JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

John FRIEDLANDER et Henryk IWANIEC

Ternary quadratic forms with rational zeros

Tome 22, n° 1 (2010), p. 97-113.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_97_0>

Journal de Théorie des Nombres
de Bordeaux **22** (2010), 97-113

Ternary quadratic forms with rational zeros

par John FRIEDLANDER et Henryk IWANIEC

Dédié à Jean-Pierre Serre

Résumé. *Formes quadratiques ternaires avec zéros rationnels*
Nous considérons les formes quadratiques de Legendre

$$\varphi_{ab}(x,y,z) = ax^2 + by^2 - z^2$$

et, en particulier, une question posée par J–P. Serre, de compter le nombre de paires d' entiers $1 \leqslant a \leqslant A$, $1 \leqslant b \leqslant B$, pour lesquels la forme φ_{ab} possède un zéro rationnel et non-trivial. Sous certaines conditions faibles sur les entiers a, b, on peut trouver la formule asymptotique pour le nombre de telles formes.

Abstract. We consider the Legendre quadratic forms

$$\varphi_{ab}(x,y,z) = ax^2 + by^2 - z^2$$

and, in particular, a question posed by J–P. Serre, to count the number of pairs of integers $1 \leqslant a \leqslant A$, $1 \leqslant b \leqslant B$, for which the form φ_{ab} has a non-trivial rational zero. Under certain mild conditions on the integers a, b, we are able to find the asymptotic formula for the number of such forms.

1. Introduction

In his paper [7] J–P. Serre considered, among other things, the question of how many forms

$$\varphi_{ab}(x,y,z) = ax^2 + by^2 - z^2 \tag{1}$$

have a non-trivial rational zero. Interest in these forms dates back to Legendre. We study the family of such forms with integer coefficients $1 \leqslant a \leqslant A$, $1 \leqslant b \leqslant B$. Serre was interested in the case $A = B$ and proved that, for $A = B$ sufficiently large, most such forms do not have such a zero, specifically, the number N of forms which do, satisfies the upper bound

$$N \ll \frac{AB}{\sqrt{\log A}\sqrt{\log B}}\ . \tag{2}$$

Manuscrit reçu le 21 octobre 2008.
J. F. is supported in part by NSERC grant A5123.
H. I. is supported in part by NSF grant DMS-08-02246.

He also noted that one can prove the lower bound $AB/(\log A)(\log B)$ and predicted that the lower bound could be improved, perhaps to match the upper bound. Subsequently, Guo [2] confirmed this by establishing an asymptotic formula (in the case $A = B$, for a slightly modified sum).

In this paper we consider some variations of Serre's problem. We begin by proving an asymptotic formula, also for a slightly modified sum, and valid so long as neither A nor B is extremely small compared to the other. Our arguments differ from those of Guo in a number of respects.

Let $N(A, B)$ denote the number of such pairs with the extra conditions that a and b are odd, squarefree, and relatively prime.

Theorem 1. *Let $\delta > 0$. For A, $B \geqslant \exp\big((\log AB)^{\delta}\big)$ we have*

$$N(A,B) = \frac{6}{\pi^3}\frac{AB}{\sqrt{\log A}\sqrt{\log B}}\Big\{1 + O\big(\frac{1}{\log A} + \frac{1}{\log B}\big)\Big\}\,, \tag{3}$$

where the implied constant depends on δ.

Our restriction that a and b be squarefree is quite natural because square factors of the coefficients can be absorbed into the variables of the form. We expect that the other constraints can also be avoided by some technical modifications and the asymptotic formula given for the original sum N (with a different constant) but we did not pursue this.

As for the restriction that neither of A, B be very small compared to the other, we expect that this could be eased considerably, certainly under the assumption of the Grand Riemann Hypothesis, albeit with a more complicated main term. In fact we are even able to establish an asymptotic formula when one of the coefficients of $\varphi_{ab}(x, y, z)$, say b, is held fixed. Let $b > 1$ be odd and squarefree. Let $N_b(A)$ be the number of $a \leqslant A$, a odd, squarefree and prime to b, such that $\varphi_{ab}(x, y, z)$ has a non-trivial rational zero.

Theorem 2. *If $b \leqslant (\log A)^C$ we have*

$$N_b(A) = \frac{c(b)}{\tau(b)}\frac{A}{\sqrt{\log A}}\Big\{D(b) + O\Big(\frac{(\log\log A)^{\frac{3}{2}}}{\sqrt{\log A}}\Big)\Big\}$$

where C is any positive constant and the implied constant depends on C. Here $c(b)$ is the arithmetic function given in (15) *and*

$$D(b) = \frac{4}{\eta_b}L(1,\chi_b)^{\frac{1}{2}}\prod_p\Big(1 - \frac{\chi_b(p)}{p}\Big)^{\frac{1}{2}}\Big(1 + \frac{\chi_b(p)}{2p+1}\Big)\,, \tag{4}$$

where $\eta_b = 3\,, 4\,, 2\,, 6$ according as $b \equiv 1\,, 3\,, 5\,, 7 \pmod 8$, respectively.

Thus, for each b, the form (1) has no non-trivial rational zero for almost all a prime to b.

By the Minkowski local–global principle (see page 42 of [6]) an indefinite quadratic form represents zero over the rationals if and only if it represents it over every p–adic field. In view of this principle it is an interesting problem to consider more generally a subset $\mathcal{P}$ of the primes and to ask how large $|\mathcal{P}|$ must be in order to conclude that almost all a fail this test for some $p \in \mathcal{P}$.

Let $N_b(A, \mathcal{P})$ be the number of a, $1 \leqslant a \leqslant A$, a squarefree, co-prime with b and such that $\varphi_{ab}(x, y, z)$ has p-adic zeros for every $p \in \mathcal{P}$.

For simplicity we consider $b > 1$, $b \equiv 1 \pmod 4$ and squarefree. Let $\mathcal{P}_b$ be the subset of odd primes in $\mathcal{P}$ which are inert in the quadratic field $\mathbb{Q}(\sqrt{b})$, that is satisfying $(b/p) = -1$.

Theorem 3. *For $b > 1$, $b \equiv 1 \pmod 4$, squarefree, we have*

$$N_b(A, \mathcal{P}) \ll A \prod_{\substack{p \leqslant A \\ p \in \mathcal{P}_b}} \left(1 - \frac{1}{p}\right) . \tag{5}$$

Corollary 1. *Suppose that $\mathcal{P}_b$ is sufficiently large that*

$$\sum_{p \in \mathcal{P}_b} \frac{1}{p} = \infty .$$

Then, for almost all a, squarefree and co-prime with $2b$, the quadratic form $\varphi_{ab}(x, y, z)$ has no p-adic zero for at least one prime $p \in \mathcal{P}$.

Note that the upper bound in Theorem 3 holds for completely general sets $\mathcal{P}$. We are also interested in obtaining a lower bound of the same quality and we succeed in doing so for completely general sets $\mathcal{P}$ as long as $\mathcal{P}_b$ is somewhat smaller than it is when $\mathcal{P}$ is the full set of primes.

Theorem 4. *Let $b > 1$, $b \equiv 1 \pmod 4$, squarefree. Assume that $\mathcal{P}$ satisfies*

$$\sum_{\substack{p \leqslant x \\ p \in \mathcal{P}_b}} \frac{1}{p} < \kappa \log\log x$$

with some constant $0 \leqslant \kappa < 1/2$ and all sufficiently large x. Then, for all sufficiently large A

$$N_b(A, \mathcal{P}) \asymp A \prod_{\substack{p \leqslant A \\ p \in \mathcal{P}_b}} \left(1 - \frac{1}{p}\right) . \tag{6}$$

H.I. wishes to thank the University of Toronto for their hospitality during the period this work was begun and finished and both authors wish to thank the Banff International Research Station for their hospitality during a period in which a substantial part of the paper was completed. We also thank the referee for a careful reading of the paper.

We dedicate this paper to Jean–Pierre Serre, both for the beauty of his mathematics and also in recognition of his support, during many years, for analytic number theory. We also thank him for important comments on an earlier draft of the paper and in particular for drawing our attention to the work of Guo.

2. A characterization using Hilbert symbols

In the case of (1) the local-global principle is characterized by the requirement that the Hilbert symbol (see pages 19-20 of [6]) satisfy

$$\left(\frac{a,b}{p}\right) = 1 \ , \tag{7}$$

for every p. If $p \nmid 2ab$ then (7) always holds. For $p = 2$ we require

$$\left(\frac{a,b}{2}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = 1. \tag{8}$$

Thus we see that we can only get a solution if at least one of the odd integers a and b is congruent to one modulo four. The sum $N(A,B)$ can thus be decomposed into three (out of four) subsums, $N_{11}(A,B)$, $N_{13}(A,B)$, $N_{31}(A,B)$, in accordance with the residue classes modulo four of a and b respectively.

The estimation of each of these three is almost identical and gives rise to asymptotically the same amount. Therefore we shall place emphasis on one of them, the contribution from the pairs a, b satisfying the additional constraint

$$a \equiv b \equiv 1 \,(\mathrm{mod}\, 4) \ . \tag{9}$$

For the remaining primes our local requirement becomes

$$\left(\frac{a,b}{p}\right) = \left(\frac{b}{p}\right) = 1 \ , \tag{10}$$

if $p \mid a$, and

$$\left(\frac{a,b}{p}\right) = \left(\frac{a}{p}\right) = 1 \ , \tag{11}$$

if $p \mid b$. This indicates that the problem reduces to counting integers with certain restrictions on their prime factors. That in turn suggests the possibility of using a sieve method and indeed Serre applied a sieve argument in his original proof of the upper bound (2). The problem has also been studied subsequently in Section 4.5 of [1] wherein Cojocaru and Murty, by a different sieve argument, derive a non-trivial upper bound, but not of the expected order of magnitude.

Put $< a, b >= 1$ if all of the local conditions are satisfied and put $< a, b >= 0$ otherwise. Therefore we have

$$N(A,B) = \sum_{\substack{a\leqslant A\ b\leqslant B\\ 2ab \text{ squarefree}}}\sum < a, b > \ .$$

Suppose that at least one of a and b is congruent to one modulo four. Then we can express the symbol $< a, b >$ in terms of Jacobi symbols by using the law of quadratic reciprocity as follows:

$$\begin{aligned} < a, b > &= \frac{1}{\tau(ab)} \prod_{p|ab} \Big(1 + \Big(\frac{a}{p}\Big)\Big)\Big(1 + \Big(\frac{b}{p}\Big)\Big) \\ &= \frac{1}{\tau(ab)} \sum_{k\ell=a} \sum_{mn=b} \Big(\frac{k\ell}{m}\Big)\Big(\frac{mn}{k}\Big) \\ &= \frac{1}{\tau(ab)} \sum_{k\ell=a} \sum_{mn=b} \Big(\frac{k}{n}\Big)\Big(\frac{\ell}{m}\Big) \ . \end{aligned} \tag{12}$$

If we were to count the forms φ_{ab} with multiplicity then the divisor function factor $1/\tau(ab)$ would not be present and the problem would be much easier, but we wish to concentrate on the more natural question of Serre. The problem thus reduces to the estimation of sums over Hilbert symbols and thereby to sums over Jacobi symbols. Similar sums also occur in the very recent work of Fouvry and Klüners [3].

By (12) we have

$$N_{11}(A,B) = \sum_{\substack{k\ell\leqslant A,\ mn\leqslant B\\ 2k\ell mn \text{ squarefree}\\ k\equiv\ell \,(\mathrm{mod}\, 4),\ m\equiv n \,(\mathrm{mod}\, 4)}}\sum\sum\sum \frac{1}{\tau(k\ell mn)}\Big(\frac{k}{n}\Big)\Big(\frac{\ell}{m}\Big) \ , \tag{13}$$

while in the cases of N_{13}, N_{31}, the second, respectively first, of the $(\mathrm{mod}\, 4)$ congruences requires a minus sign. Note that, since k, ℓ, m, n are pairwise coprime, the divisor function can be split.

3. Lemmas

The proofs of our first two theorems are based on results concerning character sums.

Lemma 1. *Let $\chi \,(\mathrm{mod}\, q)$ be a Dirichlet character and $(d, q) = 1$. Then, we have for $x \geqslant 2$,*

$$\begin{aligned} \sum_{\substack{n\leqslant x\\ (n,d)=1}} \mu^2(n)\frac{\chi(n)}{\tau(n)} = \delta_\chi c(dq)\frac{x}{\sqrt{\log x}}\Big\{1 + O\Big(\frac{(\log\log 3dq)^{\frac{3}{2}}}{\log x}\Big)\Big\} \\ + O_C\big(\tau(d)qx(\log x)^{-C}\big) \ , \end{aligned} \tag{14}$$

with any $C > 0$. Here, δ_χ is zero unless χ is the principal character, in which case $\delta_\chi = 1$ and

$$c(r) = \pi^{-\frac{1}{2}} \prod_p \Big(1 + \frac{1}{2p}\Big)\Big(1 - \frac{1}{p}\Big)^{\frac{1}{2}} \prod_{p|r} \Big(1 + \frac{1}{2p}\Big)^{-1} . \tag{15}$$

This lemma has the following immediate consequence of independent interest, and it is in this more general form that we shall use it.

Corollary 2. *Let $(ad, q) = 1$ where $q = q_1 q_2$ with $(q_1, q_2) = 1$. For χ_2 a character modulo q_2 We have*

$$\sum_{\substack{n \leqslant x \\ (n,d)=1 \\ n \equiv a \,(\mathrm{mod}\, q_1)}} \mu^2(n) \frac{\chi_2(n)}{\tau(n)} = \delta_{\chi_2} \frac{c(dq)}{\varphi(q_1)} \frac{x}{\sqrt{\log x}} \Big\{ 1 + O\Big(\frac{(\log\log 3dq)^{\frac{3}{2}}}{\log x} \Big) \Big\} + O_C\big(\tau(d) q x (\log x)^{-C}\big) . \tag{16}$$

This is an analogue of Landau's theorem on the number of integers which are the sum of two squares and also of the Siegel-Walfisz theorem for primes in arithmetic progressions. Actually, our proofs of these in Section 8 go along such lines. Note that both of the above results are trivial if q exceeds $(\log x)^C$. This limitation comes as usual from that in Siegel's theorem.

Since we can use Lemma 1 only for relatively small moduli we require an additional tool to cover the larger ranges. For this we use the following estimate for general bilinear forms in the Jacobi symbol.

Lemma 2. *Let α_m, β_n be any complex numbers supported on odd integers and bounded by one. Then we have*

$$\sum_{m \leqslant M} \sum_{n \leqslant N} \alpha_m \beta_n \Big(\frac{m}{n}\Big) \ll \big(MN^{\frac{5}{6}} + M^{\frac{5}{6}} N\big)\big(\log 3MN\big)^{\frac{7}{6}} , \tag{17}$$

where the implied constant is absolute.

We shall prove this in Section 9 using ideas originally due to Heilbronn [4] and frequently exploited since. This result is useful if both M and N exceed a sufficiently high power of $\log 3MN$.

The proof of Theorem 3 requires the following estimate for the mean value of a fairly general non-negative multiplicative function.

Lemma 3. *Let $f(m)$ be a non-negative multiplicative function such that*

$$\sum_{y < p \leqslant x} f(p) \frac{\log p}{p} \leqslant \alpha \log \frac{x}{y} + \beta$$

for all $2 \leqslant y \leqslant x$ *where* $\alpha \geqslant 0,\ \beta \geqslant 1$ *are constants. Then*

$$\sum_{m \leqslant x} \mu^2(m) f(m) \ll (\alpha+\beta)\frac{x}{\log x} \prod_{p \leqslant x} \Big(1 + \frac{f(p)}{p}\Big) \ .$$

This lemma is well-known in principle and has a simple proof. For the proof of Theorem 4 we shall require a result from sieve theory.

4. Proof of Theorem 1

In this section we give the proof of Theorem 1, subject to the verification in the following sections of Lemmas 1 and 2. We begin with the formula (13) for $N_{11}(A,B)$.

Let $V \geqslant 3$ be a parameter to be chosen later (as a large power of $\log AB$). If $k \leqslant V$ and $\ell \leqslant V$ we trivially get a contribution

$$O(V^2 B) \ , \tag{18}$$

and similarly, if $m \leqslant V$ and $n \leqslant V$, we trivially get a contribution

$$O(V^2 A) \ . \tag{19}$$

Next, if $k \leqslant V$ and $n \leqslant V$ then we apply Lemma 2 for the sum over $(\frac{\ell}{m})$, getting an amount

$$\begin{aligned} &\ll \sum_{k \leqslant V} \sum_{n \leqslant V} \frac{A}{k}\frac{B}{n}\Big(k^{\frac16} A^{-\frac16} + n^{\frac16} B^{-\frac16}\Big)(\log AB)^{\frac76} \\ &\ll AB\big(V^{\frac16} A^{-\frac16} + V^{\frac16} B^{-\frac16}\big)(\log AB)^{\frac76} \ . \end{aligned} \tag{20}$$

Similarly, if $\ell \leqslant V$ and $m \leqslant V$ then we apply Lemma 2 for the sum over $(\frac{k}{n})$, getting a contribution again bounded by (20).

In the range $k > V$ and $n > V$ we again apply Lemma 2, but now to the sum over k and n, getting an amount

$$O\Big(ABV^{-\frac16}(\log AB)^{\frac{13}{6}}\Big) \ . \tag{21}$$

Similarly, in the range $\ell > V$ and $m > V$ we again get a contribution satisfying the same bound (21).

Now there are two remaining ranges:

$$k \leqslant V\,, \quad m \leqslant V\,, \quad 2km \text{ squarefree}, \tag{22}$$

$$\ell \leqslant V\,, \quad n \leqslant V\,, \quad 2\ell n \text{ squarefree}. \tag{23}$$

By symmetry, the contribution of these two ranges is identical so we may concentrate on (22). For each pair $k \leqslant V$, $m \leqslant V$, $2km$ squarefree, we need

to consider the sum

$$S_{k,m} = \sum_{\substack{\ell\leqslant A/k,\ n\leqslant B/m\\ (\ell n,2km)=1,\ (\ell,n)=1\\ \ell\equiv k\,(\mathrm{mod}\,4),\ n\equiv m\,(\mathrm{mod}\,4)}}\sum \frac{\mu^2(\ell)}{\tau(\ell)}\frac{\mu^2(n)}{\tau(n)}\Big(\frac{k}{n}\Big)\Big(\frac{\ell}{m}\Big)\ . \tag{24}$$

We intend to apply Lemma 1 twice, for the characters

$$\chi_k = \Big(\frac{k}{*}\Big) \quad \text{and} \quad \chi_m = \Big(\frac{*}{m}\Big)\ .$$

Before doing so however we need to remove the condition $(\ell, n) = 1$ which we do by means of the Möbius function, summed over common divisors d of ℓ and n. Having done so we interchange the order of summation, split the sum into two according to whether d is small or large. We give a trivial bound for the larger d and arrive at:

$$\begin{aligned} S_{k,m} = \sum_{\substack{d\leqslant\Delta\\ (d,2km)=1}} \frac{\mu(d)}{\tau^2(d)}\Big(\frac{d}{m}\Big)\Big(\frac{k}{d}\Big) \sum_{\substack{\ell\leqslant A/kd\\ (\ell,2kd)=1,\\ \ell\equiv kd\,(\mathrm{mod}\,4)}} \frac{\mu^2(\ell)}{\tau(\ell)}\Big(\frac{\ell}{m}\Big) \\ \sum_{\substack{n\leqslant B/md\\ (n,2md)=1\\ n\equiv m\,(\mathrm{mod}\,4)}} \frac{\mu^2(n)}{\tau(n)}\Big(\frac{k}{n}\Big) + O\Big(\frac{AB}{\Delta km}\Big)\ . \end{aligned} \tag{25}$$

Here, the error term, after being summed over k, m, is

$$O\Big(\Delta^{-1}AB(\log V)^2\Big)\ . \tag{26}$$

The sums over ℓ and n are now in the proper form for an application of Corollary 2 to each. There will be no main term unless both characters are principal, that is $k = m = 1$. The contribution from the error terms in Corollary 2 when one or both of the characters is non-principal, after being summed over d, k, m is, for any C, bounded by

$$O(ABV^3[(\log A)^{-C} + (\log B)^{-C}])\ . \tag{27}$$

The primary amount, coming to (24) from the case $k = m = 1$ when both of the characters are principal, is given by the product $G_d(A)G_d(B)$ where

$$\begin{aligned} G_d(A) &= \frac{c(4d)A}{2d\sqrt{\log A/d}}\Big\{1 + O\Big(\frac{(\log\log 3d)^{\frac{3}{2}}}{\log A}\Big)\Big\} \\ &= \frac{c(4d)A}{2d\sqrt{\log A}}\Big\{1 + O(\frac{\log 2d}{\log A})\Big\}\ . \end{aligned}$$

We input this product and then sum over d. We obtain

$$\frac{AB}{\sqrt{\log A}\sqrt{\log B}}\Big\{\sum_{d\text{ odd}}\mu(d)\Big(\frac{c(4d)}{2d\tau(d)}\Big)^2+O\Big(\frac{1}{\log A}+\frac{1}{\log B}+\frac{1}{\Delta}\Big)\Big\}\,, \tag{28}$$

where the last term in the error comes from re-extending the summation over d to infinity.

If we take, say $\Delta=(\log AB)^4$, then the error terms in (26) and (28) are acceptable for the theorem. Next, we need to choose V so that the error terms in (18) – (21) are admissible. A little computation shows that $V=(\log AB)^{22}$ suffices. Once having this choice, we choose C in (27) sufficiently large, say $C=68/\delta$ where δ was given in the statement of the theorem.

It remains to evaluate the constant in the main term of (28). By (15)

$$c(4d)=\frac{4}{5}\,c(1)\prod_{p\mid d}\Big(1+\frac{1}{2p}\Big)^{-1}\,,$$

so that the constant in question is

$$\begin{aligned}\sum_{d\text{ odd}}&=\frac{1}{4}\Big(\frac{4}{5}c(1)\Big)^2\prod_{p>2}\Big(1-\frac{1}{\big(1+\frac{1}{2p}\big)^2(2p)^2}\Big)\\&=\frac{1}{6\pi}\prod_p\Big(\big(1+\frac{1}{2p}\big)^2\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{(2p+1)^2}\Big)=\frac{1}{\pi^3}\,.\end{aligned}$$

Recall that this constant is the one which comes from the range (22) so to get the constant for N_{11} we need to double this to include the range (23). Then, to include the contributions from N_{13} and N_{31}, we need to triple that. This completes the proof of Theorem 1.

5. Proof of Theorem 2

We give the details in the case $b\equiv 3\,(\bmod 4)$, b squarefree, $b\neq 1$. By (12) we have

$$\begin{aligned}N_b(A)&=\sum_{\substack{a\leqslant A\\ a\equiv 1\,(\bmod 4)\\ 2ab\text{ squarefree}}}<a,b>\\&=\frac{1}{\tau(b)}\sum_{mn=b}\sum_{\substack{k\ell\leqslant A\\ k\equiv\ell\,(\bmod 4)\\ (k\ell,2b)=1}}\mu^2(k\ell)\Big(\frac{k}{n}\Big)\Big(\frac{\ell}{m}\Big)\tau(k\ell)^{-1}\,.\end{aligned}$$

(In the case $b\equiv 1\,(\bmod 4)$ the condition $k\equiv\ell\,(\bmod 4)$ disappears and the remainder of the proof is almost identical.)

If $m \neq 1$ and $n \neq 1$ then by Corollary 2 we get a contribution

$$\ll \frac{1}{\tau(b)} \sum_{mn=b} \sum_{\substack{k \leqslant \sqrt{A} \\ (k\,b)=1}} \tau(bk) bA k^{-1} (\log A)^{-C}$$
$$\ll \tau(b) bA (\log A)^{2-C} \ .$$

The remaining terms contribute

$$\frac{2}{\tau(b)} \sum_{\substack{k\ell \leqslant A \\ k \equiv \ell \,(\mathrm{mod}\ 4) \\ (k\ell, 2b)=1}} \sum \mu^2(k\ell) \Big(\frac{k}{b}\Big) \tau(k\ell)^{-1} \ .$$

The terms with $k > \sqrt{A}$ contribute, by Corollary 2, the amount

$$O\big(bA(\log A)^{1-C}\big) \ .$$

For each $k \leqslant \sqrt{A}$ we execute the summation over ℓ using Corollary 2 with $d = bk$, $q_1 = 4$, $q_2 = 1$ getting

$$\frac{c(4bk)}{\varphi(4)} \frac{A}{k\sqrt{\log A/k}} \Big\{1 + O\Big(\frac{(\log\log bk)^{\frac{3}{2}}}{\log A}\Big)\Big\} + O\Big(\tau(bk) \frac{bA}{k} (\log A)^{-C}\Big) \ .$$

Hence we obtain

$$\begin{aligned} N_b(A) &= \frac{2}{\tau(b)} \sum_{\substack{k \leqslant \sqrt{A} \\ k \text{ odd}}} \mu^2(k) \Big(\frac{k}{b}\Big) \frac{2c(bk)}{5\tau(k)} \frac{A}{k\sqrt{\log A/k}} \Big\{1 + O\Big(\frac{(\log\log A)^{\frac{3}{2}}}{\log A}\Big)\Big\} \\ &\qquad + O\big(\tau(b) bA (\log A)^{2-C}\big) \\ &= \frac{4c(b)}{5\tau(b)} \frac{A}{\sqrt{\log A}} \ D(b) + O\Big(\frac{c(b)}{\tau(b)} \frac{A}{\log A} (\log\log A)^{\frac{3}{2}}\Big) \\ &\qquad + O\big(\tau(b) bA (\log A)^{2-C}\big) \ , \end{aligned}$$

where

$$D(b) = \sum_{k \,\text{odd}} \mu^2(k) \Big(\frac{k}{b}\Big) \prod_{p \mid k} \Big(1 + \frac{1}{2p}\Big)^{-1} \big(k\tau(k)\big)^{-1} \ .$$

Here the series over k is also given by the product

$$D(b) = \prod_{p>2} \Big[1 + \Big(\frac{p}{b}\Big) \Big(1 + \frac{1}{2p}\Big)^{-1} (2p)^{-1}\Big] = \prod_{p>2} \Big[1 + \frac{\chi_b(p)}{2p+1}\Big] \ ,$$

which is the same as the Euler product (4). This completes the proof.

6. Proof of Theorem 3

From Section 2, ignoring the condition (11) we have

$$N_b(A,\mathcal{P}) \leqslant \sum_{\substack{a\leqslant A\\ 2ab \text{ squarefree}\\ (a,P_b)=1}} 1\ ,$$

where P_b is the product of the primes $p \leqslant A$ and in $\mathcal{P}_b$. This is the mean value of the multiplicative function with $f(p) = 1$ on primes neither dividing $2b$ nor in $\mathcal{P}$ and 0 at other primes. Therefore, Lemma 3 yields

$$N_b(A,\mathcal{P}) \ll \frac{A}{\log A}\prod_{\substack{p\leqslant A\\ p\nmid P_b}}\Big(1+\frac{1}{p}\Big) \ll A\prod_{\substack{p\leqslant A\\ p\mid P_b}}\Big(1-\frac{1}{p}\Big)$$

which completes the proof.

7. Proof of Theorem 4

From Section 2 we have

$$N_b(A,\mathcal{P}) = \sum_{\substack{a\leqslant A\\ 2ab \text{ squarefree}\\ (a,P_b)=1}} w(a)\ ,$$

where

$$w(a) = \prod_{\substack{p\mid b\\ p\in\mathcal{P}}}\frac{1}{2}\Big(1+\Big(\frac{a}{p}\Big)\Big)\ .$$

Note that $w(a)$ is the characteristic function of the condition (11) for primes $p \in \mathcal{P}$. This sum can be viewed as the sifted sum $S(\mathcal{A}, A)$ for the sequence $\mathcal{A} = w(a)$ over integers a with $2ab$ squarefree, sifted by the set of primes $\mathcal{P}_b$.

The sieve requires a good approximation for the congruence sums

$$A_d = \sum_{\substack{a\leqslant A\\ (a,2b)=1\\ a\equiv 0\,(d)}}^{\flat} w(a)$$

for d squarefree, $(d, 2b) = 1$. Here $\flat$ restricts the summation to squarefree integers. Since $w(a)$ is periodic with period b we have

$$A_d = \sum_{\beta\,(\mathrm{mod}\ 2b)}^{*} w(\beta)\sum_{\substack{a\leqslant A\\ a\equiv\beta\,(2b)\\ a\equiv 0\,(d)}}^{\flat} 1\ .$$

The inner sum is equal to

$$\sum\nolimits^{\flat} = \sum_{\substack{a\leqslant A/d\\ a\equiv\beta\bar{d}\,(2b)\\ (a,2bd)=1}}^{\flat} 1 = \sum_{(\alpha,2bd)=1}\mu(\alpha)\sum_{\delta|d}\mu(\delta)\sum_{\substack{a\leqslant A/d\alpha^2\delta\\ \alpha\equiv\beta'\,(2b)}} 1$$

$$= \sum_{\substack{\alpha<\sqrt{A/d}\\ (\alpha,2bd)=1}}\mu(\alpha)\sum_{\delta|d}\mu(\delta)\Big(\frac{A}{2bd\alpha^2\delta}+O(1)\Big)$$

$$= \frac{A}{2bd}\frac{\varphi(d)}{d}\prod_{p\nmid 2bd}\Big(1-\frac{1}{p^2}\Big)+O\big(\tau(d)\sqrt{A/d}\big)$$

$$= \frac{2A}{3\zeta(2)bd}\prod_{p|b}\Big(1-\frac{1}{p^2}\Big)\prod_{p|d}\Big(1+\frac{1}{p}\Big)^{-1}+O\big(\tau(d)\sqrt{A/d}\big)\ .$$

We have

$$\sum_{\beta\,(\mathrm{mod}\ 2b)}^{*} w(\beta) = \frac{1}{\tau_{\mathcal{P}}(b)}\sum_{\beta\,(\mathrm{mod}\ 2b)}^{*}\sum_{\substack{m|b\\ m|P}}\Big(\frac{\beta}{m}\Big) = \frac{\varphi(b)}{\tau_{\mathcal{P}}(b)}$$

where P is the product of the primes in $\mathcal{P}$ and $\tau_{\mathcal{P}}(b)$ denotes the number of divisors of b composed of primes in $\mathcal{P}$. Hence, we conclude that

$$A_d = \frac{2bg(bd)A}{3\zeta(2)\tau_{\mathcal{P}}(b)}+O\big(\tau(d)\sqrt{A/d}\big)\ , \tag{29}$$

where g is the multiplicative function given by

$$g(p) = \big(p+1\big)^{-1}\ , \tag{30}$$

and the implied constant depends on b. The approximation (29) also holds trivially for d not squarefree in which case we set $g(d)=0$ because $A_d = 0$ and hence so does the remainder term. Therefore we can write $A_d = Xg(d)+r_d$ where

$$X = \frac{2bg(b)A}{3\zeta(2)\tau_{\mathcal{P}}(b)}$$

and

$$\sum_{\substack{d\leqslant D\\ (d,2b)=1}}|r_d| \ll \sqrt{AD}\log D\ .$$

In sieve terminology this means that our sequence has level of distribution

$$D = A\big(\log A\big)^{-4}\ .$$

The sieve needed here has dimension $\kappa < 1/2$ which is very convenient for lower bounds and as a result we obtain Theorem 4. The precise sieve statement appears in a forthcoming book on sieve methods by the authors.

The full details of this result are entwined in the book so thoroughly as to make impractical their inclusion here. Alternatively, see [5].

One could also try to prove Theorem 4 using the theory of multiplicative functions. However, the lack of multiplicativity of the function $w(a)$ makes it unclear how to proceed without giving up positivity. On the other hand, the sieve is more flexible in this regard; actually it also can be used to treat the problem for more general sequences of coefficients a.

8. Proof of Lemma 1

The sum (14) is given by Perron's formula, cf page 60 of [8]:

$$\frac{1}{2\pi i}\int_{2-iT}^{2+iT} Z_d(s,\chi)\frac{x^s}{s}ds + O\Big(\frac{x}{T}\log x\Big)\ ,$$

with any $1 \leqslant T \leqslant x$, where $Z_d(s,\chi)$ is the corresponding generating Dirichlet series

$$\begin{aligned} Z_d(s,\chi) &= \sum_{(n,d)=1} \mu^2(n)\frac{\chi(n)}{\tau(n)}n^{-s} = \prod_{p\nmid d}\Big(1+\frac{\chi(p)}{2p^s}\Big) \\ &= \prod_{p\mid d}\Big(1+\frac{\chi(p)}{2p^s}\Big)^{-1} L(s,\chi)^{\frac12}R(s,\chi)\ , \end{aligned}$$

and $R(s,\chi)$ is given by the Euler product

$$R(s,\chi) = \prod_p \Big(1+\frac{\chi(p)}{2p^s}\Big)\Big(1-\frac{\chi(p)}{p^s}\Big)^{\frac12}\ ,$$

which converges absolutely for $\operatorname{Re} s > \frac12$.

We move the integration to the contour consisting of the straight line segments from $2-iT$ left to $1-\eta-iT$, then upward to $1-\eta$ then to the right to $1-T^{-1}$, followed by a positively oriented circle centred at $s=1$ returning to $1-T^{-1}$, then, again on straight line segments, left to $1-\eta$, upward to $1-\eta+iT$, and finally right to $2+iT$.

We make the choices $T=\exp(c\sqrt{\log x})$ and $\eta = c(\varepsilon)/q^\varepsilon \log T$ for small ε, where the constants are chosen so that one may apply the Theorems of de la Vallée Poussin and of Siegel. By those theorems, we do not cross any singularities in this change of the contour, and, as in the proofs of those theorems, the contribution coming from those line segments not along the real line is bounded by

$$O\Big(\tau(dq)x\exp\Big(-\frac{c(\varepsilon)\log x}{q^\varepsilon\log T}\Big)(\log x)^2\Big)\ .$$

If χ is not principal then $Z_d(s,\chi)$ is holomorphic so the contribution from the integrals over the real segment cancel and that around the circle vanishes so we have no main term.

If $\chi = \chi_0 \,(\mathrm{mod}\, q)$ is principal then we have

$$Z_d(s,\chi_0) = \prod_{p\nmid dq}\Big(1+\frac{1}{2p^s}\Big) = L_{dq}(s)\zeta(s)^{\frac12}R(s)\ ,$$

where

$$L_d(s) = \prod_{p\mid d}\Big(1+\frac{1}{2p^s}\Big)^{-1}$$

and

$$R(s) = \prod_{p}\Big(1+\frac{1}{2p^s}\Big)\Big(1-\frac{1}{p^s}\Big)^{\frac12}\ .$$

Writing

$$\zeta(s) = \frac{1}{s-1}\{1+O(|s-1|)\}$$

we find that the integral on the small circle is bounded by $O(\tau(dq)x/\sqrt{T})$ which is admissible and it remains to estimate the integrals on the real segments which, in case of the principal character, do not cancel.

For, $s=\sigma\pm\varepsilon i$ with $\frac23\leqslant\sigma<1$ and $\varepsilon>0$, $\varepsilon\to0$,

$$\zeta(s)^{\frac12} = \frac{\mp i}{\sqrt{1-\sigma}}\left\{1+O(1-\sigma)\right\}\ ,$$

respectively. On the same segment we also have

$$R(s) = R(1)\{1+O(1-\sigma)\},\qquad s^{-1} = 1+O(1-\sigma)\ ,$$

and

$$L_d(s) = \sum_{h\mid d^\infty}\frac{a(h)}{h^s} = \sum_{\substack{h\mid d^\infty\\ h\leqslant\sqrt{x}}}\frac{a(h)}{h^s} + O\Big(\frac{\tau(d)^{\frac14}}{x}\Big)\ ,$$

where $|a(h)|\leqslant 1/\tau(h)$.

We require the following formulae:

$$\begin{aligned}\int_{1-\eta}^1\frac{y^\sigma}{\sqrt{1-\sigma}}\,d\sigma &= \int_{-\infty}^1\frac{y^\sigma}{\sqrt{1-\sigma}}\,d\sigma + O(y^{1-\eta})\\ &= \frac{\sqrt{\pi}y}{\sqrt{\log y}} + O(y^{1-\eta})\ ,\end{aligned}$$

and similarly,

$$\int_{1-\eta}^1 y^\sigma\sqrt{1-\sigma}\,d\sigma \leqslant \int_{-\infty}^1 y^\sigma\sqrt{1-\sigma}\,d\sigma = \frac{\pi y}{2(\log y)^{\frac32}}\ ,$$

for any $y\geqslant 2$. We shall apply these for $y=x/h,\ h\leqslant\sqrt{x}$. Letting $\mathcal{C}$ denote the part of the contour running over the real line segments, we find that

the corresponding integral $(1/2\pi i)\int_{\mathcal{C}}$ is given by

$$\frac{R(1)}{\pi}\int_{1-\eta}^{1}\frac{x^{\sigma}}{\sqrt{1-\sigma}}\Big\{\sum_{\substack{h\mid(dq)^{\infty}\\ h\leqslant\sqrt{x}}}\frac{a(h)}{h^{\sigma}}+O\Big(\frac{\tau(dq)}{x^{\frac{1}{4}}}\Big)\Big\}\{1+O(1-\sigma)\}\,d\sigma$$

$$=\frac{R(1)}{\pi}\sum_{\substack{h\mid(dq)^{\infty}\\ h\leqslant\sqrt{x}}}a(h)\Big\{\frac{\sqrt{\pi}x/h}{\sqrt{\log x/h}}\Big(1+O(\frac{1}{\log x})\Big)+O\Big((x/h)^{1-\eta}\Big)\Big\}$$

$$+O\big(x^{\frac{3}{4}}\tau(dq)\big)\ .$$

In the sum over h we replace

$$\frac{1}{\sqrt{\log x/h}}=\frac{1}{\sqrt{\log x}}\Big(1+O\Big(\frac{\log h}{\log x}\Big)\Big)\ ,$$

and then expand the sum over h to all $h\mid(dq)^{\infty}$. The leading term gives $L_{dq}(1)$ and the tail of the series is bounded by $O(x^{3/4}\log 2dq)$.

To estimate the contribution from the error term $O\big(\frac{\log h}{\log x}\big)$ we use

$$\sum_{h\mid(dq)^{\infty}}\frac{|a(h)|}{h}\log h=-\Big(\prod_{p\mid dq}(1-\frac{1}{2p^{s}})^{-1}\Big)'_{s=1}$$

$$\ll\prod_{p\mid dq}(1-\frac{1}{2p})^{-1}\sum_{p\mid dq}\frac{\log p}{p}\ ,$$

together with the bounds

$$\prod_{p\mid r}\Big(1-\frac{1}{p}\Big)^{-1}\ll\log\log 3r\ ,\qquad\sum_{p\mid r}\frac{\log p}{p}\ll\log\log 3r\ .$$

Putting these together we obtain

$$\frac{1}{2\pi i}\int_{\mathcal{C}}=\frac{R(1)}{\sqrt{\pi}}L_{dq}(1)\frac{x}{\sqrt{\log x}}\Big\{1+O\Big(\frac{x(\log\log 3dq)^{\frac{3}{2}}}{\log x}\Big)\Big\}$$

$$+O\big(x^{\frac{3}{4}}\tau(dq)\big)+O(x^{1-\eta/2})\ .$$

This completes the proof of Lemma 1. The corollary follows at once by the orthogonality relation for Dirichlet characters modulo q_1.

9. Proof of Lemma 2

We denote by $\mathcal{B}(M,N)$ the sum on the left hand side of (17). By symmetry we can assume $M\geqslant N$. We apply Hölder's inequality, obtaining

$$\big|\mathcal{B}(M,N)\big|^{3}\leqslant N^{2}\sum_{n}|\sum_{m}|^{3}\leqslant N^{2}\sum_{m_1}\sum_{m_2}\sum_{m_3}\Big|\sum_{n}\gamma_n\Big(\frac{m_1m_2m_3}{n}\Big)\Big|\ ,$$

where $|\gamma_n|\leqslant 1$.

Next, we rid ourselves of the remaining set of unknown coefficients by applying Cauchy's inequality. This gives

$$\begin{aligned}|\mathcal{B}(M,N)|^6 &\leqslant N^4 \sum_{m_1}\sum_{m_2}\sum_{m_3} \tau_3(m_1m_2m_3) \sum_{\ell\leqslant M^3} \Big|\sum_n \gamma_n\Big(\frac{\ell}{n}\Big)\Big|^2 \\ &\ll N^4M^3(\log 2M)^6 \sum_{n_1}\sum_{n_2}\Big|\sum_\ell \Big(\frac{\ell}{n_1n_2}\Big)\Big| \\ &\ll N^4M^3(\log 2M)^6\Big(M^3 \sum_{n_1n_2=\square} 1 + N^4\Big)\ .\end{aligned}$$

Since the last sum, the number of solutions to $n_1n_2 = \square$, is $\ll N\log N$, this completes the proof.

10. Proof of Lemma 3

By partial summation we obtain

$$\sum_{p\leqslant x} f(p)\log p \ll (\alpha+\beta)x\ .$$

Hence, for any $1 \leqslant y \leqslant x$ we have

$$\begin{aligned}S(y) = \sum_{m\leqslant y} \mu^2(m)f(m)\log m &= \sum\sum_{np\leqslant y} \mu^2(np)f(np)\log p \\ &\ll (\alpha+\beta)\, y \sum_{n\leqslant y} \frac{\mu^2(n)}{n} f(n) \\ &\leqslant (\alpha+\beta)\, y \prod_{p\leqslant x}\Big(1+\frac{f(p)}{p}\Big)\ .\end{aligned}$$

By partial summation we can remove the log factor and the lemma follows.

References

[1] COJOCARU A. C. AND MURTY M. R., *An Introduction to Sieve Methods and their Applications*. London Math. Soc. Student Texts **66**. Cambridge University Press, Cambridge, 2005.

[2] GUO C. R., *On solvability of ternary quadratic forms*. Proc. London Math. Soc. **70** (1995), 241–263.

[3] FOUVRY É. AND KLÜNERS J., *On the 4-rank of class groups of quadratic number fields*. Invent. Math. **167** (2007), 455–513.

[4] HEILBRONN H., *On the averages of some arithmetical functions of two variables*. Mathematika **5** (1958), 1–7.

[5] IWANIEC H., *Rosser's sieve*. Acta Arith. **36** (1980), 171–202.

[6] SERRE J–P., *A Course of Arithmetic*. Springer, New York, 1973.

[7] SERRE J–P., *Spécialisation des éléments de* $\mathrm{Br}_2(Q(T_1,\cdots,T_n))$. C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), 397–402.

[8] TITCHMARSH E. C., *The Theory of the Riemann Zeta-Function*, 2nd ed., revised by D.R. Heath-Brown. Clarendon Press, Oxford, 1986.

John Friedlander
University of Toronto
40 St. George Street
Toronto, ON M5S 2E4, Canada
E-mail: frdlndr@math.toronto.edu

Henryk Iwaniec
Department of Mathematics
Rutgers University
110 Frelinghuysen Rd.
Piscataway, NJ 08903, USA
E-mail: iwaniec@math.rutgers.edu