ACTA ARITHMETICA
XVII(1970)

Conspectus materiae tomi XVII, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlich Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Addresse der Schriftleitung und des Austausches	Адрес Редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und die folgende sind zu beziehen durch	Томы IV и следующие можно получить через

Ars Polona, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule	Prize of an issue	Preis für ein Heft	Цена номера

$ 4.00

Les volumes I–III sont à obtenir chez	Volumes I–III are available at	Die Bände I–III sind zu beziehen durch	Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

On the divisor-sum problem for binary cubic forms

by

G. Greaves (Reading)

1. Introduction. Let the numbers

$$1 \leqslant a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n \leqslant \ldots \tag{1.1}$$

be some particular sequence of positive integers. Following the work of Dirichlet on the sequence $a_n = n$, one enquires whether or not one has, as $Z \to \infty$,

$$\sum_{a_n \leqslant Z} d(a_n) \sim b_1 N(Z) \log Z, \tag{1.2}$$

for some constant b_1, where $N(Z)$ is the number of a_n not exceeding Z and $d(n)$ is the number of positive divisors of n. Several such problems have been considered in the past; we mention the case $a_n = |f(n)|$, where $f(n)$ is a polynomial of degree not exceeding 2. A result of the type (1.2) is then obtainable by a well-known elementary method; for a more advanced technique, and for further references to the literature, we mention the paper [3] of Hooley. His results give, for the polynomial $f(n) = n^2 + a$ $(a \neq -k^2)$, a formula

$$\sum_{|f(n)| \leqslant Z} d\big(|f(n)|\big) = b_2 Z^{1/2} \log Z + b_3 Z^{1/2} + O(Z^{4/9} \log^3 Z).$$

His method depends on a consideration of the exponential sum

$$\sum_{1 \leqslant l \leqslant L} \sum_{\substack{1 \leqslant u \leqslant l \\ f(u) \equiv 0 \pmod{l}}} e^{2\pi i g u/l} \tag{1.3}$$

and is applicable when $f(n)$ is any irreducible quadratic. However, the problem of obtaining corresponding results when the degree of $f(n)$ exceeds 2 appears to be very hard. The best known result in this direction is that of Erdös [2], who establishes, for each irreducible polynomial $f(n)$, the inequalities

$$b_4 Z \log Z \leqslant \sum_{1 \leqslant n \leqslant Z} d\big\{f(n)\big\} \leqslant b_5 Z \log Z.$$

We shall here turn our attention to the problem when the sequence (a_n) is given not by a polynomial in one variable but by the numbers representable as $a_n = |f(r,s)|$, where $f(r,s)$ is a binary form and the a_n are counted according to multiplicity of representation. For the general sequence (a_n) the sum in (1.2) is given by

$$\sum_{a_n\leqslant Z} d(a_n) = \sum_{a_n\leqslant Z}\sum_{l\mid a_n} 1 = \sum_{l\leqslant Z^{1/2}} + \sum_{m\leqslant Z^{1/2}} - \sum_{l,m\leqslant Z^{1/2}} \tag{1.4}$$

$$= 2\sum_{1\leqslant l\leqslant Z^{1/2}}\sum_{\substack{a_n\leqslant Z\\ a_n\equiv 0 \pmod l}} 1 - \sum_{1\leqslant l\leqslant Z^{1/2}}\sum_{\substack{a_n\leqslant lZ^{1/2}\\ a_n\equiv 0 \pmod l}} 1,$$

whence it appears we should consider

$$\sum_{\substack{|f(r,s)|\leqslant Z\\ f(r,s)\equiv 0 \pmod l}} 1 = \sum_{\substack{1\leqslant a,b\leqslant l\\ f(a,b)\equiv 0 \pmod l}} \sum_{|f(a+lX,b+lY)|\leqslant Z} 1,$$

for $1\leqslant l\leqslant Z^{1/2}$. In the case when $f(r,s)$ is a definite form, of degree ν, say, an elementary lattice-point method leads to an asymptotic estimate

$$b_5 Z^{2/\nu}/l^2 + O(Z^{1/\nu}/l)$$

for the inner sum on the right, but this becomes imprecise when $l \geqslant Z^{1/\nu}$. This elementary approach will thus fail when $\nu \geqslant 3$, the more so should the form $f(r,s)$ be indefinite. Nevertheless it will in fact turn out to be possible to obtain a result of the required type in the case $\nu = 3$. The method depends on a consideration of the exponential sum

$$S(g,h;l) = \sum_{\substack{1\leqslant r,s\leqslant l\\ f(r,s)\equiv 0 \pmod l}} \exp\big(2\pi i(gr+hs)/l\big),$$

which may be compared with (1.3). Here, however, we shall obtain an estimate for $S(g,h;l)$ for each l, and ultimate success depends on the fact that the resulting estimate for

$$\sum_{1\leqslant l\leqslant L} |S(g,h;l)|$$

is relatively more powerful than that obtainable for the sum (1.3). However, the fact that we are working with a binary form rather than with a polynomial in one variable introduces complications in other directions.

Throughout, $f(x,y)$ denotes a fixed binary cubic form

$$f(x,y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3,$$

irreducible over the integers, having non-zero discriminant

$$D = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3.$$

We define $\Delta = a_0a_3D$. We assume that $D < 0$, so that the curve $f(x,y) = 1$ has just one real asymptote, omitting consideration of the case $D > 0$ save in the statement of the final result. We do not consider the related problem arising when $f(x,y)$ fails to be irreducible over the integers.

For brevity of notation where no confusion results, we frequently omit the argument of $f(x,y)$ or of $f(r,s)$; r, s denote the integer variables corresponding to the real x, y. Thus (1.5) below reappears as

$$\Sigma_1 = \sum_{|f|\leqslant Z} d(|f|).$$

Other abbreviations used include the notation $e^{2\pi ix} = e(x)$. Certain limiting operations are to be interpreted according to the instructions

$$\sum_{g=-\infty}^{\infty} = \lim_{G\to\infty}\sum_{g=-G}^{G}, \qquad \sum_{g,h=-\infty}^{\infty} = \sum_{g=-\infty}^{\infty}\sum_{h=-\infty}^{\infty},$$

with possibly some additional restrictions on the values assumed by g, h. The Landau symbol O implies constants that depend at most on the coefficients in f and on ε, which as usual denotes, on each appearance, an arbitrary positive real number, to be thought of as being small. Z denotes a continuous positive real variable to be understood as tending to ∞; z is a subsidiary variable on the same footing as Z.

Our actual result is an asymptotic formula for

$$\Sigma_1 = \sum_{|f(r,s)|\leqslant Z} d\big(|f(r,s)|\big). \tag{1.5}$$

The result appears at the end of Section 7. We do not claim that the estimate $O(Z^{9/14+\varepsilon})$ for the error term in it is anything like the best possible; in fact we believe that an appreciably better estimate for it should be practicable by suitable improvements in the analysis we use. Here we concern ourselves merely with obtaining an estimate $O(Z^{2/3-\delta})$ for some $\delta > 0$. Accordingly we make no attempt at further precision when estimating quantities that only contribute factors of Z^ε to the final error term.

The corresponding problem for binary quadratic forms has not, perhaps, been considered from quite the present point of view in the literature. For the definite quadratic x^2+y^2, however, the problem is simply that of asymptotically estimating $\sum d(n)r(n)$, where $r(n)$ is the number of representations of n as r^2+s^2, and this is very closely related to the problems of estimating $\sum d^2(n)$ and $\sum r^2(n)$ that were considered some time ago by Wilson [9]. His methods take advantage of the multiplicative properties of quadratic forms and of the resulting properties of the appropriate Dirichlet series.

One source of difficulty in our problem is that as the form $f(x, y)$ is indefinite the function $|f(x, y)|$ does not have continuous derivatives on the asymptote of the curve $|f(x, y)| = 1$. Another is that the region $|f(x, y)| \leqslant Z$ is not bounded. For these reasons most of the work will involve, instead of $|f(x, y)|$, a related function $m(x, y)$, with the definition of which we commence the argument.

I am greatly indebted to Professor Hooley for much valuable assistance and encouragement during the preparation of this paper, the substance of which formed part of my doctoral thesis (Bristol, 1967). My thanks are also due to the Science Research Council for financial support.

2. Preliminary definitions and lemmas. Since we are supposing that the curve $f(x, y) = 1$ has only one real asymptote, we can choose a real non-singular linear transformation

$$x = \alpha u + \beta v, \quad y = \gamma u + \delta v \quad (\alpha\delta \neq \beta\gamma) \tag{2.11}$$

such that the form $f(x, y)$ transforms to

$$h(u, v) = f(\alpha u + \beta v, \gamma u + \delta v) = v(u^2 + v^2), \tag{2.12}$$

so that the real asymptote is now the line $v = 0$. Let $\lambda = \lambda(Z)$ be a real number, to be specified later, which depends on Z and satisfies

$$3 < \lambda < Z^{1/2}, \quad \lambda \to \infty \text{ as } Z \to \infty. \tag{2.13}$$

Define

$$k(u, v) = \left(\frac{8}{27(1+\lambda^2)}\right)^{1/2}\left(u^2 + \frac{3+\lambda^2}{2}v^2\right)^{3/2}. \tag{2.14}$$

The line-pair $|u| = \lambda|v|$ divides the (u, v)-plane into four sectors. We define a function $n(u, v)$, differing from $|h(u, v)|$ only in the two smaller sectors that contain the asymptote $v = 0$, by

$$n(u, v) = \begin{cases} |h(u, v)| & \text{if} \quad |u| \leqslant \lambda|v|, \\ k(u, v) & \text{if} \quad |u| > \lambda|v|. \end{cases} \tag{2.15}$$

The function $m(x, y)$ will be that obtained by transforming back to the (x, y)-plane by (2.11), so that it satisfies

$$m(\alpha u + \beta v, \gamma u + \delta v) = n(u, v), \tag{2.16}$$

which defines $m(x, y)$, since $\alpha\delta \neq \beta\gamma$. Let $k(u, v)$ meanwhile transform into $g(x, y)$, say, so that $g(x, y)$ is given by

$$g(\alpha u + \beta v, \gamma u + \delta v) = k(u, v). \tag{2.17}$$

Make the further substitution

$$\psi^2 = u^2 - \lambda^2 v^2, \quad \eta^2 = (1+\lambda^2)v^2,$$

so that

$$h(u, v) = \eta(\psi^2 + \eta^2)/\sqrt{1+\lambda^2},$$

and

$$k(u, v) = \left(\frac{8}{27(1+\lambda^2)}\right)^{1/2}(\psi^2 + \tfrac{3}{2}\eta^2)^{3/2} = (\tfrac{2}{3}\psi^2 + \eta^2)^{3/2}/\sqrt{1+\lambda^2}.$$

Thus

$$k^2(u, v) - h^2(u, v) = \frac{\psi^4}{1+\lambda^2}\left(\frac{1}{3}\eta^2 + \frac{8}{27}\psi^2\right) \tag{2.21}$$

$$= \frac{1}{27(1+\lambda^2)}(u^2 - \lambda^2 v^2)^2(8u^2 + (9+\lambda^2)v^2),$$

whence it appears, since $k(u, v) \geqslant 0$, that

$$|h(u, v)| \leqslant k(u, v), \tag{2.22}$$

with equality only when $|u| = \lambda|v|$. The region $|h(u, v)| \leqslant z$ can consequently, for any z, be dissected into the three disjoint regions

$$\begin{aligned} \mathscr{S}_1(z) &= \{u, v\colon |h(u, v)| \leqslant z, \ |u| \leqslant \lambda|v|\}, \\ \mathscr{S}_2(z) &= \{u, v\colon k(u, v) \leqslant z, \ |u| > \lambda|v|\}, \\ \mathscr{S}_3(z) &= \{u, v\colon |h(u, v)| \leqslant z < k(u, v), \ |u| > \lambda|v|\}. \end{aligned} \tag{2.31}$$

Application of the transformation (2.11) gives a corresponding dissection of the region $|f(x, y)| \leqslant z$ into three disjoint regions $\mathscr{R}_i(z)$. The inequality (2.22) and (2.15) give $|h(u, v)| \leqslant n(u, v)$, with equality only when $|u| \leqslant \lambda|v|$. Hence $|f(x, y)| \leqslant m(x, y)$, and the $\mathscr{R}_i(z)$ are given by

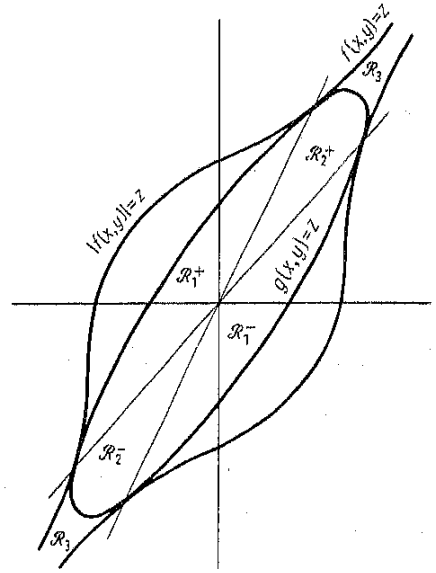
$$\begin{aligned} \mathscr{R}_1(z) &= \{x, y\colon |f(x, y)| = m(x, y) \leqslant z\}, \\ \mathscr{R}_2(z) &= \{x, y\colon |f(x, y)| < m(x, y) \leqslant z\}, \\ \mathscr{R}_3(z) &= \{x, y\colon |f(x, y)| \leqslant z < m(x, y)\}. \end{aligned} \tag{2.32}$$

Further, denote by L the line-pair

$$L = \{x, y\colon |\delta x - \beta y| = \lambda|\gamma x - \alpha y|\}, \tag{2.33}$$

into which $|u| = \lambda|v|$ transforms under (2.11).

The reader may find a geometrical interpretation of these definitions helpful. The curve $k(u, v) = z$ is an ellipse, which, as appears from (2.21), touches the cubics $|h(u, v)| = z$ at their intersections with the line-pair $|u| = \lambda|v|$, which lie, for large λ, close to the asymptote $v = 0$ of the cubics. The configuration, in the (x, y)-plane, is illustrated in the figure.



Subdivision of $\mathscr{R}_1(z)$ and $\mathscr{R}_2(z)$ into the regions $\mathscr{R}_1^+(z)$, etc., is performed as the figure suggests. Assign the points of $\mathscr{S}_1(z)$ to $\mathscr{S}_1^+(z)$ or $\mathscr{S}_1^-(z)$ according as $v \geqslant 0$ or $v < 0$, and those of $\mathscr{S}_2(z)$ to $\mathscr{S}_2^+(z)$ or $\mathscr{S}_2^-(z)$ according as $u > 0$ or $u < 0$. The regions $\mathscr{R}_1^+(z)$, etc., of the (x, y)-plane are then given by applying (2.11), so that for example

$$\mathscr{R}_1^+(z) = \{x, y: (x, y) \in \mathscr{R}_1(z), (\gamma x - \alpha y)(\beta\gamma - \alpha\delta) \geqslant 0\}. \tag{2.34}$$

It appears that the level-curves of the function $m(x, y)$ have everywhere continuously turning tangents; the analytic statement of this property, together with other information on the function $m(x, y)$ that is required, is contained in the following lemmas.

LEMMA 1. (i) *The function $m(x, y)$ defined in* (2.16) *and its first partial derivatives* $\dfrac{\partial m}{\partial x}, \dfrac{\partial m}{\partial y}$ *exist everywhere and are continuous functions of x, y.*

(ii) *The higher derivatives of $m(x, y)$ exist except perhaps on the lines L given by* (2.33). *In the region $m(x, y) \leqslant z$ they satisfy the inequalities*

$$\frac{\partial m}{\partial x}, \frac{\partial m}{\partial y} = O(\lambda^{2/3} z^{2/3}); \quad \frac{\partial^2 m}{\partial x^2}, \frac{\partial^2 m}{\partial y^2} = O(\lambda^{4/3} z^{1/3});$$

$$\frac{\partial^3 m}{\partial x^3}, \frac{\partial^3 m}{\partial y^3} = O(\lambda^2). \tag{2.4}$$

(i) It suffices, on applying the transformation (2.11), to establish the corresponding properties for $n(u, v)$. But, for example,

$$\frac{\partial n}{\partial v} = \begin{cases} (u^3 + 3v^2)\operatorname{sign} v & \text{if} \quad |u| < \lambda|v|, \\ \left(\dfrac{2}{3(1+\lambda^2)}\right)^{1/2} (3+\lambda^2) v \left(u^2 + \dfrac{3+\lambda^2}{2} v^2\right)^{1/2} & \text{if} \quad |u| > \lambda|v|, \end{cases} \tag{2.5}$$

where $\operatorname{sign} v = v/|v|$ if $v \neq 0$. It suffices to consider the possibility of a discontinuity across the line segment $0 \leqslant u = \lambda v$, where, however,

$$\left(\frac{2}{3(1+\lambda^2)}\right)^{1/2} (3+\lambda^2) v \left(u^2 + \frac{3+\lambda^2}{2} v^2\right)^{1/2} = (3+\lambda^2) v^3 = (u^3 + 3v^2)\operatorname{sign} v.$$

Hence $\dfrac{\partial n}{\partial v}$ is everywhere continuous; so, similarly, are $\dfrac{\partial n}{\partial u}$ and n.

(ii) It suffices, on using (2.11), to establish the corresponding inequalities for all the partial derivatives of $n(u, v)$ that are of the appropriate orders. The inequality $n(u, v) \leqslant z$ implies

(a) when $|u| \leqslant \lambda|v|$, that $|v(u^2 + v^2)| \leqslant z$, so that

$$|u| \leqslant \lambda^{1/3} (u^2|v|)^{1/3} = O(\lambda^{1/3} z^{1/3}), \quad |v| \leqslant z^{1/3}, \tag{2.61}$$

and

(b) when $|u| > \lambda|v|$, that $\left(\dfrac{8}{27(1+\lambda^2)}\right)^{1/2} \left(u^2 + \dfrac{3+\lambda^2}{2} v^2\right)^{3/2} \leqslant z$, so that, since $\lambda > 3$,

$$u, \lambda v = O\left(u^2 + \frac{3+\lambda^2}{2} v^2\right)^{1/2} = O(\lambda^{1/3} z^{1/3}). \tag{2.62}$$

From (2.5) we have

$$\frac{\partial n}{\partial v} = O(\lambda^{2/3} z^{2/3}),$$

and it can be similarly shown that

$$\frac{\partial n}{\partial u} = O(\lambda^{1/3} z^{2/3}) = O(\lambda^{2/3} z^{2/3}).$$

For the higher derivatives we have for example that

$$\frac{\partial^2 n}{\partial v^2} = \begin{cases} 6|v| & \text{if} \quad |u| < \lambda|v|, \\ \left(\frac{2}{3(1+\lambda^2)}\right)^{1/2}\left\{(3+\lambda^2)\left(u^2+\frac{3+\lambda^2}{2}v^2\right)^{1/2} + \right. & \\ \left. + \frac{(3+\lambda^2)^2}{2\lambda^2}(\lambda v)^2\left(u^2+\frac{3+\lambda^2}{2}v^2\right)^{-1/2}\right\} & \text{if} \quad |u| > \lambda|v| \end{cases}$$

$$= O(\lambda^{4/3}z^{1/3}),$$

by (2.6), and

$$\frac{\partial^3 n}{\partial v^3} = \begin{cases} 6\operatorname{sign} v & \text{if} \quad |u| < \lambda|v|, \\ \left(\frac{2}{3(v+\lambda^2)}\right)^{1/2}\left\{\frac{3(3+\lambda^2)^2}{2\lambda}(\lambda v)\left(u^2+\frac{3+\lambda^2}{2}v^2\right)^{-1/2} - \right. & \\ \left. - \frac{(3+\lambda^2)^3}{4\lambda^3}(\lambda v)^3\left(u^2+\frac{3+\lambda^2}{2}v^2\right)^{-3/2}\right\} & \text{if} \quad |u| > \lambda|v| \end{cases}$$

$$= O(\lambda^2).$$

Similar results hold for the five other relevant derivatives, and the result of the lemma follows.

LEMMA 2. *With the region $\mathscr{R}_3(z)$ as defined in* (2.32), *we have*

$$\iint_{\mathscr{R}_3(z)} dx\,dy = O(z^{2/3}/\lambda^{1/3}), \tag{2.71}$$

$$\sum_{(r,s)\in\mathscr{R}_3(Z)} 1 = O(Z^{2/3}/\lambda^{1/3}), \tag{2.72}$$

the sum being over the integer points of $\mathscr{R}_3(Z)$.

Use of (2.11) gives

$$\iint_{\mathscr{R}_3(z)} dx\,dy = |\alpha\delta-\beta\gamma| \iint_{\mathscr{S}_3(z)} du\,dv.$$

In the region $\mathscr{S}_3(z)$ the equations (2.31), (2.12) and (2.14) give, for some constant c_1, that $|v| \leqslant z/u^2$ and $|u| \geqslant c_1(\lambda z)^{1/3}$. Hence

$$\iint_{\mathscr{R}_3(z)} dx\,dy = O\Big(\int_{c_1(\lambda z)^{1/3}}^{\infty} du \int_0^{z/u^2} dv\Big) = O(z^{2/3}/\lambda^{1/3}). \tag{2.73}$$

Proceed to (2.72). Let us denote by $\mathscr{R}_4(z)$ that subset of $\mathscr{R}_3(z)$ in which $|y| \leqslant z^{1/2}$, and by $\mathscr{R}_5(z)$ that in which $|y| > z^{1/2}$. Then $\mathscr{R}_4(z)$ has area $O(z^{2/3}/\lambda^{1/3})$, by (2.71). Also, a simple argument shows that its perimeter is $O(z^{1/2})$. Hence, taking $z = Z$,

$$\sum_{(r,s)\in\mathscr{R}_4(Z)} 1 = O(Z^{2/3}/\lambda^{1/3}) + O(Z^{1/2}) = O(Z^{1/3}/\lambda^{1/3}), \tag{2.74}$$

since we specified $\lambda < Z^{1/2}$ in (2.12). It is shown in Chapter 1 of [4] that

$$\sum_{\substack{0<f(r,s)\leqslant Z \\ |s|>Z^{5/8}}} 1 = O(Z^{3/8}),$$

and the same method gives

$$\sum_{(x,y)\in\mathscr{R}_5(Z)} 1 = O(Z^{1/2}).$$

With (2.73), this yields (2.72).

For the subsequent development of the argument we require one further lemma, a version of the Poisson sum-formula, in which we use the following terminology. Call a region $\mathscr{T}$ of an (x, y)-plane simple if it is enclosed by a simple closed Jordan curve, traced by $\big(x(t), y(t)\big)$, say, such that $x(t)$ and $y(t)$ have a finite number of turning points. It then follows that the boundary of a simple region is met by any line parallel to an axis, the y-axis, say, in a finite number of points. The case of Lemma 3 in which $\mathscr{T}$ is the circle $x^2+y^2 \leqslant a$ and $\theta(x, y) = a-x^2-y^2$ is established in [5]; we adapt the procedure used therein to our purposes.

LEMMA 3. *Suppose that a function $\theta(x, y)$ is continuous in a simple region $\mathscr{T}$ including its boundary, on which $\theta(x, y) = 0$. Suppose also that $\mathscr{T}$ can be divided into a finite number of simple sub-regions $\mathscr{T}_j$ such that in the interior of each $\mathscr{T}_j$ the functions $\frac{\partial^2\theta}{\partial x^2}$ and $\frac{\partial^2\theta}{\partial y^2}$ are continuous and bounded. Then*

$$\sum_{(r,s)\in\mathscr{T}} \theta(r, s) = \sum_{g,h=-\infty}^{\infty} \iint_{\mathscr{T}} e(gx+hy)\theta(x, y)\,dx\,dy.$$

Here, the infinite summation and the notation $e(x)$ have the significance described in the introduction.

We have first

$$\sum_{a\leqslant s\leqslant b} f(s) = \sum_{h=-\infty}^{\infty} \int_a^b e(hy)f(y)\,dy, \tag{2.81}$$

certainly valid if $f(a) = f(b) = 0$ and $f(y)$ is continuous and of bounded variation in $a \leqslant y \leqslant b$. A proof is indicated in [5]. For each x define

$$\Theta(x) = \sum_{(x,s)\in\mathscr{T}} \theta(x, s),$$

the summation being over the indicated integers s. A finite number of applications of (2.81) gives

$$\Theta(x) = \sum_{h=-\infty}^{\infty} \int_{(x,y)\in\mathscr{T}} e(hy)\theta(x, y)\,dy. \tag{2.82}$$

Since $\theta(x,y)$ vanishes on the boundary of $\mathscr{T}$, integration by parts gives

$$\int\limits_{(x,y)\in\mathscr{T}} e(hy)\theta(x,y)\,dy = \frac{-1}{2\pi i h}\int\limits_{(x,y)\in\mathscr{T}} \frac{\partial\theta}{\partial y}(x,y)e(hy)\,dy.$$

Consider the contribution to the integral on the right from one of the sub-regions $\mathscr{T}_j$. The range of integration consists of a finite number of intervals (y_{2i}, y_{2i+1}), over any one of which

$$\int\limits_{y_{2i}}^{y_{2i+1}} e(hy)\frac{\partial\theta}{\partial y}(x,y)\,dy = \frac{1}{2\pi i h}\left\{e(hy)\frac{\partial\theta}{\partial y}(x,y)\Big|_{y_{2i}}^{y_{2i+1}} - \int\limits_{y_{2i}}^{y_{2i+1}} e(hy)\frac{\partial^2\theta}{\partial y^2}(x,y)\,dy\right\}.$$

But $\dfrac{\partial^2\theta}{\partial y^2}$ and $\dfrac{\partial\theta}{\partial y}$ are bounded in $\mathscr{T}_j$, so we obtain

$$\Big|\int\limits_{(x,y)\in\mathscr{T}} e(hy)\theta(x,y)\,dy\Big| \leqslant c_2/h^2, \tag{2.83}$$

for some constant c_2, depending only on $\mathscr{T}$ and the function θ.

The region $\mathscr{T}$ is contained within some rectangle $X_1 \leqslant x \leqslant X_2$, $Y_1 \leqslant y \leqslant Y_2$, and we may extend the definition of the continuous and piecewise smooth function $\theta(x,y)$ over it by defining $\theta(x,y) = 0$ outside $\mathscr{T}$. Then $\Theta(X_1) = \Theta(X_2) = 0$. Also we can show that $\Theta(x)$ is continuous and of bounded variation in $X_1 \leqslant x \leqslant X_2$. For we have, for any dissection $X_1 = x_0 < x_1 < \ldots < x_n = X_2$ of (X_1, X_2),

$$\sum_{1\leqslant i\leqslant n}|\Theta(x_i)-\Theta(x_{i-1})| = \sum_{1\leqslant i\leqslant n}\Big|\sum_{Y_1\leqslant s\leqslant Y_2}\theta(x_i,s)-\theta(x_{i-1},s)\Big| \leqslant \sum_{Y_1\leqslant s\leqslant Y_2}\sum_{1\leqslant i\leqslant n}|\theta(x_i,s)-\theta(x_{i-1},s)|,$$

which is bounded, in virtue of the conditions on $\theta(x,y)$. Furthermore,

$$|\Theta(x)-\Theta(x')| \leqslant \sum_{Y_1\leqslant s\leqslant Y_2}|\theta(x,s)-\theta(x',s)|,$$

which is small for small $|x-x'|$, by the continuity of $\theta(x,y)$.

Application of the summation formula (2.81) to $\Theta(x)$ gives

$$\sum_{X_1\leqslant r\leqslant X_2}\Theta(r) = \sum_{g=-\infty}^{\infty}\int\limits_{X_1}^{X_2} e(gx)\Theta(x)\,dx = \sum_{g=-\infty}^{\infty}\int\limits_{X_1}^{X_2} dx\sum_{h=-\infty}^{\infty}\int\limits_{(x,y)\in\mathscr{T}} e(gx+hy)\theta(x,y)\,dy,$$

by (2.82). We can, using (2.83), invert the order of h-summation and x-integration, obtaining

$$\sum_{(r,s)\in\mathscr{T}}\theta(r,s) = \sum_{g,h=-\infty}^{\infty}\iint\limits_{\mathscr{T}} e(gx+hy)\theta(x,y)\,dx\,dy,$$

as required.

3. Preliminary decomposition of Σ_1. We are now in a good position to commence the investigation of the sum Σ_1 defined in (1.5). With the regions $\mathscr{R}_i(Z)$ as defined by (2.32) we have

$$\Sigma_1 = \sum_{(r,s)\in\mathscr{R}_1(Z)\cup\mathscr{R}_2(Z)} d(|f|) + \sum_{(r,s)\in\mathscr{R}_3(Z)} d(|f|),$$

the symbol f being, as explained in the introduction, an abbreviation for $f(r,s)$. Use of Lemma 2 and the estimate

$$d(n) = O(n^\varepsilon) \tag{3.11}$$

gives

$$\Sigma_1 = \sum_{(r,s)\in\mathscr{R}_1(Z)\cup\mathscr{R}_2(Z)} d(|f|) + O(Z^{2/3+\varepsilon}/\lambda^{1/3}). \tag{3.12}$$

Let the sequence (a_n) of (1.1) now be that of numbers a_n representable as

$$a_n = |f(r,s)|\colon\ (r,s)\in\mathscr{R}_1(Z)\cup\mathscr{R}_2(Z),$$

the number a appearing exactly t times in (a_n) if it is thus representable just t times. By (2.32), the region $\mathscr{R}_1(z)\cup\mathscr{R}_2(z)$ is given by $m(x,y)\leqslant z$, and in it we have $|f(x,y)|\leqslant m(x,y)$. Hence the a_n all satisfy $a_n \leqslant Z$, and (1.4) becomes

$$\sum_{\substack{(r,s)\in\mathscr{R}_1(Z)\cup\mathscr{R}_2(Z)\\(r,s)\neq(0,0)}} d(|f|) = 2\sum_{1\leqslant l\leqslant Z^{1/2}}\sum_{\substack{m\leqslant Z\\ f\equiv 0\,(\mathrm{mod}\,l)}} 1 - \sum_{1\leqslant l\leqslant Z^{1/2}}\sum_{\substack{m\leqslant lZ^{1/2}\\ f\equiv 0\,(\mathrm{mod}\,l)}} 1 + O(Z^{1/2}) = 2\Sigma_2 - \Sigma_3 + O(Z^{1/2}), \tag{3.13}$$

say, where the inner sums are now over the lattice points (r,s) — including $(0,0)$, whence the error term — that satisfy the indicated conditions. Since we stipulated $\lambda < Z^{1/2}$ in (2.13) we now have from (3.12)

$$\Sigma_1 = 2\Sigma_2 - \Sigma_3 + O(Z^{2/3+\varepsilon}/\lambda^{1/3}). \tag{3.14}$$

The sums Σ_2 and Σ_3 are both expressible in terms of the function

$$A(L,z,a) = \sum_{1\leqslant l\leqslant L}\sum_{\substack{m\leqslant zl^a\\ f\equiv 0\,(\mathrm{mod}\,l)}} 1 \tag{3.21}$$

by the equations

$$\Sigma_2 = A(Z^{1/2}, Z, 0), \qquad \Sigma_3 = A(Z^{1/2}, Z^{1/2}, 1). \tag{3.22}$$

For any increasing function $\Phi(z)$ denote by $\Phi_{(2)}(z)$ its second integral

$$\Phi_{(2)}(z) = \int_0^z dz_1 \int_0^{z_1} \Phi(z_2)\,dz_2. \tag{3.31}$$

Inversion of the order of integration and the summation involved in the definition of $A(L, z, \alpha)$ gives, in this notation,

$$A_{(2)}(L, z, \alpha) = \sum_{1\leqslant l\leqslant L} \sum_{\substack{m\leqslant zl^{\alpha} \\ f\equiv 0 \,(\mathrm{mod}\, l)}} \tfrac{1}{2}(z - ml^{-\alpha})^2. \tag{3.32}$$

Similarly, if we define

$$J(z) = \iint_{m\leqslant z} dx\,dy, \tag{3.33}$$

then

$$J_{(2)}(z) = \iint_{m\leqslant z} \tfrac{1}{2}(z-m)^2\,dx\,dy. \tag{3.34}$$

Denote by (a, b) a typical root of the congruence

$$f(a, b) \equiv 0 \,(\mathrm{mod}\, l). \tag{3.41}$$

When $r \equiv a, s \equiv b \,(\mathrm{mod}\, l)$ make the transformation

$$r = a + lR, \quad s = b + lS, \tag{3.42}$$

and define

$$M_{a,b} = M_{a,b}(R, S) = m(a + lR, b + lS).$$

Then (3.32) becomes

$$A_{(2)}(L, z, \alpha) = \sum_{1\leqslant l\leqslant L} \sum_{\substack{1\leqslant a,b\leqslant l \\ f(a,b)\equiv 0 \,(\mathrm{mod}\, l)}} \sum_{M_{a,b}\leqslant zl^{\alpha}} \tfrac{1}{2}(z - M_{a,b}l^{-\alpha})^2. \tag{3.51}$$

Recall that the line-pair L given by (2.33) divides the region $m \leqslant z$ into the four regions $\mathscr{R}_1^+(z)$, etc., defined as indicated in (2.34). A straightforward argument shows that these are simple, in the sense described in connection with Lemma 3. As was pointed out in Lemma 1, the function $m(x, y)$ can be differentiated any number of times in each of these regions. Thus, on using (3.42), we see that we may apply Lemma 3 to the inner sum in (3.51), to obtain

$$A_{(2)}(L, z, \alpha) = \sum_{1\leqslant l\leqslant L} \sum_{a,b} \sum_{g,h=-\infty}^{\infty} \iint_{M_{a,b}\leqslant zl^{\alpha}} \tfrac{1}{2}(z - M_{a,b}l^{-\alpha})^2 e(gX + hY)\,dX\,dY. \tag{3.52}$$

Transforming back to the (x, y)-plane by (3.42) gives

$$A_{(2)}(L, z, \alpha) = \sum_{1\leqslant l\leqslant L} \frac{1}{l^2} \sum_{a,b} \sum_{g,h=-\infty}^{\infty} \iint_{m\leqslant zl^{\alpha}} \frac{1}{2}(z - ml^{-\alpha})^2 e\left(\frac{g(x-a) + h(y-b)}{l}\right) dx\,dy.$$

The region of integration is independent of a, b, so this gives

$$A_{(2)}(L, z, \alpha) = \sum_{1\leqslant l\leqslant L} l^{-2-2\alpha} \sum_{g,h=-\infty}^{\infty} \overline{S}(g, h; l) I(g, h; l, zl^{\alpha}), \tag{3.53}$$

where

$$S(g, h; l) = \sum_{\substack{1\leqslant a,b\leqslant l \\ f(a,b)\equiv 0 \,(\mathrm{mod}\, l)}} e\left(\frac{ga + hb}{l}\right), \tag{3.6}$$

$\overline{S}(g, h; l)$ is its complex conjugate, and

$$I(g, h; l, z) = \iint_{m\leqslant z} \frac{1}{2}(z-m)^2 e\left(\frac{gx + hy}{l}\right) dx\,dy. \tag{3.7}$$

From the above expression for $A_2(L, z, \alpha)$ an asymptotic formula for it could, using what follows, be derived. The leading term in this formula would be that in $g = h = 0$, in which $S(g, h; l)$ reduces to $\tau(l)$, the number of roots of (3.41), and $I(g, h; l, z)$ to $J_{(2)}(z)$ as given in (3.34). Accordingly we recast (3.53) as

$$\begin{aligned} A_{(2)}(L, z, \alpha) &= \sum_{1\leqslant l\leqslant L} \frac{\tau(l)}{l^{2+2\alpha}} J_{(2)}(zl^{\alpha}) + \sum_{1\leqslant l\leqslant L} \frac{1}{l^{2+2\alpha}} \sum_{g^2+h^2>0} \overline{S}(g, h; l) I(g, h; l, zl^{\alpha}) \\ &= \Sigma_4(L, z, \alpha) + \Sigma_5(L, z, \alpha), \end{aligned} \tag{3.8}$$

say, where the summation over g, h is to be interpreted as indicated in the introduction. What will actually be derived is an asymptotic formula for the second z-derivative $A(L, z, \alpha)$ of $A_{(2)}(L, z, \alpha)$. To this end we need asymptotic expressions not for $J_{(2)}(z)$ but for $J(z)$, and for the resulting sums over l. We also need upper bounds for $S(g, h; l)$ and $I(g, h; l, z)$ when $g^2 + h^2 > 0$. These topics form the subject matter of the next three sections.

4. The integrals $I(g, h; l, z)$ and $J(z)$. First consider $J(z)$, as defined in (3.33). We have

$$J(z) = \iint_{|f|\leqslant z} dx\,dy + O\Big(\iint_{\mathscr{R}_3(z)} dx\,dy\Big) = \iint_{|f|\leqslant z} dx\,dy + O(z^{2/3}/\lambda^{1/3}),$$

by Lemma 2. The last integral was evaluated in Chapter 1 of [4], and we obtain (bearing in mind that in [4] the symbol D has a different meaning)

$$J(z) = c_3 z^{2/3} + O(z^{2/3}/\lambda^{1/3}), \tag{4.11}$$

where

$$c_3 = \frac{\sqrt{3}}{2|D|^{1/6}} \cdot \frac{\Gamma^2(\frac{1}{3})}{\Gamma(\frac{2}{3})}. \tag{4.12}$$

When $g^2+h^2>0$ we shall establish

$$I(g,h;l,z) = O\left(l^3\lambda^2 z^{5/3}(g^2+h^2)^{-3/2}\right). \tag{4.2}$$

Suppose, for example, that $g \neq 0$. Then

$$I(g,h;l,z) = \frac{l}{2\pi i g}\iint_{m\leqslant z}(z-m)\frac{\partial m}{\partial x}\,e\left(\frac{gx+hy}{l}\right)dx\,dy$$
$$= \frac{l^2}{4\pi^2 g^2}\iint_{m\leqslant z}\left\{(z-m)\frac{\partial^2 m}{\partial x^2}-\left(\frac{\partial m}{\partial x}\right)^2\right\}e\left(\frac{gx+hy}{l}\right)dx\,dy,$$

the two integrations by parts being permitted by the results of Lemma 1. Now consider separately the contribution from each of the sub-regions $\mathscr{R}_1^+(z)$, etc., defined as indicated in (2.34). Over any one of these, denoted by $\mathscr{R}$, say, a further partial integration shows that the contribution to $I(g,h;l,z)$ is

$$\frac{l^3}{8\pi^2 i g^3}\oint_{\partial\mathscr{R}}\left\{(z-m)\frac{\partial^2 m}{\partial x^2}-\left(\frac{\partial m}{\partial x}\right)^2\right\}e\left(\frac{gx+hy}{l}\right)dx- \tag{4.3}$$
$$-\frac{l^3}{8\pi^2 i g^3}\iint_{\mathscr{R}}\left\{(z-m)\frac{\partial^3 m}{\partial x^3}-3\frac{\partial m}{\partial x}\frac{\partial^2 m}{\partial x^2}\right\}e\left(\frac{gx+hy}{l}\right)dx\,dy,$$

the first integral being one round the boundary of $\mathscr{R}$. A simple argument based on (2.6) shows that

$$\oint_{\partial\mathscr{R}} dx = O(\lambda^{1/3}z^{1/3}),$$

while (4.1) gives

$$\iint_{\mathscr{R}} dx\,dy = O(z^{2/3}).$$

Estimates for the integrands in (4.3) are provided by Lemma 1, and we find

$$I(g,h;l,z) = O(l^3\lambda^2 z^{5/3}/|g|^3).$$

We supposed $g\neq 0$; a similar inequality holds if $h\neq 0$, and (4.2) follows.

We also require the trivial estimate

$$I(g,h;l,z) = O(z^{8/3}); \tag{4.4}$$

this follows from (4.11).

5. The sum $\sum_{1\leqslant l\leqslant L}\tau(l)/l^{2-2\alpha/3}$. Asymptotic formulae will be required for this sum when $\alpha=0$ or $\alpha=1$. These expressions will be derived via an appropriate consideration of the Dirichlet series

$$T(s) = \sum_{l=1}^{\infty}\tau(l)/l^{1+s}, \tag{5.1}$$

which, for some s_0, converges absolutely when $s>s_0$. The trivial estimate $\tau(l)\leqslant l^2$ shows we can take $s_0=2$; it will however appear that $s_0=1$ is best possible.

First, we require the following lemmas concerning the values assumed by $\tau(l)$. Define

$$g(x) = f(x,1), \tag{5.2}$$

so that $g(x)$ is a polynomial in x, irreducible over the rationals, having discriminant D and leading coefficient a_0. Denote by $\varrho(l)$ the number of roots of the congruence

$$g(r)\equiv 0 \pmod{l}.$$

LEMMA 4. *For any prime power p^ν we have*

$$\varrho(p^\nu) = O(1).$$

There is a proof in [7].

For the number $\tau(l)$ of roots of the corresponding homogeneous congruence the following result holds.

LEMMA 5. *With $\varrho(l)$ as defined above, we have*

(i) *if p is prime and $p\nmid a_0a_3$,*

$$\tau(p) = (p-1)\varrho(p)+1;$$

(ii) *for any prime p,*

$$\tau(p^\nu) = O(p^{4\nu/3}).$$

(i) Since $p\nmid a_0a_3$ the roots r,s of $f(r,s)\equiv 0 \pmod p$ satisfy either $r\equiv s\equiv 0 \pmod p$ or $(r,p)=(s,p)=1$. When $(s,p)=1$ the substitution $r\equiv os \pmod p$ shows that, given s, there are $\varrho(p)$ solutions for $r \pmod p$.

(ii) For any r,s define λ,μ, temporarily abandoning the notation of (2.13), by

$$p^\lambda = (r,p^\nu), \quad p^\mu = (s,p^\nu).$$

Consider first those roots for which $\lambda,\mu\geqslant\nu/3$. Since $\lambda\geqslant\nu/3$ is equivalent to $\lambda\geqslant -[-\nu/3]$, the number of such roots is

$$p^{2(\nu+[-\nu/3])} = O(p^{4\nu/3}). \tag{5.31}$$

Of the remaining roots, it suffices to consider those for which $\mu < \nu/3$, $\mu \leqslant \lambda$. On making the substitution $r = p^\lambda r_1$, $s = p^\mu s_1$, we find they are given by the solutions for r_1, s_1, λ, μ of

$$\begin{cases} f(p^\lambda r_1, p^\mu s_1) \equiv 0 \pmod{p^\nu}, \quad (r_1, p) = (s_1, p) = 1, \\ 1 \leqslant r_1 \leqslant p^{\nu-\lambda},\ 1 \leqslant s_1 \leqslant p^{\nu-\mu},\ 0 \leqslant \mu < \nu/3,\ \mu \leqslant \lambda. \end{cases} \tag{5.32}$$

These solutions satisfy

$$f(p^{\lambda-\mu} r_1, s_1) \equiv 0 \pmod{p^{\nu-3\mu}}.$$

The substitution $r_1 \equiv \omega s_1 \pmod{p^{\nu-3\mu}}$ shows that for given s_1, λ, μ the number of r_1 satisfying (5.32) is at most $O\{(p^{3\mu-\lambda}+1)N\}$, where N is the number of roots of the congruence

$$g(p^{\lambda-\mu}\omega) = p^{3(\lambda-\mu)} a_0 \omega^3 + p^{2(\lambda-\mu)} a_1 \omega^2 + p^{\lambda-\mu} a_2 \omega + a_3 \equiv 0 \pmod{p^{\nu-3\mu}}. \tag{5.33}$$

We now show that N is bounded, independently of p, λ, μ and ν. Define δ by $p^\delta \| a_3$. Then $N = 0$ unless $\min\{\lambda-\mu, \nu-3\mu\} \leqslant \delta$. If $\nu - 3\mu \leqslant \delta$ then $p^{\nu-3\mu} \leqslant a_3$, and $N \leqslant a_3 = O(1)$. If $\lambda - \mu \leqslant \delta$ then the coefficients in (5.33) are bounded, and so, by a finite number of applications of Lemma 5, we again have $N = O(1)$.

Summation over the values of s_1, λ and μ indicated in (5.32) gives, using (5.31),

$$\begin{aligned} \tau(p^\nu) &= O\Big\{ \sum_{\mu < \nu/3} \sum_{\mu \leqslant \lambda \leqslant \nu} p^{\nu-\mu}(p^{3\mu-\lambda}+1)\Big\} + O(p^{4\nu/3}) \\ &= O\Big(p^\nu \sum_{\mu<\nu/3} p^{2\mu} \sum_{\lambda \geqslant \mu} p^{-\lambda} + p^\nu \sum_{\mu<\nu/3} p^{-\mu} \sum_{\lambda \leqslant \nu} 1\Big) + O(p^{4\nu/3}) = O(p^{4\nu/3}), \end{aligned}$$

as required.

Next, we turn our attention to $\varrho(p)$. With $g(x)$ as defined in (5.2), let $K(\theta)$ be the field obtained by adjoining a root of $g(\theta) = 0$ to the rationals. For all save a finite number of p, sufficient information on $\varrho(p)$ is obtained by means of the following result, due to Dedekind.

LEMMA 6. *Suppose $p \nmid D$, so that in $K(\theta)$ the principal ideal (p) factorises as a product*

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r$$

of distinct prime ideals $\mathfrak{p}_i$, where $1 \leqslant r \leqslant 3$. Then $\varrho(p)$ is equal to the number of $\mathfrak{p}_i$ whose norm $N(\mathfrak{p}_i)$ satisfies $N(\mathfrak{p}_i) = p$.

For a proof, see [1], for example.

We introduce the Dedekind ζ-function of the field $K(\theta)$,

$$\zeta(s) = \sum_{n=1}^{\infty} t(n)/n^s, \tag{5.4}$$

where

$$t(n) = \sum_{N\mathfrak{a}=n} 1,$$

the summation being over the ideals $\mathfrak{a}$ of $K(\theta)$. We use the following estimate for the number of $\mathfrak{a}$ satisfying $N\mathfrak{a} \leqslant z$:

LEMMA 6′. *As $z \to \infty$,*

$$\sum_{n \leqslant z} t(n) = h_0 z + O(z^{5/6+\varepsilon}),$$

where $h_0 \neq 0$.

There is a proof, by an elementary method, in [8]. Alternatively, the more powerful analytic method described in [6] can be used. Either method in fact gives a result stronger than the above. This, however, is all that we require.

The constant h_0 is the residue at $s = 1$ of $\zeta(s)$.

With the aid of these lemmas we can first obtain a useful expression for the Dirichlet series $T(s)$ defined in (5.1). For $s > s_0$ we have, since $\tau(l)$ is a multiplicative function of l,

$$\begin{aligned} T(s) &= \prod_p \sum_{\nu=1}^{\infty} \frac{\tau(p^\nu)}{p^{\nu s}} \\ &= \prod_{p \mid \Delta} \Big\{1 + \sum_{\nu=1}^{\infty} \frac{O(p^{4\nu/3})}{p^{\nu+\nu s}}\Big\} \prod_{p \nmid \Delta} \Big\{1 + \frac{\varrho(p)}{p^s} + \frac{O(1)}{p^{s+1}} + \sum_{\nu=2}^{\infty} \frac{O(p^{4\nu/3})}{p^{\nu+\nu s}}\Big\}, \end{aligned}$$

by Lemma 6, where $\Delta = a_0 a_3 D$. Hence

$$T(s) = \prod_{p \mid \Delta} \Big\{1 + \sum_{\nu=1}^{\infty} \frac{O(p^{\nu/3})}{p^{\nu s}}\Big\} \prod_{p \nmid \Delta} \Big\{\Big(1 - \frac{1}{p^s}\Big)^{-\varrho(p)}\Big\} R_1(s), \tag{5.51}$$

where, as follows after a little calculation,

$$R_1(s) = \prod_{p \nmid \Delta} \Big\{1 + \frac{O(1)}{p^{s+1}} + \sum_{\nu=2}^{\infty} \frac{O(p^{\nu/3})}{p^{\nu s}}\Big\}. \tag{5.52}$$

The function $\zeta(s)$ of (5.4) is expressible as an Euler product

$$\zeta(s) = \prod_{\mathfrak{p}} \{1 - (N\mathfrak{p})^{-s}\}^{-1}.$$

When $p \nmid D$ there are, by Lemma 6, exactly $\varrho(p)$ prime ideals $\mathfrak{p}$ with $N\mathfrak{p} = p$, so

$$\zeta(s) = \prod_{\mathfrak{p} \mid \Delta} \{1 - (N\mathfrak{p})^{-s}\}^{-1} \prod_{p \nmid \Delta} (1 - p^{-s})^{-\varrho(p)} \Big\{1 + \frac{O(1)}{p^{2s}} + \frac{O(1)}{p^{3s}}\Big\}^{-1}.$$

Thus (5.51) gives

$$T(s) = \zeta(s)\prod_{p\mid\Delta}\Big\{1+\sum_{\nu=1}^{\infty}\frac{O(p^{\nu/3})}{p^{\nu s}}\Big\}\prod_{p\nmid\Delta}\{1-(Np)^{-s}\}R_1(s)R_2(s),$$

where

$$R_2(s) = \prod_{p\nmid\Delta}\Big\{1+\frac{O(1)}{p^{2s}}+\frac{O(1)}{p^{3s}}\Big\}.$$

Hence

$$T(s) = \zeta(s)\prod_{p\mid\Delta}\Big\{1+\sum_{\nu=1}^{\infty}\frac{O(p^{\nu/3})}{p^{\nu s}}\Big\}\prod_{p\nmid\Delta}\Big\{1+\frac{O(1)}{p^{s+1}}+\sum_{\nu=2}^{\infty}\frac{O(p^{\nu/3})}{p^{\nu s}}\Big\} \tag{5.61}$$
$$= \zeta(s)R(s),$$

say.

We also express $R(s)$ as a series

$$R(s) = \sum_{n=1}^{\infty} r(n)/n^s. \tag{5.62}$$

When $s_0 > 5/6$ (and $s \geqslant s_0$) we have

$$\sum_{\nu=2}^{\infty}\frac{O(p^{\nu/3})}{p^{\nu s}} = O(p^{-2(s_0-1/3)}),$$

and $\sum n^{-2(s_0-1/3)}$ converges, so that the infinite product (and hence the series) for $R(s)$ converge absolutely, to a non-zero limit. In particular

$$R(1) \neq 0. \tag{5.63}$$

Let $F(L)$ be the "coefficient-sum"

$$F(L) = \sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l}$$

of the series $T(s)$. By (5.1), (5.4) and (5.6) we have

$$F(L) = \sum_{1\leqslant mn\leqslant L} r(m)t(n) = \sum_{1\leqslant m\leqslant L} r(m)\Big\{h_0\frac{L}{m}+O\Big(\frac{L}{m}\Big)^{5/6+\varepsilon}\Big\},$$

by Lemma 6′. Hence

$$F(L) = h_0R(1)L - h_0L\sum_{m>L}\frac{r(m)}{m}+O\Big(L^{5/6+\varepsilon}\sum_{1\leqslant m\leqslant L}|r(m)|/m^{5/6+\varepsilon}\Big)$$
$$= h_0R(1)L+O\Big(L^{5/6+\varepsilon}\sum_{m=1}^{\infty}|r(m)|/m^{5/6+\varepsilon}\Big)$$
$$= h_0R(1)L+O(L^{5/6+\varepsilon}) = c_4L+v(L),$$

say. Note that we have, from (5.63) and Lemma 6′,

$$c_4 = h_0R(1) \neq 0. \tag{5.71}$$

The results we require are now easily obtained by partial summation. We have

$$\sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l^2} = \sum_{1\leqslant l\leqslant L}\frac{F(l)-F(l-1)}{l} = \sum_{1\leqslant l\leqslant L}\frac{F(l)}{l(l+1)}+\frac{F(|L|)}{|L|+1} \tag{5.72}$$
$$= c_4\sum_{1\leqslant l\leqslant L+1}\frac{1}{l}+\sum_{1\leqslant l\leqslant L}\frac{v(l)}{l(l+1)}+O(L^{-1/6+\varepsilon})$$
$$= c_4\log L+c_4\gamma+\sum_{l=1}^{\infty}\frac{v(l)}{l(l+1)}+O(L^{-1/6+\varepsilon})$$
$$= c_4\log L+c_5+O(L^{-1/6+\varepsilon}),$$

say. Also

$$\sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l^{4/3}} = \sum_{1\leqslant l\leqslant L}\frac{F(l)}{3l^{4/3}}\{1+O(l^{-1})\}+\frac{F(|L|)}{(|L|+1)^{1/3}} \tag{5.73}$$
$$= \tfrac{3}{2}c_4L^{2/3}+O(L^{1/2+\varepsilon}).$$

We remark that it is possible to identify the constants c_4 and c_5 as

$$c_4 = G(1), \quad c_5 = G'(1), \tag{5.8}$$

where the function $G(s)$, continuous for $s \geqslant s_0 > 5/6$, is defined by

$$G(s) = (s-1)\zeta(s)R(s).$$

This identification is, however, of no particular importance in the sequel.

6. The exponential sums $S(g, h; l)$. In a sense the preceding work has been mainly analytic; the principal number-theoretic content of the argument is in the derivation of upper bounds for the sums $S(g, h; l)$ given in (3.6). These appear in Lemma 9; first we obtain an estimate for a related sum $S^{(1)}(g, h; l)$, subject to a special restriction on g, h and l.

We make the convention that the "greatest common divisors" $(0, l)$, $(g, 0, l)$, $(0, h, l)$ and $(0, 0, l)$ are to be defined by reading l for 0. The results of this section then remain valid, where applicable, even when $gh = 0$.

LEMMA 7. *Define*

$$S^{(1)}(l) = S^{(1)}(g, h; l) = \sum_{\substack{1\leqslant r,s\leqslant l;(r,s,l)=1\\ f(r,s)\equiv 0 \pmod l}} e\Big(\frac{gr+hs}{l}\Big).$$

Then, if $(g, h, l) = 1$,

$$S^{(1)}(l) = O\{(f(-h, g), l)\}.$$

If $l = l_1 l_2$ and $(l_1, l_2) = 1$ then a familiar method gives

$$S^{(1)}(l) = S^{(1)}(l_1) S^{(1)}(l_2).$$

Hence

$$S^{(1)}(l) = \prod_{p^a \| l} S^{(1)}(p^a), \tag{6.11}$$

and it suffices to establish the result in the case $l = p^a$.

We have in fact

$$S^{(1)}(p^a) = \sum_{1 \leqslant t \leqslant p^a} e(t/p^a)\psi(t), \tag{6.12}$$

where $\psi(t)$ is the number of incongruent solutions of

$$f(r, s) \equiv 0, \quad gr + hs \equiv t \pmod{p^a}, \quad (r, s, p) = 1. \tag{6.13}$$

Let $(t, p^a) = w$. Then we shall show

$$\psi(t) = \psi(w). \tag{6.14}$$

For $(t, p^a) = (w, p^a)$ and so there exists a u such that

$$ut \equiv w \pmod{p^a}, \quad (u, p) = 1.$$

If r, s satisfy (6.13) then $r' = ur$, $s' = us$ satisfy

$$f(r', s') \equiv 0, \quad gr' + hs' \equiv w \pmod{p^a}, \quad (r', s', p) = 1,$$

and so $\psi(t) \leqslant \psi(w)$. Similarly $\psi(w) \leqslant \psi(t)$, and (6.14) follows.

Equation (6.12) now gives

$$\begin{aligned} S^{(1)}(p^a) &= \sum_{w | p^a} \psi(w) \sum_{\substack{1 \leqslant t \leqslant p^a \\ (t, p^a) = w}} e(t/p^a) \\ &= \sum_{w | p^a} \psi(w)\mu(p^a/w) = \psi(p^a) - \psi(p^{a-1}), \end{aligned} \tag{6.15}$$

by well-known properties of the Möbius function $\mu(w)$.

Since $(g, h, l) = 1$ we have for primes p dividing l that $(g, h, p) = 1$. For such primes p we shall prove that $\psi(p^a)$ and $\psi(p^{a-1})$ are both $O\{(f(h, g), p^a)\}$. We may suppose that $(g, p) = 1$. It then follows from (6.13) that for $w = p^a$ or $w = p^{a-1}$ we have, except when $a = w = 1$, that $\psi(w)$ is the number of roots of

$$f(w - hs, gs) \equiv 0 \pmod{p^a}, \quad (s, p) = 1. \tag{6.16}$$

Thus $\psi(p^a)$ is, for all a, the number of roots of

$$s^3 f(-h, g) \equiv 0 \pmod{p^a}, \quad (s, p) = 1,$$

and so is zero unless $p^a | f(-h, g)$, whence

$$\psi(p^a) = O\{(f(-h, g), p^a)\}. \tag{6.17}$$

When $a \geqslant 2$, $\psi(p^{a-1})$ is, from (6.16), the number of roots of

$$s^3 f(-h, g) + p^{a-1} s^2 f_1(-h, g) \equiv 0 \pmod{p^a}, \quad (s, p) = 1,$$

and so

$$\psi(p^{a-1}) = O\{(f(-h, g), p^a)\}. \tag{6.18}$$

When $a = 1$ we can show from (6.13) that $\psi(p^{a-1})$ is the number of roots of

$$f(1 - hs, gs) \equiv 0 \pmod{p},$$

which does not exceed 3 unless $p | f(-h, g)$, and so (6.18) still holds.

The result of the lemma now follows from (6.11), (6.15), (6.17) and (6.18).

LEMMA 8. *If $(kl, \Delta) = 1$, with $\Delta = a_0 a_3 D$ (as in the introduction), and if $\Sigma(k, l) = \Sigma(k, l; r', s')$ is the number of solutions r, s of $1 \leqslant r, s \leqslant kl$; $(r, s, kl) = 1$; $r \equiv r'$, $s \equiv s' \pmod{l}$, $f(r, s) \equiv 0 \pmod{kl}$, where $f(r', s') \equiv 0 \pmod{l}$, $(r', s', l) = 1$, then*

(i) *$\Sigma(k, l)$ is independent of the choice of r', s' subject to the above conditions,*

(ii) $\Sigma(k, l) = O(k^2)$.

Furthermore, if $p | l$ for all primes p dividing k then

(iii) $\Sigma(k, l) = O(k)$.

As did $S^{(1)}(g, h; l)$, $\Sigma(k, l)$ possesses a multiplicative property. Put

$$k = \prod_p p^\varkappa, \quad l = \prod_p p^\lambda$$

so that for each p one at most of the numbers $\varkappa = \varkappa(p)$ and $\lambda = \lambda(p)$ may vanish. Define $r'_p, s'_p \pmod{p^\lambda}$ by the relations

$$r' \equiv \sum_p \frac{kl}{p^{\varkappa+\lambda}} r'_p, \quad s' \equiv \sum_p \frac{kl}{p^{\varkappa+\lambda}} s'_p \pmod{l}.$$

Then

$$\Sigma(k, l; r', s') = \prod_p \Sigma(p^\varkappa, p^\lambda; r'_p, s'_p). \tag{6.21}$$

If r, s satisfy $f(r, s) \equiv 0 \pmod{p^\gamma}$; $(r, s, p) = 1$, where $\gamma \geqslant 1$, then all the roots of

$$f(r_1, s_1) \equiv 0 \pmod{p^{\gamma+1}}; \quad (r_1, s_1, p) = 1; \quad r_1 \equiv r, \quad s_1 \equiv s \pmod{p}$$

are given, on setting $r_1 = r + up^\gamma$, $s_1 = s + vp^\gamma$, by those of

$$uf_r(r, s) + vf_s(r, s) + \frac{f(r, s)}{p^\gamma} \equiv 0 \pmod{p}, \tag{6.22}$$

since $\gamma \geqslant 1$. Here $p \nmid a_0 D$, since $a_0 D | \Delta$, so for some polynomials A, B

$$A(r,s)f(r,s) + B(r,s)f_r(r,s) = a_0 D s^6,$$

since a_0 is the leading coefficient and Ds^6 the discriminant of $f(r,s)$, as a polynomial in r. Hence if $p | f(r,s)$ and $p | f_r(r,s)$ we have $p|s$. Therefore, since p is also prime to $a_3 D$,

$$\big(f_r(r,s), f_s(r,s), p\big) = (r,s,p) = 1.$$

Thus (6.22) has p roots.

Consider first the primes p dividing l, for which $\lambda \geqslant 1$. The above gives

$$\Sigma(p^\varkappa, p^\lambda) = p^\varkappa$$

(independently of r'_p, s'_p), by an induction on $\varkappa$. If $p \nmid l$ we have

$$\Sigma(p^\varkappa, p^\lambda) = \sum_{\substack{1 \leqslant r,s \leqslant p^\varkappa, (r,s,p)=1 \\ f(r,s) \equiv 0 \,(\mathrm{mod}\, p^\varkappa)}} 1 = O(p^{2\varkappa}),$$

again independent of r'_p, s'_p.

The results of the lemma now follow on using (6.21).

Next we obtain, for some moduli l, an estimate for the sums $S^{(1)}(g,h;l)$ independent of the hypothesis $(g,h,l) = 1$ of Lemma 7.

LEMMA 9. *Suppose* $(l, \Delta) = 1$. *Set* $(g,h,l) = \eta$, $g = \eta g_1$, $h = \eta h_1$, $l = \eta l_1$. *Then*

$$S^{(1)}(g,h;l) = O\big\{\eta^2 \big(f(-h_1, g_1), l_1\big)\big\}.$$

For

$$\begin{aligned} S_1(g,h;l) &= \sum_{\substack{1 \leqslant r,s \leqslant l, (r,s,l)=1 \\ f(r,s) \equiv 0 \,(\mathrm{mod}\, l)}} e\left(\frac{g_1 r + h_1 s}{l_1}\right) \\ &= \sum_{\substack{1 \leqslant r_1, s_1 \leqslant l_1, (r_1, s_1, l_1) = 1 \\ f(r_1, s_1) \equiv 0 \,(\mathrm{mod}\, l_1)}} e\left(\frac{g_1 r_1 + h_1 s_1}{l_1}\right) \Sigma(\eta, l_1; r_1, s_1) \\ &= \Sigma(\eta, l_1) S^{(1)}(g_1, h_1; l_1) = O\big\{\eta^2 |S^{(1)}(g_1, h_1; l_1)|\big\}, \end{aligned}$$

$\Sigma(l, l_1)$ being independent of r_1, s_1 by Lemma 7. Lemma 6 now yields the stated result.

Now we are in a position to obtain an estimate for the unrestricted sum $S(g,h;l)$. Set $l = kk'$, where $(k, \Delta) = 1$ and $p | k'$ implies $p | \Delta$. Then $(k,k') = 1$ and we have

$$S(g,h;l) = S(l) = S(k) S(k'). \tag{6.31}$$

For $S(k')$ we use a fairly trivial estimate. A procedure similar to that used to derive (6.15) gives

$$S(k') = \sum_{w | k'} \psi_1(w) \mu(k'/w) = O\Big\{\sum_{w | k'} \psi_1(w)\Big\},$$

where $\psi_1(w)$ is the number of roots of

$$f(r,s) \equiv 0, \quad gr + hs \equiv w \pmod{k'},$$

in which the second congruence, considered alone, has at most $k'(g,h,k')$ roots. Set

$$(g,h,k') = \delta', \quad k' = \delta' k'_1 \tag{6.32}$$

then

$$S(k') = O\{k' \delta' d(k')\} = O(\delta'^{2+\varepsilon} k_1'^{1+\varepsilon}). \tag{6.33}$$

For $S(k)$ consider first the case where k is a power $p^\varkappa$ of a prime p (not dividing Δ). We have

$$S(k) = \sum_{\alpha \leqslant \varkappa} \sum_{\substack{1 \leqslant r,s \leqslant k; (r,s,k) = p^\alpha \\ f(r,s) \equiv 0 \,(\mathrm{mod}\, k)}} e\left(\frac{gr+hs}{k}\right).$$

Consider first the subsum over values of α satisfying $\alpha \geqslant \varkappa/3$, for which the congruence condition is vacuous. Denoting by α_0 the least such α and setting $k = p^{\alpha_0} k_1$ the sum is

$$\begin{aligned} S^{(0)}(k) &= \sum_{1 \leqslant r,s \leqslant k; r \equiv s \equiv 0 \,(\mathrm{mod}\, p^{\alpha_0})} e\left(\frac{gr+hs}{k}\right) \\ &= \sum_{1 \leqslant r_1, s_1 \leqslant k_1} e\left(\frac{gr_1 + hs_1}{k_1}\right) = \sum_{1 \leqslant n_1 \leqslant k_1/\delta} e\left(\frac{\delta_1 n_1}{k_1}\right) \psi(n_1), \end{aligned}$$

where $\delta_1 = (g,h,k_1)$ and $\psi(n_1)$ is the number of roots r_1, s_1 of

$$gr_1 + hs_1 \equiv \delta_1 n_1 \pmod{k_1},$$

that is to say $\psi(n_1) = \delta_1 k_1$, independently of n_1. Thus

$$S^{(0)}(k) = \begin{cases} 0 & \text{if} \quad \delta_1 < k_1, \\ k_1^2 & \text{if} \quad \delta_1 = k_1. \end{cases} \tag{6.41}$$

For the remainder of $S(k)$ we have, setting $p^\alpha = A$,

$$\begin{aligned} S(k) - S^{(0)}(k) &= \sum_{\alpha < \alpha_0} \sum_{\substack{1 \leqslant r', s' \leqslant k/A, (r', s', k/A) = 1 \\ f(r', s') \equiv 0 \,(\mathrm{mod}\, k/(k, A^3))}} e\left(\frac{gr' + hs'}{k/A}\right) \\ &= \sum_{\alpha < \alpha_0} \sum \left(\frac{(k, A^3)}{A}, \frac{k}{(k, A^3)}\right) S^{(1)}\left(g, h; \frac{k}{(k, A^3)}\right), \end{aligned}$$

by the procedure used in the proof of Lemma 9. Part (iii) of Lemma 8 applies here to show (using the result of Lemma 9)

$$S(k)-S^{(0)}(k) = O\Big\{\sum_{A|k}\frac{(k,A^3)}{A}\,\delta_A^2\big(f(-h_1,g_1),k_2\big)\Big\}, \tag{6.42}$$

wherein

$$\delta_A = \big(g,h,k/(k,A^3)\big),\quad g=\delta_A g_1,\quad h=\delta_A h_1,\quad k_2 = k/(k,A^3)\delta_A. \tag{6.43}$$

Here, the term in $A=1$ majorises the estimate (6.41) for $S^{(0)}(k)$, so this provides an upper estimate for $S(k)$ as well as for $S(k)-S^{(0)}(k)$.

Read the definitions (6.43) as applying for all k, A $(A|k)$. Then the right side of (6.42), having been shown to express $S(k)$ for $k=p^\varkappa$, does so for all k prime to A, by the multiplicative properties of the functions involved.

Observe that since $\delta_A|k$, $\delta'|k'$ and $(k,k')=1$ we can by the definition (6.32) of δ' substitute

$$g=\delta'\delta_A g_2,\qquad h=\delta'\delta_A h_2$$

and obtain

$$S(k) = O\Big\{\sum_{A|k}\frac{(k,A^3)}{A}\,\delta_A^2\big(f(-h_2,g_2),k_2\big)\Big\}. \tag{6.5}$$

In the sequel, the only references involving $S(g,h;l)$ will be to the result of the following lemma, to the effect that the estimate for $S(g,h;l)$ implied by the above is in a certain "average" sense, not much larger than $O(1)$.

LEMMA 10. *Define*

$$Q(G,L) = \sum_{1\leqslant l\leqslant L;\,0<g^2+h^2\leqslant G}|S(g,h;l)|.$$

Then

$$Q(G,L) = O(L^{1+\varepsilon}G^{1+\varepsilon}).$$

The above results (6.3), (6.5) give, using the same notation,

$$Q(G,L) = O\Big\{L^\varepsilon\sum_{1\leqslant kk'\leqslant L}\ \sum_{A|k}\ \sum_{(\delta'\delta_A)^2/(g^2+h^2)\leqslant G}(\delta'\delta_A)^2k'(k,A^3)A^{-1}\big(f(-h_2,g_2),k_2\big)\Big\}.$$

Set $k=Ak_1$, so $(k,A^3)A^{-1}=(A^2,k_1)=\xi$, say, and let $k_2=k_1/\xi\delta_A$. Then

$$Q(G,L) = O\Big\{L^\varepsilon\sum_{\xi\leqslant L}\xi\sum_{\substack{A\leqslant L\\ A^2\equiv 0\,(\mathrm{mod}\,\xi)}}\ \sum_{\delta'k_1'A\xi\delta_Ak_2\leqslant L}\ \sum_{(\delta'\delta_A)^2(g_2^2+h_2^2)\leqslant G}(\delta\delta_A)^2k_1'\delta_3\Big\}$$

where $\delta_3=\big(f(-h_2,g_2),k_2\big)$. Set $k_2=\delta_3k_3$. Then the conditions of summation imply

$$\delta_3\leqslant L/\delta'k_1'A\xi\delta_Ak_3,\qquad \sum_{\delta_3}1\leqslant d\{f(-h_2,g_2)\}=O(G^\varepsilon).$$

Insertion of the inequality bounding δ_3 followed by summation over possible values of δ_3 gives

$$Q(G,L) = O\Big\{L^{1+\varepsilon}G^\varepsilon\sum_\xi\sum_{\substack{\delta'k_1'A\xi\delta_Ak_3\leqslant L\\ A^2\equiv 0\,\mathrm{mod}\,\xi}}\delta'\delta_AA^{-1}k_3^{-1}\sum_{g_2^2+h_2^2\leqslant G/(\delta'\delta_A)^2}1\Big\},$$

in which the inner sum is $O\{G/(\delta'\delta_A)^2\}$. So after summation over g_2, h_2, δ', δ_A and k_3 we find

$$Q(G,L) = O\Big\{L^{1+\varepsilon}G^{1+\varepsilon}\sum_{k_1'\leqslant L}\ \sum_{\xi\leqslant L}\ \sum_{\substack{A^2\equiv 0\,(\mathrm{mod}\,\xi)\\ A\leqslant L}}A^{-1}\Big\}.$$

But

$$\sum_{\xi\leqslant L}\ \sum_{\substack{A^2\equiv 0\,(\mathrm{mod}\,\xi)\\ A\leqslant L}}A^{-1} = \sum_{A\leqslant L}A^{-1}\sum_{\xi|A^2}1 = O(L^\varepsilon),$$

and if $p_1,p_2,\dots,p_r$ are the distinct primes dividing A then

$$\sum_{k_1'\leqslant L}1 = O\Big\{\sum_{p_1^{\nu_1}p_2^{\nu_2}\dots p_r^{\nu_r}\leqslant L}1\Big\} = O(L^\varepsilon).$$

The result of the lemma follows.

7. Completion of the proof. We begin by obtaining from the results of Sections 4 and 6 an upper bound, in the relevant cases $\alpha=0,1$, for the sum $\Sigma_5(L,z,\alpha)$ defined in (3.8). Let

$$G(l) = l^{2-2\alpha/3}z^{-2/3}\lambda^{4/3}, \tag{7.1}$$

where λ is the parameter of (2.13). Then by (4.2) and (4.4) we have

$$\begin{aligned}\Sigma_5(L,z,\alpha) &= O\Big(z^{8/3}\sum_{1\leqslant l\leqslant L}\ \sum_{0<g^2+h^2\leqslant G(l)}l^{-2+2\alpha/3}|S(g,h;l)|\Big)+\\ &\quad+O\Big(\lambda^2z^{5/3}\sum_{1\leqslant l\leqslant L}\ \sum_{g^2+h^2>G(l)}l^{1-\alpha/3}(g^2+h^2)^{-3/2}|S(g,h;l)|\Big),\\ &= O\{z^{8/3}\Sigma_6(\alpha)\}+O\{\lambda^2z^{5/3}\Sigma_7(\alpha)\},\end{aligned} \tag{7.2}$$

say. Here the summation over g,h in $\Sigma_7(\alpha)$ should be interpreted in the first place in accordance with the conventions of the introduction. However, the definition (3.6) of $S(g,h;l)$ gives the trivial estimate

$$|S(g,h;l)|\leqslant l^2,$$

and so the double series in (7.2) converges absolutely, and can accordingly be rearranged in any manner.

For $\Sigma_6(\alpha)$ we have

$$\Sigma_6(\alpha) = O\Big(\sum_{1\leqslant l\leqslant L} a_l l^{-2+2\alpha/3}\Big),$$

where

$$\sum_{1\leqslant l\leqslant L} a_l = \sum_{1\leqslant l\leqslant L} \sum_{0<g^2+h^2\leqslant G(L)} |S(g,h;l)| = Q\big(G(L),L\big) = O\big(\{LG(L)\}^{1+\varepsilon}\big),$$

by Lemma 10. Hence, by partial summation,

$$\Sigma_6(\alpha) = O\Big\{\sum_{1\leqslant l\leqslant L} l^{-2+\varepsilon+2\alpha/3} G^{1+\varepsilon}(l)\Big\} = O\big(Lz^{-2/3}\lambda^{4/3}\big)^{1+\varepsilon} = O\big(L^{1+\varepsilon}z^{-2/3}\lambda^{4/3+\varepsilon}\big), \tag{7.3}$$

by (7.1).

Next, define

$$b_l = \sum_{g^2+h^2>G(l)} |S(g,h;l)|(g^2+h^2)^{-3/2}. \tag{7.4}$$

The condition $g^2+h^2 > G(l)$ of summation can, from (7.1), be re-expressed as

$$l \leqslant \{z^{2/3}\lambda^{-4/3}(g^2+h^2)^{1/(2-2\alpha/3)}\} = G^{-1}(g^2+h^2),$$

$G^{-1}(h)$ being the function inverse to $G(l)$. Hence, by the absolute convergence of the series involved, we have

$$\sum_{1\leqslant l\leqslant L} b_l = \sum_{g^2+h^2>0} (g^2+h^2)^{-3/2} \sum_{\substack{1\leqslant l\leqslant L\\ l\leqslant G^{-1}(g^2+h^2)}} |S(g,h;l)| = \sum_{s=1}^{\infty} c_s s^{-3/2},$$

where

$$\sum_{1\leqslant s\leqslant S} c_s = O\Big(\sum_{0<g^2+h^2\leqslant S} \sum_{\substack{1\leqslant l\leqslant L\\ l\leqslant G^{-1}(s)}} |S(g,h;l)|\Big) = O\big(S^{1+\varepsilon}\min\{L, G^{-1}(S)\}^{1+\varepsilon}\big),$$

by Lemma 10. A partial summation now gives

$$\begin{aligned}\sum_{1\leqslant l\leqslant L} b_l &= O\Big(\sum_{s\leqslant G(L)} s^{-3/2+\varepsilon}\{G^{-1}(s)\}^{1+\varepsilon}\Big) + O\Big(\sum_{s>G(L)} L^{1+\varepsilon}s^{-3/2+\varepsilon}\Big)\\ &= O\big(L^{1+\varepsilon}\{G(L)\}^{-1/2+\varepsilon}\big) = O\big(L^{\alpha/3+\varepsilon}z^{1/3+\varepsilon}\lambda^{-2/3}\big).\end{aligned}$$

Hence, from (7.2) and (7.4),

$$\Sigma_7(\alpha) = \sum_{1\leqslant l\leqslant L} b_l l^{1-\alpha/3} \leqslant L^{1-\alpha/3}\sum_{1\leqslant l\leqslant L} b_l = O\big(L^{1+\varepsilon}z^{1/3+\varepsilon}\lambda^{-2/3}\big),$$

since $0\leqslant\alpha\leqslant 1$. This, with (7.2) and (7.3), gives

$$\Sigma_5(L,z,\alpha) = O\big(L^{1+\varepsilon}z^{2+\varepsilon}\lambda^{4/3+\varepsilon}\big). \tag{7.5}$$

We do not examine the asymptotic behaviour of $\Sigma_4(L,z,\alpha)$ as such, but first recover the behaviour of $A(L,z,\alpha)$ in terms of it. The differencing argument involved is based on the following well-known result, the proof of which is straightforward.

LEMMA 11. *For any increasing function $\Phi(z)$ denote by $\Delta^{(2)}_{z;h}\Phi(z)$ the second difference*

$$\Phi(z+2h) - 2\Phi(z+h) + \Phi(z).$$

Then, when $h>0$,

$$\Delta^{(2)}_{z;h}\Phi_{(2)}(z-2h) \leqslant h^2\Phi(z) \leqslant \Delta^{(2)}_{z;h}\Phi_{(2)}(z),$$

$\Phi_{(2)}(z)$ being the second z-integral of $\Phi(z)$ defined in (3.31).

Suppose henceforth that $0<h<z$, and first take $\Phi(z) = J(zl^{\alpha})$, as defined by (3.33), so that $\Phi_{(2)}(z) = l^{-2\alpha}J_{(2)}(zl^{\alpha})$. This gives, for some $0<\theta<1$,

$$\Delta^{(2)}_{z;h}\{J_{(2)}(zl^{\alpha})\} = h^2 l^{2\alpha} J\{(z+2\theta h)l^{\alpha}\} = c_3 h^2 l^{8\alpha/3} z^{2/3}\{1+O(h/z)+O(\lambda^{-1/3})\},$$

by the formula (4.11) for $J(z)$. Thus, from (3.8) and (7.5),

$$\begin{aligned}&\Delta^{(2)}_{z;h}\{\Lambda_{(2)}(L,z,\alpha)\}\\ &\qquad = c_3 h^2 z^{2/3}\sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l^{2-2\alpha/3}}\{1+O(h/z)+O(\lambda^{-1/3})\} + O\big(L^{1+\varepsilon}\lambda^{4/3+\varepsilon}z^{2+\varepsilon}\big).\end{aligned}$$

A second application of Lemma 11 gives

$$A(L,z,\alpha) = c_3 z^{2/3}\Big(\sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l^{2-2\alpha/3}}\Big)\{1+O(h/z)+O(\lambda^{-1/3})\} + O\big(L^{1+\varepsilon}\lambda^{4/3+\varepsilon}z^{2+\varepsilon}/h^2\big).$$

We wish to apply this result in the cases $L = Z^{1/2}$, $z = Z$, $\alpha = 0$ and $L = Z^{1/2}$, $z = Z^{1/2}$, $\alpha = 1$ occurring in (3.22). In either case the results (5.7) show firstly that the natural choice of h, viz.

$$h = L^{1/3}\lambda^{4/9}z^{7/9}\Big(\sum_{1\leqslant l\leqslant L}\frac{\tau(l)}{l^{2-2\alpha/3}}\Big)^{-1/3},$$

does in fact satisfy $0<h<z$, for large enough Z, provided that

$$\lambda < Z^{1/8-\delta} \tag{7.6}$$

for some $\delta>0$. Furthermore we find, with this h,

$$A(Z^{1/2},Z,0) = c_3 Z^{2/3}(\tfrac{1}{2}c_4\log Z + c_5) + O\{E(Z,\lambda)\},$$

$$A(Z^{1/2},Z^{1/2},1) = c_3 c_4 Z^{2/3} + O\{E(Z,\lambda)\},$$

where

$$E(Z,\lambda) = Z^{7/12+\varepsilon} + \lambda^{-1/3}Z^{2/3}\log Z + Z^{11/18+\varepsilon}\lambda^{4/9+\varepsilon},$$

so that on specifying $\lambda = Z^{1/14}$, which satisfies the requirements of (2.13) and (7.6), we obtain

$$E(Z,\lambda) = O\big(Z^{9/14+\varepsilon}\big).$$

With (3.14) and (3.22) this yields the case $D<0$ of our principal result.

THEOREM. *Let $f(x,y)$ be a binary cubic form, irreducible over the integers. Then there exist constants C_1, C_2, depending on f, such that, as $Z\to\infty$,*

$$\Sigma_1 = \sum_{|f(r,s)|\leqslant Z} d(|f(r,s)|) = C_1 Z^{2/3}\log Z + C_2 Z^{2/3} + O(Z^{9/14+\varepsilon}),$$

for any fixed $\varepsilon>0$.

From (4.12), it appears that C_1 and C_2 are in fact given by

$$C_1 = \frac{\sqrt{3}}{|D|^{1/6}}\cdot\frac{\Gamma^2(\frac{1}{3})}{\Gamma(\frac{2}{3})}c_4, \qquad C_2 = \frac{\sqrt{3}}{|D|^{1/6}}\cdot\frac{\Gamma^2(\frac{1}{3})}{\Gamma(\frac{2}{3})}(2c_5-c_4),$$

where c_4 and c_5 are as defined in (5.7), or as given by the alternative expressions (5.8). Since $c_4\neq 0$, we have $C_1\neq 0$, so the sum Σ_1' is in fact asymptotic to $C_1 Z\log Z$.

The proof for the case $D>0$ is similar in principle, the principal differences relating to the definition of the appropriate function m. Furthermore the above expressions for C_1 and C_2 should be multiplied by a factor $\sqrt{3}$, as should the expression for c_3 in (4.12). We suppress all other details.

References

[1] R. Dedekind, Ges. Math. Werke, 1 Bd., pp. 202–232.

[2] P. Erdös, *On the sum $\sum d\{f(k)\}$*, J. London Math. Soc. 27 (1952), pp. 7–15.

[3] C. Hooley, *On the number of divisors of quadratic polynomials*, Acta Math. 110 (1963), pp. 97–114.

[4] — *On binary cubic forms*, J. Reine Angew. Math. 226 (1967), pp. 30–87.

[5] E. Landau, *Vorlesungen über Zahlentheorie*, 2, Hirzel 1927.

[6] — *Einfuhrung in die Theorie der Algebraische Zahlen*, Teubner 1928.

[7] T. Nagell, *Introduction to Number Theory*, New York 1951.

[8] H. Weyl, *Algebraic Theory of Numbers*, Princeton 1940.

[9] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) 21 (1922), pp. 235–255.

UNIVERSITY OF READING
Reading, Great Britain

Received on 3. 8. 1968

ACTA ARITHMETICA
XVII (1970)

Structure of maximal sum-free sets in C_p

by

H. P. YAP (Singapore)

1. Introduction and definitions. Let G be an additive group with non-empty subsets S and T. Let $S\pm T=\{s\pm t;\ s\in S, t\in T\}$ respectively, $\overline{S}$ be the set complement of S in G and $|S|$ be the cardinal of S. We abbreviate $\{f\}$, where $f\in G$, to f. If $S+S$ and S have no element in common, then we say that S is a sum-free set in G or that S is sum-free in G. If S is a sum-free set in G and if for every sum-free set T in G, $|S|\geqslant|T|$, then S is said to be a maximal sum-free set in G. We denote by $\lambda(G)$ the cardinal of a maximal sum-free set in G. We say that S is in arithmetic progression with the difference d if $S=\{s, s+d, \ldots, s+nd\}$ for some $s, d\in G$ and some integer $n\geqslant 0$.

Let C_p be the additive group of residues mod the prime p. In [5], we proved that $\lambda(C_p)=k+1$ if $p=3k+2$ and $\lambda(C_p)=k$ if $p=3k+1$. (We note that most of the results in [5] were generalized and improved by Diananda and Yap, see [1].) In [4], we proved that (i) if S is a maximal sum-free set in C_p, $p=3k+2$, then $-S\equiv\{-s;\ s\in S\}=S$; (ii) there are altogether $(p-1)/2$ distinct maximal sum-free sets S_j, $j=1,2,\ldots,(p-1)/2$, in C_p, given by

$$S_j=\{js;\ s\in S_0\}, \qquad j=1,2,\ldots,(p-1)/2,$$

where $S_0=\{1+3i;\ i=0,1,\ldots,k\}$; and (iii) any two maximal sum-free sets in C_p are isomorphic.

In this note, we shall study the structural properties of maximal sum-free sets in C_p, $p=3k+1$.

2. Main theorems. We shall make use of the following lemmas and theorems.

LEMMA 1. *Let $A=\{a+id;\ i=0,1,\ldots,r\}$ be a set of residues modulo m with $(d,m)=1$ and $1\leqslant r\leqslant m-3$. If $A=\{b+id';\ i=0,1,\ldots,r\}$, then $d'\equiv\pm d \pmod m$* ([3]).

LEMMA 2. *Let $A=\{a+id;\ i=1,2,\ldots,r\}$ be a set of residues modulo m with $(d,m)=1$ and $2\leqslant r\leqslant(m+1)/2$. Then A can be written in only*