[5] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeitschr. 2 (1918), pp. 52-154.

[6] W. Narkiewicz, *On algebraic number fields with nonunique factorization*, Coll. Math. 12 (1964), pp. 59-68.

[7] — *On algebraic number fields with nonunique factorization II*, Colloq. Math. 15 (1966), pp. 49-58.

[8] — *On natural numbers having unique factorization in a quadratic number field*, Bull. Acad. Pol. Sci. 14 (1966), pp. 17-18.

MATHEMATICAL INSTITUTE OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 9. 9. 1965

ACTA ARITHMETICA
XII (1966)

The representation of primes by cubic polynomials

by

P. A. B. Pleasants (Cambridge)

1. Introduction. Let

$$\phi(x_1, \ldots, x_n) = \phi(\boldsymbol{x}) = C(\boldsymbol{x})+Q(\boldsymbol{x})+L(\boldsymbol{x})+N \tag{1}$$

be a cubic polynomial with integral coefficients, where $C(\boldsymbol{x})$ denotes the cubic part of ϕ, $Q(\boldsymbol{x})$ the quadratic part, and so on. An obvious necessary condition for $\phi(\boldsymbol{x})$ to represent infinitely many primes is that for any given integer $m > 1$ there is some integer point $\boldsymbol{x}$ for which $\phi(\boldsymbol{x})$ is not divisible by m. The object of the present paper is to prove that in certain circumstances of reasonable generality, this necessary condition is also sufficient.

The investigation is based on the Hardy-Littlewood method, as modified by Davenport in his treatment of homogeneous cubic equations ([1] and [2]). Let $\mathscr{P}$ be any parallelepiped of suitable shape (that is, with bounding hyperplanes parallel to certain particular hyperplanes) in n dimensional space, such that $C(\boldsymbol{x})$ is positive in and on the boundary of $\mathscr{P}$. Let P be a large positive number. Then the number of integer points $\boldsymbol{x}$ in the expanded parallelepiped $P\mathscr{P}$ is asymptotic to VP^n, where V is the volume of $\mathscr{P}$, and the values of $\phi(\boldsymbol{x})$ at these points lie between fixed positive multiples of P^3. Let $\mathscr{M}(P)$ denote the number of these integer points for which the value of $\phi(\boldsymbol{x})$ is a prime. It is reasonable to expect that $\mathscr{M}(P)$ should be approximately proportional to $VP^n/\log P^3$ for large P, subject to the above necessary condition.

In the present paper we shall prove, subject to a further condition, that

$$\mathscr{M}(P) \sim \frac{VP^n}{\log P^3}\mathfrak{S} \quad \text{as} \quad P \to \infty, \tag{2}$$

where $\mathfrak{S}$ is a positive constant (the 'singular series' for the problem) depending only on $\phi(\boldsymbol{x})$. Following Davenport and Lewis [4] we define the invariant $h = h(C)$ to be the least positive integer for which $C(\boldsymbol{x})$

is representable identically as

$$L_1Q_1+\ldots+L_hQ_h, \tag{3}$$

where $L_1, \ldots, L_h$ and $Q_1, \ldots, Q_h$ are linear and quadratic forms respectively, with integral coefficients (or, equivalently, with rational coefficients). Another form of the definition is to say that $n-h$ is the greatest dimension of any linear space contained in the hypersurface $C(\boldsymbol{x}) = 0$. Plainly $1 \leqslant h \leqslant n$. We shall state our principal result in terms of an invariant h^* which is closely related to h and which arises naturally from the analysis in the present instance.

DEFINITION. *We define $h^* = h^*(C)$ to be the greatest integer with the property that there exists a linear substitution $\boldsymbol{x} = \boldsymbol{T}\boldsymbol{y}$, where $\boldsymbol{T}$ is a non-singular integral $n \times n$ matrix, such that*

$$C(\boldsymbol{x}) = C_1(\boldsymbol{y})+\ldots+C_s(\boldsymbol{y}) \tag{4}$$

and

$$\sum_{i=1}^{s} h(C_i) = h^*, \tag{5}$$

where $C_1, \ldots, C_s$ are cubic forms in disjoint sets of variables.

It is clear from this definition that h^* is a rational invariant of C and that $h \leqslant h^* \leqslant n$. We can now state our main result as follows.

THEOREM. *If $h^* \geqslant 8$, and if, for any positive integer $m > 1$, there is some $\boldsymbol{x}$ such that $\phi(\boldsymbol{x}) \not\equiv 0 \pmod m$, then the asymptotic formula* (2) *holds.*

The condition $h^* \geqslant 8$ enables us to estimate a cubic exponential sum, on the same general lines as in Davenport and Lewis [4]. But as we have also to deal with an exponential sum extended over primes, we need the estimate for the cubic exponential sum in a form which is applicable beyond the range considered by Davenport or by Davenport and Lewis. This entails a repetition of much of their work in a more precise form. There are also some complications connected with the 'splitting' of cubic forms, and it is for this reason that we have to restrict ourselves to parallelepipeds $\mathscr{P}$ of a particular shape. On the other hand, the treatment of the singular series and the singular integral for the present problem is much simpler than the corresponding treatment for a purely cubic equation.

2. Bilinear equations. It is convenient in the present work to write a cubic form $C(\boldsymbol{x})$ as

$$C(\boldsymbol{x}) = \sum_{1\leqslant i\leqslant j\leqslant k\leqslant n} c_{ijk}x_ix_jx_k, \tag{6}$$

so as to avoid the numerical coefficients 3 and 6 which occur when the summations run independently from 1 to n. With $C(\boldsymbol{x})$ we associate the bilinear forms

$$B_j(\boldsymbol{x}|\boldsymbol{y}) = \sum_{i=1}^{n}\sum_{k=1}^{n} c'_{ijk}x_iy_k \quad (1 \leqslant j \leqslant n), \tag{7}$$

where c'_{ijk} is a symmetrical function of the three suffixes and is given, for $i \leqslant j \leqslant k$, by

$$c'_{ijk} = \begin{cases} 6c_{ijk} & \text{if} \quad i=j=k, \\ 2c_{ijk} & \text{if} \quad i=j<k \text{ or } i<j=k, \\ c_{ijk} & \text{if} \quad i<j<k. \end{cases} \tag{8}$$

Throughout this section the cubic form $C(\boldsymbol{x})$ is supposed to be fixed, and $h = h(C)$ denotes the invariant defined in § 1.

LEMMA 1. *Suppose that $n-h < r \leqslant n$ and that R is large. Then the number of integer points $\boldsymbol{x}$ with $|\boldsymbol{x}| < R$ for which the bilinear equations*

$$B_j(\boldsymbol{x}|\boldsymbol{y}) = 0 \quad (i \leqslant j \leqslant n) \tag{9}$$

have exactly r linearly independent solutions in $\boldsymbol{y}$ is $\ll R^{2n-h-r}$.

Proof. This is a slight generalization of Lemma 3 of [2], which is itself the case $h = n$ of the present lemma. (If $h = n$ then $C(\boldsymbol{x})$ does not represent 0, and this was the hypothesis of the lemma just mentioned.) The generalization in question has already occurred as Lemma 2 of [4], but we outline the proof for the sake of completeness.

We define $\mathfrak{X}$ as in the proof of Lemma 3 of [2], and we assume that $\mathfrak{X}$ contains more than AR^{2n-h-r} points $\boldsymbol{x}$, and reach a contradiction if A is sufficiently large. The proof proceeds as in the lemma cited, except that the rank of the matrix of partial derivatives is now at most $h-n+r-1$ instead of being at most $r-1$. At the conclusion of the proof we have $h-n+r-1$ homogeneous linear equations in the r unknowns $K_1, \ldots, K_r$. Their solutions provide a linear space of points $\boldsymbol{Y}$ of dimension at least $n-h+1$, and $C(\boldsymbol{Y}) = 0$ identically on this linear space. This contradicts the definition of h, since $n-h$ is the greatest dimension of any linear space contained in the cubic cone $C(\boldsymbol{x}) = 0$. This proves the lemma.

DEFINITION. *A cubic form $C(\boldsymbol{x})$ is said to split if there exists a linear substitution $\boldsymbol{x} = \boldsymbol{T}\boldsymbol{y}$, where $\boldsymbol{T}$ is a non-singular integral $n \times n$ matrix, such that*

$$C(\boldsymbol{x}) = C_1(\boldsymbol{y})+C_2(\boldsymbol{y}) \tag{10}$$

identically, where C_1, C_2 are cubic forms, neither vanishing identically, in two disjoint sets of n_1 and n_2 variables respectively. ($n_1+n_2 = n$.)

LEMMA 2. *If $C(\boldsymbol{x})$ does not split, and R is large, the number of pairs $\boldsymbol{x}, \boldsymbol{y}$ of integer points which satisfy* (9) *and*

$$0 < |\boldsymbol{x}| < R, \quad 0 < |\boldsymbol{y}| < R \tag{11}$$

is $\leqslant R^{2n-h-n^{-1}}(\log R)^c$, *where c is a positive constant.*

Proof. We follow the arguments of Lemma 6 of [2]. We suppose that there are more than $R^{2n-h-n^{-1}}(\log R)^c$ pairs of points $\boldsymbol{x}, \boldsymbol{y}$, and reach a contradiction if c is sufficiently large.

For $1 \leqslant r \leqslant n$, let $\mathfrak{X}_r$ denote the set of integer points with $0 < |\boldsymbol{x}| < R$ for which the equations (9) have exactly r linearly independent solutions in $\boldsymbol{y}$. Then there is some r for which there are more than $n^{-1}R^{2n-h-n^{-1}}(\log R)^c$ pairs $\boldsymbol{x}, \boldsymbol{y}$, satisfying (9) and (11) and with $\boldsymbol{x}$ in $\mathfrak{X}_r$.

Let $N(\boldsymbol{x})$ denote the number of these pairs for a particular $\boldsymbol{x}$ in $\mathfrak{X}_r$. Then

$$\sum_{\boldsymbol{x}} N(\boldsymbol{x}) > n^{-1}R^{2n-h-n^{-1}}(\log R)^c. \tag{12}$$

Further, by Lemma 1 above, if $r > n-h$,

$$\sum_{\boldsymbol{x}} 1 \ll R^{2n-h-r}, \tag{13}$$

and this estimate remains trivially valid if $r \leqslant n-h$. We divide the points $\boldsymbol{x}$ in $\mathfrak{X}_r$ into subsets, placing in the sth subset $(s = 0, 1, \ldots)$ those for which

$$c_1 R^r 2^{-s-1} \leqslant N(\boldsymbol{x}) < c_1 R^r 2^{-s},$$

where c_1 is a constant so chosen (as it can be) that $N(\boldsymbol{x}) < c_1 R^r$ for all $\boldsymbol{x}$ in $\mathfrak{X}_r$. Since the parameter s takes $\ll \log R$ values, there must exist some subset which contributes an amount $\gg R^{2n-h-n^{-1}}(\log R)^{c-1}$ to the sum (12). If ϱ is defined by $2^s = R^\varrho$, the number of points $\boldsymbol{x}$ in the subset is

$$\gg R^{2n-h-n^{-1}-(r-\varrho)}(\log R)^{c-1}, \tag{14}$$

and to each of these points $\boldsymbol{x}$ there correspond $\gg R^{r-\varrho}$ points $\boldsymbol{y}$. By (13) we must have $0 \leqslant \varrho < n^{-1}$.

For each point $\boldsymbol{x}$ in this subset we choose a minimal basis $\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(r)}$ for the solutions of the bilinear equations, in accordance with Lemma 5 of [2]. As in the proof of Lemma 6 of [2] we have

$$|\boldsymbol{y}^{(1)}| \ldots |\boldsymbol{y}^{(r)}| \ll R^\varrho.$$

Here $|\boldsymbol{y}^{(j)}| = U_j$ is a positive integer, and to a given value of U_j there correspond $\ll U_j^{n-1}$ possibilities for the point $\boldsymbol{y}^{(j)}$. Hence the number of possibilities, independent of $\boldsymbol{x}$, for the minimal basis is

$$\ll \sum_{U_1 \ldots U_r \ll R^\varrho} (U_1 \ldots U_r)^{n-1} \ll R^{\varrho(n-1)} \sum_{U \ll R^\varrho} d_r(U),$$

where $d_r(U)$ denotes the number of ways of expressing U as a product of r positive integers. By a well known estimate,

$$\sum_{U \leqslant M} d_r(U) \ll M(\log M)^{r-1},$$

so the number of possibilities for the minimal basis is

$$\ll R^{n\varrho}(\log R)^{r-1}.$$

Since the number of points $\boldsymbol{x}$ satisfies (14), there must be some minimal basis which occurs for a set of points $\boldsymbol{x}$ numbering

$$\gg R^{2n-h-n^{-1}-r-(n-1)\varrho}(\log R)^{c-r}.$$

All points $\boldsymbol{x}$ which give rise to this basis constitute a lattice, and provided $c > r$ the last inequality shows that the dimension of this lattice must be at least $2n-h-r$, since $\varrho < 1/n$.

Hence there exist $2n-h-r$ points $\boldsymbol{x}^{(p)}$ and r points $\boldsymbol{y}^{(q)}$ such that

$$B_j(\boldsymbol{x}^{(p)}|\boldsymbol{y}^{(q)}) = 0$$

for each choice of p and q. Each set of points is linearly independent.

The two linear spaces, of dimensions $2n-h-r$ and r, generated by these sets of points intersect in a linear space of dimension at least $(2n-h-r)+r-n = n-h$. If they intersected in a space of higher dimension than this we should have a contradiction to the definition of h, since all points $\boldsymbol{z}$ of the intersection are representable as linear combinations both of the points $\boldsymbol{x}^{(p)}$ and of the points $\boldsymbol{y}^{(q)}$, and therefore satisfy $C(\boldsymbol{z}) = 0$.

Hence there exist $n-r$ of the points $\boldsymbol{x}^{(p)}$ which together with the r points $\boldsymbol{y}^{(q)}$ form a linearly independent set of n points. The substitution

$$\boldsymbol{x} = u_1\boldsymbol{x}^{(1)} + \ldots + v_1\boldsymbol{y}^{(1)} + \ldots$$

from $x_1, \ldots, x_n$ to $u_1, \ldots, u_{n-r}, v_1, \ldots, v_r$ gives

$$C(\boldsymbol{x}) = C_1(u_1, \ldots, u_{n-r}) + C_2(v_1, \ldots, v_r)$$

identically, as in the proof of Lemma 6 of [2]. This contradicts the hypothesis that $C(\boldsymbol{x})$ does not split, and the proof is complete.

3. The cubic exponential sum: estimation in terms of $S^*(\alpha, \boldsymbol{B})$.

We return to the consideration of a cubic polynomial $\phi(\boldsymbol{x})$ of the type (1), where $C(\boldsymbol{x})$ has invariant $h^* = h^*(C)$.

LEMMA 3. *There exists a non-singular rational linear substitution $\boldsymbol{x} = \boldsymbol{U}\boldsymbol{z}$ with the following properties:*

(i) *integer points $\boldsymbol{x}$ correspond to integer points $\boldsymbol{z}$ whose coordinates satisfy certain homogeneous linear congruences to a fixed modulus d;*

(ii) *we have*

$$\phi(\boldsymbol{x}) = \psi_1(\boldsymbol{z})+\ldots+\psi_s(\boldsymbol{z}) \tag{15}$$

identically, where $\psi_i(\boldsymbol{z})$ is a cubic polynomial with rational coefficients and $d^3\psi_i(\boldsymbol{z})$ has integral coefficients;

(iii) *the cubic part $C_i(\boldsymbol{z})$ of $\psi_i(\boldsymbol{z})$ is a form in n_i variables, where $n_1+\ldots+n_s \leqslant n$, and the sets of variables are disjoint;*

(iv) *each form $C_i(\boldsymbol{z})$, considered as a form in n_i variables, does not split;*

(v) *we have*

$$h(C_1)+\ldots+h(C_s) = h^*. \tag{16}$$

Proof. We can suppose that none of the cubic forms $C_i(\boldsymbol{y})$ ($i = 1, \ldots, s$) in the expression (4) splits. For if, say, $C_1(\boldsymbol{y})$ splits a further non-singular integral linear substitution gives an expression for $C(\boldsymbol{x})$ in the form

$$C(\boldsymbol{x}) = C_1'(\boldsymbol{z})+C_1''(\boldsymbol{z})+C_2(\boldsymbol{z})+\ldots+C_s(\boldsymbol{z}).$$

It is clear that $h(C_1')+h(C_1'') \geqslant h(C_1)$ [1], since representations of C_1' and C_1'' as $\sum L_\nu Q_\nu$ lead to a similar representation of C_1, and hence, by the definition of h^*, $h(C_1')+h(C_1'') = h(C_1)$. Thus $h(C_1')+\ldots+h(C_s) = h^*$. Repeating this process at most n times we obtain an integral non-singular substitution $\boldsymbol{x} = \boldsymbol{T}\boldsymbol{y}$ which gives an expression for $C(\boldsymbol{x})$ of the type (4) such that (5) is satisfied and none of the forms $C_i(\boldsymbol{y})$ splits for $i = 1, \ldots, s$.

In the substitution $\boldsymbol{x} = \boldsymbol{T}\boldsymbol{y}$, integer points $\boldsymbol{y}$ give rise to integer points $\boldsymbol{x}$, but not necessarily conversely. If $d = |\det \boldsymbol{T}|$, then the points $\boldsymbol{y}$ which correspond to integer points $\boldsymbol{x}$ consist of all points $\boldsymbol{y} = d^{-1}\boldsymbol{z}$, where $\boldsymbol{z}$ is an integer point whose coordinates satisfy certain homogeneous linear congruences to the modulus d. Taking $\boldsymbol{U} = d^{-1}\boldsymbol{T}$, we have $\boldsymbol{x} = \boldsymbol{U}\boldsymbol{z}$, and on replacing $C_i(d^{-1}\boldsymbol{z})$ by $C_i(\boldsymbol{z})$ in our notation, we obtain all the results stated.

We consider now cubic exponential sums of the form

$$S(\alpha; \phi, \mathscr{R}) = \sum_{\boldsymbol{x} \in P\mathscr{R}} e\big(\alpha\phi(\boldsymbol{x})\big), \tag{17}$$

where $\phi(\boldsymbol{x})$ is a cubic polynomial, $\mathscr{R}$ is a region of $\boldsymbol{x}$ space, α is a real number, and P is a large positive number. The general principles by which conditional estimates can be found for such a sum when $\mathscr{R}$ is a box (that is, a cartesian product of intervals) were developed in [1], [2], and [4], and we now apply these principles with certain modifications to obtain similar estimates when $\mathscr{R}$ is a parallelepiped of a certain shape.

[1] The simple example $C_1' = y_1^3$, $C_1'' = y_2^3$, where $h(C_1') = h(C_1'') = h(C_1) = 1$, shows that there need not be equality here.

It is convenient in the present work to write the cubic part $C(\boldsymbol{x})$ of a cubic polynomial $\phi(\boldsymbol{x})$ as in (6). Associated with this cubic part are the bilinear forms (7).

LEMMA 4. *For a fixed box $\mathscr{B}$ and a fixed cubic polynomial ϕ we have*

$$|S(\alpha; \phi, \mathscr{B})|^4 \ll P^n \sum_{\boldsymbol{x}} \sum_{\boldsymbol{y}} \prod_{j=1}^{n} \min\big(P, \|\alpha B_j(\boldsymbol{x}|\boldsymbol{y})\|^{-1}\big) \tag{18}$$

where the sum is over integer points $\boldsymbol{x}, \boldsymbol{y}$ satisfying $|\boldsymbol{x}| \ll P$, $|\boldsymbol{y}| \ll P$.

Proof. This is essentially Lemma 3.1 of [1], with minor modifications. First, we have a cubic polynomial ϕ in place of a cubic form, as is legitimate in accordance with the observation made in connection with that lemma. Secondly we have αB_j instead of B_j because Lemma 3.1 of [1] was stated for a real cubic form. Thirdly the numerical factor 6 preceding B_j is omitted because of our different notation for $C(\boldsymbol{x})$ and $B_j(\boldsymbol{x}|\boldsymbol{y})$ in (6) and (7). Hence the result.

Now let $\phi(\boldsymbol{x})$ be the cubic polynomial (1) of the theorem and let $\mathscr{P}$ be a parallelepiped in $\boldsymbol{x}$ space which corresponds under the substitution $\boldsymbol{x} = \boldsymbol{U}\boldsymbol{z}$ of Lemma 3 to a box in $\boldsymbol{z}$ space. We write

$$S(\alpha) = S(\alpha; \phi, \mathscr{P}). \tag{19}$$

Also we define $S^*(\alpha, \boldsymbol{B})$ for any set of bilinear forms as in (7) by

$$S^*(\alpha, \boldsymbol{B}) = P^n \sum_{\boldsymbol{x}} \sum_{\boldsymbol{y}} \prod_{j=1}^{n} \min\big(P, \|\alpha B_j(\boldsymbol{x}|\boldsymbol{y})\|^{-1}\big), \tag{20}$$

where the sum is over integer points $\boldsymbol{x}, \boldsymbol{y}$ with $|\boldsymbol{x}| \ll P$, $|\boldsymbol{y}| \ll P$.

In the next lemma we apply the result of Lemma 4 to the decomposition of $\phi(\boldsymbol{x})$ given in (15) of Lemma 3. If the variables in the cubic polynomials $\psi_1(\boldsymbol{z}), \ldots, \psi_s(\boldsymbol{z})$ were disjoint, and if $\boldsymbol{z}$ were an arbitary integer point, the sum $S(\alpha)$ would factorize into a product of sums $S(\alpha; \psi_i, \mathscr{B}_i)$ in n_i variables taken over boxes $P\mathscr{B}_i$. In reality the position is not so simple, but the ultimate effect is the same.

LEMMA 5. *We have*

$$|S(\alpha)|^4 \ll P^{4n-4\Sigma n_i} S^*(\alpha, \boldsymbol{B}_1) \ldots S^*(\alpha, \boldsymbol{B}_s), \tag{21}$$

where for each i the set of bilinear forms $\boldsymbol{B}_i$ is the set of n_i bilinear forms corresponding to the cubic form $C_i(d\boldsymbol{z})$ of Lemma 3 in n_i variables, and $\boldsymbol{x}, \boldsymbol{y}$ in (20) run through integer points in n_i dimensional space.

Proof. Let $\boldsymbol{z}_0$ be any one of the finite set of representative solutions of the homogeneous linear congruences (mod d) satisfied by $\boldsymbol{z}$ in Lemma 3. Then we can put $\boldsymbol{z} = d\boldsymbol{u}+\boldsymbol{z}_0$, where $\boldsymbol{u}$ is an arbitary integer point.

Substituting in (15) and (17), with $\mathscr{P}$ in place of $\mathscr{R}$, we obtain for $S(\alpha)$ an expression as a finite number (corresponding to the various choices of $\mathbf{z}_0$) of exponential sums of the form

$$(22)\qquad \sum_{\mathbf{u}} e\Big(\alpha\big(\psi_1(d\mathbf{u}+\mathbf{z}_0)+\ldots+\psi_s(d\mathbf{u}+\mathbf{z}_0)\big)\Big).$$

If $\mathscr{B}$ is the box in $\mathbf{z}$ space which corresponds to the parallelepiped $\mathscr{P}$ in $\mathbf{x}$ space, the summation is extended over all integer points $\mathbf{u}$ in the box $d^{-1}(P\mathscr{B}-\mathbf{z}_0)$ in $\mathbf{u}$ space.

We apply to this sum the estimate given by Lemma 4. Since the result depends only on the cubic part of the polynomial, it is independent of $\mathbf{z}_0$. There is a minor discrepancy in that the box of summation depends (though only by a bounded translation) on $\mathbf{z}_0$, but this is plainly of no importance, since it can be remedied by modifying the constants in the conditions $|\mathbf{x}| \ll P$, $|\mathbf{y}| \ll P$.

We obtain (18), with bilinear forms B_j which are associated with the cubic part of

$$\psi_1(d\mathbf{u}+\mathbf{z}_0)+\ldots+\psi_s(d\mathbf{u}+\mathbf{z}_0),$$

which is

$$C_1(d\mathbf{u})+\ldots+C_s(d\mathbf{u}).$$

Since the variables in these cubic forms are disjoint, the bilinear forms fall into sets of $n_1, \ldots, n_s, n-\sum n_i$ bilinear forms, and the variables in different sets are disjoint. Also the $n-\sum n_i$ bilinear forms in the last set are identically zero. Accordingly, the expression on the right of (18) factorizes, the typical factor being $S^*(\alpha, \mathbf{B}_i)$, where there are n_i bilinear forms $\mathbf{B}_i$, namely those associated with the cubic form $C_i(d\mathbf{u})$. There is also a factor $AP^{4(n-\sum n_i)}$ corresponding to the bilinear forms which are identically zero, where A is a constant depending on the ranges of summation of $\mathbf{x}$ and $\mathbf{y}$. This proves the lemma.

4. The estimation of $S^*(\alpha, \mathbf{B})$ when $h = n$. In this section and the next we obtain an estimate for $S^*(\alpha, \mathbf{B})$, defined in (20), conditional on the Diophantine character of α. We shall take the bilinear forms $\mathbf{B}$ to be those associated with a cubic form in n variables which does not split, so that Lemma 2 is available for application. Later we shall apply these results to each factor on the right of (21), and at that stage we shall have to replace n by n_i and h by $h_i = h(C_i)$.

In the present section we suppose that $h = n$, and treat the case $h < n$ in the next section. We follow the lines of argument leading up to Lemma 13 of [2]. The estimate obtained there involved a parameter θ satisfying $\Delta_0 \leqslant \theta \leqslant \frac{3}{4}+\Delta$, where Δ_0, Δ are small fixed positive numbers. For the present purpose we need an estimate that is valid also when θ is near 0, and therefore it is necessary to rework the greater part of the argument. We shall use a parameter U in place of P^θ; ultimately U will assume various values, but the smallest of these will be a large power of L, where

$$(23)\qquad L = \log P.$$

It will be convenient to reason indirectly, by developing the consequences of the hypothesis that, for a particular α,

$$(24)\qquad S^*(\alpha, \mathbf{B}) > P^{4n} U^{-n}.$$

Lemma 6. *Subject to* (24), *the number of pairs $\mathbf{x}, \mathbf{y}$ of integer points satisfying*

$$(25)\qquad |\mathbf{x}| \ll P, \quad |\mathbf{y}| \ll P, \quad \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| < P^{-1}$$

is

$$(26)\qquad \gg P^{2n} U^{-n} L^{-n}.$$

Proof. This is Lemma 3.2 of [1], with only trivial differences.

Lemma 7. *Suppose that*

$$(27)\qquad 1 < T < U < PL^{-2}.$$

Then, subject to (24), *one of the following three alternatives holds:*

(I) *there are* $\gg U^n T^{-n} L^{2n-1}$ *pairs* $\mathbf{x}, \mathbf{y}$ *of integer points satisfying*

$$(28)\qquad 0 < |\mathbf{x}| \ll UL^2, \quad 0 < |\mathbf{y}| \ll UL^2, \quad \mathbf{B}(\mathbf{x}|\mathbf{y}) = 0;$$

(II) *there are* $\gg U^n T^{-n} L^{2n-1}$ *integer points* $\mathbf{x}$ *with*

$$(29)\qquad 0 < |\mathbf{x}| \ll UL^2,$$

to each of which there corresponds an integer point $\mathbf{y}$ *with*

$$(30)\qquad 0 < |\mathbf{y}| \ll UL^2, \quad \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| \ll P^{-3} U^2 L^4;$$

(III) α *has a rational approximation* a/q *satisfying*

$$(31)\qquad (a, q) = 1, \quad 1 \leqslant q < U^2 L^4 T^{-1}, \quad |q\alpha - a| < P^{-3} U^2 L^5.$$

Proof. Since $U < PL^{-2}$, the number in (26) is substantially greater than P^n. Hence the result of Lemma 6 remains correct if in (25) we add the conditions $\mathbf{x} \neq 0$, $\mathbf{y} \neq 0$.

Suppose that to each point $\mathbf{y}$ of Lemma 6 there correspond $N(\mathbf{y})$ points $\mathbf{x} \neq 0$, so that

$$\sum_{0 < |\mathbf{y}| \ll P} N(\mathbf{y}) \gg P^{2n} U^{-n} L^{-n}.$$

This remains true if we restrict $\boldsymbol{y}$ to points for which

$$N(\boldsymbol{y}) > c_2 P^n U^{-n} L^{-n},$$

since there are $\ll P^n$ possible points $\boldsymbol{y}$. (Here c_2 is a suitable positive constant, and similarly for c_3, etc. later.)

For each such $\boldsymbol{y}$ we apply Lemma 8 of [2] with $\boldsymbol{u} = \boldsymbol{x}$ and with

$$L_j(\boldsymbol{u}) = aB_j(\boldsymbol{u}|\boldsymbol{y}).$$

We take $A = P$ and $Z = c_3$ as in the proof of Lemma 9 of [2], and have

$$V(Z) = N(\boldsymbol{y}) > c_2 P^n U^{-n} L^{-n}.$$

We can choose Z_1 subject to (29) of [2], and this condition takes the form

$$c_4 P^{-1} UL < Z_1 < 1.$$

We take $Z_1 = c_4 P^{-1} UL^2$. Then (30) of [2] gives

$$V(Z_1) \gg (P^{-1}UL^2)^n V(Z) = (P^{-1}UL^2)^n N(\boldsymbol{y}).$$

Hence, for each $\boldsymbol{y}$ in the set in question, there are $\gg (P^{-1}UL^2)^n N(\boldsymbol{y})$ points $\boldsymbol{x}$ satisfying

$$(32) \qquad 0 < |\boldsymbol{x}| \ll UL^2, \qquad \|a\boldsymbol{B}(\boldsymbol{x}|\boldsymbol{y})\| \ll P^{-2}UL^2.$$

Hence the number N of pairs $\boldsymbol{x}, \boldsymbol{y}$ satisfying (32) and

$$(33) \qquad 0 < |\boldsymbol{y}| \ll P$$

satisfies

$$(34) \qquad N \gg (P^{-1}UL^2)^n \sum_{\boldsymbol{y}} N(\boldsymbol{y}) \gg P^n L^n.$$

Now let $N_1(\boldsymbol{x})$ denote the number of points $\boldsymbol{y}$ which correspond to a given point $\boldsymbol{x}$, so that

$$(35) \qquad \sum_{0<|\boldsymbol{x}|\ll UL^2} N_1(\boldsymbol{x}) = N \gg P^n L^n.$$

This remains true if we limit ourselves to points $\boldsymbol{x}$ for which

$$N_1(\boldsymbol{x}) > c_5 P^n L^n (UL^2)^{-n}.$$

We divide these points into subsets, placing in the sth subset $(s = 0, 1, \ldots)$ those for which

$$(36) \qquad 2^s c_5 P^n U^{-n} L^{-n} < N_1(\boldsymbol{x}) \leqslant 2^{s+1} c_5 P^n U^{-n} L^{-n}.$$

Since $N_1(\boldsymbol{x}) \ll P^n$, we have $2^s \ll U^n L^n$, so the number of values of s is $\ll L$. Hence there is some s with the property that there are

$$\gg P^n L^n (2^s P^n U^{-n} L^{-n})^{-1} L^{-1} = 2^{-s} U^n L^{2n-1}$$

points $\boldsymbol{x}$ in the sum (35) for which $N_1(\boldsymbol{x})$ satisfies (36).

For each such $\boldsymbol{x}$ we apply Lemma 8 of [2] with $\boldsymbol{u} = \boldsymbol{y}$ and with $L_j(\boldsymbol{u}) = aB_j(\boldsymbol{x}|\boldsymbol{u})$. We take

$$Z = c_6 P^{-1/2} U^{1/2} L, \qquad A = P^{3/2} U^{-1/2} L^{-1},$$

whereupon (33) and the second inequality of (32) become the inequalities (27) of [2]. Hence, for the present application, we have

$$(37) \qquad V(Z) = N_1(\boldsymbol{x}) \gg 2^s P^n U^{-n} L^{-n},$$

by (36).

Suppose first that $2^s \geqslant T^n$. The condition on Z_1 in (29) of [2] becomes

$$c_7 P^{-1/2} U^{1/2} L\, 2^{-s/n} P^{-1} UL \leqslant Z_1 \leqslant P^{-1/2} U^{1/2} L,$$

and is satisfied if we take

$$Z_1 = c_7 P^{-3/2} U^{3/2} L^2 T^{-1}.$$

Then

$$V(Z_1) \gg (P^{-3/2} U^{3/2} L^2 T^{-1} P^{1/2} U^{-1/2} L^{-1})^n V(Z) \gg 2^s T^{-n}.$$

The inequalities (27) of [2] with Z_1 in place of Z become

$$(38) \qquad 0 < |\boldsymbol{y}| \ll ULT^{-1}, \qquad \|a\boldsymbol{B}(\boldsymbol{x}|\boldsymbol{y})\| \ll P^{-3} U^2 L^3 T^{-1}.$$

Since the number of points $\boldsymbol{x}$ is $\gg 2^{-s} U^n L^{2n-1}$, the number of pairs $\boldsymbol{x}, \boldsymbol{y}$ satisfying (38) and

$$0 < |\boldsymbol{x}| \ll UL^2$$

is

$$\gg U^n L^{2n-1} T^{-n}.$$

If, for all these pairs, we have $\boldsymbol{B}(\boldsymbol{x}|\boldsymbol{y}) = 0$, then alternative (I) of the enunciation holds. If not, we obtain (as in the proof of Lemma 9 of [2]) a rational approximation a/q to a satisfying

$$q \ll U^2 L^3 T^{-1}, \qquad |qa - a| \ll P^{-3} U^2 L^3 T^{-1}.$$

This implies alternative (III) of the enunciation.

Suppose now that $2^s < T^n$. Then there are $\gg T^{-n} U^n L^{2n-1}$ points $\boldsymbol{x}$ for each of which the number of corresponding points $\boldsymbol{y}$ satisfies (36).

The first conclusion of Lemma 8 of [2] tells us that one such point $\boldsymbol{y}$ satisfies

$$0 < |\boldsymbol{y}| \ll PN_1(\boldsymbol{x})^{-1/n} \ll UL,$$
$$\|\alpha\boldsymbol{B}(\boldsymbol{x}\,|\,\boldsymbol{y})\| \ll P^{-2}UL^2N_1(\boldsymbol{x})^{-1/n} \ll P^{-3}U^2L^3.$$

This implies alternative (II) of the enunciation, and the proof is complete.

LEMMA 8. *Suppose that alternative* (II) *of Lemma* 7 *holds and that alternatives* (I) *and* (III) *do not hold. Suppose also that*

$$U^4L^8 < P^3T. \tag{39}$$

Then there exist integers $m_1, \ldots, m_n$, depending on α and P, such that there are $\gg U^nT^{-3n}L^{2n-1}$ integer points $\boldsymbol{x}$ with

$$0 < |\boldsymbol{x}| \ll UL^2, \tag{40}$$

to each of which there corresponds an integer point $\boldsymbol{y}$ satisfying

$$0 < |\boldsymbol{y}| \ll UL^2, \quad B_j(\boldsymbol{x}\,|\,\boldsymbol{y}) = m_j \quad (j = 1, \ldots, n). \tag{41}$$

Proof. Alternative (II) asserts the existence of $\gg U^nT^{-n}L^{2n-1}$ integer points $\boldsymbol{x}$ satisfying (29), to each of which there corresponds an integer point $\boldsymbol{y}$ satisfying (30). Not all the values of $B_j(\boldsymbol{x}\,|\,\boldsymbol{y})$ for all these pairs are 0, for that would imply alternative (I). Choosing one pair and one j for which $B_j(\boldsymbol{x}\,|\,\boldsymbol{y}) \neq 0$ we obtain integers a, q such that

$$(a, q) = 1, \quad 1 \leqslant q \ll U^2L^4, \quad |q\alpha - a| < P^{-3}U^2L^4. \tag{42}$$

We must have

$$q \gg U^2L^4T^{-1}, \tag{43}$$

since otherwise alternative (III) would hold.

We proceed as in the proof of Lemma 10 of [2]. For each $\boldsymbol{x}$ and $\boldsymbol{y}$ occurring in alternative (II), we put

$$aB_j(\boldsymbol{x}\,|\,\boldsymbol{y}) = qt_j + u_j,$$

where t_j, u_j are integers and $|u_j| \leqslant \frac{1}{2}q$. We obtain

$$\begin{aligned} |u_j| &\leqslant q\|\alpha B_j(\boldsymbol{x}\,|\,\boldsymbol{y})\| + |q\alpha - a|\,|B_j(\boldsymbol{x}\,|\,\boldsymbol{y})| \\ &\ll qP^{-3}U^2L^4 + P^{-3}U^2L^4U^2L^4 \\ &\ll P^{-3}U^4L^8. \end{aligned}$$

Thus $|u_j| \ll T$ by (39).

The integers t_j, u_j depend on $\boldsymbol{x}$; but the number of possibilities for $u_1, \ldots, u_n$ is $\ll T^n$, and these are independent of $\boldsymbol{x}$. So the number of $\boldsymbol{x}$ for which $u_1, \ldots, u_n$ have the same values is (for suitable values) $\gg U^nT^{-2n}L^{2n-1}$. For these $\boldsymbol{x}$ the values of $B_j(\boldsymbol{x}\,|\,\boldsymbol{y})$ are determined to the modulus q, and since

$$|B_j(\boldsymbol{x}\,|\,\boldsymbol{y})| \ll U^2L^4, \qquad q \gg U^2L^4T^{-1},$$

the number of possibilities for the values of the $B_j(\boldsymbol{x}\,|\,\boldsymbol{y})$ is $\ll T^n$. It follows that the number of points $\boldsymbol{x}$ for which $B_j(\boldsymbol{x}\,|\,\boldsymbol{y}) = m_j$ is $\gg U^nT^{-3n}L^{2n-1}$ for suitable $m_1, \ldots, m_n$. This proves the result.

LEMMA 9. *The alternative* (II) *of Lemma* 7 *is superfluous if*

$$T^{3n} < (UL)^{1-\varepsilon} \tag{44}$$

for some fixed $\varepsilon > 0$, and (39) *holds.*

Proof. The equations $B_j(\boldsymbol{x}\,|\,\boldsymbol{y}) = m_j$ are non-homogeneous linear equations in $\boldsymbol{y}$ for given $\boldsymbol{x}$; their determinant $H(\boldsymbol{x})$ is not identically zero by Lemma 1 of [2]. The number of integer points $\boldsymbol{x}$ with $|\boldsymbol{x}| < UL^2$ for which $H(\boldsymbol{x}) = 0$ is $\ll (UL^2)^{n-1}$, and this is small compared with the number of integer points $\boldsymbol{x}$ mentioned in Lemma 8, by (44). Hence the assertion of Lemma 8 remains true if we add to (40) the condition $H(\boldsymbol{x}) \neq 0$.

We now argue as in the proof of Lemma 12 of [2], and appeal to Lemma 11 of that paper with $R = UL^2$, which is permissible since $m_1, \ldots, m_n$ are $\ll (UL^2)^2$. We infer that the number of integer points $\boldsymbol{x}$ with $|\boldsymbol{x}| < UL^2$ for which $H(\boldsymbol{x}) \neq 0$ and the equations $B_j(\boldsymbol{x}\,|\,\boldsymbol{y}) = m_j$ have an integer solution in $\boldsymbol{y}$ is

$$\ll R^{n-1+\frac{1}{2}\varepsilon} \ll (UL^2)^{n-1+\frac{1}{2}\varepsilon}.$$

But, by (44), this contradicts the assertion that the number of such points is $\gg U^nT^{-3n}L^{2n-1}$. Hence the result.

LEMMA 10. *There exist positive numbers c_8, c_9, c_{10}, depending only on n, with the following property. Suppose that*

$$U > L^{c_8}, \tag{45}$$

$$U^{4-n^{-2}} < P^3L^{-c_9}. \tag{46}$$

Then, for any real α, either

$$S^*(\alpha, \boldsymbol{B}) \leqslant P^{4n}U^{-n} \tag{47}$$

or there exists a rational approximation a/q to α satisfying

$$(a, q) = 1, \quad 1 \leqslant q < U^{2-n^{-2}}L^{c_{10}}, \quad |q\alpha - a| < P^{-3}U^2L^5. \tag{48}$$

Proof. We define T by

$$T^nL^{1+c} = U^{n^{-1}},$$

where c is the constant of Lemma 2. The condition (27) of Lemma 7 is satisfied, by (45) and (46), provided c_8 is suitably chosen. Similarly the conditions (39) of Lemma 8 and (44) of Lemma 9 are satisfied.

If (47) does not hold then one of the three alternatives of Lemma 7 must hold. Alternative (II) is superfluous by Lemma 9. We now show that alternative (I) is impossible by appealing to Lemma 2 with $h = n$ and with $R = UL^2$. If alternative (I) were to hold, we should have

$$R^{n-n^{-1}} L^c \gg U^n T^{-n} L^{2n-1},$$

that is,

$$U^{n-n^{-1}} L^{2n-2n^{-1}+c} \gg U^n U^{-n^{-1}} L^{1+c} L^{2n-1},$$

which is false.

There remains only alternative (III), which gives the result stated since

$$U^2 L^4 T^{-1} = U^{2-n^{-2}} L^4 L^{(1+c)/n}.$$

This completes the proof.

5. The estimation of $S^*(\alpha, \boldsymbol{B})$ when $h < n$.

We have the same situation as in the preceding section except that now $h < n$. The proof of the desired estimate is now much simpler, as we do not need to consider alternative (II). But the result is in general weaker.

LEMMA 11. *With the notation and hypotheses of Lemma* 10, *either*

$$S^*(\alpha, \boldsymbol{B}) \leqslant P^{4n} U^{-h} \tag{49}$$

or there exists a rational approximation to α satisfying (48).

Proof. Under the hypothesis $S^*(\alpha, \boldsymbol{B}) > P^{4n} U^{-h}$ we have, as the analogue of Lemma 6, that the number of pairs of integer points satisfying (25) is $\gg P^{2n} U^{-h} L^{-n}$. We follow now the lines of proof of Lemma 7. The first step, with the same choice of Z_1 as before, gives the existence of $\gg P^n U^{n-h} L^n$ pairs $\boldsymbol{x}, \boldsymbol{y}$ satisfying (32) and (33).

In the second stage of the argument we now get (37) replaced by

$$V(Z) = N_1(\boldsymbol{x}) \gg 2^s P^n U^{-h} L^{-n}.$$

Also (36) is replaced by

$$2^s c_5 P^n U^{-h} L^{-n} < N_1(\boldsymbol{x}) \leqslant 2^{s+1} c_5 P^n U^{-h} L^{-n},$$

but the lower bound for the number of points $\boldsymbol{x}$ is the same as before.

We apply Lemma 8 of [2] with

$$Z_1 = c_7 P^{-3/2} U^{3/2} L^2 T_1^{-1},$$

where $T_1 > 1$ is to be chosen later. This satisfies the condition (29) of [2] provided

$$T_1 < U^{1-h/n}. \tag{50}$$

We obtain the existence of

$$\gg U^{2n-h} L^{2n-1} T_1^{-n}$$

pairs $\boldsymbol{x}, \boldsymbol{y}$ satisfying

$$\begin{cases} 0 < |\boldsymbol{x}| < UL^2, \quad 0 < |\boldsymbol{y}| < c_7 ULT_1^{-1}, \\ \|\alpha \boldsymbol{B}(\boldsymbol{x}|\boldsymbol{y})\| < c_7 P^{-3} U^2 L^3 T_1^{-1}. \end{cases} \tag{51}$$

If $B_j(\boldsymbol{x}|\boldsymbol{y}) = 0$ for each j and for all these pairs, we can appeal to Lemma 2. Taking $R = UL^2$, this informs us that the number of pairs is

$$\ll (UL^2)^{2n-h-n^{-1}} L^c.$$

This contradicts the above assertion if T_1 is chosen by

$$T_1 = U^{n^{-2}} L^{-c_{11}}$$

with a suitable c_{11}. This amply satisfies (50).

Hence there is some pair $\boldsymbol{x}, \boldsymbol{y}$ and some j for which $B_j(\boldsymbol{x}|\boldsymbol{y}) \neq 0$, and this leads in the usual way from (51) to a rational approximation a/q to α satisfying

$$(a, q) = 1, \quad 1 \leqslant q \ll U^2 L^3 T_1^{-1},$$
$$|q\alpha - a| \ll P^{-3} U^2 L^3 T_1^{-1}.$$

These conditions are somewhat stronger than those asserted in (48), so the proof is complete.

6. The estimates for $S(\alpha)$ and $S_{a,q}$.

LEMMA 12. *Let $\phi(\boldsymbol{x})$ be a cubic polynomial as in* (1). *Let $\mathscr{P}$ be a fixed parallelepiped of a suitable shape in n dimensional space; let P be large, and let $S(\alpha)$ be defined by* (19) *and* (17). *Let U satisfy* (45), (46). *Then either*

$$|S(\alpha)| \leqslant P^n U^{-h^*/4}, \tag{52}$$

where $h^* = h^*(C)$, or α has a rational approximation a/q satisfying

$$(a, q) = 1, \quad 1 \leqslant q < U^{2-n^{-2}} L^{c_{10}}, \quad |q\alpha - a| < P^{-3} U^2 L^5. \tag{53}$$

Proof. We use the estimate for $|S(\alpha)|$ given in (21), and apply the results of Lemma 10 or Lemma 11 to each of the factors $S^*(\alpha, \boldsymbol{B}_i)$ on the right. If α does not have a rational approximation satisfying (53), then *a fortiori* it does not have a rational approximation satisfying the corresponding inequalities with n replaced by n_i, since $n_i < n$. Hence by one or other of the lemmas mentioned (according as $h_i = n_i$ or $h_i < n_i$) we have

$$|S^*(\alpha, \boldsymbol{B}_i)| \leqslant P^{4n_i} U^{-h_i}.$$

Thus, by (21) and (16),

$$|S(\alpha)|^4 \ll P^{4n-4\Sigma n_i} P^{4\Sigma n_i} U^{-\Sigma h_i} \ll P^{4n} U^{-h^*}.$$

This proves the result.

Lemma 13. *Let a, q be integers with $(a, q) = 1$ and $q > 0$. Let*

$$S_{a,q} = \sum_{z (\mathrm{mod}\, q)} e\left(\frac{a}{q}\phi(z)\right). \tag{54}$$

Then

$$|S_{a,q}| \ll q^{n-h^*/(8-4n^{-2})}(\log q)^{c_{12}}. \tag{55}$$

Proof. We appeal to Lemma 12 with $\alpha = a/q$ and with P to be chosen later. The second alternative of Lemma 12 is the existence of integers a', q' such that

$$(a', q') = 1, \quad 1 \leqslant q' < U^{2-n^{-2}} L^{c_{10}}, \quad |q'a/q - a'| < P^{-3} U^2 L^5.$$

Suppose that

$$P^3 U^{-2} L^{-5} > q. \tag{56}$$

Then the last inequality implies that

$$a'/q' = a/q,$$

and this is excluded by the preceding inequality if

$$U^{2-n^{-2}} L^{c_{10}} \leqslant q. \tag{57}$$

Thus if (56) and (57) are satisfied, the estimate (52) becomes applicable.

The parallelepiped $P\mathscr{P}$ in the definition of $S(\alpha)$ in (17) and (19) is given by n conditions of the type

$$\lambda_j P < a_{1j} x_1 + \ldots + a_{nj} x_n < \mu_j P,$$

where the a_{ij} are fixed rational numbers and the λ_j, μ_j are fixed. The number of integer points satisfying these inequalities and lying in a given residue class $(\mathrm{mod}\, q)$ is

$$A(P/q)^n + O\big((P/q)^{n-1}\big),$$

where A is a positive constant. Hence

$$S(a/q) = AP^n q^{-n} S_{a,q} + O(P^{n-1} q).$$

Combining this with (52) we obtain

$$|S_{a,q}| \ll q^n U^{-h^*/4} + P^{-1} q^{n+1}.$$

Choose $P = q^{n+1}$, so that the last term becomes negligible, and choose U so that

$$U^{2-n^{-2}} (\log P)^{c_{10}} = q.$$

Then (56) and (57) are satisfied, and so are (45) and (46), which are needed for the validity of Lemma 12. We obtain the desired result (55).

7. Minor arcs. Let $\mathscr{E}(U)$ denote the set of all real α in $0 < \alpha < 1$ which have a rational approximation a/q satisfying (53), and let $\mathscr{C}\mathscr{E}(U)$ denote the complement of this set relative to that interval. We define the minor arcs $\mathfrak{m}$ to be $\mathscr{C}\mathscr{E}(U_1)$, where

$$U_1 = L^{c_{13}} \tag{58}$$

for a suitable large constant c_{13}.

Let f_1, f_2 denote the lower bound and upper bound of $C(x)$ for x in $\mathscr{P}$, so that $0 < f_1 < f_2$, and let g_1, g_2 satisfy

$$0 < g_1 < f_1 < f_2 < g_2. \tag{59}$$

Define $T(\alpha)$ by

$$T(\alpha) = \sum_{g_1 P^3 < p < g_2 P^3} e(\alpha p), \tag{60}$$

where p runs through primes.

Lemma 14. *If $h^* \geqslant 8$ we have*

$$\int_{\mathfrak{m}} |S(\alpha) T(-\alpha)|\, d\alpha \ll P^n L^{-c_{14}}, \tag{61}$$

where c_{14} is large when c_{13} is large.

Proof. The set $\mathscr{E}(U)$ increases with U, and if

$$U^{4-n^{-2}} L^{c_{10}-5} > P^3 \tag{62}$$

it consists of the whole interval $0 < \alpha < 1$. For, by the classical theorem of Dirichlet on Diophantine approximation, there is always a rational approximation to α satisfying

$$(a, q) = 1, \quad 1 \leqslant q < U^{2-n^{-2}} L^{c_{10}}, \quad |q\alpha - a| \leqslant U^{-2+n^{-2}} L^{-c_{10}},$$

and (62) ensures that this implies (53).

Denote by $\mathscr{F}(U)$ the complement of $\mathscr{E}(U)$ relative to $\mathscr{E}(2U)$. Then the whole interval $0 < \alpha < 1$ can be decomposed into

$$\mathscr{E}(U_1),\ \mathscr{F}(U_1),\ \mathscr{F}(2U_1),\ \ldots,\ \mathscr{F}(2^s U_1),$$

where s is the least integer such that $U = 2^{s+1}U_1$ satisfies (62). Hence $\mathfrak{m}$ is the union of

$$\mathscr{F}(U_1),\ \mathscr{F}(2U_1),\ \ldots,\ \mathscr{F}(2^s U_1).$$

Plainly $s \ll L$.

Take $U = 2^t U_1$, where $0 \leqslant t \leqslant s$, and write temporarily $\mathscr{F}$ for $\mathscr{F}(U)$. Then for α in $\mathscr{F}$ we have

$$|S(\alpha)| \ll P^n U^{-h^*/4}$$

by Lemma 12, since the values of U under consideration satisfy (45), (46). Also

$$|\mathscr{F}| \leqslant |\mathscr{E}(2U)| \leqslant \sum_q \sum_a 2q^{-1}P^{-3}(2U)^2 L^5,$$

where the summation is over

$$1 \leqslant q < (2U)^{2-n^{-2}}L^{c_{10}}, \quad 1 \leqslant a \leqslant q.$$

Hence

$$|\mathscr{F}| \ll P^{-3}U^2L^5(U^{2-n^{-2}}L^{c_{10}}).$$

It follows that

$$\begin{aligned}\int_{\mathscr{F}} |S(\alpha)T(-\alpha)|\,d\alpha &\leqslant P^n U^{-h^*/4}\int_{\mathscr{F}} |T(-\alpha)|\,d\alpha \\ &\leqslant P^n U^{-h^*/4}\{|\mathscr{F}|\}^{1/2}\Big\{\int_0^1 |T(-\alpha)|^2\,d\alpha\Big\}^{1/2} \\ &\ll P^n U^{-h^*/4}\{P^{-3}U^{4-n^{-2}}L^{5+c_{10}}\}^{1/2}\{P^3L^{-1}\}^{1/2} \\ &\ll P^n U^{2-h^*/4-1/2n^2}L^{c_{15}},\end{aligned}$$

where c_{15} depends only on n. Since $h^* \geqslant 8$, the last expression is

$$\ll P^n U^{-1/2n^2}L^{c_{15}}.$$

Since there are $\ll L$ sets $\mathscr{F}$, and this estimate applies to each of them, and the least value of U is U_1 which satisfies (58), we deduce (61).

It may be observed that Lemma 14 makes no use of the fact that p in (60) runs through primes, except in so far as it uses an estimate for the number of primes in the range of summation.

8. Major arcs. We denote by $\mathfrak{M}_{a,q}$ the interval for α defined by

$$\left|\alpha - \frac{a}{q}\right| < P^{-3}L^k, \tag{63}$$

where k is a positive constant, and we denote by $\mathfrak{M}$ the union of these intervals for

$$0 \leqslant a < q, \quad (a, q) = 1, \quad 1 \leqslant q \leqslant L^k. \tag{64}$$

The intervals (63) are then plainly disjoint. If we choose k so that

$$k > (2-n^{-2})c_{13}+c_{10}, \quad k > 2c_{13}+5, \tag{65}$$

then $\mathfrak{M}$ contains $\mathscr{E}(U_1)$, where U_1 is given by (58).

Lemma 15. *If α is in $\mathfrak{M}_{a,q}$ then,*

$$S(\alpha) = q^{-n}S_{a,q}I(\beta) + O(P^{n-1}L^{2k}), \tag{66}$$

where

$$I(\beta) = \int_{P\mathscr{P}} e\big(\beta(\phi\boldsymbol{\xi})\big)\,d\boldsymbol{\xi} \tag{67}$$

and

$$\beta = \alpha - \frac{a}{q}.$$

Proof. We have, writing $\mathbf{x} = q\mathbf{y}+\mathbf{z}$,

$$S(\alpha) = \sum_{\mathbf{z}(\bmod q)} e\left(\frac{a}{q}\phi(\mathbf{z})\right)\sum_{\mathbf{y}} e\big(\beta\phi(q\mathbf{y}+\mathbf{z})\big),$$

where the summation is over the parallelepiped

$$(Pq^{-1})\mathscr{P} - q^{-1}\mathbf{z}.$$

We can regard this parallelepiped as a union of

$$V(Pq^{-1})^n + O\big((Pq^{-1})^{n-1}\big)$$

cubes of side 1, together with a boundary zone which contains $O\big((Pq^{-1})^{n-1}\big)$ integer points and also has volume $O\big((Pq^{-1})^{n-1}\big)$. Each cube corresponds to a single term of the sum, and we can replace this term by

$$\int e\big(\beta\phi(q\boldsymbol{\eta}+\mathbf{z})\big)\,d\boldsymbol{\eta} + O\big(|\beta|\,q^3(Pq^{-1})^2\big),$$

where the integral is taken over the cube. Putting together the integrals, and allowing for the boundary zone, we obtain

$$S(\alpha) = q^{-n}S_{a,q}I(\beta) + O\big(q^n|\beta|\,q^3(Pq^{-1})^{n+2}\big) + O\big(q^n(Pq^{-1})^{n-1}\big).$$

Since $|\beta| < P^{-3}L^k$ and $q \leqslant L^k$, we obtain (66).

Lemma 16. *If α is in $\mathfrak{M}_{a,q}$ we have*

$$T(\alpha) = \frac{\mu(q)}{\varphi(q)}I_1(\beta) + O\big(P^3\exp(-c_{16}L^{1/2})\big), \tag{68}$$

where

$$I_1(\beta) = \int_{g_1P^3}^{g_2P^3} \frac{e(\beta x)}{\log x}\,dx. \tag{69}$$

Proof. See K. Prachar, *Primzahlverteilung* (Springer, 1957), VI, Satz 3.3. In the result given there the definite integral is replaced by the corresponding sum, but it is easily seen that the difference between the sum and the integral is $O(L^{k-1})$.

LEMMA 17. *If* $h^* \geqslant 8$ *we have*

$$(70)\qquad \int_{\mathfrak{M}} S(\alpha)T(-\alpha)\,d\alpha$$
$$= \{\mathfrak{S}+O(L^{-c_{17}}\} \int_{|\beta|<P^{-3}L^k} I(\beta)I_1(-\beta)\,d\beta+O\big(P^n\exp(-c_{18}L^{1/2})\big),$$

where

$$(71)\qquad \mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q},$$

and c_{18} *is any number satisfying* $0 < c_{18} < c_{16}$.

Proof. For α in $\mathfrak{M}_{a,q}$ we multiply together the approximations to $S(\alpha)$ and $T(-\alpha)$ given in Lemmas 15 and 16. The main term is

$$\frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q} I(\beta) I_1(-\beta),$$

and on summing over a and then q, we obtain the desired main term, except that instead of $\mathfrak{S}+O(L^{-c_{17}})$ we get

$$\sum_{q\leqslant L^k} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q}.$$

Since $|q^{-n}S_{a,q}| \ll q^{-1-\delta}$ for some fixed positive δ, by Lemma 13 with the fact that $h^* \geqslant 8$, the above finite sum differs from the infinite sum $\mathfrak{S}$ by an amount $O(L^{-c_{17}})$, for a suitable positive constant c_{17}.

The products of the various other terms in the approximations give an amount

$$\ll q^{-1-\delta}P^{n+3}\exp(-c_{16}L^{1/2})+\varphi(q)^{-1}P^{n+2}L^{2k-1}+P^{n+2}L^{2k}\exp(-c_{16}L^{1/2}),$$

on using the trivial estimates $|I(\beta)| \ll P^n$, $|I_1(\beta)| \ll P^3L^{-1}$. Integrating this over $|\beta| < P^{-3}L^k$ and then summing over a, q subject to (64) we obtain the error term stated.

9. The singular series.

LEMMA 18. *Suppose that for every integer* $m > 1$ *there is some integer point* $\boldsymbol{x}$ *such that* $\phi(\boldsymbol{x}) \not\equiv 0 \pmod{m}$. Then

$$(72)\qquad \mathfrak{S} > 0.$$

Proof. It follows from well known arguments that

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n} S_{a,q}$$

is a multiplicative function of q. Hence, by (71),

$$\mathfrak{S} = \prod_{\tilde{\omega}} \Big(1-\frac{1}{\tilde{\omega}-1}\tilde{\omega}^{-n}\sum_{a=1}^{\tilde{\omega}-1} S_{a,\tilde{\omega}}\Big),$$

where $\tilde{\omega}$ runs through the primes. For large $\tilde{\omega}$ the factor is

$$1+O(\tilde{\omega}^{-1-\delta}),$$

by the inequality used in the proof of Lemma 17. Hence to prove that $\mathfrak{S} > 0$ it suffices to prove that

$$\sum_{a=1}^{\tilde{\omega}-1} \tilde{\omega}^{-n} S_{a,\tilde{\omega}} < \tilde{\omega}-1$$

for each prime $\tilde{\omega}$.

Since

$$\tilde{\omega}^{-n} S_{a,\tilde{\omega}} = \tilde{\omega}^{-n} \sum_{\boldsymbol{z}(\mathrm{mod}\,\tilde{\omega})} e\Big(\frac{a}{\tilde{\omega}}\phi(\boldsymbol{z})\Big),$$

the inequality holds unless $\phi(\boldsymbol{z}) \equiv 0 \pmod{\tilde{\omega}}$ for all $\boldsymbol{z}$, and this was excluded in the hypothesis.

10. Proof of the theorem. We defined $\mathscr{M}(P)$ to be the number of integer points $\boldsymbol{x}$ in $P\mathscr{P}$ for which $\phi(\boldsymbol{x})$ is a prime. By the definitions of f_1, f_2, g_1, g_2 in § 7 we have $g_1P^3 < \phi(\boldsymbol{x}) < g_2P^3$ for all $\boldsymbol{x}$ in $P\mathscr{P}$. Hence, by (19), (17) and (60),

$$(73)\qquad \mathscr{M}(P) = \int_0^1 S(\alpha)T(-\alpha)\,d\alpha.$$

We dissect this integral into one over $\mathfrak{M}$ and one over $\mathscr{C}\mathfrak{M}$.

We have already observed in § 8 that if k satisfies (65) then $\mathfrak{M}$ contains $\mathscr{E}(U_1)$, from which it follows that

$$\mathscr{C}\mathfrak{M} \subset \mathscr{C}\mathscr{E}(U_1) = \mathfrak{m}.$$

Hence, by Lemma 14,

$$\int_{\mathscr{C}\mathfrak{M}} |S(\alpha)T(-\alpha)|\,d\alpha \ll P^nL^{-c_{14}},$$

where c_{14} can be taken large by taking k large. It now follows from Lemma 17 that

$$\mathscr{M}(P) = \{\mathfrak{S}+O(L^{-c_{17}})\}J(P)+O(P^nL^{-c_{14}}), \tag{74}$$

where

$$J(P) = \int\limits_{|\beta|<P^{-3}L^k} I(\beta)I_1(-\beta)\,d\beta. \tag{75}$$

By the definition of $I(\beta)$ in (67),

$$\begin{aligned} I(\beta) &= P^n\int\limits_{\mathscr{P}} e\big(\beta\phi(P\boldsymbol{\xi})\big)\,d\boldsymbol{\xi} \\ &= P^n\int\limits_{\mathscr{P}} e\big(\beta P^3C(\boldsymbol{\xi})\big)\,d\boldsymbol{\xi}+O(P^n|\beta|P^2) \\ &= P^n\int\limits_{\mathscr{P}} e\big(\beta P^3C(\boldsymbol{\xi})\big)\,d\boldsymbol{\xi}+O(P^{n-1}L^k). \end{aligned}$$

By the definition of $I_1(\beta)$ in (69),

$$\begin{aligned} I_1(\beta) &= P^3\int\limits_{g_1}^{g_2}\frac{e(\beta P^3x)}{\log P^3x}\,dx \\ &= \frac{P^3}{3L}\int\limits_{g_1}^{g_2} e(\beta P^3x)\,dx-\frac{P^3}{3L}\int\limits_{g_1}^{g_2}\frac{e(\beta P^3x)\log x}{3L+\log x}\,dx \\ &= \frac{P^3}{3L}\int\limits_{g_1}^{g_2} e(\beta P^3x)\,dx+O\big(P^3L^{-2}\min(1,|\beta P^3|^{-1})\big), \end{aligned}$$

the second estimate in the minimum coming from the mean value theorem.

We multiply together these approximations and substitute them in (75). The main term is

$$\frac{P^{n+3}}{3L}\int\limits_{|\beta|<P^{-3}L^k}\Big\{\int\limits_{\mathscr{P}} e\big(\beta P^3C(\boldsymbol{\xi})\big)\,d\boldsymbol{\xi}\Big\}\Big\{\int\limits_{g_1}^{g_2} e(-\beta P^3x)\,dx\Big\}\,d\beta = \frac{P^n}{3L}J_1(L^k),$$

where

$$J_1(\lambda) = \int\limits_{-\lambda}^{\lambda}\Big\{\int\limits_{\mathscr{P}} e\big(\gamma C(\boldsymbol{\xi})\big)\,d\boldsymbol{\xi}\Big\}\Big\{\int\limits_{g_1}^{g_2} e(-\gamma x)\,dx\Big\}\,d\gamma. \tag{76}$$

The error terms are majorized by

$$\begin{aligned} &P^{n-1}L^kP^3L^{-1}\int\limits_{|\beta|<P^{-3}L^k} d\beta+P^3L^{-2}P^n\int\limits_{|\beta|<P^{-3}L^k}\min(1,|\beta P^3|^{-1})\,d\beta \\ &\qquad \ll P^{n-1}L^kP^3L^{-1}P^{-3}L^k+P^{n+3}L^{-2}P^{-3}\log L \ll P^nL^{-2}\log L. \end{aligned}$$

Hence

$$J(P) = \frac{P^n}{3L}J_1(L^k)+O(P^nL^{-2}\log L). \tag{77}$$

By (76),

$$J_1(\lambda) = \int\limits_{\mathscr{P}} d\boldsymbol{\xi}\int\limits_{g_1}^{g_2}\frac{\sin 2\pi\lambda\big(C(\boldsymbol{\xi})-x\big)}{\pi\big(C(\boldsymbol{\xi})-x\big)}\,dx = \int\limits_{\mathscr{P}} d\boldsymbol{\xi}\int\limits_{g_1-C(\boldsymbol{\xi})}^{g_2-C(\boldsymbol{\xi})}\frac{\sin 2\pi\lambda t}{\pi t}\,dt.$$

The limit of the inner integral is 1 as $\lambda\to\infty$, and this limit is uniform in $\boldsymbol{\xi}$, since

$$\begin{aligned} g_1-C(\boldsymbol{\xi}) &\leqslant g_1-f_1 < 0, \\ g_2-C(\boldsymbol{\xi}) &\geqslant g_2-f_2 > 0. \end{aligned}$$

Hence

$$\lim_{\lambda\to\infty}J_1(\lambda) = \int\limits_{\mathscr{P}} d\boldsymbol{\xi} = V. \tag{78}$$

It follows from (74), (77), (78) that

$$\mathscr{M}(P)\sim\frac{VP^n}{3L}\mathfrak{S} \quad \text{as} \quad P\to\infty,$$

and $\mathfrak{S}>0$ by Lemma 18. This proves the Theorem.

I am grateful to Prof. H. Davenport for suggesting the problem discussed in this paper and for his help and suggested improvements in the preparation of the work for the publication.

References

[1] H. Davenport, *Cubic forms in thirty-two variables*, Philos. Trans. Roy. Soc., London, A, 251 (1959), pp. 193-232.

[2] — *Cubic forms in sixteen variables*, Proc. Roy. Soc., London, A, 272 (1963), pp. 285-303.

[3] — *Analytic methods for Diophantine equations and Diophantine inequalities*, Ann Arbor, Michigan, 1962.

[4] H. Davenport and D. J. Lewis, *Non-homogeneous cubic equations*, Journ. London Math. Soc. 39 (1964), pp. 657-671.

Reçu par la Rédaction le 17. 1. 1966