MATHEMATICS OF COMPUTATION
Volume 76, Number 259, July 2007, Pages 1589–1617
S 0025-5718(07)01976-X
Article electronically published on February 19, 2007

QUADRATIC FORMS THAT REPRESENT ALMOST THE SAME PRIMES

JOHN VOIGHT

Abstract. Jagy and Kaplansky exhibited a table of 68 pairs of positive definite binary quadratic forms that represent the same odd primes and conjectured that their list is complete outside of "trivial" pairs. In this article, we confirm their conjecture, and in fact find all pairs of such forms that represent the same primes outside of a finite set.

1. Introduction

The forms $x^2 + 9y^2$ and $x^2 + 12y^2$ represent the same set of prime numbers, namely, those primes p which can be written $p = 12n + 1$ for some positive integer n. What other like pairs of forms exist? Jagy and Kaplansky [JK] performed a computer search for pairs that represent the same set of odd primes and found certain "trivial" pairs which occur infinitely often and listed other sporadic examples. They conjecture that their list is complete.

Using the tools of class field theory, in this article we give a provably complete list of such pairs. By a *form* Q we mean an integral positive definite binary quadratic form $Q = ax^2+bxy+cy^2 \in \mathbb{Z}[x, y]$; the *discriminant* of Q is $b^2-4ac = D = df^2 < 0$, where d is the discriminant of $\mathbb{Q}(\sqrt{D})$ or the *fundamental discriminant*, and $f \geq 1$. We will often abbreviate $Q = \langle a, b, c\rangle$.

Throughout, we look for forms that represent the same primes outside of a finite set—we then say that they represent *almost the same primes*. A form represents the same primes as any equivalent form under the action of the group $GL_2(\mathbb{Z})$. Hence from now on (except in the statement of Proposition 2.4, see Remark 2.5, and in the proof of Lemma 7.2), we insist that a form be $GL_2(\mathbb{Z})$-*reduced*, i.e., $0 \leq b \leq a \leq c$. Moreover, the set of primes represented by a form is finite (up to a finite set, it is empty) if and only if the form is nonprimitive, that is to say $\gcd(a, b, c) > 1$, and any two nonprimitive forms represent almost the same primes. We therefore also insist that a form be *primitive*, so that the set of primes represented is infinite.

If Q_1, Q_2 are forms which represent almost the same primes, we write $Q_1 \sim Q_2$; it is clear that $\sim$ defines an equivalence relation on the set of forms. To every equivalence class C of forms, we associate the set $\delta(C)$ of fundamental discriminants d of the forms in C as well as the set $\Delta(C)$ of discriminants D of forms in C.

Received by the editor September 16, 2005 and, in revised form, July 25, 2006.
2000 *Mathematics Subject Classification.* Primary 11E12; Secondary 11E16, 11R11.
Key words and phrases. Binary quadratic forms, number theory.
The author's research was partially supported by an NSF Graduate Fellowship. The author would like to thank Hendrik Lenstra, Peter Stevenhagen, and the reviewer for their helpful comments, as well as William Stein and the MECCAH cluster for computer time.

The main result of this article is the following (Theorem 6.2).

Theorem. *There are exactly* 67 *equivalence classes* C *of forms with* $\#\delta(C) \geq 2$. *There are exactly* 6 *classes with* $\#\delta(C) = 3$ *and there is no class with* $\#\delta(C) \geq 4$.

Corollary. *There are exactly* 111 *pairs of forms* Q_1, Q_2 *with fundamental discriminants* $d_1 \neq d_2$ *such that* $Q_1 \sim Q_2$.

The forms are listed in Tables 1–5 at the end of this article.

As a complement to this theorem, we characterize forms $Q_1 \sim Q_2$ with the same fundamental discriminant $d_1 = d_2$ (Theorem 7.4).

Theorem. *Let* $Q_1 = \langle a_1, b_1, c_1 \rangle$ *be a form with* $|D_1| > 4$. *Then there exists a form* $Q_2 \sim Q_1$ *such that* $|D_2| > |D_1|$ *and* $d_1 = d_2 = d$ *if and only if one of the following holds:*

(i) $d \equiv 1 \pmod 8$ *and* $2 \nmid D_1$;
(ii) $2 \mid D_1$ *and either* $b_1 = a_1$ *or* $a_1 = c_1$.

These theorems together prove the conjecture of Jagy and Kaplansky in the affirmative regarding pairs that represent the same odd primes. (See also Remark 6.4 at the end of this article.)

We now give an outline of the proof. To a form Q, we associate an ideal class in an imaginary quadratic order and, by the Artin map, to this ideal class we associate an element of a ring class group (Proposition 2.4). The representability of a prime p by the form Q then amounts to a certain splitting condition on p in the ring class field associated to Q. Therefore, two forms Q_1, Q_2 represent almost the same primes if and only if they give rise to the same splitting data, which can be formally thought of as an open and closed subset $S \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (Lemma 3.6). By Galois theory, such a set has a (unique) minimal field of definition L (Proposition 3.5).

We first treat the case when the forms Q_1, Q_2 have different fundamental discriminants $d_1 \neq d_2$. Group theoretic considerations show that Q_1, Q_2 have the same genus class field, contained in the field L, and that their ring class groups are *of type dividing* $(2, \ldots, 2, 4)$, i.e., they can be embedded in $(\mathbb{Z}/2\mathbb{Z})^r \oplus \mathbb{Z}/4\mathbb{Z}$ for some $r \in \mathbb{Z}_{\geq 0}$ (Proposition 4.5). We then extend existing methods for bounding class groups of imaginary quadratic fields and, using a computer, effectively determine all possible ring class extensions which may arise from the forms $Q_1 \sim Q_2$ (§5). From this finite data we can then list all possible pairs of quadratic forms which represent almost the same primes (§6).

When Q_1, Q_2 have the same fundamental discriminant $d_1 = d_2$, we can by classical methods determine necessary and sufficient conditions for $Q_1 \sim Q_2$ (§7).

As a side result which may be of independent interest, we provide the following classification of class groups of quadratic orders (Theorem 8.2).

Proposition. *There are at least* 226 *and at most* 227 *fundamental discriminants* $D = d < 0$ *such that* $\mathrm{Cl}(d)$ *is of type dividing* $(2, \ldots, 2, 4)$, *and there are at least* 199 *and at most* 205 *such discriminants* D *of nonmaximal orders.*

These orders are listed in Tables 7–16 at the end of this article.

2. Ring class fields

In this section, we fix notation and summarize without proof the few results we will need from class field theory and the theory of L-functions (see e.g. [Cox], [La], and [Wa]).

Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field of discriminant $d < 0$ with ring of integers A. For an integer $f \geq 1$, consider the order $A_f = \mathbb{Z} + fA$; the discriminant of A_f is $D = df^2$. There is a bijection between the set $I(A)$ of ideals of A coprime to f and the set $I(A_f)$ of ideals of A_f coprime to f, given by $\mathfrak{a} \mapsto \mathfrak{a} \cap A_f$ and conversely $\mathfrak{a}_f \mapsto \mathfrak{a}_f A$. Let $\mathrm{Cl}_f(d) = \mathrm{Cl}(D) = \mathrm{Pic}(A_f)$ be the class group of the order A_f, namely the group of invertible A_f-ideals modulo principal A_f-ideals. Given an ideal $\mathfrak{a} \subset A$ prime to f, the A_f-module $\mathfrak{a} \cap A_f$ is trivial in $\mathrm{Cl}(D)$ if and only if $\mathfrak{a}$ is principal and generated by an element α with $\alpha \equiv z \pmod{fA}$ for some $z \in \mathbb{Z}$. We write $h_f(d) = h(D) = \#\,\mathrm{Cl}(D)$.

Proposition 2.1 ([Cox, §9])**.** *There is a unique field $R_{(f)} \supset K$ inside $\overline{K}$ that is abelian over K with the following properties:*

(i) *Each prime $\mathfrak{p}$ of K coprime to f is unramified in $R_{(f)}$.*
(ii) *There is an isomorphism*

$$\mathrm{Cl}_f(d) \cong \mathrm{Gal}(R_{(f)}/K),$$
$$[\mathfrak{p} \cap A_f] \mapsto \mathrm{Frob}_{\mathfrak{p}}$$

for each prime $\mathfrak{p}$ of K coprime to f.

The field $R_{(f)}$ is the largest abelian extension of K of conductor dividing (f) in which all but finitely many primes of K inert over $\mathbb{Q}$ split completely.

The exact sequence

$$1 \to \mathrm{Gal}(R_{(f)}/K) \to \mathrm{Gal}(R_{(f)}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1$$

splits, and a choice of splitting gives an isomorphism

$$\mathrm{Gal}(R_{(f)}/\mathbb{Q}) \cong \mathrm{Gal}(R_{(f)}/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$$

where the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(R_{(f)}/K)$ by inversion $\sigma \mapsto \sigma^{-1}$.

The field $R_{(f)}$ is called the *ring class field of K of modulus f*, and the map $\mathrm{Cl}_f(d) \cong \mathrm{Gal}(R_{(f)}/K)$ is known as the *Artin isomorphism*.

Remark 2.2. As $\mathrm{Gal}(R_{(f)}/K)$ is abelian, we see from the proposition that the conjugacy class of an element $\sigma \in \mathrm{Gal}(R_{(f)}/K)$ in $\mathrm{Gal}(R_{(f)}/\mathbb{Q})$ is equal to $\{\sigma, \sigma^{-1}\}$.

Corollary 2.3. *Let $f_1, f_2 \in \mathbb{Z}_{\geq 1}$, and let $f = \gcd(f_1, f_2)$. Then $R_{(f_1)} \cap R_{(f_2)} = R_{(f)}$.*

Proof. The conductor of $R_{(f_1)} \cap R_{(f_2)}$ divides both (f_1) and (f_2); therefore it divides (f) and has all but finitely many primes of K inert over $\mathbb{Q}$ split completely, hence $R_{(f_1)} \cap R_{(f_2)} \subset R_{(f)}$. Note also that $R_{(f)} \subset R_{(f_1)} \cap R_{(f_2)}$ since $f \mid f_1$ and $f \mid f_2$; therefore equality holds. □

Proposition 2.4 ([Cox, Theorem 7.7])**.** *Let $D = df^2 < 0$ be a discriminant. Then there is a bijection between the set of $SL_2(\mathbb{Z})$-reduced forms of discriminant D and the set of ideal classes in $\mathrm{Cl}(D)$ by the identifications*

$$Q = \langle a, b, c \rangle = ax^2 + bxy + cy^2 \longleftrightarrow [\mathfrak{a}] = [(a, (-b + f\sqrt{d})/2)].$$

Let Q be a form, with $Q \leftrightarrow [\mathfrak{a}]$ for $\mathfrak{a}$ an ideal of A and $[\mathfrak{a}]$ associated to $\sigma \in \mathrm{Gal}(R_{(f)}/K)$ under the Artin map. Let $p \nmid f$ be prime. Then p is represented by Q if and only if $[\mathfrak{a}]$ contains an integral ideal of norm p, which holds if and only if we have $\mathrm{Frob}_p = \{\sigma, \sigma^{-1}\} \subset \mathrm{Gal}(R_{(f)}/\mathbb{Q})$.

Remark 2.5. When considering primes represented by a form, we naturally link a Frobenius element together with its inverse; note that exactly one element of any conjugacy class $\{\sigma, \sigma^{-1}\}$ is associated with a $GL_2(\mathbb{Z})$-reduced form.

Remark 2.6. Since $h_f(d) = [R_{(f)} : K]$, it follows from the Chebotarev density theorem that the density of the set of primes represented by Q is equal to $1/(2h_f(d))$ if the corresponding element σ has order ≤ 2 (i.e., $\sigma = \sigma^{-1}$) and $1/h_f(d)$ otherwise.

Lemma 2.7. *The forms Q_1, Q_2 represent almost the same primes ($Q_1 \sim Q_2$) if and only if for almost all primes p of $\mathbb{Q}$, we have*

$$\mathrm{Frob}_p = \{\sigma_1, \sigma_1^{-1}\} \subset \mathrm{Gal}(R_1/\mathbb{Q}) \Longleftrightarrow \mathrm{Frob}_p = \{\sigma_2, \sigma_2^{-1}\} \subset \mathrm{Gal}(R_2/\mathbb{Q}).$$

Remark 2.8. It follows from this that if Q_1, Q_2 are forms with the same discriminant $D_1 = D_2$, then $Q_1 \sim Q_2$ if and only if $Q_1 = Q_2$.

Proposition 2.9. *The field $P_{(f)} \subset R_{(f)}$ given by*

$$\mathrm{Gal}(P_{(f)}/K) \cong \mathrm{Cl}_f(d)/\mathrm{Cl}_f(d)^2$$

is the largest subextension of $R_{(f)} \supset K$ with Galois group $\mathrm{Gal}(R_{(f)}/K)$ of exponent dividing 2. Moreover, the extension $P_{(f)} \supset \mathbb{Q}$ is itself abelian and of exponent 2, and is the largest abelian subextension of $R_{(f)} \supset \mathbb{Q}$.

The field $P_{(f)}$ is called the *genus class field of K of modulus f*.

Proof. This follows immediately from Proposition 2.1, as inversion acts trivially on a group of exponent dividing 2. □

We can compute the genus class field explicitly as follows. For p an odd prime we write $p^* = (-1)^{(p-1)/2}p$.

Corollary 2.10. *Let $p_1, \ldots, p_r$ be the odd primes dividing D and let*

$$K^* = K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*}).$$

Then the genus class field $P_{(f)}$ of K is as follows:

$$P_{(f)} = \begin{cases} K^*(\sqrt{-1}), & \text{if } d \equiv 1 \pmod 4 \text{ and } 4 \parallel f, \\ K^*(\sqrt{-1}, \sqrt{2}), & \text{if } d \equiv 1 \pmod 4 \text{ and } 8 \mid f, \\ K^*(\sqrt{2}), & \text{if } d \equiv 4 \pmod 8 \text{ and } 4 \mid f, \\ K^*(\sqrt{-1}), & \text{if } d \equiv 0 \pmod 8 \text{ and } 2 \mid f, \\ K^*, & \text{otherwise.} \end{cases}$$

Proof. See [Cox, §6A] for the case $f = 1$. The case $f > 1$ is a standard calculation and follows in a similar way. □

Corollary 2.11. *The odd primes p which ramify in $P_{(f)}$ are exactly the odd primes that divide D.*

If G is an abelian group and $n \in \mathbb{Z}_{>0}$, then we define $G[n] = \{g \in G : ng = 0\}$.

Corollary 2.12. *If d has g distinct prime factors, then $\mathrm{Cl}(d)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{g-1}$.*

For a fundamental discriminant $d < 0$, let

$$\chi(n) = \chi_d(n) = \left(\frac{d}{n}\right)$$

denote the Kronecker symbol.

Lemma 2.13 ([Cox, Theorem 7.24]). *The sequence*

$$1 \to A_f^* \to A^* \to (A/fA)^*/(\mathbb{Z}/f\mathbb{Z})^* \to \mathrm{Cl}_f(d) \to \mathrm{Cl}(d) \to 1,$$

is exact, and

$$h(D) = \frac{h(d)f}{[A^* : A_f^*]} \prod_{p|f} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right).$$

In the sequel, we will use lower bounds on the sizes of the class groups of quadratic fields. If we write

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(d/n)}{n^s}$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$, then

$$h(d) = \frac{\sqrt{|d|}}{\pi} L(1,\chi)$$

for $|d| > 4$ (see e.g. [D, §6]). By the Brauer-Siegel theorem, $\log h(d)$ is asymptotic to $\log(\sqrt{|d|})$ as $|d| \to \infty$; by a result of Siegel [S], we know that for every $\epsilon > 0$, there exists a constant $c(\epsilon)$ such that

$$L(1,\chi) > \frac{c(\epsilon)}{|d|^{\epsilon}};$$

however, this constant $c(\epsilon)$ is not known to be effectively computable. Therefore we will use the following result on the size of $L(1,\chi)$.

Lemma 2.14 (Tatuzawa [T]). *For any $0 < \epsilon < 1/2$, there is at most one fundamental discriminant $d < 0$ with $\log|d| > \max(1/\epsilon, 11.2)$ satisfying*

$$L(1,\chi) \le 0.655 \frac{\epsilon}{|d|^{\epsilon}}.$$

3. Fields of definition

We now proceed with a bit of Galois theory. The reader may prefer on a first reading to skip to the next section and refer back when needed.

Let K be a field with separable closure $\overline{K}$ and absolute Galois group $G = \mathrm{Gal}(\overline{K}/K)$, equipped with the Krull topology. Let E be a finite extension of K contained in $\overline{K}$ and let $\mathrm{Hom}_K(E,\overline{K})$ denote the set of K-embeddings $E \hookrightarrow \overline{K}$; if E is Galois over K, then $\mathrm{Hom}_K(E,\overline{K})$ is identified with $\mathrm{Gal}(E/K)$. We have a restriction map

$$\begin{aligned} \mathrm{res}_E : G &\to \mathrm{Hom}_K(E,\overline{K}) \\ \sigma &\mapsto \mathrm{res}_E(\sigma) = \sigma|_E. \end{aligned}$$

The map res_E is continuous if the finite set $\mathrm{Hom}_K(E,\overline{K})$ is equipped with the discrete topology.

Lemma 3.1. *A subset $S \subset G$ is open and closed if and only if there exist a finite extension $L \supset K$ contained in $\overline{K}$ and a set $T \subset \mathrm{Hom}_K(L,\overline{K})$ such that $S = \mathrm{res}_L^{-1}(T)$.*

Proof. Given $T \subset \mathrm{Hom}_K(L, \overline{K})$, note that T is open and closed (in the discrete topology) and res_L is a continuous map.

Conversely, suppose $S \subset G$ is open and closed. Then for every $\sigma \in S$, there exists an open neighborhood $U_\sigma = \mathrm{res}_{E_\sigma}^{-1}(\sigma|_{E_\sigma}) \subset S$ of σ given by some finite extension $E_\sigma \supset K$. Together these give an open cover $\{U_\sigma\}_{\sigma \in S}$ of S. Since G is compact and S is closed, S is itself compact and therefore is covered by $\{U_\sigma\}_{\sigma \in S'}$ for $S' \subset S$ a finite subset. Let L be the compositum of the fields E_σ for $\sigma \in S'$, and let

$$T = \{\tau \in \mathrm{Hom}_K(L, \overline{K}) : \tau|_{E_\sigma} = \sigma|_{E_\sigma} \text{ for some } \sigma \in S'\}.$$

Then by construction $S = \mathrm{res}_L^{-1}(T)$. □

Definition 3.2. Given an open and closed set $S \subset G$, we say that L is a *field of definition for* S if $L \supset K$ is a finite extension and there is a subset $T \subset \mathrm{Hom}_K(L, \overline{K})$ such that $S = \mathrm{res}_L^{-1}(T)$.

Remark 3.3. If L is a field of definition with $S = \mathrm{res}_L^{-1}(T)$ for some subset $T \subset \mathrm{Hom}_K(L, \overline{K})$, then in fact $T = S|_L$. Therefore L is a field of definition for S if and only if $\mathrm{res}_L^{-1}(S|_L) = S$, i.e., for every $\sigma \in G$ and $\tau \in S$ such that $\sigma|_L = \tau|_L$ we have $\sigma \in S$. It follows immediately from this that if L is a field of definition for S and $M \supset L$ is a finite extension, then M is also a field of definition for S.

Put in these terms, Lemma 3.1 states that every open and closed subset $S \subset G$ has a field of definition.

Definition 3.4. A field of definition L for S is *minimal* if for every field of definition E for S, we have $L \subset E$.

If a minimal field of definition L exists, it is obviously unique.

Proposition 3.5. *For any open and closed set $S \subset G$, there exists a minimal field of definition $L(S)$ for S.*

Proof. Consider the set

$$H(S) = \{\sigma \in G : S\sigma = S\} \subset G;$$

we claim that $L(S) = \overline{K}^{H(S)}$.

The set $H(S)$ is clearly a subgroup of G. Let $L \supset K$ be a finite extension with $H = \mathrm{Gal}(\overline{K}/L)$. Then by Remark 3.3, the field L is a field of definition for S if and only if the following statement holds:

$$\text{For all } \sigma \in G \text{ and } \tau \in S, \text{ if } \sigma|_L = \tau|_L, \text{ then } \sigma \in S.$$

Note $\sigma|_L = \tau|_L$ if and only if $\tau^{-1}\sigma \in H$, therefore L is a field of definition if and only if for all $\tau \in S$, we have $\tau H \subset S$, which holds if and only if $SH = S$, i.e., $H \subset H(S)$, or equivalently $L \supset \overline{K}^{H(S)} = L(S)$. Since a field of definition for S exists by Lemma 3.1, we see that $L(S)$ is a finite extension of K. Therefore $L(S)$ is the minimal field of definition for S. □

We now relate this notion to representation of primes. Let K be a number field. Let Π be the set of equivalence classes of sets of primes of K, where two sets are equivalent if they differ only by a finite set. To every open and closed set $S \subset G$ which is closed under conjugation, we can associate a set $\mathcal{P}(S)$ of primes of K: namely, if L is a field of definition for S, we associate the set

$$\mathcal{P}(S) = \{\mathfrak{p} \text{ a prime of } K : \mathfrak{p} \nmid \mathrm{disc}(L/K),\ \mathrm{Frob}_\mathfrak{p} \subset S|_L\},$$

where $\mathrm{Frob}_{\mathfrak{p}}$ is the Frobenius class at the prime $\mathfrak{p}$. If M is another field of definition for S, then the two sets given by L and M differ by only a finite set, contained in the set of primes that ramify in L or in M, and hence we have a well-defined element $\mathcal{P}(S) \in \Pi$.

Lemma 3.6. *The above association $S \mapsto \mathcal{P}(S)$ is injective. The minimal field of definition for S is Galois over K.*

Proof. Suppose that $S \neq S'$. By Remark 3.3, the compositum of a field of definition for S and for S' is a field of definition for both. Therefore there exists a common field of definition L for S, S' which by the same remark we may take to be Galois over K, hence $S|_L \neq S'|_L$. Suppose then that $\sigma \in S|_L \setminus S'|_L$; by the Chebotarev density theorem [La, p. 169], there exist infinitely many primes $\mathfrak{p}$ of K such that $\mathrm{Frob}_{\mathfrak{p}}$ is equal to the conjugacy class of σ, which is disjoint from $S'|_L$ since S' is closed under conjugation. Therefore $\mathcal{P}(S) \neq \mathcal{P}(S')$.

For the second statement, let S be a set with minimal field of definition L and let $\alpha \in G$. Then the set $\alpha S \alpha^{-1}$ has minimal field of definition αL: we have $\alpha\sigma\alpha^{-1}|_{\alpha L} = \alpha\tau\alpha^{-1}|_{\alpha L}$ if and only if $\sigma|_L = \tau|_L$. Therefore if S is closed under conjugation, then $\alpha L = L$ and the minimal field of definition is Galois over K. □

4. Characterizing equivalence via class groups

In this section, we characterize the class groups which can arise from a pair of quadratic forms which represent almost the same primes. In particular (Proposition 4.5), if the forms have different fundamental discriminants, we show that they must either be of exponent dividing 2 or of type $(2, \ldots, 2, 4)$. This proposition allows us to give necessary and sufficient conditions for the existence of such pairs with different fundamental discriminants (Theorem 4.7) and the same fundamental discriminant (Proposition 4.8).

Throughout the following sections, we will utilize the following notation.

Notation 4.1. Let Q denote a (primitive, $GL_2(\mathbb{Z})$-reduced, integral positive definite binary quadratic) form of discriminant $D = df^2$, where $d < 0$ is the fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$, and let R be the ring class field of K of modulus f with $h(D) = \#\,\mathrm{Cl}(D) = [R : K]$ and genus class field $P \supset K$. By Proposition 2.1, the form Q corresponds to an ideal class $[\mathfrak{a}]$ and to an element $\sigma \in \mathrm{Gal}(R/K)$. We define the set

$$S = \mathrm{res}_R^{-1}(\{\sigma, \sigma^{-1}\}) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Note that $\mathcal{P}(S)$ (as in Lemma 3.6) is the set of primes represented by Q, up to a finite set (contained in the set of primes dividing f).

The set S is open and closed in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and closed under conjugation. Let $L = L(S)$ be the minimal field of definition for S, which exists by Proposition 3.5; since R is a field of definition for S, we have $L \subset R$. (Note here we take the base field in §2 to be $\mathbb{Q}$.)

Lemma 4.2. *We have $[R : L] \leq 2$, and $[R : L] = 2$ if and only if $\sigma|_L$ has order 2 and σ has order 4. Moreover, we have $P \subset L$.*

Proof. Since $S|_R = \{\sigma, \sigma^{-1}\}$, we have

$$2 \geq \#S|_R = [R : L](\#S|_L),$$

so $[R : L] \leq 2$. Moreover, $[R : L] = 2$ if and only if $\#S|_R = 2$ and $\#S|_L = 1$, which holds if and only if $\sigma|_L = \sigma^{-1}|_L$ and $\sigma \neq \sigma^{-1}$, i.e., $\sigma|_L$ has order 2 and σ has order 4.

To prove that $P \subset L$, note that in either case $\mathrm{Gal}(R/L)$ is generated by $\sigma^2 \in \mathrm{Cl}_f(d)^2 = \mathrm{Gal}(R/P)$. □

Now suppose that Q_1 and Q_2 are a pair of forms, following Notation 4.1 with appropriate subscripts. It is immediate from Lemma 2.7 that Q_1 and Q_2 have the same set $\mathcal{P}(S)$ (up to a finite set) and by the injectivity of Lemma 3.6 the same set S, hence the same minimal field of definition L.

Lemma 4.3. *If $Q_1 \sim Q_2$, then we have $K_1K_2 \subset L$, and K_1K_2 is fixed by all elements of S. Moreover, we have equality of genus class fields $P_1 = P_2$.*

Proof. This follows immediately from the fact that $K_i \subset P_i \subset L$ and that P_i is the maximal subextension of $L/\mathbb{Q}$ of exponent dividing 2. □

We denote this common genus class field by $P = P_1 = P_2$.

Corollary 4.4. *If $Q_1 \sim Q_2$, then $\sigma_1|_P = \sigma_2|_P$.*

Proof. Note $\sigma_2|_P = \sigma_2^{-1}|_P$. Since $P \subset L$, by Lemma 2.7 we conclude $\sigma_1|_P = \sigma_2|_P$. □

We now distinguish two cases, depending on whether Q_1, Q_2 have the same fundamental discriminant.

Proposition 4.5. *Suppose $Q_1 \sim Q_2$ and $K_1 \neq K_2$. Then for $i = 1, 2$, the group $\mathrm{Gal}(R_i/K_i)$ is of type dividing $(2, \ldots, 2, 4)$, and the minimal field of definition is equal to the common genus class field, i.e., $L = P$.*

Proof. Let $\alpha \in \mathrm{Gal}(L/\mathbb{Q})$ be any element of order not dividing 2. From Proposition 2.1 we have

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L/K_i) \rtimes \mathrm{Gal}(K_i/\mathbb{Q})$$

where the nontrivial element of $\mathrm{Gal}(K_i/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(L/K_i)$ by inversion. Suppose that $\alpha \in \mathrm{Gal}(L/\mathbb{Q})$ is an element of order > 2. Then in fact $\alpha \in \mathrm{Gal}(L/K_i)$, since every element of $\mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/K_i)$ has order 2. Therefore the centralizer of α in $\mathrm{Gal}(L/\mathbb{Q})$ is the group $\mathrm{Gal}(L/K_i)$. Hence if such an α exists, then K_i is determined by L, so $K_1 = K_2$. So $K_1 \neq K_2$ implies that $\mathrm{Gal}(L/\mathbb{Q})$ is of exponent 2, and then from the exact sequence

$$0 \to \mathrm{Gal}(R_i/L) \to \mathrm{Gal}(R_i/K_i) \to \mathrm{Gal}(L/K_i) \to 0$$

and the fact that $[R_i : L] \leq 2$ we see that $\mathrm{Gal}(R_i/K_i)$ is of type dividing $(2, \ldots, 2, 4)$.

The second statement then follows, since then $L \subset P$. □

Remark 4.6. This proposition answers a question of Jagy and Kaplansky [JK]. Two ideal classes are said to be in the same *genus* if their ratio is a square of an ideal class. Jagy and Kaplansky call a form Q *bi-idoneal* if its genus consists of only Q and its inverse; in their terminology, every "non-trivial" pair of forms (i.e., $d_1 \neq d_2$) representing the same primes they found was bi-idoneal.

Proposition 4.5 shows that this always holds: if Q_1, Q_2 represent the same primes outside a finite set and $d_1 \neq d_2$, then Q_1 and Q_2 are bi-idoneal. This follows from the fact that a finite abelian group G has $\#(G^2) \leq 2$ if and only if G is of type dividing $(2, \ldots, 2, 4)$.

We can now formulate necessary and sufficient conditions for the existence of pairs which represent almost the same primes with different fundamental discriminants.

Theorem 4.7. *Let Q_1, Q_2 be forms, and suppose that $K_1 \neq K_2$. Then $Q_1 \sim Q_2$ if and only if both of the following hold:*

(i) *R_1 and R_2 have the same genus class field P, and*
$$\sigma_1|_P = \sigma_2|_P \in \mathrm{Gal}(P/K_1K_2).$$
(ii) *For $i = 1, 2$, the group $\mathrm{Gal}(R_i/K_i)$ is either of exponent dividing 2, or is of type $(2, \ldots, 2, 4)$ and σ_i has order 4.*

Proof. We have shown these conditions are necessary: condition (i) follows from Lemma 4.3 and Corollary 4.4, and (ii) follows from Proposition 4.5.

Now we show that these conditions are also sufficient. For $i = 1, 2$, let L_i be the minimal field of definition of S_i (as in Notation 4.1, with subscripts). From Lemma 4.2 and (i), we have $P \subset L_i$, and since R_i is a field of definition for S_i we have $L_i \subset R_i$. We will now show that in fact $L_i = P$. From (ii), either $\mathrm{Gal}(R_i/K_i)$ is of exponent dividing 2 and $R_i = L_i = P$ already, or $\mathrm{Gal}(R_i/K_i)$ is of type $(2, \ldots, 2, 4)$ and σ_i has order 4. But then P is a field of definition for S_i, since $\mathrm{res}_R^{-1}(\sigma_i|_P) = \{\sigma_i, \sigma_i^{-1}\}$, hence $L_i \subset P$, so $L_i = P$ in this case as well. Therefore $L_1 = L_2 = L$.

Now let p be a prime which is unramified in R_1R_2. Then $\sigma_1 \in \mathrm{Frob}_p|_L$ if and only if $\sigma_2 \in \mathrm{Frob}_p|_L$, so then $Q_1 \sim Q_2$ by Lemma 2.7. □

To conclude this section, we consider the case when two forms have the same fundamental discriminant.

Proposition 4.8. *Let Q_1, Q_2 be forms with $d_1 = d_2 = d$.*

Suppose that $f_1 \mid f_2$, and let
$$\phi : \mathrm{Cl}(D_2) \to \mathrm{Cl}(D_1)$$
be the natural (restriction) map. Then $Q_1 \sim Q_2$ if and only if $\phi(\sigma_2) = \sigma_1$ and one of the following holds: either ϕ is an isomorphism, or

(†) *The kernel of ϕ has order 2, generated by σ_2^2, and σ_1 has order 2.*

More generally, we have $Q_1 \sim Q_2$ if and only if there exists a form Q of discriminant $D = df^2$ with $Q_1 \sim Q \sim Q_2$, where $f = \gcd(f_1, f_2)$.

Proof. From Proposition 2.1, we conclude that $R_1 \subset R_2$. If $R_1 = R_2$, then ϕ is an isomorphism. Otherwise, by Lemma 4.2, we have $[R_2 : R_1] = 2$ and $Q_1 \sim Q_2$ if and only if $\mathrm{res}_{R_2}^{-1}(\sigma_1) = \{\sigma_2, \sigma_2^{-1}\}$, where σ_2 has order 4 and σ_1 has order 2. Now σ_1 has order 2 if and only if $\sigma_2^2 \in \ker\phi$, and $\ker\phi$ is generated by σ_2^2 if and only if σ_2 has order 4, which is condition (†). This proves the first statement.

To prove the second statement, let $R = R_f$. Then by Corollary 2.3, $R_1 \cap R_2 = R$. Since $L \subset R_1, R_2$ we see that $L \subset R$; therefore by Remark 3.3 the field R is a field of definition for S. Let Q be the form of discriminant df^2 associated to $\sigma_1|_R$. Again

by Lemma 4.2, we see that either $R_1 = R$, in which case $Q_1 \sim Q$, or $[R_1 : R] = 2$, in which case $L = R$ and as above we have $Q_1 \sim Q$. Similarly, let Q' be the form of discriminant df^2 associated to $\sigma_2|_R$. Then $Q_2 \sim Q'$. Since $Q_1 \sim Q_2$, we have $Q \sim Q'$. But Q and Q' have the same discriminant, which implies that $Q = Q'$, by Remark 2.8. □

5. Bounding class groups

Recall as in the introduction, to every equivalence class C of forms, we associate the set $\delta(C)$ of fundamental discriminants of the forms in C as well as the set $\Delta(C)$ of discriminants of forms in C. In this section, we will prove that there are only finitely many equivalence classes C with $\#\delta(C) \geq 2$. More precisely, we will prove the following statement.

Proposition 5.1. *The sets*

$$\mathcal{D}_\delta = \bigcup_{\#\delta(C)\geq 2} \delta(C) \quad \text{and} \quad \mathcal{D}_\Delta = \bigcup_{\#\delta(C)\geq 2} \Delta(C),$$

are finite and effectively computable. Moreover, $\#\mathcal{D}_\delta \leq 226$ *and* $\#\mathcal{D}_\Delta \leq 425$.

First note the following lemma.

Lemma 5.2 ([We, Lemma 5])**.** *Let* $K = \mathbb{Q}(\sqrt{d})$ *have discriminant* $d < 0$*, let* $\mathfrak{a}$ *be an integral ideal of* $K = \mathbb{Q}(\sqrt{d})$ *and let* c *be a positive integer such that* $\mathfrak{a}^c$ *is principal. If* $\mathfrak{a}$ *is not a principal ideal generated by a rational integer and* $\mathfrak{a}$ *is prime to* d*, then* $(N\mathfrak{a})^c > |d|/4$.

To prove this lemma, one shows that if $(\alpha) = \mathfrak{a}^c$, then α is not a rational integer by considering the factorization of $\mathfrak{a}$ in K, and therefore $N(\mathfrak{a}^c) = N(\alpha)^c > |d|/4$.

Corollary 5.3. *If* $\mathrm{Cl}(d)$ *has exponent* c*, then for all primes* p *such that* $p^c \leq d/4$ *we have* $(d/p) \neq 1$.

Proof. Suppose that $(d/p) = 1$; then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in the ring of integers A of $K = \mathbb{Q}(\sqrt{d})$. Since $N\mathfrak{p} = p$ is not a square, we know that $\mathfrak{p}$ is not generated by a rational integer. The lemma then implies that $(N\mathfrak{p})^c = p^c > d/4$. □

Lemma 5.4. *If* $\mathrm{Cl}_f(d)$ *is of type dividing* $(2, \ldots, 2, 4)$ *and* $|d| > 2500$*, then* $f \in \{1, 2, 3, 4, 6, 8, 12\}$.

Proof. Recall the exact sequence of Lemma 2.13:

$$1 \to (A/fA)^*/(\mathbb{Z}/f\mathbb{Z})^* \to \mathrm{Cl}_f(d) \to \mathrm{Cl}(d) \to 1,$$

where we note that $|d| > 4$ implies $A_f^* = A^*$.

Since the map $\mathrm{Cl}_f(d) \to \mathrm{Cl}(d)$ is surjective, we see that $\mathrm{Cl}(d)$ is itself of type dividing $(2, \ldots, 2, 4)$. Let p be an odd prime such that $p \mid f$. From Proposition A.1, we conclude that $p^2 \nmid f$ and $p = 3$ or $p = 5$. When $|d| > 2500$, or equivalently when $|d/4| > 5^4$, we cannot have $5 \mid f$, for this can happen only if $(d_i/5) = 1$, which contradicts Corollary 5.3. If $2 \mid f$, then since $(d/2) = 1$ cannot occur, and $(d/2) = -1$ implies $3 \mid \mathrm{Cl}_f(d)$, we must have $(d/2) = 0$. But then again from the proposition we see that $16 \nmid f$ and $24 \nmid f$. □

Let Q_1, Q_2 be forms with $d_1 \neq d_2$. Let K_0 be the real quadratic field contained in K_1K_2.

Lemma 5.5. *Let $Q_1 \sim Q_2$ and suppose $|d_{\min}| = \min\{|d_1|, |d_2|\} > 2500$. Then*

$$K_0 \in \{\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\}.$$

Moreover, if $p^4 \leq |d_{\min}|/4$ and p is inert in K_0, then p ramifies in K_1 and K_2.

Proof. By Lemma 4.3, the ring class fields R_1 and R_2 have the same genus class field, and by Proposition 4.5, the group $\mathrm{Cl}_{f_i}(d_i)$ is of type dividing $(2, \ldots, 2, 4)$ for $i = 1, 2$. By Corollary 2.11, the same set of odd primes divides the discriminants D_1, D_2. Then by Lemma 5.4, we see that $d_1/d_2 \in 2^{\mathbb{Z}}3^{\mathbb{Z}}$. Therefore the discriminant of K_0 is supported only at the primes 2 and 3, and K_0 is one of the fields listed.

Let p be a prime with $p^4 \leq d_{\min}/4$ which is inert in K_0. We know that $(d_1/p), (d_2/p) \neq 1$, by Corollary 5.3. We cannot have $(d_1/p) = (d_2/p) = -1$, as then $(d_1 d_2/p) = 1$, so p splits in K_0. Therefore say $(d_1/p) = 0$; then p is ramified in K_1 so p is ramified in $K_1K_2 = K_0K_2$, so p is ramified in K_2 as well. □

Remark 5.6. This lemma proves that given a fundamental discriminant d with $|d| > 2500$, one can explicitly determine all possibilities for fundamental discriminants d' of forms Q' with $Q' \sim Q$.

Lemma 5.7. *Let $p_1 = 3$, $p_2 = 5$, ... be the sequence of odd primes in increasing order, and for each $t \in \mathbb{Z}_{\geq 1}$ let*

$$\widehat{d}_t = 4p_1 \ldots p_{t-1}.$$

Let $d < -3$ be a fundamental discriminant with g distinct prime factors, and let $t \in \mathbb{Z}_{\geq 1}$. Then

$$|d| \geq \widehat{d}_t p_t^{g-t}.$$

Proof. First, we prove that $|d| \geq \widehat{d}_g$. If $d \equiv 0 \pmod 4$, then this is clear. If $d \equiv 1 \pmod 4$ and $g = 1$, then by assumption $|d| \geq 7 > 4$. If $g \geq 2$, then $p_g \geq 5$, and therefore

$$|d| \geq p_1 \ldots p_g \geq 4p_1 \ldots p_{g-1}.$$

It then follows that $|d| \geq \widehat{d}_g \geq \widehat{d}_t p_t^{g-t}$ for $g \geq t$. But for $g < t$, we also have

$$|d| \geq \widehat{d}_g = \frac{\widehat{d}_t}{p_{g+1} \cdots p_t} \geq \frac{\widehat{d}_t}{p_t^{t-g}}$$

as claimed. □

By the preceding two lemmas, we can apply the result of Tatuzawa (Lemma 2.14) to obtain the following.

Proposition 5.8. *Let Q_1, Q_2 be forms representing almost the same primes such that $d_1 \neq d_2$. Then we have $\min\{|d_1|, |d_2|\} \leq B = 80604484 = 4 \cdot 67^4$.*

Proof. Apply Lemma 2.14 with $\epsilon = 1/\log B$. Note that $\log B > 11.2$. Since there is at most one possible exceptional discriminant, we may assume without loss of generality that $d = d_1$ is not exceptional, hence

$$h(d) > \left(\frac{0.655}{\pi}\right) \frac{|d|^{1/2 - 1/\log B}}{\log B}.$$

We suppose that $|d| > B$ and derive a contradiction. By Lemma 5.5, every prime $p \leq 67$ which is inert in K_0 must divide d. Let g be the number of distinct prime

factors of d; since $\#\operatorname{Cl}(d)[2] = 2^{g-1}$ (Corollary 2.12) and $\operatorname{Cl}(d)$ is of type dividing $(2,\dots,2,4)$, we see that $h(d) \leq 2^g$.

For $b \in \mathbb{Z}_{>0}$, let

$$d_0(b,q) = \prod_{\substack{2<p\leq b \\ (p/q)=-1}} p.$$

From Lemma 5.5, we have three cases to consider. If $K_0 = \mathbb{Q}(\sqrt{2})$, then p is inert in K_0 if and only if $p \equiv 3, 5 \pmod 8$. Therefore

$$d_0(67,8) = \prod_{\substack{p\leq 67 \\ p\equiv 3,\,5\ (8)}} p = 3\cdot 5\cdot \ldots \cdot 61 \cdot 67 > 2.4\cdot 10^{16},$$

and by Lemma 5.5, we have $d_0(67,8) \mid d$, so $|d| \geq d_0(67,8)$. For $K_0 = \mathbb{Q}(\sqrt{3})$, the prime p is inert in K_0 if and only if $p \equiv 5, 7 \pmod{12}$, so $d_0(67,12) = 5\cdot\ldots\cdot 53\cdot 67$, and $d_0(67,12) \mid d$ so $|d| > 6.3\cdot 10^{13}$. In a similar way, for $K_0 = \mathbb{Q}(\sqrt{6})$, we obtain $d_0(67,24) = 7\cdot 11\cdot\ldots\cdot 61 > 2.8\cdot 10^{13}$.

In any case, we see that $|d| > 2.8\cdot 10^{13}$, and hence

$$2^g \geq h(d) > \left(\frac{0.655}{\pi \log B}\right)(2.8\cdot 10^{13})^{1/2-1/\log B} > 10897$$

so $g \geq 14$.

By Lemma 5.7, we have $|d| \geq \widehat{d}_{14}\cdot 47^{g-14}$, where $\widehat{d}_{14} > 2.6\cdot 10^{17}$. But this implies that

$$\begin{aligned} 2^g \geq h(d) &> \left(\frac{0.655}{\pi \log B}\right)\widehat{d}_{14}^{\,1/2-1/\log B}\left(47^{1/2-1/\log B}\right)^{g-14} \\ &> 226989\cdot 2^{g-14}, \end{aligned}$$

which is a contradiction. □

Proof of Proposition 5.1. First, by an exhaustive list, we find that there are exactly 226 fundamental discriminants d with $|d| \leq B$ such that $\operatorname{Cl}(d)$ is of type dividing $(2,\dots,2,4)$. To speed up this computation, we use Corollary 5.3 to rule out many of these discriminants. This was accomplished in MAGMA. (The code is available from the author by request.) By Proposition 5.8, we have missed at most one possible fundamental discriminant from the set $\mathcal{D}_d$.

Next, we show that there are exactly 199 discriminants $D = df^2$ of nonmaximal orders with $|d| \leq B$ such that $\operatorname{Cl}_f(d)$ is of type dividing $(2,\dots,2,4)$. By Lemma 5.4, we know that $f \in \{2,3,4,6,12\}$. We can use any algorithm which computes class groups (e.g. enumeration) to check these finitely many nonmaximal orders.

Now suppose that Q_1, Q_2 are forms that represent the same primes with $|d_1| < |d_2|$. Then $|d_1| \leq B$, and we must show that $|d_2| \leq B$ as well to have computed $\mathcal{D}_d$ and therefore $\mathcal{D}_D$ as well. If $|d_1| \leq 2500$, then from the list of discriminants we see that $|D_1| \leq 29568$; since $\mathbb{Q}(\sqrt{d_2}) \subset P_1$, we see from Lemma 4.3 that $|d_2| \leq 4\cdot 29568 < B$. Otherwise, by Remark 5.6, there are only 3 possibilities for d_2, and since $|d_1| \leq 10920$, it follows that $|d_2| \leq 12\cdot 10920 \leq B$ as well, completing the proof. □

6. Finding the pairs of quadratic forms

To conclude, we list all forms with $K_1 \neq K_2$. Using Corollary 2.10, we first compute the genus class field for each of the 425 discriminants found in §5. We find 86 pairs of discriminants for which the genus class fields are equal.

We now apply Theorem 4.7. If the class group of both discriminants are both of exponent 2, then for every $\sigma \in \mathrm{Gal}(R/K_1K_2)$, we obtain a pair corresponding to $\sigma_i = \sigma \in \mathrm{Gal}(R/K_i)$. For each i such that $\mathrm{Gal}(R_i/K_i)$ has a factor $\mathbb{Z}/4\mathbb{Z}$, we proceed as follows: for each $\sigma \in \mathrm{Gal}(R_i/K_1K_2) \subset \mathrm{Gal}(R_i/K_i)$ of order 4, we compute the fixed field of $\sigma|_P$ by finding a prime $p \nmid D_i$ represented by the form $Q \leftrightarrow \sigma$, and compute (using Legendre symbols) the largest subfield of P in which p splits completely. Then every pair σ_1, σ_2 with the same fixed subfield (so that $\sigma_1|_P = \sigma_2|_P$) gives rise to a pair of forms.

Example 6.1. The discriminants $D_1 = -1056 = -264 \cdot 2^2$ and $D_2 = -2112 = -132 \cdot 4^2$ give rise to the common genus class field $P = \mathbb{Q}(i, \sqrt{2}, \sqrt{-3}, \sqrt{-11})$, each with class group of type $(2, 2, 4)$. The forms of order 4 of discriminant -1056 are

$$\langle 5, 2, 53\rangle, \langle 15, 12, 20\rangle, \langle 7, 6, 39\rangle, \langle 13, 6, 21\rangle,$$

and those of discriminant -2112 are

$$\langle 17, 8, 32\rangle, \langle 21, 18, 29\rangle, \langle 7, 4, 76\rangle, \langle 19, 4, 28\rangle.$$

The first form $\langle 5, 2, 53\rangle$ represents the prime 5, so we compute the Legendre symbols

$$(-1/5), (2/5), (-3/5), (-11/5),$$

and find the fixed field $\mathbb{Q}(i, \sqrt{6}, \sqrt{-11}) \subset P$. Continuing in this way, we find that only the pair $\langle 7, 6, 39\rangle$ and $\langle 7, 4, 76\rangle$ have a common fixed field, namely the field $\mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{11})$, and this proves that they represent the same primes (those which are congruent to $7, 79, 127, 151, 175 \pmod{264}$).

Carrying out this calculation for each of the 86 pairs, and supplementing this list with any pairs arising from the same fundamental discriminant, we obtain the forms listed in Tables 1–5.

Theorem 6.2. *There are exactly* 67 *equivalence classes of forms C such that $\#\delta(C) \geq 2$. There are exactly* 6 *classes with $\#\delta(C) = 3$, and there is no class with $\#\delta(C) \geq 4$.*

Definition 6.3. The *exceptional set* E of a form Q is the set of primes p such that Q represents p and there exists a form $Q' \sim Q$ such that Q' does not represent p.

Remark 6.4. Jagy and Kaplansky [JK] miss the two pairs

$$\langle 5, 0, 6\rangle, \langle 11, 4, 14\rangle \quad \text{and} \quad \langle 3, 0, 40\rangle, \langle 27, 12, 28\rangle$$

in their "near misses" (those pairs with exceptional set not contained in $\{2\}$). Moreover, the form $\langle 4, 4, 9\rangle$ in their paper should be $\langle 4, 4, 19\rangle$.

7. Forms with the same fundamental discriminant

In this section, we treat the case when the forms have the same fundamental discriminant. We will again use Notation 4.1. Throughout, let Q_1, Q_2 be forms with $d_1 = d_2 = d < 0$.

If $f_1 = f_2$, so that $D_1 = D_2$, then by Remark 2.8 either $Q_1 = Q_2$ or $Q_1 \not\sim Q_2$. So without loss of generality we may assume that $f_1 < f_2$.

We begin with a general lemma about quadratic forms.

Definition 7.1. Let Q be a form of discriminant $D < 0$ and let $r \in \mathbb{Z}_{\geq 1}$. The form Q' is an *r-lift* of Q if the following conditions hold:

(a) Q and Q' have the same fundamental discriminant $d = d'$.
(b) The discriminant of Q' satisfies $D' = r^2 D$.
(c) In the natural (restriction) map

$$\phi : \mathrm{Cl}(D') \to \mathrm{Cl}(D)$$

we have $\phi(\sigma') = \sigma$, where $\sigma \leftrightarrow Q$ and $\sigma' \leftrightarrow Q'$.

Lemma 7.2. *Let $Q = \langle a, b, c\rangle$ be an $SL_2(\mathbb{Z})$-reduced form associated to σ. Then σ has order dividing 2 if and only if $0 = b$ or $b = a$ or $a = c$.*

Suppose that σ has order dividing 2 and $2 \mid D$. Then Q has a 2-lift Q' with $Q' \leftrightarrow \sigma'$ of order 2 if and only if $0 = b$.

Proof. Throughout this proof, we require only that forms be $SL_2(\mathbb{Z})$-reduced rather than $GL_2(\mathbb{Z})$-reduced, but we maintain all other assumptions on our forms, as in the introduction. Recall that Q is $SL_2(\mathbb{Z})$-reduced if and only if $|b| \leq a \leq c$ and $b = 0$ if either $|b| = a$ or $a = c$.

The first statement of the lemma is classical: The opposite of the form Q is the form $SL_2(\mathbb{Z})$-equivalent to $Q' = \langle a, -b, c\rangle$. But this form is already $SL_2(\mathbb{Z})$-reduced, unless $|b| = a$ or $a = c$, and in either of these cases in fact Q' is $SL_2(\mathbb{Z})$-equivalent to Q, so that σ has order dividing 2.

For the second statement, first suppose $0 = b$ and that a is odd. Note that the form $Q' = \langle a, 0, 4c\rangle$ is a 2-lift of Q, since the set of primes which it represents is a subset of those represented by Q. If c is odd, then a 2-lift is $\langle 4a, 0, c\rangle$ if $4a \leq c$ and $\langle c, 0, 4a\rangle$ if $4a > c$. This concludes this case, because if a and c are both even, then Q is not primitive.

Next, suppose that $b = a$. Then since D is even, a is even, so c is odd. Therefore a 2-lift of Q is the form $SL_2(\mathbb{Z})$-equivalent to $Q' = \langle 4a, 2a, c\rangle$, which is either Q' if $4a < c$, or $\langle c, -2a, 4a\rangle$ if $2a < c < 4a$, or $\langle c, 2(c-a), 4a + c\rangle$ if $c < 2a$; we cannot have $4a = c$ or $2a = c$, as then c is even and Q is not primitive. In any case, the 2-lift visibly has order > 2; therefore all 2-lifts have order > 2 since they differ by an element of the kernel which is of order dividing 2, by Proposition A.1.

Finally, suppose $a = c$. Here, we know that b is even so a is odd, and a 2-lift of Q is the form $SL_2(\mathbb{Z})$-equivalent to $Q' = \langle a, 2b, 4a\rangle$, which is Q' if $2b < a$ and $\langle a, 2(b-a), 5a - 2b\rangle$ if $2b > a$; we cannot have $2b = a$, since a is odd. This form has order dividing 2 if and only if $b = a$ which is impossible (a must be even from the previous paragraph), and otherwise this lift has order > 2. □

Proposition 7.3. *Let Q_1, Q_2 be forms with $d_1 = d_2 = d$ and $f_1 < f_2$. Then $Q_1 \sim Q_2$ if and only if Q_2 is the unique 2- or the unique 4-lift of Q_1.*

Proof. First, suppose that $f_1 \mid f_2$ and that A_{f_1} and A_{f_2} have the same number of roots of unity. Note that the set of primes represented by Q_2 is contained in the set of primes represented by Q_1 up to a finite set if and only if Q_2 is an r-lift of Q_1 for some $r \in \mathbb{Z}_{>1}$. Moreover, if there exist two such r-lifts Q_2, Q_2', then these two forms will represent disjoint, infinite nonempty sets of primes. Putting these together, we see that $Q_1 \sim Q_2$ if and only if Q_2 is the unique r-lift of Q_1 for some $r \in \mathbb{Z}_{>1}$.

From Lemma 4.2 we have $[R_2 : R_1] \in \{1, 2\}$. On the other hand, by Lemma 4.3, R_1 and R_2 have the same genus class field, so from Corollary 2.10, if $p \nmid d$ is an odd prime, then $p \mid f_1$ if and only if $p \mid f_2$. From Lemma 2.13 we have

$$(*) \qquad [R_2 : R_1] = \frac{h(D_2)}{h(D_1)} = u\frac{f_2}{f_1} \in \{1, 2\}$$

where

$$u = \begin{cases} \left(1 - \left(\frac{d}{2}\right)\frac{1}{2}\right), & \text{if } 2 \nmid f_1 \text{ and } 2 \mid f_2; \\ 1, & \text{otherwise.} \end{cases}$$

From Proposition 4.8, there exists a form Q of discriminant df^2 with $f = \gcd(f_1, f_2)$ such that $Q_1 \sim Q \sim Q_2$. But since $u \in \frac{1}{2}\mathbb{Z}$ we see from $(*)$ that $f_i/f \in 2^{\mathbb{Z}}$ for $i = 1, 2$, so $f_2/f_1 \in 2^{\mathbb{Z}}$ as well, and hence since $f_1 < f_2$ we have $f = f_1 \mid f_2$ and $Q = Q_1$. Moreover, we have $u = 1/2$ or $u = 1$, and hence either $f_2 = 2f_1$ or $f_2 = 4f_1$, so Q_2 is the unique 2- or 4-lift of Q_1.

To conclude, suppose that the two orders have different numbers of roots of unity. Then $d = -3, -4$ and A_{f_1} is the maximal order and A_{f_2} is not. Repeating the above analysis, we easily verify that either $f_2 = 2f_1$ or $f_2 = 4f_1$; the finitely many cases that can occur are listed in Table 6. □

To conclude, from this proposition it suffices to give necessary and sufficient conditions for the form Q_1 to have a unique 2- or 4-lift. Note that if Q_2 is the unique 4-lift of Q_1, and Q is the unique 2-lift of Q_1, then in fact Q_2 is the unique 2-lift of Q, and $Q_1 \sim Q \sim Q_2$. Therefore it suffices to give criteria equivalent to those occurring in Proposition 4.8.

Theorem 7.4. *Let $Q_1 = \langle a_1, b_1, c_1\rangle$ be a form. Then there exists a form $Q_2 \sim Q_1$ such that $|D_2| > |D_1|$ and $d_2 = d_1 = d$ if and only if one of the following holds:*

(i) $d \equiv 1 \pmod 8$ *and* $2 \nmid D_1$*;*
(ii) $2 \mid D_1$ *and either* $b_1 = a_1$ *or* $a_1 = c_1$*;*
(iii) $d = -3$ *and* $Q_1 \in \{\langle 1, 1, 1\rangle, \langle 1, 0, 3\rangle\}$*;*
(iv) $d = -4$ *and* $Q_1 = \langle 1, 0, 1\rangle$.

Proof. If $d = -3$ or $d = -4$, we refer to Proposition 7.3 (and Table 6) and find cases (iii) and (iv).

More generally, we apply Proposition 4.8. The map ϕ is an isomorphism if and only if $h(D_2) = h(D_1)$. By Proposition A.1, this occurs if and only if $(d/2) = 1$ (and $f_2 = 2f_1$), which is case (i).

For condition (†) from Proposition 4.8, first for any positive integer f, let

$$C(f) = \frac{(A/fA)^*}{(\mathbb{Z}/f\mathbb{Z})^*}.$$

From the functoriality of the exact sequence of Lemma 2.13, we obtain a commutative diagram

$$\begin{array}{ccccc} 1 & \longrightarrow & C(f_2) & \longrightarrow & \mathrm{Cl}_{f_2}(d) \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} \\ 1 & \longrightarrow & C(f_1) & \longrightarrow & \mathrm{Cl}_{f_1}(d) \end{array}$$

Now if (†) holds, then $C(f_2) \to C(f_1)$ is a nonsplit $\mathbb{Z}/2\mathbb{Z}$-extension, so we see from Proposition A.1 that $2 \mid D_1$. Therefore (†) holds if and only if $2 \mid D_1$, σ_1 has order 2 and σ_2 has order 4. The result now follows from Lemma 7.2. □

8. Computing class groups

To give an alternative proof of Proposition 5.1, we may also characterize with at most one possible exception all imaginary quadratic extensions having class group of type dividing $(2, \dots, 2, 4)$. This result is not needed in the sequel, but it also yields an independent result (Theorem 8.2).

It was a classical problem to characterize field discriminants whose class group has exponent dividing 2, comprised of quadratic forms which are said to be "alone in their genus". It has long been known that the Brauer-Siegel theorem implies that there are only finitely many such discriminants [Ch].

Proposition 8.1 (Weinberger [We], Louboutin [Lo])**.** *The number of discriminants $D = df^2 < 0$ such that $\mathrm{Cl}_f(d)$ has exponent dividing 2 is finite. There are at least 65 and at most 66 such fundamental discriminants, and at least 36 and at most 37 such discriminants of nonmaximal orders.*

Under the assumption of a suitable generalized Riemann hypothesis, there are exactly 65 and 36 of these discriminants, respectively.

The list of these discriminants can be found in [BS, Table 5]. Here we have a small variant of this problem, to which we may apply the same techniques.

Theorem 8.2. *There are at least 226 and at most 227 fundamental discriminants $D = d$ such that $\mathrm{Cl}(d)$ is of type dividing $(2, \dots, 2, 4)$, and at least 199 and at most 205 such discriminants D of nonmaximal orders.*

These extensions are listed in Tables 7–16. Our proof of the proposition will again rely on the result of Tatuzawa (Lemma 2.14).

Lemma 8.3. *There are effectively computable constants C_9, C_{10}, and C_{11} satisfying the following condition:*

With at most one exception, for all fundamental discriminants $d < 0$ with g distinct prime factors such that $|d| \geq C_9$ and $\mathrm{Cl}(d)$ is of type dividing $(2, \dots, 2, 4)$, we have $g \in \{10, 11\}$ and $|d| < C_g$.

Proof. Let $d < 0$ be a fundamental discriminant with g distinct prime factors and class group of type dividing $(2, \dots, 2, 4)$. Recall as in the proof of Proposition 5.8 that $h(d) \leq 2^g$.

Let C_9 be the smallest positive integer such that

$$2^9 = 512 \leq \frac{0.655}{\pi e} \frac{\sqrt{C_9}}{\log C_9}$$

(allowable, since $\sqrt{x}/\log x$ is increasing for $x \geq e^2$). A calculation shows that $\log C_9 > 23$. Now apply Lemma 2.14 with $\epsilon = 1/\log C_9$.

Suppose that d is not the exceptional discriminant. Then if $|d| \geq C_9$, we have

$$2^g \geq h(d) > \left(\frac{0.655}{\pi}\right) \frac{|d|^{1/2-1/\log C_9}}{\log C_9}.$$

In particular, this implies that

$$2^g > \frac{0.655}{\pi e} \frac{\sqrt{C_9}}{\log C_9} \geq 2^9$$

and therefore $g > 9$.

By Lemma 5.7, we have $|d| \geq \widehat{d}_9 \cdot 29^{g-9}$ and hence

$$2^g \geq h(d) > \left(\frac{0.655}{\pi}\right) \frac{\widehat{d}_9^{1/2-1/\log C_9}}{\log C_9} \left(29^{1/2-1/\log C_9}\right)^{g-9}.$$

This inequality implies that $g < 12$.

For $t \in \{10, 11\}$, let C_t be the smallest positive integer such that

$$2^t \leq \left(\frac{0.655}{\pi}\right) \frac{C_t^{1/2-1/\log C_9}}{\log C_9}.$$

Then if $|d| \geq C_g$,

$$2^g \geq h(d) > \left(\frac{0.655}{\pi}\right) \frac{d^{1/2-1/\log C_9}}{\log C_9} \geq \left(\frac{0.655}{\pi}\right) \frac{C_g^{1/2-1/\log C_9}}{\log C_9} \geq 2^g,$$

a contradiction. This completes the proof. □

We are now ready to prove the main result of this section.

Proof of Theorem 8.2. We have already computed (in the previous section) that there are exactly 226 such fundamental discriminants with $|d| \leq B$. Therefore the proposition will follow from Lemma 8.3 and Lemma 5.4 when it is shown that there are no fundamental discriminants $d < 0$ with $\mathrm{Cl}(d)$ of type dividing $(2, \ldots, 2, 4)$ satisfying one of the following conditions:

(1) $4 \cdot 67^4 = B \leq |d| < C_9$; or
(2) the integer d has exactly g distinct prime divisors, $g \in \{10, 11\}$ and $C_9 \leq |d| < C_g$.

Note that from the proof of Lemma 8.3, we find $C_9 = 25593057435 \approx 2.5 \cdot 10^{10}$, $C_{10} = 116145031943 \approx 1.1 \cdot 10^{11}$, and $C_{11} = 527083115400 \approx 5.2 \cdot 10^{11}$.

The computations in (1) and (2) can be simplified by appealing to Corollary 5.3: if $p \leq \sqrt[4]{|d|/4}$, then $(d/p) \neq 1$. We then test for each prime p such that $\sqrt[4]{|d|/4} < p \leq \sqrt{|d|/4}$ and $(d/p) = 1$ if $\mathfrak{p}^4$ is principal (working in the group of quadratic forms of discriminant d), where $(p) = \mathfrak{p}\overline{\mathfrak{p}}$. To further rule out discriminants, we may also check, given two such primes p_1, p_2, that $(\mathfrak{p}_1\mathfrak{p}_2)^2$ is principal. For d which satisfy all these conditions, we compute the class group $\mathrm{Cl}(d)$ itself (e.g. using an algorithm of Shanks) and check explicitly if it is of type dividing $(2, \ldots, 2, 4)$. A computer search in MAGMA found no such d. (The code is available from the author by request.) □

We also prove a complementary result which relies on a generalized Riemann hypothesis.

Proposition 8.4. *If the zeta function of the field $K = \mathbb{Q}(\sqrt{d})$ of discriminant $d < 0$ does not have a zero in the interval $[1 - (2/\log|d|), 1)$ and the class group of K is of type dividing $(2, \dots, 2, 4)$, then $|d| < 1.3 \cdot 10^{10}$.*

Proposition 8.5 (Louboutin [Lo])**.** *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field of discriminant d. Suppose that the zeta function of K does not have a zero in the interval $[1 - (2/\log|d|), 1)$. Then*

$$h(d) \geq \frac{\pi}{3e} \frac{\sqrt{|d|}}{\log|d|},$$

where $e = \exp(1)$.

Proof of Proposition 8.4. We follow [Lo, Théorème 2]. Let g be the number of distinct prime factors of the discriminant d. Then $\#\operatorname{Cl}(d)[2] = 2^{g-1}$ so $h(d) \leq 2^g$. From Proposition 8.5, we see that $2^g \geq (\pi/3e)\sqrt{|d|}/\log|d|$. Recall that $|d| \geq \widehat{d}_t = 4p_1 \dots p_{t-1}$ whenever $d \neq -3$. If we set

$$t_0 = \inf \left\{ t \in \mathbb{Z}_{>0} : u \geq t \Rightarrow 2^u < \left(\frac{\pi}{3e}\right) \frac{(\widehat{d}_u)^{1/2}}{\log \widehat{d}_u} \right\},$$

then $|d| < \widehat{d}_{t_0}$ (see [Lo]). We compute easily that in this case $\widehat{d}_{t_0} = 4 \cdot 3 \cdot \ldots \cdot 29 < 1.3 \cdot 10^{10}$. □

Theorem 8.6. *Under the above Riemann hypothesis, there are exactly* 226 *fundamental discriminants d such that $\operatorname{Cl}(d)$ is of type dividing $(2, \dots, 2, 4)$, and* 199 *such discriminants D of nonmaximal orders.*

This follows from Proposition 8.4 and the computations performed in the proof of Theorem 8.2.

Appendix: Ring class groups

In this appendix, we prove a proposition which characterizes ring class groups; we give a full statement for completeness.

Proposition A.1. *For $f \in \mathbb{Z}_{>0}$, we have*

$$\frac{(A/fA)^*}{(\mathbb{Z}/f\mathbb{Z})^*} \cong \prod_{p^e \| f} \frac{(A/p^eA)^*}{(\mathbb{Z}/p^e\mathbb{Z})^*}$$

where p is prime and $e > 0$. We have

$$\frac{(A/2^eA)^*}{(\mathbb{Z}/2^e\mathbb{Z})^*} \cong \begin{cases} 0, & \text{if } d \equiv 1 \pmod 8 \text{ and } e = 1, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z}, & \text{if } d \equiv 1 \pmod 8 \text{ and } e \geq 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } d \equiv 5 \pmod 8 \text{ and } e = 1, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z}, & \text{if } d \equiv 5 \pmod 8 \text{ and } e \geq 2, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-1}\mathbb{Z}, & \text{if } d \equiv 4 \pmod 8, \\ \mathbb{Z}/2^e\mathbb{Z}, & \text{if } d \equiv 0 \pmod 8, \end{cases}$$

and

$$\frac{(A/3^eA)^*}{(\mathbb{Z}/3^e\mathbb{Z})^*} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3^{e-1}\mathbb{Z}, & \text{if } d \equiv 1 \pmod 3, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3^{e-1}\mathbb{Z}, & \text{if } d \equiv 2 \pmod 3, \\ \mathbb{Z}/3^e\mathbb{Z}, & \text{if } d \equiv 3 \pmod 9, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^{e-1}\mathbb{Z}, & \text{if } d \equiv 6 \pmod 9, \end{cases}$$

and finally for $p \neq 2, 3$, we have

$$\frac{(A/p^eA)^*}{(\mathbb{Z}/p^e\mathbb{Z})^*} \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}, & \text{if } (d/p) = 1, \\ \mathbb{Z}/(p+1)\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}, & \text{if } (d/p) = -1, \\ \mathbb{Z}/p^e\mathbb{Z}, & \text{if } (d/p) = 0. \end{cases}$$

Proof. The first statement follows from the Chinese remainder theorem. From Lemma 2.13, we have

$$\#\frac{(A/p^eA)^*}{(\mathbb{Z}/p^e\mathbb{Z})^*} = p^e\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right).$$

We first treat the trivial case $p^e = 2$: then $(\mathbb{Z}/2\mathbb{Z})^*$ is the trivial group, and

$$(A/2A)^* \cong \begin{cases} \mathbb{Z}/3\mathbb{Z}, & \text{if } (d/2) = -1, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } (d/2) = 0, \\ 0, & \text{if } (d/2) = 1. \end{cases}$$

Note that

$$\frac{(A/p^eA)^*}{(\mathbb{Z}/p^e\mathbb{Z})^*} \cong \frac{(A_p/p^eA_p)^*}{(\mathbb{Z}_p/p^e\mathbb{Z}_p)^*},$$

where A_p denotes the completion of A at p and $\mathbb{Z}_p$ the ring of p-adic integers. So if $(d/p) = 1$, by [N, §II.5] we have

$$\frac{(A_p/p^eA_p)^*}{(\mathbb{Z}_p/p^e\mathbb{Z}_p)^*} \cong (\mathbb{Z}_p/p^e\mathbb{Z}_p)^* = \begin{cases} 0, & \text{if } p^e = 2, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z}, & \text{if } p = 2 \text{ and } e \geq 2, \\ \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}, & \text{otherwise.} \end{cases}$$

From now on we assume $p^e \neq 2$ and $(d/p) \neq 1$.

Let K_p denote the completion of K at p, so that A_p is its valuation ring with maximal ideal $\mathfrak{p}$ and uniformizer π. We denote by v the unique valuation on K_p normalized so that $v(p) = 1$. Let

$$V(A_p) = \{x \in A_p : v(x) > 1/(p-1)\}.$$

It follows from [N, Proposition II.5.4] that there exists a (continuous) homomorphism $\log_p : A_p^* \to A_p$, with the property that $\log_p$ restricts to an isomorphism $1 + V(A_p) \xrightarrow{\sim} V(A_p)$.

One has an exact sequence

$$0 \to \frac{1 + V(A_p)}{1 + p^eA_p} \to \left(\frac{A_p}{p^eA_p}\right)^* \to \frac{A_p^*}{1 + V(A_p)} \to 0.$$

We have an analogous exact sequence for $\mathbb{Z}_p$, and since $(1+V(A_p)) \cap \mathbb{Z}_p = 1+V(\mathbb{Z}_p)$, it injects term-by-term into the one for A_p, yielding the following exact sequence:

$$(\diamond) \qquad 0 \to \frac{\dfrac{1 + V(A_p)}{1 + p^eA_p}}{\dfrac{1 + V(\mathbb{Z}_p)}{1 + p^e\mathbb{Z}_p}} \to \frac{\left(\dfrac{A_p}{p^eA_p}\right)^*}{\left(\dfrac{\mathbb{Z}_p}{p^e\mathbb{Z}_p}\right)^*} \xrightarrow{\phi} \frac{\dfrac{A_p^*}{1 + V(A_p)}}{\dfrac{\mathbb{Z}_p^*}{1 + V(\mathbb{Z}_p)}} \to 0.$$

From the above, we see that by the logarithm map,

$$\frac{1 + V(A_p)}{1 + p^eA_p} \cong \frac{V(A_p)}{p^eA_p} \quad \text{and} \quad \frac{1 + V(\mathbb{Z}_p)}{1 + p^e\mathbb{Z}_p} \cong \frac{V(\mathbb{Z}_p)}{p^e\mathbb{Z}_p}.$$

Now let us assume that $p \neq 2, 3$. Then $V(A_p) = \mathfrak{p}$, and $V(\mathbb{Z}_p) = p\mathbb{Z}_p$. We first analyze the group

$$\ker \phi = \frac{V(A_p)/p^e A_p}{V(\mathbb{Z}_p)/p^e \mathbb{Z}_p}$$

from ($\diamond$); we claim it is cyclic. If $(d/p) = -1$, with $\epsilon \in A_p$ such that $A_p = \mathbb{Z}_p + \epsilon\mathbb{Z}_p$ as additive groups, then since $\mathfrak{p} = V(A_p) = p\mathbb{Z}_p + p\epsilon\mathbb{Z}_p$, the element $p\epsilon$ generates the group $\ker \phi$. If $(d/p) = 0$, then $V(A_p) = \pi\mathbb{Z}_p + p\mathbb{Z}_p$, so π is a generator. It follows that

$$\ker \phi \cong \begin{cases} \mathbb{Z}/p^{e-1}\mathbb{Z}, & \text{if } (d/p) = -1, \\ \mathbb{Z}/p^e\mathbb{Z}, & \text{if } (d/p) = 0. \end{cases}$$

Now we analyze the image of ϕ. We have $A_p^*/(1 + V(A_p)) \cong \mu(A_p)$ (see [N, Proposition II.5.3]), and this group can be computed as follows. Since $[K_p : \mathbb{Q}_p] = 2$ and the extension $\mathbb{Q}_p(\zeta_p)$ is a totally ramified extension of $\mathbb{Q}_p$ of degree $p - 1$, we conclude that A_p contains no p-power roots of unity. Therefore

$$\mu(A_p) \cong \begin{cases} \mathbb{Z}/(p^2 - 1)\mathbb{Z}, & \text{if } (d/p) = -1, \\ \mathbb{Z}/(p - 1)\mathbb{Z}, & \text{if } (d/p) = 0. \end{cases}$$

Since $\mu(\mathbb{Z}_p) \cong \mathbb{Z}/(p - 1)\mathbb{Z}$, putting these two pieces together, we see that in the exact sequence ($\diamond$), the kernel and image groups have orders which are relatively prime to each other and hence the exact sequence splits, and we obtain the result of the proposition.

To conclude, we must treat the cases $p = 2$, $p = 3$. Every field extension of $\mathbb{Q}_2$ of degree 2 is isomorphic to $\mathbb{Q}_2(\sqrt{c})$ for $c \in \{-1, \pm 2, \pm 3, \pm 6\}$, and similarly for $\mathbb{Q}_3$ we have $c \in \{-1, -3, 3, \}$. We leave it to the reader to verify the following: For $p = 2$,

$$\frac{(A/2^eA)^*}{(\mathbb{Z}/2^e\mathbb{Z})^*} \cong \begin{cases} \langle (-1 + \sqrt{-3})/2 \rangle \times \langle \sqrt{-3} \rangle \times \langle 1 + 2\sqrt{-3} \rangle, & \text{if } c = -3, \\ \langle \sqrt{-1} \rangle \times \langle 1 + 2\sqrt{-1} \rangle, & \text{if } c = -1, \\ \langle 1 + 2\sqrt{c} \rangle, & \text{if } c = 3, \\ \langle 1 + \sqrt{c} \rangle, & \text{if } 2 \mid c, \end{cases}$$

and for $p = 3$,

$$\frac{(A/3^eA)^*}{(\mathbb{Z}/3^e\mathbb{Z})^*} \cong \begin{cases} \langle 1 + \sqrt{-1} \rangle \times \langle 1 + 3\sqrt{-1} \rangle, & \text{if } c = -1, \\ \langle 1 + \sqrt{3} \rangle, & \text{if } c = 3, \\ \langle (1 + \sqrt{-3})/2 \rangle \times \langle 1 + 3\sqrt{-3} \rangle, & \text{if } c = -3. \end{cases}$$

Computing the orders of these elements yields the conclusion of the proposition. □

Tables

In Tables 1 and 2, we list equivalence classes with two fundamental discriminants ($\delta(C) = 2$), then in Tables 3–5 those with three fundamental discriminants, then in Table 6 the exceptional cases with one fundamental discriminant (see Theorem 7.4(iii)–(iv)). Within each table, the classes are sorted by the smallest fundamental discriminant d in each class. Every form in an equivalence class has associated to it the same genus class field P (Lemma 4.3), denoted $\mathbb{Q}[a_1, \ldots, a_r] = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$. The class group $\mathrm{Cl}_f(d)$ for each form is given by its type. The set E denotes the exceptional set for each equivalence class (6.3).

If $r \in \mathbb{Z}_{\geq 0}$, an abelian group G is said to be *of type* $(\underbrace{2, \ldots, 2}_{r}, 4)$ if

$$G \cong (\mathbb{Z}/2\mathbb{Z})^r \oplus \mathbb{Z}/4\mathbb{Z}.$$

The group G is *of type dividing* $(2, \ldots, 2, 4)$ if there is an injection of groups

$$G \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^r \oplus \mathbb{Z}/4\mathbb{Z}$$

for some $r \in \mathbb{Z}_{\geq 0}$.

In Tables 7–16, we list the orders of imaginary quadratic fields with class group of type dividing $(2, \ldots, 2, 4)$, with at most one possible exception (as in Theorem 8.2). In particular, there is no order with class group of type $(2, 2, 2, 2, 2)$ (unless this is the one exception!). The tables are sorted by the isomorphism class of the class group, and within each table the classes are first sorted by fundamental discriminant and then discriminant.

TABLE 1. Equivalence classes C of forms ($\#\delta(C) = 2$, $\#C = 2$), 1 of 2

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 1, 0, 5\rangle$	20	20	1	$\mathbb{Q}[-1, 5]$	(2)	$\{5\}$
$\langle 1, 0, 25\rangle$	100	4	5		(2)	$\emptyset$
$\langle 1, 0, 8\rangle$	32	8	2	$\mathbb{Q}[-1, 2]$	(2)	$\emptyset$
$\langle 1, 0, 16\rangle$	64	4	4		(2)	$\emptyset$
$\langle 1, 0, 9\rangle$	36	4	3	$\mathbb{Q}[-1, -3]$	(2)	$\emptyset$
$\langle 1, 0, 12\rangle$	48	3	4		(2)	$\emptyset$
$\langle 5, 0, 6\rangle$	120	120	1	$\mathbb{Q}[2, -3, 5]$	$(2, 2)$	$\{5\}$
$\langle 11, 4, 14\rangle$	600	24	5		$(2, 4)$	$\emptyset$
$\langle 5, 0, 8\rangle$	160	40	2	$\mathbb{Q}[-1, 2, 5]$	$(2, 2)$	$\{5\}$
$\langle 13, 8, 32\rangle$	1600	4	20		$(2, 4)$	$\emptyset$
$\langle 1, 0, 45\rangle$	180	20	3	$\mathbb{Q}[-1, -3, 5]$	$(2, 2)$	$\emptyset$
$\langle 1, 0, 60\rangle$	240	15	4		$(2, 2)$	$\emptyset$
$\langle 5, 0, 9\rangle$	180	20	3	$\mathbb{Q}[-1, -3, 5]$	$(2, 2)$	$\{5\}$
$\langle 9, 6, 26\rangle$	900	4	15		$(2, 4)$	$\emptyset$
$\langle 8, 0, 9\rangle$	288	8	6	$\mathbb{Q}[-1, 2, -3]$	$(2, 2)$	$\emptyset$
$\langle 9, 6, 17\rangle$	576	4	12		$(2, 4)$	$\emptyset$
$\langle 1, 0, 120\rangle$	480	120	2	$\mathbb{Q}[-1, 2, -3, 5]$	$(2, 2, 2)$	$\emptyset$
$\langle 1, 0, 240\rangle$	960	15	8		$(2, 2, 2)$	$\emptyset$
$\langle 5, 0, 24\rangle$	480	120	2	$\mathbb{Q}[-1, 2, -3, 5]$	$(2, 2, 2)$	$\{5\}$
$\langle 21, 6, 29\rangle$	2400	24	10		$(2, 2, 4)$	$\emptyset$
$\langle 3, 0, 40\rangle$	480	120	2	$\mathbb{Q}[-1, 2, -3, 5]$	$(2, 2, 2)$	$\{3\}$
$\langle 27, 12, 28\rangle$	2880	20	12		$(2, 2, 4)$	$\emptyset$
$\langle 3, 0, 56\rangle$	672	168	2	$\mathbb{Q}[-1, 2, -3, -7]$	$(2, 2, 2)$	$\{3\}$
$\langle 20, 12, 27\rangle$	2016	56	6		$(2, 2, 4)$	$\emptyset$
$\langle 8, 0, 21\rangle$	672	168	2	$\mathbb{Q}[-1, 2, -3, -7]$	$(2, 2, 2)$	$\emptyset$
$\langle 29, 12, 36\rangle$	4032	7	24		$(2, 2, 4)$	$\emptyset$
$\langle 3, 0, 80\rangle$	960	15	8	$\mathbb{Q}[-1, 2, -3, 5]$	$(2, 2, 2)$	$\{3\}$
$\langle 27, 24, 32\rangle$	2880	20	12		$(2, 2, 4)$	$\emptyset$
$\langle 7, 6, 39\rangle$	1056	264	2	$\mathbb{Q}[-1, 2, -3, -11]$	$(2, 2, 4)$	$\emptyset$
$\langle 7, 4, 76\rangle$	2112	132	4		$(2, 2, 4)$	$\emptyset$
$\langle 15, 12, 20\rangle$	1056	264	2	$\mathbb{Q}[-1, 2, -3, -11]$	$(2, 2, 4)$	$\emptyset$
$\langle 23, 12, 36\rangle$	3168	88	6		$(2, 2, 4)$	$\emptyset$

TABLE 1. (continued)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 13,6,21\rangle$	1056	264	2	$\mathbb{Q}[-1,2,-3,-11]$	$(2,2,4)$	$\emptyset$
$\langle 13,2,61\rangle$	3168	88	6		$(2,2,4)$	$\emptyset$
$\langle 8,0,39\rangle$	1248	312	2	$\mathbb{Q}[-1,2,-3,13]$	$(2,2,2)$	$\emptyset$
$\langle 15,12,44\rangle$	2496	39	8		$(2,2,4)$	$\emptyset$
$\langle 5,4,68\rangle$	1344	84	4	$\mathbb{Q}[-1,2,-3,-7]$	$(2,2,4)$	$\emptyset$
$\langle 5,2,101\rangle$	2016	56	6		$(2,2,4)$	$\emptyset$
$\langle 11,8,32\rangle$	1344	84	4	$\mathbb{Q}[-1,2,-3,-7]$	$(2,2,4)$	$\emptyset$
$\langle 11,4,92\rangle$	4032	7	24		$(2,2,4)$	$\emptyset$
$\langle 20,4,23\rangle$	1824	456	2	$\mathbb{Q}[-1,2,-3,-19]$	$(2,2,4)$	$\emptyset$
$\langle 23,20,44\rangle$	3648	228	4		$(2,2,4)$	$\emptyset$
$\langle 19,4,28\rangle$	2112	132	4	$\mathbb{Q}[-1,2,-3,-11]$	$(2,2,4)$	$\emptyset$
$\langle 19,10,43\rangle$	3168	88	6		$(2,2,4)$	$\emptyset$
$\langle 8,0,105\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 32,24,57\rangle$	6720	420	4		$(2,2,2,4)$	$\emptyset$
$\langle 21,0,40\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 45,30,61\rangle$	10080	280	6		$(2,2,2,4)$	$\emptyset$
$\langle 24,0,55\rangle$	5280	1320	2	$\mathbb{Q}[-1,2,-3,5,-11]$	$(2,2,2,2)$	$\emptyset$
$\langle 39,36,76\rangle$	10560	660	4		$(2,2,2,4)$	$\emptyset$
$\langle 33,0,40\rangle$	5280	1320	2	$\mathbb{Q}[-1,2,-3,5,-11]$	$(2,2,2,2)$	$\emptyset$
$\langle 52,36,57\rangle$	10560	660	4		$(2,2,2,4)$	$\emptyset$
$\langle 23,4,68\rangle$	6240	1560	2	$\mathbb{Q}[-1,2,-3,5,13]$	$(2,2,2,4)$	$\emptyset$
$\langle 23,18,207\rangle$	18720	520	6		$(2,2,2,4)$	$\emptyset$
$\langle 28,12,57\rangle$	6240	1560	2	$\mathbb{Q}[-1,2,-3,5,13]$	$(2,2,2,4)$	$\emptyset$
$\langle 72,48,73\rangle$	18720	520	6		$(2,2,2,4)$	$\emptyset$
$\langle 21,12,76\rangle$	6240	1560	2	$\mathbb{Q}[-1,2,-3,5,13]$	$(2,2,2,4)$	$\emptyset$
$\langle 45,30,109\rangle$	18720	520	6		$(2,2,2,4)$	$\emptyset$
$\langle 35,30,51\rangle$	6240	1560	2	$\mathbb{Q}[-1,2,-3,5,13]$	$(2,2,2,4)$	$\emptyset$
$\langle 36,12,131\rangle$	18720	520	6		$(2,2,2,4)$	$\emptyset$
$\langle 19,14,91\rangle$	6720	420	4	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,4)$	$\emptyset$
$\langle 19,16,136\rangle$	10080	280	6		$(2,2,2,4)$	$\emptyset$
$\langle 28,20,85\rangle$	9120	2280	2	$\mathbb{Q}[-1,2,-3,5,-19]$	$(2,2,2,4)$	$\emptyset$
$\langle 45,30,157\rangle$	27360	760	6		$(2,2,2,4)$	$\emptyset$
$\langle 51,48,56\rangle$	9120	2280	2	$\mathbb{Q}[-1,2,-3,5,-19]$	$(2,2,2,4)$	$\emptyset$
$\langle 59,4,116\rangle$	27360	760	6		$(2,2,2,4)$	$\emptyset$
$\langle 33,24,88\rangle$	11040	2760	2	$\mathbb{Q}[-1,2,-3,5,-23]$	$(2,2,2,4)$	$\emptyset$
$\langle 57,6,97\rangle$	22080	1380	4		$(2,2,2,4)$	$\emptyset$
$\langle 39,6,71\rangle$	11040	2760	2	$\mathbb{Q}[-1,2,-3,5,-23]$	$(2,2,2,4)$	$\emptyset$
$\langle 71,70,95\rangle$	22080	1380	4		$(2,2,2,4)$	$\emptyset$
$\langle 76,20,145\rangle$	43680	10920	2	$\mathbb{Q}[-1,2,-3,5,-7,13]$	$(2,2,2,2,4)$	$\emptyset$
$\langle 96,72,241\rangle$	87360	5460	4		$(2,2,2,2,4)$	$\emptyset$
$\langle 88,32,127\rangle$	43680	10920	2	$\mathbb{Q}[-1,2,-3,5,-7,13]$	$(2,2,2,2,4)$	$\emptyset$
$\langle 127,4,172\rangle$	87360	5460	4		$(2,2,2,2,4)$	$\emptyset$
$\langle 57,18,193\rangle$	43680	10920	2	$\mathbb{Q}[-1,2,-3,5,-7,13]$	$(2,2,2,2,4)$	$\emptyset$
$\langle 148,132,177\rangle$	87360	5460	4		$(2,2,2,2,4)$	$\emptyset$
$\langle 55,10,199\rangle$	43680	10920	2	$\mathbb{Q}[-1,2,-3,5,-7,13]$	$(2,2,2,2,4)$	$\emptyset$
$\langle 159,120,160\rangle$	87360	5460	4		$(2,2,2,2,4)$	$\emptyset$

TABLE 2. Equivalence classes C of forms ($\#\delta(C) = 2$, $\#C = 3$), 1 of 2

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 1,1,4\rangle$	15	15	1	$\mathbb{Q}[-3,5]$	(2)	$\emptyset$
$\langle 1,0,15\rangle$	60	15	2		(2)	$\emptyset$
$\langle 1,1,19\rangle$	75	3	5		(2)	$\emptyset$
$\langle 2,2,11\rangle$	84	84	1	$\mathbb{Q}[-1,-3,-7]$	$(2,2)$	$\{2\}$
$\langle 8,4,11\rangle$	336	84	2		$(2,4)$	$\emptyset$
$\langle 11,2,23\rangle$	1008	7	12		$(2,4)$	$\emptyset$
$\langle 3,0,8\rangle$	96	24	2	$\mathbb{Q}[-1,2,-3]$	$(2,2)$	$\{3\}$
$\langle 8,8,11\rangle$	288	8	6		$(2,2)$	$\emptyset$
$\langle 11,6,27\rangle$	1152	8	12		$(2,4)$	$\emptyset$
$\langle 5,2,5\rangle$	96	24	2	$\mathbb{Q}[-1,2,-3]$	$(2,2)$	$\emptyset$
$\langle 5,4,20\rangle$	384	24	4		$(2,4)$	$\emptyset$
$\langle 5,2,29\rangle$	576	4	12		$(2,4)$	$\emptyset$
$\langle 7,6,7\rangle$	160	40	2	$\mathbb{Q}[-1,2,5]$	$(2,2)$	$\emptyset$
$\langle 7,2,23\rangle$	640	40	4		$(2,4)$	$\emptyset$
$\langle 7,4,12\rangle$	320	20	4		$(2,4)$	$\emptyset$
$\langle 2,2,23\rangle$	180	20	3	$\mathbb{Q}[-1,-3,5]$	$(2,2)$	$\{2\}$
$\langle 8,4,23\rangle$	720	20	6		$(2,4)$	$\emptyset$
$\langle 3,0,20\rangle$	240	15	4		$(2,2)$	$\{3\}$
$\langle 3,0,16\rangle$	192	3	8	$\mathbb{Q}[-1,2,-3]$	$(2,2)$	$\{3\}$
$\langle 4,4,19\rangle$	288	8	6		$(2,2)$	$\emptyset$
$\langle 16,8,19\rangle$	1152	8	12		$(2,4)$	$\emptyset$
$\langle 6,6,19\rangle$	420	420	1	$\mathbb{Q}[-1,-3,5,-7]$	$(2,2,2)$	$\emptyset$
$\langle 19,12,24\rangle$	1680	420	2		$(2,2,4)$	$\emptyset$
$\langle 19,16,31\rangle$	2100	84	5		$(2,2,4)$	$\emptyset$
$\langle 11,8,11\rangle$	420	420	1	$\mathbb{Q}[-1,-3,5,-7]$	$(2,2,2)$	$\emptyset$
$\langle 11,6,39\rangle$	1680	420	2		$(2,2,4)$	$\emptyset$
$\langle 11,10,50\rangle$	2100	84	5		$(2,2,4)$	$\emptyset$
$\langle 4,4,31\rangle$	480	120	2	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,2)$	$\emptyset$
$\langle 16,8,31\rangle$	1920	120	4		$(2,2,4)$	$\emptyset$
$\langle 15,0,16\rangle$	960	15	8		$(2,2,2)$	$\emptyset$
$\langle 12,12,13\rangle$	480	120	2	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,2)$	$\emptyset$
$\langle 13,2,37\rangle$	1920	120	4		$(2,2,4)$	$\emptyset$
$\langle 13,4,28\rangle$	1440	40	6		$(2,2,4)$	$\emptyset$
$\langle 12,12,17\rangle$	672	168	2	$\mathbb{Q}[-1,2,-3,-7]$	$(2,2,2)$	$\emptyset$
$\langle 17,10,41\rangle$	2688	168	4		$(2,2,4)$	$\emptyset$
$\langle 17,4,20\rangle$	1344	84	4		$(2,2,4)$	$\emptyset$
$\langle 13,2,13\rangle$	672	168	2	$\mathbb{Q}[-1,2,-3,-7]$	$(2,2,2)$	$\emptyset$
$\langle 13,4,52\rangle$	2688	168	4		$(2,2,4)$	$\emptyset$
$\langle 13,8,40\rangle$	2016	56	6		$(2,2,4)$	$\emptyset$
$\langle 8,8,41\rangle$	1248	312	2	$\mathbb{Q}[-1,2,-3,13]$	$(2,2,2)$	$\emptyset$
$\langle 32,16,41\rangle$	4992	312	4		$(2,2,4)$	$\emptyset$
$\langle 20,12,33\rangle$	2496	39	8		$(2,2,4)$	$\emptyset$
$\langle 12,12,73\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 48,24,73\rangle$	13440	840	4		$(2,2,2,4)$	$\emptyset$
$\langle 33,12,52\rangle$	6720	420	4		$(2,2,2,4)$	$\emptyset$

TABLE 2. (continued)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 31,22,31\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 31,18,111\rangle$	13440	840	4		$(2,2,2,4)$	$\emptyset$
$\langle 31,10,55\rangle$	6720	420	4		$(2,2,2,4)$	$\emptyset$
$\langle 20,20,47\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 47,40,80\rangle$	13440	840	4		$(2,2,2,4)$	$\emptyset$
$\langle 47,42,63\rangle$	10080	280	6		$(2,2,2,4)$	$\emptyset$
$\langle 28,28,37\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 37,18,93\rangle$	13440	840	4		$(2,2,2,4)$	$\emptyset$
$\langle 37,24,72\rangle$	10080	280	6		$(2,2,2,4)$	$\emptyset$
$\langle 8,8,167\rangle$	5280	1320	2	$\mathbb{Q}[-1,2,-3,5,-11]$	$(2,2,2,2)$	$\emptyset$
$\langle 32,16,167\rangle$	21120	1320	4		$(2,2,2,4)$	$\emptyset$
$\langle 32,24,87\rangle$	10560	660	4		$(2,2,2,4)$	$\emptyset$
$\langle 41,38,41\rangle$	5280	1320	2	$\mathbb{Q}[-1,2,-3,5,-11]$	$(2,2,2,2)$	$\emptyset$
$\langle 41,6,129\rangle$	21120	1320	4		$(2,2,2,4)$	$\emptyset$
$\langle 41,10,65\rangle$	10560	660	4		$(2,2,2,4)$	$\emptyset$

TABLE 3. Equivalence classes C of forms ($\#\delta(C)=2$, $\#C=4$)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 4,4,7\rangle$	96	24	2	$\mathbb{Q}[-1,2,-3]$	$(2,2)$	$\emptyset$
$\langle 7,6,15\rangle$	384	24	4		$(2,4)$	$\emptyset$
$\langle 7,2,7\rangle$	192	3	8		$(2,2)$	$\emptyset$
$\langle 7,4,28\rangle$	768	3	16		$(2,4)$	$\emptyset$
$\langle 8,8,17\rangle$	480	120	2	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,2)$	$\emptyset$
$\langle 17,16,32\rangle$	1920	120	4		$(2,2,4)$	$\emptyset$
$\langle 17,14,17\rangle$	960	15	8		$(2,2,2)$	$\emptyset$
$\langle 17,6,57\rangle$	3840	15	16		$(2,2,4)$	$\emptyset$

TABLE 4. Equivalence classes C of quadratic forms ($\#\delta(C)=3$, $\#C=3$)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 1,0,24\rangle$	96	24	2	$\mathbb{Q}[-1,2,-3]$	$(2,2)$	$\emptyset$
$\langle 1,0,48\rangle$	192	3	8		$(2,2)$	$\emptyset$
$\langle 1,0,72\rangle$	288	8	6		$(2,2)$	$\emptyset$
$\langle 7,4,52\rangle$	1440	40	6	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,4)$	$\emptyset$
$\langle 7,6,87\rangle$	2400	24	10		$(2,2,4)$	$\emptyset$
$\langle 7,2,103\rangle$	2880	20	12		$(2,2,4)$	$\emptyset$
$\langle 15,0,56\rangle$	3360	840	2	$\mathbb{Q}[-1,2,-3,5,-7]$	$(2,2,2,2)$	$\emptyset$
$\langle 39,12,44\rangle$	6720	420	4		$(2,2,2,4)$	$\emptyset$
$\langle 36,12,71\rangle$	10080	280	6		$(2,2,2,4)$	$\emptyset$

TABLE 5. Equivalence classes C of quadratic forms ($\#\delta(C) = 3$, $\#C = 4$)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 8,0,15\rangle$	480	120	2	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,2)$	$\emptyset$
$\langle 12,12,23\rangle$	960	15	8		$(2,2,2)$	$\emptyset$
$\langle 23,22,47\rangle$	3840	15	16		$(2,2,4)$	$\emptyset$
$\langle 23,8,32\rangle$	2880	20	12		$(2,2,4)$	$\emptyset$
$\langle 11,2,11\rangle$	480	120	2	$\mathbb{Q}[-1,2,-3,5]$	$(2,2,2)$	$\emptyset$
$\langle 11,4,44\rangle$	1920	120	4		$(2,2,4)$	$\emptyset$
$\langle 11,10,35\rangle$	1440	40	6		$(2,2,4)$	$\emptyset$
$\langle 11,8,56\rangle$	2400	24	10		$(2,2,4)$	$\emptyset$
$\langle 8,8,23\rangle$	672	168	2	$\mathbb{Q}[-1,2,-3,-7]$	$(2,2,2)$	$\emptyset$
$\langle 23,16,32\rangle$	2688	168	4		$(2,2,4)$	$\emptyset$
$\langle 15,6,23\rangle$	1344	84	4		$(2,2,4)$	$\emptyset$
$\langle 23,4,44\rangle$	4032	7	24		$(2,2,4)$	$\emptyset$

TABLE 6. Equivalence classes C of quadratic forms ($\#\delta(C) = 1$)

Q	$\lvert D\rvert$	$\lvert d\rvert$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 1,1,1\rangle$	3	3	1	$\mathbb{Q}[-3]$	(1)	$\{3\}$
$\langle 1,0,3\rangle$	12	3	2		(1)	$\{3\}$
$\langle 1,1,7\rangle$	27	3	3		(1)	$\emptyset$
$\langle 1,0,1\rangle$	4	4	1	$\mathbb{Q}[-1]$	(1)	$\{2\}$
$\langle 1,0,4\rangle$	16	4	2		(1)	$\emptyset$

TABLE 7. Orders of quadratic fields with class groups of type (1)

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	1	3	8	1	8
3	2	12	11	1	11
3	3	27	19	1	19
4	1	4	43	1	43
4	2	16	67	1	67
7	1	7	163	1	163
7	2	28			

TABLE 8. Orders of quadratic fields with class groups of type (2)

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	4	48	15	1	15	115	1	115
3	5	75	15	2	60	123	1	123
3	7	147	20	1	20	148	1	148
4	3	36	24	1	24	187	1	187
4	4	64	35	1	35	232	1	232
4	5	100	40	1	40	235	1	235
7	4	112	51	1	51	267	1	267
8	2	32	52	1	52	403	1	403
8	3	72	88	1	88	427	1	427
11	3	99	91	1	91			

TABLE 9. Orders of quadratic fields with class groups of type (4)

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	11	363	39	1	39	184	1	184	723	1	723
3	13	507	39	2	156	203	1	203	763	1	763
4	6	144	43	3	387	219	1	219	772	1	772
4	7	196	52	2	208	259	1	259	955	1	955
4	8	256	55	1	55	291	1	291	1003	1	1003
4	10	400	55	2	220	292	1	292	1027	1	1027
7	3	63	56	1	56	323	1	323	1227	1	1227
7	6	252	67	3	603	328	1	328	1243	1	1243
8	4	128	68	1	68	355	1	355	1387	1	1387
11	5	275	136	1	136	388	1	388	1411	1	1411
19	3	171	148	2	592	568	1	568	1507	1	1507
19	5	475	155	1	155	667	1	667	1555	1	1555
20	2	80	163	3	1467						

TABLE 10. Orders of quadratic fields with class groups of type $(2, 2)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	8	192	168	1	168	520	1	520
7	8	448	195	1	195	532	1	532
8	6	288	228	1	228	555	1	555
15	4	240	232	2	928	595	1	595
20	3	180	280	1	280	627	1	627
24	2	96	312	1	312	708	1	708
35	3	315	340	1	340	715	1	715
40	2	160	372	1	372	760	1	760
84	1	84	408	1	408	795	1	795
88	2	352	435	1	435	1012	1	1012
120	1	120	483	1	483	1435	1	1435
132	1	132						

TABLE 11. Orders of quadratic fields with class groups of type $(2, 4)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	16	768	84	2	336	308	1	308	987	1	987	2067	1	2067
4	12	576	88	3	792	323	3	2907	1012	2	4048	2139	1	2139
4	15	900	88	4	1408	328	2	1312	1032	1	1032	2163	1	2163
4	20	1600	91	3	819	340	2	1360	1060	1	1060	2212	1	2212
7	12	1008	91	5	2275	372	2	1488	1128	1	1128	2392	1	2392
7	16	1792	115	3	1035	403	3	3627	1131	1	1131	2451	1	2451
8	12	1152	132	2	528	427	3	3843	1204	1	1204	2632	1	2632
11	15	2475	136	2	544	456	1	456	1240	1	1240	2667	1	2667
20	4	320	148	3	1332	532	2	2128	1288	1	1288	2715	1	2715
20	6	720	148	4	2368	552	1	552	1443	1	1443	2755	1	2755
24	4	384	155	3	1395	564	1	564	1635	1	1635	2788	1	2788
24	5	600	184	2	736	568	2	2272	1659	1	1659	2968	1	2968
39	4	624	187	3	1683	580	1	580	1672	1	1672	3172	1	3172
40	3	360	203	3	1827	616	1	616	1752	1	1752	3243	1	3243
40	4	640	228	2	912	651	1	651	1768	1	1768	3355	1	3355
51	5	1275	232	3	2088	708	2	2832	1771	1	1771	3507	1	3507
52	3	468	232	4	3712	820	1	820	1780	1	1780	4123	1	4123
52	4	832	235	3	2115	852	1	852	1947	1	1947	4323	1	4323
55	4	880	260	1	260	868	1	868	1992	1	1992	5083	1	5083
56	2	224	264	1	264	915	1	915	2020	1	2020	5467	1	5467
56	3	504	276	1	276	952	1	952	2035	1	2035	6307	1	6307
68	3	612												

TABLE 12. Orders of quadratic fields with class groups of type $(2, 2, 2)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
15	8	960	1092	1	1092
120	2	480	1155	1	1155
168	2	672	1320	1	1320
280	2	1120	1380	1	1380
312	2	1248	1428	1	1428
408	2	1632	1540	1	1540
420	1	420	1848	1	1848
520	2	2080	1995	1	1995
660	1	660	3003	1	3003
760	2	3040	3315	1	3315
840	1	840			

TABLE 13. Orders of quadratic fields with class groups of type $(2, 2, 4)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
7	24	4032	372	4	5952	1288	2	5152	3432	1	3432	6708	1	6708
15	16	3840	408	4	6528	1380	2	5520	3480	1	3480	6820	1	6820
20	12	2880	420	2	1680	1428	2	5712	3588	1	3588	6820	1	6820
24	10	2400	456	2	1824	1435	3	12915	3640	1	3640	7315	1	7315
39	8	2496	520	3	4680	1540	2	6160	3795	1	3795	7395	1	7395
40	6	1440	520	4	8320	1560	1	1560	3828	1	3828	7480	1	7480
55	8	3520	532	3	4788	1672	2	6688	4020	1	4020	7540	1	7540
56	6	2016	532	4	8512	1716	1	1716	4180	1	4180	7755	1	7755
84	4	1344	552	2	2208	1752	2	7008	4260	1	4260	7995	1	7995
84	5	2100	595	3	5355	1768	2	7072	4420	1	4420	8008	1	8008
88	6	3168	616	2	2464	1860	1	1860	4440	1	4440	8052	1	8052
120	4	1920	660	2	2640	1992	2	7968	4452	1	4452	8547	1	8547
132	4	2112	708	4	11328	2040	1	2040	4488	1	4488	8680	1	8680
168	4	2688	715	3	6435	2244	1	2244	4515	1	4515	8715	1	8715
228	4	3648	760	3	6840	2280	1	2280	4740	1	4740	8835	1	8835
232	6	8352	760	4	12160	2392	2	9568	5115	1	5115	8932	1	8932
260	3	2340	952	2	3808	2436	1	2436	5160	1	5160	9867	1	9867
264	2	1056	1012	3	9108	2580	1	2580	5187	1	5187	10948	1	10948
280	3	2520	1012	4	16192	2632	2	10528	5208	1	5208	11067	1	11067
280	4	4480	1032	2	4128	2760	1	2760	5412	1	5412	11715	1	11715
308	3	2772	1092	2	4368	2968	2	11872	6195	1	6195	13195	1	13195
312	4	4992	1128	2	4512	3108	1	3108	6420	1	6420	14763	1	14763
340	3	3060	1140	1	1140	3192	1	3192	6580	1	6580	16555	1	16555
340	4	5440	1240	2	4960	3220	1	3220	6612	1	6612			

TABLE 14. Orders of quadratic fields with class groups of type $(2, 2, 2, 2)$

$\lvert d\rvert$	f	$\lvert D\rvert$
840	2	3360
1320	2	5280
1848	2	7392
5460	1	5460

TABLE 15. Orders of quadratic fields with class groups of type $(2, 2, 2, 4)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
280	6	10080	2280	2	9120	8680	2	34720
420	4	6720	2760	2	11040	9240	1	9240
520	6	18720	3192	2	12768	10920	1	10920
660	4	10560	3432	2	13728	12180	1	12180
760	6	27360	3480	2	13920	14280	1	14280
840	4	13440	3640	2	14560	14820	1	14820
1092	4	17472	4440	2	17760	17220	1	17220
1320	4	21120	4488	2	17952	19320	1	19320
1380	4	22080	5160	2	20640	19380	1	19380
1428	4	22848	5208	2	20832	19635	1	19635
1540	3	13860	5460	2	21840	20020	1	20020
1540	4	24640	7140	1	7140	31395	1	31395
1560	2	6240	7480	2	29920	33915	1	33915
1848	4	29568	8008	2	32032	40755	1	40755
2040	2	8160	8580	1	8580			

TABLE 16. Orders of quadratic fields with class groups of type $(2, 2, 2, 2, 4)$

$\lvert d\rvert$	f	$\lvert D\rvert$
5460	4	87360
9240	2	36960
10920	2	43680
14280	2	57120
19320	2	77280

REFERENCES

[BS] Z.I. Borevich and I.R. Shafarevich, *Number theory*, Academic Press, New York, 1966. MR0195803 (33:4001)

[Ch] S. Chowla, *An extension of Heilbronn's class number theorem*, Quart. J. Math. Oxford Ser. **5** (1934), 304–307.

[Cox] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, John Wiley & Sons, Inc., New York, 1989. MR1028322 (90m:11016)

[D] Harold Davenport, *Multiplicative number theory*, third ed., Graduate texts in mathematics, vol. 74, Springer-Verlag, New York, 2000. MR1790423 (2001f:11001)

[J] Gerald Janusz, *Algebraic number fields*, second ed., Graduate studies in mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR1362545 (96j:11137)

[JK] William C. Jagy and Irving Kaplansky, *Positive definite binary quadratic forms that represent the same primes*, preprint.

[La] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate studies in mathematics, vol. 110, Berlin: Springer-Verlag, 1994. MR1282723 (95f:11085)

[Lo] Stéphane Louboutin, *Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes de corps quadratiques imaginaires. Application*, C. R. Acad. Sci. Paris Sér. I Math. **310** (1990), 795–800. MR1058499 (91e:11126)

[N] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999. MR1697859 (2000m:11104)

[S] C.L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.

[T] Tikao Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. **21** (1951), 163–178. MR0051262 (14:452c)

[Wa] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

[We] P.J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124. MR0313221 (47:1776)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, BERKELEY, CALIFORNIA 94720

Current address: Institute for Mathematics and its Applications, 400 Lind Hall, 237 Church Street, University of Minnesota, Minneapolis, Minnesota 55455

E-mail address: jvoight@gmail.com