ON THE NUMBER OF BINARY QUADRATIC FORMS HAVING DISCRIMINANT $1 - 4p$, $p$ PRIME

ALISON BETH MILLER AND STANLEY YAO XIAO

Abstract. In this paper we obtain an asymptotic formula for the number of $SL_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ having bounded discriminant $\Delta = 1 - 4p$, with $p$ a prime. This extends work of the first named author and has an application in counting simple $(4a + 1)$-knots of genus one.

1. Introduction

In [9], the first named author gave an account of a connection between simple $(4a + 1)$-knots of genus 1 and Alexander polynomial

$$\Delta_m(t) = mt^2 - (2m - 1)t + m, \quad m \in \mathbb{Z},$$

and binary quadratic forms of discriminant $1 - 4m$ (note that this is also the discriminant of the quadratic $\Delta_m$). In particular, there is a surjective map from such binary quadratic forms to such knots, which is injective exactly when $m = \pm p$ is a prime or negative prime, and otherwise is expected to have large kernel. As a consequence, the first named author gave interesting heuristics that showed knots with Alexander polynomial $\Delta_p(t)$ with $p$ prime should dominate the total count of such knots up to isomorphism. Determining the size of the heuristically dominant term leads to the following question, which is purely about definite binary quadratic forms:

Question: How many $SL_2(\mathbb{Z})$-classes of integral, positive definite binary quadratic forms are there whose discriminant is of the form $1 - 4p$ with $p$ prime, and bounded by $X$?

Note that here the binary quadratic forms are allowed to be imprimitive; there is no obvious topological interpretation for primitivity of the quadratic form associated to a knot. If we write $H(D)$ for the total number of $SL_2$-equivalence classes of positive definite binary quadratic forms of discriminant $D$ (this is almost the same as the Hurwitz class number, except that we are not weighting the forms that have automorphisms, and has the same asymptotics), our question asks: what is $\sum_{p \leq X} H(1 - 4p)$?

The previous paper [9] conjectured that the answer should be asymptotic to $X^{3/2}/\log X$, based on the heuristic assumption that class numbers $H(1 - 4p)$, $p$ prime, have the same statistical behaviour as the class numbers $H(1 - 4m)$ for all $m$. It applied a sieve to prove an upper bound of the form $O(X^{3/2}/\log X)$, without determining the constant explicitly. In this paper we give an exact asymptotic for the counting problem.

Theorem 1.1. We have the asymptotic formula

$$\sum_{p \leq X} H(1 - 4p) = C_{\text{Art}} \cdot \frac{2\pi}{9} \cdot \frac{X^{3/2}}{\log X} + O\left(\frac{X^{3/2}}{(\log X)^2}\right).$$

Here the constant $C_{\text{Art}}$ is Artin’s constant, given by the Euler product

$$C_{\text{Art}} = \prod_{\ell \geq 2} \left(1 - \frac{1}{\ell(\ell - 1)}\right).$$

This shows that the heuristic assumption in [9] is not quite right. Comparing with the asymptotic $\sum_{m \leq X} H(1 - 4m) = \frac{4\pi}{9} X^{3/2}$, we see that the class numbers $H(1 - 4p)$ are smaller on average than the class numbers $H(1 - 4m)$ by a factor of Artin’s constant $C_{\text{Art}}$.

Artin’s constant originally arose in the context of Artin’s conjecture on primitive roots [6], namely predicting the proportion of primes $\ell$ for which a given integer $a \neq \pm 1$ is a primitive root mod $\ell$ (this proportion
is expected to be independent of \( a \). We do not know of a direct connection between Theorem 1.1 and Artin’s conjecture.

Similar problems were considered by Friedlander and Iwaniec in [5], for the case of discriminants of the form \(-4p\), and by Nagoshi in [11] for discriminants of the form \(-p \equiv 1 \pmod{4}\) (Nagoshi notably computed all moments). Our second proof, using the analytic class number formula, is inspired by these proofs. However, in implementing this strategy we encounter additional complications: where Friedlander-Iwaniec and Nagoshi obtain a single main term, we end up with infinitely many main terms, which we must sum to obtain the final answer. These come from two sources: both because we are including non-primitive forms in our count, and because numbers of the form \( 1 - 4p \), unlike primes, are slightly more likely to be quadratic residues modulo a prime \( \ell \) than they are to be residues.

We expand on this point. While in previous works restricting to primes did not affect the average size of the class number, in our case it does, producing a factor of \( C_{\text{Art}} \) that does not appear in the total count of all binary quadratic forms.

1.1. Outline of the proofs. We will in fact give two proofs of the main theorem, one where we count in the fundamental domain of \( \text{SL}_2(\mathbb{Z}) \)-classes of positive definite binary quadratic forms having absolute discriminant bounded by \( X \), and one which computes using the class number formula. The reason for this redundancy is that the two approaches have distinct advantages: the former requires an explicit equidistribution result for roots of quadratic polynomials and gives us an opportunity to record such a result in the literature. In fact the result is easily deduced from the work of Hooley [6]. The latter approach has the advantage that it is computationally less intensive.

The first proof goes on by counting integral points in the classical Gauss fundamental domain directly. The trick is to write the discriminant equation

\[
4ac - b^2 = 4p - 1
\]

as

\[
ac = k^2 + k + p,
\]

where \( b = 2k + 1 \). Thus one reduces the problem to estimating a divisor sum of the shape

\[
\sum_{p \leq X} \sum_{k} d(k^2 + k + p).
\]

Such a sum is well within the purview of modern analytic number theory; see for example [7] for a recent example. However, the issue is that the region we are counting in is somewhat irregular in shape and so some thought is required to write down sums that can be evaluated precisely.

The key idea to do this is to note that

\[
\# \{ k \pmod{a} : a | k^2 + k + p \} = \sum_{m | a} \left( \frac{1 - 4p}{m} \right).
\]

This reduces our counting problem to evaluating sums of the shape

\[
\sum_{p} \sum_{a} \sum_{m | a} \left( \frac{1 - 4p}{m} \right).
\]

Unfortunately, sometimes we do not sum over a complete set of residues mod \( a \), so we will require an equidistribution result. Such equidistribution results are well-known; see for example the seminal work of Hooley [6]. We require an explicit error term with good dependence on \( p \), which does not appear to be in the literature. Fortunately such an estimate follows easily from Hooley’s argument in [6], and we have recorded it here as Proposition 2.5.

The rest of the argument relies on applying oscillation lemmas of sums involving Jacobi symbols and the Siegel-Walfisz theorem.
Our second proof counts binary quadratic forms with the analytic class number formula

\[ h(D) = \frac{1}{\pi} L(1, \chi_D) |D|^{1/2} \]

for negative discriminant \( D \). This formula applies to non-maximal orders, but here \( h(D) \) only counts the primitive binary quadratic forms of discriminant \( D \). Since we want to count all binary quadratic forms, our first step is to write our sum \( Q(X) = \sum_{d \geq 1} Q_d(X) \), where \( Q_d(X) \) counts only the forms \( ax^2 + bxy + cy^2 \) with content \( \gcd(a, b, c) = d \). To estimate \( Q_d(X) \), we first estimate the related quantity \( T_d(X) = \sum_{d \mid 1-4p} L(1, \chi((1 - 4p)/d^2)) \), and then apply Abel summation to the sum over \( p \).

This reduces our problem to bounding

\[ T_d(X) = \sum_{p \leq X, d^2 \mid 1-4p} L(1, \chi((1 - 4p)/d^2)) = \sum_{p \leq X, d^2 \mid 1-4p} \sum_{n \geq 1} \frac{1}{n} \left( \frac{(1 - 4p)/d^2}{n} \right). \]

As in the first method, we have a double sum of quadratic residue symbols, though now it is weighted, and the strategies we apply are similar to the first approach. We are able to cut off the sums in the \( L \)-functions at \( n \sim X^{1/2+\varepsilon} \). We then show that the range \( (\log X)^B < n < X^{1/2+\varepsilon} \) yields an error term by dividing it into dyadic intervals and using double oscillation lemma on each. Finally, for \( n \leq (\log X)^B \) we use Siegel-Walfisz to estimate the sum over \( p \); this sum is generally nonzero, so we then have to combine our Siegel-Walfisz main terms into one big main term.

1.2. Motivation from and application to knot theory. This line of research was originally motivated by a question related to knot theory. We sketch the appropriate background (See section 2 of [9] for more details.) and state the implications of our results in terms of knots and knot invariants.

Roughly speaking, an \( n \)-knot is a “nicely” embedded copy of \( S^n \) in \( S^{n+2} \), up to topological equivalence. (Here it matters that we keep track of the orientations both on \( S^n \) and \( S^{n+2} \).) The most well-known case is that of \( n = 1 \), where the classification of knots and study of their invariants is an extremely rich and active field. In higher dimensions, the study of all knots only gets more complicated, but certain special families of knots are well understood, in particular the simple \( n \)-knots, which are those for which the first \( \lfloor \frac{n}{2} \rfloor \) homotopy groups of the knot complement are “as trivial as possible” (explicitly, \( \pi_1 \) is isomorphic to \( \mathbb{Z} \) and \( \pi_i \) is trivial for \( 2 \leq i \leq \frac{n}{2} \)).

For \( n = 5 \) and \( n \geq 7 \), simple \( n \)-knots have been completely classified in terms of algebraic data: notably, this classification only depends on the dimension \( n \) modulo 4. Simple knots have a fundamental invariant, the Alexander polynomial, and Bayer and Michel proved that for a squarefree polynomial \( \Delta \in \mathbb{Z}[t] \), there are only finitely many simple \( n \)-knots with Alexander polynomial \( \Delta \).

The paper [9] studied simple \((4a+1)\)-knots of genus 1, for fixed \( a \geq 1 \) (as noted above the classification does not depend on \( a \)). These are exactly the simple \((4a+1)\)-knots with Alexander polynomial \( \Delta_m = mt^2 + (1 - 2m)t + m \) for some nonzero integer \( m \). Using the algebraic classification of simple \((4a+1)\)-knots, in [9] the first named author showed that:

**Theorem 1.2** ([9] Theorem 2.5 (vi), Corollary 2.13). Simple \((4a+1)\)-knots with Alexander polynomial \( \Delta_m \) are in bijection with \( \text{SL}_2(\mathbb{Z}[1/m]) \)-equivalence classes of binary quadratic forms over \( \mathbb{Z}[1/m] \) of discriminant \( 1 - 4m \).

Furthermore, when \( m = p \) is prime, \( \text{SL}_2(\mathbb{Z}[1/p]) \)-equivalence classes of binary quadratic forms of discriminant \( 1 - 4m \) over \( \mathbb{Z}[1/m] \) are naturally identified with \( \text{SL}_2(\mathbb{Z}) \)-equivalence classes of binary quadratic forms over \( \mathbb{Z} \) of discriminant \( 1 - 4p \).

Combining this with our Theorem 1.1 and including a factor of 2 as we are allowing both positive and negative definite forms,

**Corollary 1.3.** The total number of simple \((4a+1)\)-knots of genus 1 with Alexander polynomial \( pt^2 + (1 - 2p)t + p \) for \( p \in [1, X] \) prime is \( \sim C_{\text{Art}} \frac{4X}{\pi} X^{3/2} / (\log X) \).
The heuristics of \cite{9} indicate that most simple knots of genus 1 (ordered by the height of the Alexander polynomial) should have Alexander polynomial of this form. That is, the total number of \((4a + 1)\)-knots of genus 1 with Alexander polynomial \(mt^2 + (1 - 2m)t + m\) for \(m \in [-X, X]\) should also be \(C_{\text{Art}} \frac{48X^{3/2}}{\log X} + O(X^{3/2}/\log(X))\). It is an interesting question for future research to see if this can be proven: showing it will require getting some control on the sizes of the oriented class groups of the rings \(\mathbb{Z} \left[ \frac{1}{m} \right]^{1 + \sqrt{1 - 1/m}}\), which is more complicated when \(m\) is not prime.

Finally, we note that the algebraic invariants (the Alexander module and Blanchfield pairing, or equivalently the Seifert matrix) used to classify \((4a + 1)\)-knots for \(a \geq 1\) are also useful in the low-dimensional case \(a = 0\), though they are no longer complete invariants of the knot, and miss a lot of knot-theoretic information. Indeed, \((4a + 1)\)-knots for fixed \(a \geq 1\) are in bijection with \(S\)-equivalence classes of Seifert forms \([9][\text{Theorem 2.4}].\)

This allows us to restate the previous corollary in terms of objects of interest to low-dimensional topologists:

**Corollary 1.4.** The number of \(S\)-equivalence classes of \(2 \times 2\) Seifert matrices \(P\) with Alexander polynomial \(\det(tp - Pt) = pt^2 + (1 - 2p)t + p\) for \(p \in [1, X]\) prime is \(\sim C_{\text{Art}} \frac{42\pi}{9} X^{3/2}/(\log X)\).

## 2. Preliminary Lemmas

In this section we state several technical lemmas and propositions which will be needed for our proofs of Theorem 1.1. Some of the statements that follow will be classical and well-known, while some are new results. In particular, we believe that Proposition 2.5 and Lemma 2.2 are new. We give proofs for these results in this section.

### 2.1. An Unrestricted Version of the Double Oscillation Lemma

We begin with the statement of the following well-known lemma:

**Lemma 2.1** (Double Oscillation Lemma). Let \(\{\alpha_m\}, \{\beta_m\}\) be two sequences of complex numbers with each term having absolute value bounded by 1. Let \(M, N\) be positive real numbers. Then we have

\[
\sum_{m \leq M} \sum_{n \leq N} \alpha_m\beta_n \mu^2(2m)\mu^2(2n) \left( \frac{m}{n} \right) \ll MN \min \left\{ \left( M^{-1/2} + (N/M)^{-1/2} \right), \left( N^{-1/2} + (M/N)^{-1/2} \right) \right\}
\]

and for every \(\varepsilon > 0\),

\[
\sum_{m \leq M} \sum_{n \leq N} \alpha_m\beta_n \mu^2(2m)\mu^2(2n) \left( \frac{m}{n} \right) \ll \varepsilon MN \left( M^{-1/2} + N^{-1/2} \right) (MN)^\varepsilon
\]

**Lemma 2.1** essentially follows from the Polya-Vinogradov inequality. There are several instances in this paper where Lemma 2.1 is needed. However, the sharpest form of Lemma 2.1 requires that the sum is supported on odd squarefree numbers. We observe here that applying a squarefree sieve allows us to remove this restriction at the cost of a logarithmic factor, which is often an acceptable loss. We thus obtain the following version of Lemma 2.1

**Lemma 2.2** (Unrestricted Double Oscillation Lemma). Let \(\{\alpha_m\}, \{\beta_m\}\) be two sequences of complex numbers with each term having absolute value bounded by 1. Let \(M, N\) be positive real numbers. Then we have

\[
\sum_{m \leq M} \sum_{n \leq N} \alpha_m\beta_n \left( \frac{m}{n} \right) \ll MN (\log M + \log N) \min \left\{ \left( M^{-1/2} + (N/M)^{-1/2} \right), \left( N^{-1/2} + (M/N)^{-1/2} \right) \right\}
\]

**Proof of Lemma 2.2** We first note that, with minor modifications to the constant, we can easily get rid of the restriction that \(m\) and \(n\) must be odd, since every even squarefree number is twice an odd squarefree number. Getting rid of the squarefree restriction takes more work.
By symmetry, it is enough to show that our left hand side \( \Xi(M, N) = \sum_{m \leq M} \sum_{n \leq N} \alpha_m \beta_n \) satisfies 
\[
\Xi(M, N) \ll (M^{1/2}N + M^{3/2}N^{1/2})(\log M + \log N).
\]

We then decompose \( \Xi(M, N) \) as 
\[
\Xi(M, N) = \sum_{k \leq \sqrt{M}} \sum_{\ell \leq \sqrt{N}} \Xi_{k, \ell}(M, N)
\]
where 
\[
\Xi_{k, \ell}(M, N) = \sum_{m' \leq k^{-2}M \text{ squarefree}} \sum_{n' \leq \ell^{-2}M \text{ squarefree}} \alpha_{k^2m'} \beta_{\ell n'} \left( \frac{k^2m'}{\ell^2n'} \right).
\]
is the total contribution from all pairs \((m, n)\) of the form \((k^2m', \ell^2n')\) with \(m'\) and \(n'\) squarefree. Since \(m'\) and \(n'\) are now restricted to be squarefree, we can apply double cancellation to obtain 
\[
\Xi_{k, \ell}(M, N) \ll (k^{-1}\ell^{-2}M^{1/2}N + \ell^{-3}k^{-1}M^{3/2}N^{1/2}).
\]

Summing over \(k, \ell\) gives the bound 
\[
\Xi(M, N) \ll \sum_{k \leq \sqrt{M}} \sum_{\ell \leq \sqrt{N}} (k^{-1}\ell^{-2}M^{1/2}N + \ell^{-3}k^{-1}M^{3/2}N^{1/2}) \ll \log(M)M^{1/2}N + \log(N)M^{3/2}N^{1/2},
\]
which is of the size needed.

\[\square\]

2.2. A Siegel-Walfisz-type lemma. As is well-known by now, in problems involving summations over Jacobi symbols where both arguments are variable, it is often necessary to consider the sum over just one variable. In such cases Lemma 2.1 does not apply, and so we will require the following result which is derived from the Siegel-Walfisz theorem:

Lemma 2.3 (Siegel-Walfisz). For every \(q \geq 2\) and for every primitive character \(\chi \mod q\), we have that for any \(A > 0\) the estimate 
\[
\sum_{Y \leq p \leq X} \chi(p) \ll \sqrt{q}X(\log X)^{-A}
\]
uniformly for \(X \geq Y \geq 2\).

Although Lemma 2.3 applies to character sums over primes evaluated at prime arguments, we can easily modify the lemma to the sum \(\sum_{Y \leq p \leq X} \chi(1 - 4p)\) when \(\chi\) has odd conductor \(m\) say. Therefore 4 is invertible mod \(m\) and the map \(x \mapsto 1 - 4x\) is invertible mod \(m\).

However, in the sum \(\sum_{Y < p < X} \chi_m(p)\) we note that for \(Y > m\) the prime \(p\) never divides by \(m\), whence the 0-class never appears. Correspondingly, the 1 mod \(m\) class never appears for \(1 - 4p\) since that would imply \(m|p\), as \(m\) is odd.

If \(m = \ell\) is an odd prime, then the map \(L : x \mapsto 1 - 4x\) sends the set of primitive residues \(\{1, \ldots, \ell - 1\}\) to \(\{0, 2, \ldots, \ell - 1\}\). Indeed, there are \((p - 1)/2\) residues \(k\) each such that \(\left( \frac{k}{\ell} \right) = \pm 1\), and the image of the map contains \((p - 1)/2\) residues giving \(-1\) and \((p - 3)/2\) residues giving \(+1\), since 1 mod \(\ell\) is omitted. Thus there is one more \(-1\) than \(+1\).

However if \(m = \ell_1\ell_2\), then we see that there are 
\[
(f_1 - 1)(f_2 - 1)/4 + (f_1 - 3)(f_2 - 3)/4
\]
residues giving \(+1\) in the image of \(L\), and 
\[
(f_1 - 1)(f_2 - 3)/4 + (f_1 - 3)(f_2 - 1)/4
\]
giving \(-1\). Expanding, we see that 
\[
(f_1 - 1)(f_2 - 1) + (f_1 - 3)(f_2 - 3) - (f_1 - 1)(f_2 - 3) - (f_1 - 3)(f_2 - 1) = \ell_1\ell_2 - \ell_1 - \ell_2 + 1 + \ell_1\ell_2 - 3\ell_1 - 3\ell_2 + 9 - \ell_1\ell_2 + 3\ell_1 + \ell_2 - 3 - \ell_1\ell_2 + 3\ell_2 + \ell_1 - 3 = 4,
\]
so there will be one more \(+1\) than \(-1\).
The pattern continues, or to put it more formally: the function \( m \mapsto \sum_{\alpha \in (\mathbb{Z}/m)^*} \chi_m(1-4\alpha) \) is multiplicative on odd squarefree \( m \) by the Chinese remainder theorem. We deduce the following lemma:

**Lemma 2.4.** Let \( m > 1 \) be an odd, square-free integer and let \( \chi \) be a primitive character modulo \( m \). Then for any \( A > 0 \) we have the estimate

\[
\sum_{y \leq p \leq X} \chi(1-4p) = \frac{\mu(m)}{\phi(m)} (\text{Li}(X) - \text{Li}(Y)) + O_A \left( \sqrt{mX} (\log X)^{-A} \right)
\]

uniformly for \( X \geq Y \geq 2 \).

We will require the following result on the equidistribution of roots of a quadratic congruence:

**Proposition 2.5.** Let \( f \) be an irreducible quadratic polynomial, and let \( 0 \leq \alpha \leq \beta \leq 1 \) be real numbers. Put

\[
S_f(\alpha, \beta; n) = \#\{v \in \{0, \ldots, n-1\} : f(v) \equiv 0 \pmod n, \alpha n \leq v \leq \beta n\}.
\]

Then

\[
\sum_{n \leq X} S_f(\alpha, \beta; n) = (\beta - \alpha) \sum_{n \leq X} S_f(0, 1; n) + O \left( X^{8/9}(\log X)^{3} \right)
\]

The novelty of Proposition 2.5 lies in the explicit error term, the main asymptotic being well-known. The asymptotic is derived as a consequence of examining explicit estimates in [6] and then applying a method of Erdös-Turan, as recorded in Montgomery’s book [10].

**2.3. Proof of Proposition 2.5.** The proof begins with the following set-up. Let \( f(x) = ax^2 + bx + c \in \mathbb{Z}[x] \) be a positive definite, primitive quadratic polynomial. For a given positive integer \( n \) let \( S_f(\alpha, \beta; n) \) be as in (2.1), and put

\[
\rho_h(n) = \sum_{f(v) \equiv 0 \pmod n} e \left( \frac{hv}{n} \right)
\]

for \( h \in \mathbb{Z} \), where as usual \( e(s) = \exp(2\pi is) \). Put

\[
D_f(\alpha, \beta; X) = \sum_{n \leq X} S_f(\alpha, \beta; n) - (\beta - \alpha) \sum_{n \leq X} S_f(0, 1; n)
\]

and define the discrepancy to be

\[
D_f(X) = \sup_{0 \leq \alpha \leq \beta \leq 1} |D_f(\alpha, \beta; X)|.
\]

We then have the following result due to Erdös and Turan (see Chapter 1 of [10] for a reference):

**Lemma 2.6.** Let notation be as above. For all positive integers \( N \) the discrepancy \( D_f(X) \) satisfies the bound

\[
D_f(X) \leq \frac{X}{N + 1} + 3 \sum_{h = 1}^{N} \frac{1}{h} \left| \sum_{n \leq X} \rho_h(n) \right|
\]

Lemma 2.6 thus reduces the question of bounding \( D_f(\alpha, \beta; X) \) by bounding the term

\[
\left| \sum_{n \leq X} \rho_h(n) \right|
\]

It is known that (2.4) satisfies the bound \( O_{f,h}(X^{2/3}(\log X)^2) \), but for our purposes we need to make the dependence on \( f \) and \( h \) explicit. To do so we must settle with an older approach, due to Hooley [6], where this can be done, at the cost of a worse exponent of \( 3/4 \) for \( X \).

We give a brief description of Hooley’s approach in [6], being careful to extract the dependence on \( h \) and on \( f \). One begins by observing that the solutions to the congruence

\[
f(x) \equiv 0 \pmod n
\]

are in bijection with the number of representations of \( n \) by SL\(_2(\mathbb{Z})\)-inequivalent binary quadratic forms \( g \) having the same discriminant as \( f \). Indeed, for

\[
g(x, y) = a_2x^2 + a_1xy + a_0y^2, \Delta(g) = \Delta(f)
\]
It is standard (see [1] for a modern reference) that the fractions \( v/n \) corresponding to solutions to the congruence (2.5) are given by

\[
\frac{v}{n} = \frac{r}{\alpha t} - a_1 t + 2a_0 u + bt \quad \text{if } |t| > |u|,
\]

where \( ru - st = 1 \) and \( g \) runs over a set of pairwise inequivalent forms of discriminant \( \Delta(f) \). Similarly, one obtains the expression

\[
\frac{v}{n} = \frac{s}{\alpha u} - a_2 t + 2a_1 u + bt \quad \text{if } |t| < |u|.
\]

Let \( \theta(t,u) \) denote the representation of \( v/n \) given by (2.6) or (2.7). Let \( -D = \Delta(f) \), and let \( F(-D) \) denote a fundamental set of forms of discriminant \( -D \). We then have the following key formula:

\[
\sum_{n \leq X} \rho_h(n) = \sum_{g(t,u) \leq X} e(h \theta(t,u)).
\]

From here, examining Hooley’s argument in [6] reveals that the only further dependence on \( f \) comes from estimating the size of

\[
F_2(t) - F_1(t),
\]

where

\[
F_2(t) = \min \left\{ |t|, -\frac{a_1 t}{a_0} + \frac{1}{a_0} (a_0 X + Dt^2)^{1/2} \right\}
\]

and

\[
F_1(t) = \max \left\{ -|t|, -\frac{a_1 t}{a_0} - \frac{1}{a_0} (a_0 X + Dt^2)^{1/2} \right\}.
\]

We then see that

\[
F_2(t) - F_1(t) \ll |t| + \sqrt{\frac{X}{a_0}} + \sqrt{D} \cdot |t|
\]

with the implied constant being absolute. We note that since \( g \) is positive definite and reduced, we have \( a_0 \geq \sqrt{D} \), from which we obtain the simplified bound

\[
F_2(t) - F_1(t) \ll |t| + X^{1/2} D^{-1/4}.
\]

Examining the \( \max, \min \) functions in the definitions of \( F_1, F_2 \) we see that \( F_2(t) - F_1(t) \ll |t| \) with an absolute implied constant. Hooley’s argument in [6] then proceeds with an absolute implied constant, giving the bound

\[
\left| \sum_{n \leq X} \rho_h(n) \right| = O \left( |h|^{4/5} \sigma_{-1/2}^2(h) X^{4/5} (\log X)^2 \right),
\]

where \( \sigma_z(n) = \sum_{m|n} m^z \). Feeding this into (2.8) we obtain the bound

\[
O \left( X^{4/5} (\log X)^2 \sum_{1 \leq h \leq N} \frac{\sigma_{-1/2}^2(h)}{h^{1/5}} \right),
\]

which is the same estimate as in equation (41) in [6]. Optimizing for \( N \) in (2.8) we obtain

\[
D_f(X) = O \left( X^{8/9} (\log X)^3 \right),
\]

with absolute implied constant.
3. Counting in a fundamental domain

We now begin the first of two proofs of our main theorem. By the fundamental work of Gauss, we may parametrize \( SL_2(\mathbb{Z}) \)-equivalence classes of positive definite binary quadratic forms having discriminant bounded by \( X \) by integral points in some bounded domain:

\[
F(X) = \{(a, b, c) \in \mathbb{Z}^3 : |b| \leq a \leq c, a, c > 0, 0 < 4ac - b^2 \leq X \}.
\]

(3.1)

We remark immediately that

\[
4p - 1 = 4ac - b^2 \geq 4ac - a^2 \geq 3a^2,
\]

whence

\[
a \leq \sqrt{\frac{4p}{3}}.
\]

(3.2)

We are interested in integral points in \( F(X) \) for which

\[
4ac - b^2 = 4p - 1,
\]

where \( p \) is a prime. Clearly, this equation implies that \( b \) is odd, say \( b = 2k + 1 \). We then have the expression

\[
ac = k^2 + k + p.
\]

That the triple \((a, b, c) = (a, 2k + 1, c) \in F(X)\) implies

\[
|2k + 1| \leq a \leq \sqrt{4p/3},
\]

from which we obtain

\[
|k| \leq \frac{a - 1}{2}.
\]

(3.3)

Next note that

\[
4p - 1 = 4ac - b^2 \geq 4a^2 - b^2,
\]

hence

\[
b^2 \geq 4a^2 - 4p + 1.
\]

This lower bound is non-trivial if and only if \( a \geq \sqrt{p} \). In this case we obtain

\[
k^2 + k \geq a^2 - p,
\]

or equivalently,

\[
|k| \geq \sqrt{a^2 - p}.
\]

(3.4)

We are then led to the following sum

\[
Q(X) = \sum_{p \leq X} \left( \sum_{1 \leq a \leq \sqrt{p}} \sum_{|k| \leq a/2} 1 + \sum_{\sqrt{p} \leq a \leq \sqrt{4p/3}} \sum_{\frac{a(k^2 + k + p)}{\sqrt{a^2 - p} \leq |k| \leq a/2}} 1 \right)
\]

\[
= \sum_{p \leq X} (T_1(p) + T_2(p))
\]

\[
= Q_1(X) + Q_2(X),
\]

say.

The term \( Q_1(X) \) is already in the shape that we want, since the inner sum runs over a complete set of residues. More work, indeed, a substantial amount of work, is needed to get \( Q_2(X) \), and in particular \( T_2(p) \) into an acceptable form.

To treat \( T_2(p) \), we partition the interval \([\sqrt{p}, \sqrt{4p/3}]\) into subintervals of the shape

\[
[\kappa \sqrt{p}, (\kappa + N^{-1}) \sqrt{p})
\]
with 1 ≤ κ ≤ 2/√3 and N a large positive integer (which may depend on X). We want to estimate the sum
\[ T_2(\kappa; p) = \sum_{\kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}} \sum_{a \mid k^2 + k + p} 1. \]

Writing \( a = \sqrt{p}(\kappa + \delta) \) with \( \delta = O(N^{-1}) \) we find that
\[ \sqrt{p} = \frac{a}{\kappa + \delta} = \frac{a}{\kappa} (1 + O(N^{-1})) , \]
whence
\[ a \sqrt{1 - \kappa^{-2} + O(N^{-1})} \leq |k| \leq a/2. \]

Note that
\[ \sqrt{1 - \kappa^{-2} + O(N^{-1})} - \sqrt{1 - \kappa^{-2}} = \frac{1 - \kappa^{-2} + O(N^{-1}) - 1 + \kappa^{-2}}{\sqrt{1 - \kappa^{-2} + O(N^{-1})} + \sqrt{1 - \kappa^{-2}}} = O(N^{-1}). \]

We write
\[ T_2(\kappa; p) = \sum_{\kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}} \sum_{a \sqrt{1 - \kappa^{-2} \leq |k| \leq a/2}} 1. \]

We see that
\[ \sum_{p \leq X} \sum_{j=N}^{[2N/\sqrt{p}]} (T_2(j/N, p) - T_2^*(j/N, p)) \ll \int_1^X \int_1^{X/a} \int_1^{I_a} dbdcda, \]
where \( I_a \) is an interval of length \( O(a/N) \). The triple integral on the right satisfies
\[ \int_1^{X/a} \int_1^{I_a} dbdcda = O \left( \frac{X^{3/2}}{N} \right), \]
which will be small enough with an appropriate choice of \( N \), say \( N = \lceil (\log X)^4 \rceil \). We can then apply Proposition 2.5 to \( T_2^*(\kappa, p) \) to obtain
\[ T_2^*(\kappa, N; p) = \left( 1 - 2 \sqrt{1 - \kappa^{-2}} \right) \sum_{\kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}} \sum_{a \mid k^2 + k + p} 1 + O \left( p^{4/9} (\log p)^3 \right). \]

Summing the error term over \( p \leq X \) gives
\[ \sum_{p \leq X} p^{4/9} (\log p)^3 \ll X^{13/9} (\log X)^2. \]

We may thus focus on sums of the shape
\[ Q(\kappa, N; X) = \sum_{p \leq X} \sum_{\kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}} \sum_{a \mid k^2 + k + p} 1. \]

The innermost sum exactly counts the number of solutions to the congruence
\[ k^2 + k + p \equiv 0 \pmod{a}. \]

We know that this is given by the expression
\[ \sum_{m \mid a} \left( \frac{1 - 4p}{m} \right). \]

This gives
\[ Q(\kappa, N; X) = \sum_{p \leq X} \sum_{\kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}} \sum_{m \mid a} \left( \frac{1 - 4p}{m} \right). \]

Note that
\[ \kappa \sqrt{p} \leq a \leq (\kappa + N^{-1}) \sqrt{p}. \]
We proceed to show that
\[ \frac{a^2}{\kappa^2} \left( 1 - \frac{1}{M + 1} \right) \leq p \leq \frac{a^2}{\kappa^2}, \]

where \( M = N/\kappa \). Hence we may switch order of summation and then abuse notation to obtain

\[
Q(\kappa, M; X) = \sum_{a \leq \kappa} \sum_{a^2 (1 - M^{-1}) / \kappa^2 \leq p \leq a^2 / \kappa^2} \sum_{m|a} \left( \frac{1 - 4p}{m} \right).
\]

Writing \( Y = \kappa X^{1/2} (1 + (M - 1)^{-1}) \) for convenience and then using symmetry, we find that

\[
(3.11) \quad Q(\kappa, M; X) = \sum_{mn \leq Y} \sum_{m \leq n} \sum_{m^2 (1 - M^{-1}) / \kappa^2 \leq p \leq (mn)^2 / \kappa^2} \left( \frac{1 - 4p}{m} \right) + \left( \frac{1 - 4p}{n} \right).
\]

Our goal is to eventually take advantage of the oscillation of the Jacobi symbol; see Lemma 2.1. Before we can do so we must massage the sums \( Q(\kappa, N - 1; X) \) so that we are summing over square-free numbers, and this requires applying a square-free sieve over the terms \( m, n, 4p - 1 \). For \( m, n \) this is very easy to do but the irregularity introduced by having the variable running over primes introduces some minor difficulties.

We write

\[
(3.12) \quad Q^1(\kappa, M; X) = \sum_{mn \leq Y} \sum_{m \leq n} \sum_{m^2 (1 - M^{-1}) / \kappa^2 \leq p \leq (mn)^2 / \kappa^2} \left( \frac{1 - 4p}{m} \right) + \left( \frac{1 - 4p}{n} \right)
\]

and

\[
Q^1(\kappa, M; X) = Q(\kappa, M; X) - Q^1(\kappa, M; X).
\]

We proceed to show that \( Q^1(\kappa, M; X) \) is an error term. To do so we note that

\[
Q^1(\kappa, M; X) = \sum_{mn \leq Y} \sum_{m \leq n} \sum_{\exists k^2 | 4p - 1 \text{ s.t. } k > \xi} \left( \frac{1 - 4p}{m} \right) + \left( \frac{1 - 4p}{n} \right)
\]

\[
\leq 2 \sum_{mn \leq Y} \sum_{m \leq n} 1,
\]

where \( s \) runs over the integers instead of primes. We denote this last inner sum by \( S(X) \). We shall prove the following:

**Lemma 3.1.** We have

\[ S(X) = O \left( \frac{X}{\xi} + X^{1/2} \right) \]

**Proof.** For a fixed integer \( k \), we note that

\[
S(k; X) = \# \{ s \leq X : k^2 | 4n - 1 \}
\]

\[
= \frac{X}{k^2} + O(1).
\]

Moreover, if \( k^2 | 4n - 1 \) and \( n \leq X \), then \( k \ll X^{1/2} \). Thus

\[
S(X) \ll \sum_{\xi < k \ll X^{1/2}} \left( \frac{X}{k^2} + O(1) \right)
\]

\[
\ll \frac{X}{\xi(X)} + X^{1/2},
\]

as desired. \( \square \)
We have thus obtained the following conclusion:

**Proposition 3.2.** Let \( Q(\kappa, M; X) \) be as in (3.11) and \( Q^1(\kappa, M; X) \) be as in (3.12). Then

\[
Q(\kappa, M; X) = Q^1(\kappa, M; X) + O_A \left( \frac{X}{(\log X)^A} \right) .
\]

We denote by

\[
R_1(\kappa, M; X) = \sum_{mn \leq N} \sum_{m/n \leq \sqrt{X}/(mn^2)} \left( \frac{1 - 4p}{m} \right)
\]

and

\[
R_2(\kappa, M; X) = \sum_{mn \leq N} \sum_{m/n \leq \sqrt{X}/(mn^2)} \left( \frac{1 - 4p}{n} \right).
\]

We shall now show that \( R_1(\kappa, M; X) \) gives the expected main term (for either \( Q_1(X) \) or \( Q_2(X) \)), while \( R_2(\kappa, M; X) \) contributes negligibly. By Proposition 3.2 it suffices to consider the corresponding sums \( Q^1(\kappa, M; X), Q^2(\kappa, M; X) \), with identical restrictions on \( p \). We shall focus on the second goal for now. To show that \( Q^2(\kappa, M; X) \) is small, we shall need Lemma 2.1.

We may now deal with \( Q^2(\kappa, M; X) \). Since the Jacobi symbol depends only on \( p, n \), we do not need to worry about the \( m \)-variable. We write

\[
n = n_1n_2^2,
\]

with \( n_1 \) square-free (though not necessarily co-prime with \( n_2 \)). We then have

\[
Q^2(\kappa, M; X) = \sum_{m \leq Y^{1/2}} \sum_{m/n_2^2 \leq Y^{1/2}/m^{1/2}} \sum_{m/n_1 \leq X^{1/2}/(mn_2^2)} \sum_{\kappa \in \mathbb{Z}} \left( \frac{1 - 4p}{n_1} \right) \tag{3.13}
\]

\[
= \sum_{m \leq Y^{1/2}} \sum_{m/n_2^2 \leq Y^{1/2}/m^{1/2}} \sum_{m/n_1 \leq X^{1/2}/(mn_2^2)} \sum_{\kappa \in \mathbb{Z}} \left( \frac{1 - 4p}{n_1} \right)
\]

say.

The inner double sum in (3.13) is equal to

\[
\sum_{m/n_2^2 \leq n_1 \leq X^{1/2}/(mn_2^2)} \left( \frac{-s}{n_1} \right)
\]

which we can rewrite as

\[
\sum_{k \leq (\log X)^{2A}} \sum_{m/n_2^2 \leq n_1 \leq X^{1/2}/(mn_2^2)} \sum_{s \leq (mn_1 n_2^2)^{(1-N^{-1})}/(2\kappa k^2)} \sum_{s \text{ square-free}} \alpha_s \left( \frac{-s}{n_1} \right),
\]

where

\[
\alpha_s = \begin{cases} 1 & \text{if } (k^2s + 1)/4 \text{ is prime} \\ 0 & \text{otherwise}. \end{cases}
\]

The sum (3.14) is now amenable to Lemma 2.1 since both \( n_1, s \) are square-free. Restricting \( n_1 \) to a dyadic interval \([N_1, 2N_1]\) say we obtain the bound

\[
O_\varepsilon \left( N_1 \cdot \frac{(mn_2^2N_1^2)^{k^2}}{k^2} \left( \frac{k}{mn_2^2N_1} + \frac{1}{N_1^{1/2}} \right) X^\varepsilon \right) = O_\varepsilon \left( X^\varepsilon \left( \frac{mn_2^2N_1^2}{k} + \frac{(mn_2^2)^2N_1^{5/2}}{k^2} \right) \right).
\]

Summing over \( k \) and \( N_1 \ll X^{1/2}/mn_2^2 \) and noting that \( k = O_{A, \varepsilon}(X^\varepsilon) \), we get a total contribution at most

\[
O_{A, \varepsilon} \left( \frac{X^{5/4+\varepsilon}}{m^{1/2}n_2} \right).
\]
Feeding this back into (3.13) we see that
\[ Q_2^1(\kappa, N - 1; X) = O(\epsilon (X^{11/8 + \epsilon})). \]

We move on to estimating \( Q_1^1(\kappa, N - 1; X) \). Again we need to isolate the square-free part of \( m \). As before, write \( m = m_1m_2^2 \) with \( m_1 \) square-free. We note that
\[ Q_1^1(\kappa, N - 1; X) = \sum_{m \leq Y^{1/2}} \sum_{mn \leq X^{1/2}/m} \sum_{4p-1=k^2 s, s \text{ square-free}} \left( \frac{1 - 4p}{m} \right) \]
\[ = \sum_{n \leq Y} m_1^2 \sum_{m_2^2 \leq \min\{n, Y/n\}} \sum_{mn \leq X^{1/2}/n} \sum_{4p-1=k^2 s, s \text{ square-free}} \left( \frac{1 - 4p}{m_1} \right) \]
\[ = \sum_{n \leq Y} \sum_{1 < m_2 \leq \min\{n^{1/2}, X^{1/2}/n^{1/2}\}} \sum_{m_1 \leq Y/nm_2^2} \sum_{4p-1=k^2 s, s \text{ square-free}} \left( \frac{1 - 4p}{m_1} \right) \]
We must be more careful in our application of Lemma 2.1 since the sum over \( n \) is very long. Indeed, we must use the more precise variant of the lemma rather than the coarser but more convenient version with the \( \epsilon \), since the sum over \( m_1 \) is much shorter than the sum over \( p \). We shall consider the separate cases when \( n < X^{1/2}(\log X)^{-A} \) and when \( n > X^{1/2}(\log X)^{-A} \).

In the former case we restrict \( m_1 \) to dyadic intervals \([M_1, 2M_1]\) and then apply Lemma 2.1 Summing over \( M_1 \ll X^{1/2}/nm_2^2 \) we obtain the estimate
\[ O \left( \frac{X^{5/4}}{n^{2/3}m_2^{1/2}} + \frac{kX^{1/4}}{n^{3/2}m_2^2} \right) \]
for the inner double sum in the last line of (3.15). We put this back into (3.15) to obtain the sum
\[ \sum_{n \leq X^{1/2}(\log X)^{-A}} \sum_{m_2 \leq \min\{n, X^{1/2}/n\}} \frac{X^{5/4}}{n^{1/2}m_2^2}. \]
We then have
\[ \sum_{n \leq X^{1/2}(\log X)^{-A}} \sum_{m_2 \leq \min\{n, X^{1/2}/n\}} \frac{1}{n^{1/2}m_2^2} \ll \sum_{n \leq X^{1/2}(\log X)^{-A}} \frac{\log X}{n^{1/2}} \ll X^{1/4}(\log X)^{-A/2+1} \]
which suffices for our purposes by choosing \( A > 4 \).

When \( n > X^{1/2}(\log X)^{-A} \) the sum over \( m \) is very short: indeed, we see that \( m \ll (\log X)^A \). Thus we may use the Siegel-Walfisz theorem to handle the inner sum over \( p \). Applying Lemma 2.1 to (3.15) gives
\[ Q_1^1(\kappa, N - 1; X) = \sum_{X^{1/2}(\log X)^{-A} < n \leq Y} \sum_{m \leq Y/n} \left( \frac{\mu(m)}{\phi(m)} \int_{(mn)^2/k^2} dt + O_A \left( (\log X)^{-A} \right) \right). \]

The sum over the error term is
\[ O \left( X^{3/2}(\log X)^{-A+1} \right), \]
which is sufficiently small if we take $A > 2$. For the main term we rearrange as follows:

$$
\sum_{X^{1/2} < n \leq X} \sum_{m \leq X^{1/2} / n} \frac{\mu(m)}{\varphi(m)} \int_{t \leq t^{1/2} \mu(n)/m \leq X^{1/2} / n} \frac{1}{\log t} dt
$$

$$
= \int_{X}^{X} \left( \sum_{X^{1/2} < n \leq t^{1/2}} \sum_{m \leq X^{1/2} / n} \frac{\mu(m)}{\varphi(m)} \right) \frac{1}{\log t} dt
$$

$$
= \int_{X}^{X} \left( \sum_{m \leq (X^{1/2})^A} \frac{\mu(m)}{\varphi(m)} t^{1/2} \kappa \right) \left( \sum_{m \leq (X^{1/2})^A} \frac{1}{\log t} \right) dt
$$

$$
= \int_{X}^{X} \left( \sum_{m \leq (X^{1/2})^A} \frac{\mu(m)}{\varphi(m)} \left( \frac{\kappa t^{1/2}}{2mN} + O \left( \frac{t^{1/2}}{mN^2} \right) \right) \right) \frac{1}{\log t} dt
$$

$$
= \frac{\kappa}{N} \sum_{m \leq (X^{1/2})^A} \frac{\mu(m)}{m \varphi(m)} \int_{X^{1/2} / \kappa}^{X} \frac{1/2}{\log t} dt + O_A \left( X^{3/2} (\log X)^{-A+1} \right).
$$

We first note that

$$
\sum_{m \leq Z} \frac{\mu(m)}{m \varphi(m)} = \sum_{m \text{ odd}} \frac{\mu(m)}{m \varphi(m)} + O \left( Z^{-1} \right),
$$

and that the completed sum is equal to the Euler product

$$
\prod_{\ell \geq 3} \left( 1 - \frac{1}{\ell (\ell - 1)} \right) = 2C_{\text{Art}}.
$$

It follows that

$$
Q_{1}^1 (\kappa, N - 1; X) = \frac{\kappa}{N} 2C_{\text{Art}} \int_{X^{1/2} / \kappa}^{X} \frac{1/2}{\log t} dt + O_A \left( X^{3/2} (\log X)^{-A+1} \right).
$$

We now renormalize and replace $N$ with $N / \kappa$, and then consider $\kappa = j / N$ with $N \leq j \leq [2N / \sqrt{3}]$. We then consider

$$
(3.16) \sum_{N \leq j \leq [2N / \sqrt{3}]} \left( 1 - 2 \sqrt{1 - \left( \frac{j}{N} \right)^2} \right) \left( \frac{C_{\text{Art}}}{N} \int_{X^{1/2} / \kappa}^{X} \frac{1/2}{\log t} dt + O_A \left( X^{3/2} (\log X)^{-A+1} \right) \right).
$$

The sum over the error term is small by first choosing $A$ large, and then supposing $N < (\log X)^{A'}$ with $A' < A - 3$, say.

The sum

$$
\sum_{N \leq j \leq [2N / \sqrt{3}]} N^{-1} \left( 1 - 2 \sqrt{1 - (j/N)^2} \right)
$$

is a Riemann sum for the integral

$$
\int_{1}^{2 \sqrt{3}} (1 - 2 \sqrt{1 - x^{-2}}) dx = \frac{\pi}{3} - 1,
$$

and the integrand $1 - \sqrt{1 - x^{-2}}$ is decreasing on $[1, \infty)$. Hence the Riemann sum approximates the integral by

$$
\left| \sum_{N \leq j \leq [2N / \sqrt{3}]} N^{-1} \left( 1 - 2 \sqrt{(N/j)^2} \right) - \int_{1}^{2 \sqrt{3}} (1 - 2 \sqrt{1 - x^{-2}}) dx \right| \ll N^{-1}.
$$
It follows that (3.16) is equal to
\[
\left( \frac{\pi}{3} - 1 \right) C_{\text{Art}} \int_2^X \frac{t^{1/2} dt}{\log t} + O_A \left( \frac{X^{3/2}}{(\log X)^A} \right).
\]
Evaluating the analogous sum for (3.16) but over the range \(1 \leq j < N\) and summing gives
\[
(3.17) \quad Q(X) = C_{\text{Art}} \frac{\pi}{3} \int_2^X \frac{t^{1/2} dt}{\log t} + O \left( \frac{X^{3/2}}{(\log X)^A} \right).
\]
Applying integration by parts we see
\[
\int_2^X \frac{t^{1/2} dt}{\log t} = \left[ \frac{2t^{3/2}}{3\log t} \right]_2^X - \frac{2}{3} \int_2^X \frac{t^{3/2}}{(\log t)^2} dt
\]
\[
= \frac{2X^{3/2}}{3\log X} - \frac{2}{3} \int_2^X \frac{t^{1/2} dt}{(\log t)^2} + O(1),
\]
hence
\[
Q(X) = C_{\text{Art}} \frac{2\pi}{9} \frac{X^{3/2}}{\log X} + O \left( \frac{X^{3/2}}{(\log X)^2} \right)
\]
as required for the proof of Theorem 1.1.

4. ALTERNATE APPROACH VIA THE ANALYTIC CLASS NUMBER FORMULA

We now give our second proof, which is similar to the approaches of Nagoshi [11] for discriminant \(1 - 4p\) and Friedlander-Iwaniec [5] for discriminant \(-4p\), where we estimate the sum of class numbers via the analytic class number formula.

The class number formula gives
\[
h(D) = \frac{1}{\pi} L(1, \chi_D)|D|^{1/2}
\]
for any discriminant \(D < 0\): it holds even for non-fundamental \(D\), when \(h(D)\) is defined as the number of primitive equivalence classes of binary quadratic forms of discriminant \(D\). The number of all binary quadratic forms of discriminant \(D\), including the non-primitive ones, is
\[
H(D) = \sum_d h(D/d^2)
\]
where the sum is over all \(d\) such that \(D/d^2\) is a discriminant.

Summing over all \(D = 1 - 4p\) with \(p \leq X\), we can write our sum \(Q(X) = \sum_{p \leq X} H(1 - 4p)\) as
\[
Q(X) = \sum_{d \geq 1} Q_d(X)
\]
where we define \(Q_d(X) = \sum_{p \leq X, d^2 \mid 1 - 4p} h(\frac{(1 - 4p)}{d^2})\) for \(d\) odd (and \(0\) for \(d\) even). Applying the class number formula, we also have
\[
(4.1) \quad Q_d(X) = \sum_{p \leq X, d^2 \mid 1 - 4p} \frac{1}{\pi} L(1, \chi((1 - 4p)/d^2)) \left|\frac{4p - 1}{d^2}\right|^{1/2}
\]
\[
= \frac{1}{\pi d} \sum_{p \leq X, d^2 \mid 1 - 4p} \sum_{n \geq 1} \frac{(4p - 1)^{1/2}}{n} \left(\frac{(1 - 4p)/d^2}{n}\right).
\]
It will be convenient to us to first bound the related quantity
\[
T_d(X) = \sum_{p \leq X, d^2 \mid 1 - 4p} L(1, \chi((1 - 4p)/d^2)) = \sum_{p \leq X, d^2 \mid 1 - 4p} \sum_{n \geq 1} \left(\frac{(1 - 4p)/d^2}{n}\right) \frac{1}{n}.
\]
We define a multiplicative function \(c(d)\), which will feature in the leading terms.
Definition 4.1. For $d$ odd we set
\[
c(d) := \frac{1}{d^3} \prod_{\ell | d} \frac{\ell^3 - 1}{\ell^3 - \ell^2 - \ell - 1}
\]
and for $d$ even we have $c(d) = 0$.

Lemma 4.2. If $d \ll (\log X)^\alpha$ for some fixed $\alpha$, then
\[
T_d(X) = \frac{\pi^2}{12} \cdot dc(d) \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} X/\log X + o(X/\log X),
\]

Lemma 4.3.
\[
Q_d(X) = \frac{\pi}{9} c(d) \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} X^{3/2}/\log X + o(X^{3/2}/\log X)
\]

Theorem 4.4. $Q(X) = \frac{2\pi}{9} C_{\text{Art}} X^{3/2}/\log X + o(X)$.

The heart of the argument is in the proof of Lemma 4.2 which we defer to Section 4.1. We now assume it and prove the other results.

Proof of Lemma 4.3. We apply partial summation to
\[
Q_d(X) = \sum_{p \leq X \atop d^2 \mid 1-4p} \frac{1}{d^2} L(1, \chi_{(1-4p)/d^2}) \left| \frac{4p-1}{d^2} \right|^{1/2}
\]
\[
= \frac{1}{\pi d} \left( (4X - 1)^{1/2} T_d(X) + \sum_{t=1}^{X-1} \left( (4t - 1)^{1/2} - (4(t+1) - 1)^{1/2} \right) T_d(t) \right)
\]
\[
= \frac{1}{\pi d} \left( X^{1/2} (2 + O(X^{-1})) T_d(X) - \sum_{t=1}^{X-1} (t^{-1/2} + O(t^{-3/2})) T_d(t) \right)
\]
\[
= \frac{\pi}{12} \cdot c(d) \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} \left( 2(X^{3/2}/\log X) - \sum_{t=1}^{X} t^{1/2}/\log t + o(X^{3/2}/\log X) \right)
\]
\[
= (\pi/9) \cdot c(d) \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} (X^{3/2}/\log X) + o(X^{3/2}/\log X).
\]
where we apply Lemma 4.2 at the next-to-last step and use $\sum_{t=1}^{X} t^{1/2}/\log t = (\frac{2}{3} + o(1)) X^{3/2}/(\log X)$ in the last.

We now sum over $d$ to obtain the asymptotic for $Q$:

Proof of Theorem 4.4. Using $L(1, \chi_D) = O(\log D)$, we have the trivial bound
\[
Q_d(X) \ll \sum_{m \leq X \atop d^2 \mid 1-4m} \log X \frac{\sqrt{X}}{d} \approx d^{-3} X \log X.
\]
Hence we can cut off the sum at $X^\alpha$ for any $\alpha > 1/2$.
\[
Q(X) = \sum_{d \in [1,X] \text{ odd}} Q_d(X) = \sum_{d \in [1,\log(X)^\alpha] \text{ odd}} Q_d(X) + o(X^{3/2}/\log(X))
\]

We now apply Lemma 4.3 to obtain
\[
Q(X) = \sum_{d \in [1,\log(X)^\alpha] \text{ odd}} Q_d(X) + o(X^{3/2}/\log(X))
\]
\[
= \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} \left( \sum_{d \in [1,\log(X)^\alpha]} c(d) \right) X^{3/2}/\log(X) + o(X^{3/2}/\log(X))
\]
We now need to evaluate the sum \( \sum_{d=1}^{\infty} c(d) \), which we can expand as an Euler product:

\[
\sum_{d=1}^{\infty} c(d) = \sum_{d \geq 1 \text{ odd}} d^{-3} \prod_{\ell|d} \frac{\ell^3 - 1}{\ell^3 - \ell^2 - \ell - 1}
= \prod_{\ell \text{ odd}} \left( 1 + \ell^{-3}(1 - \ell^{-3})^{-1} \frac{\ell^3 - 1}{\ell^3 - \ell^2 - \ell - 1} \right)
= \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell}{\ell^3 - \ell^2 - \ell - 1}
\]

Hence \( \sum_{d \in [1, \log X]} c(d) = \prod_{\ell \text{ odd}} \frac{\ell^3 - \ell^2 - \ell}{\ell^3 - \ell^2 - \ell - 1} + o(1) \). Plugging this into (4.4), we obtain

\[
Q(X) = \frac{\pi}{9} \prod_{\ell \text{ odd}} \left( \frac{\ell^3 - \ell^2 - \ell}{\ell^3 - \ell^2 - \ell - 1} \right) \frac{X^{3/2}/\log X + o(X^{3/2}/\log X)}{\log(1/X)}
= \frac{\pi}{9} \prod_{\ell \text{ odd}} \left( 1 - \frac{1}{\ell^2 - \ell} \right) X^{3/2}/\log X + o(X^{3/2}/\log X)
= \frac{2\pi}{9} C_{Ar} X^{3/2}/\log X.
\]

as desired.

4.1. Strategy for proof of Lemma 4.2. We now need to estimate

\[
T_d(X) = \sum_{p \leq X} L(1, \chi((1 - 4p)/d^2)) = \sum_{p \leq X} \sum_{n \geq 1} \left( \frac{(1 - 4p)/d^2}{n} \right) \frac{1}{n}
\]

under the assumption that \( d \ll (\log X)^a \).

First we want to cut off the tails of the inner sums, so that we have something finite. We’ll choose \( B \) such that for any \( p \leq X \), \( d \ll (\log X)^a \)

\[
\sum_{n > B} \left( \frac{(1 - 4p)/d^2}{n} \right) \frac{1}{n} = o(1)
\]

By the partial summation argument given in [12], \( B = X^{1/2+\delta} \) works for any positive \( \delta \). Then

\[
T_d(X) = T_d(X, [1, B]) + o(X/\log X)
\]

where

\[
T_d(X, [1, B]) = \sum_{p \leq X} \sum_{1 \leq n \leq B} \left( \frac{(1 - 4p)/d^2}{n} \right) \frac{1}{n}.
\]

We now choose a second cutoff \( b < B \), which we’ll choose small enough that we can estimate \( T_d(X, b) \) by Siegel-Walfisz, and then will estimate by breaking up

\[
T_d(X, [1, b]) = T_d(X, [1, b]) + T_d(X, (b, B])
\]

where \( T_d(X, [1, b]) \) is the partial double sum with \( n \) restricted to the range \([1, b]\) and likewise for \( T_d(X, (b, B]) \).

We will estimate \( T_d(X, [1, b]) \) by Siegel-Walfisz and \( T_d(X, (b, B]) \) by double oscillation.
4.2. Estimating $T_d(X, [1, b])$. We exchange order of summation, to get

$$T_d(X, [1, b]) = \sum_{1 \leq n \leq b} \frac{1}{n} \sum_{p \leq X \atop d^2|1-4p} \left( \frac{(1-4p)/d^2}{n} \right).$$

We now estimate the inner sum. Note that $\left( \frac{(1-4p)/d^2}{n} \right)$ depends only on $p$ modulo $d^2n$, which for $n \leq b$ is bounded by a power of $\log X$. We take $b$ to be $(\log X)\beta$ for some fixed $\beta > 4$, so we get

$$\sum_{p \leq X \atop d^2|1-4p} \left( \frac{(1-4p)/d^2}{n} \right) = (\phi(d^2)^{-1})a_{n,d} \Li(X) + O(X(\log X)^{-A})$$

for any $A > 0$.

Here the constant fixed odd $d, a_{n,d}$ is a multiplicative function of $n$. Hence it is determined by its values at prime powers, which can be computed. We can then express the Dirichlet series for $a_{n,d}$ as the following Euler product

$$f_d(s) = \sum_n a_{n,d}n^{-s} = (1 + 2^{-s})^{-1} \prod_{\ell|d \text{ odd}} \left( 1 - \left( \frac{1}{\ell+1} \right) \left( \ell^{-s} + \ell^{-2s} \right) \right) \left( 1 - \ell^{-2s} \right)^{-1}$$

$$\times \prod_{\ell|d \text{ odd}} (1 - \ell^{-2s})^{-1} (1 - \ell^{-2s-1})$$

$$= (1 - 2^{-s})\zeta(2s) \prod_{\ell|d \text{ odd}} \left( 1 - \left( \frac{1}{\ell+1} \right) \left( \ell^{-s} + \ell^{-2s} \right) \right) \prod_{\ell|d} (1 - \ell^{-2s-1}).$$

Now plugging (4.6) into (4.5), we obtain

$$T_d(X, [1, b]) = \phi(d^2)^{-1} \left( \sum_{1 \leq n \leq b} \frac{a_{n,d}}{n} \right) \Li(X) + O(X(\log X)^{-A}\log b)$$

Now, this sum $\sum_{n \leq b} \frac{a_{n,d}}{n}$ converges absolutely as $b \to \infty$, with sum

$$\sum_n a_{n,d}n^{-1} = f_d(1) = \frac{1}{2} \zeta(2d) \prod_{\ell|d \text{ odd}} \left( 1 - \left( \frac{1}{\ell+1} \right) \left( \ell^{-1} + \ell^{-2} \right) \right) \prod_{\ell|d} (1 - \ell^{-3})$$

$$= \frac{1}{2} \zeta(2) \prod_{\ell|d} \left( \frac{\ell - 1}{\ell} \right) \left( \frac{\ell^3 - 1}{\ell^3 - \ell^2 - \ell - 1} \right) \prod_{\ell|d} \left( \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} \right)$$

$$= \frac{1}{2} \zeta(2) d^2 c(d) \prod_{\ell|d} \left( \frac{\ell - 1}{\ell} \right) \prod_{\ell|d} \left( \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} \right).$$

using the definition of $c(d)$ in (4.2).

Since $b \to \infty$ as $X \to \infty$, we get asymptotically

$$T(X, b) = \phi(d^2)^{-1} \cdot \frac{1}{2} \zeta(2d^2) c(d) \prod_{\ell|d} \left( \frac{\ell - 1}{\ell} \right) \prod_{\ell|d} \left( \frac{\ell^3 - \ell^2 - \ell - 1}{\ell^3 - \ell^2} \right)$$

$$= \frac{\pi^2}{12} dc(d) \prod_{\ell|d} \left( \frac{\ell^3 - \ell}{\ell^3 - \ell^2 - \ell - 1} \right)$$

4.3. Estimating $T_{[b,B]}(X)$. We will now apply the double oscillation Lemma (Lemma 2.2) to bound

$$T_{[b,B]}(X) = \sum_{p \leq X \atop d^2|1-4p} \sum_{b < n \leq B} \left( \frac{(1-4p)/d^2}{n} \right) \frac{1}{n}.$$
As suggested by Friedlander-Iwaniec in [5], we divide the interval \([b, B]\) into dyadic intervals \([a, 2a]\) and apply Lemma 2.2 on each.

**Lemma 4.5.** For \(a \ll X^{1/2}\),

\[
T_{[a, 2a]}(X) = \sum_{d \mid X} \sum_{a \leq n \leq 2a} \left(\frac{1 - 4p}{d^2}\right) \frac{1}{n} \ll X \log X \cdot a^{-1/2}
\]

**Proof.** We rewrite

\[
T_{[a, 2a]}(X) = \frac{1}{a} \sum_{d \mid X} \sum_{a \leq n \leq 2a} \frac{a}{n} \left(\frac{1 - 4p}{d^2}\right).
\]

so now all the coefficients in the inner sum are of size \(\leq 1\), and Lemma 2.2 applies to give

\[
T_{[a, 2a]}(X) \ll \frac{1}{a} \cdot aX(\log a + \log X)(a^{-1/2} + (X/a)^{-1/2}) \ll X \log X \cdot a^{-1/2},
\]

since \(a \ll X^{1/2}\).

We now apply this lemma to bound \(T_{[b, B]}(X)\) as follows:

\[
T_{[b, B]} \leq \sum_{i=0}^{[\log_2(B/b)]-1} T_{[2^ib, 2^{i+1}b]}(X) \ll X \log X \cdot b^{-1/2} \sum_{i=0}^{[\log_2(B/b)]-1} 2^{i/2} \ll X \log X b^{-1/2}.
\]

Since we have chosen \(b = (\log X)^\beta\) for \(\beta > 4\), this is an error term.

This completes the proof of Lemma 4.2.

**References**

[1] A. Balog, V. Blomer, C. Dartyge, G. Tenenbaum, *Friable values of binary forms*, Comment. Math. Helv. **87** (2012), 639-667.

[2] W. Duke, J. B. Friedlander, H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math **141** (1995), 423-441.

[3] E. Fouvry, J. Kluners, *On the 4-rank of class groups of quadratic fields*, Invent. Math. **167** (2007), 455-513.

[4] J. B. Friedlander, H. Iwaniec, *Opera de Cribro*, 57 American Mathematical Society Colloquium Publications.

[5] J. B. Friedlander, H. Iwaniec, *Hyperbolic prime number theorem*, Acta Math. **202** (2009), no. 1, 1719.

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

[7] K. Lapidova, *Explicit upper bound for the average number of divisors of irreducible quadratic polynomials*, Monatsh. Math. (4) **186** (2018), 663-673.

[8] J. Li, *A binary quadratic Titchmarsh divisor problem*, Acta. Arith. (4) **192** (2020), 341-361.

[9] A. B. Miller, *Asymptotics for the number of simple \((4a + 1)\)-knots of genus 1*, arXiv:1905.04369 [math.NT].

[10] H. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*.

[11] H. Nagoshi, *The moments and statistical distribution of class numbers of quadratic fields with prime discriminant*, Lith. Math. J. **52** (2012), no. 1, 77-94.

[12] C. L. Siegel, *The Average Measure of Quadratic Forms With Given Determinant and Signature*, Annals of Mathematics, **45** (1944), no. 4, 667-785.

**Mathematical Reviews**, 416 Fourth St., Ann Arbor, MI 48103

**Email address:** alimil@umich.edu

**Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George Street, Room 6290, Toronto, Ontario, Canada, M5S 2E4**

**Email address:** syxiao@math.toronto.edu