J. London Math. Soc. (2) 73 (2006) 415–435 © 2006 London Mathematical Society
doi:10.1112/S0024610706022629

THE PARITY PROBLEM FOR REDUCIBLE CUBIC FORMS

H. A. HELFGOTT

Abstract

Let $f \in \mathbb{Z}[x, y]$ be a reducible homogeneous polynomial of degree 3. We show that $f(x, y)$ has an even number of prime factors as often as an odd number of prime factors.

1. *Introduction*

The Liouville function $\lambda(n)$ is defined on the set of non-zero rational integers as follows:

$$\lambda(n) = \prod_{p \,|\, n} (-1)^{v_p(n)}. \tag{1.1}$$

We will find it convenient to choose a value for $\lambda(0)$; we adopt the convention that $\lambda(0) = 0$.

Let $f \in \mathbb{Z}[x, y]$ be a homogeneous polynomial not of the form $c \cdot g^2$, $c \in \mathbb{Z}$, $g \in \mathbb{Z}[x, y]$. Then, it is believed,

$$\lim_{N \to \infty} \frac{1}{N^2} \sum_{-N \leqslant x, y \leqslant N} \lambda(f(x, y)) = 0. \tag{1.2}$$

This conjecture can be traced to Chowla [**1**, p. 96]; it is closely related to the Bunyakovsky–Schinzel conjecture on primes represented by irreducible polynomials.

The one-variable analogue of (1.2) is classical for $\deg f = 1$ and quite hopeless for $\deg f > 1$. We know (1.2) itself when $\deg f \leqslant 2$. (The main ideas of the proof go back to de la Vallée-Poussin [**3**, **4**]; see [**6**, § 3.3] for an exposition.) The problem of proving (1.2) when $\deg f \geqslant 3$ has remained open until now: sieving is forestalled by the parity problem [**18**], which Chowla's conjecture may be said to embody in its pure form.

We prove (1.2) for f reducible of degree 3. In a companion paper [**9**], we prove (1.2) for f irreducible of degree 3.

Part of the importance of Chowla's conjecture resides in its applications to problems of parity outside analytic number theory. Knowing that (1.2) holds for $\deg f = 3$ allows us to conclude that in certain one-parameter families of elliptic curves the root number $W(E) = \pm 1$ averages to 0 (see [**8**, Proposition 5.6]). In § 5, we will show that the two-parameter family $y^2 = x(x + a)(x + b)$ has average root number 0 as well. In the process, we will see that, for some f, (1.2) is robust under certain twists by characters to variable moduli.

Received 10 August 2004; revised 26 September 2005.

2000 *Mathematics Subject Classification* 11N32 (primary), 11N35, 11N36 (secondary).

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

2. *Preliminaries*

2.1. *Anti-sieving*

In the next two lemmas we use an upper-bound sieve not to find almost-primes, but to split the integers multiplicatively, with the almost-primes as an error term. A treatment by means of a cognate of Vaughan's identity would also be possible, but much more cumbersome. The error term would be the same.

LEMMA 2.1. *Let $\mathcal{P} \subset \{M_1, M_1+1, \dots, M_2-1\}$ be a set of primes between the positive integers M_1 and M_2. Then there are $\sigma_d \in \mathbb{R}$ with $|\sigma_d| \leqslant 1$ and support on*

$$\{M_1 \leqslant d < M_2 : p \mid d \Rightarrow p \in \mathcal{P}\}$$

such that for any a, m, N_1 and N_2 with $0 < m < M_1$ and $N_2 \geqslant N_1$,

$$\sum_{\substack{N_1 \leqslant n < N_2 \\ n \equiv a \bmod m}} \left|1 - \sum_{d \mid n} \sigma_d\right| \ll \prod_{\substack{M_1 \leqslant p < M_2 \\ p \notin \mathcal{P}}} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{\log M_1}{\log M_2} \frac{N_2 - N_1}{m} + M_2,$$

where the implied constant is absolute.

Proof. We shall follow the nomenclature in [**12**, p. 159]. We let

$$\kappa = 1, \quad y = M_2, \quad g(d) = \begin{cases} 1/d & \text{if } p \mid d \Rightarrow p \in \mathcal{P}, \\ 0 & \text{otherwise.} \end{cases}$$

Then, by [**12**, Fundamental Lemma 6.3], there is a sequence of real numbers (λ_d^+) such that

$$\lambda_d^+ = 1, \quad |\lambda_d^+| \leqslant 1 \text{ for all } d, \quad \lambda_d^+ = 0 \text{ if } d \geqslant y, \quad \sum_{d \mid n} \lambda_d^+ \geqslant 0 \text{ for every } n$$

and

$$\sum_{d \mid P(z)} \lambda_d^+ g(d) \ll \prod_{p < z} (1 - g(p)), \tag{2.1}$$

where $z = M_2$ and $P(z) = \prod_{p<z} p$. Note now that

$$\prod_{p<z} (1 - g(p)) \ll \frac{\log M_1}{\log M_2} \prod_{M_1 \leqslant p < M_2 : p \notin \mathcal{P}} (1 - 1/p)^{-1}.$$

Hence

$$\begin{aligned} \sum_{\substack{N_1 \leqslant n < N_2 \\ n \equiv a \bmod m}} \sum_{\substack{d \mid n \\ p \mid d \Rightarrow p \in \mathcal{P}}} \lambda_d^+ &= \sum_{\substack{d \\ p \mid d \Rightarrow p \in \mathcal{P}}} \lambda_d^+ \cdot \left(\frac{N_2 - N_1}{md} + O(1)\right) \\ &= \frac{N_2 - N_1}{m} \sum_{d \mid P(z)} \lambda_d^+ g(d) + \sum_{\substack{d \\ p \mid d \Rightarrow p \in \mathcal{P}}} O(\lambda_d^+) \\ &\ll \prod_{\substack{M_1 \leqslant p < M_2 \\ p \notin \mathcal{P}}} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{\log M_1}{\log M_2} \frac{N_2 - N_1}{m} + M_2, \end{aligned}$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

where all implied constants are absolute. We set

$$\sigma_1 = 0, \quad \sigma_d = \begin{cases} -\lambda_d^+ & \text{if } p \mid d \Rightarrow p \in \mathcal{P}, \\ 0 & \text{otherwise,} \end{cases} \quad \text{for } d \neq 1.$$

Since $\sum_{d \mid n} \lambda_d^+ \geqslant 0$ for every n, we are done. □

REMARK. Fundamental Lemma 6.3 in [**12**] employs the Rosser–Iwaniec sieve, and thus gives an optimized bound for the constant in (2.1). As any constant would do for our purposes, we could use somewhat weaker results, such as Brun's 1920 sieve [**5**, § 3.4]. All the same, we are using – and need – a result different from some that go by the name of 'fundamental lemma' in the older literature: we are not assuming that $\log M_2 = o(\log N)$, and we are not requiring asymptotics.

LEMMA 2.2. *Let $K/\mathbb{Q}$ be a number field. Let $\jmath : K \to \mathbb{R}^{\deg(K/\mathbb{Q})}$ be a bijective $\mathbb{Q}$-linear map taking $\mathcal{O}_K$ to $\mathbb{Z}^{\deg(K/\mathbb{Q})}$. Let $\mathcal{P}$ be a set of prime ideals of K whose norms lie between the positive integers M_1 and M_2. Then there are $\sigma_{\mathfrak{d}} \in \mathbb{R}$ with $|\sigma_{\mathfrak{d}}| \leqslant 1$ and support on*

$$\{\mathfrak{d} : M_1 \leqslant N\mathfrak{d} < M_2, \mathfrak{p} \mid \mathfrak{d} \Rightarrow \mathfrak{p} \in \mathcal{P}\} \tag{2.2}$$

such that for any positive integer N, any lattice coset $L \subset \mathbb{Z}^{\deg(K/\mathbb{Q})}$ with index $[\mathbb{Z}^{\deg(K/\mathbb{Q})} : L] < M_1$ and any convex set $S \subset [-N, N]^{\deg(K/\mathbb{Q})}$,

$$\sum_{\jmath(x) \in S \cap L} \left| 1 - \sum_{\mathfrak{d} \mid x} \sigma_{\mathfrak{d}} \right| \ll \prod_{\substack{M_1 \leqslant p < M_2 \\ p \notin \mathcal{P}}} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{\log M_1}{\log M_2} \frac{\operatorname{Area}(S)}{[\mathcal{O}_K : L]} + N^{\deg(K/\mathbb{Q})-1} M_2^2,$$

where the implied constant depends only on K.

Proof. Set $\lambda_{\mathfrak{d}}^+$ as in a generalized Rosser–Iwaniec sieve [**2**] with sieving set $\mathcal{P}$ and upper cut $z = M_2$. Proceed as in the proof of Lemma 2.1. Set $\sigma_{(1)} = 0$, $\sigma_{\mathfrak{d}} = -\lambda_{\mathfrak{d}}^+$ for $\mathfrak{d} \neq (1)$. □

2.2. *Extensions of the Liouville function*

We define λ on $\mathbb{Q}$ by

$$\lambda\left(\frac{n_0}{n_1}\right) = \frac{\lambda(n_0)}{\lambda(n_1)} \tag{2.3}$$

and on ideals in a Galois extension $K/\mathbb{Q}$ of degree n by

$$\lambda(\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_k^{e_k}) = \prod_i \omega^{f(\mathfrak{p}_i) \cdot e_i}, \tag{2.4}$$

where ω is a fixed $(2n)$th root of unity and $f(\mathfrak{p}_i)$ is the degree of inertia of $\mathfrak{p}_i$ over $\mathfrak{p}_i \cap \mathbb{Q}$. Notice that (2.4) restricts to (2.3), which, in turn, restricts to (1.1). Note also that the above *extension* is different from the natural *generalization* λ_K:

$$\lambda_K(\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_k^{e_k}) = \prod_i (-1)^{e_i}. \tag{2.5}$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

2.3. *Quadratic forms*

We will consider only quadratic forms $ax^2 + bxy + cy^2$ with integer coefficients $a, b, c \in \mathbb{Z}$. A quadratic form $ax^2 + bxy + cy^2$ is *primitive* if $\gcd(a, b, c) = 1$.

Let n be a rational integer. We denote by $\mathrm{sq}(n)$ the largest positive integer whose square divides n. Define

$$d_n = \begin{cases} \mathrm{sq}(n) & \text{if } 4 \nmid n, \\ \mathrm{sq}(n)/2 & \text{if } 4 \mid n. \end{cases}$$

LEMMA 2.3. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a primitive, irreducible quadratic form. Let $K = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Then there are algebraic integers $\alpha_1, \alpha_2 \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$ such that*

$$Q(x, y) = \frac{N(x\alpha_1 + y\alpha_2)}{a}$$

for all $x, y \in \mathbb{Z}$. The subgroup $\mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ of $\mathcal{O}_K$ has index $[\mathcal{O}_K : \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2] = d_{b^2-4ac}$.

Proof. Set $\alpha_1 = a$, $\alpha_2 = b + \sqrt{b^2 - 4ac}/2$. □

2.4. *Lattices and convex sets*

A *lattice* is a subgroup of $\mathbb{Z}^n$ of finite index; a *lattice coset* is a coset of such a subgroup. By the *index* of a lattice coset we mean the index of the lattice of which it is a coset. For any lattice cosets L_1, L_2 with $\gcd([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) = 1$, the intersection $L_1 \cap L_2$ is a lattice coset with

$$[\mathbb{Z}^n : L_1 \cap L_2] = [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \tag{2.6}$$

In general, if L_1, L_2 are lattice cosets, then $L_1 \cap L_2$ is either the empty set or a lattice coset such that

$$\mathrm{lcm}([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) \mid [\mathbb{Z}^n : L_1 \cap L_2], \quad [\mathbb{Z}^n : L_1 \cap L_2] \mid [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \tag{2.7}$$

Since $\mathbb{Z}^n/L_j$ $(j = 1, 2)$ is a quotient of $\mathbb{Z}^n/(L_1 \cap L_2)$, we must have $[\mathbb{Z}^n : L_j] | [\mathbb{Z}^n : L_1 \cap L_2]$. The first property in (2.7) follows. Two distinct elements of $\mathbb{Z}^n/(L_1 \cap L_2)$ cannot be congruent modulo both L_1 and L_2. Thus, the natural map $\mathbb{Z}^n/(L_1 \cap L_2) \mapsto \mathbb{Z}^n/L_1 \times \mathbb{Z}^n/L_2$ must be injective. The second property in (2.7) follows.

For $S \subset [-N, N]^n$ a convex set and $L \subset \mathbb{Z}^n$ a lattice coset,

$$\#(S \cap L) = \frac{\mathrm{Area}(S)}{[\mathbb{Z}^n : L]} + O(N^{n-1}), \tag{2.8}$$

where the implied constant depends only on n. One can prove (2.8) easily: slice S and L by hyperplanes and use induction on n.

2.5. *Linear bounds*

Landau showed [**13**] that there is an effective constant $c > 0$ such that, for every $k \geqslant 0$, there is at most one primitive character χ of modulus $q \in \{2^{2^k}, 2^{2^k} + 1, \ldots, 2^{2^{k+1}} - 1\}$ such that $L(s, \chi)$ has an exceptional ('Siegel') zero $\beta > 1 - c/\log q$. We call such a modulus q *exceptional*. By Siegel's methods (see [**19**] and also

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

[**16**, pp. 74–75]), it follows that

$$\left| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod m}} \lambda(n) \right| \ll x e^{-C\sqrt{\log x}} \tag{2.9}$$

for any $x \geqslant 1$ and any a, m such that $\gcd(a, m) = 1$ and $q \nmid m$ for every exceptional modulus q larger than $(\log x)^A$. Both $C > 0$ and the implied constant depend on A. The dependence is ineffective.

Zero-density results on L-functions, together with the standard zero-free regions and bounds on $|\log L(s, \chi)|$, yield rather general results on the sum of Λ, μ, λ and the like over arithmetic progressions in short intervals. If we take as inputs the zero-density results in [**10**, (1.1)] and [**15**, Theorem 3.2], and the zero-free region in [**11**, Theorem 2], then the procedure in [**17**] yields

$$\left| \sum_{\substack{x < n \leqslant x+h \\ n \equiv a \bmod m}} \lambda(n) \right| \ll h \exp\left[-C \frac{(\log x)^{1/4}}{(\log\log x)^{3/4}} \right] + x^{\frac{7}{12}+\epsilon} \tag{2.10}$$

for any $x \geqslant 1$ and any a, m such that $\gcd(a, m) = 1$ and $q \nmid m$ for every exceptional modulus q larger than $(\log x)^A$. Both $C > 0$ and the implied constant depend on A and ϵ. The dependence is ineffective.

Neither (2.9) nor (2.10) give the best upper bounds that could conceivably be given nowadays; the zero-free region in [**11**] can be used to improve the exponent $-C\sqrt{\log x}$ in (2.9) to $-C(\log x)^{4/7}/(\log\log x)^{3/7}$, provided that the modulus m is at most $(\log x)^{3/7}(\log\log x)^{3/7}$. In fact, it seems reasonable to hope that, given current technology, one might be able to sharpen the result in [**11**] to give a zero-free region for Dirichlet L-functions almost as broad as the Korobov–Vinogradov region for the zeta function, though there is a gap in the literature at this point. If we could prove the existence of such a zero-free region, we could improve the exponent in (2.9) to $-C(\log x)^{3/5-\epsilon}$ and the exponent in (2.10) to $-C(\log x)^{1/3-\epsilon}$. Both (2.9) and (2.10), however, are already stronger than what we need; in particular, Ingham's $\frac{5}{8}$ or Hoheisel's $1 - \delta$, $\delta > 0$, would do in place of Huxley's $\frac{7}{12}$. We will certainly do without any hypothetical refinements of existing results.

The proof of Theorem 3.3 does not require the distinction between exceptional and non-exceptional moduli to be made in the application of (2.10), since the modulus q will always be smaller than $(\log x)^A$ for some constant A. Short-interval estimates will not be needed in the proofs of Theorem 4.2 or Proposition 5.1. One may avoid the use of short-interval estimates altogether by setting $M_2 = e^{\epsilon\sqrt{\log N}}$ in the proof of Theorem 3.3 and proceeding as in the proof of Proposition 5.1, at the cost of replacing the factor of $(\log\log N)/\log N$ in the statement of the theorem by a factor of $(\log\log N)/\sqrt{\log N}$; alternatively, one may prove Theorem 3.3 as we prove Theorem 4.2, namely, via the Bombieri–Vinogradov theorem, and thus keep the bound we now have in the statement of Theorem 3.3.

2.6. *Bilinear bounds*

We shall need bounds for bilinear sums involving the Liouville function. For §§ 3 and 5, the following lemma will suffice. It is simply a linear bound in disguise.

LEMMA 2.4. *Let S be a convex subset of $[-N, N]^2$. Let $L \subset \mathbb{Z}^2$ be a lattice coset of index $[\mathbb{Z}^2 : L]$ not divisible by any exceptional moduli larger than $(\log N)^A$.*

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

Let $f : \mathbb{Z} \to \mathbb{C}$ be a function with $\max_y |f(y)| \leqslant 1$. Then, for every $\epsilon > 0$,

$$\left| \sum_{(x,y) \in S \cap L} \lambda(x) f(y) \right| \ll \mathrm{Area}(S) \cdot \exp\left[-C \frac{(\log N)^{1/4}}{(\log\log N)^{3/4}} \right] + N^{\frac{19}{12}+\epsilon}, \tag{2.11}$$

where C and the implied constant in (2.11) *depend only on A and ϵ.*

Proof. For every $y \in \mathbb{Z} \cap [-N, N]$, the set $\{x : (x, y) \in L\}$ is either the empty set or an arithmetic progression $m_y \mathbb{Z} + a_y$, where $m_y | [\mathbb{Z}^2 : L]$. Let y_0 and y_1 be the least and the greatest $y \in \mathbb{Z} \cap [-N, N]$ such that $\{x : (x, y) \in S\}$ is non-empty. Let $y \in \mathbb{Z} \cap [y_0, y_1]$. Since S is convex and a subset of $[-N, N]^2$, the set $\{x : (x, y) \in S\}$ is an interval $[N_{y,0}, N_{y,1}]$ contained in $[-N, N]$. Hence

$$\begin{aligned} \left| \sum_{(x,y) \in S \cap L} \lambda(x) f(y) \right| &= \left| \sum_{\substack{y_0 \leqslant y \leqslant y_1 \\ \{x : (x,y) \in L\} \neq \emptyset}} \sum_{\substack{N_{y,0} \leqslant x \leqslant N_{y,1} \\ x \equiv a_y \bmod m_y}} \lambda(x) f(y) \right| \\ &\leqslant \sum_{\substack{y_0 \leqslant y \leqslant y_1 \\ \{x : (x,y) \in L\} \neq \emptyset}} \left| \sum_{\substack{N_{y,0} \leqslant x \leqslant N_{y,1} \\ x \equiv a_y \bmod m_y}} \lambda(x) \right|. \end{aligned}$$

By (2.9) and (2.10),

$$\begin{aligned} &\sum_{\substack{y_0 \leqslant y \leqslant y_1 \\ \{x : (x,y) \in L\} \neq \emptyset}} \left| \sum_{\substack{N_{y,0} \leqslant x \leqslant N_{y,1} \\ x \equiv a_y \bmod m_y}} \lambda(x) \right| \\ &\quad \ll \sum_{y_0 \leqslant y \leqslant y_1} (N_{y_1} - N_{y_0}) \exp\left[-C \frac{(\log N)^{1/4}}{(\log\log N)^{3/4}} \right] + N^{\frac{19}{12}+\epsilon} \end{aligned}$$

for any $\epsilon > 0$. Clearly

$$\mathrm{Area}(S) = \sum_{y=y_0}^{y_1} (N_{y,1} - N_{y,0}) + O(N).$$

Therefore

$$\left| \sum_{(x,y) \in S \cap L} \lambda(x) f(y) \right| \ll \mathrm{Area}(S) \cdot \exp\left[-C \frac{(\log N)^{1/4}}{(\log\log N)^{3/4}} \right] + N^{\frac{19}{12}+\epsilon}.$$

This completes the proof. □

By an easy modification of the proof in [**12**, § 17.3] (or by, say, [**14**, Theorem 1]), we have the following analogue of Bombieri–Vinogradov:

$$\sum_{m \leqslant \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{\substack{a \\ (a,m)=1}} \max_{x \leqslant N} \left| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod m}} \lambda(n) - \frac{1}{\phi(m)} \sum_{\substack{n \leqslant x \\ \gcd(n,m)=1}} \lambda(n) \right| \ll \frac{N}{(\log N)^A}, \tag{2.12}$$

where the implied constant depends only on A.

A simpler statement is true.

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

LEMMA 2.5. *For any $A > 0$,*

$$\sum_{m \leqslant \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_a \max_{x \leqslant N} \Big| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod m}} \lambda(n) \Big| \ll \frac{N}{(\log N)^A},$$

where the implied constant depends only on A.

Proof. Write $\mathrm{rad}(m) = \prod_{p \mid m} p$. Then

$$\sum_{d \mid \gcd(\mathrm{rad}(m), n)} \lambda(n/d) = \begin{cases} \lambda(n) & \text{if } \gcd(m,n) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned}
\sum_{m \leqslant N^{1/2}} \frac{1}{\phi(m)} \max_{x \leqslant N} \Big| \sum_{\substack{n \leqslant x \\ \gcd(n,m)=1}} \lambda(n) \Big| &= \sum_{m \leqslant N^{1/2}} \frac{1}{\phi(m)} \max_{x \leqslant N} \Big| \sum_{d \mid \mathrm{rad}(m)} \sum_{\substack{n \leqslant x \\ d \mid n}} \lambda(n/d) \Big| \\
&\leqslant \sum_{m \leqslant N^{1/2}} \frac{1}{\phi(m)} \sum_{d \mid \mathrm{rad}(m)} \max_{x \leqslant N/d} \Big| \sum_{n \leqslant x} \lambda(n) \Big| \\
&\ll \sum_{m \leqslant N^{1/2}} \frac{1}{\phi(m)} \sum_{d \mid \mathrm{rad}(m)} N/d \cdot e^{-C\sqrt{\log N/d}} \\
&\leqslant N e^{-C\sqrt{\log N^{1/2}}} \sum_{m \leqslant N^{1/2}} \frac{1}{\phi(m)} \sum_{d \mid \mathrm{rad}(m)} \frac{1}{d} \\
&\ll \frac{N}{(\log N)^A}.
\end{aligned}$$

By (2.12) this implies

$$\sum_{m \leqslant \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{\substack{a \\ \gcd(a,m)=1}} \max_{x \leqslant N} \Big| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod m}} \lambda(n) \Big| \ll \frac{N}{(\log N)^A}.$$

Now

$$\begin{aligned}
&\sum_{m \leqslant \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_a \max_{x \leqslant N} \Big| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod m}} \lambda(n) \Big| \\
&\quad = \sum_{m \leqslant \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{r \mid m} \max_{\gcd(a,m)=1} \max_{x \leqslant N} \Big| \sum_{\substack{n \leqslant x \\ n \equiv ar \bmod m}} \lambda(n) \Big| \\
&\quad < \sum_{r \leqslant N^{1/2}} \sum_{s \leqslant \frac{(N/r)^{1/2}}{(\log(N/r))^{2A+6}}} \max_{\gcd(a,s)=1} \max_{x \leqslant N/r} \Big| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod s}} \lambda(n) \Big| \\
&\quad \ll \sum_{r \leqslant N^{1/2}} \frac{N/r}{(\log N/r)^{A+1}} \ll \frac{N}{(\log N)^A}.
\end{aligned}$$

The proof is complete. □

The following lemma is to Lemma 2.4 what Bombieri–Vinogradov is to (2.9).

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

LEMMA 2.6. *Let A, K and N be positive and satisfy $K \leqslant \sqrt{N}/(\log N)^{2A+6}$. For $j = 1, 2, \dots, K$, let S_j be a convex subset of $[-N, N]^2$ and let $L_j \subset \mathbb{Z}^2$ be a lattice coset of index j. Let $f : \mathbb{Z} \to \mathbb{C}$ be a function with $\max_y |f(y)| \leqslant 1$. Then*

$$\sum_{j=1}^{K} \left| \sum_{(x,y) \in S_j \cap L_j} \lambda(x) f(y) \right| \ll \frac{N^2}{(\log N)^A},$$

where the implicit constant depends only on A.

Proof. We start with

$$\begin{aligned} \sum_{j=1}^{K} \left| \sum_{(x,y) \in S_j \cap L_j} \lambda(x) f(y) \right| &\leqslant \sum_{j=1}^{K} \sum_{y} \left| \sum_{\substack{x \\ (x,y) \in S_j \cap L_j}} \lambda(x) \right| \\ &= \sum_{j=1}^{K} \sum_{k=0}^{\lceil N/j \rceil} \sum_{y=kj}^{(k+1)j-1} \left| \sum_{\substack{x \\ (x,y) \in S_j \cap L_j}} \lambda(x) \right|. \end{aligned}$$

For any $y \in \mathbb{Z}$, the set $\{x : (x, y) \in L_j\}$ is either the empty set or an arithmetic progression of modulus $m_j | j$ independent of y. Thus the set

$$A_j = \{(x, y) \in L_j : kj \leqslant y \leqslant (k+1)j - 1\}$$

is the union of m_j sets of the form

$$B_{y_0,a} = \{(x, y) \in \mathbb{Z}^2 : x \equiv a \bmod m_j,\ y = y_0\}$$

with $kj \leqslant y_0 \leqslant (k+1)j - 1$. Since an arithmetic progression of modulus d is the union of j/d arithmetic progressions of modulus j, the set A_j is the union of j sets of the form

$$C_{x_0,a} = \{(x, y) \in \mathbb{Z}^2 : x \equiv a \bmod j,\ y = y_0\}.$$

Therefore

$$\begin{aligned} \sum_{j=1}^{K} \sum_{k=0}^{\lceil N/j \rceil} \sum_{y=kj}^{(k+1)j-1} \left| \sum_{\substack{x \\ (x,y) \in S_j \cap L_j}} \lambda(x) \right| &\leqslant \sum_{j=1}^{K} \sum_{k=0}^{\lceil N/j \rceil} \sum_{l=1}^{j} \left| \sum_{\substack{x \\ (x, y_0(k,l)) \in S_j \cap C_{y_0(k,l),a(k,l)}}} \lambda(x) \right| \\ &\leqslant \sum_{j=1}^{K} (N+j) \max_{y_0} \max_{a} \left| \sum_{\substack{x \\ (x,y_0) \in S \cap C_{y_0,a}}} \lambda(x) \right| \\ &\leqslant \sum_{j=1}^{K} (N+j) \max_{-N \leqslant b \leqslant c \leqslant N} \max_{a} \left| \sum_{\substack{b \leqslant x \leqslant c \\ x \equiv a \bmod j}} \lambda(x) \right| \\ &\leqslant \sum_{j=1}^{K} 4(N+j) \max_{0 < c \leqslant N} \max_{a} \left| \sum_{\substack{0 < x \leqslant c \\ x \equiv a \bmod j}} \lambda(x) \right|. \end{aligned}$$

We apply Lemma 2.5 and are done. □

COROLLARY 2.7. *Let A, K, N, d_0 and d_1 be positive integers such that Kd_1 is no larger than $N^{1/2}/(\log N)^{2A+6}$. For $k = 1, 2, \dots, K$, let S_k be a convex subset of $[-N, N]^2$ and let $L_k \subset \mathbb{Z}^2$ be a lattice coset of index $(r_k/d_0)k$ for some r_k*

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

dividing d_0d_1. Then

$$\sum_{k\leqslant K}\left|\sum_{(x,y)\in S_k\cap L_k}\lambda(x)\lambda(y)\right| \ll \tau(d_0d_1)\cdot\frac{N^2}{(\log N)^A},$$

where the implicit constant depends only on A.

Proof. For every $j\leqslant Kd_1$, there are at most $\tau(d_0d_1)$ lattice cosets L_k of index j. There are no lattice cosets R_k of index greater than Kd_1. The statement then follows from Lemma 2.6. □

3. *The average of λ on the product of three linear factors*

LEMMA 3.1. *Let $\mathcal{P}\subset\{M_1, M_1+1,\dots,M_2-1\}$ be a set of primes between the positive integers M_1 and M_2. Then there are $\sigma_d\in\mathbb{R}$ with $|\sigma_d|\leqslant 1$ and support on*

$$\{M_1\leqslant d<M_2 : p\mid d\Rightarrow p\in\mathcal{P}\}$$

such that

$$\sum_{(x,y)\in S\cap L} g(x)f(x,y) = \sum_{\substack{a\\(ab,c)\in S\cap L}}\sum_{b}\sum_{c}\sigma_a\, g(a)g(b)f(ab,c) + O\Bigg(\prod_{\substack{M_1\leqslant p<M_2\\p\notin\mathcal{P}}}\left(1-\frac{1}{p}\right)^{-1}\cdot\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+NM_2\Bigg)$$

for any positive integer $N>M_2$, any convex set $S\subset[-N,N]^2$, any lattice coset $L\subset\mathbb{Z}^2$ with index $[\mathbb{Z}^2:L]<M_1$, any function $f:\mathbb{Z}^2\to\mathbb{C}$ and any completely multiplicative function $g:\mathbb{Z}^2\to\mathbb{C}$ with

$$\max_{x,y}|f(x,y)|\leqslant 1,\quad \max_{y}|g(y)|\leqslant 1.$$

The implied constant is absolute.

Proof. Let $y_1=\min(\{y\in\mathbb{Z} : \exists\, x \text{ such that } (x,y)\in S\cap L\})$. There is an $l|[\mathbb{Z}^2:L]$ such that, for any $y\in\mathbb{Z}$,

$$(\exists\, x \text{ such that } (x,y)\in L) \iff (l|y-y_1).$$

Let

$$N_{j,0}=\min(\{x : (x,y_1+jl)\in S\cap L\}),$$
$$N_{j,1}=\max(\{x : (x,y_1+jl)\in S\cap L\})+1.$$

Now take σ_d as in Lemma 2.1. Then

$$\sum_{x:(x,y_1+jl)\in S\cap L}\left|1-\sum_{d\mid x}\sigma_d\right| \ll \prod_{\substack{M_1\leqslant p<M_2\\p\notin\mathcal{P}}}\left(1-\frac{1}{p}\right)^{-1}\cdot\frac{\log M_1}{\log M_2}\frac{N_{j,1}-N_{j,0}}{[\mathbb{Z}^2:L]/l}+M_2.$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

Summing this over all j we obtain

$$\sum_{(x,y)\in S\cap L}\left|1-\sum_{d\,|\,x}\sigma_d\right| \ll \prod_{\substack{M_1\leqslant p<M_2\\ p\notin\mathcal{P}}}\left(1-\frac{1}{p}\right)^{-1}\cdot\frac{\log M_1}{\log M_2}\frac{(\mathrm{Area}(S))/l}{[\mathbb{Z}^2:L]/l}+M_2N$$
$$\ll \prod_{\substack{M_1\leqslant p<M_2\\ p\notin\mathcal{P}}}\left(1-\frac{1}{p}\right)^{-1}\cdot\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+M_2N.$$

Since

$$\left|\sum_{(x,y)\in S\cap L} g(x)f(x,y)-\sum_{(x,y)\in S\cap L}\sum_{d\,|\,x}\sigma_d g(x)f(x,y)\right|$$

is at most

$$\sum_{(x,y)\in S\cap L}\left|g(x)f(x,y)-\sum_{d\,|\,x}\sigma_d g(x)f(x,y)\right| \leqslant \sum_{(x,y)\in S\cap L}\left|1-\sum_{d\,|\,x}\sigma_d\right|$$

and

$$\sum_{\substack{a\\(ab,c)\in S\cap L}}\sum_{b}\sum_{c}\sigma_a\, g(a)g(b)f(ab,c)=\sum_{(x,y)\in S\cap L}\sum_{d\,|\,x}\sigma_d g(x)f(x,y),$$

we are done. □

Lemma 3.2. *Let c_1, c_2 be integers. Let $L\subset\mathbb{Z}^2$ be a lattice. Then the set $\{(a,b)\in\mathbb{Z}^2:(a,bc_1),(a,bc_2)\in L\}$ is either the empty set or a lattice coset $L'\subset\mathbb{Z}^2$ of index dividing $[\mathbb{Z}^2:L]^2$.*

Proof. The set of all elements of L of the form (a,bc_1) is the intersection of a lattice coset of index $[\mathbb{Z}^2:L]$ and a lattice of index c_1. By (2.7) it is either the empty set or a lattice coset of index dividing $c_1[\mathbb{Z}^2:L]$. Therefore the set of all (a,b) such that (a,bc_1) is in L is either the empty set or a lattice coset L_1 of index dividing $(1/c_1)c_1[\mathbb{Z}^2:L]=[\mathbb{Z}^2:L]$. Similarly, the set of all (a,b) such that $(a,bc_2)\in L$ is either the empty set or a lattice coset L_2 of index dividing $[\mathbb{Z}^2:L]$. Therefore $L'=L_1\cap L_2$ is either the empty set or a lattice coset of index dividing $[\mathbb{Z}^2:L]^2$. □

Definition 1. For

$$A=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\\a_{31}&a_{32}\end{pmatrix}$$

we denote

$$A_{12}=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix},\quad A_{13}=\begin{pmatrix}a_{11}&a_{12}\\a_{31}&a_{32}\end{pmatrix},\quad A_{23}=\begin{pmatrix}a_{21}&a_{22}\\a_{31}&a_{32}\end{pmatrix}.$$

Theorem 3.3. *Let S be a convex subset of $[-N,N]^2$, $N>1$. Let $L\subset\mathbb{Z}^2$ be a lattice coset. Let a_{11}, a_{12}, a_{21}, a_{22}, a_{31}, a_{32} be rational integers. Then*

$$\sum_{(x,y)\in S\cap L}\lambda((a_{11}x+a_{12}y)(a_{21}x+a_{22}y)(a_{31}x+a_{32}y))\ll\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+\frac{N^2}{(\log N)^\alpha}$$

for any $\alpha>0$. The implied constant depends only on (a_{ij}) and α.

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

Proof. We can assume that A_{12} is non-singular, as otherwise the statement follows immediately from Lemma 2.4. Changing variables we obtain

$$\begin{aligned}\sum_{(x,y)\in S\cap L} &\lambda(a_{11}x+a_{12}y)\lambda(a_{21}x+a_{22}y)\lambda(a_{31}x+a_{32}y)\\ &= \sum_{(x,y)\in A_{12}S\cap A_{12}L} \lambda(x)\lambda(y)\lambda\left((a_{31}\,a_{32})A_{12}^{-1}\begin{pmatrix}x\\y\end{pmatrix}\right)\\ &= \sum_{(x,y)\in A_{12}S\cap A_{12}L} \lambda(x)\lambda(y)\lambda(q_1x+q_2y),\end{aligned}$$

where

$$q_1 = -\frac{\det(A_{23})}{\det(A_{12})} \quad\text{and}\quad q_2 = \frac{\det(A_{13})}{\det(A_{12})}.$$

Note that q_1x+q_2y is an integer for all (x,y) in $A_{12}L$. We can assume that neither q_1 nor q_2 is zero. Write $S' = A_{12}S$, $L' = A_{12}L$. Clearly $S' \subset [-N', N']^2$ for $N' = \max(|a_{11}|+|a_{12}|, |a_{21}|+|a_{22}|)N$.

Now let

$$M_1 = (\log N')^{2\alpha+2}, \quad M_2 = (N')^{\beta},$$

where $\alpha > 0$ and $\beta \in (0, 1/2)$ will be set later. Clearly $M_2 > M_1$ for $N > N_0$, where N_0 depends only on (a_{ij}), α and β.

By Lemma 3.1 with $\mathcal{P} = \{M_1 \leqslant p < M_2 : p \text{ prime}\}$,

$$\begin{aligned}\sum_{(x,y)\in S'\cap L'} \lambda(x)\lambda(y)\lambda(q_1x+q_2y) = \sum_{\substack{a\\(ab,c)\in S'\cap L'}}\sum_{b}\sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c)\\ + O\left(\frac{\log M_1}{\log M_2}\frac{\operatorname{Area}(S')}{[\mathbb{Z}^2:L']} + N'M_2\right).\end{aligned}$$

We need to split the domain:

$$\sum_{\substack{a\\(ab,c)\in S'\cap L'}}\sum_{b}\sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c) = \sum_{s=1}^{\lceil M_2/M_1\rceil} T_s,$$

where

$$T_s = \sum_{a=sM_1}^{(s+1)M_1-1} \sum_{\substack{|b|\leqslant N'/sM_1\\(ab,c)\in S'\cap L'}} \sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c).$$

By Cauchy's inequality,

$$T_s^2 \leqslant \frac{(N')^2}{sM_1}\sum_{c}\sum_{|b|\leqslant N'/sM_1}\left(\sum_{\substack{sM_1\leqslant a<(s+1)M_1\\(ab,c)\in S'\cap L'}} \sigma_a\lambda(a)\lambda(q_1ab+q_2c)\right)^2.$$

Expanding the square and changing the order of summation, we get

$$\frac{(N')^2}{sM_1}\sum_{sM_1\leqslant a_1,a_2<(s+1)M_1} \sigma_{a_1}\sigma_{a_2}\lambda(a_1a_2)\sum_{\substack{c\\(a_ib,c)\in S'\cap L'}}\sum_{|b|\leqslant N'/sM_1} \lambda(q_1a_1b+q_2c)\lambda(q_1a_2b+q_2c).$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

There are at most $M_1 \cdot 2N'(N'/sM_1)$ terms with $a_1 = a_2$. They contribute at most $2(N')^4/(s^2 M_1)$ to T_s^2, and thus no more than $((N')^2/\sqrt{M_1}) \log M_2$ to the sum $\sum_{s=1}^{\lceil M_2/M_1 \rceil} T_s$. It remains to bound

$$\sum_{\substack{sM_1 \leqslant a_1, a_2 < (s+1)M_1 \\ a_1 \neq a_2}} \sigma_{a_1}\sigma_{a_2}\lambda(a_1 a_2) \sum_{\substack{c \\ (a_i b, c) \in S' \cap L'}} \sum_{|b| \leqslant N'/sM_1} \lambda(q_1 a_1 b + q_2 c)\lambda(q_1 a_2 b + q_2 c).$$

Since $|\sigma_a| \leqslant 1$ for all a, the absolute value of this is at most

$$\sum_{\substack{a_1 = sM_1 \\ a_1 \neq a_2}}^{(s+1)M_1 - 1} \sum_{a_2 = sM_1}^{(s+1)M_1 - 1} \Bigg| \sum_{\substack{c \\ (a_i b, c) \in S' \cap L'}} \sum_{b} \lambda(q_1 a_1 b + q_2 c)\lambda(q_1 a_2 b + q_2 c) \Bigg|.$$

By Lemma 3.2 we may write $\{(b,c) \in \mathbb{Z}^2 : (a_1 b, c), (a_2 b, c) \in S' \cap L'\}$ as $S''_{a_1,a_2} \cap L''_{a_1,a_2}$ with S''_{a_1,a_2} a convex subset of $[-N'/\max(a_1,a_2), N'/\max(a_1,a_2)] \times [-N', N']$ and $L''_{a_1,a_2} \subset \mathbb{Z}^2$ a lattice coset of index dividing $[\mathbb{Z}^2 : L']^2$. Hence we have the sum

$$\sum_{\substack{a_1 = sM_1 \\ a_1 \neq a_2}}^{(s+1)M_1 - 1} \sum_{a_2 = sM_1}^{(s+1)M_1 - 1} \Bigg| \sum_{(b,c) \in S''_{a_1,a_2} \cap L''_{a_1,a_2}} \lambda(q_1 a_1 b + q_2 c)\lambda(q_1 a_2 b + q_2 c) \Bigg|. \tag{3.1}$$

Set

$$S_{a_1,a_2} = \begin{pmatrix} q_1 a_1 & q_2 \\ q_1 a_2 & q_2 \end{pmatrix} S''_{a_1,a_2}, \quad L_{a_1,a_2} = \begin{pmatrix} q_1 a_1 & q_2 \\ q_1 a_2 & q_2 \end{pmatrix} L''_{a_1,a_2}$$

and $N'' = (|q_1| + |q_2|)N'$. Clearly S_{a_1,a_2} is a convex subset of $[-N'', N'']^2$ with

$$\operatorname{Area}(S_{a_1,a_2}) = |q_1 q_2 (a_1 - a_2)| \operatorname{Area}(S'') \leqslant |q_1 q_2| M_1 \frac{4(N')^2}{sM_1} \ll \frac{N^2}{s},$$

whereas $L_{a_1,a_2} \subset \mathbb{Z}^2$ is a lattice coset of index $|q_1 q_2 (a_1 - a_2)|[\mathbb{Z}^2 : L''_{a_1,a_2}]$. (That L_{a_1,a_2} is inside $\mathbb{Z}^2$ follows from our earlier remark that $q_1 x + q_2 y$ is an integer for all (x,y) in $A_{12}L$.) Now we have

$$\sum_{\substack{a_1 = sM_1 \\ a_1 \neq a_2}}^{(s+1)M_1 - 1} \sum_{a_2 = sM_1}^{(s+1)M_1 - 1} \Bigg| \sum_{(v,w) \in S_{a_1,a_2} \cap L_{a_1,a_2}} \lambda(v)\lambda(w) \Bigg|.$$

This is at most

$$M_1^2 \max_{sM_1 \leqslant a < (s+1)M_1} \max_{\substack{-M_1 \leqslant d \leqslant M_1 \\ d \neq 0}} \Bigg| \sum_{(v,w) \in S_{a,a+d} \cap L_{a,a+d}} \lambda(v)\lambda(w) \Bigg|. \tag{3.2}$$

We can assume that $[\mathbb{Z}^2 : L] < (\log N)^\alpha$, as otherwise the bound we are attempting to prove is trivial. Hence $[\mathbb{Z}^2 : L''] \ll (\log N)^{2\alpha}$. By Lemma 2.4,

$$\Bigg| \sum_{(v,w) \in S_{a,a+d} \cap L_{a,a+d}} \lambda(v)\lambda(w) \Bigg| \ll \frac{N^2}{s} \cdot \exp\left[-\frac{1}{2} \frac{C(\log N'')^{1/4}}{(\log\log N'')^{3/4}} \right] + (N'')^{\frac{19}{12} + \epsilon}. \tag{3.3}$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

It is time to collect all terms. The total is at most a constant times

$$\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S')}{[\mathbb{Z}^2:L']} + N'M_2 + \frac{(N')^2}{\sqrt{M_1}}\log M_2 + N'N''\sqrt{M_1}\log M_2 \cdot \exp\left[-\frac{1}{2}\frac{C(\log N'')^{1/4}}{(\log\log N'')^{3/4}}\right] + N'(N'')^{\frac{19}{24}+\epsilon}\sqrt{M_2},$$

where the constant depends only on (a_{ij}) and α. Set $\beta = \frac{1}{3}$. Simplifying we obtain

$$O\left(\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]} + \frac{N^2}{(\log N)^\alpha}\right).$$

This completes the proof of Theorem 3.3. □

4. *The average of λ on the product of a linear and a quadratic factor*

We will be working with quadratic extensions $K/\mathbb{Q}$. We define

$$\jmath(x+y\sqrt{d}) = (x,y) \qquad \text{if } d \not\equiv 1 \bmod 4,$$
$$\jmath(x+y\sqrt{d}) = (x-y,2y) \quad \text{if } d \equiv 1 \bmod 4,$$

where $x, y \in \mathbb{Q}$.

For every $z \in \jmath^{-1}([-N,N]^2)$,

$$|N_{K/\mathbb{Q}}z| \ll N^2, \tag{4.1}$$

where the implied constant depends only on K. In general there is no implication in the opposite sense, as the norm need not be positive definite. For $K = \mathbb{Q}(\sqrt{d})$, $d < 0$,

$$\#\{z \in \mathcal{O}_K : N_{K/\mathbb{Q}}(z) \leqslant A\} \ll A. \tag{4.2}$$

For $K = \mathbb{Q}(\sqrt{d})$, $d > 1$,

$$\#\{z \in \jmath^{-1}([-N,N]^2) : |N_{K/\mathbb{Q}}(z)| \leqslant A\} \ll A(1+\log N). \tag{4.3}$$

In either case the implied constant depends only on d.

LEMMA 4.1. *Let $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ divisible by no rational integer $n > 1$. Then for any positive N, $y_0 \in [-N,N]$,*

$$\#\{(x,y_0) \in [-N,N]^2 : \jmath^{-1}(x,y_0) \in \mathfrak{a}\} \leqslant 2\lceil N/N_{K/\mathbb{Q}}(\mathfrak{a})\rceil.$$

Proof. For every rational integer $r \in \mathfrak{a}$, $N_{K/\mathbb{Q}}\mathfrak{a} | r$. Hence

$$\{x : \jmath^{-1}(x,y_0) \in \mathfrak{a}\}$$

is an arithmetic progression of modulus $N_{K/\mathbb{Q}}\mathfrak{a}$. □

THEOREM 4.2. *Let S be a convex subset of $[-N,N]^2$, $N > 1$. Let $L \subset \mathbb{Z}^2$ be a lattice coset. Let a_1, a_2, a_3, a_4, a_5 be rational integers such that $a_1x^2 + a_2xy + a_3y^2$ is irreducible. Then*

$$\sum_{(x,y)\in S\cap L} \lambda((a_1x^2+a_2xy+a_3y^2)(a_4x+a_5y)) \ll \frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]} + \frac{N^2}{(\log N)^\alpha}$$

for any $\alpha > 0$. The implied constant depends only on (a_{ij}) and α.

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

Proof. Write d for $a_1^2 - 4a_0a_2$, $K/\mathbb{Q}$ for $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mathfrak{N}z$ for $N_{K/\mathbb{Q}}z$ and $\overline{r+s\sqrt{d}}$ for $r - s\sqrt{d}$. By Lemma 2.3 there are $\alpha_1, \alpha_2 \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$ and a non-zero rational number k such that

$$a_1x^2 + a_2xy + a_3y^2 = k\mathfrak{N}(x\alpha_1 + y\alpha_2) = k(x\alpha_1 + y\alpha_2)\overline{(x\alpha_1 + y\alpha_2)}.$$

Hence

$$\sum_{(x,y)\in S\cap L} \lambda((a_1x^2 + a_2xy + a_3y^2)(a_4x + a_5y))$$

equals

$$\lambda(k) \sum_{(x,y)\in S\cap L} \lambda((x\alpha_1 + y\alpha_2)\overline{(x\alpha_1 + y\alpha_2)}(a_4x + a_5y)).$$

We write $\Re(r + s\sqrt{d})$ for r, $\Im(r + s\sqrt{d})$ for s. Let

$$C = \begin{pmatrix} \Re\alpha_1 & \Re\alpha_2 \\ \Im\alpha_1 & \Im\alpha_2 \end{pmatrix}^{-1}.$$

Then $a_4x + a_5y = qz + \overline{qz}$ for $z = x\alpha_1 + y\alpha_2$,

$$q = \frac{1}{2}\left(a_4c_{11} + a_5c_{21} + \frac{1}{\sqrt{d}}(a_4c_{12} + a_5c_{22})\right).$$

Define $\phi_Q : \mathbb{Z}^2 \to \mathcal{O}_K$ to be the mapping $(x, y) \mapsto (x\alpha_1 + y\alpha_2)$. Let $L' = (\jmath \circ \phi_Q)(L)$. Since $\jmath \circ \phi_Q$ is linear, it extends to a map $\varphi : \mathbb{R} \to \mathbb{R}$. Let $S' = \phi(S)$. Then

$$\sum_{(x,y)\in S\cap L} \lambda((x\alpha_1 + y\alpha_2)\overline{(x\alpha_1 + y\alpha_2)}(a_4x + a_5y)) = \sum_{\jmath(z)\in S'\cap L'} \lambda(z\overline{z}(qz + \overline{qz})).$$

Note that $qz + \overline{qz}$ is an integer for all $z \in L'$.

Let N' be the smallest integer greater than one such that $S' \subset [-N', N']^2$. (Note that $N' \leqslant c_1N$, where c_1 is a constant depending only on $\mathbb{Q}$.) Suppose $K/\mathbb{Q}$ is real. Then, by (4.3),

$$\#\left\{z \in \jmath^{-1}([-N', N']^2) : |\mathfrak{N}z| \leqslant \frac{(N')^2}{(\log N)^{\alpha+1}}\right\} \leqslant \frac{(N')^2(1 + \log N')}{(\log N)^{\alpha+1}} \ll \frac{N^2}{(\log N)^{\alpha}}.$$

The set

$$\left\{P \in [-N', N']^2 : |\mathfrak{N}(\jmath^{-1}(P))| > \frac{(N')^2}{(\log N)^{\alpha+1}}\right\}$$

is the region within a square and outside two hyperbolas. As such it is the disjoint union of at most four convex sets. Hence the set

$$S'' = S' \cap \{P \in [-N', N']^2 : |\mathfrak{N}(\jmath^{-1}(P))| > (N')^2/(\log N)^{\alpha+1}\}$$

is the disjoint union of at most four convex sets:

$$S'' = S_1 \cup S_2 \cup S_3 \cup S_4.$$

In the following, S^* will be S_1, S_2, S_3 or S_4, and as such a convex set contained in S''.

Suppose now that $K/\mathbb{Q}$ is imaginary. Then the set

$$\{P \in [-N', N']^2 : \mathfrak{N}(\jmath^{-1}(P)) > (N')^2/(\log N)^{\alpha+1}\}$$

is the region within a square and outside the circle given by

$$\{P : \mathfrak{N}(\jmath^{-1}(P)) = (N')^2/(\log N)^{\alpha+1}\}. \tag{4.4}$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

We can circumscribe about (4.4) a rhombus containing no more than

$$O((N')^2/(\log N)^{\alpha+1})$$

integer points, where the implied constant depends only on Q. We then quarter the region inside the square $[-N', N']^2$ and outside the rhombus, obtaining four convex sets S_1, S_2, S_3, S_4 inside S. We let S^* be S_1, S_2, S_3 or S_4.

For K either real or imaginary, we now have a convex set $S^* \subset [-N', N']^2$ such that, for any $z \in \mathcal{O}_K$,

$$\jmath(z) \in S^* \quad \Rightarrow \quad \mathfrak{N}z > (N')^2/(\log N)^{\alpha+1}.$$

Our task is to bound

$$\sum_{\substack{z\in\mathcal{O}_K\\ \jmath(z)\in S^*\cap L'}} \lambda(z\bar{z}(qz+\overline{qz})).$$

Set

$$M_1 = (\log N)^{20(\alpha+1)}, \quad M_2 = \frac{N^{1/2}}{4d\,|\,\mathrm{num}(\mathfrak{N}q)\,|\,[\mathcal{O}_K : L']^2(\log N)^{18\alpha+24}},$$

where, for a rational number r, $\mathrm{num}(r)$ stands for the numerator a of $r = a/b$, $\gcd(a,b) = 1$. By Lemma 2.2 with $\mathcal{P} = \{\mathfrak{p} \text{ prime} : M_1 \leqslant N\mathfrak{p} < M_2\}$,

$$\sum_{\substack{z\in\mathcal{O}_K\\ \jmath(z)\in S^*\cap L'}} \lambda(z\overline{z}(qz+\overline{qz})) = \sum_{\substack{z\in\mathcal{O}_K\\ \jmath(z)\in S^*\cap L'}} \sum_{\mathfrak{d}\,|\,z} \sigma_{\mathfrak{d}}\lambda(z\overline{z}(qz+\overline{qz})) + O\left(\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S^*)}{[\mathcal{O}_K : L']} + N'M_2^2\right). \tag{4.5}$$

Let $N'' = (9/4+|d|)(N')^2$. Then $\jmath(z) \in [-N', N']^2$ implies $|\mathfrak{N}z| \leqslant N''$. Since $\sigma_{\mathfrak{d}} = 0$ when $N\mathfrak{d} < M_1$, the first term on the right of (4.5) equals

$$\sum_{\substack{\mathfrak{b}\\ \mathfrak{N}\mathfrak{b}\leqslant N''/M_1}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a}\\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b}\\ \jmath(z)\in S^*\cap L'}} \lambda(qz+\overline{qz}).$$

We need to split the domain:

$$\sum_{\substack{\mathfrak{b}\\ \mathfrak{N}\mathfrak{b}\leqslant N''/M_1}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a}\\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b}\\ \jmath(z)\in S^*\cap L'}} \lambda(qz+\overline{qz}) = \sum_{s=1}^{\lceil \log_2(N''/M_1)\rceil} T_s, \tag{4.6}$$

where

$$T_s = \sum_{\substack{\mathfrak{b}\\ 2^{s-1}\leqslant\mathfrak{N}\mathfrak{b}\leqslant 2^s}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a}\\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b}\\ \jmath(z)\in S^*\cap L'}} \lambda(qz+\overline{qz}).$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

Note that $\lambda(\mathfrak{b}\overline{\mathfrak{b}})$, $\sigma_{\mathfrak{a}}$, $\lambda(\mathfrak{a}\overline{\mathfrak{a}})$ and $\lambda(qz+\overline{qz})$ are all real. By Cauchy's inequality,

$$T_s^2 \ll 2^{s-1} \sum_{\substack{\mathfrak{b} \\ 2^{s-1}\leqslant \mathfrak{N}\mathfrak{b}\leqslant 2^s}} \left(\sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z)\in S^*\cap L'}} \lambda(qz+\overline{qz}) \right)^2$$

$$\leqslant 2^{s-1} \sum_{\mathfrak{b}} \left(\sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}}} \sigma_{\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z)\in S^*\cap L'}} \lambda(qz+\overline{qz}) \right)^2,$$

where

$$n_{s0} = \frac{(N')^2}{2^s(\log N)^{\alpha+1}} \quad \text{and} \quad n_{s1} = \min\left(\frac{N''}{2^{s-1}}, M_2\right).$$

Expanding the square and changing the order of summation, we get

$$2^{s-1} \sum_{\substack{\mathfrak{a}_1 \\ n_{s0}<\mathfrak{N}\mathfrak{a}_1\leqslant n_{s1}}} \sum_{\substack{\mathfrak{a}_2 \\ n_{s0}<\mathfrak{N}\mathfrak{a}_2\leqslant n_{s1}}} \sigma_{\mathfrak{a}_1}\sigma_{\mathfrak{a}_2}\lambda(\mathfrak{a}_1\overline{\mathfrak{a}_1})\lambda(\mathfrak{a}_2\overline{\mathfrak{a}_2})$$
$$\times \sum_{\substack{\mathfrak{b} \\ \mathfrak{a}_1\mathfrak{b},\, \mathfrak{a}_2\mathfrak{b} \text{ principal}}} \sum_{\substack{(z_1)=\mathfrak{a}_1\mathfrak{b} \\ \jmath(z_1)\in S^*\cap L'}} \sum_{\substack{(z_2)=\mathfrak{a}_2\mathfrak{b} \\ \jmath(z_2)\in S^*\cap L'}} \lambda(qz_1+\overline{qz_1})\lambda(qz_2+\overline{qz_2}).$$

Write $\mathcal{S}(x+y\sqrt{d})$ for $\max(|x|,|y|)$. Let $r=(z_2/z_1)\cdot\mathfrak{N}\mathfrak{a}$. We have $r\in\overline{\mathfrak{a}_1}$ because

$$(r) = ((z_2)/(z_1))\cdot\mathfrak{N}\mathfrak{a}_1 = (\mathfrak{a}_2/\mathfrak{a}_1)\cdot\mathfrak{N}\mathfrak{a}_1 = \mathfrak{a}_2\cdot\overline{\mathfrak{a}_1}.$$

Since

$$\mathfrak{N}z_1 > \frac{(N')^2}{(\log N)^{\alpha+1}} \quad \text{and} \quad \mathcal{S}(z_2\overline{z_1}) \ll (N')^2,$$

where the implied constant depends only on $\mathbb{Q}$,

$$\mathcal{S}(r) = \mathcal{S}\left(\frac{z_2}{z_1}\mathfrak{N}\mathfrak{a}_1\right) = \mathcal{S}\left(\frac{z_2\overline{z_1}}{\mathfrak{N}z_1}\mathfrak{N}\mathfrak{a}_1\right) = \mathcal{S}(z_2\overline{z_1})\frac{\mathfrak{N}\mathfrak{a}}{\mathfrak{N}z_1} \ll n_{s1}(\log N)^{\alpha+1}. \tag{4.7}$$

Set

$$R_s = \jmath^{-1}([-kn_{s1}(\log N)^{\alpha+1}, kn_{s1}(\log N)^{\alpha+1}]^2),$$

where k is the implied constant in (4.7) and as such depends only on K. Changing variables we obtain

$$2^{s-1} \sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}}} \sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s \\ n_{s0}<\mathfrak{N}((r)/\mathfrak{a})\leqslant n_{s1}}} \sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}})\lambda\left(\frac{(r)}{\mathfrak{a}}\frac{\overline{(r)}}{\mathfrak{a}}\right)$$
$$\times \sum_{\substack{z \\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L' \\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}} \lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right),$$

that is, 2^{s-1} times

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}}} \sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s \\ n_{s0}<\mathfrak{N}((r)/\mathfrak{a})\leqslant n_{s1}}} \sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(r\overline{r}) \sum_{\substack{z \\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L' \\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}} \lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right). \tag{4.8}$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

We now wish to eliminate the terms coming from $\mathfrak{a}$ with non-trivial rational integer divisors; we may do so once we show that the total contribution of such terms is small. For any non-zero rational integer n,

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n\mid\mathfrak{a}}}\sum_{r\in\overline{\mathfrak{a}}\cap R_s}\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*}}1\ll\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n\mid\mathfrak{a}}}\frac{(2kn_{s1}(\log N)^{\alpha+1})^2}{\mathfrak{N}\mathfrak{a}}\left(\frac{(N')^2}{\mathfrak{N}\mathfrak{a}}+N'\right)$$
$$\ll\frac{1}{n^2}\frac{N^4(\log N)^{3\alpha+3}}{2^s}.$$

(Here $(N')^2/\mathfrak{N}\mathfrak{a}\gg N'$ because $\mathfrak{N}\mathfrak{a}\leqslant n_{s1}$ and $n_{s1}\leqslant M_2$.) Since the support of $\sigma_{\mathfrak{d}}$ is a subset of

$$\{\mathfrak{d}:M_1\leqslant\mathfrak{N}\mathfrak{d}<M_2,\quad\mathfrak{N}\mathfrak{p}<M_1\Rightarrow\mathfrak{p}\nmid\mathfrak{d}\},$$

we have that $n|\mathfrak{a}$ and $\sigma_{\mathfrak{a}}\neq 0$ imply $n\geqslant\sqrt{M_1}$. Therefore (4.8) equals

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n>1\Rightarrow n\nmid\mathfrak{a}}}\sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s\\ n_{s0}<\mathfrak{N}((r)/\mathfrak{a})\leqslant n_{s1}}}\sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(r\overline{r})\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L'\\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}}\lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right)\tag{4.9}$$

plus $O(N^4(\log N)^{3\alpha+3}/(2^s\sqrt{M_1}))$. The absolute value of (4.9) is at most

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n>1\Rightarrow n\nmid\mathfrak{a}}}\sum_{r\in\overline{\mathfrak{a}}\cap R_s}\left|\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L'\\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}}\lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right)\right|.\tag{4.10}$$

By Lemma 4.1,

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n>1\Rightarrow n\nmid\mathfrak{a}}}\sum_{r\in\overline{\mathfrak{a}}\cap R_s\cap\mathbb{Z}}\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*}}1\ll\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}}}\frac{kn_{s1}(\log N)^{\alpha+1}}{\mathfrak{N}\mathfrak{a}}\cdot\left(\frac{(N')^2}{\mathfrak{N}\mathfrak{a}}+N'\right)$$
$$\ll N^2(\log N)^{2(\alpha+1)}.$$

Thus we are left with

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1}\\ n>1\Rightarrow n\nmid\mathfrak{a}}}\sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s\\ \Im r\neq 0}}\left|\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L'\\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}}\lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right)\right|.\tag{4.11}$$

Notice that $r\in\overline{\mathfrak{a}}$ and $z\in\mathfrak{a}$ imply $(rz/\mathfrak{N}\mathfrak{a})\in\mathcal{O}_K$. Hence $(r/\mathfrak{N}\mathfrak{a})^{-1}\mathcal{O}_K\supset\mathfrak{a}$. Therefore $(r/\mathfrak{N}\mathfrak{a})^{-1}\jmath^{-1}(L')\cap\mathfrak{a}$ is either the empty set or a sublattice of $\mathfrak{a}$ of index dividing $[\mathcal{O}_K:L']$. This means that

$$L_{\mathfrak{a},r}=\{z\in\mathfrak{a}\cap\jmath^{-1}(L'):(rz/\mathfrak{N}\mathfrak{a})\in\jmath^{-1}(L')\}$$

is either the empty set or a sublattice of $\mathfrak{a}$ of index $[\mathfrak{a}:L_{\mathfrak{a},r}]$ dividing $[\mathcal{O}_K:L']^2$, whereas

$$S_{\mathfrak{a},r}=\{\jmath(z)\in S^*:\jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\}$$

is a convex subset of $[-N',N']^2$. The map

$$\kappa:(x,y)\mapsto\left(q\cdot\jmath^{-1}(x,y)+\overline{q\cdot\jmath^{-1}(x,y)},\ \frac{qr\cdot\jmath^{-1}(x,y)}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qr\cdot\jmath^{-1}(x,y)}}{\mathfrak{N}\mathfrak{a}}\right)$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

is given by the matrix

$$\begin{pmatrix} 2 & 0 \\ 2\Re r/\mathfrak{N}\mathfrak{a} & 2d\Im r/\mathfrak{N}\mathfrak{a} \end{pmatrix} \cdot \begin{pmatrix} \Re q & d\Im q \\ \Im q & \Re q \end{pmatrix} \quad \text{if } d \not\equiv 1 \bmod 4,$$

$$\begin{pmatrix} 2 & 0 \\ 2\Re/r\mathfrak{N}\mathfrak{a} & 2d\Im r/\mathfrak{N}\mathfrak{a} \end{pmatrix} \cdot \begin{pmatrix} \Re q & d\Im q \\ \Im q & \Re q \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \quad \text{if } d \equiv 1 \bmod 4.$$

The matrix corresponding to $d \not\equiv 1$ has determinant $4d\,\Im r\mathfrak{N}q/\mathfrak{N}\mathfrak{a}$, whereas the matrix corresponding to $d \equiv 1$ has determinant $2d\,\Im r\mathfrak{N}q/\mathfrak{N}\mathfrak{a}$. Hence $\kappa(\jmath(L_{\mathfrak{a},r}))$ is either the empty set or a lattice $L'_{\mathfrak{a},r}$ of index

$$[\mathbb{Z}^2 : L'_{\mathfrak{a},r}] = \begin{cases} 4d\,\Im r\mathfrak{N}q[\mathfrak{a} : L_{\mathfrak{a},r}] & \text{if } d \not\equiv 1 \bmod 4, \\ 2d\,\Im r\mathfrak{N}q[\mathfrak{a} : L_{\mathfrak{a},r}] & \text{if } d \equiv 1 \bmod 4, \end{cases}$$

and $\kappa(\jmath(S_{\mathfrak{a},r}))$ is a convex set $S'_{\mathfrak{a},r}$ contained in

$$\left[-3|d|\frac{\mathcal{S}(r)}{\mathfrak{N}\mathfrak{a}}\mathcal{S}(q)N',\ 3|d|\frac{\mathcal{S}(r)}{\mathfrak{N}\mathfrak{a}}\mathcal{S}(q)N'\right]^2,$$

which is contained in

$$\left[-3|d|\mathcal{S}(q)\frac{n_{s1}(\log N)^{\alpha+1}}{n_{s0}},\ 3|d|\mathcal{S}(q)\frac{n_{s1}(\log N)^{\alpha+1}}{n_{s0}}\right]^2,$$

which is in turn contained in

$$[-k'(\log N)^{2\alpha+2}N,\ k'(\log N)^{2\alpha+2}N]^2,$$

where k' depends only on d and q. Write (4.11) as

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\leqslant n_{s1} \\ n>1\Rightarrow n\nmid\mathfrak{a}}} \sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s \\ \Im r\neq 0}} \left| \sum_{(v,w)\in L'_{\mathfrak{a},r}\cap S'_{\mathfrak{a},r}} \lambda(v)\lambda(w) \right|. \tag{4.12}$$

Since r is in R_s, $\Im r$ takes values between $-kn_{s1}(\log N)^{\alpha+1}$ and $kn_{s1}(\log N)^{\alpha+1}$. By Lemma 4.1, $\Im r$ takes each of these values at most

$$2\lceil (kn_{s1}(\log N)^{\alpha+1})/n_{s0}\rceil \ll (\log N)^{2\alpha+2}$$

times. Thus (4.12) is bounded by a constant times

$$\frac{N''}{2^{s-1}}(\log N)^{2\alpha+2} \sum_{0<y\leqslant kM_2(\log N)^{\alpha+1}} \max_{\mathfrak{a}} \max_{r:\Im r=y} \left| \sum_{(v,w)\in L'_{\mathfrak{a},r}\cap S'_{\mathfrak{a},y}} \lambda(v)\lambda(w) \right|.$$

We may assume that $[\mathbb{Z}^2 : L] \ll (\log N)^{\alpha}$, as otherwise what we want to prove is trivial. By Corollary 2.7,

$$\sum_{0<y\leqslant kM_2(\log N)^{\alpha+1}} \max_{\mathfrak{a}} \max_{r:\Im r=y} \left| \sum_{(v,w)\in L'_{\mathfrak{a},r}\cap S'_{\mathfrak{a},y}} \lambda(v)\lambda(w) \right|$$

is

$$O\left(\tau(4d\,\mathrm{num}(\mathfrak{N}q)\,\mathrm{den}(\mathfrak{N}q)[\mathcal{O}_K : L']^2)\frac{((\log N)^{2\alpha+2}N)^2}{(\log N)^{8\alpha+9}}\right),$$

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

where $\mathrm{den}(a/b)$ stands for the denominator b of a rational number a/b, $\gcd(a,b)=1$. (Recall that $\mathrm{num}(a/b)$ stands for the numerator a.) It is time to collect all terms:

$$\begin{aligned}T_s^2 &\ll 2^{s-1}\frac{N''}{2^{s-1}}(\log N)^{2\alpha+2}\tau(4d\,\mathrm{num}(\mathfrak{N}q)\det(\mathfrak{N}q)[\mathcal{O}_K:L']^2)\frac{((\log N)^{2\alpha+2}N)^2}{(\log N)^{8\alpha+9}}\\ &\quad+2^{s-1}\left(N^2(\log N)^{2(\alpha+1)}+\frac{N^4(\log N)^{3\alpha+3}}{2^s\sqrt{M_1}}\right)\\ &\ll N^2(\log N)^{2\alpha+2+\epsilon}\frac{(\log N)^{4\alpha+4}N^2}{(\log N)^{8\alpha+9}}+2^sN^2(\log N)^{2(\alpha+1)}+N^4/(\log N)^{7\alpha+7}\\ &\ll N^4/(\log N)^{2\alpha+3-\epsilon}+2^sN^2(\log N)^{2(\alpha+1)}.\end{aligned}$$

Thus

$$\sum_{s=1}^{\lceil\log_2(N''/M_1)\rceil}T_s\ll\frac{N^2}{(\log N)^{\alpha+1}}+\frac{N^2(\log N)^{\alpha+1}}{(\log N)^{10(\alpha+1)}}\ll\frac{N^2}{(\log N)^{\alpha+1}}.$$

By (4.5) and (4.6), the left-hand side of (4.5) is at most

$$O\left(\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S^*)}{[\mathcal{O}_K:L']}+N'M_2^2\right)+\sum_{s=1}^{\lceil\log_2(N''/M_1)\rceil}T_s,$$

which, by the above, is at most

$$O\left(\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S^*)}{[\mathbb{Z}^2:L]}+\frac{N^2}{(\log N)^{36\alpha+48}}+\frac{N^2}{(\log N)^{\alpha+1}}\right).$$

As we saw before, there are at most $O(N^2/(\log N)^\alpha)$ terms in the original sum missing from the left-hand side of (4.5). Hence, the original sum is at most

$$O\left(\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+\frac{N^2}{(\log N)^\alpha}\right).$$

This completes the proof of Theorem 4.2. □

5. *Averages twisted by characters; root numbers*

Define $(a|b)=\prod_{p|b,\,p\text{ odd}}(a/p)^{v_p(b)}$, where (a/p) is the quadratic reciprocity symbol.

PROPOSITION 5.1. *Let S be a convex subset of $[-N,N]^2$, $N>1$. Let $L\subset\mathbb{Z}^2$ be a lattice coset. Then*

$$\sum_{\substack{(x,y)\in S\cap L\\ \gcd(x,y)=1}}(y|x)\cdot\lambda(xy(x-y))\ll\frac{\log\log N}{\sqrt{\log N}}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+\frac{N^2}{(\log N)^\alpha}$$

for any $\alpha>0$. The implied constant depends only on α.

Proof. Proceed as in Theorem 3.3. When applying Lemma 3.1, use $M_1=(\log N)^{2\alpha+2}$, $M_2=e^{\epsilon\sqrt{\log N}}$, where $\epsilon>0$ is a sufficiently small constant; define $\mathcal{P}$ to be the set of all primes p such that $M_1\leqslant p<M_2$ and p is not the largest

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

prime divisor of any exceptional modulus $m \leqslant N$. Instead of (3.1), we have

$$\sum_{\substack{a_1=sM_1\\ a_1\neq a_2}}^{(s+1)M_1-1} \sum_{a_2=sM_1}^{(s+1)M_1-1} |\sigma_{a_1}\sigma_{a_2}| \left| \sum_{(b,c)\in S''_{a_1,a_2}\cap L''_{a_1,a_2}} (c|a_1a_2)\lambda(a_1b-c)\lambda(a_2b-c) \right|.$$

For every $k \bmod a_1a_2$, the lattice $L'''_{a_1,a_2,k} = L''_{a_1,a_2} \cap \{(b,c) : c \equiv k \bmod a_1a_2\}$ has index dividing $[\mathbb{Z}^2 : L''_{a_1,a_2}] \cdot a_1a_2$. Define

$$L_{a_1,a_2,k} = \begin{pmatrix} a_1 & -1 \\ a_2 & -1 \end{pmatrix} L'''_{a_1,a_2,k},$$

and proceed as before. We obtain, instead of (3.2),

$$M_1^2 \max_{\substack{sM_1\leqslant a<(s+1)M_1\\ a \text{ unexceptional}}} \max_{\substack{-M_1\leqslant d\leqslant M_1\\ d\neq 0\\ a+d \text{ unexceptional}}} \sum_{k=1}^{a(a+d)} \left| \sum_{(v,w)\in S_{a,a+d}\cap L_{a,a+d,k}} \lambda(v)\lambda(w) \right|.$$

Since $a(a+d) \ll e^{2\epsilon\sqrt{\log N}}$, the additional sum $\sum_k$ is absorbed by the right-hand side of the analogue of (3.3). No invocation of Lemma 2.4 is needed here, as the Siegel estimate (2.9) suffices; in particular, no short-interval results are needed. Note also that the factor of $\prod_{M_1\leqslant p<M_2:\, p\notin\mathcal{P}}(1-1/p)^{-1}$ coming from Lemma 2.1 is bounded from above by a constant: since there are at most $O(\log\log N)$ exceptional moduli up to N, the cardinality of $\{M_1 \leqslant p < M_2 : p \notin \mathcal{P}\}$ is $O(\log\log N)$; as $M_1 = (\log N)^{2\alpha+2}$, it follows that the factor is $O(1)$. Note, finally, that every time we apply the inequality (2.9), the modulus m is not divisible by any exceptional moduli $q > [\mathbb{Z}^2 : L''_{a_1,a_2}]$. Given that $[\mathbb{Z}^2 : L''_{a_1,a_2}] \ll [\mathbb{Z}^2 : L]^2$ and that we may assume that $[\mathbb{Z}^2 : L] < (\log N)^\alpha$ (as otherwise the result to be proven is trivial), we have that m is not divisible by any exceptional moduli $q > C(\log N)^{2\alpha}$, where C is an absolute constant, and thus (2.9) is valid. □

Corollary 5.2. *For $a, b \in \mathbb{Z}$ coprime, let $E_{a,b}$ denote the elliptic curve $y^2 = x(x+a)(x+b)$. Let S be a convex subset of $[-N,N]^2$, $N > 1$. Let $L \subset \mathbb{Z}^2$ be a lattice coset. Then*

$$\sum_{\substack{(a,b)\in S\cap L\\ \gcd(a,b)=1}} W(E_{a,b}) \ll \frac{\log\log N}{\sqrt{\log N}} \frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + \frac{N^2}{(\log N)^\alpha}$$

for any $\alpha > 0$, where $W(E_{a,b})$ is the root number of $E_{a,b}$. The implied constant depends only on α.

Proof. This is in [**6**, Proposition 5.8]. It is an easy consequence of Proposition 5.1: the root number of $E_{a,b}$ equals

$$-\left(\frac{a}{\mathrm{rad}(2^{-v_2(b)}b)}\right)\left(\frac{b}{\mathrm{rad}(2^{-v_2(a)}a)}\right)\left(\frac{-a}{\mathrm{rad}(2^{-v_2(b-a)}(b-a))}\right)\mu(\mathrm{rad}(ab(a-b))),$$

and the ratio of this expression to $(y|x)\lambda(xy(x-y))$ can be handled by means of a square-free sieve [**7**, Proposition 3.12]. □

Acknowledgements. The help and counsel of my Doktorvater, H. Iwaniec, were most valuable. Thanks are also due to an anonymous referee for his detailed work.

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press

References

1. S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem* (Gordon and Breach, New York, 1965).
2. M. D. Coleman, 'The Rosser–Iwaniec sieve in number fields, with an application', *Acta Arith.* 65 (1993) 53–83.
3. Ch. J. de la Vallée-Poussin, 'Recherches analytiques sur la théorie des nombres premiers', *Brux. S. sc.* 20 B (1896) 363–397.
4. Ch. J. de la Vallée-Poussin, 'Recherches analytiques sur la théorie des nombres premiers', *Brux. S. sc.* 21 B (1897) 251–342.
5. G. Greaves, *Sieves in number theory* (Springer, Berlin, 2001).
6. H. A. Helfgott, 'Root numbers and the parity problem', Doctoral Thesis, Princeton University, 2003, arXiv:math.NT/0305435.
7. H. A. Helfgott, 'On the square-free sieve', *Acta Arith.* 115 (2004) 349–402.
8. H. A. Helfgott, 'On the behaviour of root numbers in families of elliptic curves', Preprint, 2004, arXiv:math.NT/0408141.
9. H. A. Helfgott, 'The parity problem for irreducible cubic forms', Preprint, 2005, arXiv:math.NT/0501177.
10. M. Huxley, 'Large values of Dirichlet polynomials. III', *Acta Arith.* 26 (1974/75) 435–444.
11. H. Iwaniec, 'On zeros of Dirichlet's L series', *Invent. Math.* 23 (1974) 97–104.
12. H. Iwaniec and E. Kowalski, *Analytic number theory*, AMS Colloquium Publications 53 (American Mathematical Society, Providence, RI, 2004).
13. E. Landau, 'Über die Klassenzahl imaginär-quadratischer Zahlkörper', *Göttinger Nachrichten* (1918) 285–295.
14. B. V. Levin, 'The "average" distribution of $\lambda(n)$ and $\Lambda_f(n)$ in progressions', *Topics in classical number theory*, vols I, II (Budapest, 1981) 995–1022; *Colloq. Math. Soc. J. Bolyai* 34 (North-Holland, Amsterdam, 1984).
15. J. Pintz, 'Elementary methods in the theory of L-functions. IX. Density theorems', *Acta Arith.* 49 (1988) 387–394.
16. K. Prachar, *Primzahlverteilung* (Springer, Berlin, 1957).
17. K. Ramachandra, 'Some problems of analytic number theory', *Acta Arith.* 31 (1976) 313–324.
18. A. Selberg, 'On elementary methods in primenumber-theory and their limitations', *Proc. 11th Scand. Math. Cong.* (Trondheim, 1949), in *Collected Works*, vol. I (Springer, Berlin, 1989) 388–397.
19. C. L. Siegel, 'Über die Klassenzahl quadratischer Zahlkörper', *Acta Arith.* 1 (1935) 83–86.
20. A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Math. Forschungsberichte XV (VEB Deutscher Verlag der Wissenschaften, Berlin, 1963).

H. A. Helfgott
Département de Mathématiques et Statistique
Université de Montréal
CP 6128 succ Centre-Ville
Montréal
Québec
H3C 3J7
Canada

helfgott@dms.umontreal.ca

https://doi.org/10.1112/S0024610706022629 Published online by Cambridge University Press