Werk

Titel: Sieve methods and class-number probelms. II.

Autor: NAIR, Mohan; PERELLI, Alberto

Jahr: 1988

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0388|log6

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

J. reine angew. Math. **388** (1988), 40—64

Journal für die reine und angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1988

Sieve methods and class-number problems. II

By *Mohan Nair* at Glasgow and *Alberto Perelli* at Genova

Introduction

In this paper, we continue to investigate the links between sieve upper bounds for certain polynomials in two variables and weighted sums of negative powers of values of corresponding L-functions at $s=1$. The results we obtain include a generalisation of Siegel's theorem for the size of $L(1,\chi)$ for real characters and a generalisation of the striking recent effective result of Goldfeld-Gross-Zagier (see [4]) for the class-number problem. Another of our results (Corollary 1 of Theorem 3) is a conditional effective version of Siegel's theorem which is dependent on an effective sieve upper bound for a certain polynomial in two variables which we construct. We begin by describing our basic notation, which adheres to that introduced in our first paper [6].

For any $d\in\mathbb{N}$, write $d=r^2s$ where s is square-free. It is well known that the quadratic field $\mathbb{Q}(\sqrt{-d})$, $(=\mathbb{Q}(\sqrt{-s}))$, has discriminant $-D$ where $D=s$ if $s\equiv -1 \pmod 4$ and $D=4s$ otherwise. It is also known that $\chi(n)$ defined by the Kronecker symbol $\left(\frac{-D}{n}\right)$ is a real primitive character $(\bmod D)$. We denote by $L(s,\chi)$ the associated L-function. The dependence of χ on d will always be understood even when not explicitly mentioned. We also define $\varrho_d(p)$, for each $d\in\mathbb{N}$, to be the number of solutions $n \pmod p$ of the congruence $n^2+d\equiv 0 \pmod p$.

The statement of Theorem 1 depends on polynomials $f_k=f_k(n,d)$, in two variables n and d, defined for each $k\in\mathbb{N}$ as

$$f_k(n,d)=\prod_{i=0}^{k-1}(n^2+a_i^2d)$$

where $\{a_i\}$ is a sequence of positive integers defined by $a_0=1$, $a_i=\prod_{j=1}^{2i+2}p_j-1$ $(i\geqq 1)$, where p_j denotes the j^{th} prime number. Associated with each particular f_k are the functions $\omega_{n,f_k}(p)$ defined, for each n, to be the number of solutions $d \pmod p$ of $f_k(n,d)\equiv 0 \pmod p$ and $\varrho_{d,f_k}(p)$ defined, for each d, to be the number of solutions $n \pmod p$ of $f_k(n,d)\equiv 0 \pmod p$. The sequence $\{a_i\}$ is chosen so that both $\omega_{n,f_k}(p)$ and $\varrho_{d,f_k}(p)$ are strictly less than p. There are also a number of less interesting auxiliary functions which are described after the statement of Theorem 1. These mostly depend

on the particular sequence $\{a_i\}$ that we choose and since this choice is by no means unique, Theorem 1 is indeed a representative of a class of theorems, each with a different $c_k(d)$ and A_k.

Theorem 1. *Let $k \in \mathbb{N}$. Then we have*

$$\sum_{d \leqq y} c_k(d)\, L(1,\chi)^{-k} = A_k y + O_k(y \exp(-\sqrt{\log y})), \quad y \to \infty.$$

Here $c_k(d)$ and A_k are described as follows:

$$c_k(d) = c_1(d,k)\, c(d)^k, \quad c(d) = \prod_{p \nmid 2d} \left(1 - \frac{\theta(p)}{p^2}\right) \prod_{p \mid 2d} \left(1 - \frac{\chi(p)}{p}\right)^{-1},$$

$$\theta(p) = \chi(p) \left(1 - \left(\frac{\chi(p)+1}{p}\right) + \frac{\chi(p)}{p^2}\right)^{-1},$$

$$c_1(d,k) = \prod_{p \mid P_3(k)d} \left(1 - \frac{\varrho_{d,f_k}(p)}{p}\right)\left(1 - \frac{\varrho_d(p)}{p}\right)^{-k} \prod_{p \nmid P_3(k)d} \left(1 - \frac{k\varrho_d(p)}{p}\right)\left(1 - \frac{\varrho_d(p)}{p}\right)^{-k},$$

$$A_k = \prod_{p \leqq k} \left(1 - \frac{1}{p}\right)^{-k} \prod_{p > k} \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{k}{p}\right) \frac{\varphi(P_3(k))}{P_3(k)}$$
$$\prod_{p \nmid P_3(k)} \left(1 + \frac{k-1}{p(p-k)}\right) \cdot \sum_{t \mid \frac{P_2(k)}{(P_1(k), P_2(k))}} A(k,t)/\varphi(t),$$

$$A(k,t) = \prod_{p \mid P_3(k)} \left(1 - \frac{\omega_{t,f_k}(p)}{p}\right)\left(1 - \frac{\delta(p)}{p}\right)^{-1}, \quad \delta(p) = \begin{cases} k & \text{if } p > k, \\ 0 & \text{if } p \leqq k, \end{cases}$$

$\varphi(n)$ = Euler's function,

$$P_1(k) = \prod_{p \in \mathscr{P}_1(k)} p, \quad \text{where} \quad \mathscr{P}_1(k) = \left\{p : p \,\middle|\, \prod_{i=0}^{k-1} a_i\right\},$$

$$P_2(k) = \prod_{p \in \mathscr{P}_2(k)} p, \quad \text{where} \quad \mathscr{P}_2(k) = \left\{p : p \,\middle|\, \prod_{i>j} (a_i^2 - a_j^2)\right\},$$

and finally

$$P_3(k) = \prod_{p \mid P_1(k) P_2(k)} p.$$

The constants involved here are not effectively computable. Inspite of the rather complicated form of the expression for $c_k(d)$, it is easy to see that

$$\left(\frac{\varphi(d)}{d}\right)^{2k} \ll_k c_k(d) \ll_k \left(\frac{d}{\varphi(d)}\right)^{2k}$$

$$\left(\text{in fact, } \left(\frac{\varphi(d)}{d}\right)^{2k-1} \ll_k c_k(d) \ll_k \frac{d}{\varphi(d)}\right),$$

and hence $c_k(d)$ is reasonably well-behaved for each value of $k \in \mathbb{N}$.

Dirichlet's class-number formula immediately implies, again with ineffective implicit constants,

Corollary 1.

$$\sum_{d \leq y} c_k(d)\, D^{k/2} h(-D)^{-k} = \pi^k A_k y + O_k(y \exp(-\sqrt{\log y})), \quad y \to \infty.$$

An easy application of Cauchy's inequality, together with the bounds for $c_k(d)$ mentioned earlier, implies

Corollary 2. *For any $k \in \mathbb{N}$ we have*

$$\sum_{d \leq y} L(1, \chi)^{-k} \ll_k y.$$

We can recover Siegel's theorem for such characters from Corollary 2 by noting that choosing a single term from the left hand side of the inequality we obtain

$$L(1, \chi)^{-k} \ll_k D$$

and hence, for any $\varepsilon > 0$, the choice of $k = [1/\varepsilon] + 1$, for example, would imply that

$$L(1, \chi) \gg_\varepsilon 1/D^\varepsilon.$$

As mentioned in [6], the methods which we employ in the proof of Theorem 1 would allow us to prove, with slight changes, a corresponding theorem for real characters associated with real quadratic fields. This, together with the above comments, would enable us to recover Siegel's theorem in its full generality. This is, however, not a new demonstration of Siegel's theorem which is indeed utilised in the proof of Theorem 1.

By avoiding Siegel's theorem and appealing instead to the weaker but effective Goldfeld-Gross-Zagier result in the form $L(1, \chi) \gg_\varepsilon (\log D)^{1-\varepsilon} D^{-1/2}$, we obtain

Theorem 2. *For any $\varepsilon > 0$*

$$\sum_{d \leq y} c_2(d)\, L(1, \chi)^{-2} = A_2 y + O_\varepsilon(y(\log y)^{-2+\varepsilon}), \quad y \to \infty.$$

Here, in contrast, all constants are effectively computable. Again, this could be regarded as a generalisation of the Goldfeld-Gross-Zagier theorem, which can be recovered from Theorem 2 by elementary arguments. A similar remark to the one above regarding real characters associated with real quadratic fields also applies to Theorem 2. Even without using this deep result, we can show that

$$\sum_{d \leq y} c_2(d)\, L(1, \chi)^{-2} \ll y$$

with an effective implicit constant, i.e. an upper bound of the correct magnitude. The expectation of such effective upper bounds with higher powers of $L(1, \chi)^{-1}$ has to be tempered by the fact that even

$$\sum_{d \leq y} c_3(d)\, L(1, \chi)^{-3} \ll y$$

with an effective implied constant would imply that

$$h(-D) \gg_\varepsilon D^{1/6-\varepsilon}$$

with an effective implied constant. We can, however, give a conditional result of this nature. Our basic hypothesis is

Hypothesis H(A). *Let $A \geqq 1$ be a fixed positive constant and let ε be any positive number. Then for any positive N, we have*

$$\psi(t, \chi) = O_{N, A, \varepsilon}(t(\log t)^{-N}), \quad t \to \infty,$$

uniformly for every non-principal character $\chi \pmod D$ with $D \ll (\log t)^{A-\varepsilon}$. All constants are effectively computable.

This hypothesis is in fact a weak, but effective, version of a well known implication of Siegel's theorem and since this is known to be effective for $A = 2$, H(2) is certainly true.

We now define $S_f(x, y, z)$ as follows:

$$S_f(x, y, z) = S_{f,k}(x, y, z) = |\{(n, d): n \leqq x, d \leqq y, (f_k(n, d), P(z)) = 1\}|,$$

where $f_k(n, d)$ is as defined earlier and $P(z) = \prod_{p<z} p$. Certainly, as implied by our Theorem 4 below, we have that

$$S_f(x, y, z) \ll_k xy/(\log z)^k$$

for any z with $2 \leqq z \leqq \max(x, y)$ but with an ineffective implicit constant. From an effective point of view, we have

Theorem 3. *Let $k \in \mathbb{N}$ and suppose that* H(A) *holds for some $A \geqq 1$. Then there exists an effectively computable constant $v(k)$ such that assuming that*

$$S_f(x, y, z) \ll_k xy/(\log z)^k$$

holds for some $z \geqq \exp(y^B)$, where $B > 1/A$, some x with $x \geqq y^{v(k)}$ and $y \to \infty$, then we have

$$\sum_{d \leqq y} c_k(d)\, L(1, \chi)^{-k} \ll_k y, \quad y \to \infty.$$

An effective implicit constant in the bound for $S_f(x, y, z)$ implies an effective implicit constant in the conclusion.

Since it is well known that H(2) is true, we have

Corollary 1. *Suppose that the assumptions on $S_f(x, y, z)$ in Theorem 3 hold, with $A = 2$ and effectively computable constants, for an infinite sequence of k. Then for any $\varepsilon > 0$,*

$$h(-D) \gg_\varepsilon D^{1/2-\varepsilon}$$

with an effective implicit constant.

We remark that the hypothesis in Corollary 1 is satisfied if for an infinite sequence of k,

$$S_f(x, y, z) \ll_k xy/(\log z)^k$$

for all z with $2 \leqq z \leqq \max(x, y)$ and an effective implicit constant, i.e. a result of the Theorem 1-type of [6] but applied to the polynomial $f_k(n, d)$.

This corollary follows from our earlier discussion involving Siegel's theorem and Dirichlet's class-number formula.

As a consequence of Theorem 3, we have the interesting situation that if, for some fixed $A \geqq 1$, both H(A) and suitable sieve upper bounds depending on A hold, then H(A) is true for all $A \geqq 1$. Moreover, in the light of our previous remark regarding a corresponding result concerning real quadratic fields, well known classical arguments (see e.g. [1], ch. 22) imply, under similar conditions, an effective Siegel-Walfisz theorem with a slightly weaker error term.

Our final theorem concerns a sieve upper bound for general polynomials of the f_k-type. Theorem 4, although valid for all $k \in \mathbb{N}$, is ineffective for $k \geqq 3$ through the use of Siegel's theorem.

Let $\{a_i\}$ and $\{b_i\}$ be infinite sequences of positive integers and define, for any $k \in \mathbb{N}$, the polynomial $g_k = g_k(n, d)$ by

$$g_k(n, d) = \prod_{i=1}^{k} (a_i n^2 + b_i d),$$

with $\prod_{i>j} (a_i b_j - a_j b_i) \neq 0$. Define

$$S_{g,k}(x, y, z) = |\{(n, d): n \leqq x, d \leqq y, (g_k(n, d), P(z)) = 1\}|.$$

Then we have

Theorem 4. *For any $k \in \mathbb{N}$ and $x, y \geqq 2$, we have*

$$S_{g,k}(x, y, z) \ll_{g,k} xy/(\log z)^k$$

for $2 \leqq z \leqq \max(x, y)$ and where the implicit constant is effectively computable only for $k \leqq 2$.

We remark that the conditions on $g_k(n, d)$ may be somewhat relaxed at the cost of a slight complication in detail. For example, we can show that the sequences $\{a_i\}$ and $\{b_i\}$ can also contain negative integers.

The paper was written when the first-named author was a C.N.R. Visiting Professor at the University of Genova. He would like to thank the above institutions for their generous hospitality and pleasant working conditions.

Proof of Theorem 1

Let $f_k(n, d)$, $\varrho_{d, f_k}(p)$ and $\omega_{n, f_k}(p)$ be as defined in the Introduction. The proof of Theorem 1 follows in broad outline that of Theorem 2 of [6] with suitable alterations to cope with multiple quadratic factors of $f_k(n, d)$. We begin with two lemmas which verify that we can apply the basic sieve machinery.

Lemma 1. *For any positive integers k and d, we have that*

$$\varrho_{d, f_k}(p) < p$$

for all primes p.

Proof. Let us fix d. Since the polynomial $f_k(n, d)$ is of degree $2k$ in n, we certainly have $\varrho_{d, f_k}(p) < p$ whenever $p > 2k$. Suppose that $p \leqq 2k$. We can therefore write $p = p_j$ for some j with $1 \leqq j \leqq 2k-1$. Writing $f_k(n, d)$ as

$$f_k(n, d) = \prod_{i=0}^{[\frac{j}{2}]-1} (n^2 + a_i^2 d) \prod_{i=[\frac{j}{2}]}^{k-1} (n^2 + a_i^2 d)$$

we note that the first product is of degree $2[j/2]$ in n and so contributes at most $2[j/2]$ solutions $(\mathrm{mod}\, p_j)$. No new solution $n (\mathrm{mod}\, p_j)$ arises from the second product since for $i \geqq [j/2]$, we have $2i + 2 \geqq j$ and hence, by definition of the $\{a_i\}$, $a_i \equiv -1 (\mathrm{mod}\, p_j)$. Thus for all i in the range $[j/2] \leqq i \leqq k-1$, we have that $n^2 + a_i^2 d \equiv n^2 + a_0^2 d (\mathrm{mod}\, p_j)$, so that each solution $n (\mathrm{mod}\, p_j)$ of the second product has already been counted in the first. Hence we deduce that

$$\varrho_{d, f_k}(p_j) \leqq 2\left[\frac{j}{2}\right] \leqq j < p_j$$

as required. This completes the proof of Lemma 1.

Lemma 2 concerns the corresponding analogue for $\omega_{n, f_k}(p)$.

Lemma 2. *For any positive integers k and n, with* $(n, P_1(k)) = 1$, *we have that*

$$\omega_{n, f_k}(p) < p$$

for all primes p. ($P_1(k)$ *is defined in the Introduction*).

Proof. Let us fix n with $(n, P_1(k)) = 1$. Since $f_k(n, d)$ is of degree k in d, we have that $\omega_{n, f_k}(p) < p$ whenever $p > k$. Suppose therefore that $p \leqq k$ and write $p = p_j$ for some j with $1 \leqq j \leqq k-1$. As in Lemma 1, writing $f_k(n, d)$ as

$$f_k(n, d) = \prod_{i=0}^{j-1} (a_i^2 d + n^2) \prod_{i=j}^{k-1} (a_i^2 d + n^2),$$

we see that the first product contributes at most j solutions, since the condition $(n, P_1(k)) = 1$ implies that in any term in the product we have $(a_i^2, n^2) = 1$ and hence at most one solution from each such term. Again, as before, no new solution $d \pmod{p_j}$ arises from the second product so that

$$\omega_{n, f_k}(p_j) \leqq j < p_j$$

which completes the proof of Lemma 2.

We can now proceed as in [6], step 1 of the proof of Theorem 2, to compare the conclusions of two sieve processes. Let $x, y, z \geqq 2$ and $z_0(k) < z < \min(x, y)$, where $z_0(k)$ is the smallest integer such that $P_1(k) | P(z_0(k))$. Then we have that

$$(1) \qquad \sum_{d \in y} |\{n \leqq x : (f_k(n, d), P(z)) = 1\}| = \sum_{\substack{n \leqq x \\ (n, P_1(k)) = 1}} |\{d \leqq y : (f_k(n, d), P(z)) = 1\}|.$$

We would like to apply Theorem 2. 5 of Halberstam-Richert [5] to each term on the right hand side of (1) and Theorem 2. 6 of [5] to each term on the left hand side of (1) and then sum over n and d respectively. In order to do this, we need to verify the hypotheses of the above theorems and to check that the corresponding error terms do not depend on n and d.

Using Lemma 2 and the fact that $\omega_{n, f_k}(p) \leqq k$, it is easy to see that conditions (Ω_1), $(\Omega_2(\kappa))$ and (R) of Theorem 2. 5 of [5] are indeed satisfied with $\kappa = k$ (see also the remark on p. 82 of [5]). Moreover, from [5], top of p. 30, the implicit constants in the error terms of Theorem 2. 5 depend, in our problem, at most on k. The condition required for Theorem 2. 6 of [5] is satisfied by our Lemma 1 and the remark in [5], bottom of p. 86, implies that the implicit constants in the error terms of Theorem 2. 6 depend at most on k. Hence we can apply both theorems and deduce from (1) that

$$(2) \qquad x \sum_{d \leqq y} \prod_{p < z} \left(1 - \frac{\varrho_{d, f_k}(p)}{p}\right) \{1 + O_k(v^{-v/3}) + O_k(\exp(-\sqrt{\log x}))\}$$

$$= y \sum_{\substack{n \leqq x \\ (n, P_1(k)) = 1}} \prod_{p < z} \left(1 - \frac{\omega_{n, f_k}(p)}{p}\right) \{1 + O_k(u^{-u/3}) + O_k(\exp(-\sqrt{\log y}))\},$$

where $u = \log y / \log z$ and $v = \log x / \log z$, provided that, say, $z \geqq (ck)^{2k}$ and $u, v > ck^2$, for example, with a suitable absolute constant c.

We now write the products which occur in (2) in a more simplified form. Let $P_2(k)$ and $P_3(k)$ be as defined in the Introduction. It is clear that if $p \nmid dP_3(k)$ then

i) the polynomials $n^2 + a_i^2 d$, $0 \leqq i \leqq k-1$, are all distinct (mod p),

ii) $a_i^2 d \not\equiv 0 \pmod{p}$, $0 \leqq i \leqq k-1$, and

iii) the quadratic character of $a_i^2 d \pmod{p}$ is independent of i.

Hence we can deduce that

$$\varrho_{d, f_k}(p) = k\varrho_d(p) \quad \text{if} \quad p \nmid dP_3(k),$$

where, as defined before,

$$\varrho_d(p) = |\{n \pmod{p} : n^2 + d \equiv 0 \pmod{p}\}|.$$

Similarly, it is easy to see that

$$\omega_{n, f_k}(p) = k \quad \text{if} \quad p \nmid nP_3(k).$$

Observe that since $a_{k-1} + a_0 = \prod_{j=1}^{k} p_j$, we certainly have that every prime $\leqq k$ divides $P_2(k)$, so that if $P_4(k)$ is defined by $\prod_{p \leqq k} p$, we have that $P_4(k) | P_2(k)$. We shall use this in the proof of the next lemma.

In the meantime, we can use the above deductions to write (2) in the form

$$(3) \qquad x \sum_{d \leqq y} c_1(d, k, z) \prod_{p<z} \left(1 - \frac{\varrho_d(p)}{p}\right)^k \{1 + O_k(v^{-v/3}) + O_k(\exp(-\sqrt{\log x}))\}$$

$$= y \sum_{\substack{n \leqq x \\ (n, P_1(k)) = 1}} c_2(n, k, z) \prod_{p<z} \left(1 - \frac{1}{p}\right)^k \{1 + O_k(u^{-u/3}) + O_k(\exp(-\sqrt{\log y}))\},$$

where

$$c_1(d, k, z) = \prod_{\substack{p<z \\ p | dP_3(k)}} \left(1 - \frac{\varrho_{d, f_k}(p)}{p}\right)\left(1 - \frac{\varrho_d(p)}{p}\right)^{-k} \prod_{\substack{p<z \\ p \nmid dP_3(k)}} \left(1 - \frac{k\varrho_d(p)}{p}\right)\left(1 - \frac{\varrho_d(p)}{p}\right)^{-k}$$

and

$$c_2(n, k, z) = \prod_{\substack{p<z \\ p | nP_3(k)}} \left(1 - \frac{\omega_{n, f_k}(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k} \prod_{\substack{p<z \\ p \nmid nP_3(k)}} \left(1 - \frac{k}{p}\right)\left(1 - \frac{1}{p}\right)^{-k}.$$

Moreover since $\lim_{z \to \infty} c_1(d, k, z)$ and $\lim_{z \to \infty} c_2(n, k, z)$ exist, we define

$$c_1(d, k) = \lim_{z \to \infty} c_1(d, k, z) \quad \text{and} \quad c_2(n, k) = \lim_{z \to \infty} c_2(n, k, z).$$

From now onwards, we shall fix $x=y$. On choosing $z_0=\exp(c\sqrt{\log y})$ with c sufficiently large as a function of k, it is easy to see that

$$c_1(d,k,z_0)=c_1(d,k)\{1+O_k(\exp(-\sqrt{\log y}))\}, \tag{4}$$

$$c_2(n,k,z_0)=c_2(n,k)\{1+O_k(\exp(-\sqrt{\log y}))\}. \tag{5}$$

We next need the following lemma.

Lemma 3. *We have, as* $y\to\infty$,

$$\sum_{\substack{n\leqq y\\(n,P_1(k))=1}} c_2(n,k)=A_k y+O_k((\log y)^{c_k}).$$

Here $c_k=k-1+\omega(P_2(k)/(P_1(k),P_2(k)))$ and A_k is as defined in the Introduction. The function ω in the description of c_k is, as usual, the one that counts the number of distinct prime factors of a number.

Proof. Writing, for convenience, $\omega_{n,f_k}(p)$ as $\omega_n(p)$ and each $P_i(k)$ as P_i, we have from the definition of $c_2(n,k)$ that

$$c_2(n,k)=\prod_{p\leqq k}\left(1-\frac{1}{p}\right)^{-k}\prod_{p>k}\left(1-\frac{1}{p}\right)^{-k}\left(1-\frac{k}{p}\right)\prod_{p\mid nP_3}\left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{\delta(p)}{p}}\right), \tag{6}$$

where

$$\delta(p)=\begin{cases}k & \text{if } p>k,\\ 0 & \text{if } p\leqq k.\end{cases}$$

Here we have used the earlier remark that $p\leqq k$ implies that $p\mid P_2$ and hence $p\mid P_3$. We use this again, along with the observation that $\omega_n(p)=1$ whenever $(n,P_1)=1$ and $p\mid n$, to write

$$\sum_{\substack{n\leqq y\\(n,P_1)=1}}\prod_{p\mid nP_3}\left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{\delta(p)}{p}}\right)=\sum_{\tau\mid\frac{P_2}{(P_1,P_2)}}\sum_{\substack{n\leqq y\\(n,P_1)=1\\(n,P_2)=\tau}}\prod_{\substack{p\mid n\\p\nmid P_3}}\left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}}\right)\prod_{\substack{p\mid P_3\\p\nmid n}}\left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{\delta(p)}{p}}\right). \tag{7}$$

We now simplify the second product on the right side of (7) as follows. First observe that for any n with $(n,P_1)=1$, $(n,P_2)=\tau$, we have that

$$p\nmid n,\quad p\mid P_3 \Leftrightarrow p\nmid\tau,\quad p\mid P_3.$$

Further, for all n and p with $p \nmid n$, it is clear that $\omega_n(p)$ depends on k, on the number of i such that $p|a_i$ and on the number of pairs (i,j) such that $a_i^2 \equiv a_j^2 \pmod p$, and is therefore independent of any particular choice of n. We may therefore deduce that, in (7),

$$\prod_{\substack{p|P_3\\ p\nmid n}} \left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{\delta(p)}{p}} \right) = \prod_{\substack{p|P_3\\ p\nmid \tau}} \left(\frac{1-\frac{\omega_\tau(p)}{p}}{1-\frac{\delta(p)}{p}} \right) = A(k,\tau).$$

(7) therefore simplifies to

$$(8) \qquad \sum_{\substack{n\leqq y\\ (n,P_1)=1}} \prod_{p|nP_3} \left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{\delta(p)}{p}} \right) = \sum_{\tau|\frac{P_2}{(P_1,P_2)}} A(k,\tau) \sum_{\substack{n\leqq y\\ (n,P_1)=1\\ (n,P_2)=\tau}} \prod_{\substack{p|n\\ p\nmid P_3}} \left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}} \right).$$

We now note that any n on the right side of (8) can be written as $n=mt$ with $(m,P_3)=1$ and $\ker t=\tau$, where $\ker t=\prod_{p|t} p$, and thus (8) becomes

$$(9) \qquad \sum_{\substack{n\leqq y\\ (n,P_1)=1}} \prod_{p|nP_3} \left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{1}{p}} \right) = \sum_{\tau|\frac{P_2}{(P_1,P_2)}} A(k,\tau) \sum_{\substack{mt\leqq y\\ (m,P_3)=1\\ \ker t=\tau}} \prod_{p|m} \left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}} \right)$$

$$= \sum_{\tau|\frac{P_2}{(P_1,P_2)}} A(k,\tau) \sum_{\substack{t\leqq y\\ \ker t=\tau}} \sum_{\substack{m\leqq y/t\\ (m,P_3)=1}} \prod_{p|m} \left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}} \right).$$

We may write, since $p|m$, $(m,P_3)=1$ implies that $p>k$,

$$(10) \qquad \prod_{p|m} \left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}} \right) = \prod_{p|m} \left(1-\frac{1}{p}\right) \left(\sum_{i=0}^{\infty} \left(\frac{k}{p}\right)^i \right)$$

$$= \prod_{p|m} \left(1+\frac{k-1}{p}+\frac{k(k-1)}{p^2}+\frac{k^2(k-1)}{p^3}+\cdots \right)$$

$$= \sum_{\ker h|m} \frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h},$$

where $\Omega(h)$ counts the number, with multiplicity, of prime factors of h. From (10) we have

$$(11)\qquad \sum_{\substack{m\leqq y/t\\(m,P_3)=1}}\prod_{p\mid m}\left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}}\right)=\sum_{\substack{m\leqq y/t\\(m,P_3)=1}}\sum_{\ker h\mid m}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h}$$

$$=\sum_{\substack{Q(h)\leqq y/t\\(h,P_3)=1}}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h}\sum_{\substack{m\leqq y/t\\(m,P_3)=1\\m\equiv 0\,(\mathrm{mod}\,\ker h)}}1,$$

where $Q(h)$ denotes the greatest prime divisor of h. Since $(h,P_3)=1$, the chinese remainder theorem implies that

$$(12)\qquad \sum_{\substack{m\leqq y/t\\(m,P_3)=1\\m\equiv 0\,(\mathrm{mod}\,\ker h)}}1=\sum_{(r,P_3)=1}\sum_{m\equiv c_{r,h}\,(\mathrm{mod}\,P_3\ker h)}1=\frac{\varphi(P_3)}{P_3}\frac{y}{t\ker h}+O(\varphi(P_3)),$$

where $c_{r,h}$ runs over $\varphi(P_3)$ suitable residue classes $(\mathrm{mod}\,P_3\ker h)$.

From (11) and (12) we obtain

$$(13)\qquad \sum_{\substack{m\leqq y/t\\(m,P_3)=1}}\prod_{p\mid m}\left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}}\right)=\frac{\varphi(P_3)}{P_3}\frac{y}{t}\sum_{\substack{Q(h)\leqq y/t\\(h,P_3)=1}}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h\ker h}$$

$$+O_k\left(\sum_{\substack{Q(h)\leqq y/t\\(h,P_3)=1}}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h}\right).$$

We can write

$$(14)\qquad \sum_{\substack{Q(h)\leqq y/t\\(h,P_3)=1}}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h\ker h}=\prod_{\substack{p\leqq y/t\\p\nmid P_3}}\left(1+\sum_{i=1}^{\infty}\frac{k^{i-1}(k-1)}{p^{i+1}}\right)$$

$$=\prod_{\substack{p\leqq y/t\\p\nmid P_3}}\left(1+\frac{k-1}{p(p-k)}\right)=\prod_{p\nmid P_3}\left(1+\frac{k-1}{p(p-k)}\right)\prod_{\substack{p>y/t\\p\nmid P_3}}\left(1+\frac{k-1}{p(p-k)}\right)^{-1},$$

the infinite product being absolutely convergent. We can estimate the second product on the right side of (14) by

$$(15)\qquad \prod_{\substack{p>y/t\\p\nmid P_3}}\left(1+\frac{k-1}{p(p-k)}\right)^{-1}=\exp\left(-\sum_{\substack{p>y/t\\p\nmid P_3}}\log\left(1+\frac{k-1}{p(p-k)}\right)\right)=1+O_k\left(\frac{t}{y}\right).$$

Moreover, we have that

$$(16)\qquad \sum_{\substack{Q(h)\leqq y/t\\(h,P_3)=1}}\frac{k^{\Omega(h)-\omega(h)}(k-1)^{\omega(h)}}{h}=\prod_{\substack{p\leqq y/t\\p\nmid P_3}}\left(1+\sum_{i=1}^{\infty}\frac{k^{i-1}(k-1)}{p^i}\right)$$

$$=\prod_{\substack{p\leqq y/t\\p\nmid P_3}}\left(1+\frac{k-1}{p-k}\right)=\exp\left(\sum_{\substack{p\leqq y/t\\p\nmid P_3}}\log\left(1+\frac{k-1}{p-k}\right)\right)=O_k\left(\left(\log\left(\frac{y}{t}\right)\right)^{k-1}\right).$$

Hence from (13)—(16) we deduce that

$$(17)\qquad \sum_{\substack{m\leqq y/t\\(m,P_3)=1}}\prod_{p\mid m}\left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}}\right)=\frac{\varphi(P_3)}{P_3}\prod_{p\nmid P_3}\left(1+\frac{k-1}{p(p-k)}\right)\frac{y}{t}+O_k\left(\left(\log\left(\frac{y}{t}\right)\right)^{k-1}+1\right).$$

Now we observe that

$$\sum_{\ker t=\tau}\frac{1}{t}=\frac{1}{\varphi(\tau)}$$

and that

$$(18)\qquad \sum_{\substack{t\leqq y\\\ker t=\tau}}1=O_k((\log y)^{\omega(\tau)}).$$

From (17) and (18) we obtain

$$(19)\qquad \sum_{\substack{t\leqq y\\\ker t=\tau}}\sum_{\substack{m\leqq y/t\\(m,P_3)=1}}\prod_{p\mid m}\left(\frac{1-\frac{1}{p}}{1-\frac{k}{p}}\right)=\frac{\varphi(P_3)}{P_3}\prod_{p\nmid P_3}\left(1+\frac{k-1}{p(p-k)}\right)\frac{y}{\varphi(\tau)}+O_k((\log y)^{k-1+\omega(\tau)})$$

and hence, from (19),

$$(20)\qquad \sum_{\substack{n\leqq y\\(n,P_1)=1}}\prod_{p\mid nP_3}\left(\frac{1-\frac{\omega_n(p)}{p}}{1-\frac{1}{p}}\right)$$

$$=\frac{\varphi(P_3)}{P_3}\prod_{p\nmid P_3}\left(1+\frac{k-1}{p(p-k)}\right)\sum_{\tau\mid\frac{P_2}{(P_1,P_2)}}\frac{A(k,\tau)}{\varphi(\tau)}+O_k((\log y)^{c_k}),$$

where c_k is as defined after the statement of the lemma. Lemma 3 now follows from (6) and (20).

Using (4), (5) and Lemma 3, we deduce from (3) that

$$\sum_{d\leqq y} c_1(d,k)\prod_{p<z_0}\left(1-\frac{\varrho_d(p)}{p}\right)^k = A_k y\prod_{p<z_0}\left(1-\frac{1}{p}\right)^k\{1+O_k(\exp(-\sqrt{\log y}))\}. \tag{21}$$

Now, as in step 2 of Theorem 2 in [6], we transform the product involving $\varrho_d(p)$ into one involving $\chi(p)$ $(=\chi_d(p))$. We have

$$\prod_{p<z_0}\left(1-\frac{\varrho_d(p)}{p}\right)^k = c(d)^k\prod_{p<z_0}\left(1-\frac{\chi(p)}{p}\right)^k\prod_{p<z_0}\left(1-\frac{1}{p}\right)^k\{1+O_k(\exp(-\sqrt{\log y}))\}, \tag{22}$$

where, as mentioned after the statement of Theorem 1,

$$c(d)=\prod_{p\nmid 2d}\left(1-\frac{\theta(p)}{p^2}\right)\prod_{p\mid 2d}\left(1-\frac{\chi(p)}{p}\right)^{-1}.$$

From (21) and (22) we obtain

$$\sum_{d\leqq y} c_1(d,k)\,c(d)^k\prod_{p<z_0}\left(1-\frac{\chi(p)}{p}\right)^k = A_k y\{1+O_k(\exp(-\sqrt{\log y}))\}. \tag{23}$$

Finally, as in [6], we express the product in (23) in terms of $L(1,\chi)^{-k}$. To this end we use Lemma 1 of [6] which we re-state here as

Lemma 4. *Let s and Q be real numbers with $Q\geqq 9$ and $s\geqq\log^{20}Q$. Then there are at most $O(Q^{7/8})$ distinct primitive characters to moduli not exceeding Q for which the estimate*

$$L(1,\chi)=\prod_{p<s}\left(1-\frac{\chi(p)}{p}\right)^{-1}\{1+O(s^{-1/10})+O(Q^{-1/16})\}$$

fails.

Note that in [6] the word primitive in the statement of Lemma 1 was inadvertently omitted, and the range for s should be altered to $s\geqq\log^{20}Q$.

We call "good" a discriminant $D\leqq 4y$ if it is not an exception in the sense of Lemma 4 with $Q=4y$, and "bad" otherwise. Correspondingly, a positive integer $d\leqq y$ is good if it gives rise, as explained in the Introduction, to a good D and bad otherwise. Define $c_k(d)$ by $c_k(d)=c_1(d,k)\,c(d)^k$. Estimating $c_k(d)$ rather crudely, we have that

$$\left(\frac{\varphi(d)}{d}\right)^{2k}\ll_k c_k(d)\ll_k\left(\frac{d}{\varphi(d)}\right)^{2k}$$

so that we deduce

$$\sum_{\substack{d\leqq y\\ d\text{ bad}}} c_k(d)\prod_{p<z_0}\left(1-\frac{\chi(p)}{p}\right)^k \ll_k (\log y)^{k+1}\sum_{\substack{d\leqq y\\ d\text{ bad}}} 1 \ll_k (\log y)^{k+1}\sum_{\substack{r,s\\ r^2s\leqq y,\ s\ll y^{7/8}}} 1 \ll_k y^{31/32}. \tag{24}$$

From (23) and (24) we get that

$$\sum_{\substack{d \leq y \\ d \text{ good}}} c_k(d) \prod_{p < z_0} \left(1 - \frac{\chi(p)}{p}\right)^k = A_k y \{1 + O_k(\exp(-\sqrt{\log y}))\},$$

and choosing $s = z_0$ and $Q = 4y$ in Lemma 4, we deduce that

$$\sum_{\substack{d \leq y \\ d \text{ good}}} c_k(d) L(1, \chi)^{-k} = A_k y \{1 + O_k(\exp(-\sqrt{\log y}))\}. \tag{25}$$

Until this point in the proof all constants involved are effectively computable. The ineffectiveness of Theorem 1 arises from the following estimation of

$$\sum_{\substack{d \leq y \\ d \text{ bad}}} c_k(d) L(1, \chi)^{-k}$$

which uses Siegel's theorem. Choosing $\varepsilon = 1/64k$ in Siegel's theorem, we have

$$L(1, \chi)^{-k} \ll_k D^{1/64} \ll_k y^{1/64},$$

so that

$$\sum_{\substack{d \leq y \\ d \text{ bad}}} c_k(d) L(1, \chi)^{-k} \ll_k y^{1/64} \log y \sum_{\substack{d \leq y \\ d \text{ bad}}} 1 \ll_k y^{63/64}. \tag{26}$$

Theorem 1 now follows from (25) and (26).

Proof of Theorem 2

The proof of Theorem 2 follows closely that of Theorem 1.

Choosing $k = 2$ in (25) we have that

$$\sum_{\substack{d \leq y \\ d \text{ good}}} c_2(d) L(1, \chi)^{-2} = A_2 y \{1 + O(\exp(-\sqrt{\log y}))\}. \tag{27}$$

In order to estimate the sum over bad d's we use, instead of Siegel's theorem, the following result due to Tatuzawa [7]: given any $\varepsilon > 0$,

$$L(1, \chi) > \frac{\varepsilon}{10 D^{\varepsilon}}$$

for all primitive real characters (mod D) which at most one exception. Let $\bar{D}$ be the possible exceptional modulus in Tatuzawa's theorem associated with $\varepsilon = 1/128$. We then have

$$\sum_{\substack{d \leq y \\ d \text{ bad}}} c_2(d) L(1, \chi)^{-2} \ll y^{1/64} \log y \sum_{\substack{d \leq y \\ d \text{ bad}}} 1 + \sum_{\substack{d \leq y \\ d \text{ gives} \\ \text{rise to } \bar{D}}} c_2(d) L(1, \chi)^{-2}. \tag{28}$$

Clearly,

$$S = \sum_{\substack{d \leqq y \\ d \text{ gives} \\ \text{rise to } \bar{D}}} c_2(d)\, L(1,\chi)^{-2} = \sum_{\substack{r \\ r^2 \bar{s} \leqq y}} c_2(r^2\bar{s})\, L(1,\chi)^{-2}, \tag{29}$$

where $\bar{s} = \bar{D}$ if $\bar{D} \equiv 1 \pmod 4$ and $\bar{s} = \bar{D}/4$ if $\bar{D} \equiv 0 \pmod 4$.

We now appeal to the following result of Goldfeld-Gross-Zagier (see [4]): for any $\varepsilon > 0$, there exists an effectively computable constant $c(\varepsilon) > 0$ such that

$$L(1,\chi)^{-1} \leqq c(\varepsilon) \frac{\sqrt{D}}{(\log D)^{1-\varepsilon}}. \tag{30}$$

From (29) and (30) we have that

$$\begin{aligned} S &\ll_\varepsilon \frac{\bar{D}}{(\log \bar{D})^{2-2\varepsilon}} \left(\frac{\bar{D}}{\varphi(\bar{D})}\right) \sum_{r \ll \sqrt{y/\bar{D}}} \left(\frac{r}{\varphi(r)}\right)^8 \\ &\ll_\varepsilon \frac{\bar{D}^{1/2} y^{1/2}}{(\log \bar{D})^{2-3\varepsilon}} \ll_\varepsilon y(\log y)^{-2+3\varepsilon} \end{aligned} \tag{31}$$

since, for any positive integer a,

$$\sum_{r \leqq t} \left(\frac{r}{\varphi(r)}\right)^a \ll_a t. \tag{32}$$

From (28)—(32) we get

$$\sum_{\substack{d \leqq y \\ d \text{ bad}}} c_2(d)\, L(1,\chi)^{-2} \ll_\varepsilon y^{63/64} + y(\log y)^{-2+3\varepsilon}, \tag{33}$$

and Theorem 2 follows from (27) and (33).

Remark. As we have already mentioned in the Introduction, we can avoid the use of the Goldfeld-Gross-Zagier theorem and yet get an upper bound for the sum in Theorem 2 of the correct order of magnitude.

Indeed, it follows from Gauss [3] that

$$h(-D) \geqq 2^{\omega(D)-1}.$$

From Dirichlet's class-number formula and (29), we get the estimate

$$\begin{aligned} S &\ll \frac{\bar{D}}{h(-\bar{D})^2} \sum_{\substack{r \\ r^2\bar{s} \leqq y}} \left(\frac{r^2\bar{s}}{\varphi(r^2\bar{s})}\right)^4 \ll \frac{\bar{D}}{h(-\bar{D})^2} \left(\frac{\bar{D}}{\varphi(\bar{D})}\right)^4 \cdot \sqrt{\frac{y}{\bar{D}}} \\ &\ll y^{1/2} \bar{D}^{1/2} \left(\frac{\sum_{p/\bar{D}} \left(1 + \frac{1}{p}\right)^2}{2^{\omega(\bar{D})}} \right)^2 \ll y^{1/2} \bar{D}^{1/2} \ll y. \end{aligned}$$

Using this estimate for S and (27), (28), we obtain the weaker result

$$\sum_{d\leqq y} c_2(d)\, L(1,\chi)^{-2} \ll y$$

with an effectively computable implicit constant.

Proof of Theorem 3

Let $x, y, z \geqq 2$, $z < x$, $v = \log x/\log z$ and $v > ck^2$ where $c > 0$ is some suitable constant. As in the proof of Theorem 1, from Theorem 2. 6 of [5] and Lemma 1, we get

$$S_f(x,y,z) = x \sum_{d\leqq y} \prod_{p<z} \left(1 - \frac{\varrho_{d,f_k}(p)}{p}\right) \{1 + O_k(v^{-v/3}) + O_k(\exp(-\sqrt{\log y}))\}. \tag{34}$$

Let $B > 1/A$ and choose z to be any $z \geqq z_0$ where

$$z_0 = \exp(y^B).$$

Further, let $v(k) \geqq ck^2$ be any positive number such that, letting $x = z_0^{v(k)}$, both the error terms in (34) are $\leqq 1/4$. With the above choice of z, it is easy to see that there exists a positive constant $a(k)$ such that

$$c_1(d,k,z) \geqq a(k)\, c_1(d,k) \tag{35}$$

and

$$\prod_{p<z} \left(1 - \frac{\varrho_d(p)}{p}\right)^k \geqq a(k) \prod_{p<z} \left(1 - \frac{1}{p}\right)^k \prod_{p<z} \left(1 - \frac{\chi(p)}{p}\right)^k c(d)^k. \tag{36}$$

Here, the proof of (35) follows the reasoning leading to (4) and that of (36) the discussion following (7) in [6]. From (34)—(36), as in the proof of Theorem 1, we get that

$$x \sum_{d\leqq y} c_k(d) \prod_{p<z} \left(1 - \frac{\chi(p)}{p}\right)^k \prod_{p<z} \left(1 - \frac{1}{p}\right)^k \ll_k S_f(x,y,z) \tag{37}$$

where all the constants involved are effectively computable.

Now we need the following lemma.

Lemma 5. *Let Hypothesis* H(A) *be true for some* $A \geqq 1$. *Then, for any* $N > 0$,

$$L(1,\chi) = \prod_{p<s} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \{1 + O_{N,A}(\log s)^{-N}\},$$

where $s \geqq \exp(y^B)$, *holds uniformly for all non-principal characters* (mod D), $D \ll y$, *with effectively computable constants. Here* $B > 1/A$.

Proof. The proof follows that of Lemma 22. 3 of [2]. For $1<\sigma\leqq 2$, we have

$$\sum_{p>s}\chi(p)p^{-\sigma}=-s^{-\sigma}\sum_{p\leqq s}\chi(p)+\sigma\int_{s}^{\infty}\xi^{-\sigma-1}\sum_{p\leqq\xi}\chi(p)\,d\xi=O_{N,A}((\log s)^{-N}), \tag{38}$$

uniformly for all non-principal characters (mod D), $D\ll y$, since $y\ll(\log s)^{1/B}$. Now,

$$L(\sigma,\chi)=\prod_{p\leqq s}\left(1-\frac{\chi(p)}{p^{\sigma}}\right)^{-1}\exp\left(-\sum_{p>s}\log\left(1-\frac{\chi(p)}{p^{\sigma}}\right)\right), \tag{39}$$

and

$$\sum_{p>s}\left|-\log\left(1-\frac{\chi(p)}{p^{\sigma}}\right)-\frac{\chi(p)}{p^{\sigma}}\right|\leqq\sum_{p>s}p^{-2}\leqq 2\,s^{-1}. \tag{40}$$

Lemma 5 follows from (38)—(40).

Using Lemma 5, with $s=z$, and the hypothesis of Theorem 3, we deduce from (37) that

$$x\sum_{d\leqq y}c_k(d)\,L(1,\chi)^{-k}\prod_{p<z}\left(1-\frac{1}{p}\right)^{k}\ll_k\frac{xy}{(\log z)^k}$$

and hence

$$\sum_{d\leqq y}c_k(d)\,L(1,\chi)^{-k}\ll_k y$$

as required. This completes the proof of Theorem 3.

Proof of Theorem 4

Let

$$B=\prod_{i=1}^{k}b_i,\quad P_1=\prod_{p\mid B}p,$$

$$I(p)=\{i\in[1,k]:\ b_i\equiv 0\ (\mathrm{mod}\ p)\},$$

$$\mathscr{P}_0=\{p\leqq k:\ a_i\bar{b}_i,\ i\in[1,k]\setminus I(p),\ \text{covers all residue classes (mod}\ p)\},$$

and

$$P_0=\prod_{p\in\mathscr{P}_0}p.$$

We first show that the theorem is non-trivial only if

i) $(a_i, b_i) = 1, \quad 1 \leqq i \leqq k$

and

ii) $(P_0, P_1) = 1$.

Suppose that $(a_i, b_i) > 1$ for some i, $1 \leqq i \leqq k$. Then clearly for $z > z_0(g)$, we have that

$$S_{g,k}(x, y, z) = 0, \tag{41}$$

and for $z \leqq z_0(g)$ the theorem is trivially true.

Next, assume that $q | (P_0, P_1)$ for some prime q. If $q | n$ then clearly $(g_k(n, d), P(z)) > 1$ for any $z > q$ and hence (41) again holds for all such z. Suppose therefore that $q \nmid n$. Then

$$\begin{aligned} g_k(n, d) &\equiv \prod_{i \notin I(q)} (a_i n^2 + b_i d) \prod_{i \in I(q)} a_i n^2 \\ &\equiv \prod_{i \notin I(q)} \bar{b}_i \prod_{i \notin I(q)} (a_i n^2 + b_i d) \prod_{i \in I(q)} a_i n^2 \prod_{i \notin I(q)} b_i \\ &\equiv \prod_{i \in I(q)} a_i n^2 \prod_{i \notin I(q)} (a_i \bar{b}_i n^2 + d) \prod_{i \notin I(q)} b_i \pmod{q}. \end{aligned}$$

Now since $q \nmid n$ and $q | P_0$, $a_i \bar{b}_i n^2$ runs over all residue classes (mod q) and hence the same is true for $a_i \bar{b}_i n^2 + d$. It therefore follows that $(g_k(n, d), P(z)) > 1$ for $z > q$ and hence (41) holds for $z > q$.

We shall therefore assume from now onwards that i) and ii) hold for our $g_k(n, d)$.

Now we define, as we did with f_k,

$$\varrho_{d,g}(p) = |\{n \pmod p : g_k(n, d) \equiv 0 \pmod p\}|,$$

$$\omega_{n,g}(p) = |\{d \pmod p : g_k(n, d) \equiv 0 \pmod p\}|$$

and the new function

$$\varrho_{i,d}(p) = |\{n \pmod p : a_i n^2 + b_i d \equiv 0 \pmod p\}|.$$

It is clear from the above discussion that if $z > z(g)$, $z(g)$ a suitable constant, then

$$S_{g,k}(x, y, z) = \sum_{\substack{n \leqq x \\ (n, P_1) = 1 \\ n \equiv 0 \pmod{P_0}}} |\{d \leqq y : (g_k(n, d), P(z)) = 1\}|. \tag{42}$$

Suppose that

$$z \leqq y. \tag{43}$$

We want to apply, for each n in (42), Theorem 2. 5 of [5] with $\kappa = k$. The arguments at the start of the proof of Theorem 1 imply that we need only to check that

$$\omega_{n,g}(p) < p$$

for all primes p. But $\omega_{n,g}(p) = p$ can occur only when $p \leqq k$ and $a_i \overline{b_i}$ covers all residue classes (mod p) for $i \in [1, k] \setminus I(p)$, i.e. $p \in \mathscr{P}_0$. It is easy to see that if $p | n$ then $\omega_{n,g}(p) = 1$ so that we deduce that $\omega_{n,g}(p) = p$ can only occur if $p \in \mathscr{P}_0$ and $p \nmid n$. This contradicts $n \equiv 0 \pmod{P_0}$. Hence we can apply Theorem 2. 5 of [5] to deduce

$$S_{g,k}(x, y, z) = y \sum_{\substack{n \leqq x \\ (n, P_1) = 1 \\ n \equiv 0 \pmod{P_0}}} \prod_{p < z} \left(1 - \frac{\omega_{n,g}(p)}{p}\right) \{1 + O(u^{-u/3}) + O(\exp(-\sqrt{\log y}))\}, \tag{44}$$

where $u = \log y / \log z$, $z \leqq y$ and where, as throughout this section, the implicit constants depend on the coefficients of $g_k(n, d)$. Moreover, as in the proof of Theorem 1, it is clear that there exists a constant $c(g) > 0$ such that

$$\omega_{n,g}(p) = k \tag{45}$$

provided that $p \nmid c(g) n$, and that

$$\prod_{p < z} \left(1 - \frac{\omega_{n,g}(p)}{p}\right) = c_2(n, g, z) \prod_{p < z} \left(1 - \frac{1}{p}\right)^k \tag{46}$$

with a suitable $c_2(n, g, z)$ satisfying

$$c_2(n, g, z) \ll \left(\frac{n}{\varphi(n)}\right)^{2k}. \tag{47}$$

Hence from (44)—(47) we get that

$$S_{g,k}(x, y, z) \ll \frac{x y}{(\log z)^k}, \tag{48}$$

provided that (43) holds, since it is clear from (47) that

$$\sum_{\substack{n \leqq x \\ (n, P_1) = 1 \\ n \equiv 0 \pmod{P_0}}} c_2(n, g, z) \ll x.$$

Let now

$$A=\prod_{i=1}^{k} a_i, \quad P_2=\prod_{p\mid A} p$$

$$J(p)=\{i\in[1,k]: a_i\equiv 0 \pmod p\},$$

$$\mathscr{P}_0'=\{p\leqq 2k: -\bar{a}_i b_i,\ i\in[1,k]\setminus J(p), \text{ covers all the quadratic residues, and the zero-class, (mod } p)\},$$

$$R(\mathscr{P}_0')=\{d\in\mathbb{N}: d \text{ is a quadratic residue (mod } p) \text{ for some } p\in\mathscr{P}_0'\}.$$

Let $z\leqq x$ and $z>z(g)$, where $z(g)$ is some suitable constant. Then we have

$$S_{g,k}(x,y,z)=\sum_{\substack{d\leqq y\\(d,P_2)=1\\d\notin R(\mathscr{P}_0')}} |\{n\leqq x: (g_k(n,d),P(z))=1\}|. \tag{49}$$

Indeed, it is clear that the d's with $(d,P_2)>1$ do not contribute to $S_{g,k}(x,y,z)$. Suppose now that $d\in R(\mathscr{P}_0')$ and let p be a prime in $\mathscr{P}_0'$ such that d is a quadratic residue (mod p). Then

$$\begin{aligned} g_k(n,d) &\equiv \prod_{i\in J(p)} b_i d \prod_{i\notin J(p)} (a_i n^2+b_i d) \\ &\equiv \prod_{i\in J(p)} b_i d \prod_{i\notin J(p)} a_i \prod_{i\notin J(p)} (n^2+\bar{a}_i b_i d) \pmod p. \end{aligned}$$

But $-\bar{a}_i b_i d$ runs over all the quadratic residues, and the zero-class, (mod p), hence

$$g_k(n,d)\equiv 0 \pmod p.$$

Thus, if $z>2k$, then certainly those d's with $d\in R(\mathscr{P}_0')$ do not contribute to $S_{g,k}(x,y,z)$.

In order to apply Theorem 2. 6 of [5], for each d in (49), we need to verify that

$$\varrho_{d,g}(p)<p \tag{50}$$

for all primes p. However, it is easy to see that very similar arguments to those used to prove the corresponding property for $\omega_{n,g}(p)$ show that the conditions on d in the sum in (49) imply (50). Hence we get

$$S_{g,k}(x,y,z)=x\sum_{\substack{d\leqq y\\(d,P_2)=1\\d\notin R(\mathscr{P}_0')}} \prod_{p<z}\left(1-\frac{\varrho_{d,g}(p)}{p}\right)\{1+O(v^{-v/3})+O(\exp(-\sqrt{\log x}))\} \tag{51}$$

provided that $z\leqq x$, $z>z(g)$, and where $v=\log x/\log z$. Now it is clear, as in the proof of Theorem 1, that there exists a constant $D(g)$ such that

$$\varrho_{d,g}(p)=\sum_{i=1}^{k}\varrho_{i,d}(p) \tag{52}$$

provided that $p \nmid D(g)d$. Hence, recalling that $\varrho_{d,g}(p) \geqq 0$, from (51) and (52) we get

$$S_{g,k}(x,y,z) \ll x \sum_{\substack{d \leqq y \\ (d,P_2)=1 \\ d \notin R(\mathscr{P}_0')}} \prod_{i=1}^{k} \prod_{\substack{p<z \\ p \nmid D(g)d}} \left(1 - \frac{\varrho_{i,d}(p)}{p}\right) \tag{53}$$

$$\ll x \sum_{i=1}^{k} \sum_{d \leqq y} \prod_{\substack{p<z \\ p \nmid 2D(g)d}} \left(1 - \frac{\varrho_{i,d}(p)}{p}\right)^{k},$$

by the inequality of the means. In fact, as we shall see later, we need, for the case $k=2$, a more precise estimate than that provided by (53). Clearly, we may assume, by multiplying $D(g)$ by an appropriate constant factor if necessary, that

$$2P_1P_2 \mid D(g). \tag{54}$$

Recalling that $\varrho_{i,d}(p)$ counts, for each d, the number of solutions n of $a_i n^2 + b_i d \equiv 0 \pmod{p}$, it is easy to see that $\varrho_{i,d}(p)$ counts the number of solutions n of

$$a_i(a_i n^2 + b_i d) = (a_i n)^2 + a_i b_i d \equiv 0 \pmod{p},$$

or, equivalently, of

$$n^2 \equiv -a_i b_i d \pmod{p},$$

provided that $p \nmid D(g)d$. Hence each $\varrho_{i,d}$ is the ϱ-function associated, as in [6], with the quadratic field $\mathbb{Q}(\sqrt{-a_i b_i d})$. Arguing as in Lemma 2 of [6] we get

$$\prod_{\substack{p<z \\ p \nmid D(g)d}} \left(1 - \frac{\varrho_{i,d}(p)}{p}\right)^{k} = \prod_{p<z} \left(1 - \frac{\varrho_{i,d}(p)}{p}\right)^{k} \prod_{\substack{p<z \\ p \mid D(g)d}} \left(1 - \frac{\varrho_{i,d}(p)}{p}\right)^{-k} \tag{55}$$

$$\ll \prod_{\mathrm{N}_i\mathfrak{P}<z} \left(1 - \frac{1}{\mathrm{N}_i\mathfrak{P}}\right)^{k} E_{k,i}(d),$$

where

$$E_{k,i}(d) \ll \left(\frac{d}{\varphi(d)}\right)^{2k},$$

and $\mathrm{N}_i\mathfrak{P}$ denotes the norm of the prime ideal $\mathfrak{P}$ in the field $\mathbb{Q}(\sqrt{-a_i b_i d})$.

Now, following step 3 in the proof of Theorem 1 of [6], we obtain

$$\prod_{N_i \mathfrak{P} < z} \left(1 - \frac{1}{N_i \mathfrak{P}}\right)^k \ll (\log z)^{-k} L(1, \chi_i)^{-k}, \tag{56}$$

where $\chi_i = \chi_{i,d}$ is, as in [6], the appropriate character associated with $\mathbb{Q}(\sqrt{-a_i b_i d})$, provided that

$$z \gg y^6.$$

From (53)—(56) we get that

$$S_{g,k}(x, y, z) \ll \frac{x}{(\log z)^k} \sum_{i=1}^{k} \sum_{d \leqq y} E_{k,i}(d)\, L(1, \chi_i)^{-k},$$

provided that $z \gg y^6$. Using Corollary 2 of Theorem 1 we deduce that

$$\begin{aligned} S_{g,k}(x, y, z) &\ll \frac{x}{(\log z)^k} \sum_{i=1}^{k} \left(\sum_{d \leqq y} E_{k,i}(d)^2\right)^{\frac{1}{2}} \left(\sum_{d \leqq y} L(1, \chi_i)^{-2k}\right)^{\frac{1}{2}} \\ &\ll \frac{x}{(\log z)^k} \sum_{i=1}^{k} \left(\sum_{d \leqq y} \left(\frac{d}{\varphi(d)}\right)^{4k}\right)^{\frac{1}{2}} y^{\frac{1}{2}} \ll \frac{x y}{(\log z)^k}. \end{aligned} \tag{57}$$

In the remaining range $y < z \ll y^6$, we have from (48) that

$$S_{g,k}(x, y, z) \ll S_{g,k}(x, y, y) \ll \frac{x y}{(\log y)^k} \ll \frac{x y}{(\log z)^k}. \tag{58}$$

Theorem 4, with ineffective constants, now follows from (48), (57) and (58).

We note, in fact, that the ineffectiveness comes from the use of Corollary 2 of Theorem 1 in (57). For the case $k = 2$, the use of Cauchy's inequality in (57) has to be avoided sice the corresponding bound thus obtained for

$$\sum_{d \leqq y} L(1, \chi)^{-4}$$

is ineffective. This necessitates a closer examination of the proofs of Theorems 2 and 4. As in the proof of Theorem 4 (for $k \geqq 3$), all constants may depend on the polynomial g.

From now onwards, we assume that $k = 2$ so that

$$g_2(n, d) = (a_1 n^2 + b_1 d)(a_2 n^2 + b_2 d).$$

We begin by observing that 2 is the only prime which can belong to $\mathscr{P}_0$ and it is easy to see that a necessary condition for 2 to belong to $\mathscr{P}_0$ is that $b_1 b_2$ is odd. Hence $(P_0, P_1) = 1$ for all $g_2(n, d)$, and from (48) we get that

$$S_{g,2}(x, y, z) \ll \frac{xy}{(\log z)^2} \tag{59}$$

if $z \leqq y$.

We now follow the proof of Theorem 2 in order to obtain an upper bound for a suitable weighted sum of $L(1, \chi)^{-1}$'s. Choose $x = y$ and $z_0 = \exp(c\sqrt{\log y})$, $c > 0$ a suitable constant. Then from (51) we deduce that

$$S_{g,2}(y, y, z_0) \gg y \sum_{\substack{d \leqq y \\ (d, P_1)=1 \\ d \notin R(\mathscr{P}_0')}} \prod_{p < z_0} \left(1 - \frac{\varrho_{d,g}(p)}{p}\right). \tag{60}$$

Now we want to translate the product in (60) into a product involving suitable Dirichlet characters. We first note that, as in (52),

$$\varrho_{d,g}(p) = \varrho_{1,d}(p) + \varrho_{2,d}(p)$$

if $p \nmid 2 a_1 a_2 (b_1 a_2 - a_1 b_2) d$. Next, as in step 2 of Theorem 2 of [6], we have, since, as is easily seen, $\varrho_{i,d}(p) < p$, $i = 1, 2$, for all primes p and all d occurring in (60), that

$$\begin{aligned} \prod_{p < z_0} \left(1 - \frac{\varrho_{d,g}(p)}{p}\right) &= \prod_{\substack{p < z_0 \\ p \nmid F(g) d}} \left(1 - \frac{(\varrho_{1,d}(p) + \varrho_{2,d}(p))}{p}\right) \prod_{\substack{p < z_0 \\ p \mid F(g) d}} \left(1 - \frac{\varrho_{d,g}(p)}{p}\right) \\ &= \prod_{p < z_0} \left(1 - \frac{\varrho_{1,d}(p)}{p}\right) \prod_{p < z_0} \left(1 - \frac{\varrho_{2,d}(p)}{p}\right) G(d, g, z_0) \\ &= \prod_{p < z_0} \left(1 - \frac{1}{p}\right)^2 \prod_{p < z_0} \left(1 - \frac{\chi_1(p)}{p}\right) \prod_{p < z_0} \left(1 - \frac{\chi_2(p)}{p}\right) h_1(d, z_0)\, h_2(d, z_0)\, G(d, g, z_0), \end{aligned} \tag{61}$$

where

$$F(g) = 2 a_1 a_2 (b_1 a_2 - a_1 b_2), \quad \chi_i(p) = \left(\frac{-a_i b_i d}{p}\right), \quad i = 1, 2,$$

$$G(d, g, z) = \prod_{\substack{p < z \\ p \mid F(g) d}} \left(1 - \frac{\varrho_{d,g}(p)}{p}\right)\left(1 - \frac{(\varrho_{1,d}(p) + \varrho_{2,d}(p))}{p}\right)^{-1},$$

and $h_i(d, z)$, $i = 1, 2$, correspond to the function $c(d, z)$ in step 2 of Theorem 2 of [6], but associated with χ_i. Further, as in [6], defining

$$G(d, g) = \lim_{z \to \infty} G(d, g, z)$$

and

$$h_i(d) = \lim_{z \to \infty} h_i(d, z), \quad i = 1, 2,$$

we have that for $z \geqq z_0$,

$$h_1(d,z)\, h_2(d,z)\, G(d,g,z) = h_1(d)\, h_2(d)\, G(d,g)\, \{1 + O(\exp(-\sqrt{\log y}))\}. \tag{62}$$

From (59)—(62) we have that

$$\sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} h_1(d)\, h_2(d)\, G(d,g) \prod_{p<z_0} \left(1 - \frac{\chi_1(p)}{p}\right) \prod_{p<z_0} \left(1 - \frac{\chi_2(p)}{p}\right) \ll y. \tag{63}$$

Now we can use the arguments in step 3, Theorem 2 of [6], to convert the products over primes in (63) to $L(1,\chi_1)^{-1}\, L(1,\chi_2)^{-1}$ and then Tatuzawa's theorem as in step 4, Theorem 2 of [6], to obtain from (63) that

$$\sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} h_1(d)\, h_2(d)\, G(d,g)\, L(1,\chi_1)^{-1}\, L(1,\chi_2)^{-1} \ll y. \tag{64}$$

We are now in a position to complete the proof for the case $k=2$. From (51), (61), (64), Lemma 2 of [6] and step 3 of Theorem 1 of [6], we have, for $z \gg y^6$, that

$$\begin{aligned} S_{g,2}(x,y,z) &\ll x \sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} \prod_{p<z} \left(1 - \frac{\varrho_{d,g}(p)}{p}\right) \\ &\ll x \sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} G(d,g) \prod_{p<z} \left(1 - \frac{\varrho_{1,d}(p)}{p}\right)\left(1 - \frac{\varrho_{2,d}(p)}{p}\right) \\ &\ll x \prod_{p<z} \left(1 - \frac{1}{p}\right)^2 \sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} G(d,g)\, h_1(d)\, h_2(d) \prod_{i=1}^{2} \prod_{\mathrm{N}_i \mathfrak{P} < z} \left(1 - \frac{1}{\mathrm{N}_i \mathfrak{P}}\right) \\ &\ll \frac{x}{(\log z)^2} \sum_{\substack{d \leqq y \\ (d, P_2)=1 \\ d \notin R(\mathscr{P}_0')}} G(d,g)\, h_1(d)\, h_2(d)\, L(1,\chi_1)^{-1}\, L(1,\chi_2)^{-1} \ll \frac{xy}{(\log z)^2}. \end{aligned} \tag{65}$$

In the intermediate range $y < z \ll y^6$ we have, as usual, from (59) that

$$S_{g,2}(x,y,z) \ll S_{g,2}(x,y,y) \ll \frac{xy}{(\log y)^2} \ll \frac{xy}{(\log z)^2}. \tag{66}$$

Theorem 4, for $k=2$, now follows from (59), (65) and (66).

References

[1] *H. Davenport*, Multiplicative Number Theory, 2nd edition, Berlin-Heidelberg-New York 1980.
[2] *P. D. T. A. Elliott*, Probabilistic Number Theory II, Berlin-Heidelberg-New York 1980.
[3] *C. F. Gauss*, Disquisitiones Arithmeticae, English edition, Berlin-Heidelberg-New York 1986.
[4] *B. H. Gross, D. B. Zagier*, Heegner points and derivatives of L-series, Invent. Math. **84** (1986), 225—320.
[5] *H. Halberstam, H.-E. Richert*, Sieve Methods, London-New York-San Francisco 1974.
[6] *M. Nair, A. Pirelli*, Sieve methods and class-number problems. I, J. reine angew. Math. **367** (1986), 11—26.
[7] *T. Tatuzawa*, On a theorem of Siegel, Japanese J. Math. **21** (1951) 163—178.

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland (U.K.)

Dipartimento di Matematica, Università di Genova, Via L.B. Alberti 4, 16132 Genova, Italy

Eingegangen 29. Juni 1987