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

Quadratic Diophantine Equations

G. L. Watson

Phil. Trans. R. Soc. Lond. A 1960 **253**, 227-254
doi: 10.1098/rsta.1960.0023

QUADRATIC DIOPHANTINE EQUATIONS

By G. L. WATSON

University College London

(*Communicated by H. Davenport, F.R.S.—Received 5 April 1960*)

CONTENTS

	PAGE		PAGE
1. Introduction	227	6. The singular series	242
2. Preliminary analysis	229	7. Transformation of the diagonal equation	244
3. Exclusion of minor arcs	230	8. Quadratic congruences	248
4. Approximation on major arcs	234	9. Conclusion	250
5. The asymptotic formula	238	References	254

Tartakowsky (1929) proved that a positive definite quadratic form, with integral coefficients, in 5 or more variables represents all but at most finitely many of the positive integers not excluded by congruence considerations. Tartakowsky's argument does not lead to any estimate for a positive integer which, though not so excluded, is not represented by the quadratic form. Here estimates for such an integer are obtained, in terms of the coefficients of the quadratic form. To simplify the argument and improve the estimates, the problem is slightly generalized (by considering a Diophantine equation with linear terms). A combination of analytical and arithmetical methods is needed.

1. Introduction

Let $f = f(x_1, \ldots, x_n)$ be a positive definite quadratic form with integral coefficients, and N a positive integer. Suppose that f does not represent N (that is, that the Diophantine equation $f = N$ is insoluble in integers), although the congruence $f \equiv N \pmod{m}$ is soluble to every modulus. Then Tartakowsky (1929) showed that for given f with $n \geqslant 5$ there are at most finitely many possibilities for N. It is clear from Tartakowsky's argument that his result remains valid if the problem is generalized by introducing linear terms into the Diophantine equation. I find that this generalization makes it much easier to sharpen Tartakowsky's result by estimating N in terms of the coefficients of f. Such estimates are given in:

Theorem 1. *Let $f = f(x_1, \ldots, x_n)$ be a positive definite quadratic form with integral coefficients in $n \geqslant 5$ variables, and denote its discriminant by $d(\neq 0)$. Let $b_1, \ldots, b_n, N$ be integers, N positive, such that the equation*

$$f(x_1, \ldots, x_n) + b_1 x_1 + \ldots + b_n x_n = N \tag{1}$$

has no solution in integers x_i, although the congruence

$$f(x_1, \ldots x_n) + b_1 x_1 + \ldots + b_n x_n \equiv N \pmod{m} \tag{2}$$

has for every positive integer m a solution in integers x_i depending on m. Then we have the estimates (with implied constants depending only on n)

$$N \ll |d|, \quad \text{if} \quad n \geqslant 10, \tag{3}$$

$$N \ll |d|^{5/(n-4)+(1/n)}, \quad \text{if} \quad 5 \leqslant n \leqslant 9, \tag{4}$$

$$N \ll |d|, \quad \text{if} \quad n \geqslant 6 \quad \text{and} \quad f \quad \text{is diagonal.} \tag{5}$$

In the diagonal case, denote the diagonal coefficients of f by $a_1, \ldots, a_n$, and let ϵ be an arbitrary positive number; then we have

$$N \ll a_1 a_2 a_3 a_4 (a_1 + \ldots + a_n)^{1+\epsilon}, \tag{6}$$

with an implied constant depending only on n, ϵ.

It is of interest in itself, and necessary for the proof of theorem 1, to simplify the congruence condition, replacing the variable modulus m by a fixed modulus (depending only on f). We shall prove:

THEOREM 2. *Let $f = f(x_1, \ldots, x_n), n \geqslant 4$, be a non-singular quadratic form with integral coefficients and discriminant $d(\neq 0)$. Then there exists a positive integer $m_0 = m_0(f)$, depending only on f, with the following properties. The congruence (2) is soluble in integers x_i, for every positive integer m, whenever $b_1, \ldots b_n$, N are integers such that the congruence is soluble with $m = m_0$. Further, if d' is the product of the distinct prime factors of d, then $m_0^{n-3} d'$ divides d.*

It is only in the last part of theorem 2 that the precise definition of the discriminant $d = d(f)$ (which will be given later) is important.

Theorem 1 cannot be substantially improved. The condition $n \geqslant 5$ is necessary even for Tartakowsky's result (see Ross & Pall 1946), unless a stronger congruence condition is imposed; but even with such a condition I have not been able to estimate N in case $n = 4$. I have discussed the case $n = 3$, $b_1 = b_2 = b_3 = 0$ of (1) elsewhere (Watson 1960); any analogue of theorem 1 for $n = 3$ would have to have rather subtle hypotheses. The equation

$$2(x_1^2 + \ldots + x_{n-1}^2) + (N+2) x_n^2 = N, \quad n \geqslant 5, \tag{7}$$

is obviously insoluble for large odd N, yet it satisfies all the hypotheses of theorem 1 and has $N \gg |d|$.

In theorem 2 we need the condition $n \geqslant 4$, as may be seen by considering the congruence

$$x_1^2 + x_2^2 + x_3^2 \equiv -4^h \pmod{m},$$

with arbitrarily large h; this is soluble with $m = 4 \cdot 4^h$ but not with $m = 8 \cdot 4^h$. For $n \geqslant 4$ the last part of theorem 2 gives us

$$m_0^{n-3} \ll |d|. \tag{8}$$

By considering congruences of the shape

$$f = x_1^2 + x_2^2 + x_3^2 + 8 \cdot 4^h \phi(x_4, \ldots, x_n) \equiv -4^h \pmod{m}, \tag{9}$$

we see that (8) is best possible of its kind. For (9) is soluble with $m = 4 \cdot 4^h$, but not with $m = 8 \cdot 4^h$; and we can choose $d(\phi) \ll 1$, giving $d(f) \ll 4^{(n-3)h} \ll m_0^{n-3}$.

An outline of the argument may help the reader. We begin by tackling the diagonal case of (1) analytically, by the Hardy–Littlewood method, with the simplifications introduced by Vinogradov. These incidentally seem to be important; I can neither use them for $n = 4$ nor obtain any estimate for N without them. We seek an asymptotic formula for the number of solutions of (1) in the diagonal case. Ultimately we obtain an estimate for the error of this formula good enough to show that if there is no solution (6) must hold. From the nature of the method, the same conclusion would follow with the weaker hypothesis

that the actual number of solutions does not lie between $1 \pm \epsilon$ times the analytical approximation. Unfortunately the analysis does not directly give what is sought until we introduce an additional congruence condition, which implies that the sum of the singular series is not too small. Fortunately this additional hypothesis is not needed till the main analytical difficulty has been overcome.

Now we use elementary arithmetical arguments. These show (i) that the additional condition just mentioned can be dropped, (ii) that theorem 2 is true, and (iii) that (3), (4), (5) all follow from the case $n = 5$ of (6).

2. Preliminary analysis

The diagonal case of the equation (1) of § 1 is

$$\sum_{i=1}^{n} (a_i x_i^2 + b_i x_i) = N, \tag{1}$$

where $n \geqslant 5$ and the a_i are positive integers. Without loss of generality we assume

$$|b_i| \leqslant a_i \quad (i = 1, \ldots, n). \tag{2}$$

For if not, transform (1) by putting $x_i + c_i$ for x_i, with integers c_i so chosen that

$$|b_i'| = |2a_i c_i + b_i| \leqslant a_i.$$

This substitution takes (1) into an equation of the same shape, with the same a_i and with b_i', N', $N' > N$, for b_i, N, whence (6) of § 1 must be true for (1) if it is true for the transformed equation.

Using the usual abbreviation $\mathrm{e}(\theta)$ for $\exp(2\pi i\theta)$, θ real, we define exponential sums

$$S_i(\alpha) = \sum_{(4)} \mathrm{e}(a_i x_i^2 \alpha + b_i x_i \alpha), \tag{3}$$

the summation conditions being $\quad 0 \leqslant a_i x_i^2 + b_i x_i \leqslant N \quad$ (4)

(implied by (1), (2)). Clearly the number

$$r(N) = r(a_1, \ldots, a_n;\ b_1, \ldots, b_n;\ N)$$

of solutions of (1) (not at present assumed insoluble) is given by

$$r(N) = \int_0^1 S_1(\alpha) \ldots S_n(\alpha)\, \mathrm{e}(-N\alpha)\, \mathrm{d}\alpha. \tag{5}$$

There is clearly no serious loss of generality in assuming

$$N > \max_i a_i, \tag{6}$$

which with (2), (3), (4) gives the trivial estimate

$$S_i(\alpha) \ll a_i^{-\frac{1}{2}} N^{\frac{1}{2}}. \tag{7}$$

It is well known that for real α, P, with $P \geqslant 1$, there exist coprime integers h, q, q positive, such that $q \leqslant P$ and $|\alpha - h/q| \leqslant P^{-1} q^{-1}$. From the nature of our problem we cannot begin by working with such rational approximations to α, but must instead use similar approximations to the numbers $a_i \alpha$ (with $a_i^{-\frac{1}{2}} N^{\frac{1}{2}}$ for P). These approximations, h_i/q_i, will be chosen to satisfy

$$0 < q_i \ll a_i^{-\frac{1}{2}} N^{\frac{1}{2}}, \quad (h_i, q_i) = 1, \tag{8}$$

with the usual notation for a greatest common divisor, and

$$|\beta_i| \ll a_i^{\frac{1}{2}} N^{-\frac{1}{2}} q_i^{-1}, \tag{9}$$

where $\beta_i = a_i\alpha - h_i/q_i$.

We purposely make these inequalities less precise than they could be, so that later we may have, in some cases, more than one choice of q_i. It will be convenient however to impose the obvious restriction

$$-\frac{1}{2q_i} \leqslant \beta_i < \frac{1}{2q_i}, \tag{10}$$

so that the choice of q_i determines uniquely that of h_i. It is well known that results such as the following do not depend on the implied constants in (8), (9).

LEMMA 2·1. *When* (8), (9) *hold we have*

$$S_i(\alpha) \ll a_i^{-\frac{1}{2}} N^{\frac{1}{2}+\epsilon} q_i^{-\frac{1}{2}} \tag{11}$$

$$S_i(\alpha) \ll N^{\epsilon} q_i^{-\frac{1}{2}} |\beta_i|^{-\frac{1}{2}}, \quad \textit{if} \quad \beta_i \neq 0, \tag{12}$$

and

$$\int_{(8),\,(9)} |S_i(\alpha)|^4 \,\mathrm{d}\alpha \ll a_i^{-2} N^{1+\epsilon} q_i^{-2}, \tag{13}$$

where the range of integration is the interval on which (8), (9) *hold for any one pair* h_i, q_i.

Proof. See, for example, Watson (1953) (formulae (7·1), (7·2)) for (11), (12), from which (13) follows.

Formulae (11), (12) can be combined as

$$|S_i(\alpha)|^4 \ll a_i^{-2} N^{2+\epsilon} q_i^{-2} \min(1, a_i^2 N^{-2} \beta_i^{-2}), \tag{14}$$

where $\min(1, 0^{-1})$ is to be interpreted as 1 in case $\beta_i = 0$. By multiplying (11), (12) together we find

$$|S_i(\alpha)|^4 \ll a_i^{-1} N^{1+\epsilon} q_i^{-2} |\beta_i|^{-1}, \quad \text{if} \quad \beta_i \neq 0. \tag{15}$$

Summing over h_i, q_i in (13), or otherwise, we find

$$\int_0^1 |S_i(\alpha)|^4 \,\mathrm{d}\alpha \ll a_i^{-1} N^{1+\epsilon} \tag{16}$$

(which is well known). (Note in (13), (16) that $\mathrm{d}\alpha = a_i^{-1}\,\mathrm{d}\beta_i$.)

In all these estimates we may interpret the symbol $\ll$ as indicated in theorem 1. That is, the implied constant depends at most on n, ϵ, but not on ϵ (an arbitrary positive number) unless ϵ occurs explicitly in the formula. We adhere to this convention throughout; whether or not the constant need depend on n is never material.

It will be convenient to note here that $S_i(1-\alpha)$ is the complex conjugate of $S_i(\alpha)$, and that (10) gives us $h_i \neq 0$ for $\alpha \geqslant \frac{1}{2}$.

3. EXCLUSION OF MINOR ARCS

(*a*) I use the expression *minor arcs*, loosely, to denote a set of sub-intervals of the range of integration in (5) of §2, in which it is not advisable to replace the sums $S_i(\alpha)$ by convenient approximations; one has therefore to prove that the integral over this set is negligible. A natural choice of the set of minor arcs is to take it to be the set of α, in (0, 1), on which the rational numbers $h_i/a_i q_i$ (see (8), (9) of §2) are not all equal. The first effective treatment of a

situation of this nature was made by Birch & Davenport (1958). Their method was very laborious; the following crucial lemma is based on an unpublished simplification of their argument, due to Miss J. Pitman.

LEMMA 3·1. *Let G denote the part of the interval $(0, 1)$ on which, in the notation of* §2,

$$\frac{h_1}{a_1 q_1} \neq \frac{h_2}{a_2 q_2}.$$

Then we have

$$\int_G |S_1(\alpha)\, S_2(\alpha)|^4 \,\mathrm{d}\alpha \ll a_1^{-1} a_2^{-1} N^{2+\epsilon}.$$

Proof. Let H denote the part of the interval $(0, 1)$ on which

$$\frac{h_1}{a_1 q_1} \neq \frac{h_2}{a_2 q_2}, \quad a_1^{-1}|\beta_1| \geqslant a_2^{-1}|\beta_2| \quad \text{and} \quad \alpha \geqslant \tfrac{1}{2}. \tag{1}$$

From symmetry, and by the remark at the end of §2, it will suffice to prove

$$\int_H |S_i(\alpha)\, S_2(\alpha)|^4 \,\mathrm{d}\alpha \ll a_1^{-1} a_2^{-1} N^{2+\epsilon}. \tag{2}$$

For α in H, we define an integer $t = t(\alpha)$ by

$$a_2 h_1 q_2 - a_1 h_2 q_1 = (a_1, a_2)\, t. \tag{3}$$

From (1) we have $t \neq 0$. By (9) of §2, the left member of (3) is $a_1 a_2 q_1 q_2 (a_2^{-1}\beta_2 - a_1^{-1}\beta_1)$, whence by (1) we find

$$0 < (a_1, a_2)\,|t| \ll a_2 q_1 q_2 |\beta_1| \ll N, \tag{4}$$

using also (6), (8) and (9) of §2.

Now there exist integers r, s such that

$$a_2 s - a_1 r = (a_1, a_2)\, t, \quad 0 \leqslant s < (a_1, a_2)^{-1} a_1. \tag{5}$$

From (3), (5) it is clear that there exists an integer u with

$$h_1 q_2 = s + (a_1, a_2)^{-1} a_1 u, \quad h_2 q_1 = r + (a_1, a_2)^{-1} a_2 u. \tag{6}$$

From these formulae and (6), (8) of §2, using also the obvious $h_1 \ll a_1 q_1$, we find

$$u \ll (a_1, a_2)\, q_1 q_2 \ll N. \tag{7}$$

From (1), using the remark at the end of §2, and (8) of §2, we have

$$h_1 h_2 q_1 q_2 \neq 0. \tag{8}$$

Suppose now that t, u are given. Then the second of the formulae (5), with the congruence modulo $(a_1, a_2)^{-1} a_1$ derivable from the first, determines s uniquely, whence clearly r too is uniquely determined. The right member of each of the formulae (6) is easily seen to be $\ll N^2$, so by (6), (8) there are $\ll N^{\epsilon}$ possibilities for h_1, h_2, q_1, q_2. It follows that when t, u are given, α is restricted to lie in the union of a set of $\ll N^{\epsilon}$ intervals of the shape defined in (9) of §2, with $i = 2$.

For α in any one of these intervals, take $i = 2, 1$ in (14), (15) of §2, and then use (4), (7); we find

$$\begin{aligned} |S_1(\alpha)\, S_2(\alpha)|^4 &\ll a_1^{-1} N^{1+\epsilon} q_1^{-2} |\beta_1|^{-1} a_2^{-2} N^{2+\epsilon} q_2^{-2} \min\,(1, a_2^2 N^{-2} \beta_2^{-2}) \\ &\ll a_1^{-1} a_2^{-1} N^{3+2\epsilon} |t|^{-1} (|u| + 1)^{-1} \min\,(1, a_2^2 N^{-2} \beta_2^{-2}). \end{aligned}$$

Recalling that $\mathrm{d}\alpha = a_2^{-1}\mathrm{d}\beta_2$, we see that the contribution from the interval to the left member of (2) is

$$\ll a_1^{-1}a_2^{-1}N^{2+2\epsilon}|t|^{-1}(|u|+1)^{-1}.$$

We multiply by the estimate N^{ϵ} for the number of intervals corresponding to a given pair t, u, and then sum over $0 < |t| \ll N$, $u \ll N$ (see (4), (7)). This gives us that the left member of (2) is

$$\ll a_1^{-1}a_2^{-1}N^{2+3\epsilon}(\log N)^2 \ll a_1^{-1}a_2^{-1}N^{2+4\epsilon}.$$

Here as ϵ is arbitrary we may put $\frac{1}{4}\epsilon$ for ϵ; then we have (2) and the lemma follows. We deduce:

LEMMA 3·2. *Let J denote the part of the interval $(0, 1)$ on which, in the notation of §2, the numbers h_i/a_iq_i are not all equal. Then we have*

$$\int_J |S_1(\alpha)\ldots S_n(\alpha)|\,\mathrm{d}\alpha \ll \Delta^{-\frac{1}{2}}N^{\frac{1}{2}n-\frac{5}{4}+\epsilon}(a_1a_2a_3a_4)^{\frac{1}{4}}(a_5+\ldots+a_n)^{\frac{1}{4}},$$

for arbitrary positive ϵ, where for brevity Δ is written for the product $a_1\ldots a_n$.

Proof. We use the estimate of lemma 3·1, together with three estimates obtained from (16) of §2 by putting 3, 4, 5 for i, and G for $(0, 1)$. Applying Schwarz's inequality, we deduce from these four estimates that

$$\int_G |S_1(\alpha)\ldots S_5(\alpha)|\,\mathrm{d}\alpha \ll (a_1a_2a_3a_4a_5)^{-\frac{1}{4}}N^{\frac{5}{4}+\epsilon}.$$

Now this estimate may be written as

$$\int_G |S_1(\alpha)\ldots S_5(\alpha)|\,\mathrm{d}\alpha \ll \Delta^{-\frac{1}{2}}N^{\frac{5}{4}+\epsilon}(a_1\ldots a_5)^{\frac{1}{4}}(a_6\ldots a_n)^{\frac{1}{2}},$$

and from symmetry it remains valid if G is taken to be the part of the interval $(0, 1)$ on which the five rational numbers h_i/a_iq_i, $i = 1, \ldots, 5$, are not all equal.

Using for $i \geqslant 6$ the trivial estimate (7) of §2, we deduce

$$\int |S_1(\alpha)\ldots S_n(\alpha)|\,\mathrm{d}\alpha \ll \Delta^{-\frac{1}{2}}N^{\frac{1}{2}n-\frac{5}{4}+\epsilon}(a_1a_2a_3a_4a_5)^{\frac{1}{4}}.$$

This estimate is valid over the set just mentioned; but if we put $a_5+\ldots+a_n$ for a_5, it becomes permissible to permute the suffixes $5, \ldots n$. The lemma follows.

(*b*) The set $(0, 1) - J$, with J as in lemma 3·2, is the union of a finite number of intervals. It is important that these should, except for two with end points 0, 1, have the shape $|\alpha - h/q| \leqslant \beta_0$, with q a positive integer, h an integer prime to q, and β_0 independent of h (but depending on the a_i, N and q). To see that this is possible, it is convenient to prove a more precise form of the result on Diophantine approximation used in §2.

LEMMA 3·3. *Let P, α be given real numbers, $P > 1$. Let q denote a positive integer, h an integer prime to q. Then h, q may be chosen:*

(*i*) *in at least one way, to satisfy*

$$q \leqslant P, \quad \left|\alpha - \frac{h}{q}\right| \leqslant P^{-1}q^{-1}; \tag{9}$$

(*ii*) *either to satisfy*

$$q \leqslant P, \quad \left|\alpha - \frac{h}{q}\right| \leqslant \tfrac{1}{2}P^{-1}q^{-1}, \tag{10}$$

or in at least two ways to satisfy

$$q < 2P, \quad \left|\alpha - \frac{h}{q}\right| \leqslant P^{-1}q^{-1}. \tag{11}$$

Further, there is always at most one choice satisfying (10).

Proof. We express α as a continued fraction, and denote by h'/q' the last convergent whose denominator does not exceed P. (This may mean $h'/q' = \alpha$ if α is rational.) Except in the case $\alpha = h'/q'$, in which case $h, q = h', q'$ clearly satisfies (10), let h''/q'' be the next convergent to the continued fraction; this gives $q'' > P$. We have $|h'q'' - h''q'| = 1$.

Now α lies between the two successive convergents, so $|\alpha - h'/q'| \leqslant 1/q'q''$. Hence (9) is always satisfied by the choice $h, q = h', q'$; and if this choice fails to satisfy (10), then clearly $q'' < 2P$, while the second of the inequalities (11), with $h, q = h'', q''$, is implied by $|\alpha - h''/q''| \leqslant q''^{-2}$ (a well-known property of continued fractions) and $q'' > P$.

For the last assertion let $h, q = h', q'$; h'', q'' be two solutions of (10). (10) and $P > 1$ show that $q' = q''$ is impossible; so suppose $q' < q'' \leqslant P$. Then

$$\frac{1}{q'q''} \leqslant \left|\frac{h'}{q'} - \frac{h''}{q''}\right| \leqslant \tfrac{1}{2}P^{-1}(q'^{-1} + q''^{-1}) = \frac{q' + q''}{2Pq'q''} < \frac{1}{q'q''}$$

gives a contradiction. This completes the proof of the lemma and we deduce:

LEMMA 3·4. *With a suitable convention in the choice of the rational approximations h_i/q_i to the real numbers $a_i\alpha$, the set J of Lemma 3·2 is such that, for $0 \leqslant \alpha \leqslant 1$, the conditions*

$$\frac{h_1}{a_1 q_1} = \ldots = \frac{h_n}{a_n q_n}, \quad q_i \leqslant a_i^{-\frac{1}{2}} N^{\frac{1}{2}}, \quad |\beta_i| \leqslant \tfrac{1}{2} a_i^{\frac{1}{2}} N^{-\frac{1}{2}} q_i^{-1}, \tag{12}$$

are all satisfied if and only if α is not in J.

Proof. Put $a_i^{-\frac{1}{2}}N^{\frac{1}{2}}, a_i\alpha, h_i, q_i$ for P, α, h, q in Lemma 3·3; each of the pairs of inequalities (9), (10), (11), so modified, implies (8) and (9) of §2. The following convention gives what is required:

(i) if possible, choose the h_i/q_i to satisfy (12);

(ii) if not, choose them provisionally to satisfy

$$q_i \leqslant a_i^{-\frac{1}{2}} N^{\frac{1}{2}}, \quad |\beta_i| \leqslant a_i^{\frac{1}{2}} N^{-\frac{1}{2}} q_i^{-1}; \tag{13}$$

(iii) if the choice in (ii) makes the $h_i/a_i q_i$ all equal, alter the choice of one of the h_i/q_i (for an i for which the second of the inequalities (13) would become impossible on inserting a factor $\frac{1}{2}$ on the right) by appealing to part (ii) of Lemma 3·3, modified as above.

In case (i) this choice ensures that all the conditions (12) hold and α is not in J. In the other two cases, the first of conditions (12) fails and so by the definition of J, α is in J.

(*c*) The notation can now be simplified. When (12) holds, denote by h/q (q a positive integer, h an integer prime to q) the common value of the rational numbers $h_i/a_i q_i$. From $h_i/q_i = ha_i/q$, with $(h_i, q_i) = (h, q) = 1$, it follows that $q = (a_i, q)\, q_i$. Notice that $a_i^{-1}\beta_i = \alpha - h/q$, and write $\alpha - h/q = \beta$. Thus we have integers h, q satisfying (for α not in J) the conditions

$$q > 0, \quad (h, q) = 1 \tag{14}$$

$$q \leqslant N^{\frac{1}{2}} a_i^{-\frac{1}{2}} (a_i, q) \quad (i = 1, \ldots, n) \tag{15}$$

$$|\beta| = \left|\alpha - \frac{h}{q}\right| \leqslant \tfrac{1}{2} N^{-\frac{1}{2}} q^{-1} a_i^{-\frac{1}{2}} (a_i, q) \quad (i = 1, \ldots, n). \tag{16}$$

Conversely, if h, q satisfy (14), (15), (16), then h_i, q_i defined by $h_i/q_i = ha_i/q$, $(h_i, q_i) = 1$, satisfy all the conditions (12). Note further that, by the last part of Lemma 3·3, the conditions (14) to (16) define a set of non-overlapping intervals.

If we now define $r'(N) = r'(a_1, \ldots, a_n; b_1, \ldots, b_n; N)$ by

$$r'(N) = \int_{(0,1)-J} S_1(\alpha) \ldots S_n(\alpha)\, \mathrm{e}(-N\alpha)\, \mathrm{d}\alpha,$$

then the conclusion of Lemma 3·2 implies

$$r(N) - r'(N) \ll \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n - \frac{5}{4} + \epsilon} (a_1 a_2 a_3 a_4)^{\frac{1}{4}} (a_5 + \ldots + a_n)^{\frac{1}{4}}, \tag{17}$$

and we have

$$r'(N) = \sum_{q} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \int S_1\left(\frac{h}{q} + \beta\right) \ldots S_n\left(\frac{h}{q} + \beta\right) \mathrm{e}\left(-\frac{hN}{q} - N\beta\right) \mathrm{d}\beta, \tag{18}$$

where the range of the summation over q is given by (14), (15), and that of the integration over β by (16). To obtain (18), we have to exclude from the range of integration over α the interval

$$0 \leqslant \alpha \ll \tfrac{1}{2} N^{-\frac{1}{2}} (\max a_i)^{-\frac{1}{2}} \quad (h = 0,\ q = 1)$$

and include instead the interval

$$1 \leqslant \alpha \leqslant 1 + \tfrac{1}{2} N^{-\frac{1}{2}} (\max a_i)^{-\frac{1}{2}} \quad (h = 1,\ q = 1).$$

This makes no difference because of the periodicity of the integrand.

It should be noticed that (15) neither implies nor is implied by $q \leqslant N^{\frac{1}{2}}$; and (16) does not imply $|\beta| \ll N^{-\frac{1}{2}} q^{-1}$.

4. Approximation on major arcs

(*a*) We now introduce the notation and estimates that are needed (i) to define manageable approximations to the sums $S_i(h/q + \beta)$ occurring in (18) of §3 and (ii) to estimate the errors of these approximations.

For integers a, b, q, q positive, we define

$$S(a, b, q) = \sum_{x=1}^{q} \mathrm{e}\left(\frac{ax^2 + bx}{q}\right). \tag{1}$$

For real P, β, P positive, we define

$$I(P, \beta) = \int_{-P}^{P} \mathrm{e}(\beta\xi^2)\, \mathrm{d}\xi. \tag{2}$$

For real ξ, we write as usual $[\xi]$ for the greatest integer not exceeding ξ and define

$$\Psi(\xi) = \begin{cases} 0, & \text{if } \xi = [\xi] \\ \xi - [\xi] - \frac{1}{2}, & \text{otherwise.} \end{cases} \tag{3}$$

We note that $\Psi(\xi)$ has the Fourier expansion

$$\Psi(\xi) = -\frac{1}{2\pi \mathrm{i}} \sum_{-\infty}^{\infty}{}' l^{-1}\, \mathrm{e}(l\xi), \tag{4}$$

where the accent indicates that $l = 0$ is to be omitted and terms with the same $|l|$ taken together. We gather together in the shape of a lemma some well-known results.

Lemma 4·1. *We have*

$$S(a, b, q) = 0 \quad \textit{if} \quad (a, q) \nmid b; \tag{5}$$

$$S(a, b, q) \ll q^{\frac{1}{2}} (a, q)^{\frac{1}{2}}, \quad \textit{always}; \tag{6}$$

$$I(P, \beta) \ll \min\,(P, |\beta|^{-\frac{1}{2}}) \tag{7}$$

(*where if* $\beta = 0$, $\min(P, 0^{-\frac{1}{2}})$ *means* P); *and*

$$R(\xi) \ll \begin{cases} 1, & \text{always} \\ L^{-1}\|\xi\|^{-1} & \text{if} \quad \|\xi\| \neq 0, \end{cases} \tag{8}$$

where as usual $\|\xi\|$ *denotes the minimum of* $|\xi - t|$ *for integral* t, *and*

$$R(\xi) = -\frac{1}{2\pi i} \sum_{|l|>L}{}' l^{-1} \mathrm{e}(l\xi) \tag{9}$$

is the remainder (*after* $2L$ *terms*, $L > 0$) *of the Fourier series* (4).

Proof. Put $x = q(a,q)^{-1}y + z$ in (1); this gives

$$S(a,b,q) = \sum_z \mathrm{e}\left(\frac{az^2+bz}{q}\right) \sum_y \mathrm{e}\left(\frac{by}{(a,q)}\right)$$

with the summation conditions $0 \leqslant y < (a,q)$, $1 \leqslant z \leqslant q(a,q)^{-1}$. The inner sum clearly vanishes unless (a,q) divides b; so (5) follows. Now we may assume $(a,q)|b$ in the proof of (6); but because of the trivial property

$$S(ka,kb,kq) = kS(a,b,q) \tag{10}$$

(k any positive integer) we may also suppose $(a,b,q) = 1$. This and $(a,q)|b$ give $(a,q) = 1$. With this, (6) reduces to $S(a,b,q) \ll q^{\frac{1}{2}}$ and is well known (see, for example, lemma 8 of Birch & Davenport 1958). For (7) see Vinogradov (1954) (chap. 1, lemma 14*a*). (8) is straightforward and well known (the Fourier series is boundedly convergent).

(*b*) Now we consider the problem of approximating to a sum by an integral; it is convenient to deal with it, at first, in a more general shape than is actually needed. Let A, B be real numbers, $A < B$, and a, b, q, z integers, q positive. With a temporary notation, not to be confused with that of §1, let $f(\xi)$ be a complex-valued function of the real variable ξ, such that $f'(\xi)$ exists and is continuous in $A \leqslant \xi \leqslant B$. We seek to estimate the expressions

$$\sum_{\substack{A<x<B \\ x \equiv z \,(\mathrm{mod}\, q)}} f(x) - q^{-1}\int_A^B f(\xi)\,\mathrm{d}\xi, \tag{11}$$

$$\sum_{A<x<B} \mathrm{e}\left(\frac{ax^2+bx}{q}\right) f(x) - q^{-1}S(a,b,q)\int_A^B f(\xi)\,\mathrm{d}\xi. \tag{12}$$

LEMMA 4·2. *If neither* A *nor* B *is an integer, then the expression* (11) *is equal to*

$$\Psi\left(\frac{A-z}{q}\right) f(A) - \Psi\left(\frac{B-z}{q}\right) f(B) + \int_A^B \Psi\left(\frac{\xi-z}{q}\right) f'(\xi)\,\mathrm{d}\xi. \tag{13}$$

Proof. If $q = 1$ this is Euler's summation formula; the case $q > 1$ follows on suitably changing the variables of summation and integration (see, for example, lemmas 5·1, 5·2 of Davenport 1959).

LEMMA 4·3. *For every positive* ϵ, *the expression* (12) *is*

$$\ll q^{\frac{1}{2}+\epsilon}(a,q)^{\frac{1}{2}} l_0^{-1}\{\max|f(\xi)| + (B-A+1)\max|f'(\xi)|\}, \tag{14}$$

where the maxima are taken over $A \leqslant \xi \leqslant B$, *and* l_0 *is the least value of* $|l|$ *for* $l \equiv b$ *modulo* (a,q), $l \neq 0$.

Proof. We may suppose that neither A nor B is an integer; for if A is slightly increased and B slightly decreased the expression (12) obviously alters by $\ll \max|f(\xi)|$, which is small enough since $l_0 \leqslant (a,q) \leqslant q$. So we may appeal to lemma 4·2. We also use (8), taking $L = q^3$. Thus we have to multiply the expression (13) by $\mathrm{e}((ax^2+bx)/q)$, which with $x \equiv z \pmod q$ is equal to $\mathrm{e}((az^2+bz)/q)$, and sum over $z = 1, \ldots, q$. We do this for each of the three terms of (13), and in each case deal separately with the partial sum of the Fourier series and its remainder. Thus (12) is expressed as a sum of six terms, which we dispose of one by one.

The first of these is

$$-\frac{f(A)}{2\pi i}\sum_{z=1}^{q}\mathrm{e}\left(\frac{az^2+bz}{q}\right)\sum_{0<|l|\leqslant q^3} l^{-1}\,\mathrm{e}\left(\frac{lA-lz}{q}\right) \ll |f(A)|\sum_{l}|l|^{-1}\left|\sum_{z=1}^{q}\mathrm{e}\left(\frac{az^2+bz-lz}{q}\right)\right|.$$

Using (5) and (6), with $b-l$ for b, this is

$$\ll |f(A)|q^{\frac{1}{2}}(a,q)^{\frac{1}{2}}\sum{}''|l|^{-1},$$

where Σ'' is taken over $l \neq 0$, $|l| \leqslant q^3$, $l \equiv b \pmod{(a,q)}$, and so does not exceed

$$2l_0^{-1}(1+\tfrac{1}{2}+\tfrac{1}{3}+\ldots+q^{-3}) \ll l_0^{-1}q^{\epsilon}.$$

The first term is therefore of the required order of magnitude; and two other terms involving the partial sum of the Fourier series are dealt with similarly.

Now we consider the term $f(A)\,R((A-z)/q)$. From (8), with $L = q^3$, we have

$$R((A-z)/q) \ll q^{-1} \quad \text{unless} \quad \|(A-z)/q\| \ll q^{-2},$$

which is the case for $\ll 1$ values of z. For these z we use $R \ll 1$ and thus have

$$f(A)\sum_{z=1}^{q}R\left(\frac{A-z}{q}\right) \ll |f(A)|\,(q.q^{-1}+1) \ll |f(A)|,$$

which is small enough; and $f(B)\,\Sigma R((B-z)/q)$ is dealt with similarly.

It remains to consider

$$\sum_{z=1}^{q}\mathrm{e}\left(\frac{az^2+lz}{q}\right)\int_A^B R\left(\frac{\xi-z}{q}\right)f'(\xi)\,\mathrm{d}\xi \ll q\int_A^B \max_z\left|R\left(\frac{\xi-z}{q}\right)\right||f'(\xi)|\,\mathrm{d}\xi.$$

Consider first the part of the interval $A \leqslant \xi \leqslant B$ on which $\|\xi\| \geqslant 1/4q$, which, for all integral z, implies $\|(\xi-z)/q\| \geqslant 1/4q^2$ and so, by (8) with $L = q^3$, $R((\xi-z)/q) \ll q^{-1}$. Clearly therefore the contribution to the integral from this part of the interval is small enough. On the remainder of the interval, whose measure is clearly $\ll (B-A+1)\,q^{-1}$, the crude estimate $R \ll 1$ suffices and the proof is complete.

We cannot make effective use of the factor l_0^{-1} in the estimate of lemma 4·3 except by introducing another summation.

LEMMA 4·4.

$$\sum_{\substack{h=1\\(h,q)=1}}^{q}\left|\sum_{A<x<B}\mathrm{e}\left(\frac{ahx^2+bhx}{q}\right)f(x) - q^{-1}S(ah,bh,q)\int_A^B f(\xi)\,\mathrm{d}\xi\right|$$
$$\ll q^{\frac{3}{2}+\epsilon}(a,q)^{-\frac{1}{2}}\{\max|f(\xi)| + (B-A+1)\max|f'(\xi)|\}.$$

Proof. Replace l_0^{-1} in (14) by $l_0^{-1}(h)$, where $l_0(h)$ is defined like l_0, but with bh for b. $l_0(h)$ takes a set of at most q distinct values, each of which is a positive multiple of (a, b, q) and arises from $\ll q(a, b, q)/(a, q)$ values of h. The estimate

$$\sum_h l_0^{-1}(h) \ll q^{1+\epsilon}(a, q)^{-1}$$

follows easily, and leads to the desired result.

(*c*) We now approximate to the sums $S_i(h/q+\beta)$ in (18) of §3. From the nature of our problem, the estimate for the resulting error has to be as good as possible; but there are two difficulties. First, the linear term in (3) of §2 forces us to approximate to S_i with an error estimated in terms of q, instead of $q/(a_i, q)$, as would be possible with $b_i = 0$; lemma 4·4 retrieves what is lost in this way. Secondly, our rational approximation h/q to α is neither simple nor accurate, as noted at the end of §3. Because of these difficulties it does not seem possible either to improve the estimates or to obtain them more simply, by merely quoting the literature.

We define, for $i = 1, \ldots, n$,

$$S_i^*\left(\frac{h}{q}+\beta\right) = q^{-1}S(a_ih, b_ih, q)\, a_i^{-\frac{1}{2}} I(N^{\frac{1}{2}}, \beta), \tag{15}$$

although the approximation to S_i whose error can be dealt with directly by specializing lemmas 4·3, 4·4 is not this but the more complicated expression

$$q^{-1}S(a_ih, b_ih, q)\int_{A_i}^{B_i} \mathrm{e}(a_i\beta\xi^2+b_i\beta\xi)\,\mathrm{d}\xi, \tag{16}$$

with A_i, B_i such that $\quad a_iA_i^2+b_iA_i = a_iB_i^2+b_iB_i = N, \quad A_i < B_i.$ (17)

We prove:

LEMMA 4·5. *For h, q, β satisfying* (14), (15), (16) *of* § 3, *and all positive ϵ, we have*

$$\left|S_i\left(\frac{h}{q}+\beta\right)\right| + \left|S_i^*\left(\frac{h}{q}+\beta\right)\right| \ll a_i^{-\frac{1}{2}}(a_i, q)^{\frac{1}{2}} N^{\frac{1}{2}+\epsilon}q^{-\frac{1}{2}}(1+N|\beta|)^{-\frac{1}{2}}, \tag{18}$$

$$\sum_{\substack{h=1\\(h,q)=1}}^{q} \left|S_i\left(\frac{h}{q}+\beta\right) - S_i^*\left(\frac{h}{q}+\beta\right)\right| \ll q^{\frac{3}{2}+\epsilon}(a_i, q)^{-\frac{1}{2}}(1+N|\beta|). \tag{19}$$

Proof. To obtain (18), we estimate S_i by using (14) of §2, putting $q_i = q/(a_i, q), \beta_i = a_i\beta$, as in the argument leading to (14), (15), (16) of §3. For S_i^* we use (5), (6), (15), with $a_ih, b_ih, N^{\frac{1}{2}}$ for a, b, P; and $(h, q) = 1$.

To obtain (19), put a_i, b_i, A_i, B_i for a, b, A, B in lemma 4·4, and note that A_i and B_i are $\ll a_i^{-\frac{1}{2}}N^{\frac{1}{2}}$ by (17) and (2), (6) of §2. Put $f(\xi) = \mathrm{e}(a_i\beta\xi^2+b_i\beta\xi)$, which gives $|f(\xi)| = 1$ and, for $A_i \leqslant \xi \leqslant B_i$,

$$|f'(\xi)| = |2a_i\beta\xi+b_i\beta| \ll a_i|\beta|(|\xi|+1) \ll a_i^{\frac{1}{2}}N^{\frac{1}{2}}|\beta|.$$

This would give (19) if we defined S_i^* to be the expression (16), since the sum on the left of the estimate of lemma 4·4 (with the foregoing substitutions) is S_i.

To estimate the further error resulting from replacement of the expression (16) by (15), we crudely estimate the factor $q^{-1}S(a_ih, b_ih, q)$ to be $\ll 1$, since $S(a_ih, b_ih, q)$ is a sum of q terms each with modulus 1, and consider the difference between the integral in (16) and

$a_i^{-\frac{1}{2}} I(N^{\frac{1}{2}}, \beta)$. We multiply the integral in (16) by $\mathrm{e}(b_i^2\beta/4a_i)$; since $|b_i| \leqslant a_i$ as previously noted ((2) of §2), this leads to an error

$$\ll (B_i - A_i)\left\{1 - \mathrm{e}\left(\frac{b_i^2\beta}{4a_i}\right)\right\} \ll (B_i - A_i)\left|\frac{b_i^2\beta}{a_i}\right| \ll a_i^{\frac{1}{2}} N^{\frac{1}{2}}|\beta|.$$

The integral in (16) thus becomes

$$\int_{A_i}^{B_i} \mathrm{e}\left\{a_i\beta\left(\xi + \frac{b_i}{2a_i}\right)^2\right\} \mathrm{d}\xi = a_i^{-\frac{1}{2}} \int \mathrm{e}(\beta\xi^2)\, \mathrm{d}\xi$$

on putting $a_i^{-\frac{1}{2}}\xi - b_i/2a_i$ for ξ. The limits on the right are easily seen to differ from $\pm N^{\frac{1}{2}}$ by $\ll 1$. The further error in the left member of (19) is thus less than the right member, being

$$\ll q(a_i^{\frac{1}{2}} N^{\frac{1}{2}}|\beta| + a_i^{-\frac{1}{2}}) \ll q(N|\beta| + 1).$$

5. The asymptotic formula

(*a*) We now define $r^*(N) = r^*(a_1, \ldots, a_n; b_1, \ldots, b_n; N)$ by

$$r^*(N) = \sum_q \sum_h \int S_1^*\left(\frac{h}{q} + \beta\right) \ldots S_n^*\left(\frac{h}{q} + \beta\right) \mathrm{e}\left(-\frac{hN}{q} - N\beta\right) \mathrm{d}\beta, \tag{1}$$

with summation over q, h and integration over β as in the expression for $r'(N)$ in (18) of §3. We prove:

Lemma 5·1. $r'(N) - r^*(N) \ll \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n - \frac{5}{4} + \epsilon} (a_1 a_2 a_3 a_4)^{\frac{1}{4}} (a_5 + \ldots + a_n)^{\frac{1}{4}}$.

Proof. With integration and summation as in (1), write, for $j = 1, \ldots, n$,

$$E_j = \sum_q \int \sum_h \left| S_j\left(\frac{h}{q} + \beta\right) - S_j^*\left(\frac{h}{q} + \beta\right)\right| \prod_{i \neq j} \max_h \left(\left|S_i\left(\frac{h}{q} + \beta\right)\right| + \left|S_i^*\left(\frac{h}{q} + \beta\right)\right|\right) \mathrm{d}\beta.$$

It is clear that $|r'(N) - r^*(N)| \leqslant E_1 + \ldots + E_n$; so it will suffice to prove

$$E_n \ll \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n - \frac{5}{4} + \epsilon} (a_1 a_2 a_3 a_4 a_n)^{\frac{1}{4}}. \tag{2}$$

For then on permuting the suffixes 1, 2, 3, 4, n we obtain the same estimate for $E_1, \ldots, E_4$, and permuting 5, …, n we estimate $E_5, \ldots, E_{n-1}$.

Using (15) of §3 and (19) of §4, with $i = n$, we find

$$\left|S_n\left(\frac{h}{q} + \beta\right) - S_n^*\left(\frac{h}{q} + \beta\right)\right| \ll a_n^{-\frac{1}{4}} N^{\frac{1}{4} + \epsilon} q(1 + N|\beta|).$$

Now using also (18) of §4, with $i = 1, \ldots, n-1$, we have

$$E_n \ll a_n^{\frac{1}{4}} \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n - \frac{1}{4} + \epsilon} \sum_q q^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, q)^{\frac{1}{2}} \int (1 + N|\beta|)^{\frac{1}{2}(3-n)}\, \mathrm{d}\beta.$$

The limits for β lie between $\pm N^{-\frac{1}{2}}$ by (16) of §3, so the integral over β, using $n \geqslant 5$, is $\ll N^{\epsilon - 1}$. Putting $\frac{1}{2}\epsilon$ for ϵ and noting that (6) of §2 and (15) of §3 give $q \leqslant N \leqslant N^{5n}$, we find

$$E_n \ll a_n^{\frac{1}{4}} \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n - \frac{5}{4} + \epsilon} \sum_q q^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, q)^{\frac{1}{2}}.$$

This gives (2) if we prove

$$\sum_{q=1}^{N^{5n}} q^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, q)^{\frac{1}{2}} \ll N^{\epsilon} (a_1 a_2 a_3 a_4)^{\frac{1}{4}}. \tag{3}$$

To prove (3), which will be needed again later, write $g = (\Delta, q)$, $q = gk$, and use again $n \geqslant 5$; the left member of (3) is at most

$$\sum_{g|\Delta} \sum_{k=1}^{N^{5n}} g^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, g)^{\frac{1}{2}} k^{\frac{1}{2}(3-n)} \leqslant \sum_{k=1}^{N^{5n}} k^{-1} \sum_{g|\Delta} 1 . \max_{g|\Delta} g^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, g)^{\frac{1}{2}}.$$

The product of the two sums on the right is

$$\ll (N^{5n}\Delta)^{\epsilon/10n} = (N^{5n} a_1 \dots a_n)^{\epsilon/10n} < N^{\epsilon},$$

using (6) of §2. Estimating the remaining factor by using $(a_i, g) \leqslant \min (a_i^{\frac{1}{2}} g^{\frac{1}{2}}, g)$, (3) follows and the proof of the lemma is complete. The next step is:

LEMMA 5·2. *The estimate of lemma* 5·1 *remains valid if* $r^*(N)$ *is replaced by* $r^{**}(N)$, *defined in the same way as* $r^*(N)$ *but with the range of integration over* β *extended to* $(-\infty, \infty)$.

Proof. Denote by $M = M(q)$ the bound for $N|\beta|$ given by (16) of §3. Use (18) of §4, and note that, by (7) of §4, it is valid as far as S_i^* is concerned without any restriction on β. It follows (summing over h) that

$$r^*(N) - r^{**}(N) \ll \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n+\epsilon} \sum_q q^{1-\frac{1}{2}n} \prod_{i=1}^{n} (a_i, q)^{\frac{1}{2}} \int |N\beta|^{-\frac{1}{2}n} \, \mathrm{d}\beta.$$

Here the integral is taken over $|\beta| \geqslant MN^{-1}$, and so is $\ll M^{1-\frac{1}{2}n} N^{-1} \ll M^{-\frac{1}{2}} N^{-1}$.

From the definition of M, we have, for some i,

$$M^{-\frac{1}{2}} \ll N^{-\frac{1}{4}} q^{\frac{1}{2}} a_i^{\frac{1}{4}} (a_i, q)^{-\frac{1}{2}}. \tag{4}$$

The contribution to the estimate for $r^*(N) - r^{**}(N)$ from the q for which (4) holds with $i = n$ (which as in lemma 5·1 are all at most N^{5n}) is

$$\ll a_n^{\frac{1}{4}} \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n-\frac{5}{4}+\epsilon} \sum_{q=1}^{N^{5n}} q^{\frac{1}{2}(3-n)} \prod_{i=1}^{n-1} (a_i, q)^{\frac{1}{2}} \ll \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n-\frac{5}{4}+2\epsilon} (a_1 a_2 a_3 a_4 a_n)^{\frac{1}{4}},$$

using (3). Permuting the suffixes as in Lemma 5·1 to deal with the q for which (4) holds with $i = 1, \dots, n-1$, the lemma follows.

(*b*) Now we define $A(q, N) = A(a_1, \dots, a_n; b_1, \dots, b_n; q, N)$ by

$$A(q, N) = q^{-n} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \mathrm{e}\left(-\frac{hq}{N}\right) \prod_{i=1}^{n} S(a_i h, b_i h, q). \tag{5}$$

Crudely (6) of §4 gives

$$A(q, N) \ll q^{1-\frac{1}{2}n} \prod_{i=1}^{n} (a_i, q)^{\frac{1}{2}}. \tag{6}$$

Referring to (15) of §4, we see that

$$r^{**}(N) = \Delta^{-\frac{1}{2}} \sum_q A(q, N) \int_{-\infty}^{\infty} \mathrm{e}(-N\beta) \, I^n(N^{\frac{1}{2}}, \beta) \, \mathrm{d}\beta. \tag{7}$$

Here the range of summation over q is as in (1). The integral is absolutely convergent (for $n > 2$) by (7) of §4. Putting $P = N^{\frac{1}{2}}, \xi = N^{\frac{1}{2}}\eta$, in (2) of §4, we see that

$$I(N^{\frac{1}{2}}, \beta) = N^{\frac{1}{2}} I(1, N\beta),$$

whence it is easily deduced that

$$\int_{-\infty}^{\infty} \mathrm{e}(-N\beta) \, I^n(N^{\frac{1}{2}}, \beta) \, \mathrm{d}\beta = \theta_n N^{\frac{1}{2}n-1}, \tag{8}$$

with θ_n depending only on n. Thus (7) may be rewritten as

$$r^{**}(N) = \theta_n \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n-1} \sum_q A(q, N), \tag{9}$$

again with summation over q as in (1).

The value of θ_n could be determined in various ways, making use of the fact that it depends only on n; we might for example put all the b_i equal to zero, and then compare the asymptotic formula which we shall obtain with that in, for example, Ross & Pall (1946). It is possible, however, because of the linear terms in the Diophantine equation under consideration, to give a simple and self-contained proof.

LEMMA 5·3. *The constant θ_n in* (8), (9) *is equal to $\frac{1}{2}nJ_n$, where $J_n = 2\pi^{\frac{1}{2}n}/n\Gamma(\frac{1}{2}n)$ is the content of the n-dimensional sphere $\xi_1^2 + \ldots + \xi_n^2 \leqslant 1$.*

Proof. Taking advantage of the fact that θ_n depends only on n, we specialize by taking $a_1 = \ldots = a_n = k!, b_1 = \ldots = b_n = 1$, k a large positive integer; that is, we consider the special case

$$k!(x_1^2 + \ldots + x_n^2) + x_1 + \ldots + x_n = N$$

of the equation (1) of §2. With this specialization, (5) of §4 gives $A(q, N) = 0$ unless q is prime to $k!$, in which case (6) gives $A(q, N) \ll q^{1-\frac{1}{2}n} \ll q^{-\frac{3}{4}}$. The sum over q in (9) is therefore approximately 1 for large k.

Write for brevity $X \sim Y$, X, Y being functions of k, N, to denote that the upper and lower limits of X/Y, as $N \to \infty$, both tend to 1 as $k \to \infty$. Then by the foregoing remark

$$r(N) \sim r^{**}(N) \sim \theta_n \Delta^{-\frac{1}{2}} N^{\frac{1}{2}n-1} = \theta_n (k!)^{-\frac{1}{2}n} N^{\frac{1}{2}n-1},$$

whence

$$r(1) + \ldots + r(N) \sim 2n^{-1}\theta_n (k!)^{-\frac{1}{2}n} N^{\frac{1}{2}n}.$$

But $r(1) + \ldots + r(N)$ is the number of points with integral co-ordinates in the sphere

$$k!(\xi_1^2 + \ldots + \xi_n^2) + \xi_1 + \ldots + \xi_n \leqslant N.$$

Hence

$$r(1) + \ldots + r(N) \sim V(k, N),$$

where

$$V(k, N) \sim J_n (k!)^{-\frac{1}{2}n} N^{\frac{1}{2}n}$$

is the volume of this sphere; the result follows.

(*c*) The next step in the process of approximation to is to extend to infinity the sum over q in (9); we prove:

LEMMA 5·4. *We have*

$$\sum_{q=1}^{\infty}{}' |A(q, N)| \ll N^{\epsilon - \frac{1}{4}} (a_1 a_2 a_3 a_4)^{\frac{1}{4}} (a_5 + \ldots + a_n)^{\frac{1}{4}},$$

where the accent denotes exclusion of the q in formula (9), *and the series is absolutely convergent.*

Proof. The convergence follows trivially from (6), with $n \geqslant 5$. Consider first the sum over $q > N^{2n}$, implying $q > (\max a_i)^{2n}$ ((6) of §2). For such q, $(a_i, q) < q^{1/2n}$ and so (6) gives

$$A(q, N) \ll q^{-\frac{5}{4}}, \quad \sum |A(q, N)| \ll N^{-\frac{1}{2}n}.$$

Next take the q, not exceeding N^{5n}, for which the summation condition (15) of §3 fails for $i = n$; the sum over these q may be estimated by using (6), (3), after multiplying the summand $|A(q, N)|$ by $q^{\frac{1}{2}} N^{-\frac{1}{4}} a_n^{\frac{1}{4}} (a_n, q)^{-\frac{1}{2}}$, which (for the q in question) is at least 1.

Similarly dealing with the q for which (15) of §3 fails for other values of i, the lemma follows.

Finally we replace $N^{\frac{1}{2}n-1}$ in (9) by $(N+b_1^2/4a_1+\ldots+b_n^2/4a_n)^{\frac{1}{2}n-1}$, so as to make the approximation to $r(N)$ a little easier to handle later. The final approximation is thus

$$\rho(N)=\frac{\pi^{\frac{1}{2}n}}{\Gamma(\frac{1}{2}n)}\Delta^{-\frac{1}{2}}\left(N+\frac{1}{4}\frac{b_1^2}{a_1}+\ldots+\frac{1}{4}\frac{b_n^2}{a_n}\right)^{\frac{1}{2}n-1}\mathfrak{S}(N), \tag{10}$$

where
$$\mathfrak{S}(N)=\mathfrak{S}(a_1,\ldots,a_n;\,b_1,\ldots,b_n;\,N)=\sum_{q=1}^{\infty}A(q,N)\ll\Delta^{\epsilon}a_1^{\frac{1}{2}}a_2^{\frac{1}{2}} \tag{11}$$

is the singular series, estimated by summing (6) as in the proof of (3). We have

$$r(N)-\rho(N)\ll\Delta^{-\frac{1}{2}}N^{\frac{1}{2}n-\frac{5}{4}+\epsilon}(a_1a_2a_3a_4)^{\frac{1}{4}}(a_5+\ldots+a_n)^{\frac{1}{4}} \tag{12}$$

(by (17) of §3, Lemmas 5·2 and 5·4, and $|b|\leqslant a_i<N$ ((2), (6) of §2), which give

$$\left(N+\frac{1}{4}\frac{b_1^2}{a_1}+\ldots+\frac{1}{4}\frac{b_n^2}{a_n}\right)^{\frac{1}{2}n-1}-N^{\frac{1}{2}n-1}\ll N^{\frac{1}{2}n-2}\max a_i).$$

To simplify the argument later, we prove:

LEMMA 5·5. *The estimate*

$$r(N)-\rho(N)\ll\Delta^{-\frac{1}{2}}\left(N+\frac{1}{4}\frac{b_1^2}{a_1}+\ldots+\frac{b_n^2}{a_n}\right)^{\frac{1}{2}n-\frac{5}{4}+\epsilon}(a_1a_2a_3a_4)^{\frac{1}{4}}(a_5+\ldots+a_n)^{\frac{1}{4}} \tag{13}$$

is valid without any conditions on the parameters in the equation (1) *of* §2 *except that* $n\geqslant 5$, *the* a_i *are positive integers, the* b_i *and* N *are integers, and*

$$N+\frac{1}{4}\frac{b_1^2}{a_1}+\ldots+\frac{1}{4}\frac{b_n^2}{a_n}>\tfrac{5}{4}(a_1+\ldots+a_n). \tag{14}$$

Proof. The hypotheses and conclusion of the lemma are invariant under trivial substitutions $x_i\to x_i+c_i$; hence, see (2) of §2 and the remark following, we may suppose $|b_i|\leqslant a_i$ (for all i). With this, (14) implies (6) of §2; and now all the hypotheses of §2 hold. It follows that (12), implying (13), is satisfied, which completes the proof of the lemma.

It could easily be shown (using $n\geqslant 5$) that $\mathfrak{S}(N)$ is a non-negative real number which vanishes only when congruence considerations imply $r(N)=0$, and which, if values of N for which this is the case are excluded, has a positive lower bound depending only on the a_i. Thus, interpreting 0/0 as 1, we have, from (12) or (13),

$$\frac{r(N)}{\rho(N)}\to 1\quad\text{as}\quad N\to\infty. \tag{15}$$

We seek to sharpen (15) by estimating $1-r(N)/\rho(N)$. The estimate desired follows if we can prove that the lower bound just mentioned is $\gg\Delta^{-\epsilon}$, for arbitrary positive ϵ. This is not always the case, but we show in the next section that it is true if we impose a certain congruence condition on the Diophantine equation. Then an arithmetical argument shows that the estimate for $1-r(N)/\rho(N)$ is still valid if this condition is omitted.

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

6. The singular series

(*a*) In this section it will be convenient to write

$$Q = Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} (a_i x_i^2 + b_i x_i),$$

so that the Diophantine equation (1) of § 2 is $Q = N$. We shall say that this equation satisfies the *necessary congruence condition* if the congruence $Q \equiv N \pmod m$ is soluble for every positive integer m. Denote by $C(m, N)$ the number of solutions of this congruence; then the necessary congruence condition is $C(m, N) > 0$ for all positive integers m.

It is easily shown (see for example, Vinogradov 1954, chap. II, lemma 10, for the method) that

$$\sum_{q|m} A(q, N) = m^{1-n} C(m, N). \tag{1}$$

The right member of this equation being an obviously multiplicative function of m (for fixed a_i, b_i, N) we see that

$$\sum_{q|m} A(q, N) = \prod_{p|m} \sum_{p^t|m} A(p^t, N), \tag{2}$$

where p denotes a prime. Write

$$\chi(p, N) = \sum_{t=0}^{\infty} A(p^t, N) = 1 + \sum_{t=1}^{\infty} A(p^t, N). \tag{3}$$

(Lemma 5·4 shows that this series, for each p, is absolutely convergent, as is $\mathfrak{S}(N)$.) It follows that

$$\chi(p, N) = \lim_{u \to \infty} p^{u-nu} C(p^u, N), \tag{4}$$

and, making m in (2) tend to infinity through a suitable sequence of values, that

$$\mathfrak{S}(N) = \prod_{p} \chi(p, N), \tag{5}$$

the infinite product, taken over $p = 2, 3, 5, \ldots$, being absolutely convergent.

We say that the equation $Q = N$ satisfies the *strong congruence condition* if the congruence $Q = N \pmod m$ has for every positive integer m a solution satisfying

$$\left(\frac{\partial Q}{\partial x_1}, \ldots, \frac{\partial Q}{\partial x_n}, m\right) = 1 \text{ or } 2. \tag{6}$$

Denote by $C'(m, N)$ the number of solutions of $Q \equiv N \pmod m$ that satisfy (6) also; thus the strong congruence condition is $C'(m, N) > 0$ for all positive integers m.

A well known inductive construction for the solutions of $Q \equiv N \pmod{p^u}$ and (6), with $m = p^u$, gives

$$C'(p^u, N) = p^{n-1} C'(p^{u-1}, N) \quad \text{if} \quad \begin{cases} u \geqslant 4 & (p = 2) \\ u \geqslant 2 & (p \neq 2). \end{cases}$$

The construction depends only on the assumption that Q is a polynomial with integral coefficients; it is given for Q a cubic form (but the argument is quite general) in Davenport (1959) (put $l = 1, 2$ for $p \geqslant, = 2$ in lemma 2·3). It follows that

$$C(p^u, N) \geqslant C'(p^u, N) = p^{nu-u+1-n} C'(p, N) \quad \text{for} \quad u \geqslant 2, \quad p \neq 2,$$

and

$$C(2^u, N) \geqslant C'(2^u, N) = 2^{nu-u+3-3n} C'(8, N), \quad \text{for} \quad u \geqslant 4,$$

whence by (4)

$$\chi(p, N) \geqslant \begin{cases} p^{1-n} C'(p, N) & (p \neq 2) \\ 8^{1-n} C'(8, N) & (p = 2). \end{cases} \tag{7}$$

(*b*) We seek to deduce a lower estimate for $\chi(p, N)$ from the assumption $C'(p, N) > 0$ or $C'(8, N) > 0$; (7) gives what will suffice when $p = 2$, so we are concerned with odd p. The first step is to show that the b_i may be ignored.

LEMMA 6·1. *For odd p, either $\chi(p, N) = 1$ or a suitable substitution $x_i \to x_i + t_i$ takes the congruence $Q \equiv N \pmod p$ into one of the shape*

$$a_1 x_1^2 + \ldots + a_n x_n^2 \equiv N_1 \pmod p \tag{8}$$

and (6) with $m = p$ into

$$a_1 x_1, \ldots, a_n x_n \not\equiv 0, \ldots, 0 \pmod p. \tag{9}$$

Proof. The second alternative clearly holds if integers t_i can be chosen to satisfy

$$2a_i t_i + b_i \equiv 0 \pmod p, \quad i \equiv 1, \ldots, n;$$

the integer N_1 is $N - \Sigma(a_i t_i^2 + b_i t_i)$.

If these congruences cannot be satisfied then clearly there is an i with $p | 2a_i, p \nmid b_i$. Since $p \neq 2$, assume without loss of generality that $p | a_n, p \nmid b_n$. Then (6) with $m = p$ is always satisfied, while $Q \equiv N \pmod p$ holds, for each set of values of $x_1, \ldots, x_{n-1}$, for just one value of x_n modulo p. Clearly therefore $C(p, N) = C'(p, N) = p^{n-1}$, $\chi(p, N) = 1$.

Now for odd p with $\chi(p, N) \neq 1$, $C(p, N)$ is the number of solutions of (8), $C'(p, N)$ that of (8) and (9), and these numbers are equal unless $p | N_1$.

LEMMA 6·2. *For $n \geqslant 1$, $p \nmid 2N_1$, (8) has $\gg p^{n-1}$ solutions if at most $n-2$ of the a_i are divisible by p, and otherwise either $2p^{n-1}$ or none.*

Proof. It is clear that in either case we lose nothing by supposing all the a_i prime to p; with this, the second assertion becomes trivial. In the proof of the first we may use induction for $n \geqslant 3$, choosing x_n, in at least $p - 2 \gg p$ ways, so that $a_n x_n^2 \not\equiv N_1 \pmod p$, and then counting the number of possibilities for $x_1, \ldots, x_{n-1}$, for each value of x_n.

We have now only to show that $a_1 x_1^2 + a_2 x_2^2 \equiv N_1 \pmod p$, with $p \nmid 2a_1 a_2 N_1$, has $\gg p$ solutions. We divide by $p - 1$ the number of solutions of $a_1 x_1^2 + a_2 x_2^2 \equiv N_1 x_3^2 \pmod p$ with $p \nmid x_3$. Clearly this congruence has at most $2p - 1$ solutions with $p | x_3$, so the second part of the next lemma completes the proof of this.

LEMMA 6·3. *The congruence (8), with $p \neq 2$, $N_1 = 0$, has $\gg p^{n-1}$ solutions satisfying (9), provided, in case p divides $n-2$ or more of the a_i, that it has at least one such solution. In case $n = 3$ and $p \neq 2$, $N_1 = 0$, $p \nmid a_1 a_2 a_3$, (8) has p^2 solutions.*

Proof. Again we may suppose without loss of generality that p divides none of the a_i. The case $n \leqslant 2$ is now clear, since any one solution of (8), (9), with $N_1 = 0$, yields $p - 2$ others on multiplying by $2, \ldots, p - 1$.

Assuming for the moment that the lemma is true for $n = 3$ then lemma 6·2 may be used, and counting the possibilities for the other x_i, for each of the values $1, \ldots, p$ of x_n, the case $n \geqslant 4$ is disposed of by induction.

It remains to prove that $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 \equiv 0 \pmod p$, $p \nmid 2a_1 a_2 a_3$, has just p^2 solutions. We can transform this last congruence, by a suitable change of variables, into

$$y_1 y_2 - 4a_1 a_2 a_3 y_3^2 \equiv 0 \pmod p$$

(Watson 1960, theorem 29), whence its solutions are easily counted and the proof is complete.

From (7), and the foregoing lemmas ((7) alone sufficing for $p = 2$, or indeed for $p \ll 1$), it follows that the strong congruence condition implies

$$\chi(p, N) \gg 1 \quad \text{for all } p. \tag{10}$$

(*c*) We deduce:

LEMMA 6·4 *$\mathfrak{S}(N)$ defined by (5) is a non-negative real number. If the Diophantine equation $Q = N$, $n \geqslant 5$, satisfies the strong congruence condition then $\mathfrak{S}(N)$ does not vanish and*

$$(\mathfrak{S}(N))^{-1} \ll (\max_i a_i)^{\epsilon}.$$

Proof. The first assertion is clear from (4), (5).

Now note that (10) gives

$$\max(0, -\log \chi(p, N)) \ll \log(1 + |1 - \chi(p, N)|) \ll |1 - \chi(p, N)|. \tag{11}$$

Also that (6) of § 5, with $q = p, p^2, \ldots$, and (3) give

$$1 - \chi(p, N) \ll p^{1-\frac{1}{2}n} \leqslant p^{-\frac{3}{2}} \quad \text{if} \quad p \nmid a_1 \ldots a_n. \tag{12}$$

It follows that

$$\sum_p{}' \max(0, -\log \chi(p, N)) \ll \sum_p p^{-\frac{3}{2}} \ll 1,$$

where the accent denotes the exclusion of p to which (12) is inapplicable. On the other hand, denoting the inclusion of these p only (that is, the p dividing $a_1 \ldots a_n$) by a double accent we have, for any positive ϵ, using (10),

$$\sum_p{}'' \max(0, -\log \chi(p, N)) \ll \sum_p{}'' 1 \ll \epsilon \log \max_i a_i.$$

The lemma follows.

An immediate consequence is:

LEMMA 6·5. *The hypotheses of lemma 5·5 together with the strong congruence condition for the equation $Q = N$, imply $\rho(N) \neq 0$ and*

$$\frac{r(N)}{\rho(N)} - 1 \ll \left(N + \frac{1}{4}\frac{b_1^2}{a_1} + \ldots + \frac{b_n^2}{a_n}\right)^{\epsilon - \frac{1}{4}} (a_1 a_2 a_3 a_4)^{\frac{1}{4}+\epsilon} (a_5 + \ldots + a_n)^{\frac{1}{4}+\epsilon}.$$

7. TRANSFORMATION OF THE DIAGONAL EQUATION

(*a*) Let the equation (1) of § 2, that is,

$$\sum_{i=1}^{n} (a_i x_i^2 + b_i x_i) = N, \tag{1}$$

be taken into another equation of the same shape, say

$$\sum_{i=1}^{n} (a_i' x_i'^2 + b_i' x_i) = N', \tag{2}$$

by a linear transformation of the variables, say

$$x_i = m_i x_i' + t_i. \tag{3}$$

The transformation (3) (in which the m_i are positive integers and the t_i integers) will be so chosen that the solutions of (1), (2) are in one-to-one correspondence, whence

$$r(a_1, \ldots, a_n; b_1 \ldots, b_n; N) = r(a_1', \ldots, a_n'; b_1', \ldots, b_n'; N'); \tag{4}$$

and so that further the analytic approximations to the two sides of (4) coincide, that is

$$\rho(a_1, \ldots, a_n; b_1, \ldots, b_n; N) = \rho(a'_1, \ldots, a'_n; b'_1, \ldots, b'_n; N'). \tag{5}$$

Still further, assuming that (1) satisfies the necessary congruence condition defined in § 6, the transformation (3) will be so chosen that (2) also satisfies this condition. The ultimate object, which will be achieved by successive steps, is that (2) should satisfy the strong congruence condition.

LEMMA 7·1. *Suppose that the transformation* (3) *reduces to the identity; so that equations* (1), (2) *differ, except for the accents, merely by a constant factor. Then* (4) *and* (5) *hold, and* (2) *satisfies the necessary congruence condition if* (1) *does.*

Proof. Except for (5), all the assertions are trivial. In the proof of (5) we may suppose that some prime p divides all of the a_i, b_i and N, and that $a'_i = p^{-1}a_i, b'_i = p^{-1}b_i, N' = p^{-1}N$. Now use (10) of § 5 and (5) of § 6, and write more explicitly $\chi(a_1, \ldots, a_n; b_1, \ldots, b_n; p, N)$ for $\chi(p, N)$. This shows that the ratio of the right to the left member of (5) is

$$p^{\frac{1}{2}n} p^{1-\frac{1}{2}n} \prod_q \left(\frac{\chi(p^{-1}a_1, \ldots, p^{-1}a_n; p^{-1}b_2, \ldots, p^{-1}b_n; q, p^{-1}N)}{\chi(a_1, \ldots, a_n; b_1, \ldots, b_n; q, N)} \right),$$

where q temporarily denotes a prime, and the product is taken over all primes. It is almost immediate from (4) of § 6 that each factor with $q \neq p$ is equal to 1. We have only to prove that the factor with $q = p$ is equal to p^{-1}; and this, again using (4) of § 6, reduces to proving

$$C(a_1, \ldots, a_n; b_1, \ldots, b_n; p^{u+1}, N) = p^n C(p^{-1}a_1, \ldots, p^{-1}a_n; p^{-1}b_1, \ldots, p^{-1}b_n; p^u, p^{-1}N).$$

(Here the notation $C(m, N)$ of § 6 has been replaced by $C(a_1, \ldots, a_n; b_1, \ldots, b_n; m, N)$, to avoid confusion.) This last formula is however clear; it merely expresses that each solution of a congruence modulo p^u counts, trivially, as p^n solutions of the congruence obtained by multiplying both sides, and the modulus p^u, by p. This completes the proof.

LEMMA 7·2. *The assertions of lemma* 7·1 *all hold if the transformation* (3) *is*

$$x_j = x'_j \quad \text{for } i \neq j, \qquad x_j = px'_j + t_j,$$

for some j and some prime p, provided that there exists a positive integer m such that the congruence $Q \equiv N \pmod m$ of § 6 *implies $x_j \equiv t_j \pmod p$.*

Proof. This is trivial except as regards (5), which is proved as in lemma 7·1.

It will be convenient to write

$$\mu = a_1 a_2 a_3 a_4 (a_5 + \ldots + a_n), \mu' = a'_1 a'_2 a'_3 a'_4 (a'_5 + \ldots + a'_n), \tag{9}$$

$$\left.\begin{aligned} \nu &= \nu(a_1, \ldots, a_n; b_2, \ldots, b_n; N) = N + \frac{1}{4}\sum_{i=1}^{n} \frac{b_i^2}{a_i}, \\ \nu' &= \nu(a'_1, \ldots, a'_n; b'_1, \ldots, b'_n; N'). \end{aligned}\right\} \tag{7}$$

If in (3) each m_i is 1, then, for any integers t_i, it is trivial that all the assertions of lemma 7·1 hold; and further that $\nu = \nu'$ (provided that (2) is the equation derived from (1) by the substitution (3), without multiplying or dividing by any constant). Hence ν' may, in other cases, be calculated on the assumption that the t_i all vanish.

(*b*) If the condition (6) of § 6 is not satisfied, then there must be a prime p such that the left member, which is the greatest common divisor of the numbers $2a_ix_i+b_i, m$, is divisible by p (or by 4 if $p=2$). This may be expressed by the formulae

$$p|b_i \quad \text{for each } i \text{ with } \quad p|2a_i; \tag{8}$$

$$4|b_i \quad \text{for each } i \text{ with } \quad 2|a_i, \text{ if } p=2; \tag{9}$$

$$x_i \equiv t_i \pmod{p} \quad \text{for each } i \text{ with } \quad p\nmid a_i; \tag{10}$$

where in (10) the t_i satisfy $2a_it_i+b_i \equiv 0$ modulo p or 4; by (8), (9) these congruences are soluble.

LEMMA 7·3. (*i*). *If the equation* (1) *satisfies the necessary congruence condition but not the strong one, then there exists a prime* p *such that* (8) *and* (9) *hold, while* (10) *is implied by the congruence* $Q \equiv N$ *modulo* p (*if* $p \neq 2$) *or* 8 (*if* $p=2$), *where* Q *denotes the left member of* (1).

(*ii*) *If* $p \neq 2$, *or if* $p=2$ *and one of the* a_i *is oddly even, then* p *divides at least* $n-2$ *of the* a_i; *and the transformation*

$$x_i = x_i' \quad \text{if} \quad p|a_i, \qquad px_i'+t_i \quad \text{if} \quad p\nmid a_i, \tag{11}$$

takes (1) *into an equation of the shape* (2) *from which a factor* p *can be cancelled.*

(*iii*) *If* $p=2$, *and each* a_i *is either odd or divisible by* 4, *then* 2 *divides at least* $n-4$ *of the* a_i; *and the transformation* (11) *takes* (1) *into an equation of the shape* (2) *from which a factor* 4 *can be cancelled.*

Proof. (i) It is clear from the definitions in § 6, and the foregoing argument, that (8), and (9) if $p=2$, must hold for some p for which also, for some positive m (a multiple of p or of 4) $Q \equiv N \pmod{m}$ implies (10). It is also clear (see (4) and (7) of § 6) that this implication holds, if at all, for $m=p$ or 8.

(ii), (iii). The assertions regarding the cancellation of p or 4 after the transformation (11) are obvious. For $p \neq 2$, lemma 6·2 tells us that if p divides fewer than $n-2$ of the a_i, then $Q \equiv N \pmod{p}$ has always a solution satisfying (6) of § 6.

What remains to be proved for $p=2$ follows easily if we show, using (8) and putting $n-4$ or $n-5$ of the x_i equal to 0, that each of the congruences

$$\sum_{i=1}^{4}(a_ix_i^2+b_ix_i) \equiv N \pmod 8, \quad 2\nmid a_1a_2a_3, a_4 \equiv 2 \pmod 4, \tag{12}$$

$$\sum_{i=1}^{5}(a_ix_i^2+b_ix_i) \equiv N \pmod 8, \quad 2\nmid a_1a_2a_3a_4a_5, a_4 \equiv a_5 \pmod 4, \tag{13}$$

has a solution satisfying

$$2a_1x_1+b_1 \not\equiv 0 \pmod 4 \tag{14}$$

for every integer N.

The solubility of (13) and (14) follows from that of (12) and (14) by putting $x_4=x_5$. To solve (12) and (14), choose x_1 to satisfy (14). Now note that $a_ix_i^2+b_ix_i$ can be either odd or even for $i=2$ and for $i=3$ (4) takes two values differing by 4(2) modulo 8.

LEMMA 7·4. *Assume the hypotheses of lemma* 7·3, *choose* p *as in that lemma, and let the equation* (2) *be derived from* (1) *by making the substitution* (11) *and then cancelling a factor* p *or* 4 *according as* (*ii*) *or* (*iii*) *of lemma* 7·3 *is applicable. Then all the assertions of lemma* 7·1 *hold and also*

$$\mu' < \mu, \quad \frac{\nu'}{\mu'} \geqslant \frac{\nu}{\mu}, \quad \nu' < \nu. \tag{15}$$

Proof. That the assertions of lemma 7·1 hold follows from that lemma and lemma 7·2. It may be necessary to use both these lemmas, the second more than once; thus the argument proceeds by steps, the equation (1) of each but the first being the (2) of the preceding step. There should however be no risk of confusion in the notation.

Now suppose that part (ii) of lemma 7·3 is applicable; and (see remark following (7)) that all the t_i vanish. If the factor p were not cancelled we should have $N' = N$ and $a_i', b_i' = a_i, b_i$, except for at most two values (possibly none) of i, for which $a_i', b_i' = p^2 a_i, p b_i$. Now cancelling p we have

$$N' = p^{-1}N; \quad a_i', b_i' = p a_i, b_i \quad \text{or} \quad p^{-1}a_i, p^{-1}b_i,$$

with the first alternative applicable for at most two values of i. It is clear that this gives, using (6), (7),

$$\mu' \leqslant p^{-1}\mu, \quad \nu' = p^{-1}\nu,$$

whence (15) follows.

In case (iii) of lemma 7·3 the argument is similar.

LEMMA 7·5. *If the equation* (1) *satisfies the necessary congruence condition but not the strong one, then there exists an equation* (2) *satisfying the strong congruence condition and such that* (4), (5) *and* (15) *hold.*

Proof. Apply lemma 7·4 repeatedly; for the notation, see the remark at the beginning of the proof of lemma 7·4. At each step, any value of p (not necessarily the same each time) for which the assertions of lemma 7·3 hold may be chosen. The process stops after finitely many steps since the positive integer μ decreases at each step, by (15). After the last step, the impossibility of a further step shows, by lemma 7·3, that the final equation satisfies the strong congruence condition.

(*c*) We deduce from lemmas 6·5, 7·5

THEOREM 3. *Let $r(N)$ denote the number of solutions, in integers x_i, of the equation*

$$\sum_{i=1}^{n} (a_i x_i^2 + b_i x_i) = N,$$

where $n \geqslant 5$ and the a_i are positive integers and the b_i and N integers, such that

$$N + b_1^2/4a_1 + \ldots + b_n^2/4a_n > 0.$$

Then there exists an analytical approximation $\rho(N)$ (defined in (10) *of* §5) *to $r(N)$, such that $\rho(N) \geqslant 0$, with equality if and only if some congruence*

$$\sum_{i=1}^{n} (a_i x_i^2 + b_i x_i) \equiv N (\mathrm{mod}\, m)$$

(*with m a positive integer*) *is insoluble. And if every such congruence is soluble then the estimate*

$$\frac{r(N)}{\rho(N)} - 1 \ll \left(N + \frac{1}{4}\frac{b_1^2}{a_1} + \ldots + \frac{1}{4}\frac{b_n^2}{a_n}\right)^{\epsilon - \frac{1}{4}} (a_1 a_2 a_3 a_4)^{\epsilon + \frac{1}{4}} (a_5 + \ldots + a_n)^{\epsilon + \frac{1}{4}}$$

holds for every $\epsilon > 0$, with an implied constant depending only on n, ϵ, provided that (14) *of* §5 *holds.*

Proof. With the notation of the foregoing lemmas, the desired estimate is

$$\min\left\{1, \frac{r(N)}{\rho(N)} - 1\right\} \ll \nu^{\epsilon - \frac{1}{4}} \mu^{\epsilon + \frac{1}{4}}.$$

It follows at once, for ϵ less than $\frac{1}{4}$, from

$$\frac{r(N)}{\rho(N)} - 1 \ll \nu^{\epsilon-\frac{1}{4}}\mu^{\epsilon+\frac{1}{4}} \quad \text{if} \quad \nu > 2\mu. \tag{16}$$

To prove (16) for the case in which the given equation satisfies the strong congruence condition, we appeal to lemma 6·5, noting that $\nu > 2\mu$ (crudely) implies (14) of §5.

In the other case (16) must hold for the transformed equation of lemma 7·5, whence by that lemma we have either $2 \geqslant \nu'/\mu' > \nu/\mu$ or

$$\frac{r(N)}{\rho(N)} - 1 \ll \nu'^{\epsilon-\frac{1}{4}}\mu'^{\epsilon+\frac{1}{4}} < \nu^{\epsilon+\frac{1}{4}}\mu^{\epsilon+\frac{1}{4}}$$

using (15).

Putting $r(N) = 0, \rho(N) > 0$, and replacing ϵ by ϵ' such that $\frac{1+4\epsilon'}{1-4\epsilon'} = 1+\frac{1}{5}\epsilon$, the estimate (6) of theorem 1 follows.

8. Quadratic congruences

(*a*) The results of this section are valid for indefinite as well as for definite quadratic forms, and the assumption $n \geqslant 5$ is not needed.

As in Watson (1960), the matrix $A = A(f)$ of the quadratic form $f = f(x_1, \ldots, x_n)$ is defined to be the symmetric $n \times n$ matrix whose (i,j) element is $\partial^2 f/\partial x_i \partial x_j$. The discriminant $d = d(f)$ is defined in terms of the determinant $|A|$ by

$$d = (-1)^{\frac{1}{2}n}|A| \ (n \text{ even}), \quad \tfrac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}}|A| \ (n \text{ odd}). \tag{1}$$

When the coefficients of f are integers, d is an integer. In particular,

$$d(a_1x_1^2 + \ldots + a_nx_n^2) = \begin{cases} (-4)^{\frac{1}{2}n}a_1 \ldots a_n & (n \text{ even}) \\ (-4)^{\frac{1}{2}n-\frac{1}{2}}a_1 \ldots a_n & (n \text{ odd}) \end{cases} \tag{2}$$

for a diagonal form.

For the proof of theorem 2, it is clearly sufficient to examine what conditions must be satisfied by d and the prime power modulus p^t if the congruence

$$f(x_1, \ldots, x_n) + b_1x_1 + \ldots + b_nx_n \equiv N \pmod{p^t} \tag{3}$$

is not soluble in integers, although there exist integers y_i satisfying

$$f(y_1, \ldots, y_n) + b_1y_1 + \ldots + b_ny_n \equiv N \pmod{p^{t-1}}. \tag{4}$$

The case $t = 1$, in which this assumption is vacuous, is not excluded.

Denote the left member of (4) by $N - hp^{t-1}$, h being an integer; then the substitution $x_i \to x_i + y_i$ takes (3) into a congruence of the shape

$$f(x_1, \ldots, x_n) + c_1x_1 + \ldots + c_nx_n \equiv hp^{t-1} \pmod{p^t}, \tag{5}$$

which is also insoluble. Denote by a_{ij} the coefficient of x_ix_j in f.

The following lemma will simplify the investigation of the congruence (5):

Lemma 8·1. *Every n-ary quadratic form with integral coefficients can, for any prescribed prime power p^t, be taken, by a linear transformation of the variables which has integral coefficients with determinant prime to p, into a form f satisfying one of the following congruences, identically in the variables:*

$$f(x_1, x_2, 0, \ldots, 0) \equiv x_1x_2 \pmod{p^t} \quad (n \geqslant 2), \tag{6}$$

$$f \equiv \psi(x_1, x_2) \pmod{p} \quad (n \geqslant 2), \tag{7}$$

$$f \equiv a_{11}x_1^2 \pmod{p}, \quad p \nmid a_{11}, \tag{8}$$

$$f \equiv 0 \pmod{p}, \tag{9}$$

where ψ in (7) denotes a binary quadratic form whose discriminant is prime to p and not a quadratic residue modulo p, in case p is odd, and $d(\psi) \equiv -3 \pmod 8$ if $p = 2$.

Proof. For $p \neq 2$ the lemma follows from the classical result that every quadratic form can be diagonalized modulo p^t by a transformation of the kind allowed. The diagonal coefficients that do not divide by p can, with one exception, be chosen arbitrarily and taken to be $1, -1$ alternately. The remaining one (if any) can be chosen to be either -1 or $-q$, q any non-residue modulo p. Hence noting that $x_1^2 - x_2^2$ transforms into $x_1 x_2$, we have the result, with $\psi = x_1^2 - qx_2^2$. The result however follows at once from Watson (1960), theorem 32.

When $p = 2$, (8) or (9) must clearly hold after a suitable transformation if the a_{ij} $(i \neq j)$ are all even; and if not, Watson (1960), theorem 35, or an analogous result to be found at many places in the literature, shows at once that (6) or (7) can be satisfied, with

$$\psi = x_1^2 + x_1 x_2 + x_2^2.$$

(*b*) Theorem 2 will follow from the following lemma:

LEMMA 8·2. *Let f be a quadratic form with integral coefficients and discriminant d, and let $c_1, \ldots, c_n, h$ be any integers, p any prime, and t any positive integer. Then if (5) is insoluble*

$$p^{(n-3)t+1} | d. \tag{10}$$

Proof. Supposing the lemma false for some given n, p, choose $f, c_1, \ldots, c_n, h, t$ so that (5) is insoluble, (10) false, and t as small as possible; and assume by lemma 8·1 that one of (6) to (9) holds. We shall deduce a contradiction.

Now in case (6) (5) is obviously soluble, so one of (7), (8), (9) must hold. From any of these, and (1), it is easy to see that $p^{n-2} | d$, which with the negation of (10) gives the first two of

$$t \geqslant 2, n \geqslant 4, c_1 \equiv \ldots \equiv c_n \equiv 0 \pmod{p}. \tag{11}$$

For the last of these formulae, note that if $p \nmid c_1$ then $x_1, \ldots, x_n = p^{t-1}x_1', 0, \ldots, 0$ takes (5) into a linear congruence which is clearly soluble. A similar argument shows that

$$p^t | f(x_1, \ldots, x_n) \quad \text{implies} \quad p^t | c_1 x_1 + \ldots + c_n x_n \tag{12}$$

(for integers x_i).

If (9) holds, we see from (11) that a factor p will cancel from the congruence (5), taking it into a congruence, of the same shape but with $p^{-1}f, p^{-1}c_i, t-1$ for f, c_i, t, which is also insoluble. Since $p^{(3-n)(t-1)-1}d(p^{-1}f) = p^{(3-n)t-4}d(f)$ cannot be an integer if $p^{(3-n)t-1}d(f)$ is not, that is if (10) fails, this contradicts the assumption that t is as small as possible.

If (8) holds we argue similarly, but putting px_1 for x_1 before cancelling p from (5). The new insoluble congruence so obtained has again $t-1$ in place of t, and $p^{2-n}d$ in place of d, hence $p^{(3-n)t-2}d$ in place of $p^{(3-n)t-1}d$. Again the assumption that t is as small as possible is contradicted.

Hence (7) must hold; but now the argument of lemma 8·1 tells us a little more, namely that we may suppose $f \equiv \psi(x_1, x_2) + pg(x_3, x_4) \pmod{p^t}$, for an integral form g. And applying lemma 8·1 to g, we see that we may suppose f to satisfy one of the congruences

$$f(0, 0, x_3, x_4, 0, \ldots, 0) \equiv px_3x_4 \pmod{p^t}, \tag{13}$$

$$f \equiv \psi(x_1, x_2) + p\psi(x_3, x_4) \pmod{p^2}, \tag{14}$$

$$f \equiv \psi(x_1, x_2) + pax_3^2 \pmod{p^2}, \quad p \nmid a, \tag{15}$$

$$f \equiv \psi(x_1, x_2) \pmod{p^2}. \tag{16}$$

In case (13) it follows from (11) that (5) is soluble, contrary to hypothesis. In cases (15), (16) we see from (1) that $p^{2(n-3)+1} | d$, whence the falsity of (10) gives $t \geqslant 3$ and so (12) gives $p^2 | c_3, \ldots, c_n$. It follows that after putting px_1, px_2 for x_1, x_2 in each of these two cases, and also px_3 for x_3 in case (15), a factor p^2 will cancel from (5). The new insoluble congruence so obtained has $t-2$ for t and either $p^{6-2n}d$ or $p^{4-2n}d$ for d; a straightforward calculation like that in cases (8), (9) shows that it again gives a contradiction with the assumption that t is as small as possible.

There remains only case (14), in which we drop the assumption that (10) is false and prove (5) soluble. In doing this we may take $n = 4$; the argument of lemma 8·1 shows that we may assume $f = \psi(x_1, x_2) + p\psi(x_3, x_4)$. We put px_3, px_4, x_1, x_2 for x_1, x_2, x_3, x_4, and so take f into pf; whence cancelling p from (5) we have a congruence of the same shape, with the same f, but with $t-1$ for t. Finally, repeating this argument $t-1$ times, we have only to show that $\psi \equiv h \pmod{p}$ is soluble. This is trivial for $p = 2$ and for $p | h$, and follows in other cases from lemma 6·2, so the proof is complete.

(*c*) *Proof of theorem* 2. Theorem 2 asserts in effect that the congruence (2) of §1 is soluble for every positive integer m if it is soluble for all m satisfying

$$m^{n-3} \prod_{p|d} p | d. \tag{17}$$

This hypothesis is equivalent to the solubility of the congruence for $m | m_1$, or for $m = m_1$, where m_1 is the greatest positive m satisfying (17). The further assertion of theorem 2 that this condition may be weakened to $m = m_0$ (or to $m | m_0$) for some m_0 satisfying (17), hence dividing m_1, and depending only on f, follows trivially. Now it is sufficient to take m to be a prime power p^t, and when we do so (17) reduces to (10), and the congruence (2) of §1 to (3).

Hence if the theorem is false there exist $f, b_1, \ldots, b_n, N, p$ such that (3) is insoluble for some t not satisfying (10), although it becomes soluble when t is replaced by any (smaller) number satisfying (10). Choosing the least t for which (3) is insoluble, (4) is soluble, some congruence of the shape (5) is insoluble, and lemma 8·2 gives the contradiction that t does satisfy (10).

9. Conclusion

(*a*) In this section, $f = f(x_1, \ldots, x_n)$ is a positive quadratic form, whose coefficients a_{ij} are integers. It is convenient to write

$$f_i = f(x_1, \ldots, x_i, 0, \ldots, 0), \quad \text{for} \quad i = 1, \ldots, n-1. \tag{1}$$

Each f_i is a positive i-ary form, so $d(f_i) \neq 0$. The assumption that f is positive gives $a_{ij}^2 < 4a_{ii}a_{jj}$, so

$$0 < |d(f_i)| \ll a_{11} \ldots a_{ii}. \tag{2}$$

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

Theorem 2 is applicable to the f_i with $i \geqslant 4$, and gives

$$m_0^{i-3}(f_i) \leqslant |d(f_i)|, \quad i = 4, \ldots, n-1. \tag{3}$$

The coefficients of the linear terms, also the constant term, in any equation or congruence of the shape of (1) or (2) of §1, are to be understood to be integers.

LEMMA 9·1. *If the congruence* (2) *of* §1, *that is*

$$f(x_1, \ldots, x_n) + b_1 x_1 + \ldots + b_n x_n \equiv N \pmod{m}, \tag{4}$$

is soluble (*in integers* x_i) *then it has a solution in which its left member does not exceed a bound* $B(f, m)$ *which depends only on* f *and the positive integer* m, *and satisfies*

$$B(f, m) \leqslant \frac{1}{4} \sum_{i=1}^{n}{}' a_{ii}(m, m_0(f_{i-1}))^2, \tag{5}$$

where the notation is that of theorem 2, *and* (1) *above, and the accent indicates that* $(m, m_0(f_{i-1}))$ *is to be interpreted as* m *for* $i \leqslant 4$.

Proof. The proof is by induction from $n-1$ to n. It suffices to consider the case $n \geqslant 5$; the proof for $n \geqslant 1$ and the inductive steps to $n = 2, 3, 4$ are similar but simpler. Consider the congruence, say

$$f_{n-1}(x_1, \ldots, x_{n-1}) + b_1' x_1 + \ldots + b_{n-1}' x_{n-1} \equiv N - a_{nn} t_n^2 - b_n t_n \pmod{m}, \tag{6}$$

which is derived from (4) by giving a suitably chosen value t_n to x_n. Note also that we may suppose without loss of generality

$$N = f(y_1, \ldots, y_n) + b_1 y_1 + \ldots + b_n y_n$$

for some integers y_i (the values of the x_i in the solution of (4) in the hypothesis of the lemma). Consider also the congruence

$$f_{n-1}(x_1, \ldots, x_{n-1}) + b_1' x_1 + \ldots + b_{n-1}' x_{n-1} \equiv N - a_{nn} t_n^2 - b_n t_n \pmod{m_0(f_{n-1})}. \tag{7}$$

Clearly (7) is soluble in integers $x_1, \ldots, x_{n-1}$ (a solution is $x_1, \ldots, x_{n-1} = y_1, \ldots, y_{n-1}$) if $t_n = y_n + h m_0(f_{n-1})$, for any integer h. By theorem 2, (6) is also soluble for such a choice of t_n, whence obviously for $t_n = y_n + h m_0(f_{n-1}) + km$ (h, k any integers). That is, (6) is soluble for every t_n congruent to y_n modulo the greatest common divisor $(m, m_0(f_{n-1}))$ of $m, m_0(f_{n-1})$. There exists such a t_n with

$$|t_n + b_n/2a_{nn}| \leqslant \tfrac{1}{2}(m, m_0(f_{n-1})),$$

whence

$$a_{nn} t_n^2 + b_n t_n \leqslant a_{nn}(t_n + b_n/2a_{nn})^2 \leqslant \tfrac{1}{4} a_{nn}(m, m_0(f_{n-1}))^2.$$

Now the existence of $B(f, m)$, and the inequality (5), both follow from the inductive hypothesis. (The argument is a little more subtle than it appears, since the b_i' depend on t_n; this however does not matter since the m_0 of theorem 2 does not depend on the b_i.)

LEMMA 9·2. *The bound* $B(f, m)$ *of lemma* 9·1 *satisfies*

$$B(f, m) \ll |d| + |d|^{9/n} + |(\min f)^{-3} d|^{1/(n-3)} m^2 \tag{8}$$

(*for* $n \geqslant 4$), *where* $\min f$ *denotes the minimum of* f, *and* $d = d(f)$.

Proof. Without loss of generality, we assume

$$a_{11} \leqslant \ldots \leqslant a_{nn} \tag{9}$$

and

$$a_{11} \ldots a_{nn} \ll |d|. \tag{10}$$

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

To justify the assumption (10), note that, with any definition of reduction, a reduced form satisfies such an inequality; also that every form is equivalent to a reduced form, and $B(f,m)$ is invariant under equivalence.

The argument of lemma 9·1 shows that $m_0(f)\,|m_0(f_{n-1})$ if $n \geqslant 5$, whence by (2), (3)

$$m_0^2(f_{i-1}) \leqslant m_0^2(f_5) \leqslant |d(f_5)| \ll a_{11} \dots a_{55} \quad \text{for} \quad i \geqslant 6,$$

and $m_0^2(f_4) \ll a_{11}^2 \dots a_{44}^2$. These with (5), (9) give

$$B(f,m) \ll a_{44}m^2 + (a_{11} \dots a_{44})^2 a_{55} + a_{11} \dots a_{55}a_{nn}.$$

Here the last term on the right is $\ll |d|$ by (10), except for $n \leqslant 5$, in which case it may be omitted. Similarly, the second term may be replaced by $|d|^{9/n}$. To estimate the first term notice that

$$(\min f)^3 a_{44}^{n-3} \ll a_{11}^3 a_{44}^{n-3} \leqslant a_{11} \dots a_{nn} \ll |d|,$$

by (9), (10).

(*b*) It is necessary to transform the general n-ary form ($n \geqslant 5$) into a 5-ary diagonal form with least possible discriminant. This is done by putting $y_6 = \dots = y_n = 0$, if $n \geqslant 6$, in the following lemma:

LEMMA 9·3. *By a substitution $x_i = L_i(y_i, \dots, y_n), i = 1, \dots, n$, where the L_i are suitably chosen linear forms, with integral coefficients whose determinant is not zero, f can be taken into a diagonal form $a_1y_1^2 + \dots + a_ny_n^2$, where the a_i are positive integers satisfying $a_1 = \min f$,*

$$a_1 \dots a_i \ll |d|^{i/(n+1-i)}, \quad i = 1, \dots, n, \tag{11}$$

and

$$a_2 \dots a_i \ll |a_1 d|^{(i-1)/(n+1-i)}, \quad i = 2, \dots, n. \tag{12}$$

Proof. By a preliminary integral unimodular transformation we may, as is well known, suppose that the leading coefficient a_{11} of f is equal to its minimum. By another such transformation, affecting $x_2, \dots, x_n$ only and not altering the leading coefficient, we can take $a_{12}x_2 + \dots + a_{1n}x_n$ into a multiple of x_2; that is, we may suppose $f = a_1x_1^2 + a_{12}x_1x_2 + \dots$, where the terms not written do not involve x_1, and $a_1 = \min f$. The estimate $a_1 \ll |d|^{1/n}$, which is well known and follows at once from (9), (10), is the case $i = 1$ of (11).

With these preliminaries, f goes on putting $2a_1x_2$ for x_2 and then $y_1 - a_{12}x_2$ for x_1 into a form, say f', which is clearly of the shape $a_1y_1^2 + \phi$, $\phi = \phi(x_2, \dots, x_n)$. Now on the one hand, as f' arises from f by a substitution with determinant $2a_1$, $d(f') = 4a_1^2 d(f)$; on the other hand (1) of §8 gives $d(f') = a_1 d(\phi)$ or $-4a_1 d(\phi)$, according as n is odd or even. So $d(\phi) \ll a_1|d(f)|$.

Now the proof of the lemma can be completed by induction. (For the possibility of diagonalizing f the induction is on n; for the estimates (11), (12), on i.) The estimate just obtained shows that (12) follows from (11) with $n-1, \phi, i-1$ for n, f, i. And the estimate $a_1 \ll |d|^{1/n}$ shows that (12) implies (11).

To avoid breaking the thread of the argument later, we deduce from lemmas 9·2, 9·3:

LEMMA 9·4. *If $n \geqslant 5$, then there exist linear forms L_i' in 5 variables, each with integral coefficients, such that the substitution $x_i = L_i'(y_1, \dots, y_5), i = 1, \dots, n$ takes f into a positive, diagonal form $g = a_1y_1^2 + \dots + a_5y_5^2$, with*

$$a_1 \dots a_5 \ll |d|^{5/(n-4)}, \quad m_0^2(g) \ll |d|^{5/(n-4)}, \tag{13}$$

$$B(f, m_0(g)) \ll |d| + |d|^{5/(n-4)+1/n}, \tag{14}$$

where $d = d(f)$ and the notation is that of theorem 2 and lemma 9·1.

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

Proof. Theorem 2, with 5, g for n, f, and lemma 9·3 give all the assertions except (14). Since $9/n \leqslant 1$ for $n \geqslant 9$, $\leqslant 5/(n-4)$ for $5 \leqslant n \leqslant 8$, lemma 9·2 gives (14) if the last term of (8) can be suitably estimated when m is replaced by $m_0(g)$. This term is

$$\ll |a_1^{-3}d|^{1/(n-3)} a_1 \dots a_5 \ll a_1^{-3/(n-3)+1+4/(n-4)} |d|^{1/(n-3)+4/(n-4)},$$

by (13), and (12) with $i = 5$. The exponent of a_1 is positive, so a_1 may (by (11) with $i = 1$) be replaced by $|d|^{1/n}$; now (14) follows since

$$\frac{1}{n}\left(-\frac{3}{n-3}+1+\frac{4}{n-4}\right)+\frac{1}{n-3}+\frac{4}{n-4} = \frac{5}{n-4}+\frac{1}{n}.$$

(*c*) *Completion of proof of theorem* 1. With the hypothesis of theorem 1 that the congruence (4) of this section is soluble, (14) shows that there exist integers $t_1, \dots, t_n, N'$ such that

$$f(t_1, \dots, t_n) + b_1 t_1 + \dots + b_n t_n = N'$$

and
$$m_0(g) \mid N - N', \quad \max(0, N') \ll |d| + |d|^{5/(n-4)+1/n}. \tag{15}$$

Now the insoluble equation (1) of theorem 1 goes by the trivial substitution $x_i \to x_i + t_i$ into an equation of the same shape, say $f(x_1, \dots) + b_1' x_1 + \dots = N - N'$, which is also insoluble.

This in turn goes into an insoluble equation of the shape

$$g(y_1, \dots, y_5) + b_1'' y_1 + \dots + b_5'' y_5 = N - N', \tag{16}$$

by the substitution of lemma 9·4.

Now the congruence $g(y_1, \dots) + b_1'' y_1 + \dots \equiv N - N' \pmod{m}$ is by theorem 2 soluble for every positive integer m, since by (15) it is trivially soluble (with each y_i zero) when $m = m_0(g)$. That is, the hypotheses of theorem 1 all hold for the equation (16), except that its right member may not be positive. And since g is diagonal we may appeal to the case of theorem 1 that has already been proved (§7, theorem 3), that is, use (6) of §1 for $n = 5, f = g$. This gives

$$\max(0, N - N') \ll (a_1 \dots a_5)^{1+\epsilon} \ll |d|^{5/(n-4)+1/n}$$

using (13) and putting $\epsilon = (n-4)/5n$.

From this estimate and (15), the estimates (3) and (4) of theorem 1 follow at once.

Now assume $n \geqslant 6$ and f diagonal. A similar but simpler argument shows that (with (1) of §2 insoluble, though the corresponding congruence is always soluble)

$$N \ll (a_1 \dots a_5)^{1+\epsilon} + a_1 \dots a_5 (a_5 + \dots + a_n).$$

Putting $\epsilon = 1/n$ and supposing as we may that $a_n = \max a_i$, this gives $N \ll a_1 \dots a_5 a_n$, implying (5) of theorem 1. Thus the proof of theorem 1 is complete.

The arguments could be carried a little further; for example, the constant in (5) of theorem 1 is independent of n, while the estimate for $n \geqslant 10$ can be replaced, with the notation of (1), by

$$N \ll |d(f_9)|^{10/9} + (\max_{i>9} a_{ii}) |d(f_9)|^{2/7}.$$

I am indebted to Miss Pitman for permission to use her unpublished work referred to in §3; also to Professor Davenport for reading an earlier version of this paper, making many helpful comments, and drawing my attention to Miss Pitman's work. I discussed the

problem at the Number Theory Conference at Boulder, Colorado in July 1959. I therefore take the opportunity of thanking the American Mathematical Society and the Office of Naval Research for making it possible for me to visit the United States.

References

Birch, B. J. & Davenport, H. 1958 *Acta math., Stockh.*, **100**, 259–279.
Davenport, H. 1959 *Phil. Trans.* A, **251**, 193–232.
Ross, A. E. & Pall, G. 1946 *Amer. J. Math.* **68**, 59–65.
Tartakowsky, W. 1929 *Bull. Acad. Sci. U.R.S.S.* (7), **2**, 111–122 and 165–196.
Vinogradov, I. M. 1954 *The method of trigonometrical sums in the theory of numbers*. Translated, revised and annotated by K. F. Roth & A. Davenport. London: Interscience Publishers.
Watson, G. L. 1953 *Proc. Lond. Math. Soc.* (3), **3**, 170–181.
Watson, G. L. 1960 *Integral quadratic forms*. Cambridge University Press (Cambridge Tract no. 51).

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