PRIMES OF THE FORM $x^2 + dy^2$ AND INTERACTIONS OF CLASS GROUPS

JOÃO CAMPOS-VARGAS

Abstract. We investigate how class groups of quadratic fields interact and use our results to determine the proportion $\delta^+(\Delta)$ of primes covered by the forms $x^2 + dy^2$, $1 \leq d \leq \Delta$. We establish that

$$\delta^+(\Delta) = 1 - \exp\Big(- (\alpha(\Delta) + o(1)) \frac{\sqrt{\Delta}}{\log \Delta} \Big)$$

for some $7\pi/12 \leq \alpha(\Delta) \leq 7\pi/12 + \log 4$. Moreover, inspired by a result of Kaplansky, we show that any prime that is represented by two of the forms

$$x^2 + 17y^2,\ x^2 + 65y^2,\ x^2 + 1105y^2,$$

is actually represented by all three. The same is true for $x^2 + 34y^2$, $x^2 + 66y^2$, $x^2 + 1122y^2$, and we use the interaction of the corresponding class groups to explain this phenomenon. Finally, we determine the proportion $\delta^-(\Delta)$ of primes covered by the forms $x^2 - dy^2, 1 < d \leq \Delta, \sqrt{d} \notin \mathbb{Z}$, in terms of class numbers of real quadratic fields with discriminant p, $4p$, and $8p$. In particular, we establish that

$$\delta^-(\Delta) \geq 1 - \exp\Big(- \tfrac{7}{24}\sqrt{\Delta} + O\Big(\tfrac{\sqrt{\Delta}}{\log \Delta}\Big)\Big).$$

Our result shows that an improved lower bound for $\delta^-(\Delta)$ leads to smaller class numbers in these families of discriminants.

Contents

Date: October 28, 2025.

1. Introduction

The question of representing primes using binary quadratic forms attracted many mathematicians throughout history. This goes back to Fermat in the 1600s, who wrote in a letter to Mersenne that for an odd prime p,

$$p = x^2 + y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \mod 4.$$

Fermat also wrote a characterization for primes p represented by $x^2 + 2y^2$ and $x^2 + 3y^2$ in terms of a congruence condition on p. Around a century later, Euler found the proofs for these characterizations that were lacking in Fermat's letters, which led him to the discovery of quadratic reciprocity. Then, a similar conjecture of Euler for the primes represented by $x^2 + 5y^2$ led Lagrange to formulate the first notions of genus theory.

Despite these great discoveries, Euler had other remarkable conjectures that remained open until the time of Gauss. What stood out in them is that the primes represented by the form were no longer described only by congruence conditions. For instance, Euler predicted that

$$p = x^2 + 64y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \mod 4 \text{ and } \left(\frac{2}{p}\right)_4 = 1 \tag{1}$$

where $(\frac{\cdot}{p})_4$ is the biquadratic residue symbol. Gauss, with his discovery of higher reciprocity laws, settled these conjectures.

With the development of classical class field theory, a nearly complete solution of this problem became known by the first half of the twentieth century. Namely, for any integer d there exists an integer polynomial $f_d(x)$ such that for any odd prime p not dividing d or the discriminant of $f_d(x)$,

$$p = x^2 + dy^2,\ x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{-d}{p}\right) = 1 \text{ and } f_d(x) \equiv 0 \mod p \\ \text{has an integer solution.} \end{cases}$$

For a beautiful account on this problem, see Cox's book [5].

Much less literature exists on the problem of representing primes by *multiple* forms. In fact, this only appears to have been pursued in the case of pairs of forms. Kaplansky [11] was the first to write about a curious phenomenon pertaining $x^2 + 32y^2$ and $x^2 + 64y^2$. His result shows that each

$$p \equiv 1 \mod 16 \text{ is represented by both or neither of } x^2 + 32y^2,\ x^2 + 64y^2.$$

This is surprising because the sets of primes represented by either x^2+32y^2 or x^2+64^2 cannot be described by congruence conditions alone (as the result of Gauss (1) and a companion result of Barrucand and Cohn [1] show). Nevertheless, these sets coincide on primes $p \equiv 1 \mod 16$. Other researchers [3, 9, 13] then worked to classify all pairs of forms exhibiting this coincidence.

More recently, the collective behavior of the forms $x^2+dy^2, d \geq 1$ was studied by Green and Soundararajan [8] with the goal of covering integers instead of primes. Their result shows that 0% of the integers up to N are covered by a form x^2+dy^2 with $d \leq (\log N)^{\log 2-\epsilon}$, whereas 100% of them are covered by a form with $d \leq (\log N)^{\log 2+\epsilon}$. A different story happens with primes, as the form $x^2 + y^2$ covers 50% of them (those of the form $4k + 1$), and as more forms are included this proportion grows.

Inspired by the work of Green and Soundararajan, our first result establishes bounds for the proportion of primes covered by the forms x^2+dy^2, $d\leq\Delta$:

THEOREM 1.1. *Let $\delta^+(\Delta)$ be the proportion of primes covered by the forms x^2+dy^2, $1\leq d\leq\Delta$. Then*

$$\delta^+(\Delta)=1-\exp\left(-(\alpha(\Delta)+o(1))\frac{\sqrt{\Delta}}{\log\Delta}\right),$$

where

$$\tfrac{7}{12}\pi\leq\alpha(\Delta)\leq\tfrac{7}{12}\pi+\log 4.$$

Algebraically, the proportion of primes that are *simultaneously* represented by forms $x^2+d_1y^2,\dots,x^2+d_ky^2$ appears more naturally. Theorem 4.5 establishes this proportion, which is the main ingredient to prove Theorem 1.1. Let D_i be the fundamental discriminant with the same squarefree part as $-d_i$, and denote the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{D_i}))$ by $\mathrm{Cl}(D_i)$. This proportion of primes is proportional to the size of the kernel of the map

$$\Phi:\ \mathrm{Cl}^\vee(D_1)\times\cdots\times\mathrm{Cl}^\vee(D_k)\to\mathrm{Cl}^\vee(K)$$
$$(\chi_1,\ \dots,\ \chi_k)\mapsto\chi:=\prod_{i=1}^{k}\chi_i\circ N_{K/\mathbb{Q}(\sqrt{D_i})}$$

where $K=\mathbb{Q}(\sqrt{D_1},\dots,\sqrt{D_k})$.

We say that characters $\chi_1\in\mathrm{Cl}^\vee(D_1),\dots,\chi_k\in\mathrm{Cl}^\vee(D_k)$ *interact* if $(\chi_1,\dots,\chi_k)\in\ker\Phi$. This is equivalent to the Rankin-Selberg convolution $L(s,\chi_1\otimes\cdots\otimes\chi_k)$ being a power of the Dedekind zeta function of K.

Theorem 4.5 explains the coincidences in the sets of primes represented by the forms $x^2+d_1y^2,\dots,x^2+d_ky^2$ in terms of interactions between characters of $\mathrm{Cl}(D_1),\dots,\mathrm{Cl}(D_k)$. As a byproduct of this study, we obtain two results akin to Kaplansky's, for three forms:

THEOREM 1.2.

a) Let $p\equiv 1 \mod 4$ be a prime such that $(\frac{p}{5})=(\frac{p}{13})=(\frac{p}{17})=1$. Then,

p is represented by all or exactly one of x^2+17y^2, x^2+65y^2, $x^2+1105y^2$.

b) Let $p\equiv 1,3 \mod 8$ be a prime such that $(\frac{p}{3})=(\frac{p}{11})=(\frac{p}{17})=1$. Then,

p is represented by all or exactly one of x^2+34y^2, x^2+66y^2, $x^2+1122y^2$.

As an immediate corollary, we deduce:

COROLLARY 1.3. *Let $\{d_1,d_2,d_3\}$ be either $\{17,65,1105\}$ or $\{34,66,1122\}$. Then, any prime represented by two of the forms*

$$x^2+d_1y^2,\ x^2+d_2y^2,\ x^2+d_3y^2$$

is in fact represented by all three.

We will show that $(\chi_1,\dots,\chi_k)\in\ker\Phi$ only if $\chi_i\in\mathrm{Cl}^\vee(D_i)[2^\infty]$ for every $i=1,\dots,k$, which means that only the 2-parts of the dual class groups interact. We divide the interactions into *genus* and *higher order*: genus interactions happen between characters of order at most 2 (genus characters), and is understood in terms of the common factors of $D_1,\dots,D_k$;

every other $(\chi_1, \dots, \chi_k) \in \ker \Phi$ with $\operatorname{ord} \chi_i \geq 4$ for some $i = 1, \dots, k$ will be referred to as a higher order interaction. In addition to higher order interactions, Theorem 1.2 also relies on the fact that the class numbers at hand are small powers of 2.

We also establish a version of Theorem 1.1 for indefinite forms. This result connects the proportion of primes represented by $x^2 - dy^2$, $1 < d \leq \Delta$, $\sqrt{d} \notin \mathbb{Z}$ to class numbers of real quadratic fields in prime families. In order to state this result, define for every fundamental discriminant $D > 0$ the number

$$h^*(D) = \begin{cases} 3h(D) & \text{if } D \equiv 5 \bmod 8 \text{ and } u \equiv 1 \bmod (2)\, \forall\, u \in \left(\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]\right)^\times \\ h(D) & \text{otherwise,} \end{cases} \tag{2}$$

where $h(D)$ denotes the class number of $\mathbb{Q}(\sqrt{D})$. Our result is:

THEOREM 1.4. *Let $\delta^-(\Delta)$ be the proportion of primes covered by the forms $x^2 - dy^2$, $1 < d \leq \Delta$, $\sqrt{d} \notin \mathbb{Z}$, and let $h^*(D)$ be defined by (2). Then*

$$\delta^-(\Delta) = 1 - \Theta \cdot \exp\left(O\left(\frac{\sqrt{\Delta}}{\log \Delta}\right)\right)$$

where

$$\Theta = \prod_{\substack{p \leq \Delta \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{2h^*(p)}\right) \left(\prod_{\substack{p \leq \Delta \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{2h(4p)}\right) + \prod_{\substack{p \leq \Delta/2 \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{2h(8p)}\right) \right).$$

Moreover,

$$\delta^-(\Delta) \geq 1 - \exp\left(-\tfrac{7}{24}\sqrt{\Delta} + O\left(\frac{\sqrt{\Delta}}{\log \Delta}\right)\right).$$

Unlike Theorem 1.1, the proportion $\delta^-(\Delta)$ is determined by a factor $\Theta(\Delta)$ which is provably smaller than the error term $\exp(O(\sqrt{\Delta}/\log \Delta))$. This allows us to establish the lower bound above and gives an expression for $\delta^-(\Delta)$ in terms of $h^*(p)$, $h(4p)$, and $h(8p)$. The Cohen-Lenstra heuristics [4] predicts that most of these class numbers are very small. Quantitatively, we expect

$$\delta^-(\Delta) \geq 1 - \exp(-c\,\Delta/\log \Delta)$$

for some $c > 0$. Theorem 1.4 shows that an improved lower bound for $\delta^-(\Delta)$ leads to smaller class numbers in these prime families.

Outline. Section 2 presents necessary and sufficient conditions for a prime to be represented by $x^2 - dy^2$, $d \in \mathbb{Z}$ squarefree, which are given in terms of the usual class group of $\mathbb{Q}(\sqrt{d})$ or a small extension of it. Section 3 discusses simultaneous representations of primes by $x^2 - d_1y^2$, $\dots$, $x^2 - d_ky^2$, reintroducing the map Φ above with the groups defined on Section 2. This map controls the proportion of primes simultaneously represented by these forms.

In Section 4 we study the kernel of Φ. We establish that only the 2-parts of the dual class groups interact and prove an upper bound for the order of the elements in this kernel. We also compute the size of the 2-torsion subgroup $\ker \Phi[2]$ for any squarefree $d_1, \dots, d_k$. We summarize this work in Theorem 4.5, refining a previous result from Section 3 and giving the proportion of primes simultaneously represented by $x^2 - d_1y^2$, $\dots$, $x^2 - d_ky^2$ in terms of higher order interactions. We then show that there is no higher order interactions for certain $d_1, \dots, d_k$ that appear in the proofs of Theorem 1.1 and Theorem 1.4.

We finish Section 4 with a proof of Theorem 1.2, which gives two examples of characters of order 4 interacting. Theorem 1.1 and Theorem 1.4 are proved in Section 5 based on the results from Section 4 and the evaluation of certain sums of inverses of class numbers. Proofs of results that deviated from the main discussion were postponed to the Appendix.

2. Primes of the form $x^2 - dy^2$, $d \in \mathbb{Z}$

Let D be a fundamental discriminant with squarefree part d. Whether or not a prime p is represented by $x^2 - dy^2$ depends on the splitting of p in $\mathbb{Q}(\sqrt{D})$ and the shape of the ideals above p. This situation is very simple $D = 4d < 0$, when it suffices to have principal ideals above p. We now introduce the conditions for the general case.

Let $K = \mathbb{Q}(\sqrt{D})$, $\mathcal{O}_K$ be its ring of integers, and $h(D)$ its class number. Denote by I_K the set of all fractional ideals of $\mathcal{O}_K$ and by $I_K(2)$ its subset of fractional ideals coprime to (2). Let P_K^+ be the set of principal ideals (α) with $\alpha \in \mathcal{O}_K$ and $N_{K/\mathbb{Q}}(\alpha) > 0$ and $P_{K,\mathbb{Z}}^+(2)$ be its subset of ideals (α) with $\alpha \equiv 1 \mod (2)$.

Let $\mathrm{Cl}^+(D)$ be the narrow class group I_K/P_K^+, and let $\mathrm{Cl}_{(2)}^+(D)$ be the ray class group $I_K(2)/P_{K,\mathbb{Z}}^+(2)$. Recall that the order of $\mathrm{Cl}^+(D)$ is

$$h^+(D) = \begin{cases} 2h(D) & \text{if } D > 0 \text{ and } N_{K/\mathbb{Q}}(u) = 1 \,\forall\, u \in (\mathcal{O}_K)^\times \\ h(D) & \text{otherwise.} \end{cases} \tag{3}$$

Define

$$\mathfrak{C}(D) = \begin{cases} \mathrm{Cl}_{(2)}^+(D) & \text{if } D \equiv 5 \bmod 8 \text{ and } u \equiv 1 \bmod (2) \,\forall\, u \in (\mathcal{O}_K)^\times \\ \mathrm{Cl}^+(D) & \text{otherwise} \end{cases} \tag{4}$$

and let

$$\mathfrak{h}(D) = \#\mathfrak{C}(D). \tag{5}$$

Denote the dual of a group A by $A^\vee$. The characters of $\mathfrak{C}^\vee(D)$ tell us whether or not p is represented by $x^2 - dy^2$:

Lemma 2.1. *Let p be an odd prime and D be a fundamental discriminant with squarefree part d. Assume that $p \nmid D$, and let $\mathfrak{p}$ be a prime in $\mathbb{Q}(\sqrt{D})$ lying above p. Then*

$$p = x^2 - dy^2,\ x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{D}{p}\right) = 1 \text{ and } \chi(\mathfrak{p}) = 1 \\ \text{for every } \chi \in \mathfrak{C}^\vee(D). \end{cases} \tag{6}$$

Proof. First, assume that $D = 4d$. In this case, $\mathfrak{C}(D) = \mathrm{Cl}^+(D)$ and $x^2 - dy^2$ is the principal form of $\mathbb{Q}(\sqrt{D})$, and p is represented by this form exactly when p splits in $\mathbb{Q}(\sqrt{D})$ and $\mathfrak{p}$ is a principal ideal with positive norm. This is equivalent to $(\frac{D}{p}) = 1$ and $\mathfrak{p} \in P_K^+$, which gives the result.

Next, assume that $D \equiv 1 \mod 8$. As $\mathfrak{C}(D) = \mathrm{Cl}^+(D)$, the conditions on the right-hand side are equivalent to p splitting in $\mathbb{Q}(\sqrt{D})$ and $\mathfrak{p} \in P_K^+$. This means that p is represented by the principal form $x^2 + xy + \frac{1-d}{4}y^2$, so that $4p = (2x+y)^2 - dy^2$. As $4 \mid (2x+y)^2 - dy^2$ and $d \equiv 1 \mod 8$, we must have y even otherwise 8 would divide $4p$, yielding the desired representation $p = (x + y/2)^2 - d(y/2)^2$.

Lastly, we consider the case $D \equiv 5 \mod 8$. The prime 2 is inert in $\mathbb{Q}(\sqrt{D})$, implying $(\mathcal{O}_K/(2))^\times \cong \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$. Assume now that $\mathcal{O}_K$ has a unit $u \not\equiv 1 \mod (2)$. In this case, notice that u^2 is a generator of $(\mathcal{O}_K/(2))^\times$. As before, the right-hand side conditions are equivalent to $N_{K/\mathbb{Q}}(\alpha) = p$ for some $\alpha \in \mathcal{O}_K$. We know that $\alpha \in (\mathcal{O}_K/(2))^\times$ since p is odd, which means that $\alpha(u^2)^m \equiv 1 \mod (2)$ for some choice of m. Therefore $\alpha(u^2)^m = x + y\sqrt{d}$ for some $x, y \in \mathbb{Z}$, and since $N_{K/\mathbb{Q}}(u^2) = 1$ we obtain that $p = x^2 - dy^2$.

On the other hand, if all units $u \in (\mathcal{O}_K)^\times$ satisfy $u \equiv 1 \mod (2)$, the right-hand side conditions are equivalent to $N_{K/\mathbb{Q}}(\alpha) = p$ for some $\alpha \in \mathcal{O}_K$ with $\alpha \equiv 1 \mod (2)$. Therefore $\alpha = x + y\sqrt{d}$ for some $x, y \in \mathbb{Z}$, which gives $p = x^2 - dy^2$. The result follows. □

Definition (4) captures the *Eisenstein set*, as named by Stevenhagen [15]. When $D \equiv 5 \mod 8$ and $u \equiv 1 \mod (2)$ for all $u \in (\mathcal{O}_K)^\times$, we can still understand the group $\mathfrak{C}(D)$ very explicitly in terms of the usual narrow class group $\mathrm{Cl}^+(D)$. In fact, as every ideal class in $\mathrm{Cl}^+(D)$ contains an ideal coprime to (2), there is a natural surjection $\mathfrak{C}(D) \twoheadrightarrow \mathrm{Cl}^+(D)$ defined by $[\mathfrak{a}] \mapsto [\mathfrak{a}]$. This gives a natural injection $\mathrm{Cl}^{+\vee}(D) \hookrightarrow \mathfrak{C}^\vee(D)$, in the sense that a character defined on all fractional ideals of $\mathcal{O}_K$ is also defined on those coprime to (2). We write

$$\mathrm{Cl}^{+\vee}(D) \leq \mathfrak{C}^\vee(D) \tag{7}$$

to make explicit this subgroup relation. We now compute their quotient.

Lemma 2.2. *Let $D \equiv 5 \mod 8$ be a fundamental discriminant for which all units $u \in (\mathcal{O}_K)^\times$ satisfy $u \equiv 1 \mod (2)$. Then*

$$\mathfrak{C}^\vee(D)/\,\mathrm{Cl}^{+\vee}(D) \cong \mathbb{Z}/3\mathbb{Z}.$$

Proof. It suffices to show that $\mathfrak{C}(D) \twoheadrightarrow \mathrm{Cl}^+(D)$ has kernel $\mathbb{Z}/3\mathbb{Z}$. From the definition of the groups, this kernel is $P_K^+ \cap I_K(2)/P_{K,\mathbb{Z}}^+(2)$. As all units $u \in (\mathcal{O}_K)^\times$ satisfy $u \equiv 1 \mod (2)$, we can define the map $P_K^+ \cap I_K(2) \to (\mathcal{O}_K/(2))^\times$, $(\alpha) \mapsto \bar{\alpha}$, which is surjective with kernel $P_{K,\mathbb{Z}}^+(2)$. We conclude that

$$P_K^+ \cap I_K(2)/P_{K,\mathbb{Z}}^+(2) \cong (\mathcal{O}_K/(2))^\times \cong \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$$

as 2 is inert in $\mathbb{Q}(\sqrt{D})$. □

Lastly, we remark that any extension of a non-trivial character

$$P_K^+ \cap I_K(2)/P_{K,\mathbb{Z}}^+(2) \cong \mathbb{Z}/3\mathbb{Z} \to \mathbb{C}^\times$$

to the entire group $\mathfrak{C}(D) = I_K(2)/P_{K,\mathbb{Z}}^+(2)$ is a generator of $\mathfrak{C}^\vee(D)/\,\mathrm{Cl}^{+\vee}(D)$ in Lemma 2.2.

3. Properties of multiquadratic extensions

Throughout the next two sections, fix a set of distinct fundamental discriminants $\mathcal{D} = \{D_1, \ldots, D_k\}$. Let d_i be the squarefree part of D_i, and let $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_k})$. Denote the relative norm $N_{K/\mathbb{Q}(\sqrt{D_i})}$ by N_i.

3.1. **The splitting of primes.** Our first observation is that a rational prime can be inert in at most one quadratic extension in any tower of fields leading up to K. We state this below in terms of norms.

LEMMA 3.1. *Let $\mathfrak{P}$ be a prime in K above a rational prime p. For each extension $\mathbb{Q}(\sqrt{D_i})$ where p is not inert, let $\mathfrak{p}_i$ be the prime above p and below $\mathfrak{P}$. Then, if p is not inert in any extension $\mathbb{Q}(\sqrt{D_1}), \ldots, \mathbb{Q}(\sqrt{D_k})$,*

$$N_i(\mathfrak{P}) = \mathfrak{p}_i \text{ for all } i = 1, \ldots, k.$$

Otherwise,

$$N_i(\mathfrak{P}) = \begin{cases} \mathfrak{p}_i^2 & \text{if } p \text{ is not inert in } \mathbb{Q}(\sqrt{D_i}), \\ (p) & \text{otherwise.} \end{cases}$$

Proof. Assume without loss of generality that $D_1, D_2, \ldots, D_l$ are independent over $(\mathbb{Q}^\times)^2$ for some $l \leq k$ so that $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_l})$. For each $i \leq l$, write $\mathfrak{Q}_i$ for the prime above p and below $\mathfrak{P}$ in the intermediate field $\mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_i})$. In particular, $\mathfrak{Q}_1$ is the prime above p in $\mathbb{Q}(\sqrt{D_1})$ and $\mathfrak{Q}_l = \mathfrak{P}$.

If p splits or ramifies in all extensions $\mathbb{Q}(\sqrt{D_i})$, $i = 1, \ldots, k$, then each prime $\mathfrak{Q}_i$, $i \leq l$, splits or ramifies in the next extension containing $\mathfrak{Q}_{i+1}$. This follows from the fact that the polynomial $x^2 - D_{i+1}$ splits modulo p, so that the residue field of $\mathfrak{Q}_i$ remains $\mathbb{F}_p$ over $i = 1, \ldots, l$. It follows that $N_1(\mathfrak{P}) = \mathfrak{p}_1$.

Next, assume that p is inert in some quadratic extension. Then p is inert in $\mathbb{Q}(\sqrt{D_i})$ for some $i \leq l$, otherwise the argument above would give $N_{K/\mathbb{Q}}(\mathfrak{P}) = p$, but constructing K from $\mathbb{Q}(\sqrt{D_i})$ where p is inert shows $N_{K/\mathbb{Q}}(\mathfrak{P}) \geq p^2$. Let $i_0 \leq l$ be the first index for which p is inert in $\mathbb{Q}(\sqrt{D_{i_0}})$. The residue field of $\mathfrak{Q}_i$ is $\mathbb{F}_p$ for $1 \leq i \leq i_0 - 1$ and the residue field of $\mathfrak{Q}_{i_0}$ is $\mathbb{F}_{p^2}$, as $x^2 - D_{i_0}$ has no roots modulo p. From that point on, any polynomial $x^2 - D_i$ has roots in $\mathbb{F}_{p^2}$ so the residue field of $\mathfrak{Q}_i$ remains $\mathbb{F}_{p^2}$ for $i_0 \leq i \leq l$.

If p is inert in $\mathbb{Q}(\sqrt{D_1})$, then $i_0 = 1$ and $N_1(\mathfrak{P}) = (p)$, as all primes past (p) either split or ramify. If $i_0 > 1$, the only inert prime between $\mathfrak{p}_1$ and $\mathfrak{P}$ is $\mathfrak{Q}_{i_0}$, so that $N_1(\mathfrak{P}) = \mathfrak{p}_1^2$. The result follows by rearranging the discriminants. □

3.2. **Simultaneous representations.** We now use Hecke characters of K to characterize the primes that are simultaneously represented by $x^2 - d_1y^2$, ..., $x^2 - d_ky^2$.

Let $I_K(2)$ be the set of fractional ideals of K coprime to (2) and $P^+_{K,\mathbb{Z}}(2)$ its subset of integral ideals (α) with $\alpha \equiv 1 \mod (2)$ and $N_{K/\mathbb{Q}}(\alpha) > 0$. Define the ray class group

$$\mathfrak{C}(K) := I_K(2)/P^+_{K,\mathbb{Z}}(2) \tag{8}$$

Consider the map

$$\begin{aligned} \Phi = \Phi_{\mathcal{D}} : \mathfrak{C}^\vee(D_1) \times \cdots \times \mathfrak{C}^\vee(D_k) &\to \mathfrak{C}^\vee(K) \\ (\chi_1, \ldots, \chi_k) &\mapsto \chi := \prod_{i=1}^{k} \chi_i \circ N_i \end{aligned} \tag{9}$$

with $\mathfrak{C}(D_1), \dots, \mathfrak{C}(D_k)$ defined by (4). This is well defined since for any $\alpha \equiv 1 \mod (2)$ integral in K with $N_{K/\mathbb{Q}}(\alpha) > 0$ we have $N_i(\alpha) \equiv 1 \mod (2)$ and $N_{\mathbb{Q}(\sqrt{D_i})/\mathbb{Q}} \circ N_i(\alpha) > 0$, so that $\chi((\alpha)) = \prod \chi_i \circ N_i(\alpha) = 1$.

We say that characters $\chi_1 \in \mathfrak{C}^\vee(D_1), \dots, \chi_k \in \mathfrak{C}^\vee(D_k)$ *interact* if $(\chi_1, \dots, \chi_k) \in \ker \Phi$. In terms of L-functions, this translates to

$$L(s, \chi_1 \otimes \cdots \otimes \chi_k)^{[K:\mathbb{Q}]} = \zeta_K(s)^{2^k}$$

where $L(s, \chi_1 \otimes \cdots \otimes \chi_k)$ is the Rankin-Selberg convolution of $L(s, \chi_1), \dots, L(s, \chi_k)$, and $\zeta_K(s)$ is the Dedekind zeta function of K.

Before proceeding, we note that the dual $\mathrm{Cl}^\vee(K)$ of the usual class group of K would work just as well as $\mathfrak{C}^\vee(K)$ as co-domain of the map Φ if $\mathfrak{C}(D_i) = \mathrm{Cl}(D_i)$ for all $i = 1, \dots, k$ (in fact $\mathrm{Cl}^\vee(K) \leq \mathfrak{C}^\vee(K)$ in analogy to (7)). The need for the ray class group $\mathfrak{C}^\vee(K)$ comes from the fact that $\mathfrak{C}^\vee(D_i)$ might contain characters that are only trivial on principal ideals with positive norm or are only defined on ideals coprime to (2).

The map Φ controls the primes represented simultaneously by $x^2 - d_1y^2, \dots, x^2 - d_ky^2$. We see this by the following orthogonality relation:

LEMMA 3.2. *Let $\mathfrak{P}$ be a prime in K above a rational prime p that is not inert in any extension $\mathbb{Q}(\sqrt{D_1}), \dots, \mathbb{Q}(\sqrt{D_k})$. Then,*

$$\sum_{\chi \in \operatorname{im} \Phi} \chi(\mathfrak{P}) = \begin{cases} \#\operatorname{im}\Phi & \text{if } p = x^2 - d_iy^2,\ x, y \in \mathbb{Z},\ \forall\, i = 1, \dots, k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For each $i = 1, \dots, k$, let $\mathfrak{p}_i$ be the prime in $\mathbb{Q}(\sqrt{D_i})$ below $\mathfrak{P}$, and recall from Lemma 3.1 that $N_i\mathfrak{P} = \mathfrak{p}_\mathfrak{i}$. We have

$$\#\ker\Phi \left(\sum_{\chi \in \operatorname{im}\Phi} \chi(\mathfrak{P}) \right) = \sum_{\substack{\chi_i \in \mathfrak{C}^\vee(D_i) \\ i=1,\dots,k}} \chi_1(\mathfrak{p}_\mathfrak{1}) \cdots \chi_k(\mathfrak{p}_k) = \prod_{i=1}^{k} \left(\sum_{\chi_i \in \mathfrak{C}^\vee(D_i)} \chi_i(\mathfrak{p}_i) \right),$$

and the result follows by orthogonality in each $\mathfrak{C}^\vee(D_i)$ and Lemma 2.1. □

In addition to the proportion of primes represented by $x^2 - d_1y^2, \dots, x^2 - d_ky^2$, a crucial ingredient in the proofs of Theorem 1.1 and Theorem 1.4 is the sub-proportion of such primes satisfying certain congruence conditions modulo integers coprime to $2D_1 \dots D_k$.

PROPOSITION 3.3. *Let $\mathcal{Q} = \{Q_1, \dots, Q_n\}$ be a set of pairwise coprime fundamental discriminants which are coprime to $2D_1 \dots D_k$. Let $\pi_\mathcal{D}^\mathcal{Q}(X)$ denote the number of primes p up to X for which*

$$p = x^2 - d_iy^2,\ x, y \in \mathbb{Z}\, \forall\, i = 1, \dots, k, \text{ and } \chi_{Q_j}(p) = -1\, \forall\, j = 1, \dots, n.$$

Then

$$\lim_{X \to \infty} \frac{\pi_\mathcal{D}^\mathcal{Q}(X)}{\pi(X)} = \frac{1}{2^n \#\operatorname{im}\Phi \cdot [K:\mathbb{Q}]}.$$

The congruence conditions above translate into twists of elements of $\operatorname{im}\Phi$ by quadratic characters modulo $Q_1, \dots, Q_n$. In order to prove Proposition 3.3, we need to ensure that

these twists yield non-trivial Hecke characters. We record this fact in the following lemma, whose proof we postpone to the appendix:

LEMMA 3.4. *Let Q be a fundamental discriminant coprime to $2D_1 \dots D_k$, and let $\chi \in \mathfrak{C}^\vee(K)$. Then, the twist*

$$\chi \otimes \chi_Q(\cdot) := \chi(\cdot)\, \chi_Q \circ N_{K/\mathbb{Q}}(\cdot)$$

defines a non-trivial Hecke character of K on ideals coprime to $2Q$.

Proof of Proposition 3.3. Let P be the set of primes p which are simultaneously represented by $x^2 - d_1y^2, \dots, x^2 - d_ky^2$ and $\chi_{Q_i}(p) = -1$ for every $Q_i \in \mathcal{Q}$. Recall that an unramified prime in $K = \mathbb{Q}(\sqrt{D_1}, \dots, \sqrt{D_k})$ is represented simultaneously by $x^2 - d_1y^2, \dots, x^2 - d_ky^2$ when it satisfies the conditions described in (6) for each discriminant $D = D_1, \dots, D_k$.

Take p a prime unramified in K that splits in all extensions $\mathbb{Q}(\sqrt{D_1}), \dots, \mathbb{Q}(\sqrt{D_k})$, and let $\mathfrak{P}$ be a prime in K above p. By Lemma 3.2,

$$\sum_{\substack{\chi \in \operatorname{im}\Phi \\ \{Q_{i_1}, \dots, Q_{i_\eta}\} \subset \mathcal{Q}}} (-1)^\eta\, \chi(\mathfrak{P})(\chi_{Q_{i_1}} \cdots \chi_{Q_{i_\eta}})(p) = \begin{cases} 2^n \# \operatorname{im}\Phi & \text{if } p \in P \\ 0 & \text{otherwise.} \end{cases}$$

For each $\chi \in \operatorname{im}\Phi$ and each subset $\{Q_{i_1}, \dots, Q_{i_\eta}\} \subset \mathcal{Q}$, consider the log-derivative

$$-\frac{L'}{L}(s, \chi \otimes \chi_{Q_{i_1}} \cdots \chi_{Q_{i_\eta}}) = \sum_{\mathfrak{Q}, m \geq 1} \frac{\log N\mathfrak{Q}}{(N\mathfrak{Q})^{ms}}\, \chi^m(\mathfrak{Q})(\chi_{Q_{i_1}} \cdots \chi_{Q_{i_\eta}})^m(N\mathfrak{Q}),$$

where $\mathfrak{Q}$ ranges over the primes of K and N is the norm $N_{K/\mathbb{Q}}$. Take q a prime unramified in K. By Lemma 3.1, all $\mathfrak{Q}$ in K above q satisfy $N\mathfrak{Q} = q$ if q splits in all $\mathbb{Q}(\sqrt{D_1}), \dots, \mathbb{Q}(\sqrt{D_k})$. As $K/\mathbb{Q}$ is Galois, there will be $[K : \mathbb{Q}]$ such primes. Similarly, all $\mathfrak{Q}$ in K above q satisfy $N\mathfrak{Q} = q^2$ if q is inert in some $\mathbb{Q}(\sqrt{D_1}), \dots, \mathbb{Q}(\sqrt{D_k})$. We conclude that

$$-\sum_{\substack{\chi \in \operatorname{im}\Phi \\ \{Q_{i_1}, \dots, Q_{i_\eta}\} \subset \mathcal{Q}}} (-1)^\eta \frac{L'}{L}(s, \chi \otimes \chi_{Q_{i_1}} \cdots \chi_{Q_{i_\eta}}) = 2^n \# \operatorname{im}\Phi \cdot [K : \mathbb{Q}] \sum_{p \in \mathcal{P}} \frac{\log p}{p^s} + G(s)$$

where $G(s)$ is a Dirichlet series converging absolutely in the region $\Re s > 1/2$.

By Lemma 3.4, the character $\chi \otimes \chi_{Q_{i_1}} \cdots \chi_{Q_{i_\eta}} = \chi \otimes \chi_{Q_{i_1} \cdots Q_{i_\eta}}$ is a non-trivial Hecke character of K unless χ is trivial and $\eta = 0$, in which case the corresponding L-function has a simple pole at $s = 1$. Moreover, $L(s, \chi \otimes \chi_{Q_{i_1} \cdots Q_{i_\eta}})$ has a standard zero-free region with at most one simple real zero $\beta < 1$ (see Theorem 5.35 in [10]). The result now follows from a standard argument using the explicit formula followed by partial summation. □

4. Interactions of class groups

In this section we study the kernel of the map Φ defined by (9), which records the interactions of the dual class groups $\mathfrak{C}^\vee(D_1), \dots, \mathfrak{C}^\vee(D_k)$.

4.1. **General properties.** Our next result shows that only the 2-parts of these groups can interact. Moreover, we give a bound for the order of the characters in a k-tuple of $\ker\Phi$ in terms of multiplicative independencies of $D_1,\dots,D_k$ over $(\mathbb{Q}^\times)^2$.

PROPOSITION 4.1. *Let $(\chi_1,\cdots,\chi_k)\in\ker\Phi$. For each $i=1,\dots,k$, let n_i be the minimum number of subsets $H_1,\dots,H_{n_i}\subset\{D_1,\dots,D_k\}$ for which the elements of $\{D_i\}\cup H_j$ are independent over $(\mathbb{Q}^\times)^2$ and every discriminant different from D_i is contained in some H_j. Then*

$$\chi_i^{2^{n_i+1}} \text{ is the trivial character.}$$

In particular, if all discriminants are independent over $(\mathbb{Q}^\times)^2$,

$$\operatorname{ord}\chi_i \mid 4 \text{ for every } i=1,\dots,k.$$

Moreover, we have that χ_1^2, χ_2^2 are trivial when $k=2$.

Proof. Let p be a prime that is not inert in any extension $\mathbb{Q}(\sqrt{D_1}),\dots,\mathbb{Q}(\sqrt{D_k})$. Let $\mathfrak{P}$ be a prime in K above p, and $\mathfrak{p}_1,\dots,\mathfrak{p}_k$ be the primes below $\mathfrak{P}$ in the quadratic extensions. As $(\chi_1,\cdots,\chi_k)$ is in $\ker\Phi$, Lemma 3.1 gives

$$\chi_1(\mathfrak{p}_1)\dots\chi_k(\mathfrak{p}_k)=1.$$

Take a partition $H_1,\dots,H_{n_i}$ of the discriminants different from D_i where the minimum n_i is realized (we can assume that $H_1,\dots,H_{n_i}$ are pairwise disjoint). By independence over $(\mathbb{Q}^\times)^2$, there is an automorphism σ_j of K for each H_j that fixes $\sqrt{D_i}$ and changes the sign of $\sqrt{D_l}$ for D_l in H_j. We consider the ideal

$$\mathfrak{a}=\prod_{\substack{\epsilon_j\in\{0,1\}\\ j=1,\dots,n_i}}\sigma_j^{\epsilon_j}\mathfrak{P}.$$

Notice that for any $l\neq i$ there is a σ_j that changes the sign of $\sqrt{D_l}$. Writing $\mathfrak{a}=\mathfrak{b}\sigma_j\mathfrak{b}$ shows that $N_l\mathfrak{a}=(p)^{2^{n_i-1}}$. Multiplying over all $l\neq i$ and using that $(\chi_1,\dots,\chi_k)$ is in $\ker\Phi$ gives

$$\chi_i^{2^{n_i}}(\mathfrak{p}_i)=1.$$

We proceed in the same way when p is inert in some extension $\mathbb{Q}(\sqrt{D_1}),\dots,\mathbb{Q}(\sqrt{D_k})$. If p is inert in $\mathbb{Q}(\sqrt{D_i})$, we get $\chi_i((p))=1$ automatically. Otherwise, let $\mathfrak{P}$ be a prime in K and $\mathfrak{p}_i=\mathfrak{p}_{i_1},\mathfrak{p}_{i_2},\dots,\mathfrak{p}_{i_l}$ be the primes below $\mathfrak{P}$ in the quadratic extensions $\mathbb{Q}(\sqrt{D_i})=\mathbb{Q}(\sqrt{D_{i_1}}),\mathbb{Q}(\sqrt{D_{i_2}}),\dots,\mathbb{Q}(\sqrt{D_{i_l}})$ where p is not inert. Since $(\chi_1,\dots,\chi_k)\in\ker\Phi$, we have by Lemma 3.1

$$\chi_i^2(\mathfrak{p}_i)\chi_{i_2}^2(\mathfrak{p}_{i_2})\dots\chi_{i_l}^2(\mathfrak{p}_{i_l})=1.$$

Repeating the argument above using the same partition $H_1,\dots,H_n$, we get

$$\chi_i^{2^{n_i+1}}(\mathfrak{p}_i)=1.$$

This proves that $\chi_i^{2^{n_i+1}}$ is trivial on every prime ideal of $\mathbb{Q}(\sqrt{D_i})$, so it must be the trivial character. If $D_1,\dots,D_k$ are multiplicatively independent over $(\mathbb{Q}^\times)^2$, one can take $n_i=1$ with H_1 containing all discriminants but D_i. The last assertion for $k=2$ follows easily by taking a single automorphism in the discussion above on primes that split in both extensions. The result follows. □

We remark that a similar result appeared in the work of Blomer [2] under a coprimality condition that forced the kernel to be empty. In the case where the discriminants $D_1, \dots, D_k$ are independent over $(\mathbb{Q}^\times)^2$, we will show later in Corollary 4.9 that the maximum order 4 for elements in $\ker \Phi$ is indeed attained.

A consequence of Proposition 4.1 is that extending the group $\mathrm{Cl}^{+\vee}(D_i)$ to $\mathfrak{C}^\vee(D_i)$ in the sense of (7) does not create new interactions in the kernel of Φ. In other words, all interactions happen between the 2-parts of the duals of the narrow class groups.

COROLLARY 4.2. *We have*

$$\ker \Phi \subset \mathrm{Cl}^{+\vee}(D_1)[2^\infty] \times \cdots \times \mathrm{Cl}^{+\vee}(D_k)[2^\infty].$$

Proof. This follows from definition (4), Lemma 2.2, and Proposition 4.1. □

4.2. **The genus kernel.** We now study the subgroup of $\ker \Phi$ of elements of order 2, namely

$$\ker \Phi\,[2] = \{(\chi_1, \dots, \chi_k) \in \ker \Phi : \chi_i^2 \text{ is trivial for every } i = 1, \dots, k\}. \tag{10}$$

By Corollary 4.2 we have $\chi_i \in \mathrm{Cl}^{+\vee}(D_i)[2]$ for each $i = 1, \dots, k$, so these are genus characters of the narrow class groups. For this reason, we refer to this part of the kernel as the *genus kernel* of Φ.

Our next goal is to compute the size of $\ker \Phi\,[2]$ for any set of fundamental discriminants $D_1, \dots, D_k$. We introduce some notation in order to state this result.

Given two fundamental discriminants D and D', we say that D' divides D in the sense of discriminants if there is another fundamental discriminant D'' for which $D = D'D''$. Denote this relation by $D' \mid_{\mathrm{disc}} D$. As usual, let $\omega(n)$ be the number of prime factors of n, and $\omega_{\mathrm{odd}}(n)$ be the number of odd prime factors. Let

$$\omega_*(D_1, \dots, D_k) = \omega_{\mathrm{odd}}(D_1 \dots D_k) + \begin{cases} 2 & \text{if } \#\{u \in \{-4, 8, -8\} : u \mid_{\mathrm{disc}} D_i \text{ for some } i\} \geq 2 \\ 1 & \text{if } \#\{u \in \{-4, 8, -8\} : u \mid_{\mathrm{disc}} D_i \text{ for some } i\} = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

We now state our result:

PROPOSITION 4.3. *With $\omega_*(D_1, \dots, D_k)$ defined by (11), we have*

$$\#\ker \Phi\,[2] = 2^{\omega(D_1)+\cdots+\omega(D_k)-k-\omega_*(D_1,\dots,D_k)}[K : \mathbb{Q}].$$

We will need an auxiliary lemma, whose proof we postpone to the appendix:

LEMMA 4.4. *Let D_0 be a fundamental discriminant. Assume that for every prime p sufficiently large for which*

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1, \text{ we have } \chi_{D_0}(p) = 1.$$

Then D_0 is dependent of $D_1, \dots, D_k$ over $(\mathbb{Q}^\times)^2$.

Proof of Proposition 4.3. Let $(\chi_1, \dots, \chi_k) \in \ker \Phi\,[2]$. As each χ_i is in $\mathrm{Cl}^{+\vee}(D_i)[2]$, we know by genus theory that there is a factorization $D_i = D_i'D_i''$ into fundamental discriminants for which for which $\chi_i = \chi_{D_i', D_i''}$. Our goal is to understand when $\chi = \Phi(\chi_{D_1', D_1''}, \dots, \chi_{D_k', D_k''})$ is trivial, and we will do this by testing χ against the primes of K.

Recall that χ is a character of $\mathfrak{C}(K)$, as defined in (8). A standard argument shows that each class of $\mathfrak{C}(K)$ contains infinitely many primes of K, so it suffices to show that χ is trivial on the primes of K lying above unramified odd primes p. Let $\mathfrak{P}$ be such a prime. Assume first that p is inert in some $\mathbb{Q}(\sqrt{D_i})$. By Lemma 3.1, each norm $N_i\mathfrak{P}$ is either the square of a prime or a principal ideal so that $\chi_{D_i',D_i''}(N_i\mathfrak{P}) = 1$, yielding $\chi(\mathfrak{P}) = 1$ automatically. It remains check the primes $\mathfrak{P}$ for which p splits in every quadratic extension.

In that case, $\chi(\mathfrak{P}) = 1$ translates to $\chi_{D_0}(p) = 1$, where D_0 is the unique fundamental discriminant associated to the product $D_1' \dots D_k'$ (that is, D_0 has the same squarefree part as the product). We would like to check whether the relations

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1 \text{ can imply } \chi_{D_0}(p) = 1.$$

By Lemma 4.4, this only happens when D_0 is in $\langle D_1, \dots, D_k\rangle(\mathbb{Q}^\times)^2$, and the converse is clearly true. Therefore, we would like to count the number of k-tuples

$$D_i' \mid_{\text{disc}} D_i,\ i = 1, \dots, k \text{ for which } D_1' \dots D_k' \in \langle D_1, \dots, D_k\rangle(\mathbb{Q}^\times)^2.$$

The size of $\ker \Phi\,[2]$ will be this quantity divided by 2^k, as each k-tuple of genus characters in $\ker \Phi\,[2]$ corresponds to 2^k of the k-tuples above (with two choices, D_i' and D_i'', for each discriminant).

We now factor a discriminant into prime discriminants. Set $q^* = (-1)^{\frac{q-1}{2}} q$ for $q \geq 3$ prime. For each D_i, write

$$D_i = u_i \prod_{\substack{q \mid D_i \\ q \text{ odd}}} q^*$$

where $u_i \in \{1, -4, 8, -8\}$. Notice that all factors above are also fundamental discriminants, and this factorization is unique. Moreover, the only relation between $-4, 8, -8$ and q^*, q odd prime, over $(\mathbb{Q}^\times)^2$ is $-4 \cdot 8 \equiv -8$. Define the vector space

$$W = \mathbb{F}_2^2 \times \prod_{\substack{q \mid D_1 \dots D_k \\ q \text{ odd}}} \mathbb{F}_2.$$

Let $e_1 = (0, 0; \mathbf{0})$, $e_{-4} = (1, 0; \mathbf{0})$, $e_8 = (0, 1; \mathbf{0})$, $e_{-8} = (1, 1; \mathbf{0})$, $e_{q^*} = (0, 0; \mathbf{1}_q)$ be in W, and V be the subspace of W generated by all e_{u_i} and all e_{q^*}, so that $\dim V = \omega_*(D_1, \dots, D_k)$. For $i = 1, \dots, k$, set

$$v_i = e_{u_i} + \sum_{\substack{q \mid D_i \\ q \text{ odd}}} e_{q^*}, \text{ and } V_{disc} = \langle v_1, \dots, v_k\rangle,$$

where $2^{\dim V_{disc}} = [K : \mathbb{Q}]$. Next, define the subspace of discriminant factors of D_i by

$$E_i = \langle e_{u_i}, e_{q^*} : q \mid D_i \text{ odd}\rangle,\ i = 1, \dots, k.$$

Notice that $\dim E_i = \omega(D_i)$. As $D_i' \mid_{\text{disc}} D_i$, each discriminant factor has the form

$$D_i' = u_i^{\eta_i} \prod_{\substack{q \mid D_i \\ q \text{ odd}}} (q^*)^{\epsilon_q},\ \eta_i, \epsilon_q \in \{0, 1\}, \text{ corresponding to } v_i' = \eta_i e_{u_i} + \sum_{\substack{q \mid D_i \\ q \text{ odd}}} \epsilon_q e_{q^*} \in E_i.$$

Our problem now is to count how many choices of $D_1', \dots, D_k'$ yield $v_1' + \dots + v_k' \in V_{disc}$.

To that end, consider the map

$$\begin{aligned} E_1 \times \cdots \times E_k &\to V/V_{disc} \\ (v_1', \ldots, v_k') &\mapsto (v_1' + \cdots + v_k') + V_{disc} \end{aligned}$$

Each k-tuple in its kernel corresponds to a desired choice of $D_1', \ldots, D_k'$. As each generator of V lies in at least one E_i, this map is surjective, hence its kernel has size

$$2^{\dim E_1 + \cdots + \dim E_k - \dim V + \dim V_{disc}} = 2^{\omega(D_1)+\cdots+\omega(D_k)-\omega_*(D_1,\ldots,D_k)}[K:\mathbb{Q}].$$

The result follows by grouping together the choices of D_i' and D_i'' for $i = 1, \ldots, k$, dividing the number above by 2^k. □

We now combine Proposition 3.3 and Proposition 4.3 into a single statement, which is the main tool in the proofs of Theorem 1.1 and Theorem 1.4.

THEOREM 4.5. *Let $\mathcal{D} = \{D_1, \ldots, D_k\}$ be a set of fundamental discriminants, and denote by d_i the squarefree part of D_i. Let Φ be the map defined by (9), and let $\iota(D_1, \ldots, D_k) \in \mathbb{Z}_{\geq 0}$ be such that*

$$2^{\iota(D_1,\ldots,D_k)} = \ker \Phi / \ker \Phi\,[2].$$

Let $\mathcal{Q} = \{Q_1, \ldots, Q_n\}$ be a set of pairwise coprime fundamental discriminants which are coprime to $2D_1 \ldots D_k$, and let $\pi_{\mathcal{D}}^{\mathcal{Q}}(X)$ denote the number of primes p up to X for which

$$p = x^2 - d_i y^2,\ x, y \in \mathbb{Z}\ \forall\, i = 1, \ldots, k, \text{ and } \chi_{Q_j}(p) = -1\ \forall\, j = 1, \ldots, n.$$

Then, with $\mathfrak{h}(D)$ defined by (5) and $\omega_*(D_1, \ldots, D_k)$ defined by (11), we have

$$\lim_{X\to\infty} \frac{\pi_{\mathcal{D}}^{\mathcal{Q}}(X)}{\pi(X)} = \frac{2^{\omega(D_1)+\cdots+\omega(D_k)-\omega_*(D_1,\ldots,D_k)}}{2^{n+k}\mathfrak{h}(D_1)\ldots\mathfrak{h}(D_k)} \cdot 2^{\iota(D_1,\ldots,D_k)}.$$

4.3. **Sets without higher interaction.** The proofs of Theorem 1.1 and Theorem 1.4 rely on applying inclusion-exclusion to sets of discriminants for which $\ker \Phi = \ker \Phi\,[2]$. The next result exhibits these sets.

PROPOSITION 4.6. *Take a finite subset of discriminants from*

$$D = -4, -8, -p, -8p, \text{ where } p \equiv 3 \mod 4.$$

Then $\ker \Phi = \ker \Phi\,[2]$.

We will need two auxiliary lemmas, whose proofs we present in the appendix. The first one characterizes order 4 characters of the narrow class group $\mathrm{Cl}^+(D)$ in terms of certain unramified extensions of $\mathbb{Q}(\sqrt{D})$, and it essentially goes back to the classical work of Rédei [14].

LEMMA 4.7. *Let $D = de$ be a factorization of D into fundamental discriminants, and assume that $\chi_{d,e}$ is the square of a character in $\mathrm{Cl}^{+\vee}(D)$. Then, there exists integers $x, y, z \in \mathbb{Z}\backslash\{0\}$ satisfying*

$$x^2 - dy^2 - ez^2 = 0$$

for which

$$\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}\big(\sqrt{d}, \sqrt{e}, \sqrt{x + y\sqrt{d}}\big) \text{ is unramified.}$$

Moreover, given any prime $\mathfrak{p}$ *in* $\mathbb{Q}(\sqrt{D})$ *above a rational prime* p *for which* $\chi_{D',D''}(\mathfrak{p}) = 1$ *for all genus characters* $\chi_{D',D''} \in \mathrm{Cl}^{+\vee}(D)[2]$*, and any* ψ *with* $\psi^2 = \chi_{d,e}$*, we have*

$$\psi(\mathfrak{p}) = \left(\frac{x + y\sqrt{d}}{p}\right).$$

For a thorough exposition of this topic, see Stevenhagen's article [16]. The second result states that a quartic relation cannot be implied by quadratic ones.

LEMMA 4.8. *Let* d, e *be coprime integers in* $\langle D_1, \dots, D_k\rangle(\mathbb{Q}^\times)^2 \setminus (\mathbb{Q}^\times)^2$ *such that*

$$x^2 - dy^2 - ez^2 = 0$$

for some $x, y, z \in \mathbb{Z} \setminus \{0\}$*. Assume that for every prime* p *sufficiently large for which*

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1, \text{ we have } \left(\frac{x + y\sqrt{d}}{p}\right) = 1.$$

Then $\sqrt{x + y\sqrt{d}} \in \mathbb{Q}(\sqrt{d})$.

We proceed to prove Proposition 4.6.

Proof of Proposition 4.6. Let $-8p_1, \dots, -8p_k, D_1, \dots, D_m$ be the subset of discriminants, where each D_j is $-4, -8$, or $-p$. Recall from Proposition 4.1 that the characters attached to the entries of an element in $\ker \Phi$ have order equal to a power of 2. In particular, the characters attached to the entries $\mathfrak{C}^\vee(D_j)$ are trivial as $\mathfrak{h}(D_j)$ are odd (by genus theory and Lemma 2.2).

We now assume by contradiction that there is $(\chi_1, \dots, \chi_k, \chi_0, \dots, \chi_0) \in \ker \Phi \setminus \ker \Phi\,[2]$, with χ_0 denoting the trivial character. By possibly taking powers of 2, we can assume that every χ_i has order dividing 4 and at least one of them has order exactly 4. Say $\chi_1, \dots, \chi_l$, $l \leq k$, have order 4, and the remaining characters have order 1 or 2.

For each $i = 1, \dots, l$ let $x_i, y_i, z_i \in \mathbb{Z} \setminus \{0\}$ be the integer triple associated to χ_i as described in Lemma 4.7. Let q be a prime satisfying

$$\chi_{-4}(q) = \chi_8(q) = \chi_{-8}(q) = 1 \text{ and } \chi_{p^*}(q) = 1 \,\forall \text{ odd prime } p \mid p_1 \dots p_k D_1 \dots D_m.$$

The prime q splits completely in the multiquadratic extension containing the square-root of the discriminants of the subset above. For each $i = 1, \dots, l$ let $\mathfrak{q}_i$ be a prime above q in $\mathbb{Q}(\sqrt{-8p_i})$. By Lemma 4.7,

$$\chi_i(\mathfrak{q}_i) = \left(\frac{x_i + 2y_i\sqrt{2}}{p}\right)$$

and since $(\chi_1, \dots, \chi_k, \chi_0, \dots, \chi_0) \in \ker \Phi$, it follows that

$$\left(\frac{(x_1 + 2y_1\sqrt{2}) \dots (x_l + 2y_l\sqrt{2})}{q}\right) = 1.$$

By Lemma 4.8, the product $(x_1 + 2y_1\sqrt{2}) \dots (x_l + 2y_l\sqrt{2})$ must be a square in $\mathbb{Q}(\sqrt{2})$. However, $x_i^2 - 8y_i^2 = -p_i z_i^2$, so the norm of this product is $(-1)^l p_1 \dots p_l (z_1 \dots z_l)^2$ which is not a square, a contraction. We conclude that $\ker \Phi = \ker \Phi\,[2]$. □

4.4. **Higher order interactions.** In this subsection we give two explicit examples of order 4 interactions based on the triples of forms from Theorem 1.2. We start by proving Theorem 1.2, which relies on the structure of the class groups at hand and the characterization of their order 4 characters given by Lemma 4.7. Afterwards, we show that $\ker \Phi / \ker \Phi\,[2] = 2$ for the corresponding maps Φ defined by (9).

Proof of Theorem 1.2. Let d be a squarefree number and D be the fundamental discriminant with squarefree part d. By Lemma 2.1, a prime p not dividing D is of the form $x^2 - dy^2$ if and only if p splits in $\mathbb{Q}(\sqrt{D})$ and a prime $\mathfrak{p}$ above p satisfies $\chi(\mathfrak{p}) = 1$ for all $\chi \in \mathfrak{C}^\vee(D)$. For all values $d \in \{-17, -34, -65, -66, -1105, -1122\}$ we have $D = 4d < 0$, hence by (3) and (4) the group $\mathfrak{C}(D)$ is the usual class group $\mathrm{Cl}(D)$.

In what follows, we use the data from the LMFDB [12] to determine the structure of the dual class grups $\mathrm{Cl}^\vee(D)$.

a) We have

$$\mathrm{Cl}^\vee(-68) \cong \mathbb{Z}/4\mathbb{Z},\ \mathrm{Cl}^\vee(-260) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \text{ and }\ \mathrm{Cl}^\vee(-4420) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The assumption $\chi_{-4}(p) = \chi_5(p) = \chi_{13}(p) = \chi_{17}(p) = 1$ ensures that the primes above p in $\mathbb{Q}(\sqrt{-17})$, $\mathbb{Q}(\sqrt{-65})$, and $\mathbb{Q}(\sqrt{-1105})$ satisfy all genus conditions from the class groups $\mathrm{Cl}(-68)$, $\mathrm{Cl}(-260)$, and $\mathrm{Cl}(-4420)$. It remains to show that the conditions from order 4 characters are satisfied in all or one of these groups.

We start by showing that the solution $(x, y, z) = (1, 2, 1)$ to

$$x^2 + 4y^2 - 17z^2 = 0$$

yields an unramified extension $\mathbb{Q}(\sqrt{-17}) \subset \mathbb{Q}(i, \sqrt{17}, \sqrt{1+4i})$. In fact, by Corollary 7.4 in [16] there is a twist $t \in \{\pm 1, \pm 2\}$ for which $\mathbb{Q}(\sqrt{-17}) \subset \mathbb{Q}(i, \sqrt{17}, \sqrt{t(1+4i)})$ is unramified. By Proposition 7.2, [16], exactly two such values of t make this extension unramified over 2, and the values t and $-t$ yield the same extension. Since $\mathbb{Q}(\sqrt{-17}) \subset \mathbb{Q}(i, \sqrt{17})$ is unramified, it suffices to show that $\mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{1+4i})$ is as well, and this follows from the fact that $1 + 4i$ is coprime to $(2) \subset \mathbb{Q}(i)$ and $1 + 4i \in \mathbb{Z}[i]$ is congruent to a square modulo (4). Therefore $\mathbb{Q}(\sqrt{-17}) \subset \mathbb{Q}(i, \sqrt{17}, \sqrt{1+4i})$ is unramified.

Letting $\psi_{-4,\,17}$ be a order 4 character order of $\mathrm{Cl}(-68)$ and $\mathfrak{p}_{-17}$ be a prime above p in $\mathbb{Q}(\sqrt{-17})$, we have by Lemma 4.7

$$\psi_{-4,\,17}(\mathfrak{p}_{-17}) = \left(\frac{1+4i}{p}\right).$$

Similarly, the solutions $(x, y, z) = (1, 4, 1)$ and $(x, y, z) = (-31, 6, 1)$ to

$$x^2 + 4y^2 - 65z^2 = 0 \text{ and } x^2 + 4y^2 - 1105z^2 = 0$$

yield $\mathbb{Q}(\sqrt{-65}) \subset \mathbb{Q}(i, \sqrt{65}, \sqrt{1+8i})$, $\mathbb{Q}(\sqrt{-1105}) \subset \mathbb{Q}(i, \sqrt{1105}, \sqrt{-31+12i})$ unramified. Letting $\psi_{-4,\,65}$ and $\psi_{-4,\,1105}$ be characters of order 4 of $\mathrm{Cl}(-260)$ and $\mathrm{Cl}(-4420)$, and $\mathfrak{p}_{-65}$ and $\mathfrak{p}_{-1105}$ be primes above p in $\mathbb{Q}(\sqrt{-65})$ and $\mathbb{Q}(\sqrt{-1105})$, we have by Lemma 4.7

$$\psi_{-4,\,65}(\mathfrak{p}_{-65}) = \left(\frac{1+8i}{p}\right) \text{ and } \psi_{-4,\,1105}(\mathfrak{p}_{-1105}) = \left(\frac{-31+12i}{p}\right).$$

Therefore

$$\psi_{-4,\,17}(\mathfrak{p}_{-17})\,\psi_{-4,\,65}(\mathfrak{p}_{-65})\,\psi_{-4,\,1105}(\mathfrak{p}_{-1105}) = 1,$$

so that one or all of these factors equal to one. Using that the order 4 characters above together with the genus characters generate their corresponding dual class groups, we deduce that p satisfies the conditions in one or all of the class groups. The result follows.

b) We proceed as above. We have

$$\mathrm{Cl}^\vee(-136) \cong \mathbb{Z}/4\mathbb{Z},\ \mathrm{Cl}^\vee(-264) \cong \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \text{ and }\ \mathrm{Cl}^\vee(-4488) \cong \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

The primes above p satisfy all genus conditions from their corresponding class groups. Next, we show that the solutions $(x,y,z) = (3,1,1), (-5,-1,1)$, and $(-7,-8,1)$ to

$$x^2+8y^2-17z^2=0,\ x^2+8y^2-33z^2=0,\ \text{and } x^2+8y^2-561z^2=0$$

yield $\mathbb{Q}(\sqrt{-34}) \subset \mathbb{Q}(\sqrt{-2},\sqrt{17},\sqrt{3+2\sqrt{-2}})$, $\mathbb{Q}(\sqrt{-66}) \subset \mathbb{Q}(\sqrt{-2},\sqrt{33},\sqrt{-5-2\sqrt{-2}})$, and $\mathbb{Q}(\sqrt{-1122}) \subset \mathbb{Q}(\sqrt{-2},\sqrt{561},\sqrt{-7+16\sqrt{-2}})$ unramified.

We focus on the first extension. Notice that $(\sqrt{3+2\sqrt{-2}}+\sqrt{3-2\sqrt{-2}})^2 = 2(3+\sqrt{17})$, therefore

$$\mathbb{Q}\Big(\sqrt{-2},\sqrt{17},\sqrt{3+2\sqrt{-2}}\Big) = \mathbb{Q}\Big(\sqrt{-2},\sqrt{17},\sqrt{2(3+\sqrt{17})}\Big).$$

For any odd prime q, the primes above q in $\mathbb{Q}(\sqrt{-34})$ do not ramify in the extension above. In fact, the intermediate extension $\mathbb{Q}(\sqrt{-34}) \subset \mathbb{Q}(\sqrt{-2},\sqrt{17})$ is unramified over q and either $3+2\sqrt{-2}$ or $2(3+\sqrt{17})$ is a unit modulo (q). To see that no primes above 2 ramify, it suffices to notice that $3+2\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ is coprime to (2) and congruent to a square modulo (4). This shows that the extension $\mathbb{Q}(\sqrt{-34}) \subset \mathbb{Q}(\sqrt{-2},\sqrt{17},\sqrt{3+2\sqrt{-2}})$ is unramified.

The same argument shows that the other two extensions are unramified as well. Letting $\psi_{-8,17}$, $\psi_{-8,33}$, and $\psi_{-8,561}$ be order 4 characters of $\mathrm{Cl}(-136)$, $\mathrm{Cl}(-264)$, and $\mathrm{Cl}(-4488)$, and $\mathfrak{p}_{-34}$, $\mathfrak{p}_{-66}$, and $\mathfrak{p}_{-1122}$ be primes above p in $\mathbb{Q}(\sqrt{-34})$, $\mathbb{Q}(\sqrt{-66})$, and $\mathbb{Q}(\sqrt{-1122})$, we have by Lemma 4.7

$$\psi_{-8,17}(\mathfrak{p}_{-34}) = \left(\frac{3+2\sqrt{-2}}{p}\right),\ \psi_{-8,33}(\mathfrak{p}_{-66}) = \left(\frac{-5-2\sqrt{-2}}{p}\right),$$
$$\text{and } \psi_{-8,561}(\mathfrak{p}_{-1122}) = \left(\frac{-7-16\sqrt{-2}}{p}\right).$$

Therefore

$$\psi_{-8,17}(\mathfrak{p}_{-34})\,\psi_{-8,33}(\mathfrak{p}_{-66})\,\psi_{-8,561}(\mathfrak{p}_{-1122}) = 1$$

and the conclusion follows as before. □

Corollary 1.3 is an immediate consequence of Theorem 1.2:

Proof of Corollary 1.3. Let p be a prime represented by two of these forms. Then, for every odd prime q dividing $d_1d_2d_3$, we have

$$\left(\frac{p}{q}\right) = 1.$$

When $\{d_1,d_2,d_3\} = \{17,65,1105\}$, the equation $x^2+d_iy^2 = p$ taken modulo 4 implies that $p \equiv 1 \bmod 4$. Similarly, when $\{d_1,d_2,d_3\} = \{34,66,1122\}$ we must have $p \equiv 1,3 \bmod 8$. Therefore the conditions from Theorem 1.2 are met, and as p is represented by at least two of the forms, it must be represented by all three. □

The results above show that there are higher order interactions between the dual class groups attached to the forms from Theorem 1.2.

COROLLARY 4.9. *Let $\mathcal{D}$ be either $\{-68,-260,-4420\}$ or $\{-136,-264,-4488\}$ and $\Phi=\Phi_{\mathcal{D}}$ be the map defined by (9). Then*

$$\ker\Phi/\ker\Phi\,[2]=2.$$

Proof. Write $\mathcal{D}=\{D_1,D_2,D_3\}$ with $|D_1|<|D_2|<|D_3|$ and let d_i denote the squarefree part of $-D_i$. By Corollary 1.3, any prime represented simultaneously by $x^2+d_1y^2$, $x^2+d_2y^2$ is also represented by $x^2+d_3y^2$. We now use Theorem 4.5 to compare the proportion of primes represented simultaneously by the first two forms and by all three.

By (3) and (4) we know that $\mathfrak{C}(D_i)=\mathrm{Cl}(D_i)$ for all three discriminants, and from the data of the LMFDB [12] we see that $\mathfrak{h}(D_1)=4$, $\mathfrak{h}(D_2)=8$, and $\mathfrak{h}(D_3)=16$. Moreover by Proposition 4.1 the map $\Phi_{\{D_1,D_2\}}$ defined by (9) satisfies $\ker\Phi_{\{D_1,D_2\}}=\ker\Phi_{\{D_1,D_2\}}[2]$, hence it follows from Theorem 4.5 that the proportion of primes represented simultaneously by $x^2+d_1y^2$, $x^2+d_2y^2$ is $\frac{1}{64}$. Similarly, Theorem 4.5 tells us that the proportion of primes represented simultaneously by $x^2+d_1y^2$, $x^2+d_2y^2$, $x^2+d_3y^2$ is $2^{\iota(D_1,D_2,D_3)}/128$, where $2^{\iota(D_1,D_2,D_3)}=\ker\Phi/\ker\Phi\,[2]$. Since these proportions match, we conclude that $\ker\Phi/\ker\Phi\,[2]=2$. □

5. Covering primes by $x^2\pm dy^2$, $d\le\Delta$

In this section we use the theory developed above to determine the proportion of primes covered by $x^2\pm dy^2$, $d\le\Delta$, leading up to the statements of Theorem 1.1 and Theorem 1.4. The main ingredient here is Theorem 4.5, combined with a result about sums of inverses of class numbers.

5.1. Sums of inverses of class numbers.

The bounds in Theorem 1.1 and Theorem 1.4 ultimately come from summing inverses of class numbers in certain prime families, which by the class number formula translates into a sum of inverses $L(1,\chi_D)^{-1}$. The next result adapts the work of Granville and Soundararajan [7] on the distribution of $L(1,\chi_D)$ to find the first negative moment over these families.

LEMMA 5.1. *Let $a\in(\mathbb{Z}/8\mathbb{Z})^\times$ and $u\in\{1,-4,8,-8\}$ be a fundamental discriminant. Then*

$$\sum_{\substack{p\le x\\ p\equiv a \bmod 8}}\frac{1}{L(1,\chi_{up^*})}=\frac{1}{4}\cdot\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right).$$

We postpone the proof to the appendix. In terms of class numbers, this translates to

COROLLARY 5.2. *We have*

$$\sum_{\substack{p\le x\\ p\equiv 3 \bmod 4}}\frac{1}{h(-8p)}\sim\frac{\pi}{2\sqrt{2}}\cdot\frac{\sqrt{x}}{\log x}$$

and for $a \in \{\bar{3}, \bar{7} \pmod 8\}$,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{h(-p)} \sim \frac{\pi}{2} \cdot \frac{\sqrt{x}}{\log x}.$$

Moreover

$$\sum_{\substack{p \le x \\ p \equiv 3 \bmod 4}} \frac{1}{h(4p)} \ge \frac{\sqrt{x}}{2} + O\left(\frac{\sqrt{x}}{\log x}\right), \quad \sum_{\substack{p \le x \\ p \equiv 3 \bmod 4}} \frac{1}{h(8p)} \ge \frac{\sqrt{x}}{2\sqrt{2}} + O\left(\frac{\sqrt{x}}{\log x}\right)$$

and for $a \in \{\bar{1}, \bar{5} \pmod 8\}$,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{h(p)} \ge \frac{\sqrt{x}}{2} + O\left(\frac{\sqrt{x}}{\log x}\right).$$

Proof. First, let $u \in \{1, 8\}$ be a fundamental discriminant and $a \in \{\bar{3}, \bar{7} \pmod 8\}$. By the class number formula, $h(-up) = \sqrt{up} \cdot L(1, \chi_{-up})/\pi$ for every $-3 \neq -up < 0$, $p \equiv 3 \mod 4$. Therefore

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{h(-up)} = \frac{\pi}{\sqrt{u}} \sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{-up})} \cdot \frac{1}{\sqrt{p}} + O(1).$$

By partial summation,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{-up})} \cdot \frac{1}{\sqrt{p}} = \sum_{n \le x} S_n \left(\frac{1}{2n^{3/2}} + O\left(\frac{1}{n^{5/2}}\right)\right) + \frac{S_{[x]}}{\sqrt{[x]+1}}$$

where

$$S_n = \sum_{\substack{p \le n \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{-up})} \sim \frac{n}{4 \log n}.$$

by Lemma 5.1. The first two claims follow.

Next, let $u \in \{1, -4, -8\}$ be a fundamental discriminant and let $a \in (\mathbb{Z}/8\mathbb{Z})^\times$ satisfy $(-1)^{\frac{a-1}{2}} u > 0$. By the class number formula, $h(up) = \sqrt{up} L(1, \chi_{up})/2 \log \varepsilon_{up}$ for every $p \equiv a \mod 4$, where ε_{up} is the fundamental unit of $\mathbb{Q}(\sqrt{up})$. As $\varepsilon_{up} \ge \sqrt{up}/2$, we have

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{h(up)} \ge \frac{1}{\sqrt{u}} \sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{up})} \cdot \frac{\log(p/4)}{\sqrt{p}}.$$

By partial summation,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{up})} \cdot \frac{\log(p/4)}{\sqrt{p}} = \sum_{n \le x} S_n \left(\frac{\log n}{2n^{3/2}} + O\left(\frac{1}{n^{3/2}}\right)\right) + S_{[x]} \cdot \frac{\log[x/4]}{\sqrt{[x]+1}}$$

where

$$S_n = \sum_{\substack{p \le n \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{up})} = \frac{n}{4 \log n} + O\left(\frac{n}{\log^2 n}\right)$$

by Lemma 5.1. The result follows. □

5.2. **Proofs of Theorem 1.1 and Theorem 1.4.** We start with Theorem 1.1.

Proof of Theorem 1.1. The forms x^2+dy^2, $1 \le d \le \Delta$ cover the same primes as those with $1 \le d \le \Delta$ squarefree, so it suffices to consider this second set. We first establish the lower bound for the proportion $\delta^+(\Delta)$. Denote by $\mathcal{D}$ the set of all fundamental discriminants

$$-4, -8, -p, -8p, \text{ where } p \equiv 3 \mod 4$$

is a prime and the discriminants $-p$ and $-8p$ are in $\mathcal{D}$ when $p \le \Delta$ and $2p \le \Delta$, respectively.

We proceed to compute, via inclusion-exclusion, the proportion of primes represented by the forms x^2+dy^2, where d is the squarefree part of some $D \in \mathcal{D}$. As $d \le \Delta$, this gives a lower bound for $\delta^+(\Delta)$. In this process, Theorem 4.5 will provide us with the proportion of primes up to X represented simultaneously by each subset of $\mathcal{D}$, and as there are finitely many such subsets, we obtain a proportion after combining all subsets and letting $X \to \infty$.

For any subset $\{D_1, \dots, D_k\} \subset \mathcal{D}$, consider the map $\Phi = \Phi_{\{D_1,\dots,D_k\}}$ defined by (9). By Proposition 4.6, we have $\ker \Phi = \ker \Phi\,[2]$ where $\ker \Phi\,[2]$ is defined by (10). We set aside the discriminants -4 and -8 and consider

$$\mathcal{D}_0 = \{-p_1, \dots, -p_a, -8q_1, \dots, -8q_b, -r_1, -8r_1, \dots, -r_c, -8r_c\} \subset \mathcal{D} \setminus \{-4, -8\}.$$

By Theorem 4.5, the term corresponding to $\mathcal{D}_0$ in the inclusion-exclusion is

$$\frac{1}{2^{\mathbf{1}(b+c>0)}} \prod_{i=1}^{a} \frac{-1}{2\mathfrak{h}(-p_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(-8q_i)} \prod_{i=1}^{c} \frac{1}{\mathfrak{h}(-r_i)\mathfrak{h}(-8r_i)}, \tag{12}$$

where $\mathfrak{h}(D)$ is defined in (5).

Next, consider the collective contribution of the subsets $\mathcal{D}_0$, $\mathcal{D}_0 \cup \{-4\}$, $\mathcal{D}_0 \cup \{-8\}$, and $\mathcal{D}_0 \cup \{-4, -8\}$ to the inclusion-exclusion. By Theorem 4.5, this is exactly the contribution in (12) multiplied by $1 - \frac{1}{2} - \frac{1}{2} + \frac{1}{2} = \frac{1}{2}$ if $b + c > 0$ and by $1 - \frac{1}{2} - \frac{1}{2} + \frac{1}{4} = \frac{1}{4}$ if $b + c = 0$. In both cases these subsets contribute

$$\frac{1}{4} \prod_{i=1}^{a} \frac{-1}{2\mathfrak{h}(-p_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(-8q_i)} \prod_{i=1}^{c} \frac{1}{\mathfrak{h}(-r_i)\mathfrak{h}(-8r_i)}.$$

Summing over all subsets $\mathcal{D}_0 \subset \mathcal{D} \setminus \{-4, -8\}$, we obtain

$$\delta^+(\Delta) \ge 1 - \frac{1}{4} \prod_{\substack{p \le \Delta \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{2\mathfrak{h}(-p)} - \mathbf{1}_{2p \le \Delta} \left(\frac{1}{\mathfrak{h}(-8p)} - \frac{1}{\mathfrak{h}(-p)\mathfrak{h}(-8p)}\right)\right). \tag{13}$$

We now establish the upper bound. Consider

$$\mathcal{D}^- = \mathcal{D} \setminus \{-p, -8p : p \equiv 3 \mod 4,\ p \le \sqrt{\Delta}\}.$$

and

$$\mathcal{Q} = \{p^* : p \le \sqrt{\Delta},\ p \text{ odd prime}\}.$$

We will compute the proportion of primes q that are *not* represented by any x^2+dy^2 with d the squarefree part of some $D \in \mathcal{D}^-$ and for which $\chi_Q(q) = -1$ for all discriminants $Q \in \mathcal{Q}$. Such q cannot be represented by a form x^2+dy^2 with $d \le \Delta$, providing an upper bound for $\delta^+(\Delta)$.

To see this, let D be the fundamental discriminant with squarefree part d. Consider the factorization into prime discriminants

$$D = u \prod_{\substack{p \mid D \\ p \text{ odd}}} p^*$$

where $u \in \{1, -4, 8, -8\}$. In order for q to be represented by $x^2 + dy^2$, it must satisfy the character conditions described in Lemma 2.1. In particular, by (7), it must satisfy the genus conditions from the narrow class group $\mathrm{Cl}^{+\vee}(D)$. This means that

$$\chi_u(q) = 1 \text{ and } \chi_{p^*}(q) = 1 \text{ for odd } p \mid D.$$

Therefore $u \in \{1, 8\}$ (as $-4, -8 \in \mathcal{D}^-$) and every $p \mid D$ odd is greater than $\sqrt{\Delta}$. If $u = 1$, then $D \leq \Delta$ is a squarefree integer with prime factors greater than $\sqrt{\Delta}$, so that $D = -p$, $p \equiv 3 \mod 4$, $p > \sqrt{\Delta}$. If $u = 8$, then $D/8 \leq \Delta/2$ is a squarefree integer with prime factors greater than $\sqrt{\Delta}$, so that $D = -8p$, $p \equiv 3 \mod 4$, $p > \sqrt{\Delta}$. In both cases $D \in \mathcal{D}^-$, and by assumption q cannot be represented by $x^2 + dy^2$.

The proportion of primes q satisfying the conditions above is computed as in the lower bound (13), via inclusion-exclusion on the subsets of $\mathcal{D}^-$ using the proportions provided by Theorem 4.5. The coprimality between elements of $\mathcal{D}^-$ and $\mathcal{Q}$ ensures that the conditions coming from characters χ_Q, $Q \in \mathcal{Q}$, only affect the proportion by a factor of $1/2^{|\mathcal{Q}|}$.

As $\mathcal{D}^- \subset \mathcal{D}$, Proposition 4.6 still ensures that $\ker \Phi = \ker \Phi\,[2]$ for any map Φ defined by (9) on a subset of $\mathcal{D}^-$. As before, consider the subset

$$\mathcal{D}_0^- = \{-p_1, \dots, -p_a, -8q_1, \dots, -8q_b, -r_1, -8r_1, \dots, -r_c, -8r_c\} \subset \mathcal{D}^-.$$

The previous argument shows that the collective contribution of $\mathcal{D}_0$, $\mathcal{D}_0 \cup \{-4\}$, $\mathcal{D}_0 \cup \{-8\}$, and $\mathcal{D}_0 \cup \{-4, -8\}$ in the process of inclusion-exclusion is

$$\frac{1}{2^{|\mathcal{Q}|}} \cdot \frac{1}{4} \prod_{i=1}^{a} \frac{-1}{2\mathfrak{h}(-p_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(-8q_i)} \prod_{i=1}^{c} \frac{1}{\mathfrak{h}(-r_i)\mathfrak{h}(-8r_i)}.$$

Summing over all subsets $\mathcal{D}_0^- \subset \mathcal{D}^-$ not containing -4 or -8, we obtain

$$\delta^+(\Delta) \leq 1 - \frac{1}{2^{|\mathcal{Q}|}} \cdot \frac{1}{4} \prod_{\substack{\sqrt{\Delta} < p \leq \Delta \\ p \equiv 3 \mod 4}} \left(1 - \frac{1}{2\mathfrak{h}(-p)} - \mathbf{1}_{p \leq \Delta/2} \left(\frac{1}{\mathfrak{h}(-8p)} - \frac{1}{\mathfrak{h}(-p)\mathfrak{h}(-8p)}\right)\right). \quad (14)$$

Now notice that

$$1 - \frac{1}{2\mathfrak{h}(-p)} - \mathbf{1}_{p \leq \Delta/2} \left(\frac{1}{\mathfrak{h}(-8p)} - \frac{1}{\mathfrak{h}(-p)\mathfrak{h}(-8p)}\right) = \exp\left(-\frac{1}{2\mathfrak{h}(-p)} - \frac{\mathbf{1}_{p \leq \Delta/2}}{\mathfrak{h}(-8p)} + O\left(\frac{1}{\mathfrak{h}(-p)^2} + \frac{1}{\mathfrak{h}(-8p)^2}\right)\right) \quad (15)$$

since $\mathfrak{h}(D)$ grows as $D \to -\infty$. Recall from the definitions (4) and (5) that $\mathfrak{h}(-p) = h(-p)$ if $p \equiv 7 \mod 8$ and $\mathfrak{h}(-8p) = h(-8p)$ for all p. For $p \equiv 3 \mod 8$, $p \neq 3$, we have

$\mathfrak{h}(-p) = 3h(-p)$ by Lemma 2.2. It follows by Corollary 5.2 that

$$\sum_{\substack{p\le\Delta\\ p\equiv 3 \bmod 4}} \frac{1}{2\mathfrak{h}(-p)} = \frac{1}{2}\sum_{\substack{p\le\Delta\\ p\equiv 7 \bmod 8}} \frac{1}{h(-p)} + \frac{1}{6}\sum_{\substack{p\le\Delta\\ p\equiv 3 \bmod 8}} \frac{1}{h(-p)} + O(1) \sim \frac{\pi}{3}\cdot\frac{\sqrt{\Delta}}{\log\Delta}$$

and

$$\sum_{\substack{p\le\Delta/2\\ p\equiv 3 \bmod 4}} \frac{1}{\mathfrak{h}(-8p)} = \sum_{\substack{p\le\Delta/2\\ p\equiv 3 \bmod 4}} \frac{1}{h(-8p)} \sim \frac{\pi}{4}\cdot\frac{\sqrt{\Delta}}{\log\Delta}.$$

The same estimates show that

$$\sum_{\substack{p\le\sqrt{\Delta}\\ p\equiv 3 \bmod 4}} \frac{1}{\mathfrak{h}(-p)} + \frac{1}{\mathfrak{h}(-8p)} \ll \frac{\Delta^{\frac{1}{4}}}{\log\Delta}.$$

We conclude that

$$\sum_{\substack{\Delta_0<p\le\Delta\\ p\equiv 3 \bmod 4}} \frac{1}{2\mathfrak{h}(-p)} + \frac{\mathbf{1}_{p\le\Delta/2}}{\mathfrak{h}(-8p)} \sim \frac{7\pi}{12}\cdot\frac{\sqrt{\Delta}}{\log\Delta} \tag{16}$$

for any $\Delta_0 \le \sqrt{\Delta}$.

At last, we use Tatuzawa's result (see Theorem 22.8, [10]) and the class number formula to deduce that $h(D) \gg D^{5/12}$ effectively for all D with at most one exception, say D_0, for which we have $h(D_0) \ge 1$. Therefore the sum of error terms in (15) is bounded by

$$\sideset{}{^\flat}\sum_{-8\Delta\le D<0} \frac{1}{\mathfrak{h}(D)^2} \ll \Delta^{1/6} \tag{17}$$

where $\sum^\flat$ indicates a sum over fundamental discriminants.

Combining (13), (14), (15), (16), and (17), and using the prime number theorem to say that $|\mathcal{Q}| \sim 2\frac{\sqrt{\Delta}}{\log\Delta}$, we conclude

$$\exp\left(-\left(\tfrac{7}{12}\pi + \log 4 + o(1)\right)\frac{\sqrt{\Delta}}{\log\Delta}\right) \le 1-\delta^+(\Delta) \le \exp\left(-\left(\tfrac{7}{12}\pi + o(1)\right)\frac{\sqrt{\Delta}}{\log\Delta}\right).$$

The theorem follows. □

We now prove Theorem 1.4 following the ideas from Theorem 1.1.

Proof of Theorem 1.4. Notice that the forms $x^2 - dy^2$ with $d \le \Delta$, $\sqrt{d} \notin \mathbb{Z}$ cover the same primes as those with $2 \le d \le \Delta$ squarefree, so we only consider the latter set. Let $\mathcal{D}$ be the set of all fundamental discriminants

$$8, p, 4q, 8q, \text{ where } p \equiv 1 \bmod 4 \text{ and } q \equiv 3 \bmod 4$$

are primes and the discriminants p, $4q$ and $8q$ are in $\mathcal{D}$ when $p \le \Delta$, $q \le \Delta$ and $2q \le \Delta$, respectively. We will compute, via inclusion-exclusion, the proportion of primes represented by the forms $x^2 - dy^2$, where d is the squarefree part of some $D \in \mathcal{D}$. Since all such d are bounded by Δ, this yields a lower bound for $\delta^-(\Delta)$.

We accomplish this using Theorem 4.5 to determine the proportion of primes represented simultaneously by forms attached to each subset $\mathcal{D}_0 = \{D_1, \dots, D_k\} \subset \mathcal{D}$. For each such $\mathcal{D}_0$, the map $\Phi = \Phi_{\mathcal{D}_0}$ defined by (9) satisfies $\ker \Phi = \ker \Phi\,[2]$, where $\ker \Phi\,[2]$ is defined by (10). To see this, notice that for D equals 8 or $p \in \mathcal{D}$ the group $\mathrm{Cl}^+(D)$ has odd order by genus theory. For D equals $4q, 8q \in \mathcal{D}$ we have $\mathrm{Cl}^+(D)[2] \cong \mathbb{Z}/2\mathbb{Z}$, and by criterion (iv) in Lemma 4.2, [16] the group $\mathrm{Cl}^+(D)$ has no element of order 4. Therefore $\mathrm{Cl}^+(D)[2^\infty] = \mathrm{Cl}^+(D)[2]$ for any $D \in \mathcal{D}$, and it follows from Corollary 4.2 that $\ker \Phi = \ker \Phi\,[2]$.

We now look at the contributions of

$$\mathcal{D}_0 = \{p_1, \dots, p_z, 4q_1, \dots, 4q_a, 8r_1, \dots, 8r_b, 4s_1, 8s_1, \dots, 4s_c, 8s_c\} \subset \mathcal{D}$$

and $\mathcal{D}_0 \cup \{8\}$ in the process of inclusion-exclusion. Assume first that either $ab \geq 1$ or $c \geq 1$. Then by Theorem 4.5 the contribution of $\mathcal{D}_0$ is

$$\frac{1}{4} \prod_{i=1}^{z} \frac{-1}{2\mathfrak{h}(p_i)} \prod_{i=1}^{a} \frac{-1}{\mathfrak{h}(4q_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(8r_i)} \prod_{i=1}^{c} \frac{2}{\mathfrak{h}(4s_i)\mathfrak{h}(8s_i)}$$

and the contribution of $\mathcal{D}_0 \cup \{8\}$ is the value above multiplied by -1, so together they do not contribute. Assume next that $ab = 0$, $c = 0$, and $a + b \geq 1$. The contribution of $\mathcal{D}_0$ is

$$\frac{1}{2} \prod_{i=1}^{z} \frac{-1}{2\mathfrak{h}(p_i)} \prod_{i=1}^{a} \frac{-1}{\mathfrak{h}(4q_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(8r_i)}$$

and the contribution of $\mathcal{D}_0 \cup \{8\}$ is the value above multiplied by $-\frac{1}{2}$, so together they yield

$$\frac{1}{4} \prod_{i=1}^{z} \frac{-1}{2\mathfrak{h}(p_i)} \prod_{i=1}^{a} \frac{-1}{\mathfrak{h}(4q_i)} \prod_{i=1}^{b} \frac{-1}{\mathfrak{h}(8r_i)}.$$

Lastly, assume that $a = b = c = 0$. The sets $\mathcal{D}_0$ and $\mathcal{D}_0 \cup \{8\}$ contribute $\prod_{i=1}^{z}(-2\mathfrak{h}(p_i))^{-1}$ and $-\frac{1}{2}\prod_{i=1}^{z}(-2\mathfrak{h}(p_i))^{-1}$ respectively, so their total contribution is

$$\frac{1}{2} \prod_{i=1}^{z} \frac{-1}{2\mathfrak{h}(p_i)}.$$

Summing over all subsets $\mathcal{D}_0 \subset \mathcal{D}$ not containing 8, we obtain that

$$\delta^-(\Delta) \geq 1 - \frac{1}{4} \prod_{\substack{p \leq \Delta \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{2\mathfrak{h}(p)}\right) \left(\prod_{\substack{q \leq \Delta \\ q \equiv 3 \bmod 4}} \left(1 - \frac{1}{\mathfrak{h}(4q)}\right) + \prod_{\substack{2q \leq \Delta \\ q \equiv 3 \bmod 4}} \left(1 - \frac{1}{\mathfrak{h}(8q)}\right) \right). \tag{18}$$

We now find an upper bound for $\delta^-(\Delta)$. Consider

$$\mathcal{D}^- = \mathcal{D} \setminus \{p, 4q, 8q : p \equiv 1 \bmod 4,\ q \equiv 3 \bmod 4,\ p, q \leq \sqrt{\Delta}\}$$

and

$$\mathcal{Q} = \{p^* : p \leq \sqrt{\Delta},\ p \text{ odd prime}\}.$$

We compute the proportion of primes r that are not represented by any form $x^2 - dy^2$ where d is the squarefree part of some $D \in \mathcal{D}^-$ and for which $\chi_Q(r) = -1$ for all $Q \in \mathcal{Q}$. A prime r satisfying these conditions cannot be represented by any form $x^2 - dy^2$, $d \leq \Delta$, and that gives an upper bound for $\delta^-(\Delta)$.

To see that such r cannot be represented by any of these forms, let D be a fundamental discriminant with squarefree part $d \leq \Delta$ with factorization into prime discriminants

$$D = u \prod_{\substack{p \mid D \\ p \text{ odd}}} p^*$$

where $u \in \{1, -4, 8, -8\}$. By Lemma 2.1 and (7), the conditions coming from the subgroup $\mathrm{Cl}^+(D)[2]$ of genus characters forces that

$$\chi_u(r) = 1 \text{ and } \chi_{p^*}(r) = 1 \text{ for odd } p \mid D$$

in order for r to be represented by $x^2 - dy^2$. This means that $u \in \{1, -4, -8\}$ (since $8 \in \mathcal{D}^-$) and every odd prime $p \mid D$ is greater than $\sqrt{\Delta}$. If $u = 1$ we must have $D = p$ prime with $p > \sqrt{\Delta}$, $p \equiv 1 \mod 4$. If $u = -4$ then $D = 4q$ with $q > \sqrt{\Delta}$ prime and $q \equiv 3 \mod 4$, and if $u = -8$ then $D = 8q$ with $q > \sqrt{\Delta}$ prime and $q \equiv 3 \mod 4$. This means that $D \in \mathcal{D}^-$ but by assumption r is not represented by $x^2 - dy^2$.

The proportion of primes r satisfying the conditions above is computed by inclusion-exclusion using Theorem 4.5, exactly as in (18). The only difference is that the $|\mathcal{Q}|$ character conditions add a factor of $2^{-|\mathcal{Q}|}$ to the proportion, yielding

$$\delta^-(\Delta) \leq$$
$$1 - \frac{1}{4 \cdot 2^{|\mathcal{Q}|}} \prod_{\substack{\sqrt{\Delta} < p \leq \Delta \\ p \equiv 1 \mod 4}} \left(1 - \frac{1}{2\mathfrak{h}(p)}\right) \left(\prod_{\substack{\sqrt{\Delta} < q \leq \Delta \\ q \equiv 3 \mod 4}} \left(1 - \frac{1}{\mathfrak{h}(4q)}\right) + \prod_{\substack{\sqrt{\Delta} < q \leq \Delta/2 \\ q \equiv 3 \mod 4}} \left(1 - \frac{1}{\mathfrak{h}(8q)}\right) \right). \tag{19}$$

Now, using (3), definitions (4) and (5), and the fact the ring of integers of $\mathbb{Q}(\sqrt{4q})$ and $\mathbb{Q}(\sqrt{8q})$ have no unit of norm -1 when $q \equiv 3 \mod 4$, we deduce that $\mathfrak{h}(4q) = 2h(4q)$ and $\mathfrak{h}(8q) = 2h(8q)$. Similarly, we see that $\mathfrak{h}(p) = h^*(p)$ when $p \equiv 1 \mod 4$ as the ring of integers of $\mathbb{Q}(\sqrt{p})$ has a unit of norm -1. Moreover, we have $|\mathcal{Q}| = O(\sqrt{\Delta}/\log \Delta)$ and notice that the factors over $p, q \leq \sqrt{\Delta}$ in Θ missing from the upper bound (19) contribute at most $\exp(O(\sqrt{\Delta}/\log \Delta))$. We conclude from (18) and (19) that

$$\delta^-(\Delta) = 1 - \Theta \cdot \exp\left(O\left(\tfrac{\sqrt{\Delta}}{\log \Delta}\right)\right).$$

For the last assertion, notice that

$$\sum_{\substack{p \leq \Delta \\ p \equiv 1 \mod 4}} \log\left(1 - \frac{1}{2h^*(p)}\right) \leq -\frac{1}{6} \sum_{\substack{p \leq \Delta \\ p \equiv 1 \mod 4}} \frac{1}{h(p)} \leq -\tfrac{1}{6} \cdot \sqrt{\Delta} + O(\tfrac{\sqrt{\Delta}}{\log \Delta}),$$
$$\sum_{\substack{q \leq \Delta \\ q \equiv 3 \mod 4}} \log\left(1 - \frac{1}{2h(4q)}\right) \leq -\frac{1}{2} \sum_{\substack{q \leq \Delta \\ q \equiv 3 \mod 4}} \frac{1}{h(4q)} \leq -\tfrac{1}{4} \cdot \sqrt{\Delta} + O(\tfrac{\sqrt{\Delta}}{\log \Delta}),$$
$$\sum_{\substack{q \leq \Delta/2 \\ q \equiv 3 \mod 4}} \log\left(1 - \frac{1}{2h(8q)}\right) \leq -\frac{1}{2} \sum_{\substack{q \leq \Delta/2 \\ q \equiv 3 \mod 4}} \frac{1}{h(8q)} \leq -\tfrac{1}{8} \cdot \sqrt{\Delta} + O(\tfrac{\sqrt{\Delta}}{\log \Delta}).$$

by Corollary 5.2. We conclude that

$$\delta^{-}(\Delta) \geq 1 - \exp\left(-\tfrac{7}{24}\sqrt{\Delta} + O\left(\tfrac{\sqrt{\Delta}}{\log \Delta}\right)\right).$$

The theorem follows. □

Appendix

In this section we give proofs to some of the technical results above. We restate them here for convenience.

Lemma 3.4. *Let Q be a fundamental discriminant coprime to $2D_1 \dots D_k$, and let $\chi \in \mathfrak{C}^{\vee}(K)$. Then, the twist*

$$\chi \otimes \chi_Q(\cdot) := \chi(\cdot)\, \chi_Q \circ N_{K/\mathbb{Q}}(\cdot)$$

defines a non-trivial Hecke character of K on ideals coprime to $2Q$.

Proof. Given an integer $m \geq 1$, let $I_K(m)$ be the subset of integral ideals of K coprime to (m) and $P^{+}_{K,\mathbb{Z}}(m)$ its subset of principal ideals (α) with $\alpha \equiv a \mod (m)$, $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$, and $N_{K/\mathbb{Q}}(\alpha) > 0$. Set

$$\mathfrak{C}_{(m)}(K) := I_K(m)/P^{+}_{K,\mathbb{Z}}(m),$$

so that $\mathfrak{C}(K)$, as defined by (8), equals $\mathfrak{C}_{(2)}(K)$.

A standard argument shows that every class of $\mathfrak{C}(K)$ contains infinitely many primes of K, so in particular it contains primes coprime to (Q). This means that the natural map $\mathfrak{C}_{(2Q)}(K) \twoheadrightarrow \mathfrak{C}(K)$ is surjective, and by taking duals we obtain

$$\mathfrak{C}^{\vee}(K) \leq \mathfrak{C}^{\vee}_{(2Q)}(K).$$

The character $\chi_Q \circ N_{K/\mathbb{Q}}$ belongs to $\mathfrak{C}^{\vee}_{(2Q)}(K)$, which shows that $\chi \otimes \chi_Q \in \mathfrak{C}^{\vee}_{(2Q)}(K)$ is a Hecke character. Lastly notice that the norm of the conductor of $\chi_Q \circ N_{K/\mathbb{Q}}$ is a multiple of Q which is not the case for the conductor of χ, hence this twist is non-trivial. The result follows. □

Lemma 4.4. *Let D_0 be a fundamental discriminant. Assume that for every prime p sufficiently large for which*

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1, \text{ we have } \chi_{D_0}(p) = 1.$$

Then D_0 is dependent of $D_1, \dots, D_k$ over $(\mathbb{Q}^{\times})^2$.

Proof. We proceed by contradiction and assume that D_0 is independent of $D_1, \dots, D_k$ over $(\mathbb{Q}^{\times})^2$. This means that $\sqrt{D_0}$ is not in $K = \mathbb{Q}(\sqrt{D_1}, \dots, \mathbb{Q}(\sqrt{D_k})$, so that $K(\sqrt{D_0})$ is a quadratic extension of K which is Galois over $\mathbb{Q}$ (it is the splitting field of $(t^2 - D_0)(t^2 - D_1) \dots (t^2 - D_k)$). Hence there is a an automorphism σ of $K(\sqrt{D_0})$ that fixes K and changes the sign of $\sqrt{D_0}$.

By Chebotarev's density theorem, infinitely many unramified primes p have Frobenius σ. These primes split completely in K but the primes above it are inert in $K(\sqrt{D_0})/K$. For these primes,

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1 \text{ and } \chi_{D_0}(p) = -1,$$

a contradiction. The result follows. □

LEMMA 4.7. *Let $D = de$ be a factorization of D into fundamental discriminants, and assume that $\chi_{d,e}$ is the square of a character in $\mathrm{Cl}^{+\vee}(D)$. Then, there exists integers $x, y, z \in \mathbb{Z}\backslash\{0\}$ satisfying*

$$x^2 - dy^2 - ez^2 = 0$$

for which

$$\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}\big(\sqrt{d}, \sqrt{e}, \sqrt{x + y\sqrt{d}}\big) \text{ is unramified.}$$

Moreover, given any prime $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{D})$ above a rational prime p for which $\chi_{D',D''}(\mathfrak{p}) = 1$ for all genus characters $\chi_{D',D''} \in \mathrm{Cl}^{+\vee}(D)[2]$, and any ψ with $\psi^2 = \chi_{d,e}$, we have

$$\psi(\mathfrak{p}) = \left(\frac{x + y\sqrt{d}}{p}\right).$$

Proof. We know by the work of Rédei [14] that $\chi_{d,e}$ is a square in $\mathrm{Cl}^{+\vee}(D)$ if and only if $D = de$ is a "splitting of the second kind". This means that for every prime q dividing e we have $(\frac{d}{q}) = 1$, and vice-versa, which in turn implies that $x^2 - dy^2 - ez^2 = 0$ has integer solutions. As (x, y, z) ranges over these solutions, the fields

$$F = \mathbb{Q}\big(\sqrt{d}, \sqrt{e}, \sqrt{x + y\sqrt{d}}\big)$$

yield all unramified extensions of $\mathbb{Q}(\sqrt{D})$ which are cyclic of order 4 and contain $\mathbb{Q}(\sqrt{d}, \sqrt{e})$. For further details, see [16].

By class field theory, the character ψ comes from composing the Frobenius map of one of the unramified extensions $F/\mathbb{Q}(\sqrt{D})$ above with a homomorphism $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{D})) \cong \mathbb{Z}/4\mathbb{Z} \to \mathbb{C}^\times$ of order 4. The condition $\chi_{d,e}(\mathfrak{p}) = 1$ ensures that $\mathfrak{p}$ is not inert in the extension $\mathbb{Q}(\sqrt{d}, \sqrt{e})/\mathbb{Q}(\sqrt{D})$, hence the Frobenius $\psi(\mathfrak{p})$ indicates whether or not the primes above $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{d}, \sqrt{e})$ are inert in F. Therefore

$$\psi(\mathfrak{p}) = \left(\frac{x + y\sqrt{d}}{p}\right).$$

At last, notice that the conditions $\chi_{D',D''}(\mathfrak{p}) = 1$ for all genus characters imply that $\psi(\mathfrak{p})$ is constant over all square-roots ψ of $\chi_{d,e}$. The result follows. □

LEMMA 4.8. *Let d, e be coprime integers in $\langle D_1, \ldots, D_k\rangle(\mathbb{Q}^\times)^2 \setminus (\mathbb{Q}^\times)^2$ such that*

$$x^2 - dy^2 - ez^2 = 0$$

for some $x, y, z \in \mathbb{Z} \setminus \{0\}$. Assume that for every prime p sufficiently large for which

$$\chi_{D_1}(p) = 1, \ldots, \chi_{D_k}(p) = 1, \text{ we have } \left(\frac{x + y\sqrt{d}}{p}\right) = 1.$$

Then $\sqrt{x + y\sqrt{d}} \in \mathbb{Q}(\sqrt{d})$.

Proof. Let $\alpha = x + y\sqrt{d}$. We proceed by contradiction and assume that $\sqrt{\alpha}$ is not in $\mathbb{Q}(\sqrt{d})$. Then $\sqrt{\alpha}$ is also not contained in $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_k})$. To see this, consider the field $F = \mathbb{Q}(\sqrt{de})(\sqrt{\alpha})$. By Lemma 5.1 from [16], the extension $F/\mathbb{Q}$ is Galois with dihedral

group of order 8. However, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ has no element of order 4, hence F cannot be a subfield of K. It follows that $\sqrt{\alpha} \notin K$.

Therefore $K(\sqrt{\alpha})$ is a quadratic extension of K, and it is also Galois over $\mathbb{Q}$ as it is the splitting field of $(t^2 - D_1)\dots(t^2 - D_k)(t^4 - 2t^2x + ez^2)$. Hence there is an automorphism σ of $K(\sqrt{\alpha})$ with fixed field K. By Chebotarev's density theorem, infinitely many unramified primes p have Frobenius element equal to σ. These primes split completely in K but the primes above it are inert in $K(\sqrt{\alpha})/K$, which implies that

$$\chi_{D_1}(p) = 1, \dots, \chi_{D_k}(p) = 1 \text{ and } \left(\frac{x + y\sqrt{d}}{p}\right) = -1,$$

a contradiction. The result follows. □

LEMMA 5.1. *Let $a \in (\mathbb{Z}/8\mathbb{Z})^\times$ and $u \in \{1, -4, 8, -8\}$ be a fundamental discriminant. Then*

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{up^*})} = \frac{1}{4} \cdot \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Proof. We first remove characters χ_{up^*} attached to potential Siegel zeros. There are $\ll \log x$ such characters with $p \le x$, for which $L(1, \chi_{up^*})^{-1} \ll \sqrt{p}$ by the class number formula. For the remaining characters, we have by Lemma 2.3 in [7] with $Z = \exp((\log x)^{10})$ that

$$\frac{1}{L(1, \chi_{up^*})} = \sum_{n=1}^{\infty} \chi_{up^*}(n) \frac{\mu(n)}{n} e^{-n/Z} + O\left(\tfrac{1}{p}\right),$$

and notice that the right-hand side is bounded absolutely by $\ll \log Z = (\log x)^{10}$. Therefore,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \frac{1}{L(1, \chi_{up^*})} = \sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \sum_{n=1}^{\infty} \chi_{up^*}(n) \frac{\mu(n)}{n} e^{-n/Z} + O(\sqrt{x} \log x). \tag{20}$$

Set $N = (\log x)^{10}$ and let S_1, S_2, S_3 be the contributions coming from $n = 1$, $2 \le n \le N$, $N < n$ in (20), respectively, so that

$$\sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \sum_{n=1}^{\infty} \chi_{up^*}(n) \frac{\mu(n)}{n} e^{-n/Z} = S_1 + S_2 + S_3. \tag{21}$$

By Dirichlet's theorem,

$$S_1 = \frac{x}{4 \log x} + O\left(\frac{x}{\log^2 x}\right). \tag{22}$$

For the second term, notice that

$$S_2 \le \sum_{\substack{n=2 \\ n \text{ squarefree}}}^{N} \frac{1}{n} \left| \sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \chi_{up^*}(n) \right| \le \sum_{\substack{n=2 \\ n \text{ squarefree}}}^{N} \frac{1}{n} \left| \sum_{\substack{p \le x \\ p \equiv a \bmod 8}} \left(\frac{p}{n}\right) \right|.$$

The condition $p \equiv a \pmod 8$ can be obtained by a linear combination of the characters $(\frac{p}{n})$, $\chi_{-8}(p)(\frac{p}{n})$, and $\chi_8(p)(\frac{p}{n})$, so we have

$$S_2 \ll \sum_{|D|\leq 8N}^{\flat} \frac{1}{|D|} \left| \sum_{p\leq x} \chi_D(p) \right| \tag{23}$$

where $\sum^{\flat}$ indicates a sum over fundamental discriminants.

Tatuzawa's effective bound for $L(1,\chi_D)$ (see Theorem 22.8 in [10]) gives us that

$$L(1,\chi_D) \gg \frac{1}{|D|^{1/20}}.$$

for all $|D| \gg 1$ with at most one possible exception, which we denote by D_0. Hence for all $D \neq D_0$, a potential Siegel zero β of $L(s,\chi_D)$ satisfies

$$\beta < 1 - \frac{c_1}{D^{1/15}}$$

for some constant $c_1 > 0$ (as derived in (12) of §14, [6]). It follows by (8) of §20 [6] that for every $D \neq D_0$ with $|D| \leq 8N = 8(\log x)^{10}$ we have

$$\sum_{n\leq x} \Lambda(n)\chi_D(n) = O\left(\frac{x}{\exp(c_2(\log x)^{1/3})}\right).$$

for some constant $c_2 > 0$. We conclude by partial summation that

$$\sum_{p\leq x} \chi_D(p) = O\left(\frac{x}{\exp(c_2(\log x)^{1/3})}\right) \tag{24}$$

for every $D \neq D_0$, $|D| \leq 8N$.

We now turn to the exceptional discriminant D_0. If $D_0 \leq (\log x)^{3/2}$, we again use (8) of §20 [6] combined with (12) of §14 [6] to conclude as before that

$$\sum_{p\leq x} \chi_{D_0}(p) = O\left(\frac{x}{\exp(c_3(\log x)^{1/5})}\right)$$

for some constant $c_3 > 0$. Otherwise, we bound $\sum_{p\leq x} \chi_{D_0}(p)$ trivially. In either case

$$\frac{1}{|D_0|}\left|\sum_{p\leq x} \chi_{D_0}(p)\right| = O\left(\frac{x}{(\log x)^{5/2}}\right), \tag{25}$$

and combining (23), (24), and (25) we obtain

$$S_2 \ll \frac{x}{(\log x)^{5/2}}. \tag{26}$$

For the last term, write

$$S_3 = \sum_{\substack{p\leq x \\ p\equiv a \bmod 8}} \sum_{n>N}^{\infty} \chi_{up^*}(n)\frac{\mu(n)}{n}e^{-n/Z} \leq \sum_{|D|\leq 8x}^{\flat} \left|\sum_{n>N}^{\infty} \chi_D(n)\frac{\mu(n)}{n}e^{-n/Z}\right|.$$

By Cauchy-Schwarz,

$$\left(\sum_{|D|\leq 8x}^{\flat}\left|\sum_{n>N}^{\infty}\chi_D(n)\frac{\mu(n)}{n}e^{-n/Z}\right|\right)^2 \ll x\sum_{|D|\leq 8x}^{\flat}\left|\sum_{n>N}^{\infty}\chi_D(n)\frac{\mu(n)}{n}e^{-n/Z}\right|^2$$
$$= x\sum_{m,n>N}\frac{\mu(m)\mu(n)}{mn}e^{-(m+n)/Z}\sum_{|D|\leq 8x}^{\flat}\chi_D(mn).$$

The diagonal $m=n$ contributes $\ll x^2\sum_{n>N}1/n^2 \ll x^2/N = x^2/(\log x)^{10}$. The off-diagonal is bounded by

$$x\sum_{\substack{n>N^2\\ n\neq\square}}\frac{d(n)}{n}e^{-2\sqrt{n}/Z}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right| \leq x\sum_{\substack{n=1\\ n\neq\square}}^{\infty}\frac{d(n)}{n}e^{-2\sqrt{n}/Z}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right|.$$

Therefore,

$$S_3 \ll \frac{x}{(\log x)^5} + \sqrt{x}\left(\sum_{\substack{n=1\\ n\neq\square}}^{\infty}\frac{d(n)}{n}e^{-2\sqrt{n}/Z}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right|\right)^{1/2}. \tag{27}$$

The summation on the right side of (27) is almost the same as the one in equation (5.3) of [7] when $z=2$ (the only difference being the weight $e^{-2\sqrt{n}/Z}$). An identical argument to that of [7] works to bound this expression, and we sketch it below.

By choosing $k=[\log\log x]$ and applying Hölder's inequality with exponents $\alpha=2k$, $\beta=2k/(2k-1)$ we get

$$\sum_{\substack{n=1\\ n\neq\square}}^{\infty}\frac{d(n)}{n}e^{\frac{-2\sqrt{n}}{Z}}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right| \leq \left(\sum_{n=1}^{\infty}\frac{d(n)^\beta}{n}e^{\frac{-2\sqrt{n}}{Z}}\right)^{\frac{1}{\beta}}\left(\sum_{\substack{n=1\\ n\neq\square}}^{\infty}\frac{e^{\frac{-2\sqrt{n}}{Z}}}{n}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right|^{2k}\right)^{\frac{1}{2k}}.$$

The first factor on the right-hand side is $\ll \log^3 Z = (\log x)^{30}$. We bound the second factor by breaking it into dyadic blocks $2^j\leq n<2^{j+1}$, $j\geq 0$, and using Lemmas 4.1 and 4.4 from [7] in the ranges $2^j\leq x^{2k/(k+1)}$, $x^{2k/(k+1)}<2^j\leq x^{4k/3}$, and $x^{4k/3}<2^j$. We obtain

$$\left(\sum_{\substack{n=1\\ n\neq\square}}^{\infty}\frac{e^{\frac{-2\sqrt{n}}{Z}}}{n}\left|\sum_{|D|\leq 8x}^{\flat}\chi_D(n)\right|^{2k}\right)^{\frac{1}{2k}} \ll x^{1-\frac{1}{2(k+1)}}(2k\log x)^{2k^4}.$$

Combining these bounds, we get

$$S_3 \ll \frac{x}{(\log x)^5} + \frac{x}{\exp\left(c_4(\log x)^{1/2}\right)}. \tag{28}$$

for some constant $c_4>0$. The result now follows from (20), (21), (22), (26), and (28). □

References

[1] Pierre Barrucand and Harvey Cohn, *One some class-fields related to primes of type x^2+32y^2*, J. Reine Angew. Math. **262/263** (1973), 400–414. MR327713

[2] Valentin Blomer, *Binary quadratic forms with large discriminants and sums of two squareful numbers. II*, J. London Math. Soc. (2) **71** (2005), no. 1, 69–84. MR2108246

[3] David Brink, *Five peculiar theorems on simultaneous representation of primes by quadratic forms*, J. Number Theory **129** (2009), no. 2, 464–468. MR2473893
[4] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62. MR756082
[5] David A. Cox, *Primes of the form x^2+ny^2*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication. MR1028322
[6] Harold Davenport, *Multiplicative number theory*, Third, Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by Hugh L. Montgomery. MR1790423
[7] A. Granville and K. Soundararajan, *The distribution of values of $L(1,\chi_d)$*, Geom. Funct. Anal. **13** (2003), no. 5, 992–1028. MR2024414
[8] Ben Green and Kannan Soundararajan, *Covering integers by x^2+dy^2*, J. Inst. Math. Jussieu **24** (2025), no. 3, 847–889. MR4891407
[9] Hiroto Horiba, Masanari Kida, and Genki Koda, *Galois theoretic study on simultaneous representation of primes by binary quadratic forms*, J. Number Theory **213** (2020), 370–387. MR4091946
[10] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214
[11] Irving Kaplansky, *The forms $x+32y^2$ and $x+64y^2$*, Proc. Amer. Math. Soc. **131** (2003), no. 7, 2299–2300. MR1963780
[12] The LMFDB Collaboration, *The L-functions and modular forms database*, 2025. [Online; accessed 1 August 2025].
[13] Eric Mortenson, *Threefield identities and simultaneous representations of primes by binary quadratic forms*, J. Number Theory **133** (2013), no. 11, 3902–3920. MR3084305
[14] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171** (1934), 55–60. MR1581419
[15] Peter Stevenhagen, *On a problem of Eisenstein*, Acta Arith. **74** (1996), no. 3, 259–268. MR1373712
[16] ———, *Redei reciprocity, governing fields and negative Pell*, Math. Proc. Cambridge Philos. Soc. **172** (2022), no. 3, 627–654. MR4416572

Email address: joaoccv@stanford.edu

Department of Mathematics, Stanford University, Stanford, CA 94305.