments (see, for example, Davenport 1962, lemma 6) that

$$\mathfrak{S} = \prod_p \chi(p),$$

where

$$\chi(p) = \sum_{\nu=0}^{\infty} \sum_{\mathbf{A}} (p^\nu)^{-N} S_0(\mathbf{A}, p^\nu)$$

in which $\mathbf{A} = (A_1, \ldots, A_R)$ runs through residue classes $(\mathrm{mod}\, p^\nu)$ with $(A_1, \ldots, A_R, p) = 1$. It follows from lemma 23 that

$$\sum_{\mathbf{A}} (p^\nu)^{-N} |S_0(\mathbf{A}, p^\nu)| \ll p^{-\frac{3}{2}\nu}.$$

Hence

$$|\chi(p) - 1| \ll p^{-\frac{3}{2}},$$

and so there exists p_0 such that

$$\prod_{p > p_0} \chi(p) > \tfrac{1}{2}.$$

For an individual $p \leqslant p_0$ it follows from standard arguments (Davenport 1962, lemma 8 for the case $R = 1$) that

$$\chi(p) = \lim_{\nu \to \infty} \frac{M(p^\nu)}{p^{\nu(N-R)}},$$

where $M(p^\nu)$ denotes the total number of solutions of the congruences to the modulus p^ν corresponding to the equations (43). The existence of a non-singular solution in the p-adic field implies that the above limit is positive. Hence the product of $\chi(p)$ for $p \leqslant p_0$ is positive, and this proves the lemma.

We can now summarize the situation reached as a result of the analysis which began in § 6. We need the hypothesis made at the beginning of § 6 that the coefficient matrix has no column all 0. We need also the hypothesis of lemma 12, which in particular supersedes the hypothesis that the forms $f_1, \ldots, f_R$ are linearly independent. If k is even we need also the hypothesis, made in § 7, that the equations (43) have a real non-singular solution. Then, combining (101) and the results of lemmas 28 to 31, we get $\mathscr{N}(P) \to \infty$ as $P \to \infty$. Hence:

Lemma 32. *Suppose that all N variables occur explicitly in the equations* (43). *Suppose that any linear combination, not identically zero, of the forms* $f_1, \ldots, f_R$ *contains more than* $(2H + 3k - 1)\, R$

variables explicitly, where $H = [3k \log Rk]$. *Suppose the equations* (43) *have a non-singular solution in every p-adic field, and further, if k is even, a real non-singular solution. Then the equations* (43) *have infinitely many solutions in integers.*

13. Proofs of theorems 1 and 2

Lemma 32 contains essentially two hypotheses if k is odd, and three if k is even. One of these is the hypothesis that the equations (1) have a non-singular p-adic solution, for every prime p. By theorem 4 this will be true if

$$Q_S \geqslant \begin{cases} [9S^2k \log 3Sk] & \text{if } k \text{ is odd}, \\ [48S^2k^3 \log 3Sk^2] & \text{if } k \text{ is even}. \end{cases} \tag{129}$$

Here Q_S denotes the least number of variables that occur explicitly in any set of S independent linear combinations with rational coefficients (not all 0) of $f_1, \ldots, f_R$. The inequality (129) is to hold for $S = 1, \ldots, R$.

The second essential hypothesis of lemma 32 can be reformulated in the above notation as

$$Q_1 > (2H + 3k - 1)\,R, \tag{130}$$

where $H = [3k \log Rk]$. Now

$$(2H + 3k - 1)\,R = 2R[3k \log Rk] + 3kR - R < [9Rk \log 3Rk].$$

Thus both the hypotheses (129) and (130) will be satisfied if

$$Q_S \geqslant \begin{cases} [9RSk \log 3Rk] & \text{if } k \text{ is odd}, \\ [48RSk^3 \log 3Rk^2] & \text{if } k \text{ is even}, \end{cases} \tag{131}$$

for $S = 1, 2, \ldots, R$.

If k is even, the hypothesis (131) is made explicitly in theorem 2, as also is the hypothesis of non-singular real solubility, needed in lemma 32. Thus the proof of theorem 2 is now complete.

To prove theorem 1, it suffices to show that when k is odd, the hypothesis (131) is superfluous, provided that

$$N \geqslant [9R^2k \log 3Rk]. \tag{132}$$

We proceed by induction on R. If $R = 1$ the condition (131) reduces to (132). Now suppose that $R > 1$ and that the result of theorem 1, with R replaced by $R_1 < R$, has already been established.

If (131) holds for $S = 1, \ldots, R$ there is nothing more to prove. If not, there is some S, necessarily less than R in view of (132), for which

$$Q_S < [9RSk \log 3Rk].$$

We can replace the original R equations by an equivalent system in which S of the equations contain only Q_S variables explicitly. We give these variables the value 0. There remain $R - S$ equations in $N - Q_S$ unknowns. By the inductive hypothesis, with $R_1 = R - S$, these equations have a solution in integers, not all 0, provided that

$$N - Q_S \geqslant [9(R-S)^2 k \log 3(R-S)k],$$

this being the appropriate form of (132).

The last condition is satisfied, because

$$\begin{aligned} N-Q_S &\geqslant [9R^2k\log 3Rk]-[9RSk\log 3Rk]+1 \\ &\geqslant [9R(R-S)\,k\log 3Rk] \\ &\geqslant [9(R-S)^2k\log 3(R-S)\,k]. \end{aligned}$$

This completes the proof of theorem 1.

References

Birch, B. J. 1957 Homogeneous forms of odd degree in a large number of variables. *Mathematika* **4**, 102–105.

Birch, B. J. 1962 Forms in many variables. *Proc. Roy. Soc.* A **265**, 245–263.

Bonnesen, T. & Fenchel, W. 1934 *Theorie der konvexen Körper*, Ergebnisse der Math. III, 1. Berlin: Springer.

Chevalley, C. 1935 Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Hamburg* **11**, 73–75.

Chowla, S. & Shimura, G. 1963 On the representation of zero by a linear combination of k-th powers. *Norske Vid. Selsk. Forh.* **36**, 169–176.

Davenport, H. 1939*a* On Waring's Problem for cubes. *Acta Math.* **71**, 123–143.

Davenport, H. 1939*b* On Waring's Problem for fourth powers. *Ann. Math.* **40**, 731–747.

Davenport, H. 1962 *Analytic methods for Diophantine equations and Diophantine inequalities.* Ann Arbor: Campus Publishers.

Davenport, H. & Lewis, D. J. 1963 Homogeneous additive equations. *Proc. Roy. Soc.* A **274**, 443–460.

Davenport, H. & Lewis, D. J. 1966 Cubic equations of additive type. *Phil. Trans. Roy. Soc.* A **261**, 97–136.