[6] G. Jacob, Thèse Sci. Maths., Univ. Paris 7 (1975).
[7] — *Un théorème de factorization des produits d'endomorphismes de $K^n$*, J. Algèbra 63 (1980), p. 389–412.
[8] K. Lamèche, *Quelques propriétés des séries rationnelles en variables non commutatives*, J. Combinatorial Theory (A) 14 (1973), p. 128–135.
[9] K. Mahler, *On the Taylor coefficients of rational functions*, Proc. Cambridge Phil. Soc. 52 (1956), p. 39–48.
[10] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen*, J. Reine Angew. Math. 151 (1928), p. 687–706.
[11] G. Pólya et G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, 2. Band 8. Abschnitt, Springer Verlag, Berlin–Heidelberg–New York 1971.
[12] G. Rauzy, *Ensembles arithmétiquement denses*, C. R. Acad. Sci. Paris Sér. A 265 (1967), p. 37–38.
[13] C. Reutenauer, *Une caractérisation de la finitude de l'ensemble des coefficients d'une série rationnelle en variables non commutatives*, ibid. 284 (1977), p. 1159–1162.
[14] — *Une topologie sur le monoïde libre*, Semigroup Forum 18 (1979), p. 33–49.
[15] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), p. 107–116.
[16] M. P. Schützenberger, *On the definition of a family of automata*, Information and Control 4 (1961), p. 245–270.

*Reçu le 11.5.1978* (1070)

ACTA ARITHMETICA
XXXIX (1981)

# A problem of Erdös on sums of two squarefull numbers

by

R. W. K. Odoni (Exeter)

**0. Introduction.** In a recent list [6] of solved and unsolved problems, P. Erdös notes that many interesting questions arise when one attempts to imitate the proofs of results on quadratic forms (and in particular sums of squares) when considering their apparent analogues for *squarefull numbers*, that is, positive integers $n$ such that, when $p$ is prime and $p|n$, then $p^2|n$. (Erdös calls these *powerful numbers*.)

Our concern in this paper is to answer, in the negative, Erdös's question as to whether the number of natural numbers $\leqslant x$ which are sums of two squarefull numbers $\sim Cx(\log x)^{-1/2}$ (which is the expected quantity, by analogy with Landau's well known result [10] for sums of two squares). We shall achieve this by proving

Theorem 1. *Let $\mathscr{U}$ denote the set of sums of two squarefull numbers. Then there exist positive constants $\alpha$, $\beta$ and $\gamma$ such that*

$$\text{(I)} \qquad \operatorname{card}\mathscr{U}\cap[1,x] > \alpha x(\log x)^{-1/2}\exp(\beta\log\log x/\log\log\log x)$$

*for all $x > \gamma$.*

We remark that Theorem 1 is not necessarily so surprising as it seems at first glance, since A. O. L. Atkin [1] has shown how a slight "perturbation" of the sequence, $S$, of natural squares can yield a sequence $S'$ for which $S' \dotplus S'$ has positive natural density. There is no relation between Atkin's arguments and our own, however.

The proof of Theorem 1 is rather complicated, and therefore requires some preliminary discussion. We view Erdös's problem as one on the representation of natural numbers by at least one of a large set of positive definite binary integral quadratic forms. We note that $\mathscr{U}$ is identical with the set of all integers represented by at least one of the quadratic forms

$$F_{mn} = F_{mn}(x,y) = m^3x^2 + n^3y^2 \quad \text{for} \quad m, n \geqslant 1,\ m \leqslant n \text{ and } (m,n) = 1.$$

Since we only require an $\Omega$-result for $\mathscr{U}$, it will suffice to replace $\mathscr{U}$ in Theorem 1 by any subset $\mathscr{U}_1$ of $\mathscr{U}$. We take advantage of this in order to

simplify the problem. As a first simplification, we take $\mathscr{U}_1$ to be the set of squarefree members of $\mathscr{U}$. This helps to lighten the analysis, since $F_{mn}$ can only represent a squarefree number *properly*, this is, with $(x, y) = 1$, and such representations are straightforward to handle. One would naively expect $\operatorname{card}\mathscr{U}_1 \cap [1, x]$ to be $> c\operatorname{card}\mathscr{U} \cap [1, x]$ for some absolute $c > 0$, so that little is being wasted in Theorem 1.

A second simplification is to replace $\mathscr{U}_1$ by its subset $\mathscr{U}_2$, consisting of those integers prime to $2pq$ which are represented by any of the forms $F_{pq}$, where $p_0 < p < q$ are odd primes. This simplification is *a priori* likely to cause more damage than the first simplification, but it has the major advantage that the genus structure for forms of discriminant $-4p^3q^3$ is much simpler than in the general case of discriminant $-4m^3n^3$.

Our third simplification is to truncate the size of $p$ and $q$ in the $F_{pq}$ under consideration; for the moment let us take $p_0 < p < q \leqslant y$, where $y = y(x)$ is to be chosen later. The corresponding subset of $\mathscr{U}_2$ will be denoted by $\mathscr{U}'$, and it will be $\operatorname{card}\mathscr{U}' \cap [1, x]$ that we shall bound from below. Let $\mathscr{F}_{pq}$ denote the set of members $u'$ of $\mathscr{U}'$ represented by $F_{pq}$, where $(u', 2pq) = 1$ and $p_0 < p < q \leqslant y$. Then

$$\mathscr{U}' = \bigcup_{p_0<p<q\leqslant y} \mathscr{F}_{pq}. \tag{0.1}$$

We now appeal to a simple combinatorial result; if $(X_j)_{j\in J}$ is any finite collection of finite sets, then

$$\operatorname{card}\bigcup_{j\in J} X_j \geqslant \sum_{j\in J}\operatorname{card} X_j - \tfrac{1}{2}\sum_{i\neq j}\sum\operatorname{card}(X_i \cap X_j). \tag{0.2}$$

In this we take $X_j = \mathscr{F}_{pq} \cap [1, x]$, where $j$ is the ordered pair $(p, q)$, so that $\mathscr{U}' \cap [1, x] = \bigcup_{j\in J} X_j$. We thus need:

(i) a lower bound for $\operatorname{card}\mathscr{F}_{pq} \cap [1, x]$, uniform for $p_0 < p < q \leqslant y = y(x)$;

(ii) an upper bound for $\operatorname{card}\{\mathscr{F}_{pq} \cap \mathscr{F}_{p'q'} \cap [1, x]\}$, valid for the same range of $p, p'$ and $q, q'$;

(iii) an optimal choice of $y(x)$ to exploit (0.2).

Of these, (i) is by far the most difficult part to accomplish; it will occupy us in §§ 1–12, culminating in

THEOREM 2. *Provided $D = 4p^3q^3$ satisfies $q > p > p_0$ and $(\log D)^{c_{53}\log\log D} \leqslant \log x$, where $x > x_0$, then*

$$\operatorname{card}\mathscr{F}_{pq} \cap [1, x] > c_{57}x(\log x)^{-1/2}, \tag{II}$$

*where the $c_n$ are positive absolute constants.*

In § 13 we shall solve (ii) by proving



THEOREM 3. *For sufficiently large $x$, if*

$$(\log\Delta)^{c_{61}\log\Delta} \leqslant \log x, \quad \text{where} \quad \Delta = 16p^3q^3p'^3q'^3, \text{ with } p, q, p', q' > p_0,$$

*we have*

$$\operatorname{card}\{\mathscr{F}_{pq} \cap \mathscr{F}_{p'q'} \cap [1, x]\} \leqslant c_{59}(\log\Delta)^{c_{60}}x(\log x)^{-3/4}. \tag{III}$$

Finally, in § 14, we shall deduce Theorem 1 from Theorems 2 and 3.

**1. Classical results on binary quadratic forms.** We assemble here for future use some classical definitions and theorems on representations by binary forms with integral coefficients.

DEFINITION 1.1. Two integral binary quadratic forms $F_1(X, Y)$ and $F_2(X, Y)$ are *equivalent* if there exists an invertible $\mathbf{Z}$-linear transformation

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix},$$

of determinant $+1$, such that $F_2(X, Y)$ goes over to $F_1(X, Y)$ under this transformation.

DEFINITION 1.2. The form $ax^2 + bxy + cy^2$ is *primitive* if the highest common factor $(a, b, c)$ is 1. If we define the *discriminant* $d$ of $ax^2 + bxy + cy^2$ to be $b^2 - 4ac$, it is readily seen that equivalence preserves discriminants and primitivity. The number, $h(d)$, of equivalence classes of primitive binary forms of discriminant $d$ is well known to be finite. (See [5], pp. 140–141.)

In the sequel we shall only consider the case $d = -4p^3q^3$ with $p_0 < p < q \leqslant y$, where $p$ and $q$ are prime. We have the basic

LEMMA 1.1. *The positive integer $n$ (prime to $2pq$) is properly represented by some primitive form of discriminant $-4p^3q^3$ if and only if $(-pq)$ is a square* (mod $n$). (See [5], pp. 135–136.)

We shall also be involved with a weaker concept of equivalence of forms, namely that of *rational equivalence*, whereby two primitive forms $F_1(x, y)$ and $F_2(x, y)$ are rationally equivalent if there exists a rational matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

of determinant $+1$, such that $F_2(X, Y)$ goes over to $F_1(X, Y)$ under

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto A\begin{pmatrix} X \\ Y \end{pmatrix}.$$

The equivalence classes here are called *genera*. All primitive forms of a given discriminant $d$ which represent a given integer $n$ (prime to $2d$)

must lie in the same genus, and those integers $n$ (prime to $2d$) represented by some form in a given genus can be determined by calculating a finite number of Legendre symbols involving $n$ and the prime divisors of $2d$.

Our immediate aim is that of distinguishing arithmetically the set of all integers prime to $2pq$ which are represented by $F(x, y) = p^3x^2 + q^3y^2$, and we shall do this by dealing with the general problem of which $n$ are represented by a given primitive form $f$ of some discriminant $d$. The neatest solution of the latter is provided by using the correspondence procedure between classes of primitive forms and regular ideal classes in orders of quadratic fields, which goes back to Dedekind and Weber ([15], pp. 331–375). For our purposes it is enough to say the following:

(1) An *order* $\mathcal{O}$, in an algebraic number field $K$, is a free $\mathbf{Z}$-module of rank $[K: \mathbf{Q}]$, which is contained in $\mathbf{Z}_K$, the ring of integers of $K$, as a noetherian subring with 1, in which every prime ideal $\neq 0$ is maximal. An order, $\mathcal{O}$, is necessarily of the form $\mathbf{Z} + \mathfrak{a}$, where $\mathfrak{a}$ is some ideal in $\mathbf{Z}_K$. The highest common factor, $\mathfrak{f}$, (in $\mathbf{Z}_K$) of these ideals $\mathfrak{a}$ is called the *conductor* of $\mathcal{O}$, and is largest ideal of $\mathbf{Z}_K$ contained in $\mathcal{O}$. An ideal $\mathfrak{a}$ of $\mathcal{O}$ for which $\mathfrak{a} + \mathfrak{f} = \mathcal{O}$ is said to be *regular*. Regular ideals of $\mathcal{O}$ have unique factorization into products of powers of regular prime (maximal) ideals. Two regular ideals $\mathfrak{a}$ and $\mathfrak{b}$ are (strictly) *equivalent* if $\mathfrak{a}(\lambda) = \mathfrak{b}(\mu)$, where $(\lambda)$ and $(\mu)$ are principal regular ideals, and $N_{K/\mathbf{Q}}(\lambda\mu) > 0$. Multiplication of ideals induces a finite abelian group structure on the set of regular ideal classes of $\mathcal{O}$.

(2) By considering the operations of extending ideals from $\mathcal{O}$ to $\mathbf{Z}_K$, and contracting ideals from $\mathbf{Z}_K$ to $\mathcal{O}$, it is easy to show that the regular ideal class group $\mathfrak{H}(\mathcal{O})$, of $\mathcal{O}$, is naturally isomorphic to $\mathfrak{H}^*(\mathcal{O})$, the quotient of $I^{\mathfrak{f}}$, the group of fractional ideals of $\mathbf{Z}_K$ prime to $\mathfrak{f}$, by the group of principal fractional ideals $(\alpha) = \alpha\mathbf{Z}_K$, in which $N_{K/\mathbf{Q}}(\alpha) > 0$ and $\alpha = \lambda/\mu$, where $\lambda, \mu \in \mathcal{O}$ and $\lambda\mathcal{O} + \mathfrak{f} = \mu\mathcal{O} + \mathfrak{f} = \mathcal{O}$. The isomorphism is induced by $\mathfrak{a}\ (\subseteq \mathcal{O}) \mapsto \mathfrak{a}\mathbf{Z}_K$.

(3) The correspondence between primitive binary quadratic forms and regular ideal classes of quadratic orders is given in detail in [15], and depends on the concept of an oriented (or "ordered") $\mathbf{Z}$-basis for a regular ideal in an order. We do not explicitly need the full details, but we shall merely indicate how the correspondence procedure can be used to determine which (primitive) forms represent a given integer $n$.

We use the notation $\mathscr{R}(n)$ to denote the set of regular ideal classes (in the appropriate order $\mathcal{O}$ of $\mathbf{Q}(\sqrt{d})$) corresponding to the classes of primitive forms of discriminant $d$ which represent $n$. In fact, when $d = -4p^3q^3$, we have $\mathcal{O} = \mathbf{Z} + pq\mathbf{Z}_K$. We are assuming that $(n, 2d) = 1$. In the power set of $\mathfrak{H}(\mathcal{O})$, we define the product of two subsets $A$, $B$ of $\mathfrak{H}(\mathcal{O})$ to be $AB = \{ab;\ a \in A, b \in B\}$, where $ab$ is the product in $\mathfrak{H}(\mathcal{O})$. With this



definition, we have the basic identity

$$\mathscr{R}(nn') = \mathscr{R}(n)\mathscr{R}(n') \quad \text{if} \quad (n, n') = 1. \tag{1.1}$$

Thus, to determine $\mathscr{R}(n)$, we need merely determine $\mathscr{R}(l^k)$ for all primes $l \nmid 2d$. In fact, we can also say that $\mathscr{R}(n)$ consists precisely of the set of classes of $\mathfrak{H}^*(\mathcal{O})$ occupied by ideals $\mathfrak{a} \subseteq \mathbf{Z}_K$ for which $N\mathfrak{a} = n$. (This comes from the correspondence procedure.) Since only squarefree $n$ interest us in our applications, we thus need only know the $\mathscr{R}(l)$ for primes $l \nmid 2pq$.

Now $\mathscr{R}(l)$ is empty unless $\left(\frac{-pq}{l}\right) = 1$, and this just says that $(l)$ splits as the product of two distinct prime ideals $\mathscr{L}_1, \mathscr{L}_2$ in the ring of integers of $\mathbf{Q}(\sqrt{d})$, if $d = -4p^3q^3$. Since $(l)$ is in the identity class of $\mathfrak{H}^*(\mathcal{O})$, $\mathscr{L}_1$ and $\mathscr{L}_2$ lie in inverse classes $\mathscr{C}$, $\mathscr{C}^{-1}$, and both have norm $l$. Thus

$$\mathscr{R}(l) = \{\mathscr{C}, \mathscr{C}^{-1}\}. \tag{1.2}$$

Finally in this section, we define genera of regular ideals, and note their relation to genera of forms. Two regular ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ are *in the same genus* if $N(\mathfrak{a}\mathbf{Z}_K) = N_{K/\mathbf{Q}}(\lambda)N(\mathfrak{b}\mathbf{Z}_K)$, where $\lambda\mathbf{Z}_K$ is in the identity class of $\mathfrak{H}^*(\mathcal{O})$. The set of genera of regular ideals forms a group in the obvious manner, and it is isomorphic to a quotient of $\mathfrak{H}(\mathcal{O})$ (hence is also a finite abelian group). The correspondence procedure between primitive form classes and regular ideal classes induces a 1 : 1 correspondence between genera of forms and genera of regular ideals. In all quadratic fields, the genus groups of orders are elementary abelian 2-groups (or $\mathbf{Z}_2$-vector spaces), since the square of any regular ideal is obviously in the identity genus. In the case $d = -4p^3q^3$, the genus group is either $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, and we do not need to know which of them for our applications.

**2. The integers represented by a given form.** A major difficulty confronting the discussion of the set of integers represented by a given form is that the set in question is not, in general, characterized merely by rational congruence criteria, which do suffice for the coarser description offered by genera. Although Bernays [2] and the author ([12], by a different method) obtained good results for the number of $n$, $1 \leqslant n \leqslant x$, represented by a given form $f$ for fixed $d$, and as $x \to \infty$, the methods used cannot easily be adapted to cover the case when $d$ and $x$ both $\to \infty$, and it is this case which concerns us here. We shall get round this obstacle by considering only those $n \leqslant x$ (prime to $2pq$, and squarefree) which "have enough prime divisors of the right types". To explain this phrase, we recall that $\mathscr{R}(n) = \prod_{l \mid n} \mathscr{R}(l)$, by (1.1), where the $l$ are primes. By (1.2), each $\mathscr{R}(l)$

is of the form $\{\mathscr{C}_l, \mathscr{C}_l^{-1}\} = \mathscr{C}_l^{-1}\{1, \mathscr{C}_l^2\}$. Each ideal in the class $\mathscr{C}_l^2$ belongs to $G_0$, the group of classes in the principal (i.e. identity) genus. We look for a particularly small family $(\mathscr{C}_j)_{j\in J}$ in $\mathfrak{H}^*(\mathscr{O})$ for which $\prod_{j\in J}\{1, \mathscr{C}_j^2\} = G_0$. If $n$ has at least one prime factor $l_j$ with $\mathscr{R}(l_j) = \{\mathscr{C}_j, \mathscr{C}_j^{-1}\}$, it follows that $\mathscr{R}(n) =$ an entire genus, i.e. $n$ is represented (properly) by *all* forms in a given genus. The genus in question is determined by rational congruence criteria involving only $n$ and the divisors of $2d$. Obviously we are only interested in the genus containing $F_{pq} = F = p^2x^2 + q^2y^2$.

We shall now prove a lemma showing how efficiently such a family $(\mathscr{C}_j)_{j\in J}$ can be chosen. We say that a set $(x_j)_{j\in J}$ of elements of a finite additive abelian group $A$ is a *good system of weights for* $A$ if the elements $\sum_{j\in J}\varepsilon_j x_j$, with each $\varepsilon_j$ independently 0 or 1, cover $A$. We then have

LEMMA 2.1. *If $A$ is an abelian group with $N < \infty$ elements, then there exists a good system of weights for $A$ with $\leqslant 2\log_2 N$ elements.*

(This is not necessarily best possible, but it is good enough for our needs.)

Proof. Suppose first that $A$ is cyclic, $A \cong \mathbf{Z}_N$. By considering the 2-adic (i.e. binary-digit) expansion of positive integers, it is clear that $x_j \equiv 2^j \pmod N$, $j = 1, \ldots, 1+[\log_2 N]$, is a good system of weights for $A$.

Now suppose that $A$ is a direct sum $B \oplus C$. If $(b_j)_{j\in J_1}$ is a good system of weights for $B$, and $(c_j)_{j\in J_2}$ is a good system of weights for $C$, then it is clear that $\{(b_j, o_c); j \in J_1\} \cup \{(o_B, c_j); j \in J_2\}$ will be a good system of weights for $B \oplus C = A$. From this, and our observation about finite cyclic groups, we see that if $A$ is the direct sum of cyclic groups of prime-power orders $n_1, \ldots, n_k$, then a good system of weights will exist with

$$\leqslant \sum_{i=1}^{k}(1+[\log_2 n_i]) \leqslant k + \sum_{i=1}^{k}\log_2 n_i = k + \log_2 N$$

members. Since each $n_i \geqslant 2$, we have $2^k \leqslant N$, $k \leqslant \log_2 N$, and the lemma is proved.

Now let $h$ denote the order of the groups $\mathfrak{H}(\mathscr{O}) \cong \mathfrak{H}^*(\mathscr{O})$. We know that, in the group $G_0$ of classes in the principal genus, there exists a good system of weights $(x_j)_{j\in J}$ with $\#J \leqslant 2\log_2 \#G_0$. The celebrated Gauss duplication theorem [8] tells us that (in additive notation) $G_0 = 2\mathfrak{H}^*(\mathscr{O})$, the image of $\mathfrak{H}^*(\mathscr{O})$ under the endomorphism $x \mapsto 2x$. For each $x_j$, with $j \in J$, choose a preimage $\mathscr{C}_j$. Then $(\mathscr{C}_j)_{j\in J}$ will be our "particularly small family" giving $\prod_{j\in J}\{1, \mathscr{C}_j^2\} = G_0$; it contains $\leqslant 2\log_2(h/4)$ elements.

**3. Some associated Dirichlet series.** We consider positive integers $n$, prime to $2pq$, squarefree, and properly represented by the whole genus containing $F$, via the mechanism explained in § 2. Denote the set of these $n$ by $\mathscr{M}$. For $\sigma = \mathrm{Re}\, s > 1$, the Dirichlet series

$$\sum_{m\in\mathscr{M}} m^{-s} = M(s) \tag{3.1}$$

will converge absolutely, and will be a regular function of $s = \sigma + it$. We shall express $M(s)$ in terms of $L$- and $\zeta$-functions; an application of Perron's summation formula to (3.1) will then yield upper and lower bounds for $\#\{m \in \mathscr{M}; m \leqslant x\}$, which is the quantity of interest to us.

For each $\mathscr{C} \in \mathfrak{H}^*(\mathscr{O})$, define the Euler product

$$f(s, \mathscr{C}) = \prod_l{}^{*}(1 + l^{-s}) \quad (\sigma > 1), \tag{3.2}$$

where $l$ runs through all primes $\nmid 2pq$ for which $\mathscr{C} \in \mathscr{R}(l)$.

For all positive integers $n$ prime to $2pq$, all ideals of $\mathbf{Z}_K$ ($K = \mathbf{Q}(\sqrt{\bar{d}})$) with norm $n$ are in the same genus, and we call this the genus of $n$, by abuse of language. Since the genus group is a finite elementary abelian 2-group, its characters can only take the values $\pm 1$. By abuse of notation, if $\gamma$ is such a character, we write $\gamma(\eta)$ for the common value of all $\gamma(\mathfrak{a})$ with $N\mathfrak{a} = n$. We also write

$$f(s, \mathscr{C}, \gamma) = \prod_l{}^{*}\left(1 + l^{-s}\gamma(l)\right) \quad (\sigma > 1), \tag{3.3}$$

with the same convention as in (3.2).

Consider now, for arbitrary genus characters $\gamma$,

$$\varphi(s, \gamma) = \prod_{j\in J}\{1 - f^{-1}(s, \mathscr{C}_j, \gamma)\}\prod_{\mathscr{C}}{}^{\#} f(s, \mathscr{C}, \gamma) \quad (\sigma > 1), \tag{3.4}$$

where $(\mathscr{C}_j)_{j\in J}$ is the family introduced at the end of § 2, and, in $\prod^{\#}$, $\mathscr{C}$ runs through a set of representatives of all subsets of $\mathfrak{H}^*(\mathscr{O})$ of the type $\{x, x^{-1}\}$.

On multiplying out the Euler products in (3.4), the right-hand side is seen to be a Dirichlet series of the form $\sum^{*}\gamma(n)n^{-s}$, taken over a certain set of positive squarefree integers, prime to $2pq$, with $(-pq/n) = 1$, and each such $n$ is properly represented by a *full* genus of forms; the intersection of this set with the set of integers of the same genus as $F$ is precisely $\mathscr{M}$. If $g$ ($= 4$ or $8$) is the number of genera, it follows by orthogonality of group characters that

$$M(s) = g^{-1}\sum_{\gamma}\bar{\gamma}(F)\varphi(s, \gamma) \quad (\sigma > 1), \tag{3.5}$$

where $\sum_{\gamma}$ is taken over all $g$ genus characters $\gamma$.

Our immediate task is to express the $\varphi(s, \gamma)$ (and hence $M(s)$) in terms of $L$- and $\zeta$-functions, whose analytic properties are better known.

The Dirichlet $L$-function associated with a character $\chi$ of $\mathfrak{H}^*(\mathcal{O})$ is, by definition,

$$L(s,\chi) = \prod_{\mathfrak{p}\in I^{\mathfrak{f}}} \big(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}\big)^{-1} \quad (\sigma>1), \tag{3.6}$$

the product being taken over all prime ideals in $I^{\mathfrak{f}}$. Assume now that $\gamma$ is a genus character; it may be regarded as a character of $\mathfrak{H}^*(\mathcal{O})$, and we have

$$L(s,\gamma) = \prod_{\substack{l\nmid 2pq\\ l\text{ unsplit}}} (1-l^{-2s})^{-1} \prod_{\substack{l\nmid 2pq\\ l\text{ split}}} \big(1-\gamma(l)l^{-s}\big)^{-2} \quad (\sigma>1). \tag{3.7}$$

It is clear, on the other hand, that

$$\prod_{\mathscr{C}}{}^{\#} f^2(s,\mathscr{C},\gamma) = \prod_{\substack{l\nmid 2pq\\ l\text{ split}}} \big(1+\gamma(l)l^{-s}\big)^2 \quad (\sigma>1). \tag{3.8}$$

Hence

$$L^{-1}(s,\gamma)\prod_{\mathscr{C}}{}^{\#} f^2(s,\mathscr{C},\gamma) = \prod_{\substack{l\nmid 2pq\\ l\text{ unsplit}}} (1-l^{-2s}) \prod_{\substack{l\nmid 2pq\\ l\text{ split}}} (1-l^{-2s})^2 \quad (\sigma>1), \tag{3.9}$$

since $\gamma^2$ is $\chi_0$, the identity character. Consequently, as the right-hand side of (3.9), and its reciprocal are regular and absolutely bounded for, say, $\sigma\geqslant 3/4$, we can write

$$\prod_{\mathscr{C}}{}^{\#} f(s,\mathscr{C},\gamma) = \sqrt{L(s,\gamma)}\cdot G(s,\gamma), \tag{3.10}$$

where $G(s,\gamma)^{\pm 1}$ is regular and uniformly bounded for $\sigma\geqslant 3/4$, and (3.10) holds to the right of any zeros of $L(s,\gamma)$.

To complete the analysis of singularities of $\varphi(s,\gamma)$, it remains to deal with the factors $1-f^{-1}(s,\mathscr{C}_j,\gamma)$ for $j\in J$. Using (3.6), we have, for all characters $\chi$ of $\mathfrak{H}^*(\mathcal{O})$,

$$\log L(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{f}} \log\big(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}\big)^{-1} \quad (\sigma>1). \tag{3.11}$$

If $N\mathfrak{p}=l^2$, $\mathfrak{p}=(l)$ is in the principal class, and so $1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}=1-l^{-2s}$. We thus have, for non-principal $\mathscr{C}$,

$$\begin{aligned} h^{-1}\sum_{\chi}\overline{\chi}(\mathscr{C})\log L(s,\chi) &= h^{-1}\sum_{\substack{l\text{ split}\\ l\nmid 2pq}}\sum_{\mathfrak{p}\mid l}\sum_{\chi}\overline{\chi}(\mathscr{C})\log\big(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}\big)^{-1}\\ &= h^{-1}\sum_{\chi}\overline{\chi}(\mathscr{C})\sum_{\substack{\mathfrak{p}\mid l\\ l\text{ split}}}\sum_{n=1}^{\infty} n^{-1}l^{-ns}\chi(\mathfrak{p}^n)\\ &= \sum_{l\text{ split}}\sum_{\mathfrak{p}\mid l}\sum_{\substack{n=1\\ \mathfrak{p}^n\in\mathscr{C}}}^{\infty} n^{-1}l^{-ns}\\ &= s(\mathscr{C})\sum_{\mathscr{C}\in\mathscr{R}(l)} l^{-s} + R(s,\chi) \quad (\sigma>1), \end{aligned} \tag{3.12}$$



where $s(\mathscr{C})=2$ if $\mathscr{C}=\mathscr{C}^{-1}$, and $=1$ if not, while $R(s,\mathscr{C})$ is regular and absolutely bounded for $\sigma\geqslant 3/4$. We also remark for future reference that if $\mathscr{C}$ is principal we obtain a similar result to (3.12), involving an extra term which can be absorbed into $R(\cdot,\mathscr{C})$. It is important to note that, for $\sigma\geqslant 3/4$,

$$\sum_{\mathscr{C}\in A} |R(s,\mathscr{C})| \text{ is absolutely bounded} \tag{3.13}$$

for any subset $A$ of $\mathfrak{H}^*(\mathcal{O})$, since, for $\mathscr{C}\neq\mathscr{C}_0$,

$$\begin{aligned} |R(s,\mathscr{C})| &= \Big|\sum_{\substack{l\text{ split}\\ l\nmid 2pq}}\sum_{\mathfrak{p}\mid l}\sum_{\substack{n\geqslant 2\\ \mathfrak{p}^n\in\mathscr{C}}} l^{-ns}n^{-1}\Big|\\ &\leqslant \sum_{l}\sum_{\mathfrak{p}\mid l}\sum_{\substack{n\geqslant 2\\ \mathfrak{p}^n\in\mathscr{C}}} l^{-n\sigma}n^{-1} \leqslant \sum_{l}\sum_{\mathfrak{p}}\sum_{\substack{n\geqslant 2\\ \mathfrak{p}^n\in\mathscr{C}}} l^{-3n/4}n^{-1}\\ &\leqslant K_1\sum_{l}\sum_{\substack{\mathfrak{p}\in\mathscr{C}\\ \mathfrak{p}\mid l}} l^{-3/2}, \end{aligned}$$

whence

$$\sum_{\mathscr{C}\in A}|R(s,\mathscr{C})| \leqslant K_1\sum_{l} l^{-3/2} < K,$$

where $K$ is absolute, and this gives (3.13).

Combining (3.12) and (3.3), we obtain

$$f(s,\mathscr{C},\gamma) = T(s,\mathscr{C};\gamma)\prod_{\chi} L(s,\chi)^{\alpha(\mathscr{C},\gamma;\chi)}, \tag{3.14}$$

in which the $T^{\pm 1}(s,\mathscr{C};\gamma)$ (and any products thereof) are regular and uniformly bounded for $\sigma\geqslant 3/4$, and the exponents $\alpha(\mathscr{C},\gamma;\chi)$ are given by

$$\alpha(\mathscr{C},\gamma;\chi) = \gamma(\mathscr{C})\overline{\chi}(\mathscr{C})/hs(\mathscr{C}). \tag{3.15}$$

Formula (3.14) applies at any point to the right of any poles or zeros of the $L(s,\chi)$. It is well known that the $L(s,\chi)$ extend to meromorphic functions in the complex $s$-plane, and that, for $\chi\neq\chi_0$, $L^{\pm 1}(s,\chi)$ is regular near $s=1$, while $L(s,\chi_0)$ has a simple pole at $s=1$. This shows that $f(s,\mathscr{C},\gamma)$ has a singularity of the type $(s-1)^{-\gamma(\mathscr{C})/hs(\mathscr{C})}$ at $s=1$.

**4. Behaviour and growth of $L$-functions near $s=1$.** Now let $\gamma$ be a genus character. We consider the problem of estimating the contour integral

$$I(\gamma) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{w^s}{s^2}\varphi(s,\gamma)\,ds, \tag{4.1}$$

where $w$ is large, and $c>1$. $I(\gamma)$ will occur when estimating $\mathscr{M}(w)$. More precisely, we shall need to consider what happens to $I(\gamma)$ as both $|d|$

and $x \to \infty$ in some suitably related way. In view of (3.14), we need some bounds for $|L(s,\chi)|^{\pm 1}$ on abscissae near 1, in terms of $D = |d|$, and also some information on the location of the zeros of $L(s,\chi)$. If $\chi$ is a non-real character we can use estimates of Landau [11] and Fogels [7], namely:

$$|L(\sigma,\chi)| < c_1 \log^2 D \quad \text{for} \quad 1 - \frac{c_2}{\log D} \leqslant \sigma \leqslant 1; \tag{4.2}$$

$$|L^{-1}(\sigma,\chi)| < c_3' \log^2 D (\log\log D)^{3/4} < c_3 \log^2 D \quad \text{for} \quad 1 - \frac{c_2}{\log D} \leqslant \sigma \leqslant 1; \tag{4.3}$$

$$|L^{\pm 1}(\sigma+it,\chi)| < c_4 \log^3 D (2+t^2) \tag{4.4}$$

in a region

$$\Omega\colon\ 1 - \frac{c_5}{\log D(2+t^2)} \leqslant \sigma \leqslant 1 \tag{4.5}$$

(which contains no zeros of $L$).

In the above, and in all later analysis, we use $c_n$ to denote a positive absolute constant.

When $\chi$ is a real character, then it must in fact be a genus character (using Gauss's duplication theorem). In that case, if the prime ideal $\mathfrak{p} \nmid \mathfrak{f}$, $\chi(\mathfrak{p}) = \chi_1(N\mathfrak{p}) = \chi_1(l)$ or $\chi_1(l^2)$ is a quadratic residue symbol (Kronecker symbol) of $l$ or $l^2$, with respect to some conductor dividing $d$. We have the following results:

(4.2) *also holds for $\chi$ real, non-principal, while, when $\chi = \chi_0$, we have*:

$$|(s-1)L(s,\chi_0)| < c_0 \quad \textit{for} \quad 0 \leqslant \sigma \leqslant 1,\ t \textit{ bounded}; \tag{4.6}$$

(4.7) *$L(s,\chi)$ has all its zeros (with one possible exception) to the left of the region $\Omega$ defined in* (4.5); *the estimate* (4.4) *holds for $|t| \geqslant 2$, for all characters $\chi$, real or complex* (see Davenport [4], Ch. 14);

(4.8) *If $\chi$ is real, $\chi \neq \chi_0$, then*

$$|L(1,\chi)| > c(\varepsilon) D^{-\varepsilon} \quad \textit{for all } \varepsilon > 0$$

(see Siegel [14] or Davenport [4], pp. 130–134). A similar estimate holds for $|L(s,\chi)|$ if $|s-1| \leqslant c'(\varepsilon) D^{-\varepsilon}$.

We now require an estimate for $|L(s,\chi)|^{-1}$ for $\chi$ real and $s$ near 1. We apply the following

LEMMA (Jutila [9], Lemma 3a). *The number of zeros of $L(s,\chi)$ (with $\chi \neq \chi_0$) in the square*

$$1 - \lambda/\log D \leqslant \sigma \leqslant 1, \quad |t| \leqslant \lambda/2\log D, \tag{4.9}$$



*with $1 \leqslant \lambda \leqslant c_6 \log D$, is at most*

$$0.6029\lambda + 6.829 < \lambda + 7. \tag{4.10}$$

We shall apply this with $\lambda = c_6 \log D$, in the following way: using the Hadamard factorization of $L(s,\chi)$, we have

$$\frac{L'(2,\chi)}{L(2,\chi)} - \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\varrho} \left( \frac{1}{2-\varrho} - \frac{1}{s-\varrho} \right) + O(1), \tag{4.11}$$

(see Davenport [4], p. 85), if $s \neq$ any zero $\varrho'$ of $L(s,\chi)$, where $\varrho$ runs through all zeros, it being assumed that $|t| < c_7$. Since $L'(2,\chi)/L(2,\chi)$ is absolutely bounded, we find

$$\left| \frac{L'(s,\chi)}{L(s,\chi)} \right| \leqslant \sum_{\varrho} \left| \frac{(s-2)}{(2-\varrho)(s-\varrho)} \right| + O(1). \tag{4.12}$$

We wish to apply (4.12) in the intersection of $\Omega$ with the square (4.9). We divide the sum over $\varrho$ into two parts, the first over those in the square (4.9), and the second over all remaining $\varrho$. The latter sum is

$$< c_8 \sum_{\text{all } \varrho} |2-\varrho|^{-2} < c_9 \log D, \tag{4.13}$$

by [4], p. 91. If we ensure that $|s-\varrho| \geqslant c^*(\varepsilon) D^{\varepsilon}$ for all $\varrho$, we find that the other sum over $\varrho$ is

$$\leqslant c^{**}(\varepsilon) D^{\varepsilon} \log D < c^{\#}(\varepsilon) D^{\varepsilon} \quad (\forall \varepsilon > 0). \tag{4.14}$$

Integration over any path of length $O(1)$ yields

$$|\log L(s,\chi)| < c_{\bullet} D^{\varepsilon} \text{ on paths of length } O(1) \text{ in } \Omega \cap (4.9), \tag{4.15}$$

if $|s-\varrho| \geqslant c^*(\varepsilon) D^{-\varepsilon}$ for all zeros $\varrho$ and all $s$ on the path. In particular, we find that

$$|L(s,\chi)|^{-1} < \exp(c_{\bullet} D^{\varepsilon}) \quad (\chi \neq \chi_0), \tag{4.16}$$

there. This estimate could no doubt be improved at the cost of some extra work, but will suffice for our requirements. We note also that (4.16) holds even if $\chi = \chi_0$, since the pole at $s = 1$ can be absorbed into the sum over zeros if $|s-1| \geqslant c^*(\varepsilon) D^{-\varepsilon}$.

**5. Decomposition of $I(\gamma)$.** We now consider the problem of giving an upper bound for $I(\gamma)$ when $\gamma \neq \chi_0$. (It will turn out that $I(\chi_0)$ is of a larger order of magnitude than the other $I(\gamma)$.) We first deform the vertical contour from $c - i\infty$ to $c + i\infty$ into $\bigcup_{1 \leqslant j \leqslant 4} \mathscr{L}_j$, where $\mathscr{L}_1$ consists of the pair of antiparallel line segments $t = \pm \frac{1}{2} c'(\varepsilon) D^{-\varepsilon} x^{-1}$, $1 - \frac{1}{2} c'(\varepsilon) \leqslant \sigma \leqslant 1$, $\mathscr{L}_2$ consists of the semicircle $\sigma \geqslant 1$, $|s-1| = \frac{1}{2} c'(\varepsilon) x^{-1} D^{-\varepsilon}$, $\mathscr{L}_3$ consists of the

line joining $1-\frac{1}{2}c'(\varepsilon)D^{-\varepsilon}+\frac{1}{2}ic'(\varepsilon)x^{-1}D^{-\varepsilon}$ to $1-c_5/\log D(2+c_6^2/4)+ic_6/2$, and its mirror image in $t=0$, while $\mathscr{L}_4$ consists of the two infinite arcs $|t|\geqslant c_6/2$, $\sigma=1-c_5/\log D(2+t^2)$. The orientations are chosen to make the union $\bigcup_j \mathscr{L}_j$ homotopic to the original vertical contour. It follows from Cauchy's theorem that $I(\gamma)=\sum_{1\leqslant j\leqslant 4} I_j(\gamma)$, where

$$I_j(\gamma)=\frac{1}{2\pi i}\int_{\mathscr{L}_j}\frac{x^s}{s^2}\varphi(s,\gamma)\,ds. \tag{5.1}$$

It turns out that $I_1(\chi_0)$ dominates all other terms $I_j(\gamma)$, as we shall see later. Let us now take $\gamma\neq\chi_0$ and estimate the $I_j(\gamma)$ for $j=1,2,3,4$, in that order. For this we need bounds for $\varphi(s,\gamma)$ on the appropriate contours, and it is convenient to separate the cases into individual paragraphs.

**6. Estimation of $I_1(\gamma)$, $\gamma\neq\chi_0$.** We must first estimate $\varphi(s,\gamma)$ on $\mathscr{L}_1$, and, in view of (3.5) and (3.10), we have, for $\gamma\neq\chi_0$,

$$|\varphi(s,\gamma)|<c_{10}|L(s,\gamma)|^{1/2}\prod_{j\in J}|1-f^{-1}(s,\mathscr{C}_j,\gamma)|,$$

while (3.14) gives, in conjunction with the estimates of § 4, and on choosing a suitable $J$ with $\#J<c_{11}\log h$,

$$|\varphi(s,\gamma)|\leqslant c_{12}(\varepsilon)(c_3\log^3 D)^{c_{13}\log h}|s-1|^{-c_{14}\log h/h}\exp\left(\frac{8\varepsilon\log D\log h}{h}\right)\quad\text{on}\quad\mathscr{L}_1.$$

Since (by Siegel's theorem [14] on class-numbers of imaginary quadratic fields, and the relation between class-numbers of related orders (see [3], p. 153)) $\log h/\log D\to\frac{1}{2}$ as $D\to\infty$, we have

$$|\varphi(s,\gamma)|\leqslant c_{13}(\varepsilon)(c_3\log^3 D)^{c_{15}\log D}|s-1|^{-c_{14}\log h/h}\quad\text{on}\quad\mathscr{L}_1. \tag{6.1}$$

But

$$|I_1(\gamma)|\leqslant(2\pi)^{-1}\int_{\mathscr{L}_1}\left|\frac{x^s}{s^2}\varphi(s,\gamma)\right||ds|,$$

so we obtain

$$|I_1(\gamma)|\leqslant c_{16}(\varepsilon)(c_3\log^3 D)^{c_{15}\log D}x(\log x)^{-1+\frac{c_{14}\log h}{h}}\quad(\gamma\neq\chi_0), \tag{6.2}$$

since

$$\int_0^\infty x^{-\nu}y^{-c\log h/h}dy=\Gamma\left(1-\frac{c\log h}{h}\right)(\log x)^{\frac{c\log h}{h}-1}. \tag{6.3}$$



**7. Estimation of $I_2(\gamma)$, $\gamma\neq\chi_0$.** It is easily seen that (6.1) is also satisfied on $\mathscr{L}_2$. We put $s=1+re^{i\theta}$, $0\leqslant\theta\leqslant\pi$, where $r=\frac{1}{2}c'(\varepsilon)x^{-1}D^{-\varepsilon}$. Then

$$\begin{aligned}|I_2(\gamma)|&\leqslant c_{17}\int_0^\pi(6.1)x^\sigma|rie^{i\theta}d\theta|\\&\leqslant c_{18}x^{1+r}r^{1-c_{14}\log h/h}c_{13}(\varepsilon)(c_3\log^3 D)^{c_{15}\log D}\\&\leqslant c_{19}x^{c_{14}\log h/h}D^{c_{20}\log\log D}\quad\text{(if, say, }\varepsilon=1/10).\end{aligned} \tag{7.1}$$

**8. Estimation of $I_3(\gamma)$, $\gamma\neq\chi_0$.** Using (4.16), and noting that

$$|s-1|^{-c_{14}\log h/h}\leqslant\left(c_{21}(\varepsilon)D^\varepsilon\right)^{c_{14}\log h/h}\quad\text{on}\quad\mathscr{L}_3,$$

we find that

$$|I_3(\gamma)|\leqslant c_{22}(\varepsilon)(c_3\log^3 D)^{c_{15}\log D}\left(c_{21}(\varepsilon)D^\varepsilon\right)^{c_{14}\log h/h}\exp\frac{c_{23}(\varepsilon)D^\varepsilon}{h}\int_{\sigma_1}^{\sigma_2}x^\sigma d\sigma, \tag{8.1}$$

where $\sigma_1<\sigma_2$ are the values of $\sigma=\mathrm{Re}\,s$ at the end-points of $\mathscr{L}_3$. Since

$$\int_{\sigma_1}^{\sigma_2}x^\sigma d\sigma\leqslant x^{1-\frac{1}{2}c'(\varepsilon)D^{-\varepsilon}}(\log x)^{-1},$$

we find

$$|I_3(\gamma)|<c_{24}(\varepsilon)(c_3\log^3 D)^{c_{15}\log D}x^{1-\frac{1}{2}c'(\varepsilon)D^{-\varepsilon}}(\log x)^{-1}. \tag{8.2}$$

**9. Estimation of $I_4(\gamma)$, $\gamma\neq\chi_0$.** The estimate (4.4) readily yields the bound

$$|\varphi(s,\gamma)|\leqslant c_{25}\left(\log D(2+t^2)\right)^{c_{26}\log h}\quad\text{on}\quad\mathscr{L}_4. \tag{9.1}$$

On breaking the $t$-interval $[c_6/2,\infty)$ into the two parts, $[c_6/2,D]$ and $[D,\infty)$, and estimating the integrals separately, we obtain the estimate

$$|I_4(\gamma)|\leqslant c_{27}x^{1-c_{28}/\log D}(\log D)^{c_{29}\log D}. \tag{9.2}$$

**10. Estimates for $I_1(\chi_0)$.** As we have mentioned before, it is the $I_1(\chi_0)$-contribution which dominates any linear combination of the integrals $I(\gamma)$. We shall aim to produce good upper and lower bounds for $I_1(\chi_0)$. We note first from (3.5) and (3.10) that

$$\begin{aligned}\varphi(s,\chi_0)&=G(s,\chi_0)\sqrt{L(s,\chi_0)}\prod_{j\in J}\{1-f^{-1}(s,\mathscr{C}_j,\chi_0)\}\quad(\sigma>1),\\&=G_1(s,\chi_0)\sqrt{\zeta(s)}\prod_{j\in J}\{1-f^{-1}(s,\mathscr{C}_j,\chi_0)\},\end{aligned} \tag{10.1}$$

where $G_1$ is similar to $G$, and the domain of validity of (10.1) can be extended into suitable zero-free regions of the $L(s,\chi)$. Now, in view of (3.14), the

$f^{-1}(s, \mathscr{C}_j, \chi_0)$ have zeros at $s = 1$, of (fractional) orders $(h\varepsilon(\mathscr{C}))^{-1}$. On $\mathscr{L}_1$ we have

$$|f^{-1}(s, \mathscr{C}_j, \chi_0)| \leqslant |s-1|^{1/h\varepsilon(\mathscr{C})} c_{30} \log^3 D. \tag{10.2}$$

We divide $\mathscr{L}_1$ into two parts, $\mathscr{L}_{11}$, on which $|\sigma - 1| < \mu = c_{31}(\log D)^{-c_{32}\log D}$, and $\mathscr{L}_{12}$, the remainder. On $\mathscr{L}_{11}$, we see from (10.2) that the product

$$\prod_j |1 - f^{-1}(s, \mathscr{C}_j, \chi_0)| > c_{33}. \tag{10.3}$$

It follows readily that, with obvious notation,

$$|I_{11}| > c_{34} \int_{1-\mu}^{1} \frac{x^\sigma}{\sigma^2}(1-\sigma)^{-1/2} d\sigma > c_{35} x (\log x)^{-1/2}, \tag{10.4}$$

provided

$$\log x (\log D)^{-c_{32}\log D} > c_{36}. \tag{10.5}$$

The integral $I_{12}$ (along $\mathscr{L}_{12}$) is bounded by

$$c_{37}(\log D)^{c_{38}\log D} c_{39}(\varepsilon) D^\varepsilon \int_{1-\sigma'(\varepsilon)D^{-\varepsilon}}^{1-\mu} x^\sigma d\sigma,$$

giving a bound

$$|I_{12}| < c_{41}(\log D)^{c_{42}\log D} x^{1 - c_{31}(\log D)^{-c_{32}\log D}} (\log x)^{-1}. \tag{10.6}$$

This is $< \frac{1}{2} c_{35} x (\log x)^{-1/2}$ provided

$$(\log D)^{c_{44}\log D} \leqslant c_{45} \log x. \tag{10.7}$$

It is now clear that, for $x$, $D$ constrained by (10.5) and (10.7),

$$cx(\log x)^{-1/2} < |I_1| < Cx(\log x)^{-1/2}, \tag{10.8}$$

where $c$, $C$ are positive absolute constants.

**11. Estimates for $I_j(\chi_0)$, $j \neq 1$.** It remains now to estimate the $I_j(\chi_0)$ for $j \neq 1$, in order to complete our investigation of the $I(\gamma)$. First, to deal with $I_2(\gamma)$, we use the bound

$$|\varphi(s, \chi_0)| \leqslant c_{46}(\log D)^{c_{47}\log D} |s-1|^{-1/2}$$

for $|s-1| = r = \frac{1}{2}\sigma'(\varepsilon) D^{-\varepsilon} x^{-1}$, obtainable by simple modifications of the arguments of § 7 and § 10. This gives

$$|I_2(\chi_0)| \leqslant c_{48}(\log D)^{c_{47}\log D} x^{1+r} r^{1/2} \leqslant c_{49}(\varepsilon) x^{1/2} (\log D)^{c_{50}\log D}, \tag{11.1}$$



For $I_3(\chi_0)$, we imitate § 8, the only change being the use of the estimate

$$|s-1|^{-1/2} \leqslant c_{51}(\varepsilon) D^\varepsilon \quad \text{on} \quad \mathscr{L}_3.$$

We arrive at a bound of the same form as (8.2). In analogous manner, the argument of § 9 is easily modified to cover $I_4(\chi_0)$.

**12. The lower bound for $\mathscr{M}(x)$.** Let us recall that

$$\mathscr{M}(x) = \sum_{\substack{m \in \mathscr{M} \\ m \leqslant x}} 1, \tag{12.1}$$

with $\mathscr{M}$ defined as in § 3. Using (3.1), we have

$$\mathscr{N}(x) \overset{\text{def}}{=} \sum_{\substack{m \leqslant x \\ m \in \mathscr{M}}} \log x/m = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{x^s}{s^2} M(s)\, ds, \tag{12.2}$$

by Mellin inversion. Using (3.5),

$$\mathscr{N}(x) = g^{-1} \sum_\gamma \bar{\gamma}(F) \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{x^s}{s^2} \varphi(s, \gamma)\, ds = g^{-1} \sum_\gamma \bar{\gamma}(F) I(\gamma), \tag{12.3}$$

where $g$, the number of genera, divides 8. As a result of §§ 6–11, we find that

$$\mathscr{N}(x) > c_{52} x (\log x)^{-1/2}, \tag{12.4}$$

provided that $D$ and $x$ are chosen so as to make $I_1(\chi_0)$ the dominant term, and certainly, therefore, if we impose the condition

$$(\log D)^{c_{53}\log D} < \log x \tag{12.5}$$

for some suitably large $c_{53}$. Also, by § 10, we have

$$\mathscr{N}(x) < c_{54} x (\log x)^{-1/2}, \tag{12.6}$$

subject to (12.5). It is now clear that

$$\log c_{55}^{-1} \cdot \mathscr{M}(x) \geqslant \sum_{\substack{c_{55} x < m \leqslant x_1 \\ m \in \mathscr{M}}} \log x/m \geqslant c_{56} x (\log x)^{-1/2},$$

so that

$$\mathscr{M}(x) \geqslant c_{57} x (\log x)^{-1/2}. \tag{12.7}$$

Theorem 2 follows immediately.

**13. The proof of Theorem 3.** In the notation of the introduction, we consider $\mathscr{H} = \mathscr{F}_{pq} \cap \mathscr{F}_{p^*q^*}$, where $p_0 < p < q$, $p_0 < p^* < q^*$, and the ordered pairs $(p, q)$ and $(p^*, q^*)$ are distinct. We want a suitable upper bound for card $\mathscr{H} \cap [1, x]$. For this, we first put $d = -4p^3q^3$, $d^* = -4p^{*3}q^{*3}$.

An integer $n$, prime to $dd^*$, is properly represented by some forms of each discriminant if and only if $\left(\frac{d}{n}\right) = \left(\frac{d^*}{n}\right) = 1$, and this happens for squarefree such $n$ if and only if $\left(\frac{d}{l}\right) = \left(\frac{d^*}{l}\right) = 1$ for all primes $l|n$, $l \nmid 2pqp^*q^*$.

Let $L = KK^*$ be the compositum of the fields $K = Q(\sqrt{d})$ and $K^* = Q(\sqrt{d^*})$. If the prime $l$ does not divide the discriminant of $L$, the condition $\left(\frac{d}{l}\right) = \left(\frac{d^*}{l}\right) = 1$ is precisely the condition that $l$ split as a product of two prime ideals in both $K$ and $K^*$, or equally that $l$ split as a product of four distinct prime ideals in $L$, it being clear that $[L: Q] = 4$, since $d \neq d^*$. Let $\mathscr{H}^*$ be the set of all positive squarefree integers composed entirely of rational primes unramified in $L$, which split completely in $L$. It is clear that $\mathscr{H}^* \supseteq \mathscr{H}$, and that

$$H^*(s) \overset{\text{def}}{=} \sum_{h \in \mathscr{H}^*} h^{-s} = \prod_{l \text{ split}} (1 + l^{-s}) \qquad (\sigma > 1). \tag{13.1}$$

If $\zeta_L(s)$ is the Dedekind zeta-function of $L$, then ([13], p. 79, § 7) it is clear that, for $\sigma > 1$,

$$\prod_{l \text{ split}} (1 - l^{-s})^{-4} = G_2(s)\zeta_L(s), \tag{13.2}$$

where $G_2^{\pm 1}(s)$ is regular and absolutely bounded for $\sigma \geqslant 3/4$. It follows that

$$H^*(s) = G_3(s)\zeta_L^{1/4}(s), \tag{13.3}$$

where $G_3^{\pm 1}(s)$ is regular and absolutely bounded for $\sigma \geqslant 3/4$. It is clear that (13.3) provides an analytic continuation for $H^*(s)$ into a region to the left of $\sigma = 1$, free of zeros of $\zeta_L(s)$. This zeta-function can be expressed as the product of the Riemann zeta-function and three Dirichlet $L$-series with real characters, of conductors dividing $\Delta = dd^*$. We may use the estimates of § 4, replacing $D$ by $\Delta$, and we can then imitate the analysis of § 10 and § 12, obtaining

$$c_{58}(\varepsilon)\Delta^{-\varepsilon}x(\log x)^{-3/4} \leqslant \sum_{\substack{h \in \mathscr{H}^* \\ h \leqslant x}} 1 \leqslant c_{59}(\varepsilon)(\log \Delta)^{c_{60}}x(\log x)^{-3/4}, \tag{13.4}$$

provided

$$(\log \Delta)^{c_{61}\log\Delta} \leqslant \log x, \tag{13.5}$$

and this immediately gives Theorem 3.



**14. Conclusion of the proof of Theorem 1.** We now substitute into (0.2) the results of Theorems 2 and 3, summing over pairs $(p, q)$ of primes with $p_0 < p < q \leqslant y(x)$, and obtaining

$$\text{card } \mathscr{U} \cap [1, x] \geqslant c_{57}x(\log x)^{-1/2} \sum_{p_0 < p < q \leqslant y(x)} 1 - c_{59}x(\log x)^{-3/4} \sum_{(p,q) \neq (p^*, q^*)} (\log \Delta)^{c_{60}}, \tag{14.1}$$

provided that (12.5) and (13.5) hold. Now it is clear (from weak versions of the prime number theorem) that

$$\sum_{p_0 < p < q \leqslant y} 1 \geqslant c_{62}(y/\log y)^2, \tag{14.2}$$

and that

$$\sum_{(p,q) \neq (p^*, q^*)} (\log \Delta)^{c_{60}} \leqslant c_{63}(\log y)^{c_{64}}(y/\log y)^4 \leqslant c_{65}y^4(\log y)^{c_{66}}. \tag{14.3}$$

If we were not constrained by (12.5) and (13.5), the largest available $y = y(x)$ would yield the best lower bound in (14.1). The optimal value of $y$ would nearly be

$$y = (\log x)^{1/8}(\log\log x)^{-c_{67}},$$

and we should obtain

$$\text{card } \mathscr{U} \cap [1, x] > c_{68}x(\log x)^{-1/4}(\log\log x)^{-c_{69}}. \tag{14.4}$$

Unfortunately, (12.5) and (13.5) prevent such a choice of $y$; in fact we are forced to choose

$$(\log y)^{c_{70}\log y} \leqslant \log x. \tag{14.6}$$

The best realisable bound in Theorem 1 will occur when equality holds in (14.6), and this is equivalent to

$$y = \exp\left(c_{71}\log\log x/\log\log\log x\left(1 + O\left(\frac{\log\log\log\log x}{\log\log\log x}\right)\right)\right), \tag{14.7}$$

$$(\ll (\log x)^{\varepsilon} \text{ for any } \varepsilon > 0).$$

Substituting this into (14.1), we obtain Theorem 1.

**15. Concluding remarks.** At some further cost in complexity, one could attempt to handle forms $F_{mn} = m^3x^2 + n^3y^2$, with $m$ and $n$ having several prime divisors (up to some function of $x$). It is not clear how much improvement could be made to Theorem 1 by this method.

We remark that, in proving Theorem 1, we have made no attempt to assign numerical values to the constants $c_n$. In many cases this could be done, but it is important to remember that no *effective* lower bounds for $|L(1, \chi)|$ with $\chi$ real, $\chi \neq \chi_0$, are yet known, so that the constants $c_n(\varepsilon)$ and $c(\varepsilon)$, $c'(\varepsilon)$, $c^*(\varepsilon)$, arising at various points in our analysis, are not known functions of $\varepsilon$.

**References**

[1] A. O. L. Atkin, *On pseudo-squares*, Proc. London Math. Soc. (3) 14A (1965), pp. 22–27.

[2] P. Bernays, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven binaren quadratischen Formen einer nichtquadratischen Diskriminante*, Dissertation, Göttingen 1912.

[3] Z. I. Borevič and I. R. Šafarevič, *Number theory*, Academic Press, New York 1966.

[4] H. Davenport, *Multiplicative number theory*, Markham Publ. Comp., Chicago 1967.

[5] — *The higher arithmetic*, Hutchinson University Library, London 1968.

[6] P. Erdös, *Problems and results on consecutive integers*, Publ. Math. Debrecen 23 (1976), pp. 271–282.

[7] E. Fogels, *On the theory of abstract primes, III*, Acta Arith. 11 (1965), pp. 293–331.

[8] B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monographs No. 10, 1950, pp. 167–168.

[9] M. Jutila, *On two theorems of Linnik*, Ann. Acad. Sci. Fenn., Ser. A, I 458 (1970), pp. 7–32.

[10] E. Landau, *Handbuch der Primzahlverteilung*, Bd. 2, Teubner, Leipzig 1909, pp. 643–644.

[11] — *Zur Theorie der Heckeschen Zetafunktionen, welche komplexen Charakteren entsprechen*, Math. Z. 4 (1919), pp. 152–162.

[12] R. W. K. Odoni, *On norms of integers in a full module of an algebraic number field and the distribution of values of binary integral quadratic forms*, Mathematika 22 (1975), pp. 108–111.

[13] — *On the norms of algebraic integers*, ibid. 22 (1975), pp. 71–80.

[14] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), pp. 83–86.

[15] H. Weber, *Lehrbuch der Algebra*, vol. III, Vieweg, Braunschweig 1908.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF EXETER

*Received on 20.5.1978* (1074)

ACTA ARITHMETICA
XXXIX (1981)

# On Linnik's constant

by

S. GRAHAM (Pasadena, Calif.)

Let $q$ be a large positive integer, $(a, q) = 1$, and $p(q, a)$ the least prime $p \equiv a \pmod q$. The celebrated theorem of Linnik ([12], [13]) states that there exists an absolute constant $C$ such that $p(q, a) < q^C$ for $q$ sufficiently large. The first to obtain an explicit value for $C$ was Pan [16], who proved that $C \leqslant 5448$. This was subsequently improved to 770 ([2]), 550 ([10]), 168 ([3]), 80 ([11]), and 36 ([5]). In this paper, we show that one may take $C = 20$.

THEOREM 1. *If $q$ is sufficiently large and $(a, q) = 1$, then there is a prime $p \equiv a \pmod q$ such that $p < q^{20}$.*

Our proof depends on several results concerning zeros of $L$-functions. Let $\varrho = \beta + i\gamma$ denote a generic zero of $L(s, \chi)$, where $\chi$ is a character mod $q$. Miech [14] has shown that $\prod_{\chi \bmod q} L(s, \chi)$ has at most one zero in the region

$$1 - \frac{.05}{\log q(|\gamma| + 2)} \leqslant \beta < 1. \tag{1}$$

Schoenfeld has informed me that the constant .05 may be replaced by .10367. However, the following two theorems are superior for our purposes.

THEOREM 2. *For $\nu = 1, 2$, let*

$$\varrho_\nu = 1 - \frac{\xi_\nu}{\log qT} + i\gamma_\nu$$

*be a zero of $L(s, \chi_\nu)$, where $\chi_\nu$ is a character* mod $q$, *$|\gamma_\nu| \leqslant T$, and $T \geqslant 1$. Suppose that if $\chi_1 = \chi_2$ then $\varrho_1 \neq \varrho_2$, or if $\chi_1 = \overline{\chi}_2$ then $\varrho_1 \neq \bar{\varrho}_2$. If $q$ is sufficiently large, then*

$$\xi_2 \geqslant .752 - \left(\frac{\sqrt{\xi_1^2 + 8\xi_1} - \xi_1}{2}\right) \tag{2}$$

*and*

$$\max(\xi_1, \xi_2) \geqslant 6/29. \tag{3}$$