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

Cubic Equations of Additive Type

H. Davenport and D. J. Lewis

Phil. Trans. R. Soc. Lond. A 1966 **261**, 97-136
doi: 10.1098/rsta.1966.0060

CUBIC EQUATIONS OF ADDITIVE TYPE*

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

AND D. J. LEWIS
University of Michigan

(*Received* 30 *December* 1965)

CONTENTS

It is proved that two simultaneous equations of the form

$$a_1 x_1^3 + \ldots + a_n x_n^3 = 0,$$
$$b_1 x_1^3 + \ldots + b_n x_n^3 = 0,$$

with integral coefficients, are soluble (with not all of $x_1, \ldots, x_n$ zero) in p-adic integers for every prime p if $n \geqslant 16$, and are soluble in integers if $n \geqslant 18$. The condition $n \geqslant 16$ in the former result is best possible.

1. Introduction

In a previous paper (Davenport & Lewis 1963) we investigated the solubility of an equation of the type

$$a_1 x_1^k + a_2 x_2^k + \ldots + a_n x_n^k = 0, \tag{1}$$

where $a_1, \ldots, a_n$ are rational integers, both in p-adic integers (where p is an arbitrary prime) and in rational integers. The p-adic case appears to be a necessary preliminary to the rational case, and any method for proving solubility in rational integers must fail if there is a prime power modulus for which the congruence corresponding to the equation is insoluble. We proved that (1) has a non-trivial solution in every p-adic field if $n > k^2$, and we proved the same in the rational field (subject to the condition that the coefficients are not all of the same sign if k is even), except when $7 \leqslant k \leqslant 17$.

In the present paper we investigate the solubility of two simultaneous equations, each

* This paper was written while Professor Lewis was holding a Senior Visiting Fellowship at Cambridge under a research grant made by the Science Research Council.

of the type (1), but we limit ourselves to the case $k = 3$. Thus we shall be concerned with two simultaneous equations of the type

$$\left.\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + \ldots + a_n x_n^3 = 0, \\ b_1 x_1^3 + b_2 x_2^3 + \ldots + b_n x_n^3 = 0, \end{aligned}\right\} \tag{2}$$

and again we investigate solubility both in the p-adic field (for all p) and in the rational field.

We must first recall the known results for a single equation with $k = 3$.

Theorem 1A. *Any equation*

$$a_1 x_1^3 + a_2 x_2^3 + \ldots + a_n x_n^3 = 0 \tag{3}$$

has a solution in p-adic integers, not all 0, *if $n \geqslant 7$, and this is not always true if $n = 6$.*

Theorem 2A. *Any equation* (3) *has a solution in rational integers, not all* 0, *if $n \geqslant 8$.*

Although these are known results, we outline the proofs for the convenience of the reader in an appendix (§ 11).

As regards the simultaneous equations (2), we prove first:

Theorem 1. *Any two simultaneous equations of the type* (2) *have a solution in p-adic integers, not all* 0, *if $n \geqslant 16$; and this is not always true if $n = 15$.*

To justify the last assertion, we take $p = 7$ and we take the equations to be

$$\left.\begin{aligned} \Phi(x_1, \ldots, x_5) + 7\Phi(y_1, \ldots, y_5) + 7^2\Phi(z_1, \ldots, z_5) = 0, \\ \Psi(x_1, \ldots, x_5) + 7\Psi(y_1, \ldots, y_5) + 7^2\Psi(z_1, \ldots, z_5) = 0, \end{aligned}\right\} \tag{4}$$

where

$$\left.\begin{aligned} \Phi(x_1, \ldots, x_5) &= x_1^3 + 2x_2^3 + 6x_3^3 - 4x_4^3, \\ \Psi(x_1, \ldots, x_5) &= \qquad x_2^3 + 2x_3^3 + 4x_4^3 + x_5^3. \end{aligned}\right\} \tag{5}$$

It can be verified (see § 5) that Φ and Ψ are not both divisible by 7 unless $x_1, \ldots, x_5$ are all divisible by 7, and this implies that the equations (4) have no non-trivial solution in the 7-adic field.

The proof of theorem 1 involves the consideration of many cases, and when $p = 3$ the logical structure of the proof is complicated. The arguments used depend heavily on the additive character of the forms, and on the fact that 3 is not a number of the form $p-1$.

For application in the proof of Theorem 2 we need to have (when possible) a non-singular p-adic solution of the equations (2), that is, a solution for which

$$\frac{\partial(F, G)}{\partial(x_i, x_j)} \neq 0 \tag{6}$$

for some i, j, where F, G denote the forms in (2). We prove:

Corollary to theorem 1. *The equations* (2) *have a non-singular p-adic solution provided $n \geqslant 16$ and provided that every form $\lambda F + \mu G$ (λ, μ not both* 0) *contains at least* 7 *variables with non-zero coefficients.*

The last condition is essential, since otherwise there could be a form $\lambda F + \mu G$ which did not vanish except when all the variables explicitly present in it vanished, and then any solution of $F = G = 0$ would be singular.

As regards solubility in rational integers, we prove:

THEOREM 2. *Any two simultaneous equations of the type* (2) *have a solution in rational integers, not all* 0, *if* $n \geqslant 18$.

An important consideration in the proof of theorem 2 is the number of times the same ratio may occur among the ratios a_i/b_i. We are able to dismiss the case in which some ratio occurs at least 7 times by appealing to theorem 2A (see § 6). Thus we can suppose that no ratio occurs more than 6 times. We use a modified form of the Hardy–Littlewood method, on the lines of Davenport's treatment (1939) of Waring's problem. Here we employ a lemma (lemma 19) on the number of solutions of two equations of a particular type in 12 variables. But the success of the proof hinges on being able to allocate the original 18 variables for different treatment, to satisfy a variety of requirements.

We need the corollary to theorem 1 to ensure that the singular series arising from the Hardy–Littlewood treatment of the problem shall be positive (though for this application a weaker form of theorem 1 with 18 in place of 16 would suffice).

2. THE p-ADIC NORMALIZATION OF TWO ADDITIVE FORMS

The arguments of the present section apply to two diagonal forms of any degree k. If

$$\left.\begin{aligned} F &= a_1 x_1^k + a_2 x_2^k + \ldots + a_n x_n^k \\ G &= b_1 x_1^k + b_2 x_2^k + \ldots + b_n x_n^k \end{aligned}\right\} \tag{7}$$

are two such forms, we define

$$\vartheta(F, G) = \prod_{i \neq j} (a_i b_j - a_j b_i). \tag{8}$$

LEMMA 1. (i) *If*

$$\left.\begin{aligned} F'(x_1, \ldots, x_n) &= F(p^{\nu_1} x_1, \ldots, p^{\nu_n} x_n), \\ G'(x_1, \ldots, x_n) &= G(p^{\nu_1} x_1, \ldots, p^{\nu_n} x_n), \end{aligned}\right\} \tag{9}$$

then
$$\vartheta(F', G') = p^{2k(n-1)\nu} \vartheta(F, G), \tag{10}$$

where
$$\nu = \nu_1 + \ldots + \nu_n. \tag{11}$$

(ii) *If*
$$\left.\begin{aligned} f(x_1, \ldots, x_n) &= \lambda F(x_1, \ldots, x_n) + \mu G(x_1, \ldots, x_n), \\ g(x_1, \ldots, x_n) &= \rho F(x_1, \ldots, x_n) + \sigma G(x_1, \ldots, x_n), \end{aligned}\right\} \tag{12}$$

then
$$\vartheta(f, g) = (\lambda\sigma - \mu\rho)^{n(n-1)} \vartheta(F, G). \tag{13}$$

Proof. (i) We have
$$a'_i b'_j - a'_j b'_i = p^{k(\nu_i + \nu_j)} (a_i b_j - a_j b_i),$$
and
$$\sum_{i \neq j} (\nu_i + \nu_j) = 2(n-1)\nu.$$

(ii) If α_i, β_i are the coefficients of x_i^k in f and g respectively, then

$$\alpha_i \beta_j - \alpha_j \beta_i = (\lambda\sigma - \mu\rho)(a_i b_j - a_j b_i),$$

and the number of factors in the product (8) is $n(n-1)$. This proves lemma 1.

We shall call two pairs of forms of the type (7), with integral coefficients, *equivalent* if one pair can be obtained from the other by a combination of the operations (i) and (ii) of lemma 1; here $\nu_1, \ldots, \nu_n$ are integers (positive, negative or zero) and λ, μ, σ, ρ are rational

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

numbers with $\lambda\sigma-\mu\rho \neq 0$. We note that the operations (i) and (ii) are commutative. If the equations $F = G = 0$ have a non-trivial solution in the p-adic field then so do the equations for every equivalent pair of forms.

From now onwards, until § 5, we shall postulate that

$$\vartheta(F, G) \neq 0. \tag{14}$$

This property is plainly preserved under equivalence. From each class of equivalent pairs of forms with integral coefficients, we select a pair of forms for which the power of p dividing $\vartheta(F, G)$ is minimal; this is obviously possible since the power is non-negative. We call such a pair of forms *normalized*. (A similar definition has been used in several other recent papers on p-adic equations; see for example Birch & Lewis (1965) and the references given there.)

We observe that a normalized pair of forms is by no means unique, and indeed any operation of type (ii) with $\lambda\sigma-\mu\rho$ not divisible by p changes a normalized pair into another normalized pair. We call such an operation a *unimodular change of basis*.

To any form H with integral coefficients there corresponds a form H^* with coefficients in the finite field of p elements, these coefficients being congruent (mod p) to the corresponding coefficients of H. Variables explicitly present in H will not necessarily be explicitly present in H^*. By the *rank* of a form we shall understand the number of variables occurring explicitly in it.

LEMMA 2. *A normalized pair of forms can be written as*

$$\left.\begin{aligned} F &= F_0+pF_1+\ldots+p^{k-1}F_{k-1}, \\ G &= G_0+pG_1+\ldots+p^{k-1}G_{k-1}, \end{aligned}\right\} \tag{15}$$

where F_i, G_i are forms in m_i variables, and these sets of variables are disjoint for $i = 0, 1, \ldots, k-1$. Moreover, each of the m_i variables occurs in one at least of F_i, G_i with a coefficient not divisible by p. We have

$$m_0+m_1+\ldots+m_{j-1} \geqslant jn/k \quad \textit{for} \quad j = 1, \ldots, k. \tag{16}$$

Further, if q_j denotes the minimum number of variables occurring explicitly in any form $\lambda^* F_j^* + \mu^* G_j^*$ (where λ^*, μ^* are not both 0) then

$$m_0+\ldots+m_{j-1}+q_j \geqslant (j+\tfrac{1}{2})\, n/k \quad \textit{for} \quad j = 0, \ldots, k-1. \tag{17}$$

Note. We remark that the numbers $m_0, m_1, \ldots, q_0, q_1, \ldots$ are invariant under unimodular change of basis.

Proof. We can certainly express a normalized pair of forms as

$$F = F_0+pF_1+\ldots, \quad G = G_0+pG_1+\ldots,$$

where we put in F_j and G_j those terms $a_i x_i^k$, $b_i x_i^k$ for which p^j is the highest power of p dividing both a_i and b_i. Then the sets of variables occurring in F_0, G_0, in F_1, G_1, and so on are obviously disjoint.

We now prove that the forms F_j and G_j are empty if $j \geqslant k$. This follows from the minimal property of $\vartheta(F, G)$; for if $a_i x_i^k$, $b_i x_i^k$ were terms in F, G with a_i, b_i both divisible by p^k we could diminish the power of p dividing $\vartheta(F, G)$ by an operation of type (i), namely that of putting $x_i = p^{-1}x_i'$, while preserving the integral character of the coefficients.

It remains to prove (16) and (17). Let $x_1, \ldots, x_m$, where $m = m_0 + \ldots + m_{j-1}$, denote the variables in $F_0, G_0, \ldots, F_{j-1}, G_{j-1}$. Then the forms

$$F' = p^{-j} F(px_1, \ldots, px_m, x_{m+1}, \ldots, x_n),$$
$$G' = p^{-j} G(px_1, \ldots, px_m, x_{m+1}, \ldots, x_n)$$

have integral coefficients and are equivalent to F, G. By (10) and (13) of lemma 1,

$$\vartheta(F', G') = p^{-2jn(n-1)+2k(n-1)m} \vartheta(F, G).$$

By the definition of a normalized pair, we have $m \geqslant jn/k$, and this proves (16).

In proving (17), we can suppose without loss of generality that q_j is the number of variables occurring explicitly in G_j^*. Let these variables be $x_{m+1}, \ldots, x_{m+q}$, where $q = q_j$. Then the forms

$$F'' = p^{-j} F(px_1, \ldots, px_{m+q}, x_{m+q+1}, \ldots, x_n),$$
$$G'' = p^{-j-1} G(px_1, \ldots, px_{m+q}, x_{m+q+1}, \ldots, x_n)$$

have integral coefficients and are equivalent to F, G. By (10) and (13) of lemma 1,

$$\vartheta(F'', G'') = p^{-(2j+1)\, n(n-1) + 2k(n-1)\,(m+q)} \vartheta(F, G).$$

Hence $m+q \geqslant (j+\frac{1}{2})\, n/k$, whence (17). This completes the proof of lemma 2.

3. The case $p \neq 3$

In the present section we suppose that F, G are additive cubic forms in 16 variables which satisfy (14) and are normalized in the sense of the preceding section. In particular the conclusions of lemma 2 hold. Thus by (16) and (17), with $k = 3$, we have

$$m_0 \geqslant 6, \tag{18}$$

$$q_0 \geqslant 3. \tag{19}$$

Our object is to prove (lemma 10) that the congruences $F \equiv G \equiv 0 \pmod{p}$ have a non-singular solution, that is, a solution for which

$$\frac{\partial F}{\partial x_i}\frac{\partial G}{\partial x_j} - \frac{\partial F}{\partial x_j}\frac{\partial G}{\partial x_i} \not\equiv 0 \pmod{p} \tag{20}$$

for some i, j. Since $p \neq 3$, this condition is equivalent to

$$(a_i b_j - a_j b_i)\, x_i x_j \not\equiv 0 \pmod{p} \tag{21}$$

for some i, j. This will easily lead to a solution of the p-adic equations $F = G = 0$ (see § 5).

In proving the result just stated, we are concerned only with the forms F_0, G_0; or, more precisely, with F_0^* $(=F^*)$, G_0^* $(=G^*)$. By making a suitable unimodular change of basis (which does not disturb the normalization) we can ensure that G_0^* is a form of minimal rank among all forms $\lambda^* F_0^* + \mu^* G_0^*$, where λ^*, μ^* are not both 0, and that F_0^* has minimal rank among all such forms with $\lambda^* \neq 0$. By the definitions of the preceding sections, the number of variables occurring explicitly in G_0^* is q_0, and the number of variables occurring explicitly in the pair F_0^*, G_0^* is m_0.

Let s denote the number of variables occurring explicitly in both F_0^* and G_0^*, let t denote the number occurring explicitly in G_0^* but not in F_0^*, and let r denote the number occurring explicitly in F_0^* but not in G_0^*. We have

$$r+s+t = m_0 \geqslant 6, \quad s+t = q_0 \geqslant 3. \tag{22}$$

With an obvious notation, we can write

$$F_0^* = a_1 y_1^3 + \ldots + a_r y_r^3 + b_1 x_1^3 + \ldots + b_s x_s^3, \tag{23}$$

$$G_0^* = \qquad c_1 x_1^3 + \ldots + c_s x_s^3 + d_1 z_1^3 + \ldots + d_t z_t^3. \tag{24}$$

If t were 0 we could replace F_0^* by $F_0^* - b_1 c_1^{-1} G_0^*$ which would be of lower rank, contrary to the choice of F_0^*. Hence $t \geqslant 1$. Also $r+s = \text{rank } F_0^* \geqslant \text{rank } G_0^* = s+t$. Hence

$$r \geqslant t \geqslant 1. \tag{25}$$

By the choice of notation, all the coefficients a_i, b_i, c_i, d_i are non-zero (in the finite field of p elements). By multiplying F_0^* and G_0^* throughout by suitable constants, we can ensure that

$$a_1 = 1, \quad d_1 = 1. \tag{26}$$

We observe that the number of suffixes i for which b_i/c_i has a particular value cannot exceed t. For if it did, and the ratio b_i/c_i were λ, the form $F_0^* - \lambda G_0^*$ would contain fewer than $r+s$ variables, contrary to the choice of F_0^*. In particular, if $t = 1$ the ratios

$$b_1/c_1, \ldots, b_s/c_s$$

are all distinct.

In proving lemma 10 we can suppose that $p \equiv 1 \pmod 3$. For if $p \equiv -1 \pmod 3$, every residue class is a cubic residue, and therefore we can omit the exponents 3 in (23) and (24). We can solve the resulting linear congruences with $y_1 \not\equiv 0$ and $z_1 \not\equiv 0$, and this solution satisfies (21). Henceforward we assume that $p \equiv 1 \pmod 3$.

We need the following known results on cubic congruences.†

LEMMA 3. *The congruence*

$$ax^3 + by^3 + cz^3 \equiv d \pmod p$$

is always soluble if $abcd \not\equiv 0 \pmod p$.

Proof. Davenport & Lewis (1963), lemma 1, with $k = 3$.

LEMMA 4. *The congruence*

$$ax^3 + by^3 + cz^3 \equiv 0 \pmod p$$

is always soluble with one at least of $x, y, z \not\equiv 0 \pmod p$.

Proof. Lewis (1957), theorem 1.

LEMMA 5. *For* $p \equiv 1 \pmod 3$, *the congruence*

$$ax^3 + by^3 \equiv c \pmod p$$

is always soluble if $abc \not\equiv 0 \pmod p$ *and* $p \neq 7$; *and it is soluble when* $p = 7$ *unless* $b \equiv \pm a$ *and* $c \equiv \pm 4a$.

† A referee has pointed out that the results of lemmas 3, 4 and 5 can be deduced from Gauss's determination of the number of solutions of $ax^3 + by^3 \equiv c \pmod p$ in his *Disquisitiones Arithmeticae* (art. 358).

Proof. The assertion for $p > 7$ is theorem 3 (with $k = 3$) of Chowla, Mann & Straus (1959).

If $ax^3 + by^3 \equiv c \pmod 7$ is not soluble, we must have $z \equiv 0$ in the congruence of lemma 4, whence $a/b \equiv$ a cube, that is, $b \equiv \pm a \pmod 7$. In this case $ax^3 + by^3$ assumes the values 0, $\pm a$, $\pm 2a$ only and therefore $c \equiv \pm 4a \pmod 7$.

LEMMA 6. *If $r \geqslant 3$ the congruences*

$$F_0^* \equiv G_0^* \equiv 0 \pmod p \tag{27}$$

have a non-singular solution.

Proof. Since $q_0 = s + t \geqslant 3$, we can solve $G_0^* \equiv 0 \pmod p$, by lemma 4, with some variable appearing explicitly in G_0^* different from zero. Let $\xi_1, \xi_2, \ldots, \xi_s, \zeta_1, \ldots, \zeta_t$ be such a solution. Now we solve $F_0^* \equiv 0$, which takes the form

$$a_1 y_1^3 + \ldots + a_r y_r^3 + (b_1 \xi_1^3 + \ldots + b_s \xi_s^3) \equiv 0 \pmod p.$$

By lemmas 3 and 4 this congruence has a solution with some $y_i \not\equiv 0$. Since the ratio corresponding to the y_i (namely $1/0$) is different from the other ratios, the values

$$y_1, \ldots, y_r, \xi_1, \ldots, \xi_s, \zeta_1, \ldots, \zeta_t$$

provide a non-singular solution of $F_0^* \equiv G_0^* \equiv 0 \pmod p$.

LEMMA 7. *If $r = t = 2$ the congruences* (27) *have a non-singular solution.*

Proof. We have $s \geqslant 2$ by (22), and

$$F_0^* \equiv y_1^3 + a_2 y_2^3 + b_1 x_1^3 + \ldots + b_s x_s^3,$$
$$G_0^* \equiv \qquad c_1 x_1^3 + \ldots + c_s x_s^3 + z_1^3 + d_2 z_2^3.$$

Suppose first that $p \neq 7$. By lemma 5 we can then solve the congruences

$$y_1^3 + a_2 y_2^3 + b_1 \equiv 0 \pmod p,$$
$$z_1^3 + d_2 z_2^3 + c_1 \equiv 0 \pmod p,$$

and for such a solution one at least of $y_1, y_2 \not\equiv 0$ and one at least of $z_1, z_2 \not\equiv 0$. Since the ratios corresponding to the y's and to the z's are unequal, $y_1, y_2, 1, 0, \ldots, z_1, z_2$ is a non-singular solution.

Suppose now that $p = 7$. The same argument succeeds unless $a_2 \equiv \pm 1$ or $d_2 \equiv \pm 1$. Suppose that $a_2 \not\equiv \pm 1$ and $d_2 \equiv \pm 1$. As x_1^3 and x_2^3 assume the values 0, ± 1, the form $c_1 x_1^3 + c_2 x_2^3$ assumes at least four distinct non-zero values modulo 7. One at least of these is assumed by $-(z_1^3 + d_2 z_2^3)$. Hence we can solve $G_0^* \equiv 0 \pmod 7$ with one at least of $x_1, x_2 \not\equiv 0$ and one at least of $z_1, z_2 \not\equiv 0$. For these values of x_1, x_2, let $B = b_1 x_1^3 + b_2 x_2^3$. We can solve $y_1^3 + a_2 y_2^3 + B \equiv 0$ by lemma 5 and the fact that y_1, y_2 may be 0 if $B \equiv 0$. Then $y_1, y_2, x_1, x_2, 0, \ldots, 0, z_1, z_2$ is a solution of (27) which is non-singular since the ratios corresponding to the x's and the z's are different. We have a similar argument if $a_2 \equiv \pm 1$ and $d_2 \not\equiv \pm 1$. If $a_2 \equiv \pm 1$ and $d_2 \equiv \pm 1$ there is an obvious solution with the x_i all 0.

LEMMA 8. *If $r = 2$ and $t = 1$ the congruences* (27) *have a non-singular solution.*

Proof. We have $s \geqslant 3$ by (22), and moreover by an earlier remark the ratios

$$b_1/c_1, \ldots, b_s/c_s$$

are all different. The forms are

$$F_0^* = y_1^3 + a_2 y_2^3 + b_1 x_1^3 + \ldots + b_s x_s^3,$$
$$G_0^* = \qquad c_1 x_1^3 + \ldots + c_s x_s^3 + z^3.$$

By lemma 3 we can solve $G_0^* \equiv 0$ with $z = 1$, and plainly such a solution will have some $x_i \not\equiv 0$. If we can then solve $F_0^* \equiv 0$ in y_1, y_2 we shall have a non-singular solution of $F_0^* \equiv G_0^* \equiv 0 \pmod{p}$. By lemma 5 this is possible unless $p = 7$, $a_2 \equiv \pm 1 \pmod 7$ and $B = b_1 x_1^3 + b_2 x_2^3 + b_3 x_3^3 \equiv \pm 4 \pmod 7$ whenever $G_0^* \equiv 0 \pmod 7$. Henceforward we suppose this to be the case, and without loss of generality we may assume that the c_i are restricted to the values 1, 2 and 4.

Apart from permutations, there are the following possibilities for c_1, c_2 and c_3:

(1)	1,	1,	1;	(6)	2,	2,	1;
(2)	2,	2,	2;	(7)	2,	2,	4;
(3)	4,	4,	4;	(8)	4,	4,	1;
(4)	1,	1,	2;	(9)	4,	4,	2;
(5)	1,	1,	4;	(10)	1,	2,	4.

We shall show that in each of these cases our supposition leads to inconsistent linear congruence conditions on the b_i; hence the supposition must be false and the congruences (27) have a non-singular solution.

Cases (1), (6), (8). The solution $x_1 = 1$, $x_2 = -1$, $x_3 = 0, z = 0$ of $G_0^* \equiv 0$ gives

$$B = b_1 - b_2 \equiv \pm 4 \pmod 7.$$

The solution $0, 0, 1, -1$ of $G_0^* \equiv 0$ gives $b_3 \equiv \pm 4 \pmod 7$. The solution $1, -1, 1, -1$ gives $b_1 - b_2 + b_3 \equiv \pm 4 \pmod 7$. These congruence conditions are inconsistent.

Cases (4), (5). The solution $1, 0, 0, -1$ gives $b_1 \equiv \pm 4 \pmod 7$. The solution $0, 1, 0, -1$ gives $b_2 \equiv \pm 4 \pmod 7$. The solution $1, -1, 0, 0$ gives $b_1 - b_2 \equiv \pm 4 \pmod 7$. Again these conditions are inconsistent.

Cases (2), (3). The solution $1, -1, 0, 0$ gives $b_1 - b_2 \equiv \pm 4 \pmod 7$, and by symmetry we get $b_2 - b_3 \equiv \pm 4 \pmod 7$, and $b_3 - b_1 \equiv \pm 4 \pmod 7$, which are inconsistent conditions.

Cases (7), (9). The solution $1, -1, 0, 0$ gives $b_1 - b_2 \equiv \pm 4 \pmod 7$. The solution $1, 0, 1, 1$ gives $b_1 + b_3 \equiv \pm 4 \pmod 7$. The solution $0, 1, 1, 1$ gives $b_2 + b_3 \equiv \pm 4 \pmod 7$. These conditions are inconsistent.

Case (10). The solution $1, 0, 0, -1$ gives $b_1 \equiv \pm 4 \pmod 7$. The solution $0, 1, 1, 1$ gives $b_2 + b_3 \equiv \pm 4 \pmod 7$. The solution $1, 1, 1, 0$ gives $b_1 + b_2 + b_3 \equiv \pm 4 \pmod 7$. These conditions are inconsistent.

This completes the proof of lemma 8.

LEMMA 9. *If* $r = t = 1$ *the congruences* (27) *have a non-singular solution.*

Proof. We have $s \geq 4$ by (22), and again the ratios $b_1/c_1, \ldots, b_s/c_s$ are distinct. The forms are

$$F_0^* = y^3 + b_1 x_1^3 + \ldots + b_s x_s^3,$$
$$G_0^* = \qquad c_1 x_1^3 + \ldots + c_s x_s^3 + z^3.$$

We choose representatives A, B of the two classes of cubic non-residues (mod p) such that
$$1+A+B \equiv 0 \pmod{p}.$$
This is possible, for if A_0, B_0 are arbitrary representatives, by lemma 4 the congruence
$$X^3+A_0Y^3+B_0Z^3 \equiv 0 \pmod{p}$$
has a non-trivial solution and it is easily seen that such a solution has $XYZ \not\equiv 0$. Thus we can take $A = A_0Y^3X^{-3}$, $B = B_0Z^3X^{-3}$.

Without loss of generality we can suppose that c_1, c_2, c_3, c_4 are restricted to the values 1, A and B. The possibilities for c_1, c_2, c_3, c_4, apart from permutations, are:

(1)	1,	1,	1,	1;	(9)	A,	A,	A,	1;
(2)	1,	1,	A,	A;	(10)	A,	A,	B,	1;
(3)	1,	1,	B,	B;	(11)	B,	B,	A,	1;
(4)	A,	A,	A,	A;	(12)	B,	B,	B,	1;
(5)	A,	A,	B,	B;	(13)	1,	1,	A,	B;
(6)	B,	B,	B,	B;	(14)	A,	A,	A,	B;
(7)	1,	1,	A,	1;	(15)	B,	B,	A,	B.
(8)	1,	1,	B,	1;					

Cases (1) *to* (6). In these $c_1 \equiv c_2$ and $c_3 \equiv c_4$, and hence from the distinctness of the ratios b_i/c_i we have $b_1 \not\equiv b_2$ and $b_3 \not\equiv b_4$. We can solve the congruence $G_0^* \equiv 0 \pmod{p}$ by taking $x_1 \equiv -x_2 \equiv \xi \pmod{p}$, $x_3 \equiv -x_4 \equiv \eta \pmod{p}$, and $z \equiv 0 \pmod{p}$. The congruence $F_0^* \equiv 0 \pmod{p}$ then becomes
$$y_1^3+(b_1-b_2)\,\xi^3+(b_3-b_4)\,\eta^3 \equiv 0 \pmod{p}.$$
By lemma 4, this congruence has a non-trivial solution and hence a solution with one at least of $\xi, \eta \not\equiv 0 \pmod{p}$. We then have a non-singular solution of (27), the non-singularity being satisfied by reference either to the variables x_1, x_2 (if $\xi \not\equiv 0$) or to the variables x_3, x_4 (if $\eta \not\equiv 0$).

Cases (7) *to* (12). Again $b_1 \not\equiv b_2$. We can solve $G_0^* \equiv 0 \pmod{p}$ by taking
$$x_1 \equiv -x_2 \equiv \xi \pmod{p}, \quad x_3 \equiv 0 \pmod{p}, \quad x_4 \equiv -z \equiv \zeta \pmod{p}.$$
The congruence $F_0^* \equiv 0 \pmod{p}$ becomes
$$y^3+(b_1-b_2)\,\xi^3+b_4\zeta^3 \equiv 0 \pmod{p}.$$
As above, we can solve this with either ξ or $\zeta \not\equiv 0$, and this gives a non-singular solution of (27).

Cases (13), (14), (15). Again $b_1 \not\equiv b_2$. We solve $G_0^* \equiv 0 \pmod{p}$ by taking $x_1 \equiv -x_2 \equiv \xi$, $x_3 \equiv x_4 \equiv z \equiv \zeta$ (note that $A+B+1 \equiv 0$). The congruence $F_0^* \equiv 0 \pmod{p}$ becomes
$$y^3+(b_1-b_2)\,\xi^3+(b_3+b_4)\,\zeta^3 \equiv 0 \pmod{p}.$$
This last congruence has a solution with ξ or $\zeta \not\equiv 0$ (if $b_3+b_4 \equiv 0$ we take $y \equiv \xi \equiv 0$, $\zeta \equiv 1$), and this gives a non-singular solution of (27).

This completes the proof of lemma 9.

Lemma 10. *If F, G is a pair of normalized p-adic forms ($p \neq 3$) in $n \geqslant 16$ variables, then the congruences*

$$F^* \equiv G^* \equiv 0 \pmod{p}$$

have a non-singular solution.

Proof. When F, G are normalized forms in $n \geqslant 16$ variables, the hypotheses of lemmas 6 to 9 cover all possibilities for r, s and t. Hence these lemmas imply the conclusion.

4. The case $p = 3$

Our object in this section will be to prove (lemma 18) that a pair of forms in $n \geqslant 16$ variables over the 3-adic field satisfying (14) and normalized in the sense of § 2 is equivalent to a pair of forms F, G such that the congruences

$$F \equiv G \equiv 0 \pmod{9}$$

have a solution for which
$$(a_i b_j - a_j b_i)\, x_i x_j \not\equiv 0 \pmod{3} \tag{28}$$
for some i, j. Such a solution will be called a *non-singular solution modulo* 9.

An important part is played in this section by the fact that $x^3 \equiv x \pmod{3}$. This enables us to treat diagonal cubic forms (mod 3) as linear forms (mod 3). [Of course such is not the case modulo 9.] In particular two diagonal cubic forms in three variables have a non-trivial zero modulo 3.

We note further that if

$$a_1/b_1, \quad a_2/b_2, \quad a_3/b_3 \quad \text{are distinct} \pmod{3} \tag{29}$$

then the congruences
$$\left.\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 &\equiv 0 \pmod{3}, \\ b_1 x_1^3 + b_2 x_2^3 + b_3 x_3^3 &\equiv 0 \pmod{3} \end{aligned}\right\} \tag{30}$$
have a solution with $x_1 x_2 x_3 \not\equiv 0 \pmod{3}$. Also if

$$a_1/b_1 \equiv a_2/b_2 \not\equiv a_3/b_3 \equiv a_4/b_4 \pmod{3} \tag{31}$$

then the congruences
$$\left.\begin{aligned} a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_4 x_4^3 &\equiv 0 \pmod{3}, \\ b_1 x_1^3 + b_2 x_2^3 + b_3 x_3^3 + b_4 x_4^3 &\equiv 0 \pmod{3} \end{aligned}\right\} \tag{32}$$
have a solution with $x_1 x_2 x_3 x_4 \not\equiv 0 \pmod{3}$. A set of three variables, say x_1, x_2, x_3, whose ratios satisfy (29) or a set of four variables, say x_1, x_2, x_3, x_4, whose ratios satisfy (31) will be called an *essential set*. When we speak of a solution corresponding to an essential set we shall mean a solution of (30) or (32) such that *none* of the variables is $\equiv 0 \pmod{3}$. Such solutions necessarily satisfy (28) for some x_i, x_j in the set.

Our first sequence of lemmas 11 to 15, does not assume that F, G are normalized. We simply consider any forms
$$\left.\begin{aligned} F &= F_0 + 3F_1 + 3^2 F_2, \\ G &= G_0 + 3G_1 + 3^2 G_2, \end{aligned}\right\} \tag{33}$$
where F_i, G_i are diagonal cubic forms in m_i variables in which each term x_j^3 occurs in at least one of F_i, G_i with a coefficient not divisible by 3, and the sets of variables for $i = 0, 1, 2$ are disjoint. We do not now assume that $\Sigma m_i \geqslant 16$.

As before, we define q_i, for $i = 0, 1, 2$, to be the minimal number of variables appearing in any form in the pencil $\lambda^* F_i^* + \mu^* G_i^*$, where λ^*, μ^* are not both 0. Note that

$$m_i \geqslant q_i + 1 \quad \text{if} \quad q_i > 0.$$

The variables appearing in F_i, G_i fall into blocks according to the ratio of their coefficients modulo 3. If the number of variables with ratio η^* is h then the rank of $F_i^*-\eta^*G_i^*$ is m_i-h. Hence $m_i-h \geqslant q_i$, that is,

$$h \leqslant m_i-q_i.$$

In particular, if $q_i \geqslant 1$ then the variables in F_i, G_i fall into two or more non-empty blocks of equal ratios. Also, if $q_i \geqslant 2$ then either there are three or more non-empty blocks of equal ratios or there are two blocks, each containing at least two variables. Thus $q_i \geqslant 2$ implies the existence of an essential set among the variables in F_i, G_i.

LEMMA 11. *If F, G is a pair of forms such that either*

$$q_0 \geqslant 2 \quad and \quad q_1 \geqslant 1,$$

or

$$q_1 \geqslant 2 \quad and \quad q_2 \geqslant 1,$$

or

$$q_2 \geqslant 2 \quad and \quad q_0 \geqslant 1,$$

then the pair F, G is equivalent to a pair which has a non-singular zero modulo 9.

Proof. First suppose that $q_0 \geqslant 2$ and $q_1 \geqslant 1$. As noted above there is an essential set of variables among those appearing explicitly in F_0, G_0. Let $\mathbf{a}$ be a solution corresponding to this set. Put $F_0(\mathbf{a}) = 3\alpha$, $G_0(\mathbf{a}) = 3\beta$. The congruences

$$F_0(\mathbf{a})+3F_1(\mathbf{w}) \equiv 3(\alpha+F_1(\mathbf{w})) \equiv 0 \pmod 9,$$
$$G_0(\mathbf{a})+3G_1(\mathbf{w}) \equiv 3(\beta+G_1(\mathbf{w})) \equiv 0 \pmod 9$$

are equivalent to two linear (possibly non-homogeneous) congruences (mod 3), which are obviously soluble since, as remarked above, $q_1 \geqslant 1$ implies at least two distinct ratios among the variables occurring in F_1, G_1. This solution is non-singular (mod 9) since $\mathbf{a}$ comes from an essential set.

Now suppose that $q_1 \geqslant 2$ and $q_2 \geqslant 1$. We multiply each of the variables in F_0, G_0 by 3 and divide both forms by 3. The resulting forms are equivalent to F, G and have

$$q_0 \geqslant 2, \quad q_1 \geqslant 1;$$

whence they have a non-singular zero modulo 9. Similarly, if $q_2 \geqslant 2$ and $q_0 \geqslant 1$ we multiply each of the variables in F_0, G_0, F_1, G_1 by 3 and divide both forms by 9 to obtain a pair of equivalent forms for which $q_0 \geqslant 2$ and $q_1 \geqslant 1$.

LEMMA 12. *If*

$$q_0 \geqslant 4 \quad and \quad m_1 \geqslant 1$$

then the forms F, G have a non-singular zero modulo 9.

Proof. We note that if F, G have a non-singular zero modulo 9 so does any pair obtained from F, G by a unimodular change of basis. After making a unimodular change of basis we can suppose that G_0^* is a form of minimal rank among the forms $\lambda^*F_0^*+\mu^*G_0^*$ (where λ^*, μ^* are not both 0) and that F_0^* is a form of minimal rank among those with $\lambda^* \neq 0$. With an obvious notation, we can write

$$\left.\begin{aligned} F_0^* &= a_1y_1^3+\ldots+a_ry_r^3+b_1x_1^3+\ldots+b_sx_s^3, \\ G_0^* &= \qquad\qquad\qquad\quad c_1x_1^3+\ldots+c_sx_s^3+d_1z_1^3+\ldots+d_tz_t^3. \end{aligned}\right\} \tag{34}$$

Here our hypothesis implies that $s+t \geqslant 4.$ (35)

Also, as in § 3, our conventions imply that

$$r \geqslant t \geqslant 1, \tag{36}$$

and at most t of the b_i/c_i have the same value. Since the ratios b_i/c_i are $\not\equiv 0$ or ∞ they are $\equiv \pm 1 \pmod 3$, whence $t = 1$ would give $s \leqslant 2$, contrary to (35). Thus we have $t \geqslant 2$.

We now show that there are at least two disjoint essential sets among the variables in F_0, G_0.

Case 1. *Suppose* $t \geqslant 4$. Then $r \geqslant 4$ and clearly there are two disjoint sets of type (31), namely y_1, y_2, z_1, z_2 and y_3, y_4, z_3, z_4.

Case 2. *Suppose* $t = 3$. Then $r \geqslant 3$ and $s \geqslant 1$. In this case y_1, y_2, z_1, z_2 and y_3, x_1, z_3 are two disjoint essential sets.

Case 3. *Suppose* $t = 2$. Then $r \geqslant 2$ and $s \geqslant 2$. In this case x_1, y_1, z_1 and x_2, y_2, z_2 are disjoint essential sets.

We multiply the solution corresponding to one of the essential sets by T_1 and the solution corresponding to the other essential set by T_2. Then

$$F_0 + 3F_1 \equiv 3(\alpha_1 T_1^3 + \alpha_2 T_2^3 + \sum_1^{m_1} \lambda_i w_i^3) \pmod 9,$$

$$G_0 + 3G_1 \equiv 3(\beta_1 T_1^3 + \beta_2 T_2^3 + \sum_1^{m_1} \mu_i w_i^3) \pmod 9,$$

where $\alpha_1, \beta_1, \alpha_2, \beta_2$ are 3-adic integers and $w_1, \ldots, w_{m_1}$ are the variables in F_1, G_1. By hypothesis $m_1 \geqslant 1$. To find a non-singular zero modulo 9, it suffices to solve

$$\left.\begin{aligned} \alpha_1 T_1^3 + \alpha_2 T_2^3 + \lambda_1 w_1^3 &\equiv 0 \pmod 3, \\ \beta_1 T_1^3 + \beta_2 T_2^3 + \mu_1 w_1^3 &\equiv 0 \pmod 3, \end{aligned}\right\} \tag{37}$$

with at least one of $T_1, T_2 \not\equiv 0 \pmod 3$. Since there are three variables the congruences (37) have a non-trivial solution. Since $m_1 \geqslant 1$, at least one of $\lambda_1, \mu_1 \not\equiv 0 \pmod 3$ and consequently this solution cannot have $T_1 \equiv T_2 \equiv 0 \pmod 3$. Thus the solution includes a non-zero multiple of a solution corresponding to an essential set, and so is non-singular.

Lemma 13. *If* $q_0 \geqslant 6$ *and* $m_0 \geqslant 9$

then the forms F, G *have a non-singular zero modulo* 9.

Proof. The proof is on the same general lines as for the preceding two lemmas, except that we do not use F_1, G_1; indeed they may be empty. This time we show that there are at least three disjoint essential sets among the variables in F_0, G_0. On multiplying the solution corresponding to the first essential set by T_1, the second by T_2, etc., we obtain

$$F_0 \equiv 3(\alpha_1 T_1^3 + \alpha_2 T_2^3 + \alpha_3 T_3^3) \equiv 0 \pmod 9,$$

$$G_0 \equiv 3(\beta_1 T_1^3 + \beta_2 T_2^3 + \beta_3 T_3^3) \equiv 0 \pmod 9.$$

These congruences necessarily have a solution with one of the $T_i \not\equiv 0 \pmod 3$, and hence the resulting solution is a non-singular zero of F, G (modulo 9).

We now show how to choose the three disjoint essential sets. Once again, after a unimodular change of basis, we can assume that F_0, G_0 are as in (34), that (36) holds, that

$$r+s+t \geqslant 9, \quad s+t \geqslant 6, \tag{38}$$

and that any ratio b_i/c_i occurs at most t times. Since the b_i/c_i are necessarily congruent to ± 1 (mod 3), we have

$$s \leqslant 2t.$$

Since $s+t \geqslant 6$ the possibility $t = 1$ is excluded, and if $t = 2$ we must have $s = 4$ and $r \geqslant 3$.

Case 1. *Suppose that* $t \geqslant 6$. Then $r \geqslant 6$ and there are three essential sets of type (31).

Case 2. *Suppose that* $t = 5$. Then $r \geqslant 5$ and $s \geqslant 1$. We take the three sets to be:

$$y_1, y_2, z_1, z_2; \quad y_3, y_4, z_3, z_4; \quad y_5, x_1, z_5.$$

Case 3. *Suppose that* $t = 4$. Then $r \geqslant 4$ and $s \geqslant 2$. We take the three sets to be:

$$y_1, y_2, z_1, z_2; \quad y_3, x_1, z_3; \quad y_4, x_2, z_4.$$

Case 4. *Suppose that* $t = 3$. Then $r \geqslant 3$, $s \geqslant 3$. We take the three sets to be

$$x_i, y_i, z_i \quad (i = 1, 2, 3).$$

Case 5. *Suppose that* $t = 2$. Then $r \geqslant 3$ and $s = 4$ as noted earlier. We can suppose that $b_3/c_3 \not\equiv b_4/c_4$ (mod 3). We take the three sets to be: x_1, y_1, z_1; x_2, y_2, z_2; x_3, x_4, y_3.

This completes the proof of lemma 13.

Lemma 14. *If*

$$q_0 \geqslant 4 \quad \textit{and} \quad m_0 \geqslant 7 + q_0$$

then the forms F, G have a non-singular zero modulo 9.

Proof. By lemma 12 we can suppose that $m_1 = 0$. By lemma 13 we can suppose that $q_0 = 4$ or 5.

Once again, following a unimodular change of basis, we can suppose that G_0^* has minimal rank among the forms $\lambda^* F_0^* + \mu^* G_0^*$, where λ^*, μ^* are not both 0, and that F_0^* has minimal rank among those forms for which $\lambda^* \neq 0$. We can write F_0, G_0 (mod 9) as

$$\left.\begin{aligned} F_0 &\equiv a_1 y_1^3 + \ldots + a_r y_r^3 + b_1 x_1^3 + \ldots + b_s x_s^3 + 3(f_1 z_1^3 + \ldots + f_t z_t^3) \quad (\text{mod } 9), \\ G_0 &\equiv 3(e_1 y_1^3 + \ldots + e_r y_r^3) + c_1 x_1^3 + \ldots + c_s x_s^3 + d_1 z_1^3 + \ldots + d_t z_t^3 \quad (\text{mod } 9), \end{aligned}\right\} \tag{39}$$

where none of $a_i, b_i, c_i, d_i \equiv 0$ (mod 3). We know that

$$s+t = 4 \text{ or } 5 \quad \text{and} \quad r \geqslant 7. \tag{40}$$

Also we recall that not more than t of the ratios b_i/c_i can have the same particular value (mod 3). As in lemma 12 this implies that $t \geqslant 2$. We have $a_i \equiv \pm 1$ (mod 3), and we can suppose that

$$a_i \equiv 1 \quad (\text{mod } 3),$$

on replacing y_i by $-y_i$ where necessary. Thus $a_i \equiv 1$ or 4 or 7 (mod 9), and since $r \geqslant 7$ there must be three of them that are mutually congruent, say

$$a_5 \equiv a_6 \equiv a_7 \quad (\text{mod } 9).$$

We first form two disjoint essential sets from $y_1, \ldots, y_4, x_1, \ldots, x_s, z_1, \ldots, z_t$. This can be done as in lemma 12, since $s+t \geqslant 4$. We multiply a solution corresponding to one essential set by T_1 and a solution corresponding to the other essential set by T_2. Finally, we put

$$y_5 = y_6 = y_7 = Y.$$

Then
$$F_0 \equiv 3(\alpha_1 T_1^3 + \alpha_2 T_2^3 + Y^3) \equiv 0 \pmod 9,$$
$$G_0 \equiv 3(\beta_1 T_1^3 + \beta_2 T_2^3 + \gamma Y^3) \equiv 0 \pmod 9,$$

the unit coefficient of Y in the first congruence coming from the fact that

$$a_5 + a_6 + a_7 \equiv 3 \pmod 9.$$

These congruences have a solution with one at least of $T_1, T_2, Y \not\equiv 0 \pmod 3$. Obviously no such solution has $T_1 \equiv T_2 \equiv 0 \pmod 3$. It follows that this solution is a non-singular zero modulo 9 for the pair F, G.

LEMMA 15. *If*

$$F \equiv a_1 y_1^3 + \ldots + a_r y_r^3 + b_1 x_1^3 + \ldots + b_q x_q^3 + 3(f_2 w_2^3 + \ldots + f_u w_u^3) \pmod 9,$$
$$G \equiv 3(e_1 y_1^3 + \ldots + e_r y_r^3) + c_1 x_1^3 + \ldots + c_q x_q^3 + 3w_1^3 + 3(g_2 w_2^3 + \ldots + g_u w_u^3) \pmod 9,$$

where none of $a_i, c_i \equiv 0 \pmod 3$ *and if*

$$r \geqslant 5, \quad q \geqslant 2$$

then F, G *have a non-singular zero modulo* 9.

Proof. As before, we can assume that

$$a_i \equiv 1 \pmod 3 \quad \text{for} \quad i = 1, \ldots, r,$$

so that the a_i are restricted to the values 1, 4 and 7 (mod 9). Consequently, there are either three equal a_i or three distinct a_i (mod 9), and in either case the sum of these three a_i is $\equiv 3 \pmod 9$. We take them to be a_3, a_4, a_5.

We can form an essential set from the variables y_1, y_2, x_1, x_2, and we multiply a solution corresponding to this essential set by T. We also put $y_3 = y_4 = y_5 = Y$ and put

$$w_2 = \ldots = w_u = 0.$$

Then
$$F \equiv 3(\alpha T^3 + Y^3) \equiv 0 \pmod 9,$$
$$G \equiv 3(\beta T^3 + \gamma Y^3 + w_1^3) \equiv 0 \pmod 9.$$

These congruences have a solution with one at least of $T, Y, w_1 \not\equiv 0 \pmod 3$. For such a solution $T \not\equiv 0 \pmod 3$ since otherwise $Y \equiv w_1 \equiv 0 \pmod 3$. Thus F, G have a non-singular zero (mod 9).

For the remainder of this section we suppose that F, G is a normalized pair of forms in $n \geqslant 16$ variables. By lemma 2 and the hypothesis that $n \geqslant 16$, we have

$$m_0 \geqslant 6, \quad m_0 + m_1 \geqslant 11, \quad m_0 + m_1 + m_2 \geqslant 16, \tag{41}$$
$$q_0 \geqslant 3, \quad m_0 + q_1 \geqslant 8, \quad m_0 + m_1 + q_2 \geqslant 14. \tag{42}$$

LEMMA 16. *If F, G are normalized forms in $n \geqslant 16$ variables and $q_0 \geqslant 4$ then they are equivalent to a pair of forms which have a non-singular zero modulo* 9.

Proof. By lemma 11 the conclusion holds unless $q_1 = 0$ and $q_2 \leqslant 1$. By (42) we then have

$$m_0 \geqslant 8, \quad m_0 + m_1 \geqslant 13.$$

By lemma 12 the conclusion holds unless $m_1 = 0$, in which case $m_0 \geqslant 13$. Now by lemma 13 the conclusion holds unless $q_0 = 4$ or 5. But in that event, we have $m_0 \geqslant 8 + q_0$, and by lemma 14 the conclusion holds.

LEMMA 17. *If F, G are normalized forms in $n \geqslant 16$ variables, and $q_0 = 3$, then they are equivalent to a pair of forms which have a non-singular zero modulo* 9.

Proof. We can suppose that G_0^* has minimal rank among all forms $\lambda_0^* F_0^* + \mu_0^* G_0^*$, where λ_0^*, μ_0^* are not both 0. We can also suppose that either F_1^* or G_1^* has minimal rank among all forms $\lambda_1^* F_1^* + \mu_1^* G_1^*$, where λ_1^*, μ_1^* are not both 0. For in the contrary case there will be a form $\lambda_1^* F_1^* + \mu_1^* G_1^*$ of minimal rank, where $\lambda_1^* \mu_1^* \neq 0$. Then we replace F by $F + \mu_1 \lambda_1^{-1} G$; this does not disturb the minimal property of G_0^*, and the new F_1^* is of minimal rank among all forms that are linear combinations of F_1^*, G_1^*.

By lemma 11 the conclusion of the present lemma holds unless $q_1 = 0$ and $q_2 = 0$ or 1. By (42) this implies that

$$m_0 \geqslant 8, \quad m_0 + m_1 \geqslant 13. \tag{43}$$

There are exactly 3 $(= q_0)$ variables occurring explicitly in G_0^*, say x_1, x_2, x_3. There are $r = m_0 - 3 \geqslant 5$ variables occurring explicitly in F_0^* and not in G_0^*, say $y_1, \ldots, y_r$. Thus we can write

$$F_0 = a_1 y_1^3 + \ldots + a_r y_r^3 + g_1 x_1^3 + g_2 x_2^3 + g_3 x_3^3,$$

$$G_0 = 3(e_1 y_1^3 + \ldots + e_r y_r^3) + c_1 x_1^3 + c_2 x_2^3 + c_3 x_3^3,$$

where all a_i and all c_i are $\not\equiv 0 \pmod 3$. We can suppose without loss of generality that

$$a_i \equiv 1 \pmod 3, \quad c_i \equiv 1 \pmod 3. \tag{44}$$

Since $q_1 = 0$ and one of the forms F_1^*, G_1^* is of minimal rank among all forms

$$\lambda_1^* F_1^* + \mu_1^* G_1^*,$$

we have either F_1^* or G_1^* identically zero. Suppose first that F_1^* is identically 0 and G_1^* is not. Then we have the situation of lemma 15 in which there is a variable (w_1 in the hypothesis of that lemma) which occurs explicitly in G_1^* but not in F_1^*. Since $r \geqslant 5$ and $q_0 = 3$, the hypotheses of lemma 15 are satisfied and the conclusion of the present lemma follows.

We can now suppose that G_1^* is identically 0. In this case we prove that $e_1, \ldots, e_r$ cannot all be mutually congruent (mod 3). If $e_i \equiv e \pmod 3$ for $i = 1, \ldots, r$, then $(G - 3eF)^*$ contains only the three variables x_1, x_2, x_3, and the coefficients of the y_i^3 in $G - 3eF$ are all divisible by 9. Also $(G_1 - 3eF_1)^*$ is identically 0. Let F', G', be the forms F, $G - 3eF$ after putting $x_i = 3x_i'$ $(i = 1, 2, 3)$. All the coefficients of G' are divisible by 9, whence, by lemma 1, we have

$$\vartheta(F', 3^{-2}G') = 3^{18(n-1)-2n(n-1)} \vartheta(F, G).$$

But $n \geqslant 16$ and hence $\vartheta(F', 3^{-2}G') < \vartheta(F, G)$, contrary to the hypothesis that F, G is a normalized pair. Hence the e_i are not mutually congruent (mod 3).

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

Suppose that F_1^* and G_1^* both vanish, so that $m_1 = 0$. Then $r \geq 10$ by (43), since $r = m_0 - q_0 \geq 13-3$. Since there are three possible values for the e_i (mod 3), there is one set of at least four of the e_i which are mutually congruent, say e_1, e_2, e_3, e_4. Put $a_i = 1+3\alpha_i$. One at least of $1+\alpha_1+\alpha_2+\alpha_3$, $1+\alpha_1+\alpha_2+\alpha_4$, $1+\alpha_1+\alpha_3+\alpha_4$, $1+\alpha_2+\alpha_3+\alpha_4$ must be $\not\equiv 0 \pmod 3$, since their sum is $\equiv 1 \pmod 3$. We may suppose that

$$1+\alpha_1+\alpha_2+\alpha_3 = A \not\equiv 0 \pmod 3.$$

Taking $y_1 = y_2 = y_3 = X$, we get

$$\begin{aligned} a_1 y_1^3 + a_2 y_2^3 + a_3 y_3^3 &\equiv 3(1+\alpha_1+\alpha_2+\alpha_3)\, X^3 \\ &\equiv 3AX^3 \pmod 9, \\ 3(e_1 y_1^3 + e_2 y_2^3 + e_3 y_3^3) &\equiv 9e_1 X^3 \equiv 0 \pmod 9. \end{aligned}$$

Since the e_i are not all mutually congruent (mod 3) we can suppose that $e_5 \not\equiv e_4 \pmod 3$. Putting $y_4 = -y_5 = Y$, we get

$$\begin{aligned} a_4 y_4^3 + a_5 y_5^3 &\equiv 3(\alpha_4-\alpha_5)\, Y^3 \pmod 9, \\ 3(e_4 y_4^3 + e_5 y_5^3) &\equiv 3EY^3 \pmod 9, \end{aligned}$$

where $E \not\equiv 0 \pmod 3$. From the variables y_6, y_7, x_1, x_2, x_3 we can form an essential set, and we multiply a corresponding solution by T. Then

$$\begin{aligned} F &\equiv 3(AX^3 + (\alpha_4-\alpha_5)\, Y^3 + \alpha T^3) \equiv 0 \pmod 9, \\ G &\equiv 3(EY^3 \qquad\qquad\qquad + \beta T^3) \equiv 0 \pmod 9, \end{aligned}$$

where $AE \not\equiv 0 \pmod 3$. These congruences have a solution with not all of

$$X, Y, T \equiv 0 \pmod 3,$$

and hence one with $T \not\equiv 0 \pmod 3$. As usual this implies the existence of a non-singular solution of $F \equiv G \equiv 0 \pmod 9$.

Finally, we suppose that G_1^* is identically 0 and $F_1^* = \Sigma h_i w_i^3$ is not identically 0, say $h_1 \not\equiv 0 \pmod 3$. We can suppose that $e_1 \not\equiv e_2 \pmod 3$. On putting $y_1 = -y_2 = X$, we get

$$\begin{aligned} a_1 y_1^3 + a_2 y_2^3 &\equiv 3(\alpha_1-\alpha_2)\, X^3 \equiv 3BX^3 \pmod 9, \\ 3(e_1 y_1^3 + e_2 y_2^3) &\equiv 3(e_1-e_2)\, X^3 \equiv 3EX^3 \pmod 9, \end{aligned}$$

where $E \not\equiv 0 \pmod 3$. From the variables y_3, y_4, x_1, x_2, x_3 we form an essential set and multiply a corresponding solution by T. Put all but the first variable in F_1^* equal to 0. Then

$$\begin{aligned} F &\equiv 3(BX^3 + \alpha T^3 + h_1 w_1^3) \equiv 0 \pmod 9, \\ G &\equiv 3(EX^3 + \beta T^3) \qquad\quad \equiv 0 \pmod 9, \end{aligned}$$

where $Eh_1 \not\equiv 0 \pmod 3$. These congruences have a solution with $T \not\equiv 0 \pmod 3$, and hence $F \equiv G \equiv 0 \pmod 9$ has a non-singular solution.

This completes the proof of lemma 17.

Lemma 18. *If F, G is a pair of normalized forms in $n \geq 16$ variables then F, G are equivalent to a pair of forms which have a non-singular zero modulo* 9.

Proof. Lemmas 16 and 17 and formulae (41) and (42).

5. Proof of theorem 1 and its corollary

Proof of Theorem 1. Let F, G be diagonal cubic forms with rational integral coefficients in $x_1, x_2, \ldots, x_n$, where $n \geqslant 16$. Theorem 1 asserts that there is a non-trivial p-adic integral solution of the equations $F = G = 0$, and this is equivalent to the assertion that the congruences

$$F \equiv G \equiv 0 \pmod{p^\nu} \tag{45}$$

have, for every positive integer ν, a solution in which not all of $x_1, x_2, \ldots, x_n$ are divisible by p.

In proving this assertion we can suppose without loss of generality that $\vartheta(F, G) \neq 0$. For if $\vartheta(F, G) = 0$ we replace F, G by

$$F' = F + p^{\nu+1}(c_1 x_1^3 + \ldots + c_n x_n^3),$$
$$G' = G + p^{\nu+1}(d_1 x_1^3 + \ldots + d_n x_n^3),$$

where $c_1, \ldots, c_n, d_1, \ldots, d_n$ are integers chosen (as they obviously can be) so that $\vartheta(F', G') \neq 0$. The congruences (45) are equivalent to the congruences

$$F' \equiv G' \equiv 0 \pmod{p^\nu},$$

and the solubility of the latter (with $x_1, \ldots, x_n$ not all divisible by p) implies that of the former.

Case 1. *Suppose that* $p \neq 3$. By lemma 10 the congruences

$$F \equiv G \equiv 0 \pmod{p} \tag{46}$$

have a solution for which

$$\frac{\partial F}{\partial x_i}\frac{\partial G}{\partial x_j} - \frac{\partial F}{\partial x_j}\frac{\partial G}{\partial x_i} \not\equiv 0 \pmod{p} \tag{47}$$

for some i, j. We apply a well known method (sometimes called Newton approximation) which establishes, by induction on μ, the solubility of

$$F \equiv G \equiv 0 \pmod{p^\mu} \tag{48}$$

subject to (47). The inductive hypothesis is satisfied for $\mu = 1$. Suppose it is satisfied for a particular $\mu \geqslant 1$, and let $\mathbf{x}$ be a solution of (48) subject to (47). Putting $\mathbf{y} = \mathbf{x} + p^\mu \mathbf{t}$, we obtain

$$F(\mathbf{y}) \equiv F(\mathbf{x}) + p^\mu \sum_{i=1}^{n} \frac{\partial F}{\partial x_i} t_i \pmod{p^{\mu+1}},$$

$$G(\mathbf{y}) \equiv G(\mathbf{x}) + p^\mu \sum_{i=1}^{n} \frac{\partial G}{\partial x_i} t_i \pmod{p^{\mu+1}}.$$

Thus we shall have $F(\mathbf{y}) \equiv G(\mathbf{y}) \equiv 0 \pmod{p^{\mu+1}}$ provided $t_1, \ldots, t_n$ satisfy the linear congruences

$$p^{-\mu}F(\mathbf{x}) + \sum_{i=1}^{n} \frac{\partial F}{\partial x_i} t_i \equiv 0 \pmod{p},$$

$$p^{-\mu}G(\mathbf{x}) + \sum_{i=1}^{n} \frac{\partial G}{\partial x_i} t_i \equiv 0 \pmod{p}.$$

These are soluble since the linear forms in $t_1, \ldots, t_n$ are non-proportional $\pmod{p}$, by (47). Further, since $\mathbf{y} \equiv \mathbf{x} \pmod{p^\mu}$, $\mu \geqslant 1$, the condition (47) remains valid when $\mathbf{x}$ is replaced by $\mathbf{y}$. This proves the result.

Case 2. *Suppose that* $p = 3$. As we observed in §2 it suffices to prove the p-adic solubility for an equivalent pair of forms. By lemma 18 there is an equivalent pair F, G such that the congruences

$$F \equiv G \equiv 0 \pmod 9$$

are soluble with

$$9^{-1}\left(\frac{\partial F}{\partial x_i}\frac{\partial G}{\partial x_j} - \frac{\partial F}{\partial x_j}\frac{\partial G}{\partial x_i}\right) \not\equiv 0 \pmod 3,$$

that is

$$x_i x_j (a_i b_j - a_j b_i) \not\equiv 0 \pmod 3, \tag{49}$$

for some i, j. It suffices to prove (for $\mu \geqslant 2$) the solubility of

$$F \equiv G \equiv 0 \pmod{3^\mu}$$

subject to (49). The proof is again by induction on μ, but now we put $\mathbf{y} = \mathbf{x} + 3^{\mu-1}\mathbf{t}$. We obtain

$$F(\mathbf{y}) \equiv F(\mathbf{x}) + 3^\mu \Sigma a_i x_i^2 t_i \pmod{3^{\mu+1}},$$

$$G(\mathbf{y}) \equiv G(\mathbf{x}) + 3^\mu \Sigma b_i x_i^2 t_i \pmod{3^{\mu+1}}.$$

Again the linear forms are non-proportional (mod 3) by (49), and the conclusion follows.

It remains only to prove the last assertion of theorem 1, which follows from the insolubility of the equations (4) in the 7-adic field. It suffices to prove that the congruences

$$\Phi = x_1^3 + 2x_2^3 + 6x_3^3 - 4x_4^3 \equiv 0 \pmod 7,$$

$$\Psi = x_2^3 + 2x_3^3 + 4x_4^3 + x_5^3 \equiv 0 \pmod 7,$$

have no solution except the trivial one.

Put

$$\Theta = 2x_2^3 + 6x_3^3 - 4x_4^3.$$

The only non-trivial solutions of $\Psi \equiv 0 \pmod 7$ are given by

$$\pm(x_2^3, \ldots, x_5^3) = (1, 0, 0, -1), \quad (1, -1, 0, 1), \quad (0, 1, 1, 1), \quad (1, 1, 1, 0), \quad (1, 1, -1, 1).$$

The values of Θ for the sets of values on the right are

$$\Theta \equiv 2, \quad -4, \quad 2, \quad 4, \quad -2,$$

respectively. Since ± 2 and ± 4 are cubic non-residues (mod 7), none of the sets gives a solution of

$$\Phi \equiv x_1^3 + \Theta \equiv 0 \pmod 7.$$

This proves the result.

Remark. Although we have stated theorem 1 only for forms with rational integral coefficients, the same result for forms with p-adic coefficients follows at once from theorem 1.

Proof of the corollary to theorem 1. Let

$$\left.\begin{aligned} F &= a_1 x_1^3 + \ldots + a_n x_n^3, \\ G &= b_1 x_1^3 + \ldots + b_n x_n^3. \end{aligned}\right\} \tag{50}$$

The variables fall into blocks, with variables in the same block if the ratios of their coefficients a_i/b_i are the same. Since $n \geqslant 16$, by theorem 1 the equations (50) have a non-trivial p-adic integral solution, say $\xi_1, \ldots, \xi_n$ with $\xi_1 \neq 0$. If this solution were non-singular we should have the desired result. If it is singular and $\xi_i \neq 0$ then x_1 and x_i belong to the same block. Let $x_1, \ldots, x_r$ be the variables in the block containing x_1. Then all the non-zero ξ_i must have $1 \leqslant i \leqslant r$. We can pass to an equivalent pair of equations of the shape

$$c_1 x_1^3 + \ldots + c_r x_r^3 + a_{r+1} x_{r+1}^3 + \ldots + a_n x_n^3 = 0,$$
$$d_{r+1} x_{r+1}^3 + \ldots + d_n x_n^3 = 0,$$

where none of the c_i or d_j is 0, and where $c_1 \xi_1^3 + \ldots + c_r \xi_r^3 = 0$. By hypothesis the second equation contains at least 7 variables explicitly. Hence, by theorem 1A, we can find $\beta_{r+1}, \ldots, \beta_n$, not all 0, such that

$$d_{r+1} \beta_{r+1}^3 + \ldots + d_n \beta_n^3 = 0.$$

If

$$a_{r+1} \beta_{r+1}^3 + \ldots + a_n \beta_n^3 = 0$$

then $\xi_1, \ldots, \xi_r, \beta_{r+1}, \ldots, \beta_n$ is a non-singular solution of the equations (50).

We can now suppose that

$$A = a_{r+1} \beta_{r+1}^3 + \ldots + a_n \beta_n^3 \neq 0,$$

and we consider

$$c_1(\xi_1 + y)^3 + c_2 \xi_2^3 + \ldots + c_r \xi_r^3 + A u^3 = 0.$$

This is equivalent to

$$3c_1 \xi_1^2 y + 3c_1 \xi_1 y^2 + c_1 y^3 + A u^3 = 0, \tag{51}$$

where c_1, ξ_1 and A are all $\neq 0$. Take $u \neq 0$ and divisible by a high power of p. Then (51) has a solution for y of the form

$$y = (-A/3c_1 \xi_1^2)\, u^3 + \lambda_6 u^6 + \lambda_9 u^9 + \ldots, \tag{52}$$

where the series is convergent in the p-adic sense if u is divisible by a sufficiently high power of p. Under this same condition we have

$$\xi_1 + y \neq 0.$$

Now $\xi_1 + y, \xi_2, \ldots, \xi_r, u\beta_{r+1}, \ldots, u\beta_n$ is a non-singular solution of (50), since $\xi_1 + y \neq 0$ and $\beta_i u \neq 0$ for some $i > r$.

6. Preliminaries to the proof of theorem 2

In theorem 2 we can suppose that $n = 18$, since if $n > 18$ we can equate to zero the last $n - 18$ variables.

As explained in § 1, we first dispose of the case in which there are 7 or more of the ratios a_i/b_i in the equations (2) that are equal. Without loss of generality (by taking a linear combination of the equations) we can suppose that the equations are

$$a_1 x_1^3 + \ldots \qquad + a_{18} x_{18}^3 = 0, \tag{53}$$
$$b_8 x_8^3 + \ldots + b_{18} x_{18}^3 = 0. \tag{54}$$

(Some of the coefficients here may be zero.) By theorem 2A the equation (54) has a solution in integers $\xi_8, \ldots, \xi_{18}$, not all 0. It now suffices to solve the equation

$$a_1 x_1^3 + \ldots + a_7 x_7^3 + u^3(a_8 \xi_8^3 + \ldots + a_{18} \xi_{18}^3) = 0$$

in integers $x_1, \ldots, x_7, u$, not all 0, and again this is possible by theorem 2A. Thus the assertion is justified, and from now onwards we shall assume that *no ratio occurs more than 6 times among the a_i/b_i*. In particular, therefore, at least 3 distinct ratios occur.

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

The general plan of the proof will be to divide the 18 variables in (2) into 10 and 8, say $x_1, \ldots, x_{10}$ and $x_{11}, \ldots, x_{18}$, in a manner to be explained in § 8. Since the ratios

$$a_1/b_1, \ldots, a_{10}/b_{10}$$

are not all equal, there exists a real solution of the linear equations

$$\left.\begin{aligned} a_1\chi_1+\ldots+a_{10}\chi_{10} &= 0, \\ b_1\chi_1+\ldots+b_{10}\chi_{10} &= 0, \end{aligned}\right\} \tag{55}$$

with no χ_i zero. Without loss of generality (by changing x_i into $-x_i$, if necessary) we can suppose that $\chi_i > 0$ $(i=1, \ldots, 10)$. We choose positive constants κ_i, κ_i' to satisfy

$$\kappa_i < \chi_i^{\frac{1}{3}} < \kappa_i'. \tag{56}$$

For each $i = 1, \ldots, 10$ we define an exponential sum

$$T_i(\gamma) = \sum_{\kappa_i P < x < \kappa_i' P} e(\gamma x^3), \tag{57}$$

where γ is a real variable and P is large; and we also define a shorter exponential sum

$$U(\gamma) = \sum_{P^{\frac{4}{5}} < x < 2P^{\frac{4}{5}}} e(\gamma x^3). \tag{58}$$

Let $\mathcal{N}(P)$ denote the number of solutions of the equations (2) in integers $x_1, \ldots, x_{18}$ subject to

$$\kappa_i P < x_i < \kappa_i' P \quad (i=1, \ldots, 10), \tag{59}$$

$$P^{\frac{4}{5}} < x_i < 2P^{\frac{4}{5}} \quad (i=11, \ldots, 18). \tag{60}$$

Our aim will be to prove that $\mathcal{N}(P) \to \infty$ as $P \to \infty$, and this will prove theorem 2.

Let α, α' be real variables, and let

$$\gamma_i = a_i\alpha + b_i\alpha' \quad (i=1, \ldots, 18). \tag{61}$$

We can express $\mathcal{N}(P)$ as a double integral, namely

$$\mathcal{N}(P) = \int_0^1 \int_0^1 T_1(\gamma_1)\ldots T_{10}(\gamma_{10})\, U(\gamma_{11})\ldots U(\gamma_{18})\, d\alpha\, d\alpha', \tag{62}$$

and this is the starting point of the proof.

We define the *major arcs* (though the name is something of a misnomer, since they are squares) to consist of those α, α' which admit simultaneous rational approximations B/R, B'/R with

$$\left|\alpha - \frac{B}{R}\right| < \frac{1}{RP^{2+\delta}}, \quad \left|\alpha' - \frac{B'}{R}\right| < \frac{1}{RP^{2+\delta}}, \tag{63}$$

where
$$(B, B', R) = 1 \quad \text{and} \quad 1 \leqslant R \leqslant P^{1-\delta}. \tag{64}$$

Here δ is a sufficiently small number, independent of P. These major arcs are non-overlapping, for if $B_1/R_1 \neq B_2/R_2$ we have

$$|B_1/R_1 - B_2/R_2| \geqslant 1/R_1R_2 > (1/R_1 + 1/R_2)\, P^{-2-\delta}.$$

We denote an individual major arc by $\mathfrak{M}(B, B', R)$, and the totality of the major arcs by $\mathfrak{M}$. We define the *minor arcs* $\mathfrak{m}$ to consist of the rest of the square $0 < \alpha < 1$, $0 < \alpha' < 1$.

As usual in applications of the Hardy–Littlewood method, the principal difficulty lies in estimating the contribution made by the minor arcs to the integral in (62). This will be the subject of the next two sections. The general idea will be to deduce the estimate from

$$\max_{(\alpha,\alpha')\in\mathfrak{m}} |T_1(\gamma_1)\dots T_6(\gamma_6)| \int_0^1\int_0^1 |T_7(\gamma_7)\dots U(\gamma_{18})|\,\mathrm{d}\alpha\,\mathrm{d}\alpha', \tag{65}$$

but the choice of the 6 factors to be taken outside will need careful consideration.

We shall prove (lemma 26) that it is possible to divide the 18 ratios a_i/b_i (among which no one ratio occurs more than 6 times) into 3 sets of 6 such that, in each set of 6, no one ratio occurs more than twice. One such set of 6 will give rise to $T_1(\gamma_1), \dots, T_6(\gamma_6)$, and the other two (some of which will be allotted to exponential sums T and some to exponential sums U) will give rise to $T_7(\gamma_7), \dots, U(\gamma_{18})$ in (65).

The treatment of the double integral in (65) will be based on the lemmas of the next section. The estimation of the factors taken outside in (65) will be based on Weyl's inequality and the estimates of Davenport (1939), but of course it will be necessary to correlate, as far as possible, the Diophantine character of the various linear combinations $\gamma_1, \dots, \gamma_6$ of α and α'. This will be the theme of § 8.

7. Two equations in 12 variables

The object of the present section is to prove the following

Lemma 19. *Suppose that of the 6 ratios*

$$a_7/b_7,\quad a_8/b_8,\quad a_{11}/b_{11},\quad a_{12}/b_{12},\quad a_{13}/b_{13},\quad a_{14}/b_{14}, \tag{66}$$

either (i) $a_7/b_7, a_8/b_8, a_{13}/b_{13}$ *are distinct and* $a_{11}/b_{11} = a_7/b_7, a_{12}/b_{12} = a_8/b_8$,

or (ii) $a_7/b_7, a_8/b_8, a_{11}/b_{11}, a_{12}/b_{12}, a_{13}/b_{13}$ *are distinct.*

Then†
$$\int_0^1\int_0^1 |T_7(\gamma_7)\,T_8(\gamma_8)\,U(\gamma_{11})\,U(\gamma_{12})\,U(\gamma_{13})\,U(\gamma_{14})|^2\,\mathrm{d}\alpha\,\mathrm{d}\alpha' \ll P^{\frac{26}{5}+\epsilon} \tag{67}$$

for large P and any fixed $\epsilon > 0$.

We can suppose without loss of generality that $a_{13}/b_{13} = a_{14}/b_{14}$, for by Cauchy's inequality the integral does not exceed the geometric mean of two integrals, one with γ_{13} in place of γ_{14} and one with γ_{14} in place of γ_{13}.

In either case, the integral in (67) represents the number of solutions of the simultaneous equations

$$\left.\begin{aligned} &a_7x_7^3+a_8x_8^3+a_{11}x_{11}^3+a_{12}x_{12}^3+a_{13}x_{13}^3+a_{14}x_{14}^3\\ &\quad= a_7y_7^3+a_8y_8^3+a_{11}y_{11}^3+a_{12}y_{12}^3+a_{13}y_{13}^3+a_{14}y_{14}^3,\\ &b_7x_7^3+b_8x_8^3+b_{11}x_{11}^3+b_{12}x_{12}^3+b_{13}x_{13}^3+b_{14}x_{14}^3\\ &\quad= b_7y_7^3+b_8y_8^3+b_{11}y_{11}^3+b_{12}y_{12}^3+b_{13}y_{13}^3+b_{14}y_{14}^3, \end{aligned}\right\} \tag{68}$$

where the variables are integers subject to

$$\left.\begin{aligned} \kappa_i P < x_i, y_i < \kappa_i' P \quad (i=7,8),\\ P^{\frac{4}{5}} < x_i, y_i < 2P^{\frac{4}{5}} \quad (i=11,12,13,14). \end{aligned}\right\} \tag{69}$$

† We use Vinogradov's notation $\ll$ to indicate an inequality with an unspecified constant factor.

In case (i) we can form linear combinations of the two equations to eliminate x_7 (and therefore also x_{11}) or to eliminate x_8 (and therefore also x_{12}). Replacing x_7 by x and x_8 by X, and recalling that $a_{13}/b_{13} = a_{14}/b_{14}$, and relettering the coefficients and the remaining variables, we obtain two equations of the form

$$\left.\begin{aligned} ax^3+a_1x_1^3+a_3x_3^3+a_4x_4^3 &= ay^3+a_1y_1^3+a_3y_3^3+a_4y_4^3,\\ bX^3+b_2x_2^3+ka_3x_3^3+ka_4x_4^3 &= bY^3+b_2y_2^3+ka_3y_3^3+ka_4y_4^3,\end{aligned}\right\} \tag{70}$$

subject to

$$\left.\begin{aligned} \kappa_7 P < x, y < \kappa_7' P, \quad \kappa_8 P < X, Y < \kappa_8' P,\\ P^{\frac{4}{5}} < x_i, y_i < 2P^{\frac{4}{5}}.\end{aligned}\right\} \tag{71}$$

As a consequence of the hypothesis of case (i), none of the new coefficients is 0. We shall investigate the number of solutions of (70), (71) in lemmas 20 to 22.

In case (ii) we can again form linear combinations of the two equations (68) to eliminate x_7 or x_8, but now none of the other variables disappears. With a similar change of notation, we obtain two equations of the form

$$\left.\begin{aligned} ax^3+a_1x_1^3+a_2x_2^3+a_3x_3^3+a_4x_4^3 &= ay^3+a_1y_1^3+a_2y_2^3+a_3y_3^3+a_4y_4^3,\\ bX^3+b_1x_1^3+b_2x_2^3+ka_3x_3^3+ka_4x_4^3 &= bY^3+b_1y_1^3+b_2y_2^3+ka_3y_3^3+ka_4y_4^3,\end{aligned}\right\} \tag{72}$$

again subject to (71). In consequence of the hypotheses of case (ii), none of the new coefficients is 0, and the ratios

$$a_1/b_1, \quad a_2/b_2, \quad a_3/ka_3$$

are distinct. We shall investigate the number of solutions of (72), (71) in lemmas 23 to 25.

In connexion with the estimate (67), we note that the number of solutions of either (70) or (72) with corresponding variables equal, that is, the number of possibilities for x, X, x_1, x_2, x_3, x_4 in (71), is proportional to $P^{2+4(\frac{4}{5})} = P^{\frac{26}{5}}$.

LEMMA 20. *The number of solutions of* (70) *subject to* (71), *with* $x = y$ *and* $X = Y$ *is* $\ll P^{\frac{26}{5}+\epsilon}$ *for any fixed* $\epsilon > 0$.

Proof. The number of possibilities for x, y, X, Y is $\ll P^2$. The remaining variables satisfy

$$a_1x_1^3+a_3x_3^3+a_4x_4^3 = a_1y_1^3+a_3y_3^3+a_4y_4^3,$$

$$b_2x_2^3+ka_3x_3^3+ka_4x_4^3 = b_2y_2^3+ka_3y_3^3+ka_4y_4^3.$$

These are equivalent to

$$ka_1x_1^3-b_2x_2^3 = ka_1y_1^3-b_2y_2^3,$$

$$a_3x_3^3+a_4y_4^3-a_3y_3^3-a_4y_4^3 = a_1y_1^3-a_1x_1^3.$$

The first equation has $\ll P^{\frac{4}{5}(2+\epsilon)}$ solutions in x_1, x_2, y_1, y_2, and when these variables have particular values, the second equation has $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions in x_3, x_4, y_3, y_4. [The number of divisors of a positive integer m is $\ll m^{\epsilon}$.] Hence the number of solutions of (70) with $x = y$, $X = Y$ is $\ll P^{2+\frac{8}{5}(2+\epsilon)}$, as stated.

LEMMA 21. *The number of solutions of* (70) *subject to* (71), *with* $x = y$ *and* $X \neq Y$ *is* $\ll P^{\frac{26}{5}+\epsilon}$.

Proof. The number of possibilities for x, y is $\ll P$. The remaining variables satisfy the equations

$$a_1x_1^3+a_3x_3^3+a_4x_4^3 = a_1y_1^3+a_3y_3^3+a_4y_4^3, \tag{73}$$

$$bX^3+b_2x_2^3+ka_3x_3^3+ka_4x_4^3 = bY^3+b_2y_2^3+ka_3y_3^3+ka_4x_4^3. \tag{74}$$

The last equation can be replaced by

$$bX^3+b_2x_2^3-ka_1x_1^3 = bY^3+b_2y_2^3-ka_1y_1^3. \tag{75}$$

We put $Y = X+T$ and rewrite (75) and (73) as

$$b\Delta_T(X^3)+b_2(y_2^3-x_2^3) = ka_1(y_1^3-x_1^3), \tag{76}$$

$$a_3(x_3^3-y_3^3)+a_4(x_4^3-y_4^3) = a_1(y_1^3-x_1^3), \tag{77}$$

where $\Delta_T(X^3) = (X+T)^3-X^3$. Since $T \neq 0$ and

$$\Delta_T(X^3) > 3X^2|T| \gg P^2|T|,$$

and all other terms in (76) have absolute value $\ll P^{\frac{12}{5}}$, it follows that

$$0 < |T| \ll P^{\frac{2}{5}}.$$

If $x_1 = y_1$ then the number of possibilities for x_1, y_1 is $\ll P^{\frac{4}{5}}$, and the number of possibilities for x_3, y_3, x_4, y_4 in (77) is $(P^{\frac{4}{5}})^{2+\epsilon}$, and the number of possibilities for x_2, y_2 is $\ll P^{\frac{8}{5}}$. Then T, X are determined by (76) with $\ll P^{\epsilon}$ solutions. Thus the number of solutions of (70) of the kind under consideration in this lemma, with $x_1 = y_1$, is

$$\ll P^{1+\frac{4}{5}+\frac{4}{5}(2+\epsilon)+\frac{8}{5}} \ll P^{5+\epsilon}.$$

If $x_1 \neq y_1$ and $x_3 = y_3$, the values of x_1, y_1 determine those of x_4, y_4 with $\ll P^{\epsilon}$ possibilities, and the values of x_2, y_2 determine those of X, T with $\ll P^{\epsilon}$ possibilities. Thus the number of solutions of this type is

$$\ll P^{1+\frac{4}{5}(5+\epsilon)} \ll P^{5+\epsilon}.$$

We can now limit ourselves to solutions with $x_1 \neq y_1$ and $x_3 \neq y_3$. Let $S(T, x_1, y_1, x_4, y_4)$ denote the number of solutions of (76) and (77) with prescribed values of the variables indicated. Then the total number S of solutions is given by

$$S = \sum_{T, x_1, y_1, x_4, y_4} S(T, x_1, y_1, x_4, y_4).$$

By Cauchy's inequality

$$S^2 \leqslant \{\sum_{T, x_1, y_1, x_4, y_4} 1\}\{\sum_{T, x_1, y_1, x_4, y_4} S^2(T, x_1, y_1, x_4, y_4)\} \ll \{P^{\frac{2}{5}+4(\frac{4}{5})}\}\{S_1\}, \tag{78}$$

say.

Here S_1 can be interpreted as the number of solutions, in all the variables, of the four equations

$$b\Delta_T(X^3)+b_2(y_2^3-x_2^3) = ka_1(y_1^3-x_1^3), \tag{79}$$

$$b\Delta_T(X'^3)+b_2(y_2'^3-x_2'^3) = ka_1(y_1^3-x_1^3), \tag{80}$$

$$a_3(x_3^3-y_3^3)+a_4(x_4^3-y_4^3) = a_1(y_1^3-x_1^3), \tag{81}$$

$$a_3(x_3'^3-y_3'^3)+a_4(x_4^3-y_4^3) = a_1(y_1^3-x_1^3). \tag{82}$$

Consider first solutions of this system with $X = X'$. By subtracting (79), (80) we get the equation

$$y_2^3-x_2^3 = y_2'^3-x_2'^3,$$

which has $\ll P^{\frac{4}{5}(2+\epsilon)}$ solutions. There are also $\ll P^{1+\frac{2}{5}}$ possibilities for T and X $(=X')$. Then x_1, y_1 are determined with $\ll P^{\epsilon}$ possibilities, since $x_1 \neq y_1$. Turning now to (81), (82) we see that x_4, y_4 determine x_3, y_3, x_3', y_3' with $\ll P^{\epsilon}$ possibilities, since $x_3 \neq y_3$ and $x_3' \neq y_3'$.

Thus the number of solutions of (79) to (82) with $X = X'$ is

$$\ll P^{\frac{4}{5}(2+\epsilon)+1+\frac{2}{5}+\frac{8}{5}+\epsilon} \ll P^{\frac{23}{5}+2\epsilon}.$$

Consider now solutions of (79) to (82) with $X \neq X'$. Here the values of x_2, y_2, x_2', y_2' determine those of X, X', T with $\ll P^{\epsilon}$ possibilities, since they determine the value of

$$\Delta_T(X'^3) - \Delta_T(X^3) = 3T(X'-X)(X'+X+T),$$

and none of the three factors is 0. Then x_1, y_1 are determined by (79) with $\ll P^{\epsilon}$ possibilities, since $x_1 \neq y_1$, and finally the values of x_4, y_4 determine those of x_3, y_3, x_3', y_3' with $\ll P^{\epsilon}$ possibilities from (81), (82), since $x_3 \neq y_3$ and $x_3' \neq y_3'$. Thus the number of solutions of the type under consideration is $\ll (P^{\frac{4}{5}})^{6+\epsilon}$.

We now have
$$S_1 \ll P^{\frac{24}{5}+\epsilon}.$$

Substitution in (78) gives
$$S^2 \ll P^{\frac{18}{5}+\frac{24}{5}+\epsilon},$$

whence
$$S \ll P^{\frac{21}{5}+\epsilon}.$$

Hence the number of solutions of (70) and (71) with $x = y$, $X \neq Y$ is

$$\ll P^{5+\epsilon} + PS \ll P^{\frac{26}{5}+\epsilon}.$$

This proves lemma 21.

Lemma 22. *The number of solutions of* (70), *subject to* (71), *with* $x \neq y$ *and* $X \neq Y$ *is* $\ll P^{\frac{26}{5}+\epsilon}$.

Proof. We put $y = x+t$, $Y = X+T$ and rewrite (70) as

$$a\Delta_t(x^3) + a_1 y_1^3 + a_3 y_3^3 + a_4 y_4^3 = a_1 x_1^3 + a_3 x_3^3 + a_4 x_4^3, \tag{83}$$

$$b\Delta_T(X^3) + b_2 y_2^3 + ka_3 y_3^3 + ka_4 y_4^3 = b_2 x_2^3 + ka_3 x_3^3 + ka_4 x_4^3. \tag{84}$$

As in the proof of the preceding lemma, we have

$$0 < |t| \ll P^{\frac{2}{5}}, \quad 0 < |T| \ll P^{\frac{2}{5}}.$$

Let S denote the number of solutions of (83), (84) in all the variables.

Let $R(\alpha, \beta)$ denote the number of representations of α, β by the right hand sides of (83), (84) and let $S(t, T, \alpha, \beta)$ denote the number of representations of α, β by the left hand sides when t, T have particular values. Then

$$S = \sum_{t, T, \alpha, \beta} R(\alpha, \beta)\, S(t, T, \alpha, \beta).$$

Hence
$$S^2 \leqslant \{\sum_{t, T, \alpha, \beta} R^2(\alpha, \beta)\}\{\sum_{t, T, \alpha, \beta} S^2(t, T, \alpha, \beta)\} \ll \{P^{\frac{4}{5}} \sum_{\alpha, \beta} R^2(\alpha, \beta)\}\{S_1\}, \tag{85}$$
say.

We first estimate $\Sigma R^2(\alpha, \beta)$. This is the number of solutions of

$$a_1 x_1^3 + a_3 x_3^3 + a_4 x_4^3 = a_1 x_1'^3 + a_3 x_3'^3 + a_4 x_4'^3,$$

$$b_2 x_2^3 + ka_3 x_3^3 + ka_4 x_4^3 = b_2 x_2'^3 + ka_3 x_3'^3 + ka_4 x_4'^3.$$

These imply that
$$ka_1 x_1^3 - b_2 x_2^3 = ka_1 x_1'^3 - b_2 x_2'^3.$$

This equation has $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions, and when the variables in this equation have given values, the equation

$$a_3 x_3^3 + a_4 x_4^3 - a_3 x_3'^3 - a_4 x_4'^3 = a_1(x_1'^3 - x_1^3)$$

has $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions in x_3, x_4, x_3', x_4'. Hence

$$\sum_{\alpha,\beta} R^2(\alpha,\beta) \ll P^{\frac{16}{5}+\epsilon}.$$

Thus (85) becomes $$S^2 \ll \{P^{4+\epsilon}\}\{S_1\}. \tag{86}$$

Here S_1 denotes the number of solutions of the system

$$a\Delta_t(x^3) + a_1 y_1^3 + a_3 y_3^3 + a_4 y_4^3 = \alpha, \tag{87}$$

$$a\Delta_t(x'^3) + a_1 y_1'^3 + a_3 y_3'^3 + a_4 y_4'^3 = \alpha, \tag{88}$$

$$b\Delta_T(X^3) + b_2 y_2^3 + ka_3 y_3^3 + ka_4 y_4^3 = \beta, \tag{89}$$

$$b\Delta_T(X'^3) + b_2 y_2'^3 + ka_3 y_3'^3 + ka_4 y_4'^3 = \beta \tag{90}$$

in all the variables.

(I) *Consider first solutions of* (87) *to* (90) *with* $x = x'$ *and* $X = X'$. Here we have

$$a_1 y_1'^3 + a_3 y_3'^3 + a_4 y_4'^3 = a_1 y_1^3 + a_3 y_3^3 + a_4 y_4^3, \tag{91}$$

$$b_2 y_2'^3 + ka_3 y_3'^3 + ka_4 y_4'^3 = b_2 y_2^3 + ka_3 y_3^3 + ka_4 y_4^3. \tag{92}$$

If $a_3 y_3'^3 + a_4 y_4'^3 = a_3 y_3^3 + a_4 y_4^3$, then $y_1'^3 = y_1^3$ and $y_2'^3 = y_2^3$. The number of possibilities for all the variables in (91), (92) is $\ll P^{4(\frac{4}{5})+\epsilon}$. In addition the number of possibilities for x, X, t, T is $\ll P^{2+2(\frac{2}{5})}$. This gives $\ll P^{6+\epsilon}$ solutions of (87) to (90).

If $a_3 y_3'^3 + a_4 y_4'^3 \neq a_3 y_3^3 + a_4 y_4^3$, then the values of y_3', y_4', y_3, y_4 in (91) and (92) determine y_1', y_1 with $\ll P^{\epsilon}$ possibilities and similarly y_2', y_2. This again gives $\ll P^{4(\frac{4}{5})+\epsilon}$ solutions of (91), (92), with the same conclusion as before.

(II) *Consider next solutions of* (87) *to* (90) *with* $x = x'$ *and* $X \neq X'$. (This covers also the possibility $x \neq x'$ and $X = X'$.) We choose $y_2, y_3, y_4, y_2', y_3', y_4'$ arbitrarily. This determines T, X, X' with $\ll P^{\epsilon}$ possibilities, on subtracting (89), (90). Further, on subtracting (87), (88) we have y_1, y_1' determined with $\ll P^{\epsilon}$ possibilities. Finally, there are $\ll P^{1+\frac{2}{5}}$ possibilities for t, x, x'. Thus we get $\ll P^{\frac{31}{5}+\epsilon}$ solutions for (87) to (90).

(III) *Consider finally solutions of* (87) *to* (90) *with* $x \neq x'$ *and* $X \neq X'$. We choose all the eight variables $y_1, y_2, y_3, y_4, y_1', y_2', y_3', y_4'$ arbitrarily, and then t, x, x', T, X, X' are determined with $\ll P^{\epsilon}$ possibilities. This gives $\ll P^{\frac{32}{5}+\epsilon}$ solutions for (87) to (90).

We can now say that $S_1 \ll P^{\frac{32}{5}+\epsilon}$, and (86) gives

$$S^2 \ll P^{4+\epsilon} P^{\frac{32}{5}+\epsilon},$$

whence $$S \ll P^{\frac{26}{5}+\epsilon}.$$

This proves lemma 22.

LEMMA 23. *The number of solutions of* (72), *subject to* (71), *with* $x = y$ *and* $X = Y$ *is* $\ll P^{\frac{26}{5}+\epsilon}$.

Proof. There are $\ll P^2$ possibilities for x, y, X, Y, and the remaining variables satisfy

$$a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 + a_4 x_4^3 = a_1 y_1^3 + a_2 y_2^3 + a_3 y_3^3 + a_4 y_4^3, \tag{93}$$

$$b_1 x_1^3 + b_2 x_2^3 + ka_3 x_3^3 + ka_4 x_4^3 = b_1 y_1^3 + b_2 y_2^3 + ka_3 y_3^3 + ka_4 y_4^3, \tag{94}$$

where the ratios $a_1/b_1, a_2/b_2, 1/k$ are distinct. The second equation can be replaced by

$$(ka_1-b_1)\,x_1^3+(ka_2-b_2)\,x_2^3 = (ka_1-b_1)\,y_1^3+(ka_2-b_2)\,y_2^3. \tag{95}$$

This has $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions in x_1, y_1, x_2, y_2, and when these are fixed, the equation (93) has $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions in x_3, y_3, x_4, y_4. Thus we obtain

$$\ll P^{2+\frac{4}{5}(4+\epsilon)} \ll P^{\frac{26}{5}+\epsilon}$$

solutions of (72).

Lemma 24. *The number of solutions of* (72) *subject to* (71), *with* $x = y$ *and* $X \neq Y$, *is* $\ll P^{\frac{26}{5}+\epsilon}$.

Proof. There are $\ll P$ choices for x, y. We have

$$a_1 x_1^3+a_2 x_2^3+a_3 x_3^3+a_4 x_4^3 = a_1 y_1^3+a_2 y_2^3+a_3 y_3^3+a_4 y_4^3. \tag{96}$$

The number of solutions of this equation, subject to (71), is

$$\int_0^1 |U(a_1\alpha)\; U(a_2\alpha)\; U(a_3\alpha)\; U(a_4\alpha)|^2\,\mathrm{d}\alpha.$$

By repeated use of Cauchy's inequality this can be majorized by

$$\int_0^1 |U(\alpha)|^8\,\mathrm{d}\alpha.$$

By the result of Hua (1938), this is $\ll (P^{\frac{4}{5}})^{5+\epsilon}$. Then X, Y are determined with $\ll P^{\epsilon}$ possibilities. Thus there are $\ll P^{4+\epsilon}$ solutions of (96) and therefore $\ll P^{5+\epsilon}$ solutions of (72) of the type under consideration.

Lemma 25. *The number of solutions of* (72), *subject to* (71), *with* $x \neq y$ *and* $X \neq Y$ *is* $\ll P^{\frac{26}{5}+\epsilon}$.

Proof. We proceed as in the proof of lemma 22, though now all four of the variables x_i and all four of the variables y_i occur in the equations analogous to (83), (84).

In the present case, $\Sigma R^2(\alpha,\beta)$ represents the number of solutions of

$$a_1 x_1^3+a_2 x_2^3+a_3 x_3^3+a_4 x_4^3 = a_1 x_1'^3+a_2 x_2'^3+a_3 x_3'^3+a_4 x_4'^3,$$

$$b_1 x_1^3+b_2 x_2^3+ka_3 x_3^3+ka_4 x_4^3 = b_1 x_1'^3+b_2 x_2'^3+ka_3 x_3'^3+ka_4 x_4'^3.$$

By eliminating x_3, x_4, x_3', x_4' we get an equation with $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ solutions in x_1, x_2, x_1', x_2', and then one of the above equations leaves $\ll (P^{\frac{4}{5}})^{2+\epsilon}$ possibilities for x_3, x_4, x_3', x_4'. Hence

$$\Sigma R^2(\alpha,\beta) \ll P^{\frac{16}{5}+\epsilon}$$

as before, and so (86) remains valid.

Now S_1 denotes the number of solutions of the system

$$a\Delta_t(x^3)+a_1 y_1^3+a_2 y_2^3+a_3 y_3^3+a_4 y_4^3 = \alpha, \tag{97}$$

$$a\Delta_t(x'^3)+a_1 y_1'^3+a_2 y_2'^3+a_3 y_3'^3+a_4 y_4'^3 = \alpha, \tag{98}$$

$$b\Delta_T(X^3)+b_1 y_1^3+b_2 y_2^3+ka_3 y_3^3+ka_4 y_4^3 = \beta, \tag{99}$$

$$b\Delta_T(X'^3)+b_1 y_1'^3+b_2 y_2'^3+ka_3 y_3'^3+ka_4 y_4'^3 = \beta. \tag{100}$$

(I) *Consider first solutions with* $x = x'$ *and* $X = X'$. By the same argument as in the estimation of $\Sigma R^2(\alpha,\beta)$ above, applied to the equations obtained by subtracting (97), (98) and

(99), (100), there are $\ll P^{\frac{16}{5}+\epsilon}$ possibilities for $y_1, y_2, y_3, y_4, y_1', y_2', y_3', y_4'$. There are also $\ll P^{2+2(\frac{2}{5})}$ possibilities for x, x', X, X', t, T. This gives a contribution to S_1 that is $\ll P^{6+\epsilon}$.

(II) *Consider next solutions with* $x = x'$ *and* $X \neq X'$. The equation obtained by subtracting (97), (98) has $\ll (P^{\frac{4}{5}})^{5+\epsilon}$ solutions in $y_1, \ldots, y_4, y_1', \ldots, y_4'$, by the same application of Hua's theorem as above. Then (99), (100) give $\ll P^{\epsilon}$ possibilities for T, X, X'. There are also $\ll P^{1+\frac{2}{5}}$ possibilities for t, x. Thus we get a contribution to S_1 that is $\ll P^{\frac{27}{5}+\epsilon}$.

(III) *Consider finally solutions with* $x \neq x'$ *and* $X \neq X'$. As in the proof of lemma 22, the number of such solutions is $\ll P^{\frac{32}{5}+\epsilon}$.

Thus we can take $S_1 \ll P^{\frac{32}{5}+\epsilon}$ in (86), and this gives $S \ll P^{\frac{26}{5}+\epsilon}$ as before.

Proof of lemma 19. This follows, by virtue of the preliminary remarks, from lemmas 20 to 22 in case (i) and from lemmas 23 to 25 in case (ii).

8. Allocation of variables and treatment of the minor arcs

In this section we estimate the contribution made by the minor arcs $\mathfrak{m}$ to the integral (62) for $\mathcal{N}(P)$. As explained in § 6, this estimation is based on the expression (65); but we have first to decide upon a permutation of the 18 variables before allotting them in order to the ranges (59) and (60), and so to the corresponding exponential sums (57), (58).

Lemma 26. *The* 18 *suffixes can be divided into three sets in such a way that within each set the same ratio* a_i/b_i *occurs at most twice.*

Proof. Let the sets of suffices giving equal ratios comprise $l_1, l_2, \ldots, l_\nu$ suffixes, where

$$6 \geqslant l_1 \geqslant l_2 \geqslant \ldots \geqslant l_\nu \geqslant 1, \quad l_1 + l_2 + \ldots + l_\nu = 18.$$

We describe the sets of suffices for convenience as blocks, and call l_i the length of the ith block.

We form a set of six suffixes by taking two from the first block (provided $l_1 \geqslant 2$) and two from the second block (provided $l_2 \geqslant 2$) and so on, making the total up to six by using blocks of length 1 as necessary. This is plainly possible, and in this set of six suffixes the same ratio a_i/b_i can occur at most twice.

There remain twelve suffices. We divide these again into blocks of suffixes with the same value of a_i/b_i. If $l_1', l_2', \ldots, l_\mu'$ are the lengths of the blocks, then

$$4 \geqslant l_1' \geqslant l_2' \geqslant \ldots \geqslant l_\mu' \geqslant 1, \quad l_1' + l_2' + \ldots + l_\mu' = 12.$$

The fact that $l_1' \leqslant 4$ follows from the fact that at most three of the original blocks can have length $\geqslant 5$, and every such block has lost two elements.

We distinguish two possibilities. If $\mu = 4$ and $l_1' = l_2' = l_3' = l_4' = 3$, we take two from the first block, two from the second block, one from the third block and one from the fourth block, to constitute the second set of six. The remainder form the third set of six. Each of these sets has the desired property that, for the suffixes in the set, the same ratio a_i/b_i occurs at most twice.

In any other case, there are at most three blocks satisfying $l_i' \geqslant 3$. We repeat the original operation, taking two suffixes from the longest block, and so on. This produces a second set with the desired property, and for the six remaining suffices the length of each block is $\leqslant 2$, so that this set also has the desired property.

This proves the result.

LEMMA 27. *By a suitable permutation of the eighteen suffixes we can ensure that*

(i) *no ratio occurs more than twice among* $a_1/b_1, \ldots, a_6/b_6$;

(ii) *the suffixes* 7, 8, 11, 12, 13, 14 *satisfy the requirements of lemma* 19;

(iii) *the suffixes* 9, 10, 15, 16, 17, 18 *also satisfy* (mutatis mutandis) *the requirements of lemma* 19.

Proof. We take one of the three sets of suffixes constructed in lemma 26 as 1, …, 6. Thus (i) is satisfied.

Each of the other sets of six has ratios a_i/b_i which fall into one or other of the following four types:

$$A,\quad A,\quad B,\quad B,\quad C,\quad C;$$
$$A,\quad A,\quad B,\quad B,\quad C,\quad D;$$
$$A,\quad A,\quad B,\quad C,\quad D,\quad E;$$
$$A,\quad B,\quad C,\quad D,\quad E,\quad F;$$

where it is understood that different letters denote different ratios. We renumber the corresponding suffixes as

$$7,\quad 11,\quad 8,\quad 12,\quad 13,\quad 14$$

in the first two cases, and as $13,\quad 14,\quad 11,\quad 12,\quad 7,\quad 8$

in the last two cases. Then the set of suffixes 7, 8, 11, 12, 13, 14 satisfies (i) of lemma 19 in the first two cases and (ii) of lemma 19 in the last two cases.

Similarly, we renumber the suffixes of the third set as 9, 10, 15, 16, 17, 18, and this set again satisfies (i) or (ii) of lemma 19 with 9, 10 in place of 7, 8 and 15 to 18 in place of 11 to 14.

LEMMA 28. *After the permutation of lemma* 27 *we have*

$$\int_0^1\int_0^1 |T_7(\gamma_7)\ldots T_{10}(\gamma_{10})\, U(\gamma_{11})\ldots U(\gamma_{18})|\,\mathrm{d}\alpha\,\mathrm{d}\alpha' \ll P^{\frac{26}{5}+\epsilon}. \tag{101}$$

Proof. Since the suffices 7, 8, 11, 12, 13, 14 satisfy the requirements of lemma 19, it follows from that lemma that

$$\int_0^1\int_0^1 |T_7(\gamma_7)\, T_8(\gamma_8)\, U(\gamma_{11})\, U(\gamma_{12})\, U(\gamma_{13})\, U(\gamma_{14})|^2\,\mathrm{d}\alpha\,\mathrm{d}\alpha' \ll P^{\frac{26}{5}+\epsilon}.$$

Similarly $$\int_0^1\int_0^1 |T_9(\gamma_9)\, T_{10}(\gamma_{10})\, U(\gamma_{15})\, U(\gamma_{16})\, U(\gamma_{17})\, U(\gamma_{18})|^2\,\mathrm{d}\alpha\,\mathrm{d}\alpha' \ll P^{\frac{26}{5}+\epsilon}.$$

Now (101) follows by Cauchy's inequality.

LEMMA 29. *Suppose that, for some i with* $1 \leqslant i \leqslant 6$,

$$|T_i(\gamma_i)| = P^{1-\theta}, \tag{102}$$

where $$\theta \leqslant \tfrac{1}{4}-2\delta. \tag{103}$$

Then γ_i has a rational approximation A/Q satisfying

$$1 \leqslant Q \ll P^{3\theta}, \quad \left|\gamma_i - \frac{A}{Q}\right| \ll \frac{1}{Q^{\frac{1}{3}}P^{3-\theta}}. \tag{104}$$

Proof. By Dirichlet's theorem on Diophantine approximation, there exists a rational approximation A/Q to γ_i such that

$$1 \leqslant Q \leqslant P^{2+\delta}, \quad \left|\gamma_i - \frac{A}{Q}\right| < \frac{1}{QP^{2+\delta}}.$$

Write $\beta = \gamma_i - A/Q$.

If $Q > P^{1-\delta}$ we appeal to lemma 13 of Davenport (1939), which is essentially Weyl's inequality. (It related to a sum extended over $P < x < 2P$ instead of over $\kappa_i P < x < \kappa_i' P$, but that is of no significance.) This gives

$$|T_i(\gamma_i)| \ll P^{\frac{3}{4}+\delta},$$

which is contrary to (102) and (103). Hence $Q \leqslant P^{1-\delta}$.

We now appeal to lemma 9 of Davenport (1939), which asserts that

$$|T_i(\gamma_i)| \ll Q^{-\frac{1}{3}} \min(P, P^{-2}|\beta|^{-1}).$$

Comparing this with (102) we obtain

$$P^{1-\theta} \ll Q^{-\frac{1}{3}}P, \quad P^{1-\theta} \ll Q^{-\frac{1}{3}}P^{-2}|\beta|^{-1},$$

and these lead to the conclusions (104).

Lemma 30. *Suppose that (α, α') is in $\mathfrak{m}$. Let i, j be two of the suffixes $1, \ldots, 6$ for which*

$$a_i b_j - a_j b_i \neq 0. \tag{105}$$

Then either
$$|T_i(\gamma_i)| < P^{\frac{3}{4}+2\delta}, \tag{106}$$

or
$$|T_j(\gamma_j)| < P^{\frac{3}{4}+2\delta}, \tag{107}$$

or
$$|T_i(\gamma_i)\, T_j(\gamma_j)| < P^{\frac{5}{3}+\delta}. \tag{108}$$

Proof. Suppose that (106) and (107) are false. Then, if

$$|T_i(\gamma_i)| = P^{1-\theta_i}, \quad |T_j(\gamma_j)| = P^{1-\theta_j},$$

both θ_i and θ_j satisfy the condition (103) of lemma 29. By that lemma there exist rational approximations A_i/Q_i and A_j/Q_j to γ_i and γ_j respectively such that

$$1 \leqslant Q_i \ll P^{3\theta_i}, \quad \left|\gamma_i - \frac{A_i}{Q_i}\right| \ll \frac{1}{Q_i^{\frac{1}{3}}P^{3-\theta_i}},$$

$$1 \leqslant Q_j \ll P^{3\theta_j}, \quad \left|\gamma_j - \frac{A_j}{Q_j}\right| \ll \frac{1}{Q_j^{\frac{1}{3}}P^{3-\theta_j}}.$$

By (61)
$$(a_i b_j - a_j b_i)\,\alpha = b_j \gamma_i - b_i \gamma_j,$$

with a similar equation for α'. Hence α, α' have simultaneous approximations B/R, B'/R with $(B, B', R) = 1$ and
$$R \mid (a_i b_j - a_j b_i)\, Q_i Q_j.$$

Hence
$$R \ll P^{3\theta_i + 3\theta_j}. \tag{109}$$

Also
$$|\alpha-B/R| \ll |\gamma_i-A_i/Q_i|+|\gamma_j-A_j/Q_j|$$
$$\ll Q_i^{-\frac{1}{3}}P^{-3+\theta_i}+Q_j^{-\frac{1}{3}}P^{-3+\theta_j}$$
$$\ll R^{-1}(Q_i^{\frac{2}{3}}Q_j P^{-3+\theta_i}+Q_i Q_j^{\frac{2}{3}} P^{-3+\theta_j})$$
$$\ll R^{-1}P^{-3+3\theta_i+3\theta_j}. \tag{110}$$

The same estimate holds for $|\alpha'-B'/R|$.

If $3(\theta_i+\theta_j) \leqslant 1-2\delta$ then (109) and (110) imply that (α, α') is on the major arc $\mathfrak{M}\,(B, B'; R)$ defined by (63), (64). This contradicts the hypothesis that (α, α') is in $\mathfrak{m}$. Hence
$$\theta_i+\theta_j > \tfrac{1}{3}(1-2\delta),$$
whence
$$|T_i(\gamma_i)\, T_j(\gamma_j)| = P^{2-\theta_i-\theta_j} < P^{\frac{5}{3}+\delta}.$$
This proves (108).

Lemma 31. *For (α, α') in $\mathfrak{m}$ we have*
$$\prod_{j=1}^{6} |T_j(\gamma_j)| \ll P^{5+8\delta}. \tag{111}$$

Proof. Of the six suffixes, let i be one for which $|T_i(\gamma_i)|$ is maximal. If
$$|T_i(\gamma_i)| = P^{1-\theta}$$
then we can suppose that $\theta \leqslant \frac{1}{6}$, for otherwise
$$\prod_{j=1}^{6} |T_j(\gamma_j)| \leqslant |T_i(\gamma_i)|^6 < P^5.$$

Since at most one of the five suffixes j other than i can satisfy $a_i/b_i = a_j/b_j$, we must have at least four suffixes j for which $a_i/b_i \neq a_j/b_j$. By lemma 30, for each such j we have either
$$|T_j(\gamma_j)| < P^{\frac{3}{4}+2\delta},$$
or
$$|T_j(\gamma_j)| < P^{\frac{5}{3}+\delta-(1-\theta)}.$$
Hence
$$\prod_{k=1}^{6} |T_k(\gamma_k)| < P^{2(1-\theta)+4\phi+8\delta},$$
where
$$\phi = \max\left(\tfrac{3}{4}, \tfrac{2}{3}+\theta\right).$$
If $\theta \leqslant \frac{1}{12}$ we have
$$2(1-\theta)+4\phi = 2(1-\theta)+3 \leqslant 5,$$
and if $\frac{1}{12} \leqslant \theta \leqslant \frac{1}{6}$ we have
$$2(1-\theta)+4\phi = 2(1-\theta)+4(\tfrac{2}{3}+\theta)$$
$$= \tfrac{14}{3}+2\theta \leqslant 5.$$
Thus (111) is established.

Lemma 32. *The contribution of all (α, α') in $\mathfrak{m}$ to the integral (62) for $\mathcal{N}(P)$ is $\ll P^{\frac{51}{5}+9\delta}$.*

Proof. The result follows from lemmas 28 and 31, in view of the estimate (65).

9. Treatment of the major arcs

In this section we investigate the contribution made by the major arcs $\mathfrak{M}(B, B'; R)$, defined by (63), (64), to the integral (62) for $\mathcal{N}(P)$. We shall obtain a main term, which will be ultimately shown to be $\gg P^{\frac{52}{5}}$, and various error terms which are $o(P^{\frac{52}{5}})$.

We shall first prove (lemma 37) that the contribution made by all the major arcs with $R > P^{9\delta}$ can be absorbed in the error term.

Lemma 33. *If* (α, α') *is in* $\mathfrak{M}(B, B'; R)$ *then*

$$|T_i(\gamma_i)| \ll R_i^{-\frac{1}{3}} \min(P, P^{-2}|\beta_i|^{-1}) \tag{112}$$

for $i = 1, \ldots, 10$, *where*

$$R_i = R_i(B, B') = \frac{R}{(R, a_i B + b_i B')}, \tag{113}$$

$$\beta_i = a_i(\alpha - B/R) + b_i(\alpha' - B'/R) = a_i\beta + b_i\beta'. \tag{114}$$

Proof. By (61), (63), (113), (114) we have

$$\gamma_i = a_i\alpha + b_i\alpha' = C_i/R_i + \beta_i, \quad C_i/R_i = \frac{a_i B + b_i B'}{R},$$

so that $(C_i, R_i) = 1$. Also

$$R_i \leqslant R \leqslant P^{1-\delta}$$

by (113), (64); and

$$|\beta_i| \ll |\alpha - B/R| + |\alpha' - B'/R|$$
$$\ll R^{-1}P^{-2-\delta} \ll (R_i)^{-1}P^{-2-\delta},$$

by (114), (63), (113). The result now follows from lemma 9 of Davenport (1939); the fact that our present inequality for β_i contains an unspecified constant is of no significance.

Lemma 34. *If* (α, α') *is in* $\mathfrak{M}(B, B'; R)$ *then*

$$|U(\gamma_i)| \ll R_i^{-\frac{1}{5}} P^{\frac{4}{5}+\delta} \quad (i = 11, \ldots, 18). \tag{115}$$

Proof. Suppose first that $R_i > P^{\frac{4}{5}(1-\delta)}$. Then by lemma 14 of Davenport (1939) [where T_1 is our U], we have

$$|U(\gamma_i)| \ll P^{\frac{4}{5}(\frac{3}{4}+\delta)}.$$

Since $R_i \leqslant R \leqslant P^{1-\delta}$, this implies (115).

Suppose next that $R_i \leqslant P^{\frac{4}{5}(1-\delta)}$. By lemma 10 of Davenport (1939) we have

$$|U(\gamma_i)| \ll R_i^{-\frac{1}{3}} P^{\frac{4}{5}}.$$

This again implies (115).

Lemma 35. *We have*

$$\sum_{B, B'} (R_1 \ldots R_{10})^{-\frac{1}{3}} (R_{11} \ldots R_{18})^{-\frac{1}{5}} \ll R^{-2+\frac{1}{15}+\epsilon}, \tag{116}$$

$$\sum_{B, B'} (R_1 \ldots R_{18})^{-\frac{1}{3}} \ll R^{-3+\epsilon}, \tag{117}$$

where in each case the summation is over

$$1 \leqslant B \leqslant R, \quad 1 \leqslant B' \leqslant R, \quad (B, B', R) = 1.$$

Proof. We collect together the blocks of equal ratios among a_i/b_i $(i = 1, \ldots, 18)$; each block contains at most 6, so there are at least 3 blocks. If $a_i/b_i = a_j/b_j$ then R_i/R_j lies

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

between two positive constants, by (113). Thus if $i_1, \ldots, i_\nu$ is a representative set of suffixes, one from each block, then

$$(R_1 \ldots R_{10})^{-\frac{1}{3}} (R_{11} \ldots R_{18})^{-\frac{1}{5}} \ll R_{i_1}^{-\theta_1} \ldots R_{i_\nu}^{-\theta_\nu}, \tag{118}$$

where $\frac{1}{5} \leqslant \theta_j \leqslant 2$ $(j = 1, \ldots, \nu)$ and

$$\theta_1 + \ldots + \theta_\nu = \tfrac{10}{3} + \tfrac{8}{5} = 5 - \tfrac{1}{15}. \tag{119}$$

Let $u_j = (R, a_{i_j} B + b_{i_j} B')$ for $j = 1, \ldots, \nu$, so that $u_j | R$ and

$$R_{i_j} = R/u_j \tag{120}$$

by (113). We have $a_{i_j}/b_{i_j} \neq a_{i_k}/b_{i_k}$ if $j \neq k$. If $\delta = (u_j, u_k)$ then

$$a_{i_j} B + b_{i_j} B' \equiv 0 \pmod{\delta},$$

$$a_{i_k} B + b_{i_k} B' \equiv 0 \pmod{\delta},$$

whence
$$(a_{i_j} b_{i_k} - a_{i_k} b_{i_j})\, B \equiv 0 \pmod{\delta},$$

and similary for B'. Since $(B, B', R) = 1$, and $\delta | R$, it follows that

$$\delta | a_{i_j} b_{i_k} - a_{i_k} b_{i_j}.$$

Thus (u_j, u_k) divides a fixed non-zero number for all j, k with $j \neq k$. It follows that

$$u_1 u_2 \ldots u_\nu | KR, \tag{121}$$

where K is fixed and non-zero.

We now estimate the number of pairs B, B' in the sum (116) for which $u_1, \ldots, u_\nu$ have particular values. We have

$$a_{i_j} B + b_{i_j} B' = u_j x_j \quad (j = 1, \ldots, \nu), \tag{122}$$

and any two of these equations in B, B' have their left hand sides linearly independent. Since $\nu \geqslant 3$, we can regard $x_3, \ldots, x_\nu$ as functions of x_1, x_2, and we note that x_1, x_2 determine B, B' uniquely (since $u_1, \ldots, u_\nu$ are fixed for the moment). Plainly

$$|x_1| \ll \frac{R}{u_1}, \quad |x_2| \ll \frac{R}{u_2},$$

since $1 \leqslant B \leqslant R$, $1 \leqslant B' \leqslant R$.

The first two of the equations (122), together with the jth equation $(j \geqslant 3)$ imply a linear relation of the form

$$c_1^{(j)} u_1 x_1 + c_2^{(j)} u_2 x_2 + c^{(j)} u_j x_j = 0,$$

where
$$c_1^{(j)} = a_{i_2} b_{i_j} - a_{i_j} b_{i_2}, \quad c_2^{(j)} = a_{i_j} b_{i_1} - a_{i_1} b_{i_j}, \quad c^{(j)} = a_{i_1} b_{i_2} - a_{i_2} b_{i_1},$$

so that none of $c_1^{(j)}$, $c_2^{(j)}$, $c^{(j)}$ is 0. This gives a congruence to the modulus u_j which must be satisfied by x_1, x_2, namely

$$c_1^{(j)} u_1 x_1 + c_2^{(j)} u_2 x_2 \equiv 0 \pmod{u_j} \quad (j = 3, \ldots, \nu).$$

The moduli $u_3, \ldots, u_\nu$ of these congruences have only bounded common factors when taken in pairs, and have only bounded common factors with u_1, u_2. Hence, for given x_1, the value of x_2 is determined mod $u_3 \dots u_\nu$ with only a bounded number of possibilities. Recalling that $u_1 u_2 u_3 \dots u_\nu \ll R$ by (121), we deduce that the number of possibilities for x_2, for given x_1, is

$$\ll \frac{R}{u_2} \frac{1}{u_3 \dots u_\nu}.$$

Hence the number of possibilities for x_1, x_2, and so for B, B', is

$$\ll \frac{R^2}{u_1 u_2 \dots u_\nu}.$$

By (118) and (120) the sum in (116) is

$$\ll \sum_{\substack{u_1, \dots, u_\nu \\ (121)}} (R/u_1)^{-\theta_1} \dots (R/u_\nu)^{-\theta_\nu} \frac{R^2}{u_1 u_2 \dots u_\nu}$$

$$\ll R^{2-\theta_1-\dots-\theta_\nu} \sum_{\substack{u_1, \dots, u_\nu \\ (121)}} u_1^{\theta_1-1} u_2^{\theta_2-1} \dots u_\nu^{\theta_\nu-1}.$$

By (119) and the fact that $\theta_j \leqslant 2$, this is

$$\ll R^{-3+\frac{1}{16}} \sum_{\substack{u_1, \dots, u_\nu \\ (121)}} u_1 u_2 \dots u_\nu$$

$$\ll R^{-2+\frac{1}{16}+\epsilon}.$$

This proves (116). The proof of (117) is similar, the only difference being that (119) is replaced by

$$\theta_1 + \dots + \theta_\nu = 6.$$

LEMMA 36. *If $\beta_1, \dots, \beta_{10}$ are defined by* (114) *then*

$$\iint_{D(\tau)} \prod_{i=1}^{10} \min (P, P^{-2} |\beta_i|^{-1}) \, d\beta \, d\beta' \ll P^{4-4\tau}, \tag{123}$$

where $\tau \geqslant 0$ and $D(\tau)$ denotes the region in the (β, β') plane defined by

$$\max (|\beta|, |\beta'|) > P^{-3+\tau}. \tag{124}$$

Proof. We have, by (114),

$$\beta_i = a_i \beta + b_i \beta', \tag{125}$$

where

$$\beta = \alpha - B/R, \quad \beta' = \alpha' - B'/R.$$

It will suffice to consider the part of $D(\tau)$ for which $|\beta| \geqslant |\beta'|$, and then the range of integration for β' when β is given is $\ll |\beta|$.

If $a_i/b_i \neq a_j/b_j$, the equations (125) imply, on solving two of them, that

$$|\beta| \ll |\beta_i| + |\beta_j|. \tag{126}$$

We know that not more than four of the ratios

$$a_1/b_1, \dots, a_{10}/b_{10} \tag{127}$$

can be equal, for by lemma 27 not more than two of the first six are equal and

$$a_7/b_7 \neq a_8/b_8, \quad a_9/b_9 \neq a_{10}/b_{10}.$$

We divide the ratios (127) into blocks of equal ones, of lengths (say) $l_1, \ldots, l_\nu$, where

$$4 \geqslant l_1 \geqslant l_2 \geqslant \ldots \geqslant l_\nu \geqslant 1, \quad l_1 + \ldots + l_\nu = 10.$$

If i, j are suffixes from different blocks, (126) tells us that either $|\beta_i| \gg |\beta|$ or $|\beta_j| \gg |\beta|$. Hence $|\beta_i| \gg |\beta|$ for all i except possibly those in one particular block, and therefore

$$\prod_{i=1}^{10} \min(P, P^{-2}|\beta_i|^{-1}) \ll P^{l_1}(P^{-2}|\beta|^{-1})^{l_2+\ldots+l_\nu}.$$

It follows that the integral in (123) is

$$\begin{aligned} &\ll \int_{P^{-3+\tau}}^{\infty} P^{l_1}(P^{-2}\beta^{-1})^{l_2+\ldots+l_\nu}\beta\, d\beta \\ &\ll P^{l_1-2(l_2+\ldots+l_\nu)}(P^{3-\tau})^{l_2+\ldots+l_\nu-2} \\ &\ll P^{l_1+\ldots+l_\nu-6-\tau(l_2+\ldots+l_\nu-2)} \\ &\ll P^{4-4\tau}, \end{aligned}$$

since $$l_2 + \ldots + l_\nu = 10 - l_1 \geqslant 6.$$

Remark. If $\tau = 0$ the estimate (123) remains valid when the integral is extended over the whole plane, since the contribution of the square $|\beta| < P^{-3}$, $|\beta'| < P^{-3}$ is plainly $\ll P^4$.

It will be convenient to have on record, for use later, the analogous estimate to that just mentioned, when the product is modified by omitting any one factor. There are then still at least three blocks of suffixes, and the only change in the argument is that $l_1 + \ldots + l_\nu = 9$ instead of 10. The result is that

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \Pi' \min(P, P^{-2}|\beta_i|^{-1})\, d\beta\, d\beta' \ll P^3, \tag{128}$$

where Π' denotes a product over any 9 of $i = 1, \ldots, 10$.

LEMMA 37. *The contribution of all major arcs* $\mathfrak{M}(B, B', R)$ *with* $R > P^{9\delta}$ *to the integral* (62) *is*

$$\ll P^{\frac{52}{5}-\frac{1}{3}\delta}.$$

Proof. By lemmas 33 and 34 the contribution is

$$\ll \sum_{R > P^{9\delta}} \sum_{B, B'} \iint_{\mathfrak{M}(B,B',R)} (R_1 \ldots R_{10})^{-\frac{1}{3}} (R_{11} \ldots R_{18})^{-\frac{1}{5}} P^{8(\frac{4}{5}+\delta)} \prod_{i=1}^{10} \min(P, P^{-2}|\beta_i|^{-1})\, d\beta\, d\beta'.$$

By the remark following lemma 36 this is

$$\ll \sum_{R > P^{9\delta}} \sum_{B, B'} (R_1 \ldots R_{10})^{-\frac{1}{3}} (R_{11} \ldots R_{18})^{-\frac{1}{5}} P^{8(\frac{4}{5}+\delta)} P^4.$$

By lemma 35 this is

$$\ll P^{\frac{52}{5}+8\delta} \sum_{R > P^{9\delta}} R^{-2+\frac{1}{15}+\epsilon} \ll P^{\frac{52}{5}+8\delta-9\delta(\frac{14}{15}-\epsilon)} \ll P^{\frac{52}{5}-\frac{1}{3}\delta}.$$

This proves lemma 37.

We now turn to the contribution of the major arcs with $R \leqslant P^{9\delta}$, which provides the main term in the asymptotic formula for $\mathcal{N}(P)$.

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

The first step is to contract the major arcs $\mathfrak{M}(B, B', R)$ to $\mathfrak{M}_0(B, B', R)$, which are defined by replacing $R^{-1}P^{-2-\delta}$ in (63) by $P^{-3+\tau}$. Thus in the present notation $\mathfrak{M}_0(B, B', R)$ is defined by

$$|\beta| < P^{-3+\tau}, \quad |\beta'| < P^{-3+\tau}. \tag{129}$$

Here τ is a small positive constant to be chosen later.

Lemma 38. *The contribution of the major arcs $\mathfrak{M}(B, B', R)$ differs from that of the contracted major arcs $\mathfrak{M}_0(B, B', R)$ by $\ll P^{\frac{52}{5}-4\tau}$.*

Proof. By lemma 33 and the second estimate for $U(\gamma_i)$ used in the proof of lemma 34, the difference between the two contributions, for a particular set B, B', R, is

$$\ll P^{\frac{32}{5}}(R_1 \ldots R_{18})^{-\frac{1}{3}} \iint \prod_{i=1}^{10} \min(P, P^{-2}|\beta_i|^{-1})\, d\beta\, d\beta',$$

where the integral is taken over (124). By lemma 36 this is

$$\ll P^{\frac{52}{5}-4\tau}(R_1 \ldots R_{18})^{-\frac{1}{3}}.$$

Summing over B, B', R and using (117) we obtain the result.

Lemma 39. *For (α, α') in $\mathfrak{M}_0(B, B', R)$ we have*

$$T_i(\gamma_i) = R_i^{-1} S(C_i, R_i)\, I_i(\beta_i) + O(R_i^{\frac{2}{3}+\epsilon}) \tag{130}$$

for $i = 1, \ldots, 10$, where

$$\frac{C_i}{R_i} = \frac{a_i B + b_i B'}{R}, \quad (C_i, R_i) = 1, \tag{131}$$

and where

$$S(a, q) = \sum_{x=1}^{q} e(ax^3/q), \tag{132}$$

$$I_i(\beta) = \int_{\kappa_i P}^{\kappa'_i P} e(\beta\xi^3)\, d\xi = \frac{1}{3}\int_{(\kappa_i P)^3}^{(\kappa'_i P)^3} \eta^{-\frac{2}{3}} e(\beta\eta)\, d\eta. \tag{133}$$

Proof. This result (which is actually valid in $\mathfrak{M}(B, B', R)$ and independently of whether $R \leq P^{9\delta}$ or not) is lemma 7 of Davenport (1939), with only trifling differences. The definition of $I_i(\beta)$ used there had a finite sum in place of the last integral in (133), but the difference between the sum and the integral is $O(1)$.

Lemma 40. *The contribution of all $\mathfrak{M}_0(B, B', R)$ with $R \leq P^{9\delta}$ to the integral in (62) is*

$$\sum_{R \leq P^{9\delta}} \sum_{B, B'} \iint_{\mathfrak{M}_0(B, B', R)} T^*(\beta, \beta')\, U(\gamma_{11}) \ldots U(\gamma_{18})\, d\beta\, d\beta' + O(P^{\frac{48}{5}}), \tag{134}$$

where

$$T^*(\beta, \beta') = \prod_{i=1}^{10} R_i^{-1} S(C_i, R_i)\, I_i(\beta_i). \tag{135}$$

Proof. By lemma 4 of Davenport (1939),

$$|R_i^{-1} S(C_i, R_i)\, I_i(\beta_i)| \ll R_i^{-\frac{1}{3}} \min(P, P^{-2}|\beta_i|^{-1}). \tag{136}$$

[The combination of this with (130) was in fact the underlying justification for the result (112) of lemma 33.] The expression on the right of (136) is always greater than the error term $O(R_i^{\frac{2}{3}+\epsilon})$ in (130), since $R_i \leqslant R \leqslant P^{9\delta}$ and $P^{-2}|\beta_i|^{-1} > P^{1-\tau}$ by (129). Hence the result of multiplying together the ten approximations (130) can be written in the form

$$\left|\prod_{i=1}^{10} T_i(\gamma_i) - T^*(\beta,\beta')\right| \ll R^{\frac{2}{3}+\epsilon}\Pi'\{R_i^{-\frac{1}{3}}\min(P, P^{-2}|\beta_i|^{-1})\},$$

where Π' means that one of $i = 1, \ldots, 10$ is omitted. By (128) integration with respect to β, β' (even over the whole plane) gives

$$\ll R^{\frac{2}{3}+\epsilon}P^3\Pi' R_i^{-\frac{1}{3}} \ll P^3 R^{\frac{2}{3}+\epsilon}.$$

It suffices to multiply this by the trivial estimate $P^{\frac{32}{5}}$ for $|U(\gamma_{11})\ldots U(\gamma_{18})|$ and sum over B, B', R. This gives an amount

$$\ll P^3 P^{\frac{32}{5}} \sum_{R\leqslant P^{9\delta}} \sum_{B,B'} R^{\frac{2}{3}+\epsilon}$$

$$\ll P^{\frac{47}{5}+33\delta+\epsilon} \ll P^{\frac{48}{5}}.$$

Hence lemma 40 is established.

Lemma 41. *The contribution of all* $\mathfrak{M}_0(B, B', R)$ *with* $R \leqslant P^{9\delta}$ *to the integral in* (62) *is*

$$P^{\frac{32}{5}}\mathfrak{S}(P^{9\delta})\, I(P) + O(P^{10}), \tag{137}$$

where
$$\mathfrak{S}(P^{9\delta}) = \sum_{R\leqslant P^{9\delta}} \sum_{B,B'} \prod_{i=1}^{18}\{R_i^{-1}S(C_i, R_i)\}, \tag{138}$$

$$I(P) = \iint_{|\beta|,|\beta'|<P^{-3+\tau}} I_1(\beta_1)\ldots I_{10}(\beta_{10})\,\mathrm{d}\beta\,\mathrm{d}\beta'. \tag{139}$$

Proof. By lemma 8 of Davenport (1939) we have (the obvious analogue of (130)):

$$U(\gamma_i) = R_i^{-1}S(C_i, R_i)\, J(\beta_i) + O(R_i^{\frac{2}{3}+\epsilon}),$$

where
$$J(\beta) = \frac{1}{3}\int_{P^{\frac{12}{5}}}^{8P^{\frac{12}{5}}} \eta^{-\frac{2}{3}} e(\beta\eta)\,\mathrm{d}\eta,$$

corresponding to $I_i(\beta)$ in (133). For $|\beta| \ll P^{-3+\tau}$ we have

$$J(\beta) = \frac{1}{3}\int_{P^{\frac{12}{5}}}^{8P^{\frac{12}{5}}} \eta^{-\frac{2}{3}}\,\mathrm{d}\eta + O(|\beta|\, P^{\frac{16}{5}})$$

$$= P^{\frac{4}{5}} + O(P^{\frac{1}{5}+\tau}).$$

Hence
$$U(\gamma_i) = P^{\frac{4}{5}}R_i^{-1}S(C_i, R_i) + O(P^{\frac{1}{5}+\tau}).$$

It follows that
$$\prod_{i=11}^{18} U(\gamma_i) = P^{\frac{32}{5}}\prod_{i=11}^{18} R_i^{-1}S(C_i, R_i) + O(P^{\frac{29}{5}+\tau}).$$

Substituting this in the integral (134) we obtain the main term in (137), together with an error term. The latter is

$$\ll \sum_{R\leqslant P^{9\delta}} \sum_{B,B'} P^{2(-3+\tau)}P^{10}P^{\frac{29}{5}+\tau},$$

since $|T^*| \ll P^{10}$ and the area of $\mathfrak{M}_0$ (B, B', R) is $\ll P^{2(-3+\tau)}$. This expression is

$$\ll P^{\frac{49}{5}+3\tau+27\delta}.$$

Hence the result, on taking τ and δ sufficiently small.

LEMMA 42. *We have*

$$I(P) \sim CP^4 \tag{140}$$

as $P \to \infty$, *where* C *is a positive constant.*

Proof. Let $I_0(P)$ denote the integral (139) extended over the whole (β, β') plane instead of over $\mathfrak{M}_0(B, B', R)$. Then

$$|I(P) - I_0(P)| \ll \int\int \prod_{i=1}^{10} \min(P, P^{-2}|\beta_i|^{-1})\, d\beta\, d\beta'$$

extended over $\max(|\beta|, |\beta'|) > P^{-3+\tau}$. By lemma 36 we obtain

$$|I(P) - I_0(P)| \ll P^{4-4\tau}.$$

We have

$$I_0(P) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I_1(\beta_1)\dots I_{10}(\beta_{10})\, d\beta\, d\beta'.$$

In the second form for $I_i(\beta_i)$ in (133), we put $\eta = P^3\zeta$, and we also put $\beta = P^{-3}\omega$, $\beta' = P^{-3}\omega'$. Then

$$I_0(P) = 3^{-10}P^{10-6}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(\int_{\mathscr{E}} (\zeta_1\dots\zeta_{10})^{-\frac{2}{3}}\, e(L\omega + L'\omega')\, d\boldsymbol{\zeta}\right) d\omega\, d\omega',$$

where $\mathscr{E}$ is the box defined by

$$\kappa_i^3 < \zeta_i < \kappa_i'^3 \quad (i = 1, \dots, 10)$$

and where

$$L = L(\boldsymbol{\zeta}) = a_1\zeta_1 + \dots + a_{10}\zeta_{10},$$

$$L' = L'(\boldsymbol{\zeta}) = b_1\zeta_1 + \dots + b_{10}\zeta_{10}.$$

The equations $L(\boldsymbol{\zeta}) = L'(\boldsymbol{\zeta}) = 0$ define an 8-dimensional linear space, which passes through the point $(\chi_1, \dots, \chi_{10})$ of (55), which is in the interior of $\mathscr{E}$ by (56). Applying Fourier's integral formula twice to the last integral, in the form

$$\lim_{\lambda\to\infty}\int_{-\lambda}^{\lambda} V(t)\, e(t\omega)\, d\omega = V(0),$$

we obtain

$$I_0(P) = CP^4,$$

where C is a constant given by an 8-dimensional integral, the integrand being positive and the integration being over a positive 8-dimensional volume. This proves (140).

10. Completion of the proof of theorem 2

We have already seen in § 6 that it is legitimate to suppose that no ratio occurs more than six times among the a_i/b_i. The work of §§ 7 and 8, which was based on this supposition, led to lemma 32 which asserts that the contribution of the minor arcs to the integral in (62) is $\ll P^{\frac{51}{5}+9\delta}$. In lemmas 37, 38, 41 of § 9 it was proved that the contribution of the major arcs is given by (137). Hence, by (140),

$$\mathscr{N}(P) = P^{\frac{52}{5}}\mathfrak{S}(P^{9\delta})\{C + o(1)\} + o(P^{\frac{52}{5}}).$$

The series (138) for $\mathfrak{S}(P^{9\delta})$, when continued to infinity, is absolutely convergent by the estimate (117). Hence

$$\mathscr{N}(P) = CP^{\frac{52}{5}}\mathfrak{S} + o(P^{\frac{52}{5}}), \tag{141}$$

where $\mathfrak{S}$ is the 'singular series' defined by

$$\mathfrak{S} = \sum_{R=1}^{\infty} \sum_{B, B'} (R_1 \ldots R_{18})^{-1} S(C_1, R_1) \ldots S(C_{18}, R_{18}). \tag{142}$$

Since
$$\frac{C_i}{R_i} = \frac{a_i B + b_i B'}{R},$$

we have
$$R_i^{-1} S(C_i, R_i) = R^{-1} S(a_i B + b_i B', R).$$

Hence the definition of $\mathfrak{S}$ in (142) can be written in the alternative form

$$\mathfrak{S} = \sum_{R=1}^{\infty} \sum_{B, B'} R^{-18} S(a_1 B + b_1 B', R) \ldots S(a_{18} B + b_{18} B', R).$$

By standard methods, the series can also be expressed as

$$\prod_p \chi_p,$$

where
$$\chi_p = 1 + \sum_{\nu=1}^{\infty} \sum_{\substack{B=1 \\ (B, B', p)=1}}^{p^\nu} \sum_{B'=1}^{p^\nu} (p^\nu)^{-18} S(a_1 B + b_1 B', p^\nu) \ldots S(a_{18} B + b_{18} B', p^\nu).$$

We easily deduce from (117) that for large p

$$|\chi_p - 1| \ll p^{-3+\epsilon}.$$

Hence there exists p_0 such that
$$\prod_{p > p_0} \chi_p \geqslant \tfrac{1}{2}.$$

For a particular $p \leqslant p_0$, it follows from standard arguments that $\chi_p > 0$ provided the equations

$$F = a_1 x_1^3 + \ldots + a_{18} x_{18}^3 = 0,$$
$$G = b_1 x_1^3 + \ldots + b_{18} x_{18}^3 = 0$$

have a non-singular solution in the p-adic field. This is true by the Corollary to Theorem 1 provided that there is no form $\lambda F + \mu G$ (with $\lambda, \mu \neq 0, 0$) which contains explicitly only six or fewer variables. Subject to this condition, we have $\chi_p > 0$ for each $p \leqslant p_0$, whence

$$\mathfrak{S} > 0.$$

The condition is amply satisfied, for as remarked at the beginning of this section, no 7 of the ratios a_i/b_i are equal, and therefore each form of the pencil contains at least 12 variables explicitly. Now (141) shows that

$$\mathcal{N}(P) \to \infty \quad \text{as} \quad P \to \infty,$$

and the solubility of $F = G = 0$ in rational integers follows.

This completes the proof of theorem 2.

11. Appendix on theorems 1A, 2A.

Proof of theorem 1A. Theorem 1A is contained in theorem 2 of Lewis (1957). However, the proof given there related to the more general case in which the rational field is replaced by an algebraic number field, and then there is the complication that the prime 3 may ramify in the field. Hence it may be worth while to outline a simple proof of theorem 1A itself.

As shown in lemma 3 of Davenport & Lewis (1963), with $k = 3$, a diagonal cubic form is equivalent to a form

$$F = F_0 + pF_1 + p^2F_2,$$

where F_i is a diagonal form in m_i variables with all coefficients prime to p, and where the variables in F_0, F_1, F_2 form three disjoint sets. Moreover

$$m_0 \geqslant \tfrac{1}{3}n, \quad m_0 + m_1 \geqslant \tfrac{2}{3}n,$$

so that when $n \geqslant 7$,

$$m_0 \geqslant 3, \quad m_0 + m_1 \geqslant 5.$$

By the analogue of the argument of § 5 of the present paper (which is now very simple) it suffices to solve

$$F \equiv 0 \pmod{p} \quad \text{if} \quad p \neq 3,$$

or

$$F \equiv 0 \pmod{9} \quad \text{if} \quad p = 3,$$

with some $a_i x_i \not\equiv 0 \pmod{3}$ in both cases, that is, with some x_i which occurs explicitly in F_0 different from 0.

For $p \neq 3$, a solution satisfying the conditions exists by lemma 4 of § 3 of the present paper.

For $p = 3$, we group the variables occurring in F_0 into $[\frac{1}{2}m_0]$ disjoint pairs, with possibly one left over which we equate to zero. For each pair x_i, x_j the congruence

$$a_i x_i^3 + a_j x_j^3 \equiv 0 \pmod{3}$$

has a solution with $x_i x_j \not\equiv 0 \pmod{3}$, namely $x_i = 1$, $x_j = \pm 1$. We take such a solution for each of the disjoint pairs and multiply the first solution throughout by T_1, the second by T_2, and so on.

If $m_0 \geqslant 4$, then $[\frac{1}{2}m_0] \geqslant 2$, and

$$F \equiv 3(\alpha_1 T_1^3 + \alpha_2 T_2^3 + \ldots + c_j y_j^3) \pmod{9},$$

and if $m_0 = 3$ then $[\frac{1}{2}m_0] = 1$ and

$$F = 3(\alpha_1 T_1^3 + \ldots + c_j y_j^3) \pmod{9},$$

where y_j typifies the variables (if any) in F_1. In the former case there is a solution of $F \equiv 0 \pmod{9}$ with either T_1 or $T_2 \not\equiv 0 \pmod{3}$, without using the variables y_j. In the second case we have $m_1 \geqslant 1$ (actually $m_1 \geqslant 2$) and there is a solution with $T_1 = 1$ and a suitable y_1. In either case we get a solution with some variable which occurs explicitly in F_0 different from 0.

As regards the last clause of theorem 1A, one may consider any equation of the form

$$x_1^3 - Nx_2^3 + p(x_3^3 - Nx_4^3) + p^2(x_5^3 - Nx_6^3) = 0,$$

where p is a prime $\equiv 1 \pmod{3}$ and N is a cubic non-residue modulo p. This has only the trivial solution in the p-adic field.

Proof of theorem 2A. As has been remarked before (e.g. in Davenport & Lewis 1963) the proof requires only a natural adaptation of the method of Davenport (1939). We consider the number of solutions of

$$a_1 x_1^3 + \ldots + a_8 x_8^3 = 0, \tag{143}$$

subject to

$$\kappa_i P < x_i < \kappa_i' P \quad (i = 1, \ldots, 4),$$

$$P^{\frac{4}{5}} < x_i < 2P^{\frac{4}{5}} \quad (i = 5, \ldots, 8).$$

It is necessary first to have a solution of

$$a_1\chi_1+\ldots+a_4\chi_4=0$$

with all the $\chi_i>0$, which can be postulated without loss of generality, and to choose the κ_i and κ_i' so that

$$\kappa_i<\chi_i^{\frac{1}{3}}<\kappa_i'.$$

The number of solutions can be expressed (in the notation of the present paper) as

$$\mathcal{N}_1(P)=\int_0^1 T_1(a_1\alpha)\ldots T_4(a_4\alpha)\,U(a_5\alpha)\ldots U(a_8\alpha)\,\mathrm{d}\alpha.$$

The major and minor arcs are defined as in Davenport (1939), and the contribution of the minor arcs to the integral is $\ll P^{4+\frac{1}{10}+3\delta}$ by lemma 15 of that paper. The contribution of the major arcs is investigated on the usual lines, starting from the approximations to $T(\alpha)$ and $U(\alpha)$ given by lemmas 7 and 8 of Davenport (1939), and yields an amount

$$CP^{\frac{21}{5}}\mathfrak{S}+o(P^{\frac{21}{5}}),$$

where C is a positive constant and $\mathfrak{S}$ is the 'singular series'

$$\mathfrak{S}=\sum_{q=1}^{\infty}\sum_{(a,q)=1}q^{-8}S_{a_1a,q}\ldots S_{a_8a,q}.$$

The singular series is absolutely convergent, since

$$q^{-8}\left|S_{a_1a,q}\ldots S_{a_8a,q}\right|\ll q^{-\frac{8}{3}},$$

and $\mathfrak{S}$ is positive provided the equation (143) has a non-singular solution in the p-adic field for each prime p. Since we can suppose all $a_i\neq 0$, a non-singular solution is the same as a solution with not all the x_i zero. The existence of such a solution is ensured by theorem 1A.

References

Birch, B. J. & Lewis, D. J. 1965 Systems of three quadratic forms. *Acta Arithmetica* **10**, 423–442.

Chowla, S., Mann, H. B. & Straus, E. G. 1959 Some applications of the Cauchy–Davenport theorem. *Kon. Norske Vidensk. Selsk. Forh.* **32**, 74–80.

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

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

Hua, L. K. 1938 On Waring's problem. *Quart. J. Math.* **9**, 199–202.

Lewis, D. J. 1957 Cubic congruences. *Michigan Math. J.* **4**, 85–95.