Quadratic forms and quaternion algebras: algorithms and arithmetic

by

John Michael Voight

B.S. (Gonzaga University) 1999

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

Graduate Division
of the
University of California at Berkeley

Committee in charge:

Professor Hendrik Lenstra, Chair
Professor Bjorn Poonen
Professor Roger Purves

Spring 2005

The dissertation of John Michael Voight is approved:

Chair Date

Date

Date

University of California at Berkeley

Spring 2005

Quadratic forms and quaternion algebras: algorithms and arithmetic

Abstract

Quadratic forms and quaternion algebras: algorithms and arithmetic

by

John Michael Voight

Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Hendrik Lenstra, Chair

This thesis comes in two parts which can be read independently of one another.

In the first part, we prove a result concerning representation of primes by quadratic forms. 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. We confirm their conjecture, and in fact find all pairs of such forms that represent the same primes outside of a finite set.

In the second part, we investigate a constellation of results concerning algorithms for quaternion algebras and their application to Shimura curves. Let A be a quaternion algebra over a number field F. We discuss the computational complexity and, in many cases, give effective algorithms to solve the following problems:

- Determine if $A \cong M_2(F)$, and if so, exhibit an isomorphism;
- Find a maximal order $\mathcal{O} \subset A$; and
- Determine if a right ideal $I \subset \mathcal{O}$ is principal, and if so, exhibit a generator ξ.

We then present fast methods for computing the value of hypergeometric series to large precision. Putting these together, we are able to compute special values of the map $j : \Gamma \setminus \mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ for Γ a compact triangle group, which we may recognize as putative algebraic numbers by also computing their Galois conjugates. We apply this to construct the canonical polynomial $\Phi_{\mathfrak{N}}(x, y)$ for the curve $X_0(\mathfrak{N})$ and to find nontorsion points on some elliptic curves over number fields.

To the memory of those who stood by me

and are now gone

Contents

Acknowledgements

I am very grateful to my thesis adviser, Hendrik Lenstra, for patiently guiding my intellectual development in innumerable ways and providing support while writing this dissertation. I would like to thank Bjorn Poonen and Bernd Sturmfels for teaching me so much; Peter Stevenhagen, Pete Clark, and Jared Weinstein for their helpful comments on portions of this thesis; Samit Dasgupta and Noam Elkies for their incredible insights and encouragement; Ronald van Luijk for his constant companionship; and William Stein and the MECCAH cluster for computer time. Surviving the process of writing this dissertation was only made possible by Paul Berg. Finally, I would like to give my sincerest gratitude to Aaron Minnis, David Michaels, Kristin Olson, Missy Longshore, Mary Weaver, my mother, and the rest of my family and friends for their love and understanding.

Part I

Quadratic forms

Chapter 1

Primes represented by quadratic forms

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 $p = 12n + 1$. What other like pairs of forms exist? Jagy and Kaplansky [27] 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.

In this part, using the tools of class field theory 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 $\mathbb{Q}(\sqrt{D})$, 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 say then that they represent *almost the same primes.* A form represents the same primes as any equivalent form under the action of $GL_2(\mathbb{Z})$. Hence from now on (except in the statement of Proposition 1.2.4, see Remark 1.2.5, and in the proof of Lemma 1.2.15), 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 $\gcd(a, b, c) > 1$, so 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.

The main result of Part I is the following (Theorem 2.4.2).

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* $\#\delta(C) \geq 4$.

The forms are listed in Tables 3.1–3.5 in Chapter 3.

As a complement to this theorem, we identify those classes of forms which have the same fundamental discriminant (Theorem 2.1.2).

Theorem. *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* $4 < |D_1| < |D_2|$ *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 2.4.4 at the end of this article.)

As a side result, we are also able to give the following classification (Proposition 2.3.2) of class groups of quadratic orders. (See §§2–3 for the notation.) 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 $r \in \mathbb{Z}_{\geq 0}$.

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 3.7–3.16 in Chapter 3.

We begin by recalling some facts from Galois theory, class field theory, and the theory of binary quadratic forms (§§1.1–1.2). In this framework, the condition that two quadratic forms represent almost the same primes places restrictions on the corresponding ring class fields and their Galois groups (§1.3), which are class groups. We use a bit of group theory to determine which of these groups can occur. We then treat the case where the forms come from fields with the same fundamental discriminant (§2.1). The list of forms for which the fields have different fundamental discriminant can be effectively shown to be finite and by an exhaustive computer search all such fields can be identified (§2.2). We then prove an independent result, not needed in the sequel, listing all imaginary quadratic fields except perhaps one with class group of type dividing $(2, \ldots, 2, 4)$ (§2.3).) We then finish the analysis (§2.4).

1.1 Fields of definition

We begin with a bit of Galois theory. 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

$$\mathrm{res}_E : G \to \mathrm{Hom}_K(E, \overline{K})$$

$$\sigma \mapsto \mathrm{res}_E(\sigma) = \sigma|_E.$$

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

Lemma 1.1.1. *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 1.1.2. 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 1.1.3. If L is a field of definition with $S = \mathrm{res}_L^{-1}(T)$ for some $T \subset \mathrm{Hom}_K(L, \overline{K})$, 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 1.1.1 states that every open and closed subset $S \subset G$ has a field of definition.

Definition 1.1.4. 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 1.1.5. *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 1.1.3, the field L is a field of definition for S if and only if

$$\text{for all } \sigma \in G \text{ and for all } \tau \in S, \text{ we have } \sigma|_L = \tau|_L \text{ implies } \sigma \in S.$$

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 1.1.1, 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 A the ring of integers of K, and let L be a Galois extension of K with ring of integers B. Then for any prime $\mathfrak{p}$ of K which is unramified in L and prime $\mathfrak{q}$ of L which lies over $\mathfrak{p}$, we have a unique element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathrm{Gal}(L/K)$ such that

$$\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}(\alpha) \equiv \alpha^{\#(A/\mathfrak{p})} \pmod{\mathfrak{q}}$$

for all $\alpha \in B$. If $\mathfrak{q}'$ also lies over $\mathfrak{p}$, then $\mathfrak{q}' = \sigma(\mathfrak{q})$ for some $\sigma \in \mathrm{Gal}(L/K)$, and hence $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma \,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\, \sigma^{-1}$. We define the *Frobenius symbol of* $\mathfrak{p}$ *in* L/K to be the conjugacy class

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} : \mathfrak{q} \text{ lies over } \mathfrak{p}\}.$$

Let Π be the set of equivalence classes of sets of primes of K, where two sets are identified 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

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

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 1.1.6. *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 1.1.3, 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 [35, 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. □

1.2 Ring class fields

In this section, we summarize without proof the few results we will need from class field theory and the theory of L-functions (see e.g. [11], [35], and [62]), and we prove a result which describes a quotient of local unit groups explicitly as an abelian group (Proposition 1.2.13).

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 isomorphism classes of invertible A_f-modules. 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 $\alpha \equiv z \pmod{fA}$ and $z \in \mathbb{Z}$. We write $h_f(d) = h(D) = \#\,\mathrm{Cl}(D)$.

Proposition 1.2.1 ([11, §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 map*.

Remark 1.2.2. 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 1.2.3. *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 1.2.4 ([11, 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 1.2.5. Note that exactly one element of any conjugacy class $\{\sigma, \sigma^{-1}\}$ is associated in this way with a $GL_2(\mathbb{Z})$-reduced form, and it is this association we will use henceforth.

Remark 1.2.6. 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.

Proposition 1.2.7. *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 Galois group* $\mathrm{Gal}(P_{(f)}/\mathbb{Q})$ *is itself abelian and of exponent* 2*.*

The field $P_{(f)}$ is called the *genus class field of* K *of modulus* f. This proposition follows immediately from Proposition 1.2.1, as inversion acts trivially on a group of exponent dividing 2.

Proposition 1.2.8. *The genus class field* $P_{(f)}$ *of* K *is the compositum of all fields* $K = \mathbb{Q}(\sqrt{m})$ *of discriminant* $m \in \mathbb{Z}$ *satisfying* $m\,\mathrm{disc}(\mathbb{Q}(\sqrt{dm})) \mid D$*.*

Proof. By the preceding proposition, the group $\mathrm{Gal}(P_{(f)}/\mathbb{Q})$ is abelian and of exponent 2, so by Kummer theory it is the compositum of quadratic extensions of $\mathbb{Q}$. Let $H = \mathbb{Q}(\sqrt{m})$ be a quadratic field of discriminant $m \in \mathbb{Z}$. Note that automatically every prime of K which is inert over $\mathbb{Q}$ and unramified in HK/K splits completely in HK; therefore $H \subset P_{(f)}$ if and only if the conductor $\mathfrak{f}$ of the extension HK/K has $\mathfrak{f} \mid f$.

By the conductor-discriminant formula [62, Theorem 3.11], the conductor of the extension HK/K is equal to $\operatorname{disc}(HK/K)$, and $\operatorname{disc}(HK/\mathbb{Q}) = dmn$, where $n = \operatorname{disc}(\mathbb{Q}(\sqrt{dm}))$. But

$$\operatorname{disc}(HK/\mathbb{Q}) = N_{K/\mathbb{Q}}(\operatorname{disc}(HK/K))\operatorname{disc}(K/\mathbb{Q})^2 = N(\mathfrak{f})d^2 = \mathfrak{f}^2 d^2.$$

Putting these together, we conclude that $\mathfrak{f}^2 = mn/d$, and so $\mathfrak{f} \mid f$ if and only if $mn \mid df^2 = D$, as claimed. □

Given this proposition, we can compute the genus class field explicitly. For p an odd prime we write $p^* = (-1)^{(p-1)/2}p$.

Corollary 1.2.9. *Let $p_1, \dots, p_r$ be the odd primes dividing D and let*

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

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. Let $m \in \mathbb{Z}$ be a discriminant, and let $p \mid m$ be an odd prime. We first claim that

$$\mathbb{Q}(\sqrt{m}) \subset P_{(f)} \iff \mathbb{Q}(\sqrt{m/p^*}) \subset P_{(f)} \text{ and } \mathbb{Q}(\sqrt{p^*}) \subset P_{(f)}.$$

The direction $(\Leftarrow)$ is clear. In the other direction, suppose $\mathbb{Q}(\sqrt{m}) \subset P_{(f)}$, so that by the preceding proposition we have $m\,\mathrm{disc}(\mathbb{Q}(\sqrt{dm})) \mid D$. Since $dm/p^* \equiv dm \pmod 4$ we have

$$\mathrm{disc}\left(\mathbb{Q}(\sqrt{dm/p^*})\right) \Bigm| p^*\,\mathrm{disc}\left(\mathbb{Q}(\sqrt{dm})\right)$$

hence

$$(m/p^*)\,\mathrm{disc}\left(\mathbb{Q}(\sqrt{dm/p^*})\right) \Bigm| m\,\mathrm{disc}\left(\mathbb{Q}(\sqrt{dm})\right) \Bigm| D;$$

by the preceding proposition, we obtain $\mathbb{Q}(\sqrt{m/p^*}) \subset P_{(f)}$ as well, hence $\mathbb{Q}(\sqrt{p^*}) \subset P_{(f)}$. Therefore by the claim, to prove the proposition it suffices to check if $\mathbb{Q}(\sqrt{m})$ is contained in $P_{(f)}$ for $m = p^*$ for all odd primes p and for $m = -4, 8, -8$.

First let $m = p^*$ for p an odd prime, and let $g = \gcd(d, p^*)$. We have $n = \mathrm{disc}(\mathbb{Q}(\sqrt{dp^*})) = dp^*/g^2$, so $p^*n \mid df^2$ if and only if $(p^*/g) \mid f$ if and only if $p \mid df$, which is the statement. Next let $m = -4$. If $d \equiv 1 \pmod 4$, then $n = \mathrm{disc}(\mathbb{Q}(\sqrt{-4d})) = -4d$, hence $\sqrt{-1} \in P_{(f)}$ if and only if $-4n = 16d \mid df^2$ if and only if $4 \mid f$. If $d \equiv 4 \pmod 8$, then $n = -d/4$, hence $\sqrt{-1} \in P_{(f)}$ if and only if $d \mid df^2$, which holds automatically; this could also be proven by noting that $K(\sqrt{-1})$ is an unramified extension of K, so that $\mathbb{Q}(\sqrt{-1})$ is already contained in $P_{(1)}$. If $d \equiv 0 \pmod 8$, then $n = -d$, and $4d \mid df^2$ if and only if $2 \mid f$. Now let $m = \pm 8$. A similar calculation shows that $n = \mathrm{disc}(\mathbb{Q}(\sqrt{\pm 8d})) = \pm 8d$ or $n = \pm 2d$ according as $d \equiv 1 \pmod 4$ or $d \equiv 4 \pmod 8$, and therefore $\sqrt{\pm 2} \in P_{(f)}$ if and only if $8n \mid df^2$ if and only if $8 \mid f$ or $4 \mid f$, accordingly. And if $d \equiv 0 \pmod 8$ then $n = \pm d/8$, so $\sqrt{\pm 2} \in P_{(f)}$ for all f, for again $K(\sqrt{\pm 2})$ is an unramified extension of K. Finally, we see by the preceding that $\sqrt{\pm 2} \in P_{(f)}$ implies $\sqrt{-1} \in P_{(f)}$, and the result follows. □

If G is an abelian group and $n \in \mathbb{Z}_{>0}$, then we define $G[n] = \{g \in G : ng = 0\}$. The following two corollaries are immediate from the proposition.

Corollary 1.2.10. *The odd primes p which ramify in $P_{(f)}$ are exactly the odd primes that divide D.*

Corollary 1.2.11. *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 1.2.12 ([11, 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 functorial in f (by divisibility), and

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

We will need only part of the following proposition, but we give a full statement for completeness, as the result may be of independent interest.

Proposition 1.2.13. *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

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

and

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

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

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

Proof. The first statement follows from the Chinese remainder theorem. Throughout we assume p is a prime and $e > 0$.

For the rest, first 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.

We first deal with the case $(d/p) = 1$. Then it is easy to see [42, §II.5] that

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

From now on we assume $(d/p) \neq 1$.

Let K_p denote the completion of K at p, so that A_p is its valuation ring. Then K_p is field extension of $\mathbb{Q}_p$ with $[K_p : \mathbb{Q}_p] = 2$. In fact, if $(d/p) = -1$, then K_p is the unique unramified field extension of $\mathbb{Q}_p$ of degree 2, and if $(d/p) = 0$, then K_p is a ramified field extension of $\mathbb{Q}_p$.

We denote by v the unique valuation on K_p normalized so that $v(p) = 1$. Define:

$$\mathfrak{p} = \{x \in A_p : v(x) > 0 \text{ for all } v\},$$

$$V(A_p) = \{x \in A_p : v(x) > 1/(p-1) \text{ for all } v\},$$

$$\mu(A_p) = \{x \in A_p : x^m = 1 \text{ for some } m \in \mathbb{Z}_{>0}\}.$$

We find that $\mathfrak{p} = \pi A_p$ for some $\pi \in A_p$.

It follows from [42, Proposition II.5.4] that there exists a (continuous) homomorphism $\log_p : A_p^* \to A_p$ such that

$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

for all $x \in \mathfrak{p}$, with the property that $\log_p$ restricts to an isomorphism $1 + V(A_p) \xrightarrow{\sim} V(A_p)$. Moreover, we have that $1 + p^t A_p \xrightarrow{\sim} p^t A_p$ for all $t > 1/(p-1)$.

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

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

Now suppose $p^e \neq 2$. Then one has an exact sequence

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

the second map is well-defined, for if $x, y \in A_p^*$ satisfy $x \equiv y \pmod{p^e}$, then indeed

$$\frac{x}{y} \in 1 + p^e A_p \subset 1 + V(A_p).$$

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:

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

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

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

We compute that

$$V(A_p) = \begin{cases} \mathfrak{p}^3, & \text{if } p=2 \text{ and } (d/2)=0; \\ \mathfrak{p}^2 = 4A_2, & \text{if } p=2 \text{ and } (d/2)=-1; \\ 3A_3, & \text{if } p=3 \text{ and } (d/3)=0; \\ \mathfrak{p}, & \text{otherwise.} \end{cases}$$

Furthermore, $V(\mathbb{Z}_p)=p\mathbb{Z}_p$ for $p \neq 2$ and $V(\mathbb{Z}_2)=4\mathbb{Z}_2$.

We now exhibit an element $\beta \in A_p$ such that $V(A_p) = V(\mathbb{Z}_p) + \mathbb{Z}_p\beta$ with known valuation. First, suppose $(d/p)=-1$, and let $\epsilon \in A_p$ be such that $A_p = \mathbb{Z}_p + \epsilon\mathbb{Z}_p$ as additive groups. It follows that $v(\epsilon)=0$. By the previous paragraph,

$$V(A_p) = \begin{cases} 4\mathbb{Z}_2 + 4\epsilon\mathbb{Z}_2, & \text{if } p=2; \\ p\mathbb{Z}_p + p\epsilon\mathbb{Z}_p, & \text{otherwise.} \end{cases}$$

Thus we may take $\beta = 4\epsilon$ or $\beta = p\epsilon$, according as $p=2$ or not. Next, suppose that $(d/p)=0$. Then

$$V(A_p) = \begin{cases} \pi^3\mathbb{Z}_2 + 4\mathbb{Z}_2, & \text{if } p=2; \\ 3\mathbb{Z}_3 + 3\pi\mathbb{Z}_3, & \text{if } p=3; \\ \pi\mathbb{Z}_p + p\mathbb{Z}_p, & \text{otherwise.} \end{cases}$$

So we may take $\beta=\pi^3$, $\beta=3\pi$, or $\beta=\pi$, accordingly. It follows that the group

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

is cyclic and generated by β, and that the order of β is p^d, where $d = \lceil e - v(\beta) \rceil$. Breaking this up into cases, we obtain:

$$\frac{V(A_p)/p^eA_p}{V(\mathbb{Z}_p)/p^e\mathbb{Z}_p} \cong \begin{cases} \mathbb{Z}/2^{e-1}\mathbb{Z}, & \text{if } p = 2 \text{ and } (d/2) = 0; \\ \mathbb{Z}/2^{e-2}\mathbb{Z}, & \text{if } p = 2 \text{ and } (d/2) = -1; \\ \mathbb{Z}/3^{e-1}\mathbb{Z}, & \text{if } p = 3; \\ \mathbb{Z}/p^{e-1}\mathbb{Z}, & \text{if } p \neq 2,3 \text{ and } (d/p) = -1; \\ \mathbb{Z}/p^{e}\mathbb{Z}, & \text{if } p \neq 2,3 \text{ and } (d/p) = 0. \end{cases}$$

This completes the analysis of the kernel of ϕ in $(\diamond)$.

Now we analyze the image of ϕ. First suppose $p \neq 2, 3$. Then we have $A_p^*/(1+V(A_p)) \cong \mu(A_p)$ (see [42, Proposition II.5.3]), and this group can be computed as follows. If L_w is any local field of characteristic p with residue field k_w, then the group of roots of unity of order prime to p in L_w is isomorphic to k_w^*. 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

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

where for any $m \in \mathbb{Z}_{>0}$ we denote by μ_m the group of roots of unity of order dividing m, a cyclic group of order m. Since $\mu(\mathbb{Z}_p) = \mu_{p-1}$, putting these two pieces together, we see that in the exact sequence $(\diamond)$, the kernel and image groups have relatively prime order, so the exact sequence splits, and we obtain the result of the proposition.

If $p = 3$, then we use the fact that there are only 3 field extensions of $\mathbb{Q}_p$ of degree 2 up to isomorphism (namely, $\mathbb{Q}_3(\sqrt{c})$ where $c \in \{-3, 3, -1\}$), and we see easily that

$$\frac{A_3^*/(1+V(A_3))}{\mathbb{Z}_3^*/(1+V(\mathbb{Z}_3))} \cong \begin{cases} \mu_2, & \text{if } (d/3) = 1; \\ \mu_4, & \text{if } (d/3) = -1; \\ \mu_3, & \text{if } (d/3) = 0. \end{cases}$$

Again ($\diamond$) splits for $(d/3) \neq 0$ and also trivially when $e = 1$. If $d \equiv 6 \pmod 9$, then sequence also splits by mapping the group into $\mu_3(A_3^*) \subset A_3^*$. For $d \equiv 3 \pmod 9$, we have $K_3 \cong \mathbb{Q}_3(\sqrt{3})$, and one checks directly that the element $1 + \sqrt{3}$ is an element of order 3^e in $(A_3/3^e A_3)^*$ modulo $(\mathbb{Z}_3/3^e\mathbb{Z}_3)^*$, so the sequence does not split.

For $p = 2$, we continue in the spirit of our local computations to complete the proof. We have already dealt with the case $e = 1$ above. Every field extension of $\mathbb{Q}_2$ of degree 2 is isomorphic to $\mathbb{Q}_2(\sqrt{c})$ for $c \in \{-1, \pm 2, \pm 3, \pm 6\}$. One finds that:

$$\#\frac{A_2^*/(1+V(A_2))}{\mathbb{Z}_2^*/(1+V(\mathbb{Z}_2))} = \begin{cases} 6, & \text{if } d \equiv 5 \pmod 8; \\ 2, & \text{otherwise.} \end{cases}$$

Now ($\diamond$) splits for $(d/2) = -1$ mapping $\mu_6 \subset A_2^*$ and for $d \equiv 0 \pmod 4$ we have $c \in \{-1, 3\}$ and the sequence splits again mapping the nontrivial element to $\sqrt{c}$. The sequence does not split when $d \equiv 0 \pmod 8$, so that $c \in \{\pm 2, \pm 6\}$ because the element $1 + \sqrt{c}$ is an element of order 2^e in $(A_2/2^e A_2)^*$ modulo $(\mathbb{Z}_2/2^e\mathbb{Z})^*$. This completes the proof. □

Definition 1.2.14. 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 $\sigma' \leftrightarrow Q'$.

We now prove an elementary lemma.

Lemma 1.2.15. *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 $|b| \le a \le c$ 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 $4a \le c$ 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 1.2.13.

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. □

In the sequel, we will use lower bounds on the sizes of these class groups. 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. [13, §6]). By the Brauer-Siegel theorem, $\log h(d)$ is asymptotic to $\log(\sqrt{|d|})$ as $|d| \to \infty$; by a result of Siegel [52], 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 1.2.16 (Tatuzawa [57]). *For any $0 < \epsilon < 1/2$, there is at most one fundamental discriminant $d < 0$ with $\log|d| > \max(1/\epsilon, 11.2)$ satisfying*

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

1.3 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 1.3.7), 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 1.3.9) and the same fundamental discriminant (Proposition 1.3.10).

Notation 1.3.1. 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 $h(D) = \#\operatorname{Cl}(D) = [R : K]$ and genus class field $P \supset K$. The form Q corresponds to an ideal class $[\mathfrak{a}]$ in $\operatorname{Pic}(A_f)$, and by the Artin map (1.2.1) $[\mathfrak{a}]$ corresponds to an element $\sigma \in \operatorname{Gal}(R/K)$. We define the set

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

Note that $\mathcal{P}(S)$ 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 $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and closed under conjugation. Let $L = L(S)$ be the minimal field of definition for S, which exists by Corollary 1.1.5; 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 1.3.2. *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 $\operatorname{Gal}(R/L)$ is generated by $\sigma^2 \in \operatorname{Cl}_f(d)^2 = \operatorname{Gal}(R/P)$. □

Now suppose that Q_1 and Q_2 are a pair of forms, following Notation 1.3.1 with appropriate subscripts. Rephrasing our situation in terms of class field theory (Proposition 1.2.4), we have the following lemma.

Lemma 1.3.3. *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 1.3.4. 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 $Q_1 = Q_2$.

It is immediate from this lemma that Q_1 and Q_2 have the same set $\mathcal{P}(S)$ (up to a finite set) and by the injectivity of Lemma 1.1.6 the same set S, hence the same minimal field of definition L.

Lemma 1.3.5. *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 1.3.6. *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 1.3.3 we conclude $\sigma_1|_P = \sigma_2|_P$. □

Proposition 1.3.7. *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 1.2.1 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 $(2, \dots, 2, 4)$.

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

Remark 1.3.8. This proposition answers a question of Jagy and Kaplansky [27]. 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 1.3.7 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 $(2, \dots, 2, 4)$.

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

Theorem 1.3.9. *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 $(2, \dots, 2, 4)$ and σ_i has order 4.*

Proof. We have shown these conditions are necessary: condition (i) follows from Lemma 1.3.5 and Corollary 1.3.6 and (ii) follows from Proposition 1.3.7.

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 1.3.1, with subscripts). From Lemma 1.3.2 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 now will 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 $(2, \dots, 2, 4)$ 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 1.3.3. □

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

Proposition 1.3.10. *Let Q_1, Q_2 be forms with fundamental discriminants $d_1 = d_2 = d$.*

(a) *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:

- *ϕ is an isomorphism;*
- *(†) The kernel of ϕ has order 2, generated by σ_2^2, and σ_1 has order 2.*

(b) *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. First, we prove (a). From Proposition 1.2.1, we conclude that $R_1 \subset R_2$. If $R_1 = R_2$ then we are in case (i). Otherwise, by Lemma 1.3.2, 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 (†).

To prove the second statement, let $R = R_f$. Then by Corollary 1.2.3, $R_1 \cap R_2 = R$. Since $L \subset R_1, R_2$ we see that $L \subset R$, therefore by Remark 1.1.3 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 1.3.2, 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 1.3.4. □

Chapter 2

Finding the list of forms

In this chapter, we use the results of Chapter 1 to characterize forms which represent almost the same primes.

2.1 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 1.3.1. Throughout, 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 1.3.4 either $Q_1 = Q_2$ or $Q_1 \not\sim Q_2$. So without loss of generality we may assume that $f_1 < f_2$.

Proposition 2.1.1. *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 1.3.2 we have $[R_2 : R_1] \in \{1, 2\}$. On the other hand, by Lemma 1.3.5, R_1 and R_2 have the same genus class field, so from Proposition 1.2.9, if $p \nmid d$ is an odd prime then $p \mid f_1$ if and only if $p \mid f_2$. From Lemma 1.2.12 we have

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

where

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

From Proposition 1.3.10(b), 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 find only finitely many cases to check, and in fact again we have either $f_2 = 2f_1$ or $f_2 = 4f_1$. □

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 1.3.10.

Theorem 2.1.2. *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 apply Proposition 2.1.1 and find cases (iii) and (iv).

More generally, we apply Proposition 1.3.10. The map ϕ is an isomorphism if and only if $h(D_2) = h(D_1)$. By Proposition 1.2.13 $(*)$, this occurs if and only if $(d/2) = 1$ (and $f_2 = 2f_1$), which is case (i).

For condition (†), 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 1.2.12, we obtain a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & C(f_2) \arrow[r] \arrow[d, "\psi"] & \mathrm{Cl}_{f_2}(d) \arrow[d, "\phi"] \\
1 \arrow[r] & C(f_1) \arrow[r] & \mathrm{Cl}_{f_1}(d)
\end{tikzcd}$$

Now if (†) holds then $C(f_2) \to C(f_1)$ is a nonsplit $\mathbb{Z}/2\mathbb{Z}$-extension, so we see from $(*)$ 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 1.2.15. □

2.2 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. Recall also the Notation 1.3.1.

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 2.2.1. *The sets*

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

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

First note the following lemma.

Lemma 2.2.2 ([64, 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 2.2.3. *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 implies then that $(N\mathfrak{p})^c = p^c > d/4$. □

Lemma 2.2.4. *If $\mathrm{Cl}_f(d)$ is of type dividing and $|d| > 2500$, then $f \in \{1, 2, 3, 4, 6, 8, 12\}$.*

Proof. Recall the exact sequence of Lemma 1.2.12

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

where 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 1.2.13 (∗), we conclude that $p^2 \nmid f$ and $p = 3$ or $p = 5$. When $|d| > 2500$, we cannot have $5 \mid f$, for this can happen only if $(d_i/5) = 1$, which contradicts Corollary 2.2.3. 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 $(*)$ 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. We have the following diagram of fields:

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & K_0 \arrow[d, dash] & K_2 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Lemma 2.2.5. *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 1.3.5, the ring class fields R_1 and R_2 have the same genus class field, and by Lemma 1.3.7, the group $\mathrm{Cl}_{f_i}(d_i)$ is of type dividing $(2, \ldots, 2, 4)$ for $i = 1, 2$. By Corollary 1.2.10, the same set of odd primes divide the discriminants D_1, D_2. Then by Lemma 2.2.4, 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 2.2.3. We cannot have $(d_1/p) = (d_2/p) = -1$, as then $(d_1d_2/p) = 1$ 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 2.2.6. 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 2.2.7. *Let $p_1 = 3$, $p_2 = 5$, $\dots$ be the sequence of odd primes in increasing order, and for each $t \in \mathbb{Z}_{\geq 1}$ let*

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

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

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

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 1.2.16) to obtain the following.

Proposition 2.2.8. *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 1.2.16 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 2.2.5, 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 1.2.11) 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 2.2.5, 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 2.2.5, 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 2.2.7, 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 2.2.1. First, by exhaustive listing, 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 2.2.3 to rule out many of these discriminants. This was accomplished in MAGMA. (The code is available from the author by request.) By Proposition 2.2.8, 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 $\mathrm{Cl}_f(d)$ is of type dividing $(2, \ldots, 2, 4)$. By Lemma 2.2.4, 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 1.3.5 that $|d_2| \leq 4 \cdot 29568 < B$. Otherwise, by Remark 2.2.6, 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. □

2.3 Computing class groups

To give an alternative proof of Proposition 2.2.1, we may also characterize with at most one possible exception all imaginary quadratic extensions having class group of type dividing $(2, \ldots, 2, 4)$. This result is not needed in the sequel, but it also yields an independent result (Theorem 2.3.2).

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 [8].

Proposition 2.3.1 (Weinberger [64], Louboutin [38])**.** *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, with*

$$|D| = |d| \in \{3, 4, 7, 8, \ldots, 3003, 3315, 5460\},$$

and at least 36 *and at most* 37 *such discriminants of nonmaximal orders, with*

$$|D| \in \{3 \cdot 2^2, 3 \cdot 3^2, \ldots, 1848 \cdot 2^2\}.$$

Under the assumption of a suitable generalized Riemann hypothesis, these lists are complete.

The list of these discriminants can be found in [3, Table 5]. Here we have a small variant of this problem, to which we may apply the same techniques.

Theorem 2.3.2. *There are at least* 226 *and at most* 227 *fundamental discriminants* $D = d$ *such that* $\mathrm{Cl}(d)$ *is of type dividing* $(2, \ldots, 2, 4)$*, 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 1.2.16).

Lemma 2.3.3. *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* $(2, \ldots, 2, 4)$*, 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 $(2, \ldots, 2, 4)$. Recall as in the proof of Proposition 2.2.8 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 1.2.16 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 2.2.7, 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 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 main result of this section.

Proof of Proposition 2.3.2. 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 2.3.3 and Lemma 2.2.4 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 2.3.3, 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 Lemma 2.2.3: 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 $(2, \dots, 2, 4)$. 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 2.3.4. *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 $|d| < 1.3 \cdot 10^{10}$.*

The proof of this proposition relies on the following theorem.

Proposition 2.3.5 (Louboutin [38]). *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 2.3.4. We follow [38, Théorème 2]. Let g be the number of distinct prime factors of the discriminant d. Then $\#\,\mathrm{Cl}(d)[2] = 2^{g-1}$ so $h(d) \leq 2^g$. From Proposition 2.3.5, 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

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

then $|d| < \widehat{d}_{t_0}$ (see [38]). We compute easily that in this case $\widehat{d}_{t_0} = 4 \cdot 3 \cdot \ldots \cdot 29 < 1.3 \cdot 10^{10}$. □

Theorem 2.3.6. *Under the above Riemann hypothesis, there are exactly* 226 *fundamental discriminants d such that* $\mathrm{Cl}(d)$ *is of type dividing* $(2, \dots, 2, 4)$*, and* 199 *such discriminants D of nonmaximal orders.*

This follows from Proposition 2.3.4 and the computations performed in the proof of Proposition 2.3.2.

2.4 Finding the pairs of quadratic forms

To conclude, we list all forms with $K_1 \neq K_2$. Using Corollary 1.2.9, we first compute the genus class field for each of the 425 discriminants found in section 5. We find 86 pairs of discriminants for which the genus class fields are equal.

We now apply Theorem 1.3.9. 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 2.4.1. 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 $\mathbb{Q}(\sqrt{2},\sqrt{-3},\sqrt{11})$, 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 1–3.

Theorem 2.4.2. *There are exactly* 67 *equivalence classes of forms C with $\#\delta(C) \geq 2$. There are exactly* 6 *classes with $\#\delta(C) = 3$ and there is no class with $\#\delta(C) \geq 4$.*

Definition 2.4.3. 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 2.4.4. Jagy and Kaplansky [27] 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 $\langle 4,4,19\rangle$.

Chapter 3

Tables

In Tables 3.1–3.2, we list equivalence classes with two fundamental discriminants ($\delta(C) = 2$), then in Tables 3.3–3.5 those with three fundamental discriminants, then in Table 3.6 the exceptional cases with one fundamental discriminant (2.1.2, (iv)–(vi)). 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 1.3.5), denoted $\mathbb{Q}[a_1, \dots, a_r] = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_r})$. 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 (2.4.3).

In Tables 3.7–3.16, we list the orders of imaginary quadratic fields with class group of type dividing $(2, \dots, 2, 4)$, with at most possible exception (as in Theorem 2.3.2). 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 sorted by fundamental discriminant and then discriminant.

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		$(2,2,4)$	$\emptyset$
$\langle 13,6,21\rangle$	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		$(2,2,4)$	$\emptyset$

Table 3.1: Equivalence Classes C of Forms ($\#\delta(C) = 2$, $\#C = 2$), 1 of 2

Q	$\|D\|$	$\|d\|$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 20,4,23\rangle$	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 3.1: Equivalence Classes C of Forms ($\#\delta(C)=2$, $\#C=2$), 2 of 2

Q	$\|D\|$	$\|d\|$	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		$(2,2,4)$	$\emptyset$

Table 3.2: Equivalence Classes C of Forms ($\#\delta(C)=2$, $\#C=3$), 1 of 2

Q	$\|D\|$	$\|d\|$	f	P	$\mathrm{Cl}_f(d)$	E
$\langle 13, 2, 13\rangle$	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		$(2, 2, 2, 4)$	$\emptyset$
$\langle 31, 22, 31\rangle$	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 3.2: Equivalence Classes C of Forms ($\#\delta(C) = 2$, $\#C = 3$), 2 of 2

Q	$\|D\|$	$\|d\|$	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 3.3: Equivalence Classes C of Forms ($\#\delta(C) = 2$, $\#C = 4$)

Q	$\|D\|$	$\|d\|$	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 3.4: Equivalence Classes C of Quadratic Forms ($\#\delta(C)=3$, $\#C=3$)

Q	$\|D\|$	$\|d\|$	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 3.5: Equivalence Classes C of Quadratic Forms ($\#\delta(C)=3$, $\#C=4$)

Q	$\|D\|$	$\|d\|$	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 3.6: Equivalence Classes C of Quadratic Forms ($\#\delta(C)=1$)

$\lvert d\rvert$	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 3.7: Orders of Quadratic Fields with Class Groups of Type (1)

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	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 3.8: 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	$\lvert D\rvert$	$\lvert d\rvert$	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 3.9: 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	$\lvert D\rvert$
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 3.10: 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	$\lvert D\rvert$	$\lvert d\rvert$	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 3.11: Orders of Quadratic Fields with Class Groups of Type $(2, 4)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
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 3.12: Orders of Quadratic Fields with Class Groups of Type $(2, 2, 2)$

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	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 3.13: Orders of Quadratic Fields with Class Groups of Type $(2, 2, 4)$

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

Table 3.14: Orders of Quadratic Fields with Class Groups of Type $(2, 2, 2, 2)$

$\lvert d\rvert$	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 3.15: Orders of Quadratic Fields with Class Groups of Type $(2, 2, 2, 4)$

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

Table 3.16: Orders of Quadratic Fields with Class Groups of Type $(2, 2, 2, 2, 4)$

Part II

Quaternion algebras

Chapter 4

Quaternion algebras

In this part, we investigate a constellation of results concerning algorithms for quaternion algebras and their application to Shimura curves. We first discuss these results in brief to introduce the reader. Let F be a field not of characteristic 2.

In §4.1, we give basic definitions and results. Let A be a *quaternion algebra* over F, namely, a central simple algebra of dimension 4 over F. In §4.2, we exhibit two algorithms: in Algorithm 4.2.7, given a zerodivisor $\alpha \in A$, we compute an isomorphism $A \xrightarrow{\sim} M_2(F)$, and in Algorithm 4.2.9 we give a method for computing a *standard representation* for A (see the definitions therein). From now on, let F be a number field. In §4.3, we take up the task in Algorithm 4.3.8 of computing a *maximal order* for A, which is a natural analogue of the notion of the ring of integers of a number field. We also prove the following theorem (see Theorem 4.3.10).

Theorem. *The problem of computing a maximal order for a quaternion algebra A over any fixed number field F is probabilistic polynomial time equivalent to the problem of factoring integers.*

Finally, in §4.4, we introduce the *ideal classes* of A, and when A satisfies a condition known as the *Eichler condition*, we exhibit an algorithm which computes a set in bijection with the set of ideal classes, and furthermore we provide an algorithm which tests if a right ideal I is principal and, if F is totally real, computes a generator (Algorithm 4.4.6).

In Chapter 5, we apply these algorithms to *Shimura curves*. In §5.1, we introduce basic definitions and results concerning these curves. We will primarily investigate the case of *arithmetic compact triangle groups* $\Gamma \subset PSL_2(\mathbb{R})$ arising from the unit groups of indefinite quaternion algebras whose action on the upper half-plane $\mathfrak{H}$ yields a fundamental domain which is a compact hyperbolic triangle. In §5.2, we present fast methods for computing the value of hypergeometric series to large precision—this can safely be skipped for the reader willing to accept Algorithm 5.2.8, which provides a means of calculating the map $j : \Gamma \setminus \mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ to high precision. In §5.3, we define *CM points* and show in Algorithm 5.3.4 how to apply the Shimura reciprocity law to compute these points to high precision as complex numbers and recognize them as putative algebraic numbers by also computing their Galois conjugates. Finally, in §5.4, we give some examples of how these algorithms work in practice, and we show how to construct the canonical polynomial $\Phi_{\mathfrak{N}}(x, y)$ for the Shimura curve $X_0(\mathfrak{N})$ and to find nontorsion points on some elliptic curves over number fields.

4.1 Definitions

In this section, we introduce quaternion algebras and describe some of their basic properties. A reference for the material in this section is [59]. Throughout this section, let F be a field with $\operatorname{char} F \neq 2$, and let $\overline{F}$ be a separable closure of F. A ring is assumed to be an associative ring with 1, and an algebra over F is a ring equipped with an embedding $F \hookrightarrow A$ whose image lies in the center of A.

An algebra A over F is *central* if A has center F and A is *simple* if A has no nontrivial two-sided ideal [33, §1, p. 3]. A *quaternion algebra* A over F is a central simple algebra of dimension 4 over F. Quaternion algebras can also be characterized in one of three other ways, as indicated by the following proposition.

Proposition 4.1.1. *Let A be a central F-algebra. Then the following are equivalent:*

(i) *A is simple and* $\dim_F(A) = 4$.

(ii) *There exist $\alpha, \beta \in A$ which generate A as an F-algebra such that*

$$\alpha^2 = a, \quad \beta^2 = b, \quad \alpha\beta = -\beta\alpha$$

for some $a, b \in F^*$.

(iii) *There exists a separable F-algebra K of dimension 2, an embedding $K \hookrightarrow A$, and elements $b \in F^*$ and $\beta \in A$, such that $A = K + K\beta$ and $\beta^2 = b$, satisfying*

$$\beta\alpha = \overline{\alpha}\beta$$

for all $\alpha \in K$, where $\overline{}$ is the nontrivial F-automorphism of K.

(iv) *$A \neq F$ is simple and finite-dimensional, and there exists an F-linear involution $\overline{}$ of A such that*

$$\alpha + \overline{\alpha},\ \alpha\overline{\alpha} \in F$$

for all $\alpha \in A$.

Proof. For the equivalence (i) ⇔ (ii) ⇔ (iv), see [34, Theorems III.5.1–2]. For the equivalence (i) ⇔ (iii), see [59, §I.1, p. 1]. □

The algebra described in (ii) is denoted $\left(\dfrac{a,b}{F}\right)$; the algebra in (iii) is denoted $\left(\dfrac{K,b}{F}\right)$. An *involution* $\iota : A \to A$ is a F-linear map satisfying $\iota(\alpha\beta) = \iota(\beta)\iota(\alpha)$ for all $\alpha, \beta \in A$ and such that $\iota^2 = \mathrm{id}|_A$.

Example 4.1.2. The $\mathbb{R}$-algebra $\left(\dfrac{-1,-1}{\mathbb{R}}\right)$ is the usual division ring of quaternions over the reals, which we denote by $\mathbb{H}$.

Example 4.1.3. The ring $M_2(F) \cong \left(\dfrac{-1,1}{F}\right)$ of 2×2-matrices with coefficients in F is a quaternion algebra over F. Indeed, if $b \in F^{*2}$, then $\left(\dfrac{a,b}{F}\right) \cong M_2(F)$, an isomorphism explicitly given by

$$\alpha \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}$$

for a choice of $\sqrt{b} \in F^*$. In particular, every quaternion algebra over $\overline{F}$ is isomorphic to $M_2(\overline{F})$.

Remark 4.1.4. Note that the values a, b and K, b are not uniquely determined by A: for example, we see that

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right) \cong \left(\frac{a,-ab}{F}\right) \cong \left(\frac{au^2,b}{F}\right)$$

for any $u \in F^*$.

Remark 4.1.5. The equivalence (i) $\Leftrightarrow$ (iii) is valid in any characteristic [59, §I.1, p. 1]. We will content ourselves with the case when $\operatorname{char} F \neq 2$.

The nontrivial K-automorphism in Proposition 4.1.1(iii) extends to an involution of A by defining $\overline{\beta} = -\beta$, which is an involution as in (iv). Similarly, given a quaternion algebra $A = \left(\dfrac{a,b}{F}\right)$ and an element $\theta = x + y\alpha + z\beta + w\alpha\beta \in A$, we have an involution defined by

$$\overline{\theta} = x - (y\alpha + z\beta + w\alpha\beta).$$

In fact, any such involution $\overline{}$ of A is unique, since for all $\alpha \in A$ with $\alpha \notin F$, the map $\overline{}$ must restrict to the nontrivial F-automorphism of $F(\alpha)$; in particular, $\alpha = \overline{\alpha}$ if and only if $\alpha \in F$. This involution of A is called *conjugation.*

For the rest of this section, A will denote a quaternion algebra over F. Let $\alpha \in A$. The *reduced trace* and *reduced norm* of α are defined to be respectively

$$\begin{aligned} \operatorname{trd} : A &\to F & \qquad \operatorname{nrd} : A &\to F \\ \alpha &\mapsto \alpha + \overline{\alpha} & \alpha &\mapsto \alpha\overline{\alpha}. \end{aligned}$$

We will also refer to these maps simply as the *trace* and *norm* whenever it will not cause confusion.

One immediately verifies the following lemma.

Lemma 4.1.6. *For all $\alpha, \beta \in A$ we have*

$$\operatorname{trd}(\alpha + \beta) = \operatorname{trd}(\alpha) + \operatorname{trd}(\beta), \quad \operatorname{nrd}(\alpha\beta) = \operatorname{nrd}(\alpha) \operatorname{nrd}(\beta).$$

The element $\alpha \in A$ is invertible if and only if $\operatorname{nrd}(\alpha) \neq 0$. *Every element $\alpha \in A$ satisfies the quadratic equation*

$$\alpha^2 - \operatorname{trd}(\alpha)\alpha + \operatorname{nrd}(\alpha) = 0$$

over F. The form

$$\begin{aligned} \langle\, , \,\rangle : A \times A &\to F \\ (\alpha, \beta) &\mapsto \operatorname{trd}(\alpha\beta) \end{aligned}$$

is symmetric, bilinear, and nondegenerate. The function $\alpha \mapsto \operatorname{nrd}(\alpha)$ is a quadratic form over F.

Example 4.1.7. For $A = \left(\dfrac{a, b}{F}\right)$ and $\theta = x + y\alpha + z\beta + w\alpha\beta$, we have $\operatorname{trd}(\theta) = 2x$ and $\operatorname{nrd}(\theta) = x^2 - ay^2 - bz^2 + abw^2$.

For $A = M_2(F)$, the reduced trace and reduced norm are the trace and determinant.

For $\alpha \in A$, let $\operatorname{Tr}_{A/F}(\alpha)$ and $\operatorname{N}_{A/F}(\alpha)$ denote the trace and norm of left multiplication by α as an F-endomorphism. Since conjugation in A is unique, it follows that if one chooses an embedding $\phi : A \hookrightarrow M_2(\overline{F})$ of F-algebras (such as in 4.1.3), then

$$\operatorname{trd}(\alpha) = \operatorname{tr}(\phi(\alpha)), \quad \operatorname{nrd}(\alpha) = \det(\phi(\alpha)).$$

Since the characteristic polynomial of left multiplication by a 2 × 2-matrix on $M_2(F)$ is the square of its characteristic polynomial, we recover from the relevant terms of these polynomials the following lemma.

Lemma 4.1.8. *We have*

$$\operatorname{Tr}_{A/F}(\alpha) = 2\operatorname{trd}(\alpha), \quad N_{A/F}(\alpha) = \operatorname{nrd}(\alpha)^2.$$

We now give a criterion to determine if A is isomorphic to a matrix ring.

Lemma 4.1.9 ([59, Corollaire 2.4])**.** *A quaternion algebra $A = \left(\dfrac{a,b}{F}\right)$ has $A \cong M_2(F)$ if and only if A is not a division ring, which holds if and only if $b \in N_{K/F}(K^*)$.*

Proof. Our statement differs only in that if K is not a field, then the norm map $N_{K/F}$ is surjective. □

Let $K \supset F$ be a field containing F. Then $A_K = A \otimes_F K$ is a central simple K-algebra of dimension 4, hence a quaternion algebra over K by (4.1.1); indeed, we have

$$\left(\frac{a,b}{F}\right) \otimes_F K \cong \left(\frac{a,b}{K}\right).$$

We say K is a *splitting field* for A if $A_K \cong M_2(K)$.

For the rest of this section, F will denote a number field with ring of integers $\mathbb{Z}_F$. Let v be a place of F, and let F_v denote the completion of F at v. We say A is *unramified* at v if $A_v = A \otimes_F F_v \cong M_2(F_v)$; otherwise, A is *ramified* at v.

Note by Example 4.1.3 that a quaternion algebra is always unramified at a complex place.

Lemma 4.1.10 ([59, Theorèmes II.1.1, II.1.3])**.** *Let v be a noncomplex place of F. Then up to isomorphism there is a unique quaternion algebra A_v over F_v which is a division ring.*

Suppose v is a finite place, and let K_w denote the unramified quadratic extension of F_v and let π denote a uniformizer of F_v. Then $A_v \cong \left(\dfrac{K_w, \pi}{F_v}\right)$ is a division ring.

A place v of F is *odd* if v finite and F_v has residue field of odd characteristic, or v is real. For an odd place v and $a \in F_v^*$, we define the symbol

$$\left\{\frac{a}{v}\right\} = \begin{cases} 1, & \text{if } a \in F_v^{*2}; \\ -1, & \text{if } a \notin F_v^{*2} \text{ and } F_v(\sqrt{a})/F_v \text{ is unramified;} \\ 0, & \text{if } a \notin F_v^{*2} \text{ and } F_v(\sqrt{a})/F_v \text{ is ramified.} \end{cases}$$

Note that if $\operatorname{ord}_v(a) = 0$, then $\left\{\dfrac{a}{v}\right\} = \left(\dfrac{a}{v}\right)$, and if v is real, then $\left\{\dfrac{a}{v}\right\} = \operatorname{sgn}(v(a))$.

Proposition 4.1.11. *Let v be an odd place of F, let $a, b \in F_v$, and let $A = \left(\dfrac{a, b}{F_v}\right)$. Then $A \cong M_2(F_v)$ if and only if either $\left\{\dfrac{ab}{v}\right\} \neq 0$ or one of the equalities*

$$\left\{\frac{a}{v}\right\} = 1, \quad \left\{\frac{b}{v}\right\} = 1, \quad \left\{\frac{-ab}{v}\right\} = 1$$

holds.

Proof. Let $K_w = F_v(\sqrt{a})$. First suppose $(ab/v) \neq 0$. If $(a/v) = 1$, then K_w is not a field hence by Lemma 4.1.9, we have $A \cong M_2(F_v)$. Otherwise, $(a/v) = -1$, so K_w is the unique unramified quadratic extension of F_v (if v is real, then $K_w = \mathbb{C}$); but since $N_{K_w/F_v}(K_w^*) = F_v^*$ by [42, Corollary V.1.2] or [20, Proposition 7.3], this implies that $b \in N_{K_w/F_v}(K_v^*)$, so by Lemma 4.1.9 we have $A \cong M_2(F_v)$ again.

Next, suppose $\left\{\dfrac{ab}{v}\right\} = 0$, so then without loss of generality we may assume $\left\{\dfrac{a}{v}\right\} = 0$. Since v is odd and $A \cong \left(\dfrac{a, -ab}{F_v}\right)$, we may assume $\left\{\dfrac{b}{v}\right\} \neq 0$. Now K_w is a totally tamely ramified extension of F_v, so $b \in N_{K_v/F_v}(K_v^*)$ if and only if $\left\{\dfrac{b}{v}\right\} = 1$ (see [20, Proposition 8.2], and the discussion preceding it), which is the result. □

Quaternion algebras over number fields can be classified using results of class field theory as follows.

Proposition 4.1.12. *The number of places where A is ramified is finite and even. Given an even number of noncomplex places S of F, there exists a quaternion algebra over F, unique up to isomorphism, that ramifies exactly at the places in S.*

Proof. See [59, §III.3.1]. □

The *discriminant* of A is the cycle (see [35, VI.1]) of $\mathbb{Z}_F$ equal to the product of places of F where A is ramified. Note by Proposition 4.1.12 that the matrix ring $M_2(F)$ is the unique quaternion algebra over F which is unramified at all places of F, i.e. it is the only quaternion algebra of discriminant (1).

Proposition 4.1.13. *Let $K \supset F$ be a quadratic field extension. The following conditions are equivalent:*

(i) *K is a splitting field for A;*

(ii) *There exists an F-embedding $K \hookrightarrow A$;*

(iii) *There exists an element $\alpha \in A$ such that $F[\alpha] \cong K$;*

(iv) *For all places v of F and all places $w \mid v$ of K, the field K_w is a splitting field for A_v;*

(v) *For all places v of F which are ramified in A, we have that v does not split completely in K.*

Proof. For the equivalence (i) ⇔ (ii), see [59, §I.2] or [63, §§IX.1–2]. For (i) ⇔ (iv), see [59, Corollary III.3.5]; the statement (iv) ⇔ (v) follows from [59, Theorem III.3.8]. □

Now let F be a totally real number field of degree $[F : \mathbb{Q}] = g$. For each real place v of F, by Proposition 4.1.12 we have either $A_v \cong M_2(\mathbb{R})$ or $A_v \cong \mathbb{H}$; therefore we have an isomorphism

$$A \otimes_F \mathbb{R} \cong \prod_v A \otimes_F F_v \cong M_2(\mathbb{R})^r \times \mathbb{H}^{g-r}$$

for some $0 \leq r \leq g$. If $r = 0$, then A is said to be *definite*; otherwise, A is *indefinite*.

Example 4.1.14. Let F be a totally real number field, let $\sigma : F \hookrightarrow \mathbb{R}$, and let $A = \left(\dfrac{a,b}{F}\right)$ with $\sigma(b) > 0$. Then A is indefinite, and σ realizes $\mathbb{R}$ as a splitting field for A, as then $\sigma(b) \in \mathbb{R}^{*2}$; an explicit embedding is given by Example 4.1.3.

4.2 Fundamental algorithms for quaternion algebras

In this section, we will describe basic algorithms for computing with quaternion algebras. Throughout, A will denote a quaternion algebra over F.

An algorithm is *probabilistic* if it may call upon a generator which produces a sequence of independent, random bits; otherwise if an algorithm may not call such a generator we say it is *deterministic*. An algorithm is *polynomial time* if the number of bit operations it performs (on average over the possible outputs of the random bit generator, if the algorithm is probabilistic) is bounded by a polynomial in the number of bits of the input, known as the *size*. (See e.g. [21, §25.8] for further discussion.) A problem X is *polynomial time reducible* to a problem Y if there exists an algorithm (we will specify if it is deterministic or probabilistic) which takes an algorithm to solve problem Y and gives a solution to problem X; two problems are *polynomial time equivalent* if each is polynomial time reducible to the other. Whenever we say that there exists an algorithm, we mean that we can explicitly exhibit such an algorithm. Also, we will pay no mind to "error checking" in our algorithms—we only provide that the algorithm will run and yield correct output as announced in the algorithm if it is given valid input. For the rest of this section, we assume that we fix the ground field F and a way of encoding elements of the field F in bits, subject to the condition that the field operations in F and linear algebra over F can be performed in deterministic polynomial time. For example, we may represent rational numbers as pairs of integers in the usual way, with integer arithmetic as in [36].

Already from Proposition 4.1.1 we see that there are several ways to describe the quaternion algebra A. We say that A is given in *standard representation* by $a, b \in F^*$ if $A \cong \left(\dfrac{a,b}{F}\right)$, i.e. the quaternion algebra is specified by two nonzero elements of F. If α, β are as in Proposition 4.1.1(ii), then the elements $1, \alpha, \beta, \alpha\beta$ are an orthogonal basis for A with respect to the inner product given by the reduced trace pairing (4.1.6), and an element of A is given by its coefficients in this basis. By Example 4.1.7, we may compute the conjugation involution on A and hence the reduced trace and norm.

A *multiplication table* for A is a system of $4^3 = 64$ elements $(c_{ijk})_{i,j,k}$ of F, called *structure constants*, such that A is isomorphic to the F-algebra in the basis $e_1 = 1, e_2, e_3, e_4$ with ordinary addition and scalar multiplication by F, and multiplication given by

$$e_i e_j = \sum_{k=1}^{4} c_{ijk} e_k$$

for $i, j \in \{1, 2, 3, 4\}$. Notice that we require that the element 1 be given as part of the input basis, since we require by definition that any F-algebra be equipped with an embedding $F \hookrightarrow A$. (This is not a serious restriction, for the equations which uniquely define the element 1 in A are linear equations.)

Given a standard representation for A, we can compute directly a multiplication table for A in the basis $1, \alpha, \beta, \alpha\beta$. There also exists a deterministic polynomial time algorithm to go in the other direction—see Algorithm 4.2.9 below.

We already saw in the previous section that determining whether a quaternion algebra is isomorphic to the matrix ring is a fundamental question of interest.

Problem 4.2.1. *Given a quaternion algebra A over F, determine if $A \cong M_2(F)$.*

We may also ask for a solution to the more difficult problem of constructing an explicit isomorphism.

Problem 4.2.2. *Given a quaternion algebra A over F, determine if $A \cong M_2(F)$ and, if so, exhibit such an isomorphism.*

Remark 4.2.3. It may also be interesting to study the corresponding problem where $M_2(F)$ is replaced by another quaternion algebra A'.

An isomorphism $A \cong M_2(F)$ is given by a set of elements $e_{11}, e_{12}, e_{21}, e_{22} \in A$ satisfying the equations of the matrix units

$$e_{ij}e_{kl} = \begin{cases} e_{il}, & \text{if } j = k, \\ 0, & \text{otherwise;} \end{cases}$$

the map which sends e_{ij} to the matrix which has a 1 in the ijth entry and is zero elsewhere yields an F-algebra isomorphism $A \xrightarrow{\sim} M_2(F)$. (Note that $1 = e_{11} + e_{22} \in A$.) These elements are specified by the columns of an invertible 4×4-matrix with coefficients in F in the given basis for A.

To study Problems 4.2.1 and 4.2.2, let

$$A^0 = \{\alpha \in A : \operatorname{trd}(\alpha) = 0\}$$

be the set of trace zero elements of A. We see that $\dim_F A^0 = 3$, so choosing a basis for A^0 we may identify A^0/F^* with the points of the projective plane $\mathbb{P}^2(F)$ over F. Let Q denote the quadratic form given by the reduced norm $\operatorname{nrd} : A \to F$ restricted to A^0; then $Q = 0$ yields a *conic* $C \subset \mathbb{P}^2$ defined over F, by which we mean a nonsingular projective plane curve of degree 2.

Proposition 4.2.4. *Let A be a quaternion algebra over F. Then the following are equivalent:*

(i) *$A \cong M_2(F)$.*

(ii) *A has a nontrivial left (or right) ideal $0 \subsetneq I \subsetneq A$.*

(iii) *There exists a nonzero $\alpha \in A$ such that* $\operatorname{trd}(\alpha) = \operatorname{nrd}(\alpha) = 0$.

(iv) *The quadratic form Q represents zero over F.*

(v) *The conic C has an F-rational point.*

Proof. The only nontrivial statement is (ii) ⇒ (i), which follows from the Wedderburn-Artin Theorem [33, 3.5]. □

Therefore we are led to the following problems.

Problem 4.2.5. *Given a conic C defined over a field F, determine if C has an F-rational point.*

Problem 4.2.6. *Given a conic C defined over a field F, determine if C has an F-rational point and, if so, output an F-rational point.*

Proposition 4.2.4 shows that Problem 4.2.1 is equivalent to Problem 4.2.5. To relate this to the second problem, we must be more explicit in the identifications in Proposition 4.2.4. A zerodivisor in A (by which we always mean a nonzero zerodivisor) generates a nontrivial left ideal I, which must be of dimension 2 over F; choosing an F-basis for I, the map $A \to M_2(F)$ which sends $\alpha \in A$ to left multiplication by α on I is in fact an isomorphism. This gives rise to the following algorithm (claimed but not exhibited explicitly in [47]; see also [49, §5.1]).

Algorithm 4.2.7. Let A be a quaternion algebra over F, given by a multiplication table. Let $\alpha \in A$ be a zerodivisor. This algorithm outputs an invertible 4×4-matrix T whose columns define an isomorphism $A \xrightarrow{\sim} M_2(F)$, each row being a matrix unit.

1. [Compute generators for $A\alpha$] Compute $e_1\alpha, \dots, e_4\alpha$, and let f_1, f_2 be a maximal linearly independent subset. Write

$$f_j = \sum_{k=1}^{4} b_{jk} e_k$$

for $j = 1, 2$.

2. [Solve for matrix units] For $i = 1, \dots, 4$ and $j = 1, 2$, compute

$$e_i f_j = \sum_{k=1}^{4} a_{ijk} e_k.$$

Row reduce the augmented matrix

$$\left(\begin{array}{ccc|cccc} a_{111} & \cdots & a_{411} & b_{11} & 0 & 0 & b_{21} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{114} & \cdots & a_{414} & b_{14} & 0 & 0 & b_{24} \\ a_{121} & \cdots & a_{421} & 0 & b_{21} & b_{11} & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{124} & \cdots & a_{424} & 0 & b_{24} & b_{14} & 0 \end{array}\right).$$

Output the 4×4-matrix given by the first four rows and last four columns of this row-reduced matrix.

Proof. In Step 1, we compute a basis for the left ideal generated by α, which is a minimal (nonzero) left ideal of A and hence of dimension 2 over F. It is easy to see that the matrix units are uniquely determined by the equations in Step 2; for example, the matrix unit $e_{11} = x_{111}e_1 + \cdots + x_{114}e_4$ is the solution to the equations

$$e_{11}f_1 = f_1, \quad e_{11}f_2 = 0,$$

which in the basis e_i is given by the (redundant) eight equations defined by the first five columns in Step 2. □

The above computation only requires the solution of a system of linear equations over F, and therefore will run in deterministic polynomial time. The equivalence (4.2.4) together with Algorithm 4.2.7 proves the following.

Lemma 4.2.8. *Problem* 4.2.2 *is deterministic polynomial time equivalent to Problem* 4.2.6.

We now give a brief indication of the difficulty of Problems 4.2.5 and 4.2.6 for various fields. For a finite field $\mathbb{F}_q$, Problem 4.2.5 is trivial, since every conic over a finite field has a point—one can prove this directly or appeal to the Weil conjectures (see e.g. [25, Appendix C]). To exhibit a point, there exists a deterministic polynomial time algorithm which finds a point on a conic over a finite field with characteristic $\neq 2$, as well as probabilistic polynomial time algorithms which rely upon root extraction [65].

In a local field, we represent elements to a fixed precision (which is specified as part of the input). Then by Hensel's lemma, if a conic has good reduction over a nonarchimedean local field, then the preceding paragraph immediately implies a solution for each of these problems (the second only if the residue field is not of characteristic 2), at least to the fixed precision. If the conic does not have good reduction, then Problem 4.2.5 is equivalent to the easy problem of determining if a nonzero element is a square in a finite field, and it is easy to see that Problem 4.2.6 is equivalent (again in characteristic not 2) to the problem of finding a square root of a nonzero element in a finite field. A conic over $\mathbb{R}$ has a point if and only if the corresponding quadratic form is indefinite, which can be tested in deterministic polynomial time by checking if corresponding symmetric matrix has a nonpositive eigenvalue.

By the Hasse-Minkowski theorem, the question of whether a conic over a number field F has a rational point is determined by local conditions (see [59, Corollary III.3.2] or [6, Exercise 4]). Without loss of generality, we may assume that the conic has the form $ax^2 + by^2 + cz^2 = 0$, for $a, b, c \in \mathbb{Z}_F$ integral; then only primes which divide $2abc$ together with real places have a nontrivial condition. Over $\mathbb{Q}$, one can give a certificate (consisting of a set of rational primes and local data at each such prime) which verifies the existence of a rational point if it exists, and there are efficient algorithms [12, 53] which, given a factorization of the discriminant, first find a rational point on the conic and then attempt to find another rational point with smaller height.

Over more general fields, we notice that the literature is much less complete, and we are not presently able to do better than assisted enumeration; see Algorithm 4.4.10 below.

We conclude this section with the promised algorithm to represent a quaternion algebra in standard representation. The algorithm uses Gram-Schmidt orthogonalization to find an orthogonal basis for A with respect to pairing given by the reduced trace (4.1.6).

Algorithm 4.2.9. Let $(c_{ijk})_{i,j,k}$ be a multiplication table for A. This algorithm outputs a standard representation a, b for A, and a matrix T which either gives an isomorphism $A \cong M_2(F)$ or gives a change of basis to the standard basis for $\left(\dfrac{a,b}{F}\right)$.

1. [Compute traces] Let

$$\langle\ ,\ \rangle : F^4 \times F^4 \to F$$
$$\langle x, y\rangle = \mathrm{Tr}_{A/F}(xy)$$

   be the algebra trace form, represented by the 4×4-symmetric matrix with ijth entry equal to

$$\sum_{k,l=1}^{4} c_{ijk} c_{kll}.$$

   Let T be the 4×4 identity matrix; let $B_0 = 4$, and $i = 1$.

2. [Orthogonalize] Initialize $e_i^* = e_i$. For $j = 0, \ldots, i-1$, compute

$$\mu_{ij} = \frac{\langle e_i, e_j^*\rangle}{B_j},$$

   subtract μ_{ij} from the ijth entry of T, and subtract $\mu_{ij} e_j^*$ from e_i^*.

3. [Check for zerodivisor] Let $B_i = \langle e_i^*, e_i^*\rangle$. If $B_i = 0$, call Algorithm 4.2.7 with the zerodivisor e_i^*, output $a = -1, b = 1$ and the matrix whose columns are the outputed matrix units $e_{11}, \ldots, e_{22}$ written in the basis $e_1, \ldots, e_4$, and terminate the algorithm. If $i < 3$, increment i and return to Step 2; if $i = 3$, set the last column of T to the coefficients of $e_1^* e_2^*$ in the basis $e_1, \ldots, e_4$, and return $a = (e_1^*)^2$, $b = (e_2^*)^2$, and the matrix T.

Remark 4.2.10. Note that if only the values a, b are desired, then one can abort the procedure at $i = 3$.

Remark 4.2.11. Rónyai [47, Theorem 2.1] gives an algorithm to solve the above problem over $\mathbb{Q}$, but this algorithm tests a polynomial of degree 2 over $\mathbb{Q}$ for irreducibility; the above algorithm requires no such test.

We now prove that this algorithm terminates and gives the correct output.

Proof. We have by Lemma 4.1.8 that $2\operatorname{trd}(\alpha) = \operatorname{Tr}(A \xrightarrow{\alpha\cdot} A)$ for any $\alpha \in A$. Since

$$(e_i e_j)e_l = \left(\sum_k c_{ijk} e_k\right) e_l = \sum_k c_{ijk} \left(\sum_m c_{klm} e_m\right) = \sum_m \sum_k c_{ijk} c_{klm} e_m,$$

we know that the trace of the endomorphism given by right multiplication by $e_i e_j$ is

$$\sum_l \sum_k c_{ijk} c_{kll}$$

as in Step 1.

In Step 2, we compute the usual Gram-Schmidt orthogonalization of a basis: the elements $e_1^* = \alpha$ and $e_2^* = \beta$ satisfy $\operatorname{trd}(\alpha) = \operatorname{trd}(\beta) = \operatorname{trd}(\alpha\beta) = 0$. Therefore $\alpha^2 = a$ and $\beta^2 = b$ for some $a, b \in F$. If $a = 0$ or $b = 0$, then the algorithm has correctly found a zerodivisor; otherwise, we have $a, b \in F^*$. Now write

$$\beta\alpha = x + y\alpha + z\beta + w\alpha\beta$$

with $x, y, z, w \in F$. We find $\operatorname{trd}(\beta\alpha) = \operatorname{trd}(\alpha\beta) = 2x = 0$, so $x = 0$, and from $\operatorname{trd}(\beta\alpha^2) = a\operatorname{trd}(\beta) = 0 = ay$, we have $y = 0$ and similarly $z = 0$. Finally,

$$ab = \operatorname{nrd}(\alpha\beta) = \operatorname{nrd}(\beta\alpha) = \operatorname{nrd}(w\alpha\beta) = w^2 \operatorname{nrd}(\alpha\beta)$$

so $w^2 = 1$. If $w = 1$, then A is a commutative F-algebra, a contradiction. Therefore $w = -1$, and $\beta\alpha = -\alpha\beta$ as desired. □

Remark 4.2.12. The proof of this proposition also yields: any two elements $\alpha, \beta \in A$ such that $\operatorname{trd}(\alpha) = \operatorname{trd}(\beta) = \operatorname{trd}(\alpha\beta) = 0$ skew-commute, so that $\beta\alpha = -\alpha\beta$.

Again since only linear algebra is required, the above algorithm runs in deterministic polynomial time. From now on, unless specified otherwise we will assume that A is given in standard representation.

4.3 Computing a maximal order

In this section, let F be a number field with $g = [F : \mathbb{Q}]$, and let A be a quaternion algebra over F. We refer to [59, §I.4] and the treatise [45] for the background relevant to this section.

We first reference the existing algorithms for the ground field F; see [9, 10, 43]. A number field $F = \mathbb{Q}(b)$ is given by the data of the minimal polynomial of b (itself described by the sequence of its coefficients, given as rational numbers). Elements of F are described by their standard representation in the basis of powers of b as in [9, §4.2.2]; the size of an element of F is thus the number of bits required for this representation. If not specified, the norm $N = N_{F/\mathbb{Q}} : F \to \mathbb{Q}$ is the absolute norm.

The ring of integers of F is denoted $\mathbb{Z}_F$. Given F, there exist algorithms to compute $\mathbb{Z}_F$ (see e.g. [9, §6.1]). It is known that finding $\mathbb{Z}_F$ is deterministic polynomial time equivalent to the problem of finding the largest squarefree divisor of a positive integer [7, 36], for which no polynomial time algorithm is known. (See [5] for a way of "approximating" $\mathbb{Z}_F$.) We remark that in practice these algorithms perform well for number fields F with "reasonably small" degree and discriminant.

Now we define the corresponding objects for quaternion algebras. A $\mathbb{Z}_F$-*lattice* of A is a finitely generated $\mathbb{Z}_F$-submodule I of A satisfying the property that $FI = A$. An *order* of A is a

$\mathbb{Z}_F$-lattice which is also a subring of A. A *maximal order* of A is an order which is not properly contained in any other order. An element $\alpha \in A$ is *integral* if $\mathbb{Z}_F[\alpha]$ is a finite $\mathbb{Z}_F$-module, or equivalently if we have

$$\operatorname{trd}(\alpha), \operatorname{nrd}(\alpha) \in \mathbb{Z}_F.$$

The sum or product of two integral elements is not necessarily integral, and as a result maximal orders are not unique, unlike the case for number fields. Given a $\mathbb{Z}_F$-lattice I of A, we define the *(left-)multiplier order* to be

$$\mathcal{O}(I) = \{\alpha \in A : \alpha I \subset I\}.$$

This is an order by [45, p. 109].

The *discriminant* of an order Λ is the ideal $\mathfrak{d}(\Lambda) \subset \mathbb{Z}_F$ generated by the set

$$\{\det(\operatorname{trd}(x_i x_j))_{i,j=1}^4 : x_1, \dots, x_4 \in \Lambda\}.$$

Lemma 4.3.1. *Let $\mathfrak{d}(A)$ be the finite part of the discriminant of A. If Λ is an order of A, then Λ is maximal if and only if $\mathfrak{d}(\Lambda) = \mathfrak{d}(A)^2$.*

Proof. Recall from §4.1 that the finite part of the discriminant of A is the ideal of $\mathbb{Z}_F$ obtained as the product of all prime $\mathfrak{p}$ where A is ramified. First, note that $\Lambda \subset \Lambda'$, then $\Lambda = \Lambda'$ if and only if $\mathfrak{d}(\Lambda) = \mathfrak{d}(\Lambda')$ (see e.g. [45, Exercise 10.3]). But the order Λ is maximal if and only if $\Lambda_{\mathfrak{p}} = \Lambda \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$ is maximal for every prime $\mathfrak{p}$ of F (see [45, 11.2]), where $\mathbb{Z}_{F,\mathfrak{p}}$ is the localization of $\mathbb{Z}_F$ at $\mathfrak{p}$. The result now follows since $\mathfrak{d}(\Lambda) = \bigcap_{\mathfrak{p}} \mathfrak{d}(\Lambda_{\mathfrak{p}})$ and $\mathfrak{d}(\Lambda_{\mathfrak{p}}) = \mathfrak{p}^2$ if $\Lambda_{\mathfrak{p}}$ is a division ring by [45, Theorem 14.9] and otherwise $\mathfrak{d}(\Lambda_{\mathfrak{p}}) = (1)$. □

We will be interested in the following algorithmic problems.

Problem 4.3.2. *Find a maximal order $\mathcal{O} \subset A$.*

Problem 4.3.3. *Given an order $\Lambda \subset A$, find a maximal order $\mathcal{O} \supset \Lambda$.*

One way to specify an ideal or order Λ is by a set of generators over $\mathbb{Z}_F$; if F does not have class number 1, however, we cannot expect that Λ is a free $\mathbb{Z}_F$-module and hence there may not exist a $\mathbb{Z}_F$-basis (see [10, §1] for computational issues surrounding finitely generated modules over Dedekind domains), and this will prove computationally very inconvenient. However, there exists a $\mathbb{Z}$-basis for Λ (of cardinality $4[F : \mathbb{Q}]$), and from now on, we assume that a $\mathbb{Z}_F$-lattice is specified by a $\mathbb{Z}$-basis. Note that if Λ is an order, then since $\mathbb{Z}_F \subset \Lambda$, if one has such a basis for Λ then by linear algebra (see e.g. [9, §2.4.3]) one may compute in deterministic polynomial time a $\mathbb{Z}$-basis for $\mathbb{Z}_F$ by computing $\Lambda \cap F = \mathbb{Z}_F$.

By the above, we know already that computing a maximal order of F is algorithmically as complex as computing the largest squarefree divisor of a positive integer; therefore, we expect that the problem for a quaternion algebra A is no less complicated.

Proposition 4.3.4 ([24, Theorem 5.3]). *There exists an algorithm to solve Problem* 4.3.3 *for an arbitrary quaternion algebra A over an arbitrary number field F which runs in deterministic polynomial time if it is allowed to call oracles for the problems of factoring integers and polynomials over finite fields.*

At present, it is not known if there exist deterministic polynomial time algorithms to solve either of these problems.

The result of [24] holds more generally for semisimple algebras over $\mathbb{Q}$. For quaternion algebras, we can give a simpler and very practical algorithm. We will first need three subalgorithms.

Algorithm 4.3.5. Let Λ be an order in a quaternion algebra A, given by a $\mathbb{Z}$-basis as above. Let $\mathfrak{p} \subset \mathbb{Z}_F$ be a prime ideal and let $e \in \mathbb{Z}_{>0}$. Let $\overline{I}$ be an ideal of the finite ring $\overline{\Lambda} = \Lambda/\mathfrak{p}^e\Lambda$, represented by a $\mathbb{Z}_F/\mathfrak{p}$-basis. This algorithm computes the inverse image I of the ideal $\overline{I}$ under the projection $\Lambda \to \overline{\Lambda}$.

1. [Compute a basis for $\mathfrak{p}$] From a set of generators for $\mathfrak{p}$ and a $\mathbb{Z}$-basis for $\mathbb{Z}_F$, use linear algebra to compute a $\mathbb{Z}$-basis for $\mathfrak{p}^e$.

2. [Lift] Let I' be the set consisting of lifts for each of the elements in a basis for $\overline{I}$ to an element of Λ. For each element λ in the $\mathbb{Z}$-basis for Λ and for each element π in the $\mathbb{Z}$-basis for $\mathfrak{p}^e$, append the element $\pi\lambda$ to I'. Return a $\mathbb{Z}$-basis for I'.

We will also need the following algorithm, as in [48, Theorem 3.2].

Algorithm 4.3.6. Let Λ be an order in a quaternion algebra A given by a $\mathbb{Z}$-basis, and let I be a $\mathbb{Z}_F$-lattice in A. This algorithm computes the multiplier order $\mathcal{O}(I)$.

1. [Compute s] By linear algebra over $\mathbb{Z}$, compute a generator $s \in I \cap \mathbb{Z}$.

2. [Solve] Again by linear algebra over $\mathbb{Z}$, compute

$$\mathcal{O}(I) = \{\alpha \in s^{-1}I : \alpha I \subset I\}.$$

Return a $\mathbb{Z}$-basis for $\mathcal{O}(I)$.

Last, we will use an algorithm which works over an even $\mathfrak{p}$-adic field.

Algorithm 4.3.7. Let F be a number field, let $\mathfrak{p}$ an even prime with ramification index e, and let $a, b \in \mathbb{Z}_F$ be such that $a \not\equiv 0 \pmod{\mathfrak{p}}$. This algorithm outputs a solution to the congruence

$$x^2 - ay^2 - bz^2 + abw^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

with $x, y, z, w \in \mathbb{Z}_F/\mathfrak{p}^{2e}\mathbb{Z}_F$ and such that $x \equiv 1 \pmod{\mathfrak{p}^{2e}}$.

1. [Initialize] Let $f \in \mathbb{Z}_{\geq 1}$ be the residue class degree of $\mathfrak{p}$ so that $\#(\mathbb{Z}_F/\mathfrak{p}) = 2^f$ and let $q = 2^f$.

2. [Compute kernel] Compute a basis for the kernel of the $\mathbb{Z}_F/\mathfrak{p}$-linear map

$$\begin{aligned}\Phi : (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^4 &\to \mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F \\ (x, y, z, w) &\mapsto x^q - ay^q - bz^q + abw^q.\end{aligned}$$

Let $(x_0, y_0, z_0, w_0) \in \ker \Phi$ be such that

$$x_0 \not\equiv 0 \pmod{\mathfrak{p}}$$

and

$$(x_0, y_0, z_0, w_0) \not\equiv (x_0, x_0, x_0, x_0) \pmod{\mathfrak{p}}.$$

Let $(x_1, y_1, z_1, w_1) \in \ker \Phi$ be such that

$$x_0 x_1 + (a y_0) y_1 + (b z_0) z_1 - (a b w_0) w_1 \not\equiv 0 \pmod{\mathfrak{p}}.$$

Compute

$$(x_0 + y_0\alpha + z_0\beta + w_0\alpha\beta)(x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta) = x + y\alpha + z\beta + w\alpha\beta$$

where $\alpha^2 = a$, $\beta^2 = b$, and $\beta\alpha = -\alpha\beta$. Return the solution $(1, y/x, z/x, w/x)$.

Proof. We prove the correctness of Step 2. Let $k_{\mathfrak{p}} = \mathbb{Z}_F/\mathfrak{p}$ be the residue field at $\mathfrak{p}$. For any $\overline{a} \in k_{\mathfrak{p}}$ and any lift $a \in \mathbb{Z}_{F,\mathfrak{p}}$ of $\overline{a}$, the sequence a^{q^n} converges to an element $\widetilde{a} \in \mathbb{Z}_{F,\mathfrak{p}}$ known as the Teichmüller representative; it is the unique element $\widetilde{a}$ satisfying $\widetilde{a} \equiv a \pmod{\mathfrak{p}}$ and $\widetilde{a}^q = \widetilde{a}$. The map

$$\begin{aligned} k_{\mathfrak{p}} &\to \mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F \\ a &\mapsto \widetilde{a} \bmod \mathfrak{p}^e \end{aligned}$$

in fact gives a splitting of the exact sequence

$$0 \to \mathfrak{p}/\mathfrak{p}^e\mathbb{Z}_F \to \mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F \to k_{\mathfrak{p}} \to 0$$

of $\mathbb{Z}_F$-modules, since

$$(\widetilde{a} + \widetilde{b})^q \equiv \widetilde{a}^q + \widetilde{b}^q \equiv \widetilde{a} + \widetilde{b} \pmod{\mathfrak{p}^e}.$$

Therefore we have an isomorphism

$$\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F \cong k_{\mathfrak{p}} \oplus \mathfrak{p}/\mathfrak{p}^e\mathbb{Z}_F.$$

Now the $k_{\mathfrak{p}}$-linear map

$$\Phi|_{\mathfrak{p}} : k_{\mathfrak{p}}^4 \to k_{\mathfrak{p}}$$

$$(x, y, z, w) \mapsto x^q - ay^q - bz^q + abw^q$$

is visibly surjective, so $\dim_{k_{\mathfrak{p}}} \ker \Phi|_{\mathfrak{p}} = 3$. Since $a \not\equiv 0 \pmod{\mathfrak{p}}$, we see that there is an element $(x_0, y_0, z_0, w_0) \in \ker \Phi|_{\mathfrak{p}}$ such that $x_0 \not\equiv 0 \pmod{\mathfrak{p}}$, and by the above splitting this gives rise to an element $(x_0, y_0, z_0, w_0) \in \ker \Phi$. Now if

$$x_0x_1 + (ay_0)y_1 + (bz_0)z_1 + (abw_0)w_1 \equiv 0 \pmod{\mathfrak{p}}$$

for all $(x_1, y_1, z_1, w_1) \in \ker \Phi|_{\mathfrak{p}}$, or equivalently

$$x_1 + (ay_0/x_0)y_1 + (bz_0/x_0)z_1 + (abw_0/x_0)w_1 \equiv 0 \pmod{\mathfrak{p}},$$

then since already

$$x_1^q + ay_1^q + bz_1^q + abw_1^q \equiv x_1 + ay_1 + bz_1 + abw_1 \equiv 0 \pmod{\mathfrak{p}}$$

by dimension considerations we must have

$$x_0 \equiv y_0 \equiv z_0 \equiv w_0 \pmod{\mathfrak{p}}$$

which is impossible. The result now follows from the multiplicativity of the norm, since

$$\operatorname{nrd}(x + y\alpha + z\beta + w\alpha\beta) = x^2 - ay^2 - bz^2 + abw^2.$$

□

We are now ready to present an algorithm to solve Problem 4.3.2.

Algorithm 4.3.8. Let A be a quaternion algebra over a number field F, specified in standard representation $A = \left(\dfrac{a, b}{F}\right)$. This algorithm computes a maximal order $\mathcal{O}$ for A, given by a free $\mathbb{Z}$-basis.

1. [Compute $\mathbb{Z}_F$] Compute a $\mathbb{Z}$-basis for $\mathbb{Z}_F$ by [10, Algorithm 2.4.9].

2. [Check for $M_2(F)$] If one of $a, b, -ab \in F^{*2}$ (which we can check in polynomial time by factoring, see [37]), call Algorithm 4.2.7 to find an isomorphism $A \xrightarrow{\sim} M_2(F)$. Return generators for the inverse image of $M_2(\mathbb{Z}_F)$ and terminate the algorithm.

3. [Compute an order] Scale a, b by an appropriate nonzero square so that $a, b \in \mathbb{Z}_F$. For each $\gamma \in \{\alpha, \beta, \alpha\beta\}$, let $K = F(\gamma)$, and compute a $\mathbb{Z}$-basis for the order O_K of K satisfying the properties that $O_{K,\mathfrak{p}}$ is maximal for all odd primes $\mathfrak{p}$ and $O_{K,\mathfrak{p}} = \mathbb{Z}_{F,\mathfrak{p}}[\gamma]$ for all primes $\mathfrak{p} \mid 2$. Let Λ be order of A generated by the orders O_K. Let
$$\mathfrak{d} = \prod_K \mathfrak{d}(O_K/\mathbb{Z}_F).$$
Using [10, Algorithm 2.3.22], factor the ideal $\mathfrak{d}$ into primes.

4. [Compute an odd maximal order] Loop over all odd primes $\mathfrak{p} \mid \mathfrak{d}$. Note that $\mathfrak{p}^2 \parallel \mathfrak{d}$, so suppose $\mathfrak{p} \nmid \mathfrak{d}(O_K)$ with $K = F(\alpha)$, and $\alpha^2 = a$ with $\mathfrak{p} \nmid a\mathbb{Z}_F$. If $(a/\mathfrak{p}) = -1$, then correctly conclude that A is ramified at $\mathfrak{p}$ and the order Λ is already maximal at $\mathfrak{p}$. Otherwise, if $(a/\mathfrak{p}) = 1$, solve
$$z^2 \equiv a \pmod{\mathfrak{p}}$$
for $z \in \mathbb{Z}_F$. Then $\alpha - z$ is a zerodivisor in A. Let $\Lambda/\mathfrak{p}\Lambda = \overline{\Lambda}$, and find a $\mathbb{Z}_F/\mathfrak{p}$-basis (consisting of 2 elements) for the $\overline{\Lambda}$ ideal $\overline{I}$ generated by $\alpha - z$. Lift this to an ideal I of Λ by Algorithm 4.3.5, and replace Λ with the multiplier order $\mathcal{O}(I)$, computed as in Algorithm 4.3.6.

5. [Compute a 2-maximal order] Loop over primes $\mathfrak{p} \mid 2$. Without loss of generality, we may assume that $\operatorname{ord}_{\mathfrak{p}} a$ is even. Then scaling α by an appropriate square we may assume $\operatorname{ord}_{\mathfrak{p}} a = 0$, and we adjoin this to the generating set for Λ. By calling Algorithm 4.3.7 and

applying the Chinese Remainder theorem, find $x, y, z, w \in \mathbb{Z}_F$ satisfying

$$x^2 - ay^2 - bz^2 + abw^2 \equiv 0 \pmod 4$$

and $x \equiv 1 \pmod 4$. Let

$$\gamma = \frac{x + y\alpha + z\beta + w\alpha\beta}{2}.$$

Let $e \in \mathbb{Z}_{>0}$ be the ramification index of $\mathfrak{p}$. If the minimal polynomial of γ has a root $z \in \mathbb{Z}_F/\mathfrak{p}^{2e+1}\mathbb{Z}_F$, let $\overline{I}$ be the ideal of $\Lambda/\mathfrak{p}^{2e+1}\Lambda = \overline{\Lambda}$ generated by $\gamma - z$, and compute I and replace $\Lambda = \mathcal{O}(I)$ as in Step 4. Otherwise, by linear algebra, find an element $\delta \in A$ with $\mathrm{trd}(\delta) = 0$ such that $\delta\gamma = -\gamma\delta$ and $\delta^2 = d \in \mathbb{Z}_F$ with $\mathrm{ord}_{\mathfrak{p}}(d) \in \{0, 1\}$. Adjoin the $\mathbb{Z}_F$-span of γ and δ to Λ.

Proof. After Step 2, we may assume each of the rings $F[\alpha], F[\beta], F[\alpha\beta]$ are in fact fields.

Next, we prove that the $\mathbb{Z}_F$-lattice in Step 3 is in fact an order; we need to show it is a ring. We will prove this locally. For each prime $\mathfrak{p}$ of $\mathbb{Z}_F$, we consider the completion $\Lambda_{\mathfrak{p}} = \Lambda \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$; then we have

$$\Lambda = A \cap \bigcap_{\mathfrak{p}} \Lambda_{\mathfrak{p}}$$

by [45, Theorem 5.3(i)]. Therefore Λ is a ring if and only if each $\Lambda_{\mathfrak{p}}$ is a ring, for then it is an intersection of rings. For an even prime $\mathfrak{p}$, the $\mathbb{Z}_F$-lattice $\Lambda_{\mathfrak{p}}$ is generated by $1, \alpha, \beta, \alpha\beta$ with $\alpha^2 = a$ and $\beta^2 = b$ with $a, b \in \mathbb{Z}_{F,\mathfrak{p}}$, and $\beta\alpha = -\alpha\beta$, so this is indeed a ring. Now let $\mathfrak{p}$ be an odd prime. Then the orders O_K for each of the fields

$$K = F_{\mathfrak{p}}(\sqrt{a}),\ F_{\mathfrak{p}}(\sqrt{b}),\ F_{\mathfrak{p}}(\sqrt{-ab}),$$

are generated over $\mathbb{Z}_{F,\mathfrak{p}}$ by an element of trace zero, and by anti-commutativity of such elements (Remark 4.2.12) we see that this also forms a ring.

In Step 4, the algorithm correctly determines if A is ramified at $\mathfrak{p}$ by Proposition 4.1.11, and therefore the order is maximal by Lemma 4.3.1. Otherwise, $(a/\mathfrak{p}) = 1$ and the element $\alpha - z$

is a zerodivisor, hence the $\overline{\Lambda}$ ideal $\overline{I}$ indeed has a $\mathbb{Z}_F/\mathfrak{p}$-basis consisting of 2 elements. We then compute the lift I of this ideal to Λ. Since $\mathfrak{p}$ is odd, by Hensel's lemma we may find $\widetilde{z} \in \mathbb{Z}_{F,\mathfrak{p}}$ satisfying $\widetilde{z}^2 = a$ and $\widetilde{z} \equiv z \pmod{\mathfrak{p}}$. We may choose a pair of generators for the ideal of $A_\mathfrak{p}$ generated by $\alpha - \widetilde{z}$ which reduce modulo $\mathfrak{p}$ to the set of generators for $\overline{I}$; then these elements generate a free $\mathbb{Z}_{F,\mathfrak{p}}$-module $I_\mathfrak{p}$ of rank 2. Note that $\mathcal{O}(I_\mathfrak{p}) \cong M_2(\mathbb{Z}_{F,\mathfrak{p}})$ is the maximal order, and $\Lambda_\mathfrak{p} \subsetneq \mathcal{O}(I_\mathfrak{p})$. Clearly $x \in \mathcal{O}(I)$ if and only if $x_\mathfrak{p} \in \mathcal{O}(I_\mathfrak{p})$, so $\mathcal{O}(I)$ is maximal at $\mathfrak{p}$.

In Step 5, if we have found a proper ideal then the correctness of the algorithm follows as in the previous step. Otherwise, $F(\gamma)$ is a field; since

$$\gamma^2 - x\gamma + \frac{x^2 - ay^2 - bz^2 + abw^2}{4} = 0$$

we know γ is integral, and $F_\mathfrak{p}(\gamma)$ is the unique quadratic unramified extension of $F_\mathfrak{p}$. The correctness of the maximal order now follows again by localization and [59, Corollaire II.1.7]. □

Remark 4.3.9. The order computation in Step 2 cannot be improved to include maximal orders for each of the fields. Consider, for example, $F = \mathbb{Q}$, and the quaternion algebra $A = \left(\frac{-3, 5}{\mathbb{Q}}\right)$. Then we have the maximal orders $\mathbb{Z}[(1+\alpha)/2]$ and $\mathbb{Z}[(1+\beta)/2]$, but we find that

$$\left(\frac{1+\beta}{2}\right)\left(\frac{1+\alpha}{2}\right) = \left(\frac{1-\alpha}{2}\right)\left(\frac{1+\beta}{2}\right) + \frac{\alpha\beta}{2},$$

which is not integral (since $\alpha\beta/2$ has norm $15/4$).

Having given an algorithm which will work in practice, we prove the following result which characterizes the abstract complexity class of this problem. (This is hinted at in [48, §6].)

Theorem 4.3.10. *Problem* 4.3.2 *for any fixed number field F is equivalent in probabilistic polynomial time to the problem of factoring integers.*

To prove the theorem, we will need to use a few existing algorithms. There exists probabilistic polynomial time algorithms to factor polynomials over a finite field, such as the

Cantor-Zassenhaus algorithm; see [21, Theorem 14.14] and [9, §3.4]. In fact, for our applications, it suffices to have an algorithm to compute a square root in a finite field, for which we may use the algorithm of Tonelli and Shanks [9, §1.5.1].

Lemma 4.3.11. *The problem of factoring integral ideals $\mathfrak{a}$ of an arbitrary number field is probabilistic polynomial time equivalent to the problem of factoring integers.*

Proof. Suppose $\mathfrak{a}$ is an integral ideal of F. After factoring the absolute discriminant $d(F/\mathbb{Q})$, we can in deterministic polynomial time compute the ring of integers $\mathbb{Z}_F$ of F (see [5]). Now let $\mathfrak{a}$ be an ideal with norm $N_{F/\mathbb{Q}}(\mathfrak{a}) = a$. Compute the prime decomposition of a. For each prime $p \mid a$, one can decompose $p\mathbb{Z}_F = \prod_i \mathfrak{p}_i^{e_i}$ into primes by a probabilistic polynomial time algorithm due to Buchmann and Lenstra [9, Algorithm 6.2.9]; if one is willing to use probabilistic methods here, things are even slightly simpler (see e.g. [9, Proposition 6.2.8]). From this list of primes we easily obtain the factorization of $\mathfrak{a}$.

Conversely, if one has an algorithm to factor ideals, then one may factor $a\mathbb{Z}_F$ into primes and computing norms we recover the prime factorization of a over $\mathbb{Z}$. □

We will also make use of one other lemma.

Lemma 4.3.12. *Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_F$ be prime to 2, not a square, and not a prime power. Let*

$$S = \left\{ b \in \mathbb{Z}_F/\mathfrak{a} : \ \exists \textit{ primes } \mathfrak{p}, \mathfrak{q} \textit{ such that } \mathfrak{p}^e, \mathfrak{q}^f \parallel \mathfrak{a} \textit{ and } \left(\frac{b}{\mathfrak{p}}\right)^e \neq -1,\ \left(\frac{b}{\mathfrak{q}}\right)^f \neq -1 \right\}.$$

Then $\#S > \frac{1}{2}N(\mathfrak{a})$.

Proof. Write $a\mathbb{Z}_F = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_s^{f_s}$ where $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ are distinct prime ideals of $\mathbb{Z}_F$ and $e_1, \dots, e_r$ are odd, $f_1, \dots, f_s$ are even. By assumption, $r \geq 1$.

First, suppose that $s \geq 1$. Note that $(b/\mathfrak{q}_j)^{f_j} \neq -1$ for all $b \in \mathbb{Z}/a\mathbb{Z}$ and $j = 1, \dots, s$. Hence $b \notin S$ if and only if $(b/\mathfrak{p}_i) = 1$ for all $i = 1, \dots, r$ or $(b/\mathfrak{p}_i) = 0$ for some $i = 1, \dots, r$. By the Chinese remainder theorem, then, the number of $b \notin S$ is equal to

$$\prod_{i=1}^{r} \frac{1}{2} N(\mathfrak{p}_i)^{e_i - 1} \left(N(\mathfrak{p}_i) - 1\right) = \left(\frac{1}{2}\right)^r N(\mathfrak{a}) \prod_{i=1}^{r} \left(1 - \frac{1}{N\mathfrak{p}_i}\right) < \frac{1}{2} N(\mathfrak{a}).$$

The result now follows. Otherwise, we have $s = 0$, in which case $r \geq 2$. Then $b \notin S$ if and only if $(b/\mathfrak{p}_i) = 1$ for all i or $(b/\mathfrak{p}_i) = -1$ for all i, and so by the preceding these total

$$2N(\mathfrak{a}) \left(\frac{1}{2}\right)^r \prod_{i=1}^{r} \left(1 - \frac{1}{N\mathfrak{p}_i}\right) < \frac{1}{2} N(\mathfrak{a})$$

and again the result follows. □

Proof of Theorem 4.3.10. Since one can factor polynomials over a finite field in probabilistic polynomial time, given an algorithm to factor integers, we may compute a maximal order as in Proposition 4.3.4 or Algorithm 4.3.8.

Now we prove the converse. Suppose we have an algorithm to solve Problem 4.3.2. Let $a \in \mathbb{Z}_{>0}$ be the integer to be factored, which we may assume without loss of generality is odd, not a prime power and not a square. We can in constant time factor $d(F/\mathbb{Q})$, so we may also assume $\gcd(a, d(F/\mathbb{Q})) = 1$. It follows that the ideal $a\mathbb{Z}_F$ is also odd, not a prime power, and not a square. By Lemma 4.3.12, the probability that a random nonzero element $b \in \mathbb{Z}_F/a\mathbb{Z}_F$ has the property that there exist primes $\mathfrak{p}, \mathfrak{q}$ such that $\mathfrak{p}^e, \mathfrak{q}^f \parallel a$ and $(b/\mathfrak{p})^e \neq 1$ and $(b/\mathfrak{q})^f \neq -1$ is $> 1/2$; therefore in probabilistic polynomial time we may find such an element.

Suppose that $\gcd(a, N(b)) \neq 1$. If $\gcd(a, N(b)) \neq a$, we have found a nontrivial factor of a. Otherwise, the ideal $\mathfrak{a} = a\mathbb{Z}_F + b\mathbb{Z}_F$ is a proper divisor of $a\mathbb{Z}_F$, and we repeat the above step with $\mathfrak{a}$ in place of $a\mathbb{Z}_F$. Since $N(a\mathbb{Z}_F) = a^g$ where $g = [F : \mathbb{Q}]$, we need repeat this step only g times until we find an element b such that $\gcd(N(b), a) = 1$; since this depends only on F and not on A, we may do this in polynomial time.

Thus we may suppose that we have $(b/\mathfrak{p}) = -1$ and $(b/\mathfrak{q}) = 1$, and that e is odd. Let $A = \left(\dfrac{a, b}{F}\right)$; compute a maximal order $\mathcal{O}$ of A. Now since $\mathfrak{p}$ is prime to $d(F/\mathbb{Q})$, we know that

$\mathfrak{p}$ is unramified in F, and since $\mathfrak{p}^e \parallel a\mathbb{Z}_F$ with e odd, the extension $F(\sqrt{a})/F$ is ramified at $\mathfrak{p}$. Since $(b/\mathfrak{p}) = -1$, by Corollary 4.1.11, the algebra A is ramified at $\mathfrak{p}$. Therefore by Lemma 4.3.1, $\mathfrak{p}$ divides the discriminant $\mathfrak{d}(\mathcal{O})$.

Now we show that $\mathfrak{q} \nmid \mathfrak{d}(\mathcal{O})$. If f is even, since $\mathfrak{q}^f \parallel a\mathbb{Z}_F$, we have that $F(\sqrt{a})/F$ is unramified at $\mathfrak{q}$; since also $(b/\mathfrak{q}) \neq 0$, by the same corollary, A is unramified at $\mathfrak{q}$. And if f is odd, then since $(b/\mathfrak{q})^f = 1$ we must have $(b/\mathfrak{q}) = 1$, and again by the corollary it follows that A is unramified. Therefore $\gcd(N(d(\mathcal{O})), a)$ is a proper factor of a, and the proof is complete. □

Remark 4.3.13. Deterministically, already the problem of finding a nonsquare modulo a prime p is difficult; one unconditional result known is that the smallest quadratic nonresidue of a prime p is of size exponential in $\log p$; under condition of a generalized Riemann hypothesis, one can find a quadratic nonresidue which is of polynomial size in $\log p$.

4.4 Class group computations

In this section, we discuss the algorithmic problems analogous to those of computing class groups and units for quaternion algebras; as in the previous section, we let A be a quaternion algebra over a number field F.

Computing the class group and unit group of a number field appears to be a difficult task; we refer the reader to [36, §5] for a more complete discussion. The best known algorithms to compute these groups for a general number field are exponential in the absolute value of the discriminant, and even the case of imaginary quadratic fields shows that the size of the class group is often as large. Therefore in this section we shift our focus to a mindedly practical one and exhibit algorithms that work well in practice.

Given a number field F and its maximal order $\mathbb{Z}_F$, we know by [36, Theorem 5.5] that there exist deterministic and probabilistic algorithms which compute a set of generators for

$\mathbb{Z}_F^*$ and the structure of the class group $\mathrm{Cl}\,\mathbb{Z}_F$; see also [9, Algorithm 6.5.9]. The problem of determining whether or not an ideal is principal appears no easier, but again by [9, §6.5.10] there exists an algorithm which, given the internal calculations involved in the class group computation, determines whether or not an ideal is principal and, if so, outputs a generator.

Let I, J be right ideals of a maximal order $\mathcal{O}$ of A. We say that I and J are in the same *right ideal class*, and write $I \sim J$, if there exists an $\alpha \in A^*$ such that $I = \alpha J$, or equivalently, if I and J are isomorphic as right $\mathcal{O}$-modules. It is clear that $\sim$ defines an equivalence relation on the set of right ideals of $\mathcal{O}$; we write $[I]$ for the ideal class of I. We define the product IJ to be the right ideal generated by the set

$$\{\alpha\beta : \alpha \in I, \beta \in J\}.$$

Note that since A is non-commutative, the ideal class $[IJ]$ is not determined by the ideal classes $[I]$ and $[J]$, so the set of right ideal classes may not form a group.

Proposition 4.4.1 ([59, Théorème III.5.4])**.** *The number h of right ideal classes of is finite and is the same for every maximal order $\mathcal{O} \subset A$.*

We are led to the following problems.

Problem 4.4.2. *Given a maximal order $\mathcal{O}$ of A, compute the class number h of A; given an ideal I of $\mathcal{O}$, determine the ideal class $[I]$ of I.*

Kohel [31] has implemented algorithms in the computer algebra system MAGMA which solve this problem for definite quaternion algebras over $\mathbb{Q}$. We have nothing more to say for these problems over an arbitrary quaternion algebra over a number field. For applications to Shimura curves below, it will suffice to restrict to the case where A has at least one unramified real place; we say then that A *satisfies the Eichler condition.* For $I \subset \mathcal{O}$ a right ideal, we define $\mathrm{nrd}(I)$ to be the ideal of $\mathbb{Z}_F$ generated by the set $\{\mathrm{nrd}(x) : x \in I\}$.

Proposition 4.4.3 ([45, Corollary 34.21], [59, Théorème III.5.7])**.** *Suppose that A satisfies the Eichler condition. Then the map* nrd *gives a bijection between the set of ideal classes and the class group* $\mathrm{Cl}\,\mathbb{Z}_F$*.*

This proposition gives an immediate solution to Problem 4.4.2 when A satisfies the Eichler condition. However, we are still left with the constructive principal ideal problem.

Problem 4.4.4. *Given an ideal I of a maximal order $\mathcal{O}$, determine if I is a principal ideal and, if so, compute an an element α such that $I = \alpha\mathcal{O}$.*

We will exhibit a solution to this problem for the case when F is a totally real number field and A satisfies the Eichler condition. First, we prove a lemma which does not rely upon these hypotheses.

Lemma 4.4.5. *Let F be a number field, let A be a central simple algebra over F, let $\mathcal{O} \subset A$ be an order, let $I \subset \mathcal{O}$ be a right ideal, and let $\xi \in I$. Then ξ generates I if and only if* $\mathrm{nrd}(\xi)\mathbb{Z}_F = \mathrm{nrd}(I)$ *if and only if* $N(\mathrm{nrd}(\xi))\mathbb{Z} = N(\mathrm{nrd}(I))$.

Proof. If one first defines the norm N of a right ideal I of $\mathcal{O}$ as the product of the primes of $\mathcal{O}$ occuring in a composition series for $\mathcal{O}/I$ ([45, 24.1]) as a $\mathcal{O}$-module, then the statement $\xi\mathcal{O} = I$ if and only if $N(\xi\mathcal{O}) = N(I)$ is obvious. Since $[A : F] = 4$, then the norm N is the square of the reduced norm by [45, Theorem 24.11]. The second statement follows in the same way, in the much easier context of Dedekind domains. □

With this lemma in hand, we have the following algorithm to solve Problem 4.4.4.

Algorithm 4.4.6 (Principal ideal testing)*.* Let F be a totally real number field, let A be a quaternion algebra over F which satisfies the Eichler condition, let $\mathcal{O} \subset A$ be an order, and let $I \subset \mathcal{O}$ be an ideal. This algorithm determines if I is a principal $\mathcal{O}$-ideal and outputs a generator for I if it exists.

1. [Check norm for principality] Compute $\operatorname{nrd}(I) \subset \mathbb{Z}_F$. Test if $\operatorname{nrd}(I) \subset \mathbb{Z}_F$ is principal; if not, output a message indicating that I is not principal and terminate the algorithm. Otherwise, let $q = N(\operatorname{nrd}(I))$.

2. [Find a $\mathbb{Z}$-basis for I] Find a $\mathbb{Z}$-generating set for I and write these elements in the $\mathbb{Z}$-basis for $\mathcal{O}$. Using the MLLL algorithm [9, 2.6.8], find a $\mathbb{Z}$-basis $B = \gamma_1, \ldots, \gamma_{4g}$ for I.

3. [LLL] Let $\sigma_1, \ldots, \sigma_g$ be the g distinct real embeddings $F \hookrightarrow \mathbb{R}$. Embed $I \hookrightarrow \mathbb{R}^{4g}$ as a lattice L via the embedding

$$\mu \mapsto (\sigma_1(\mu_1), \sigma_2(\mu_1), \ldots, \sigma_g(\mu_1),\ \ldots,\ \sigma_1(\mu_4), \sigma_2(\mu_4), \ldots, \sigma_g(\mu_4)),$$

where $\mu = \mu_1 + \mu_2\alpha + \mu_3\beta + \mu_4\alpha\beta$. Compute an LLL-reduced basis L' of this lattice with respect to the ordinary inner product on $\mathbb{R}^{4g}$, and let T be the unimodular transformation such that $TL = L'$. Let $B' = TB$ be the basis for I obtained by applying T to the basis B.

4. [Check short vectors] For each μ in the $\mathbb{Z}$-linear span of B', compute $\operatorname{nrd}(x)$. If $|N(\operatorname{nrd}(\mu))| = q$, output μ and terminate the algorithm.

This algorithm terminates because if the ideal is principal, by exhaustive listing eventually an element which generates the ideal will be found. We analyze the benefit of the LLL-reduction step over the naive approach below.

Remark 4.4.7. It is tempting to embed the set of generators for I already in Step 3, but due to precision loss it will be impossible to realize this as a lattice. One could overcome this by using a rational approximation for the basis of F.

In Step 2, one may also compute the Hermite normal form [9, §2.4] of L, but this algorithm computes more than what is required and may behave very badly.

In Step 4, one may list the vectors $\mu \in B'$ in any reasonable way; one simple way is to use the *norm-lexicographical ordering*, namely, $x \prec x'$ if and only if $|x|^2 \leq |x'|^2$ and there exists a j such that $x_i = x'_i$ for all $i < j$ and $x_j < x'_j$. (To avoid problems of precision, it may again be best to use rational approximations.)

In Step 3, note that one may also compute an LLL-reduced basis with respect to an inner product other than the standard inner product. This may be useful for algebras or number fields with large discriminant, but to simplify the analysis we stick to the simplest case. Moreover, one may choose coordinates for A in any reasonable way; we again choose orthogonal coordinates to simplify the analysis.

For a lattice $L \hookrightarrow V = \mathbb{R}^n$ with basis $v_1, \dots, v_n$, we define the *discriminant* of L to be

$$\det(L) = |\det(v_1, \dots, v_n)|.$$

Lemma 4.4.8. *With the notation as in Algorithm* 4.4.6*, suppose that $I = \xi\mathcal{O}$, let Λ be the order generated by $1, \alpha, \beta, \alpha\beta$, and suppose $\Lambda \subset \mathcal{O}$. Then we have*

$$\det(L) = \frac{d(F/\mathbb{Q})^2 N_{F/\mathbb{Q}}(\mathrm{nrd}(\xi))^2}{[\mathcal{O} : \Lambda]},$$

where $I = \xi\mathcal{O}$.

Proof. Since by Lemma 4.1.8 the F-endomorphism of A given by left multiplication by ξ has determinant $\mathrm{nrd}(\xi)^2$, and it follows that the corresponding $\mathbb{Q}$-endomorphism of L has determinant $N_{F/\mathbb{Q}}(\mathrm{nrd}(\xi))^2$. Hence

$$\det(L) = \det(\xi\mathcal{O}) = N_{F/\mathbb{Q}}(\mathrm{nrd}(\xi))^2 \det(\mathcal{O}) = N(\mathrm{nrd}(\xi))^2 \frac{\det(\Lambda)}{[\mathcal{O} : \Lambda]}$$

since $\Lambda \subset \mathcal{O}$. Now the lattice Λ is block-diagonal form, and it is easy to see that $\det(\Lambda) = d(F/\mathbb{Q})^2$, so the result follows. □

Now we analyze the efficacy of the above algorithm; we are unable to prove any rigorous time bounds. Already the first step of the algorithm requires the computation of the class group of $\mathcal{O}_F$; and even if we suppose that the class group has been precomputed, there do not appear to be rigorous time bounds for the principal ideal testing algorithm [9, 6.5.10]. We note happily though that in practice, this algorithm runs quite efficiently.

Proposition 4.4.9. *Let F be a totally real field and A a quaternion algebra over F with α, β contained in an order $\mathcal{O}$. Then there exists a $C \in \mathbb{R}_{>0}$ such that for every ideal I of $\mathcal{O}$, the first basis element γ in the LLL-reduced basis B' in step* (3) *of Algorithm* 4.4.6 *satisfies*

$$|N(\operatorname{nrd}(\gamma))| \leq C|N(\operatorname{nrd}(I))|.$$

Proof. Let

$$M = \max_i\{|\sigma_i(a)|, |\sigma_i(b)|, |\sigma_i(ab)|\}.$$

Then for any

$$\gamma = x + y\alpha + z\beta + w\alpha\beta = \gamma_1 + \gamma_2\alpha + \gamma_3\beta + \gamma_4\alpha\beta,$$

we have

$$\operatorname{nrd}(\gamma) = x^2 - ay^2 - bz^2 + abw^2$$

so

$$|\sigma_i(\operatorname{nrd}(\gamma))| \leq M\left(|\sigma_i(x^2)| + \cdots + |\sigma_i(w^2)|\right) = M\sum_j |\sigma_i(\gamma_j)^2|.$$

Thus by [37, (1.9)] and Lemma 4.4.8, we have for all i, j that

$$|\sigma_i(\gamma_j)|^2 \leq |\gamma|^2 \leq 2^{(4g-1)/2}\det(L)^{1/2g} = \frac{2^{(4g-1)/2}|d(F/\mathbb{Q})|^{1/g}|N(\operatorname{nrd}(I))|^{1/g}}{[\mathcal{O}:\Lambda]^{1/2g}}.$$

We conclude that

$$|N(\operatorname{nrd}(\gamma))| = \prod_i |\sigma_i(\operatorname{nrd}(\gamma))|^2 \leq \frac{(4M)^g 2^{(4g^2-g)/2}}{[\mathcal{O}:\Lambda]^{1/2}}|d(F/\mathbb{Q})||N(\operatorname{nrd}(I))|$$

as claimed. □

Since any generator $\xi \in I$ has $N(\operatorname{nrd}(I)) = |N(\operatorname{nrd}(\xi))|$, we conclude that the algorithm produces elements which are very close to being generators.

We close with an application to finding elements in $\mathcal{O}$ of small norm, which is inspired by an algorithm of Michael Stoll.

Algorithm 4.4.10. Let $K = F(\sqrt{d})$ be a totally imaginary quadratic extension of a totally real field F with $[F : \mathbb{Q}] = g$. Let A be a quaternion algebra over F and suppose that K splits A, and let $\mathcal{O}$ be a maximal order of A. This algorithm outputs a zerodivisor $\alpha_K \in A \otimes_F K$.

1. [Basis] Using the LLL algorithm above, find a reduced basis of the trace zero part of $\mathcal{O}$ over $\mathbb{Z}$; this yields a basis $\alpha_1, \dots, \alpha_{6g}$ for the trace zero part of $\mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_K$.

2. [Compute forms] Compute

$$(x_1\alpha_1 + \cdots + x_{6g}\alpha_{6g})^2 = Q_1(x_1, \dots, x_{6g})\alpha_1 + \cdots + Q_{6g}(x_1, \dots, x_{6g})\alpha_{6g}$$

   where $Q_i \in \mathbb{Z}_F[x_1, \dots, x_{6g}]$ are quadratic forms. Let $|Q_i|$ denote these forms with every coefficient replaced by the absolute value of their norm, and let $Q = \sum_i |Q_i|$.

3. [LLL] Use LLL to reduce the standard lattice with respect to the quadratic form Q, and let B be the transformed basis.

4. [Check short vectors] For each μ in the $\mathbb{Z}$-linear span of B, compute $\mathrm{nrd}(x)$. If $\mathrm{nrd}(\mu) = 0$, output μ and terminate the algorithm.

We remark only that this algorithm seems to work in practice; it would be interesting to estimate its efficiency as above.

Chapter 5

Shimura curves

In this chapter, we apply the algorithms of Chapter 4 to an arithmetic geometric setting. In the first section, we introduce Shimura curves which arise from indefinite quaternion algebras and we prove a result concerning their field of definition in certain circumstances (5.1.2). In §5.2, we give fast methods for computing hypergeometric series to high precision, which allows us to compute parametrizations of these curves. In §5.3, we introduce CM points, which are special points on these curves defined over abelian extensions, and we give algorithms for computing them as complex numbers. In §5.4, we give an extended example and some applications.

5.1 Triangle groups

Let $\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$ where $i^2 = -1$, and let $\mathfrak{H} = \{z = x + yi \in \mathbb{C} : y > 0\}$ be the complex upper-half plane. The group

$$PSL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\} / \{\pm 1\}$$

acts on $\mathfrak{H}$ by

$$z \mapsto \gamma(z) = \frac{az+b}{cz+d}, \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{R}).$$

The *hyperbolic area* of a region D in $\mathfrak{H}$ is given by

$$\mu(D) = \int\int_D \frac{dx\,dy}{y^2}.$$

Let Γ be a discrete subgroup of $PSL_2(\mathbb{R})$ such that the orbit space $\Gamma\backslash\mathfrak{H}$ has $\mu(\Gamma\backslash\mathfrak{H}) < \infty$; we say then that Γ is a *Fuchsian group of the first kind* [30, §3.4, Theorem 4.5.2]. Two groups Γ, Γ' are said to be *commensurable* if each of the indices $[\Gamma : \Gamma \cap \Gamma'], [\Gamma' : \Gamma \cap \Gamma']$ is finite. The quotient space $\Gamma\backslash\mathfrak{H}$ can be given the structure of a Riemann surface [30, §3.6].

Every Fuchsian group Γ has a *fundamental domain* [30, §3.2], namely a connected, closed set $D \subset \mathfrak{H}$ such that the translates of D by Γ cover $\mathfrak{H}$ and the interiors of all translates are disjoint: that is to say, $\bigcup_{\gamma\in\Gamma} \gamma(D) = \mathfrak{H}$ and $D^o \cap \gamma(D)^o = \emptyset$ for all $\gamma \in \Gamma \setminus \{1\}$, where D^o is the interior of D.

An example of this situation is the modular group $\Gamma = SL_2(\mathbb{Z})$ with the usual fundamental domain (see [50, §VII.1]), and this group has been well-studied. In the following, we will exclude this case to unify the notation; more specifically, we will assume from now on that Γ has a compact fundamental domain, and therefore $\Gamma\backslash\mathfrak{H}$ is a complete curve.

The stabilizer $\Gamma_z = \{\gamma \in \Gamma : \gamma(z) = z\}$ of a point $z \in \mathfrak{H}$ is finite and cyclic [30, Theorem 2.3.5]. A point $z \in \mathfrak{H}$ is an *elliptic point* of order $k \geq 2$ if $\#\Gamma_z = k$. A maximal finite subgroup of Γ is known as an *elliptic cycle*. There are only finitely many Γ-orbits in $\mathfrak{H}$ with nontrivial stabilizer, and the set of orbits with nontrivial stabilizer are in bijective correspondence with the set of elliptic cycles up to conjugation. Choosing a point $p \in \mathfrak{H}$ not fixed by any element of $\Gamma \setminus \{1\}$, we obtain a fundamental domain for Γ given by

$$D = \{z \in \mathfrak{H} : d(z,p) \leq d(z,\gamma(p)) \text{ for all } \gamma \in \Gamma\},$$

where

$$d(z,w) = \int_\gamma \frac{\sqrt{dx^2+dy^2}}{y}$$

and γ is a hyperbolic geodesic joining z and w. The domain D is a hyperbolically convex region bounded by a union of geodesics with vertices at elliptic points [30, §3.5].

Suppose that Γ has t elliptic cycles of order $m_1, \dots, m_t$, and let $X = \Gamma\backslash\mathfrak{H}$. Then the genus $g = g(X)$ of the surface $\Gamma\backslash\mathfrak{H}$ is related to the volume $\mu(X)$ by the formula

$$\frac{1}{2\pi}\mu(X) = 2g(X) - 2 + \sum_{i=1}^{t}\left(1 - \frac{1}{m_i}\right)$$

given in [30, Theorem 4.3.1]. The structure of the group Γ is given by

$$\Gamma = \langle a_1, b_1, \dots, a_g, b_g, s_1, \dots, s_t \mid s_1^{m_1} = \ldots = s_t^{m_t} = s_1 \cdots s_r [a_1,b_1] \cdots [a_g,b_g] = 1\rangle$$

where $[a,b] = aba^{-1}b^{-1}$ [30, §4.3, p. 99], and the group Γ is said to have *signature* $(g; m_1, \dots, m_t)$.

Now let A be a quaternion algebra over a totally real field F, with $[F:\mathbb{Q}] = g$. Suppose that

$$A \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \times \mathbb{H}^{r-1}$$

as $\mathbb{R}$-algebras (see §4.1). We fix the unique real place of F at which A is unramified and identify $F \hookrightarrow \mathbb{R}$ as a subfield of $\mathbb{R}$ by this embedding; fix also an isomorphism $\iota_\infty : A \otimes_F \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$. Let $\mathcal{O}$ be a maximal order of A, let

$$\mathcal{O}_1^* = \{\gamma \in \mathcal{O}^* : \mathrm{nrd}(\gamma) = 1\} = \mathcal{O}^* \cap \iota_\infty(SL_2(\mathbb{R}))$$

be the group of elements of $\mathcal{O}$ with reduced norm 1, and let

$$\Gamma(1) = \iota_\infty(\mathcal{O}_1^*)/\{\pm 1\} \subset PSL_2(\mathbb{R}).$$

Then the group $\Gamma(1)$ is a Fuchsian group of the first kind [30, Theorem 5.2.7], [59, Theorem IV.1.1], also known as an *arithmetic Fuchsian group.* As above, it gives rise to a compact Riemann surface $\Gamma(1)\backslash\mathfrak{H}$ [30, Theorem 5.4.1]. The Riemann surface $\Gamma(1)\backslash\mathfrak{H}$ is known as a *Shimura curve.*

A theorem of Shimura implies that the Riemann surface $\Gamma(1)\backslash\mathfrak{H}$ in fact has a canonical model defined over a number field not much larger than F, which follows from its interpretation as a (coarse) moduli space for certain abelian varieties. To state this theorem, we first introduce some notation. By a *curve* over F we mean a geometrically integral separated scheme of finite type over F of dimension 1 [25, Remark 4.10.1]. Given a scheme X of finite type over a subfield of $\mathbb{C}$, we let $X_{\mathbb{C}}$ denote the associated complex analytic space [25, Appendix B]. Let $F^{(\infty)}$ denote the ray class field of F with conductor the product of all real places of F; note that F has strict class number 1 if and only if $F = F^{(\infty)}$.

Theorem 5.1.1 ([51, Main Theorem I (3.2)]). *Let $\Gamma \subset \Gamma(1)$ be a subgroup of finite index. Then there exist a projective, nonsingular curve $X(\Gamma)$ defined over $F^{(\infty)}$ and a holomorphic map $j_\Gamma : \mathfrak{H} \to X(\Gamma)_{\mathbb{C}}$ such that the map j_Γ yields an analytic isomorphism*

$$j_\Gamma : \Gamma\backslash\mathfrak{H} \xrightarrow{\sim} X(\Gamma)_{\mathbb{C}}.$$

The above property as we have stated it does not yet determine the model X canonically; one needs also a condition on so-called CM points (see §5.3 below).

There exist algorithms which compute a fundamental domain for an arithmetic group $\Gamma(1)$; such an algorithm takes as input a maximal order $\mathcal{O}$ of a quaternion algebra A and outputs the fundamental domain given by the hyperbolic convex hull of a set of vertices. The existing algorithms produce as a side result an explicit set of elements in $\mathcal{O}_1^*/\{\pm 1\}$ which map to generators of Γ as in the algorithm [29], which relies upon explicit bounds for the sizes of the coefficients of such elements in a basis for $\mathcal{O}$. We also cite [1, Chapter 5] for a detailed study of the case $F = \mathbb{Q}$, which relies upon the representation of elements by integral ternary forms. Given this convex hull, from the way the translates of a fundamental domain fit together one also obtains relations amongst these generators. If one knows in advance the signature of Γ, then one can simply solve the equations defining the group Γ inside the group $\mathcal{O}_1^*$: to find an element $s \in \mathcal{O}_1^*/\{\pm 1\}$ of order k, notice that s generates a number field $F(s) \cong K = F(\zeta_{2k})$; to find such an embedding $K \hookrightarrow A$, one must solve Problem 4.2.6.

A *modular function* f with respect to a Fuchsian group Γ is a meromorphic function $f : \mathfrak{H} \to \mathbb{C}$ such that for all $\gamma \in \Gamma$ and all $z \in \mathfrak{H}$ we have $f(\gamma(z)) = f(z)$ (see [18, §39]). The map j above is an example of a (nonconstant) modular function.

A *compact triangle group* of type (p, q, r) is a Fuchsian group Γ of signature $(0; p, q, r)$ with $p, q, r \in \mathbb{Z}_{\geq 2}$. (A triangle group which is not compact is commensurable with $SL_2(\mathbb{Z})$, itself a triangle group of type $(2, 3, \infty)$.) By the above, this means that Γ has a presentation

$$\Gamma \cong \langle s_p, s_q, s_r \mid s_p^p = s_q^q = s_r^r = s_p s_q s_r = 1 \rangle.$$

A triangle group which is arithmetic as a Fuchsian group is known as an *arithmetic triangle group*.

Let Γ be a compact triangle group with generators s_p, s_q, s_r. We may assume that the fixed points of these generators are the vertices of a *fundamental triangle* for Γ, meaning that the hyperbolic convex hull of these points is a hyperbolic triangle with angles π/p, π/q, π/r, and the union of this triangle and its image in the reflection in the geodesic connecting any two of the vertices is a fundamental region D for Γ (see [30, pp. 100–101]).

By [55], there are exactly 18 commensurability classes of compact arithmetic triangle groups. As pointed out in [15, p. 3], already these contain a number of highly interesting curves. We will content ourselves to treat this case, and suggest that the next simplest class of Shimura curves come from those which arise from two-generator arithmetic Fuchsian groups, which have also been classified [39], [40].

For the rest of this section, let Γ be a compact arithmetic triangle group associated to a quaternion algebra A over a totally real field F. By the list in [55], we know that F is Galois over $\mathbb{Q}$ and F has strict class number 1; therefore the canonical model in Theorem 5.1.1 is defined over F.

By definition, every triangle group has $g = 0$, so we have a map $j : \Gamma\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ which is defined uniquely once we assert the images of the elliptic points z_p, z_q, z_r to be $0, 1, \infty$, respectively.

Now let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ which is coprime to the discriminant of A, and let $F_{\mathfrak{N}}$ be the completion of F at the ideal $\mathfrak{N}$, and $\mathbb{Z}_{F,\mathfrak{N}}$ its ring of integers. Then we have an embedding

$$\mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$$

of $\mathbb{Z}_{F,\mathfrak{N}}$-algebras which we fix for the rest of this section; all such embeddings are conjugate by an element of $GL_2(\mathbb{Z}_{F,\mathfrak{N}})$. We denote by $\Gamma_0(\mathfrak{N})$ the subgroup of $\mathcal{O}$ whose image in the above embedding is upper triangular modulo $\mathfrak{N}$. We abbreviate $\mathbb{F}_{\mathfrak{N}} = \mathbb{Z}_F/\mathfrak{N}$, and we let $X_0(\mathfrak{N})$ be the model obtained in Theorem 5.1.1 for $\Gamma_0(\mathfrak{N})\backslash\mathfrak{H}$. These are the curves analogous to the modular curves $X_0(N)$, and hence are interesting to study.

We now prove a Galois descent theorem which gives a model for $X_0(\mathfrak{N})$ over $\mathbb{Q}$ when $\mathfrak{N}$ is Galois-stable.

Proposition 5.1.2. *Let $\mathfrak{N}$ be an ideal of $\mathcal{O}_F$ with $\mathfrak{N}^\sigma = \mathfrak{N}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, and suppose that $\Gamma_0(\mathfrak{N})$ is commensurable with a triangle group. Then $X_0(\mathfrak{N})$ has a model defined over $\mathbb{Q}$.*

Proof. The following proof is suggested by [15, p. 38]. First, we note that by the explicit determination of [56], if $\Gamma_0(\mathfrak{N})$ is commensurable with a triangle group, then in fact there exists a triangle group Γ of signature $(0; p, q, r)$ with p, q, r distinct with $\Gamma_0(\mathfrak{N}) \subset \Gamma$ such that Γ arises from a quaternion algebra over F, Galois over $\mathbb{Q}$. Such a triangle group gives a map $j : \Gamma\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ as in 5.1.1. We may and do assume as above that j maps z_p, z_q, z_r to $0, 1, \infty$.

Let S be the set of noncomplex places of F where A is ramified; let A^σ be the quaternion algebra ramified at the set $S^\sigma = \{\sigma(v) : v \in S\}$. If $A \cong \left(\dfrac{a, b}{F}\right)$, then $A^\sigma \cong \left(\dfrac{\sigma(a), \sigma(b)}{F}\right)$, and the map σ which sends the standard basis of A to the standard basis of A^σ is a *σ-isomorphism*, meaning that it is a map of $\mathbb{Q}$-algebras which restricts to σ on F. It is easy to see that $\mathcal{O}^\sigma$ is a maximal order of A^σ. Given the embedding $\mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$, we also have

$$\mathcal{O}^\sigma \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}^\sigma}) = M_2(\mathbb{Z}_{F,\mathfrak{N}}).$$

In particular, σ gives an element of $\mathrm{Aut}(PSL_2(\mathbb{F}_\mathfrak{N}))$. Furthermore, the Galois closure of the extension $X_0(\mathfrak{N}) \to X(1)$ has Galois group which is naturally identified with $PSL_2(\mathbb{F}_\mathfrak{N})$ acting on the cosets of $\Gamma_0(\mathfrak{N})$ in $\Gamma(1)$, therefore σ gives rise to a σ-automorphism of $X_0(\mathfrak{N})$, i.e. an automorphism which lies over $\sigma : \operatorname{Spec} F \to \operatorname{Spec} F$.

The ramification points of the map $X_0(\mathfrak{N}) \to X(1)$ are the elliptic points of $\Gamma_0(\mathfrak{N})$, each of which is in the $\Gamma(1)$-orbit of an elliptic point of $\Gamma(1)$, which are exactly the branch points of the map $X_0(\mathfrak{N}) \to X(1)$. We may identify $X(1)$ with the base extension of $\mathbb{P}^1_\mathbb{Q}$ to $\mathbb{C}$, and then the branch points are defined over $\mathbb{Q}$, therefore σ acts by permutation on the preimages of the branch points. Let g_0, g_1, g_∞ be the monodromy around the branch points; then the action of σ must preserve the conjugacy classes of these elements, since by the Riemann existence theorem [61, Theorem 5.14] since the data of the conjugacy class and the Galois group uniquely define the cover $X_0(\mathfrak{N}) \to X(1)$ up to isomorphism over $X(1)$. But since the group $PGL_2(\mathbb{F}_\mathfrak{N})$ is *weakly rigid* (see [61, Definition 2.15, §3.3.6], and the references contained therein), the action of σ is induced by conjugation by an element $\gamma \in PSL_2(\mathbb{F}_\mathfrak{N})$. On the other hand, since σ acts by conjugation by the element γ which as acts continuously as a linear fractional transformation on the upper-half plane, the corresponding monodromy elements $g_i^\sigma = \gamma^{-1} g_i \gamma$ are unchanged under action by conjugation. All together, by the criterion in [61, Proposition 3.6], this implies that $X_0(\mathfrak{N})$ is defined over $\mathbb{Q}$. □

5.2 Computing hypergeometric series

Throughout this section, we continue the notation from §5.1. Let Γ be a compact arithmetic triangle group acting on the upper half-plane $\mathfrak{H}$. Let s_p, s_q, s_r be elliptic generators of orders p, q, r whose fixed points z_p, z_q, z_r form the vertices of a fundamental triangle for Γ. Let $j : \Gamma\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ be the parametrization normalized so that z_p, z_q, z_r are sent to $0, 1, \infty$, respectively.

We are interested in the following problem.

Problem 5.2.1. *Given a value $z \in \mathfrak{H}$, compute the value $j(z) \in \mathbb{P}^1(\mathbb{C})$.*

In other words, we wish to explicitly compute the parametrization $j : \Gamma\backslash\mathfrak{H} \to X(1)$, and to large precision. The reader who is uninterested in these numerical concerns may safely accept Algorithm 5.2.8 and proceed to the next section.

We now provide an overview on how we solve Problem 5.2.1, which we accomplish in three steps. In the first step, we reduce the problem to one in a neighborhood of an elliptic point by making a change of variables. Let D be the fundamental domain obtained from the union of the fundamental triangle and its image in the reflection in the geodesic connecting z_p and z_r. We exhibit in Algorithm 5.2.2 a way to compute $z' \in D$ in the Γ-orbit of z. Since $j(z') = j(z)$, we replace z' by z. The point z is now near to at least one elliptic point τ of Γ. We define the linear fractional transformation

$$\begin{aligned} \mathfrak{H} &\to \mathbb{C} \\ z &\mapsto w = \frac{z-\tau}{z-\overline{\tau}}. \end{aligned}$$

This transformation maps the upper half-plane $\mathfrak{H}$ to the open unit disc and maps τ to 0. One easily recovers z from w as

$$z = \frac{\overline{\tau}w - (\overline{\tau}+\tau)}{w-1}.$$

Second, rather than computing the value $j(z)$ directly, we use the fact that $t = j(z)$

arises as an automorphic function for the group Γ. For each elliptic point τ of order s, we will exhibit a Puiseux series $\phi_\tau(t) \in t^{1/s}\mathbb{C}[[t]]$ given as an explicit quotient of two hypergeometric series (Proposition 5.2.3), such that

$$w = \phi_\tau(j(z)).$$

To conclude, we use a combination of series reversion and Newton's method which, given z (and therefore w), finds the value $t = j(z)$ such that $w = \phi_\tau(t)$.

Fundamental domain

First, we will need an algorithm which moves any point in the upper half-plane into a fundamental domain for Γ. The following is inspired by the proof of [50, Theorem VII.2].

Algorithm 5.2.2. Let $z \in \mathfrak{H}$, and let Γ be a triangle group with generators s_p, s_q, s_r whose fixed points z_p, z_q, z_r are the vertices of a fundamental triangle for Γ. Let D be the fundamental domain obtained from the union of this triangle and its image in the reflection in the geodesic connecting z_p and z_r; let z_q' be the image of z_q in this reflection. This algorithm returns an element $z' \in D$ in the Γ-orbit of z.

1. [Move by s_r] Apply s_r to z until z is in the region bounded by the geodesics through z_r and z_q, and z_r and z_q'.

2. [Check] If $z \in D$, stop. Otherwise, apply s_p until z is in the region bounded by the geodesics $z_p z_q$ and $z_p z_q'$. Return to Step 1.

One note about precision loss: one may wish to allow an error epsilon in the above calculations. The procedure works as stated for those elements of $\mathbb{C}$ which are known to infinite precision, e.g. elements of $\overline{\mathbb{Q}}$, which is the case of concern to us.

Proof. For the proof, define a map $z \mapsto (z - z_r)/(z - \overline{z_r})$; this maps the upper half-plane conformally to the unit disc, and maps z_r to 0. The element s_r now acts by rotation by $2\pi/r$

about the origin. We will prove that if z is in the region as in Step 1, then $|s_p^i z| < |z|$ for some i. Then the algorithm can only act in finitely many steps, because we obtain a Γ-orbit with strictly decreasing absolute value, and the group Γ acts discontinuously; the point $\Gamma z \cap D$ (not on the boundary) is uniquely determined by the condition that it is in the sector and has smallest possible absolute value.

To prove this latter, choose an isometry of the disc which maps z_p to 0 and such that z_r maps to the positive real axis. Then s_p acts by rotation around the origin by an angle $2\pi/p$. By assumption, the image of the point z has $|\arg(-z)| > 2\pi/p$, therefore there exists a rotation which puts z with $|\arg(-z)| < 2\pi/p$, and therefore it will have image closer to z. This completes the proof. □

Hypergeometric series

In the case of modular curves, one may utilize modular forms and q-expansions to compute with automorphic forms. We will instead use the fact that the functional inverse of any nonconstant automorphic function can be expressed by the quotient of two solutions which form a vector space basis for the solutions of a second order linear differential equation [18, Theorem 15, §44]. For a triangle group of signature $(0; p, q, r)$, this differential equation will have 3 regular singular points [18, §109] corresponding to the elliptic points. Taking these to have the j-values $0, 1, \infty$, after a bit of simplification [18, §113] (see also [2, §2.3]) we obtain the *hypergeometric differential equation*

$$z(1-z)\frac{d^2y}{dz^2} + (c - (a+b+1)y)\frac{dy}{dz} - aby = 0$$

where

$$a = \frac{1}{2}\left(1 + \frac{1}{p} - \frac{1}{q} - \frac{1}{r}\right), \quad b = \frac{1}{2}\left(1 + \frac{1}{p} - \frac{1}{q} + \frac{1}{r}\right), \quad c = 1 + \frac{1}{p}.$$

In other words, the quotient F_1/F_2 of two linearly independent solutions F_1, F_2 to this equation maps $\mathfrak{H} \cup \mathbb{R}$ to a hyperbolic triangle with interior angles $\pi/p, \pi/q, \pi/r$; it is known as a *Schwarz map.* It extends to a map on all of $\mathbb{C}$ by the Schwarz reflection principle. (For other Fuchsian groups with at least 4 elliptic points or genus > 0, one must instead look at the relevant Schwarzian differential equation; see [15, p. 8] for a discussion, and [26] for the general situation.)

The solutions to the hypergeometric differential equation have been well-studied. For the moment, let $a, b, c \in \mathbb{R}$ be arbitrary real numbers with $c \notin \mathbb{Z}_{\leq 0}$. Define the *hypergeometric series*

$$F(a,b,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!} \in \mathbb{R}[[z]]$$

where $(x)_n = x(x+1)\cdots(x+n-1)$ is the *Pochhammer symbol.* This series is also known as the ${}_2F_1$ *series* or the *Gaussian hypergeometric function*; we refer to [54, §1.1] for a historical introduction. The hypergeometric series is convergent for $z \in \mathbb{C}$ with $|z| < 1$ by the ratio test ([54, §1.1.1]). It is indeed a solution to the hypergeometric differential equation; one can see this directly by letting

$$y(z) = \sum_{n=0}^{\infty} u_n z^n$$

and substituting into the hypergeometric differential equation to obtain

$$\sum_{n=0}^{\infty} \left((n+1)(n+c)u_{n+1} - (n^2 + (a+b)n + ab)u_n\right) z^n = 0$$

and hence

$$u_{n+1} = \frac{(n+a)(n+b)}{(n+1)(n+c)} u_n.$$

We make a cut in the t-plane along the real axis from $t = 1$ to $t = \infty$, that is, we insist that $-\pi < \arg(-t) \leq \pi$ for $|t| \geq 1$. Then the function $F(a,b,c;t)$ defined by the hypergeometric series can be analytically continued to a holomorphic function in the cut plane. We can obtain this by mean of the formulas below, provided $c + 1 \notin \mathbb{Z}_{\geq 0}$ and $a - b, c - a - b \notin \mathbb{Z}$.

Proposition 5.2.3. *Let τ be an elliptic generator of Γ of order s, and let t_s be a parameter on $\mathbb{P}^1$ near $j(\tau)$. Then there exists an explicitly given Puiseux series $\phi_\tau \in t_s^{1/s}\mathbb{C}[[t_s]]$ such that*

$$w = \phi_\tau(t_s).$$

Proof. In the neighborhood of the elliptic point $t_p = j(z_p) = 0$ given by $|t| < 1$, we have a basis of solutions

$$F_1(t) = F(a, b, c; t)$$

$$F_2(t) = t^{1-c}F(1 + a - c, 1 + b - c, 2 - c; t)$$

(which come from the above and [54, 1.3.6].) We note that since $1 - c = -1/p$, we have

$$F_1(t)/F_2(t) \in t^{1/p}\mathbb{R}[[t]]$$

which uniquely defines this ratio up to a scalar C_p. The value of C_p can be recovered by plugging in $t = 1$; when $c - a - b > 0$, we have

$$F(a, b, c; 1) = \frac{\Gamma(c)\Gamma(c - a - b)}{\Gamma(c - a)\Gamma(c - b)}$$

by [54, 1.7.6], [2, Theorem 2.2.2]. Note that

$$2 - c - (1 + a - c) = c - a - b = \left(1 + \frac{1}{p}\right) - \left(1 + \frac{1}{p} + \frac{1}{q}\right) = \frac{1}{q} > 0.$$

We recover the constant by solving

$$C_p \frac{F_1(1)}{F_2(1)} = \frac{z_q - z_p}{z_q - \overline{z_p}}.$$

In a similar fashion, near the elliptic point $t_q = j(z_q) = 1$ with $|1 - t| < 1$, we have

$$F_1(1 - t) = (1 - t)^{c-a-b}F(c - a, c - b, 1 - a - b + c; 1 - t)$$

$$F_2(1 - t) = F(a, b, 1 + a + b - c; 1 - t)$$

by [54, §1.3.1], so again the ratio

$$\frac{F_1(1-t)}{F_2(1-t)} = (1-t)^{1/q}\mathbb{R}[[1-t]]$$

is correct up to a scalar. To find the constant, we now have

$$(1-a-b+c)-(c-a)-(c-b) = (1+a+b-c)-a-b = -1/p < 0$$

so we must use the formula [54, 1.3.15]

$$F(a,b,c;t) = (1-t)^{c-a-b}F(c-a,c-b,c;t)$$

which yields

$$\begin{aligned}\lim_{t\to 0^+}\frac{F_1(1-t)}{F_2(1-t)} &= \lim_{t\to 1^-} t^{c-a-b}\frac{F(c-a,c-b,1-a-b+c;t)}{F(a,b,1+a+b-c;t)}\\ &= \lim_{t\to 1^-}\frac{(1-t)^{1-c}F(1-b,1-a,1-a-b+c;t)}{(1-t)^{1-c}F(1+b-c,1+a-c,1-a-b+c;t)}\\ &= \frac{F(1-b,1-a,1-a-b+c;1)}{F(1+b-c,1+a-c,1+a+b-c;1)}\end{aligned}$$

which can be evaluated by Γ-functions since

$$1-a-b+c-(1-b)-(1-a) = (1+a+b-c)-(1+b-c)-(1+a-c) = c-1 = 1/p > 0,$$

and we find

$$C_q\frac{F_1(1)}{F_2(1)} = \frac{z_p - z_q}{z_p - \overline{z_q}}.$$

Finally, for $t_r = j(z_r) = \infty$ with $|t| > 1$, we have

$$F_1(1/t) = (1/t)^{b-a}F(b,1+b-c,1+b-a;1/t)$$

$$F_2(1/t) = F(a,1+a-c,1+a-b;1/t)$$

by [54, 1.3.2], with $b-a = 1/r$ so

$$\frac{F_1(1/t)}{F_2(1/t)} \in (1/t)^{1/r}\mathbb{R}[[1/t]]$$

and letting $t \to 1$ we have

$$1 + b - a - b - (1 + b - c) = 1 + a - b - a - (1 + a - c) = c - a - b = 1/q > 0,$$

so we may again solve for the constant.

Putting these three equations together, we have completed the proof. □

Reversion and Newton's method

To conclude this algorithm, given the Puiseux series ϕ_τ from 5.2.3 and a value $w \in \mathbb{C}$, we wish to compute the value $t = j(z)$ such that

$$w = \phi_\tau(t).$$

As a first step, we can compute the reversion of the series $w = \phi_\tau(t)$ to find a power series ψ_τ satisfying

$$\psi_\tau(w(z)) = t = j(z).$$

The greatest cost of this method is in the reversion of a dense univariate Puiseux series. Based on methods of [58] or [4] (which use variations of Newton's method), this can be accomplished in time exponential in the number of terms n of the series obtained; note that even though this is polynomial in the input size, this quickly becomes quite expensive both in terms of time and space. Moreover, one is required to use fixed floating-point numbers because the height of the coefficients involved grows linearly in n. Worse still, because the hypergeometric series converge very slowly near the boundary, the algorithm above to compute a fixed reversion of a power series will *never* be able to give an algorithm which gives a guaranteed accuracy for such points. What is needed, then, is an algorithm which will compute "more terms" for those values.

It seems difficult to give a "general routine" for evaluation of the complex hypergeometric function [44, §5.14] (see also [54, §9]!). For "moderate" values of a, b, c and limited accuracy, one may evaluate this function by direct path integration in the complex plane [44, §6.12]; this algorithm involves a collection of "black-box" routines for the integration of sets of ordinary differential equations. Forrey [19] used transformation formulas for the hypergeometric function to give methods for evaluation at all real values z and arbitrary a, b, c. We combine and vary these methods to yield a fast algorithm for evaluation of $F(a, b, c; z)$ to high accuracy at all complex z. We will be more sketchy in this section, since all machine calculations with fixed precision arithmetic are subject to a certain rounding error, and we wish to avoid extensive application of the numerical tools required to make statements completely precise.

We now give an overview for the results in the rest of this subsection. We first give estimates for evaluating the hypergeometric series $F(a, b, c; t)$ directly when $|t| < 1/2$. We then compute Taylor series expansions for the hypergeometric series and use this in Algorithm 5.2.5 to compute $F(a, b, c; t)$ also when $|t - \rho| < 1/2$, where $\rho = (1 + i)/2$. Finally, we extend this to evaluate $F(a, b, c; t)$ for all $t \in \mathbb{C}$ using functional equations as in Proposition 5.2.6, and conclude with Algorithm 5.2.7.

For $|t| < 1/2$, the hypergeometric series converges rapidly and can be evaluated directly; more precisely, we may compute the series to accuracy $< \epsilon$ with running time polynomial in $\log(1/\epsilon)$. Let

$$F(a, b, c; t)|_N = \sum_{n=0}^{N} \frac{(a)_n (b)_n}{(c)_n} \frac{t^n}{n!}.$$

For any $\epsilon > 0$, we can estimate the value $N \in \mathbb{Z}_{>0}$ required to guarantee that

$$\big| F(a, b, c; t) - F(a, b, c; t)|_N \big| < \epsilon$$

as follows. First assume that $c > a + b - 1$. Then for all

$$n > M = M(a, b, c) = \max\left\{ \frac{c - ab}{c - (a + b - 1)}, a, b, c \right\}$$

we have

$$0 < \frac{(a+n)(b+n)}{(c+n)(n+1)} = 1 - \frac{(c-(a+b-1))\,n + (c-ab)}{(c+n)(n+1)} < 1,$$

and hence

$$\left|\frac{(a)_n(b)_n}{(c)_n n!}\right| < \left|\frac{(a)_M(b)_M}{(c)_M M!}\right| = A_M.$$

Now

$$\big|F(a,b,c;t) - F(a,b,c;t)|_N\big| = \left|\sum_{n=N+1}^{\infty} \frac{(a)_n(b)_n}{(c)_n}\frac{|t|^n}{n!}\right| \leq A_M \sum_{n=N+1}^{\infty} |t|^n = A_M \frac{|t|^{N+1}}{1-|t|}$$

so it suffices to take

$$N = \left\lceil \frac{\log \epsilon(1-|t|) - \log A_M}{\log |t|} \right\rceil.$$

Hence for $|t| < 1/2$, we may take

$$N = \left\lceil \frac{\log 2A_M + \log(1/\epsilon)}{\log 2} \right\rceil$$

which is indeed a polynomial in $\log(1/\epsilon)$. We note that this upper bound will almost always be too large in practice, and we may stop adding terms as soon as they become smaller than the machine epsilon.

For the rest of this section, we will use the expression $x \approx y$ to denote an approximate equality, one that is subject to floating point round-off errors. We refer the reader to [41] for more information about the provability of the error estimates in this algorithm.

We next will consider Taylor series expansions. Repeated differentiation of the hypergeometric differential equation gives the following:

$$\begin{aligned} t(1-t)\frac{d^{n+2}F}{dt^{n+2}} &= (n(1-2t) - (a+b+1)t + c)\,\frac{d^{n+1}F}{dt^{n+1}} \\ &\quad - (n(n-1) + n(a+b+1) + ab)\,\frac{d^{n-1}F}{dt^{n-1}}. \end{aligned}$$

From the Taylor series

$$F(a,b,c;t) = \sum_{n=0}^{\infty} \frac{1}{n!}\frac{d^nF}{dt^n}(a,b,c;\tau)(t-\tau)^n$$

and the above recurrence relation, given values for $F(a,b,c;\tau)$ and $F'(a,b,c;\tau)$, we may compute an approximate value for $F(a,b,c;t)$ for t close to τ, at least when $t(1-t)$ is not too small.

Algorithm 5.2.4. Let $t,\tau \in \mathbb{C}$ be such that $|t-\tau| < 1/2$ and $|t| > 1/4$, $|1-t| > 1/4$, and let $F_\tau, F'_\tau \in \mathbb{C}$ be such that

$$F_\tau \approx F(a,b,c;\tau), \quad F'_\tau \approx \frac{dF}{dt}(a,b,c;\tau).$$

This algorithm algorithm computes $F_t, F'_t \in \mathbb{C}$ such that

$$F_t \approx F(a,b,c;t), \quad F'_t \approx \frac{dF}{dt}(a,b,c;t).$$

1. [Initialite] Assign $F_t = F_\tau + F'_\tau(t-\tau)$, $F'_t = F'_\tau$, $i = 0$.

2. [Compute series] Let

$$F''_\tau = \frac{(-i(1-2t)+(a+b+1)t+c)\,F'_\tau + (i(i-1)+i(a+b+1)+ab)F_\tau}{t(1-t)}.$$

   Let

$$\begin{aligned} F_t &= F_t + \frac{F''_\tau}{i!}(t-\tau)^i \\ F'_t &= F'_t + \frac{F''_\tau}{(i-1)!}(t-\tau)^{i-1}. \end{aligned}$$

   If the terms added are smaller than machine epsilon, return F_t, F'_t. Otherwise, let $F_\tau = F'_\tau$, let $F'_\tau = F''_\tau$, let $i = i+1$, and return to Step 2.

We may then take $\rho = (1+i)/2$ as an advantageous choice for an additional base point to evaluate the hypergeometric series.

Algorithm 5.2.5. Let $t \in \mathbb{C}$ be such that $|t| < 1/2$ or $|t-\rho| < 1/2$. This algorithm computes $F_t, F'_t \in \mathbb{C}$ such that $F_t \approx F(a,b,c;t)$ and $F'_t \approx F'(a,b,c;t)$.

1. [Evaluate the series] If $|t| < 1/2$, evaluate the hypergeometric series directly until the terms become smaller than machine ϵ. If $|t-\rho| < 1/2$, first calculate approximate values of $F(a,b,c;\rho)$ and $F'(a,b,c;\rho)$, then apply Algorithm 5.2.4.

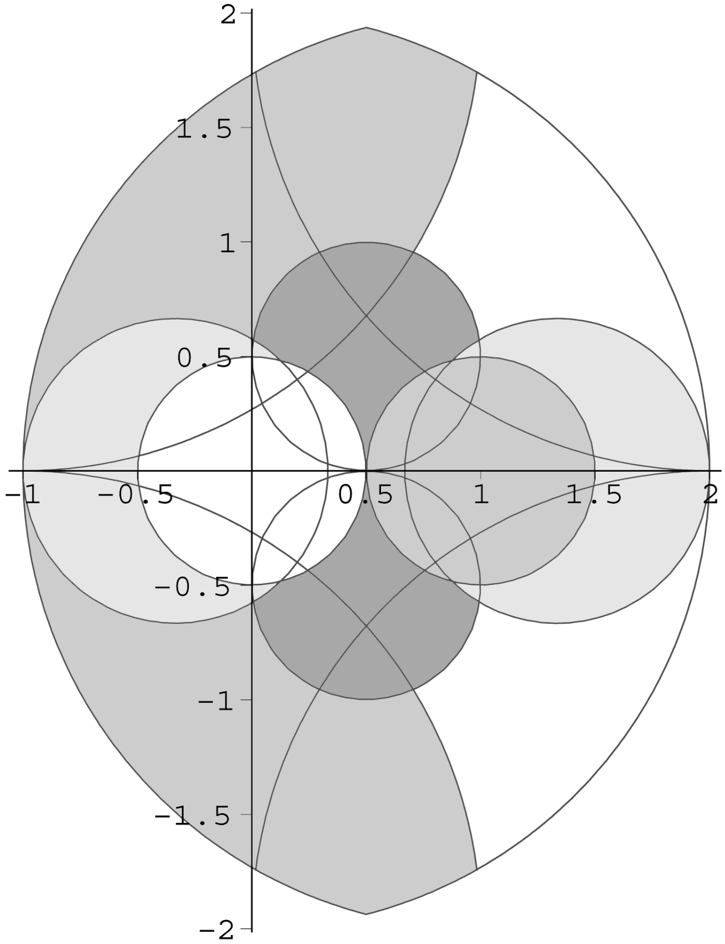

Figure 5.2.6: Covering the complex plane $\mathbb{C}$

Proposition 5.2.6. *For all $t \in \mathbb{C}$, there exists*

$$t' \in \left\{ t, \frac{1}{t}, 1-t, \frac{1}{1-t}, \frac{t}{t-1}, 1-\frac{1}{t} \right\} = W$$

such that either $|t'| < \frac{1}{2}$ or $|t' - \rho| < \frac{1}{2}$, where $\rho = (1+i)/2$.

Proof. If $|t| > 2$ or $|1-t| > 2$, we are done. For the others, we refer to the picture in Figure 5.2.6. For each t', we have drawn the regions $|t'| < 1/2$ and $|t' - \rho| < 1/2$, which are interiors of circles; these visibly cover the remaining region. □

We are now prepared to give a way of evaluating the hypergeometric series for any complex argument $t \in \mathbb{C}$. We have seen how to accomplish this for $|t| < 1/2$ and $|t - \rho| < 1/2$.

For $|1 - t| < 1/2$, we use the formula [2, (2.3.11)]

$$\begin{aligned} F(a, b, c; t) = & \\ & \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} F(a, b, a+b-c+1; 1-t) + \\ & (1-t)^{c-a-b} \frac{\Gamma(c)\Gamma(a+b-c)}{\Gamma(a)\Gamma(b)} F(c-a, c-b, c-a-b+1; 1-t). \end{aligned}$$

For $|t| > 2$, we use the formula [2, (2.3.12)]

$$\begin{aligned} F(a, b, c; t) = & \\ & \frac{\Gamma(c)\Gamma(b-a)}{\Gamma(b)\Gamma(c-a)} (-t)^{-a} F(a, a+1-c, a+1-b; 1/t) + \\ & \frac{\Gamma(c)\Gamma(a-b)}{\Gamma(a)\Gamma(c-b)} (-t)^{-b} F(b, b+1-c, b+1-a; 1/t). \end{aligned}$$

One can also easily differentiate each of these formulas to give expressions for $F'(a, b, c; t)$. Combining these with the Pfaff's formula

$$F(a, b, c; t) = (1-t)^{-a} F(a, c-b, c; t/(t-1)) = (1-t)^{c-a-b} F(c-a, c-b, c; t)$$

from [2, (2.2.6)] we obtain series for each $w(t) \in W$.

Algorithm 5.2.7. Let $t \in \mathbb{C}$. This algorithm computes $F_t, F_t' \in \mathbb{C}$ such that $F_t \approx F(a, b, c; t)$ and $F_t' \approx F'(a, b, c; t)$.

1. [Find $w(t)$] Let w, t_0 be such that $|w(t) - t_0|$ is minimal among $w(t) \in W$ and $t_0 \in \{0, (1 + i)/2\}$.

2. [Apply cases] Apply the appropriate transformation in the above, and compute using Algorithm 5.2.5.

The algorithm

Putting all of these elements together, we are now prepared to exhibit a solution to Problem 5.2.1.

Algorithm 5.2.8. Let $z \in \mathfrak{H}$ and Γ be a compact triangle group. This algorithm computes the value of $j(z) \in \mathbb{P}^1(\mathbb{C})$.

1. [Reduce to fundamental domain] Run Algorithm 5.2.2 and replace z by an element in its Γ-orbit which is also in the fundamental domain for Γ. If z is not in the fundamental triangle, replace z by its reflection about the geodesic between z_p and z_r, and apply complex conjugation to the final value obtained below.

2. [Find s] Compute the values $t = \psi_\tau(z)$ for each elliptic point τ. Let s be p, q, r depending on the smallest value $|t|, |1-t|, |1/t|$. Let $w = (z - z_s)/(z - \overline{z_s})$. Let u_0 be the value of $t^{1/s}$ which is closest in absolute value to w.

3. [Newton iteration] Apply Newton's method to the equation

$$f(u) = c_\tau u F_1(u^s) - w F_2(u^s) = 0,$$

i.e. let

$$u_{i+1} = u_i - \frac{f(u_i)}{f'(u_i)},$$

using the approximation $f(u_i)$

$$F_i(u_i^s) \approx F_i(u_0^s) + F_i'(u_0^s)(u_i^s - u_0^s) + \cdots + F_i^{(j)}(u_0^s)(u_i^s - u_0^s)^j,$$

with the values $F_i^{(j)}$ given by the recursive formula as in Algorithm 5.2.4. If the values u_i are convergent, compute these up to a machine epsilon and repeat this step with u_0 initialized to the convergent value until $f(u_0)$ is smaller than machine epsilon and go to Step 5; otherwise, go to Step 4.

4. [Numerical instability] Find a Taylor expansion for F_1, F_2 around u_0, and use a root-finding technique to find the root of $f(u) = 0$ closest to u_0, such as those in [44, Chapter 9].

5. [Output] If $s = p$, output u_0^p; if $s = q$, output $1 - u_0^q$; if $s = r$, output $1/u_0^r$.

5.3 CM points and Shimura reciprocity

In this section, we define CM points on Shimura curves, which are special points defined over certain abelian extensions. We also show how to explicitly compute these points for the case of Shimura curves coming from compact triangle groups.

Throughout this section, we let Γ be a compact arithmetic triangle group, which arises from a maximal order $\mathcal{O}$ of an indefinite quaternion algebra A which satisfies the Eichler condition defined over a totally real field F with strict class number 1. By Proposition 4.4.3, we know that every right ideal of $\mathcal{O}$ is principal.

First, we will have need to classify quadratic orders over $\mathbb{Z}_F$. A quadratic extension K of F is given by Kummer theory as $K = F(\sqrt{D})$ for an element $D \in K^*$; two such fields are isomorphic if and only if $D_1/D_2 \in F^{*2}$, and therefore the quadratic field extensions of F are classified by the group F^*/F^{*2} (see [10, §9.2.2]). A *quadratic order* over $\mathbb{Z}_F$ is a $\mathbb{Z}_F$-algebra which is a domain and a projective $\mathbb{Z}_F$-module of rank 2. Since F has class number one, each such quadratic order is equal as a $\mathbb{Z}_F$-module to $\mathbb{Z}_F \cdot 1 \oplus \mathbb{Z}_F \delta$ for some $\delta \in \mathbb{Z}_K$; the discriminant $D \in \mathbb{Z}_F$ of a minimal polynomial for δ is independent of δ up to an element of $\mathbb{Z}_F^{*2}$. Therefore the set of quadratic orders over $\mathbb{Z}_F$ is in bijection with the set of orbits of

$$\{D \in \mathbb{Z}_F : D \text{ is not a square, } D \text{ is a square modulo } 4\mathbb{Z}_F\}$$

under the action of multiplication by $\mathbb{Z}_F^{*2}$. We denote the order of discriminant D by O_D. Each such order is contained in a unique maximal order of discriminant d, known as the *fundamental* *discriminant*, with $D = df^2$ for some $f \in \mathbb{Z}_F$ unique up to $\mathbb{Z}_F^*$. We say that a quadratic order is *totally imaginary* if its field of fractions is a totally imaginary extension of F; the order O_D is totally imaginary if and only if D is totally negative.

Algorithm 5.3.1. Let O_D be a quadratic order over $\mathbb{Z}_F$, and let $D = df^2$. This algorithm computes a set of ideals $C = \{\mathfrak{a} \subset O_D\}$ which form a set of representatives for the ideal classes in the set $\mathrm{Cl}(O_d)$.

1. [Compute $\mathrm{Cl}(\mathbb{Z}_K)$] Compute $\mathbb{Z}_K$. Using Algorithm [9, 6.5.9] (or the methods of [10, §7.3]), compute the class group $\mathrm{Cl}\,\mathbb{Z}_K$ and a set of ideals $\mathfrak{a}$ representing the ideal classes of $\mathrm{Cl}\,\mathbb{Z}_K$ relatively prime to (f).

2. [Compute kernel] Compute a representative set α of elements in the group
$$\frac{(\mathbb{Z}_K/f\mathbb{Z}_K)^*}{\mathbb{Z}_K^*(\mathbb{Z}_F/f\mathbb{Z}_F)^*}.$$

3. [Output] Output the set of products $\alpha(\mathfrak{a}\cap O_D)$, the intersection computed by linear algebra.

Proof. We have an exact sequence
$$1 \to O_D^* \to \mathbb{Z}_K^* \to \frac{(\mathbb{Z}_K/f\mathbb{Z}_K)^*}{(\mathbb{Z}_F/f\mathbb{Z}_F)^*} \to \mathrm{Cl}\,O_D \to \mathrm{Cl}\,\mathbb{Z}_K \to 1$$
with the natural maps, and therefore we have an exact sequence
$$1 \to \frac{(\mathbb{Z}_K/f\mathbb{Z}_K)^*}{\mathbb{Z}_K^*(\mathbb{Z}_F/f\mathbb{Z}_F)^*} \to \mathrm{Cl}\,O_D \to \mathrm{Cl}\,\mathbb{Z}_K \to 1.$$
One computes a representative set of elements of $\mathrm{Cl}\,O_D$ as cosets of $\mathrm{Cl}\,\mathbb{Z}_K$. □

Remark 5.3.2. For the sake of efficiency, it makes sense to output just the set of ideals and elements, and allow the user to reconstruct the products. Note also that from this set of elements, one can reconstruct the structure of $\mathrm{Cl}\,O_D$ as an abelian group. Given a description of the left and right groups as abstract abelian groups, one can test each elementary abelian factor at a time to see if the sequence splits.

Let O_D be a totally imaginary quadratic order with field of fractions $K = F(\sqrt{D})$. Suppose that K splits A. Then there exists an embedding $\iota_K : K \hookrightarrow A$; more concretely, the map ι_K is given by an element $\mu \in \mathcal{O}$ whose minimal polynomial over F has discriminant D. Any two such embeddings are conjugate under an element of A^* by the theorem of Skolem-Noether [45, 7.21], so by conjugation, we may assume that $\iota_K(K) \cap \mathcal{O} = O_D$; we call such an embedding an *optimal embedding* (see [14]). Let $z = z_D$ be the unique fixed point of $\iota_K(K^*)$ in $\mathfrak{H}$, or equivalently the fixed point of $\iota_\infty(\mu)$ in $\mathfrak{H}$; we say z is a *CM point* on $\mathfrak{H}$, and $j(z)$ is a *CM point* on $X(1)$.

By class field theory, we have the Artin isomorphism

$$\mathrm{Cl}(O_D) \xrightarrow{\sim} \mathrm{Gal}(H_{(f)}/K)$$

$$[\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}$$

for all primes $\mathfrak{p}$ of K unramified in $H_{(f)}$, where $\mathrm{Cl}(O_D)$ is the group of invertible fractional ideals of O_D modulo principal ideals, and $H_{(f)}$ is the ring class field of K of conductor f.

Let $\mathfrak{c} \subset K$ be a fractional ideal of K, with $\mathfrak{c} \leftrightarrow \sigma$ under the Artin map. Then by assumption, we have

$$\iota_K(\mathfrak{c})\mathcal{O}_A = \xi\mathcal{O}_A$$

for some $\xi \in A$. From this data, we can describe the action of $\mathrm{Gal}(H_{(f)}/K)$ on $j(z)$ as follows.

Theorem 5.3.3 ([51, Shimura reciprocity law, p. 59]). *Let z_D be a CM point corresponding an order O_D with $D = df^2$. Then we have*

$$j(z) \in X(1)(H_{(f)})$$

and

$$j(z)^\sigma = j(\iota_\infty(\xi^{-1})(z)).$$

With this theorem in hand, we can use the Algorithms of §4 to compute all of the conjugates $j(z)$ under $\mathrm{Gal}(H_{(f)}/K)$.

Algorithm 5.3.4. Let O_D be a totally imaginary quadratic order over $\mathbb{Z}_F$ with field of fractions K, and let $\iota_K : O_D \hookrightarrow \mathcal{O}$ be an optimal embedding. This algorithm computes the set

$$\{j(z_D)^\sigma : \sigma \in \mathrm{Gal}(H_D/K)\} \subset \mathbb{C}.$$

1. [Compute representatives for the ring class group] By Algorithm 5.3.1, find a set G of ideals in bijection with the ring class group $\mathrm{Cl}\, O_D$.

2. [Principalize] Using Algorithm 4.4.6, for each ideal $\mathfrak{c} \in G$, find an element $\xi \in \mathcal{O}$ such that $\mathfrak{c}\mathcal{O} = \xi\mathcal{O}$.

3. [Find conjugates] Let z_D be the fixed point in $\mathfrak{H}$ of $\mu = \iota_K(K^*)$. For each ξ, compute $\iota_\infty(\xi^{-1})(z_D)$.

4. [Find j-values] For each such conjugate z, compute $j(z)$ by Algorithm 5.2.1 and output this set.

Given a complete set of conjugates t^σ of a purported algebraic number t, we can compute the polynomial

$$f(x) = \prod_{\sigma \in G} (x - t^\sigma)$$

and attempt to recognize the coefficients of this polynomial as elements of F using LLL (see [9, §2.7.2]). In fact, we will see in the next section that in certain circumstances these coefficients are rational numbers, in which case we may use the method of continued fraction expansion [9, §10.1].

5.4 Examples and applications

To test our methods, we have implemented the above algorithms for a specific example; we choose the class XI from [56]. Let F be the totally real subfield of $\mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive ninth root of unity. Then $[F : \mathbb{Q}] = 3$, and $\mathbb{Z}_F = \mathbb{Z}[b]$, where $b = -(\zeta_9 + 1/\zeta_9)$, satisfying $b^3 - 3b + 1 = 0$, and $d(F/\mathbb{Q}) = 3^4$. The number field F has strict class number 1. We choose the unique real place σ for which $\sigma(b) > 0$, and we let A be the quaternion algebra which is ramified at the other two real places and is unramified elsewhere, so that in particular it is unramified at every finite place. By Takeuchi [56, Proposition 2], we easily compute that $A \cong \left(\dfrac{-3, b}{F}\right)$.

We fix the isomorphism $\iota_\infty : A \otimes_F \mathbb{R} \cong M_2(\mathbb{R})$ as in Example 4.1.3, given explicitly as

$$\alpha \mapsto \begin{pmatrix} 0 & 3 \\ -1 & 0 \end{pmatrix} \qquad \beta \mapsto \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}.$$

By Algorithm 4.3.8, we can compute a maximal order $\mathcal{O}$ of A; since F has class number 1, we may represent $\mathcal{O}$ as a free $\mathbb{Z}_F$-module. More specifically, we note that $K = F(\alpha) = F(\sqrt{-3}) = \mathbb{Q}(\zeta_9)$ has ring of integers $\mathbb{Z}_K = \mathbb{Z}[\zeta_9]$, and hence we have the integral element $\zeta \in A$ satisfying $\zeta^9 = 1$. Extending this to a maximal order, we have

$$\mathcal{O} = \mathbb{Z}_F \oplus \mathbb{Z}_F\zeta \oplus \mathbb{Z}_F\omega \oplus \mathbb{Z}_F\eta,$$

where

$$\begin{aligned} \zeta &= -\frac{1}{2}b + \frac{1}{6}(2b^2 - b - 4)\alpha \\ \omega &= -b + \frac{1}{3}(b^2 - 1)\alpha - b\beta + \frac{1}{3}(b^2 - 1)\alpha\beta \\ \eta &= -\frac{1}{2}b\beta + \frac{1}{6}(2b^2 - b - 4)\alpha\beta. \end{aligned}$$

These elements have minimal polynomials

$$\zeta^2 + b\zeta + 1 = 0, \quad \omega^2 + 2b\omega + b^2 - 4b - 1 = 0, \quad \eta^2 - b = 0.$$

From [56, Table (3)], we know that $\Gamma = \mathcal{O}_1^*/\{\pm 1\}$ is a triangle group with signature $(2,3,9)$. Explicitly, we find the elements

$$s_p = b + \omega - 2\eta, \quad s_q = -1 + (b^2-3)\zeta + (-2b^2+6)\omega + (b^2+b-3)\eta, \quad s_r = -\zeta$$

with $s_p, s_q, s_r \in \mathcal{O}_1^*$ and satisfying the relations

$$s_p^p = s_q^q = s_r^r = s_p s_q s_r = 1$$

in $\mathcal{O}_1^*/\{\pm 1\}$; therefore by §5.1, the elliptic elements s_p, s_q, s_r generate Γ. The fixed points of these elements are $z_p = 0.395526\ldots i$, $z_q = -0.153515\ldots + 0.364518\ldots i$, and $z_r = i$, and they form the vertices of a fundamental triangle. This is shown in Figure 5.4: any shaded (or unshaded) triangle is a fundamental triangle for Γ, and the union of any shaded and unshaded triangle forms a fundamental domain for Γ.

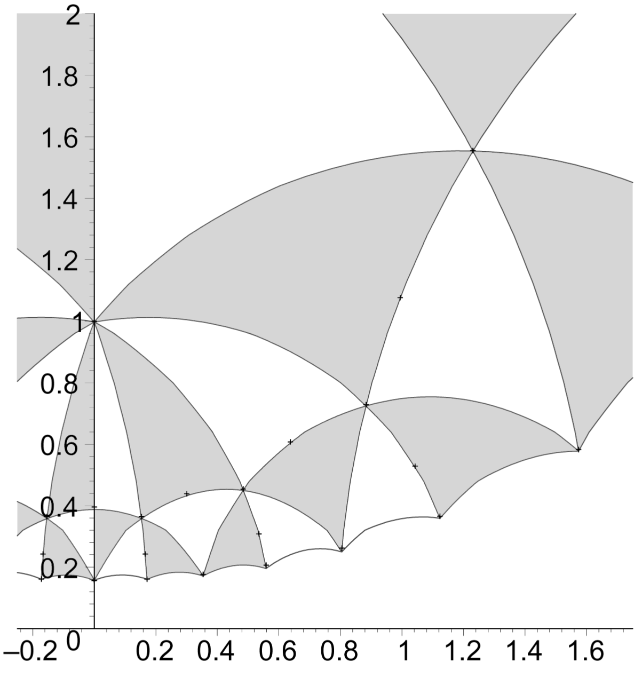

Figure 5.4: The translates of a fundamental triangle for $\Gamma(1)$

By exhaustively listing elements of $\mathcal{O}$, we find a host of optimal embeddings $\iota_K : K \hookrightarrow \mathcal{O}$ for orders with small norm and having small class number. Using the preceding algorithms, we compute the CM points for these orders, and the results are listed in Tables 1–6. There seems to be a history of computing such tables (e.g. [22, pp. 193–194]), and we are happy to make our own contribution.

Example 5.4.1. Let $K = F(\sqrt{-7})$. Let $\mu \in \mathcal{O}$ have minimal polynomial $x^2 - x + 2$, explicitly

$$\mu = (-b^2 - b + 2) + (-b^2 + 2b + 5)\zeta + (2b^2 - 2b - 8)\omega + (3b + 6)\eta.$$

The fixed point of $\iota_\infty(\mu)$ in $\mathfrak{H}$ is $-0.32\ldots + 0.14\ldots i$, which is Γ-equivalent to $z = 0.758\ldots i$, and $j(z) = -9594.703125000\ldots$ which agrees with

$$\frac{-614061}{64} = \frac{-3^5 7^1 19^2}{2^6}$$

to the precision computed.

Example 5.4.2. Now take $K = F(\sqrt{-2})$, with class number 3. We find $\mu \in \mathcal{O}$ satisfying $\mu^2 + 2 = 0$; explicitly,

$$\mu = (-b^2 - b + 1) + (-2b^2 + 2)\zeta + (2b^2 - b - 5)\omega + (-b^2 + b + 1)\eta.$$

We find the CM point $j(z) = 17137.97378464\ldots$ and its conjugates $0.583420177\ldots \pm 0.4516054442\ldots i$. We now identify the minimal polynomial and simplify the resulting number field. Let c be the real root of $x^3 - 3x + 10$; the number field $\mathbb{Q}(c)$ has discriminant $2^3 3^4$. Then $H = K(c)$, and in fact $j(z)$ agrees with

$$\frac{4015647c^2 - 10491165c + 15369346}{4096}$$

to the precision computed, and we recognize the conjugates as

$$-\frac{4015647c^2 - 10491165c - 54832574}{8192} \pm \frac{-3821175c^2 - 7058934c + 7642350}{4096}\sqrt{-2}.$$

The product of these three conjugates is the rational number

$$\frac{7^2 71^2 199^2}{2^{20}}.$$

Once one has a CM point as a purported algebraic number, it is not clear how to prove directly that such an identification is correct! What one really needs in this situation is a GZ-formula as in [22], which would identify the set of primes dividing the norm of $j(z) - j(z')$ for CM points z, z'. This is already listed as an open problem in [15, p. 42]. There has been a certain amount of work in this direction on the Arakelov geometry of Shimura curves, but this work has focused on the case of quaternion algebras over $\mathbb{Q}$, such as [46], [66], [32]; a nice formulation for the more general case of compact triangle groups seems to be in order. It is hoped that the data computed in this thesis will be useful in proving such theorems and suggesting further avenues of research.

In some cases, we can actually prove the correctness of these points by computing the canonical polynomial for the curve $X_0(\mathfrak{N})$, as follows.

First, an element $\alpha \in A^*/F^*$ which normalizes $\Gamma_0(\mathfrak{N})$ in A^*/F^* gives an element of $\mathrm{Aut}(\Gamma_0(\mathfrak{N}))$. We have such an element denoted $w_{\mathfrak{N}} \in \mathrm{Aut}(\Gamma_0(\mathfrak{N}))$, known by analogy as an *Atkin-Lehner* involution, defined to be a normalizing element $\alpha \in \mathcal{O}$ of trace zero and norm satisfying

$$\mathrm{nrd}(\alpha)\mathbb{Z}_{F,\mathfrak{N}} = \mathfrak{N},$$

in which case we say α is a *uniformizer* at $\mathfrak{N}$ (equivalently, $\mathrm{nrd}(\alpha)$ has the same valuation at all primes $\mathfrak{p} \mid \mathfrak{N}$ as $\mathfrak{N}$). For any uniformizer N at $\mathfrak{N}$ with $N < 0$, an element whose image in $M_2(\mathbb{Z}_{F,\mathfrak{N}})$ is

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

is an representative for $w_{\mathfrak{N}}$. It is easy to check as in the case of modular curves that such an element indeed normalizes $\Gamma_0(\mathfrak{N})$, and since $\alpha^2 \in \mathbb{Z}_F$, it acts as an involution on $X_0(\mathfrak{N})$.

Such an element of $\mathcal{O}$ always exists because we can find a uniformizer N which is totally negative and whose discriminant is not divisible by any prime which ramifies in A, therefore we may find an optimal embedding of the field $K(\sqrt{N})$. The set of elements of $\mathcal{O}$ map surjectively onto $M_2(\mathbb{F}_{\mathfrak{N}})$, and therefore we may conjugate an element $\alpha \in \mathcal{O}$ satisfying $\alpha^2 = N$ to also be upper triangular modulo $\mathfrak{N}$. Automatically, then, such an element will also be nilpotent as well (looking at valuations, the diagonal must also be in $\mathfrak{N}$).

We will fix for the rest of this section such an optimal embedding $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$, which can be computed as follows.

Algorithm 5.4.3. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$. This algorithm computes an embedding $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$.

1. [Find embeddings] For each prime $\mathfrak{p} \mid \mathfrak{N}$, by enumeration find an element $\alpha \in A$ such that the minimal polynomial of α modulo $\mathfrak{p}$ has a root a and such that α is primitive. Call Algorithm 4.2.7 with $\alpha - a$ to find an optimal embedding $\mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{p}})$.

2. [CRT] Use the Chinese remainder theorem to give a map $\mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$.

Algorithm 5.4.4. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$, and let $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$ be an embedding. This algorithm outputs a representative for $w_{\mathfrak{N}}$.

1. [Embed] Use the generators for $\mathcal{O}_1^*$ to find a surjective map $\mathcal{O}_1^* \to SL_2(\mathbb{F}_{\mathfrak{N}})$.

2. [Compute uniformizer] Run Step 3 of Algorithm 4.4.6 on the lattice $\mathcal{O}^0$ of trace zero elements; by enumeration, find an element $\omega \in \mathcal{O}$ such that $\omega^2 = N$, where N is a totally negative uniformizer for $\mathfrak{N}$.

3. [Conjugate] Let v be an element in the nullspace of the image of $\iota_{\mathfrak{N}}(\omega)$ in $M_2(\mathbb{F}_{\mathfrak{N}})$, and extend this to a basis v, w of $\mathbb{Z}_F/\mathfrak{N}^2$ such that the matrix whose columns are v, w has determinant 1 (mod $\mathfrak{N}$). Using $\iota_{\mathfrak{N}}$, find an element ν of $\mathcal{O}_1^*$ which maps to this matrix. Output $\nu^{-1}\omega\nu$.

Therefore we have the functions $j(z), j(w_{\mathfrak{N}}(z)) : \Gamma_0(\mathfrak{N})\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$; putting them together gives an morphism

$$\Gamma_0(\mathfrak{N})\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}.$$

The image will be a closed subvariety of dimension 1, and in the open affine set $\mathbb{A}^1_{\mathbb{C}} \times \mathbb{A}^1_{\mathbb{C}}$ removing ∞ it is described by a polynomial $\Phi_{\mathfrak{N}}(x, y)$. This polynomial has the property that $\Phi_{\mathfrak{N}}(y, x) = \Phi_{\mathfrak{N}}(x, y)$ since $w_{\mathfrak{N}}$ is an involution. The map is birational because the largest subgroup of $\Gamma(1)$ which is normalized by $w_{\mathfrak{N}}$ is the subgroup $\Gamma_0(\mathfrak{N})$. The map $X_0(\mathfrak{N}) \to X(1)$ is the map $(x, y) \mapsto x$; the degree of this map is $d = [\Gamma(1) : \Gamma_0(\mathfrak{N})]$, therefore by symmetry $\Phi_{\mathfrak{N}}(x, y)$ is a symmetric polynomial of degree d in both x and y. Now the map $j : X_0(\mathfrak{N}) \to X(1)$ is defined over F, and $w_{\mathfrak{N}}$ is an F-automorphism of $X_0(\mathfrak{N})$, so the image is exactly the base extension of the map $X_0(\mathfrak{N}) \to \mathbb{P}^1_F \times \mathbb{P}^1_F$ to $\mathbb{C}$, and hence the image is defined over F. By Proposition 5.1.2, if $\mathfrak{N}^\sigma = \mathfrak{N}$, then this polynomial has coefficients in $\mathbb{Q}$, not just F. This Galois descent also implies the following.

Proposition 5.4.5. *Let $j(z)$ be a CM point on $X(1)$ which comes from an order O_D with the property that $O_D^\sigma = O_D$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, where $K = F(\sqrt{D})$. Then $j(z)$ is fixed by $\mathrm{Gal}(F/\mathbb{Q})$.*

Proof. Let N be an odd rational prime which splits in F and such that a prime above N is principal in O_D; infinitely many such integers exist by the Chebotarev density theorem. Let $O_D = \mathbb{Z}_F[\mu]$. Then there exists an element w of trace zero and norm $4N$ in O_D; its image $w_N = \iota_K(\mu) \in \mathcal{O}$ is an Atkin-Lehner involution. We note that μ commutes with w_N, so $z = w_N(z)$, and hence $j(z) = j(w_N z)$. Therefore $j(z)$ is a root of the polynomial $\Phi_N(x, x)$. By Proposition 5.1.2, the polynomial $\Phi_N(x, x)$ has coefficients in $\mathbb{Q}$. Comparing degrees, we see that $j(z)^\sigma = j(z)$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. □

Therefore we have $\Phi_{\mathfrak{N}}(x, y) \in F[x, y]$ or even $\Phi_{\mathfrak{N}}(x, y) \in \mathbb{Q}[x, y]$. Moreover, we see from the corresponding properties of j that a projective, nonsingular model of this curve is a canonical model for $X_0(\mathfrak{N})$; we therefore call $\Phi_{\mathfrak{N}}(x,y)$ the *canonical polynomial* for $\mathfrak{N}$.

We note that $\Phi_{\mathfrak{N}}(j(z),j(z))=0$ if and only if $j(z)=j(w_{\mathfrak{N}}z)$; if z is not an elliptic point of $\Gamma(1)$, then this can happen if and only if $w_{\mathfrak{N}}z=\gamma z$ for some $\gamma\in\Gamma(1)$, i.e. the element $\mu=w_{\mathfrak{N}}\gamma\in\mathcal{O}$ fixes z. Since z is the fixed point of an element $\mu\in\mathcal{O}$, we know that the discriminant of the minimal polynomial for μ is negative at the identity real place; since also $F(\mu)\hookrightarrow A$, we know that $F(\mu)$ must be a totally imaginary extension of F, therefore z is by definition a CM point of discriminant equal to the discriminant of μ. Therefore if we are *given* the polynomial $\Phi_{\mathfrak{N}}(x,y)$, we can find provably correct values for the CM points by the roots of $\Phi_{\mathfrak{N}}(x,x)$, and recover its discriminant by the element μ.

We now give an algorithm to compute the polynomial $\Phi_{\mathfrak{N}}(x,y)$. We will first need the following algorithm.

Algorithm 5.4.6. Let $\mu\in\mathcal{O}$, and suppose that the minimal polynomial $f(x)$ of μ modulo $\mathfrak{N}$ has a root $m\in\mathbb{Z}_F/\mathfrak{N}$. This algorithm finds an element $\nu\in A$ such that $\nu^{-1}\mu\nu\in\mathcal{O}$ is upper triangular modulo $\mathfrak{N}$.

1. [Embed] Using Algorithm 5.4.3, compute an embedding $\iota_{\mathfrak{N}}:\mathcal{O}\hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}}$. Replace $\mathfrak{N}$ by $\mathfrak{N}$ divided by the ideal generated by the bottom-left element of $\iota_{\mathfrak{N}}(\mu)$. If this ideal is the unit ideal, μ is already upper-triangular in this embedding.

2. [Conjugate] If the new matrix is of the form $\begin{pmatrix} x & y \\ z & w\end{pmatrix}$, output an element $\nu\in\mathcal{O}$ of norm in $\mathfrak{N}$ which maps to
$$\begin{pmatrix} m-w & 1 \\ z & 0\end{pmatrix}.$$

Proof. This algorithm uses the root m to compute an eigenvector $(m-w,z)$ for the corresponding matrix; we easily check that conjugating by the given element gives an element which is upper-triangular. We note that $\nu^{-1}\mu\nu\in\mathcal{O}$, since this is a local property, and we have chosen ν so that this is true at $\mathfrak{N}$ and it is trivially true outside of $\mathfrak{N}$ if ν has norm $\mathfrak{N}$. □

We are now ready to exhibit an algorithm for computing the canonical polynomial $\Phi_{\mathfrak{N}}(x, y)$.

Algorithm 5.4.7. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ coprime to the discriminant of A; let $\mathcal{O}$ be a maximal order of A, and let $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$. This algorithm takes as input a library of CM points on $X(1)$ and outputs the canonical polynomial $\Phi_{\mathfrak{N}}(x, y)$ for $X_0(\mathfrak{N})$.

1. [Compute $w_{\mathfrak{N}}$] Using Algorithm 5.4.4, find a representative for $w_{\mathfrak{N}}$.

2. [Compute w-values] Let z be a CM point fixed by a primitive element $\mu \in \mathcal{O}$. Determine if the minimal polynomial of μ has a root modulo $\mathfrak{N}$ (by factorization or otherwise). If not, proceed to the next point. Otherwise, let m be a root, and use Algorithm 5.4.6 to find a conjugate of μ which is upper-triangular modulo $\mathfrak{N}$.

3. [Compute $j(wz)$] Run Algorithm 5.3.4 to compute its $\mathrm{Gal}(H/K)$-conjugates.

4. [Recognize] Recognize the minimal polynomials of each of these elements over F or $\mathbb{Q}$, depending as if $\mathfrak{N}^\sigma = \mathfrak{N}$ or not.

5. [Compositum] Find a field L (over F, $\mathbb{Q}$, respectively) of degree d, say, which splits both of these polynomials, and let $x, y \in L$ be the corresponding roots. Let θ be a primitive element for L.

6. [Add to matrix] Define a matrix M whose columns are numbered ij for $0 \leq i \leq j \leq d$. For each such ij, compute $z = x^j y^i + x^i y^j \in L$, and for $k = 0, \dots, d-1$, let the entry in row k and column ij of the matrix be the coefficient of the power of θ^k in z. If M has nullspace of dimension > 1, return to Step 2; otherwise, proceed to Step 7.

7. [Solve] Let v be the unique element in the nullspace of the matrix M. Return the polynomial obtained by the dot product of v with the vector whose ijth entry is $(x^j y^i + x^i y^j)$.

We have used this algorithm and the CM points computed above to compute the canonical polynomials $\Phi_{\mathfrak{N}}(x,y)$ for $N(\mathfrak{N}) \in \{3,8,9,17\}$, the four smallest norms. The first three can easily be recovered from known models for the curve $X_0(\mathfrak{N})$ computed by Elkies [16], [17]. The fourth is new and gives a curve of genus 1 without an obvious F-rational point, but after a choice of base point defined over some extension, CM points give rise to points on an elliptic curve defined over ring class extensions. Unfortunately, the polynomial $\Phi_{\mathfrak{N}}$ is much too large to fit in this thesis. One can verify that this polynomial is in fact correct by verifying that the monodromy group of the branched cover is correct, for which there exist effective algorithms (such as the command `monodromy` in Maple); by the Riemann existence theorem [61, Theorem 5.14], these data, together with the normalization for the branch points to occur at $0,1,\infty$, uniquely defines the cover $X_0(\mathfrak{N}) \to X(1)$.

Chapter 6

Tables

In the following tables, we list the results from the extended example in §5.4. Let F be the totally real subfield of $\mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive ninth root of unity. Then $[F:\mathbb{Q}] = 3$, and $\mathbb{Z}_F = \mathbb{Z}[b]$, where $b = -(\zeta_9 + 1/\zeta_9)$, satisfying $b^3 - 3b + 1 = 0$, and $d(F/\mathbb{Q}) = 3^4$. The number field F has strict class number 1. We choose the unique real place σ for which $\sigma(b) > 0$, and we let A be the quaternion algebra which is ramified at the other two real places and is unramified elsewhere, so that in particular it is unramified at every finite place. We obtain a Shimura curve $X(1)$ as in §5.1.

In Tables 6.1–6.2, we list ring class extensions (see §5.3). Let $D \in \mathbb{Z}_F$ be a totally imaginary discriminant such that $\sigma(D)/D \in \mathbb{Z}_F^{*2}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Then there is an order O_D in a number field K such that $[K:F] = 2$ and K is Galois over $\mathbb{Q}$. We list for the smallest such discriminants D a polynomial g which is a minimal polynomial for the ring class field $H_{(f)}$ of K of conductor f where $D = df^2$ and $d = \mathrm{disc}(K/F)$.

In Tables 6.3–6.4, we list factorizations of the norms of CM points on $X(1)$. For each discriminant D as in the preceding paragraph, there corresponds a CM point $z_D \in \mathbb{P}^1(H_{(f)})$. The

$-D$	$\lvert N(D)\rvert$	g
3	27	$\mathbb{Q}$
4	64	$\mathbb{Q}$
$4(b+2)$	192	$\mathbb{Q}$
$3(b-1)^2$	243	$\mathbb{Q}$
7	343	$\mathbb{Q}$
$5(b+2)$	375	x^2+x-1
8	512	$x^3-3x+10$
$4(b-1)^2$	576	x^2-3
11	1331	x^3+6x+1
$8(b+2)$	1536	x^2-2
12	1728	x^3-2
$9(b+2)$	2187	x^3+3
$7(b-1)^2$	3087	$x^4-2x^3+6x^2-5x+1$
15	3375	x^6+x^3-1
16	4096	$x^4-2x^3+6x^2-4x+2$
$8(b-1)^2$	4608	x^6-10x^3+1
$12(b+2)$	5184	x^6-4x^3+1
$13(b+2)$	6591	$x^4+x^3-x^2+x+1$
19	6859	$x^4+x^3+9x^2+2x+23$
20	8000	$x^6+9x^4+14x^3+9x^2+48x+44$
$11(b-1)^2$	11979	x^6-x^3-8

Table 6.1: Gal($F/\mathbb{Q}$)-stable CM Points on the $(2,3,9)$ Triangle Group (Number Fields, $|N(D)| < 12000$)

minimal polynomial of each such z_D over $\mathbb{Q}$ will have degree equal to $[H_{(f)} : K]$ by Proposition 5.4.5. We list the factorization of the numerator and denominator of the norm arising from that minimal polynomial.

In Tables 6.5–6.6, we repeat the above without assuming that D is Galois-stable, listing polynomials which generate ring class extensions and factorizations of the norms of CM points.

$-D$	$\lvert N(D)\rvert$	g
23	12167	$x^9 - 12x^7 - 11x^6 + 45x^5 + 84x^4 + 12x^3 - 99x^2 - 108x - 37$
$16(b+2)$	12288	$x^8 - 2x^7 + 10x^6 - 6x^5 + 12x^4 + 18x^3 + 6x^2 + 6x + 33$
24	13824	$x^6 - 2x^3 - 1$
$17(b+2)$	14739	$x^8 - x^7 + 2x^6 - 2x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$
$12(b-1)^2$	15552	$x^9 + 6x^3 + 2$
27	19683	$x^9 + 12x^6 - 6x^3 + 1$
$20(b+2)$	24000	$x^{14} - x^{13} - 2x^{12} + 19x^{11} - 37x^{10} - 122x^9 + 251x^8 + 211x^7$ $-589x^6 + 470x^5 - 41x^4 - 73x^3 + 22x^2 + 11x + 1$
$21(b+2)$	27783	$x^{12} - 6x^{11} + 21x^{10} - 39x^9 + 51x^8 - 36x^7$ $+30x^6 - 9x^4 - 6x^3 - 9x^2 - 3$
31	29791	$x^9 + 4x^7 + 3x^6 + 9x^5 + 13x^4 + 13x^3 + 15x^2 + 8x + 1$
$15(b-1)^2$	30375	$x^{18} + 15x^{15} + 48x^{12} + 48x^9 + 21x^6 - 3x^3 + 1$
$16(b-1)^2$	36864	$x^{16} + 8x^{13} + 12x^{12} + 24x^{10} + 96x^9 + 102x^8 + 80x^7 + 192x^6$ $+408x^5 + 508x^4 + 432x^3 + 264x^2 + 96x + 33$
$24(b+2)$	41472	$x^{18} - 6x^{17} + 15x^{16} - 42x^{15} + 177x^{14} - 546x^{13} + 1152x^{12}$ $-1986x^{11} + 3336x^{10} - 5578x^9 + 8355x^8 - 10236x^7 + 9840x^6$ $-7266x^5 + 4008x^4 - 1584x^3 + 435x^2 - 84x + 10$
36	46656	$x^{18} - 9x^{16} + 27x^{14} - 21x^{12} - 18x^8 + 45x^6 - 27x^4 + 36x^2 - 12$
$25(b+2)$	46875	$x^{14} + 2x^{13} - x^{12} - 7x^{11} + x^{10} + 16x^9 + 2x^8 - 26x^7$ $-2x^6 + 16x^5 - x^4 - 7x^3 + x^2 + 2x - 1$
40	64000	$x^{14} - 5x^{12} + 18x^{10} - 36x^8 + 51x^6 - 39x^4 + 19x^2 - 5$
$20(b-1)^2$	72000	$x^{12} + 14x^9 + 26x^6 - 86x^3 + 1$
$29(b+2)$	73167	$x^{18} - 5x^9 - 1$
$33(b+2)$	107811	$x^{18} + 6x^{17} + 27x^{16} + 102x^{15} + 375x^{14} + 1017x^{13} + 2610x^{12}$ $+6279x^{11} + 12438x^{10} + 21871x^9 + 35706x^8 + 48870x^7 + 50811x^6$ $+38829x^5 + 21717x^4 + 8964x^3 + 2748x^2 + 576x + 64$

Table 6.2: $\mathrm{Gal}(F/\mathbb{Q})$-stable CM Points on the $(2,3,9)$ Triangle Group (Number Fields, $|N(D)| > 12000$)

$-D$	Numerator	Denominator
3	1	1
4	0	1
$4(b+2)$	71^2	2^7
$3(b-1)^2$	-107^2	2^{15}
7	$-3^5 7^1 19^2$	2^6
$5(b+2)$	-179^2	2^{12}
8	$7^2 71^2 199^2$	2^{20}
$4(b-1)^2$	$-19^4 71^2$	2^{21}
11	$7^2 11^1 19^6 307^2 431^2$	$2^{30} 17^9$
$8(b+2)$	$-19^4 71^4 503^2$	$2^{21} 17^9$
12	$-11^2 71^2 503^2 971^2$	$2^{14} 17^9$
$9(b+2)$	$71^2 179^2 863^2 1511^2$	$2^{15} 17^9$
$7(b-1)^2$	$19^8 503^2 1259^2 2267^2$	$2^{24} 5^9 17^9$
15	$-7^4 11^2 127^4 359^2 431^2 1439^2$	$2^{36} 71^7$
16	$3^{14} 7^2 19^8 199^2$	$2^{21} 71^7$
$8(b-1)^2$	$-71^4 127^4 503^2 1871^2 3527^2$	$2^{21} 5^9 53^9$
$12(b+2)$	$19^{12} 71^2 163^4$	$2^{21} 107^5$
$13(b+2)$	$-19^8 179^2 307^4 467^2 647^2 1511^2 5147^2$	$2^{24} 3^9 53^9 107^9$
19	$3^{14} 19^4 71^4 107^4 3943^2$	$2^{45} 179^7$
20	$-11^2 19^{12} 71^2 199^2 379^2 739^2 2179^2 2339^2$ $4519^2 4751^2 5779^2$	$2^{38} 5^9 17^{18} 179^9$
$11(b-1)^2$	$-19^{12} 127^4 827^2 1223^2 1583^2 4787^2 7127^2$	$2^{39} 17^9 197^9$

Table 6.3: Gal($F/\mathbb{Q}$)-stable CM Points on the $(2,3,9)$ Triangle Group (Norms, $|N(D)| < 12000$)

$-D$	Numerator
23	$7^{6}11^{4}19^{18}23^{1}107^{4}251^{4}431^{2}631^{2}1747^{2}2719^{2}3671^{2}3943^{2}4231^{2}9199^{2}$
$16(b+2)$	$107^{4}503^{2}1871^{2}2447^{2}2591^{2}5903^{2}7919^{2}10079^{2}$
24	$-2^{2}19^{12}23^{2}71^{4}1871^{2}2447^{2}2591^{2}4751^{2}8783^{2}$
$17(b+2)$	$163^{4}199^{4}467^{2}863^{2}3671^{2}5147^{2}5903^{2}9791^{2}12239^{2}$
$12(b-1)^2$	$71^{2}107^{2}179^{4}251^{4}1619^{2}1871^{2}1907^{2}2339^{2}2699^{2}2843^{2}4787^{2}9719^{2}$
27	$11^{2}23^{2}71^{8}251^{2}359^{4}467^{2}683^{2}1583^{2}3851^{2}6011^{2}8423^{2}15551^{2}$
$20(b+2)$	$71^{8}127^{8}163^{4}179^{2}487^{4}971^{2}1619^{2}2591^{2}2699^{2}7451^{2}10079^{2}13859^{2}17099^{2}$
$21(b+2)$	$19^{24}199^{4}251^{4}467^{2}647^{4}2411^{2}3167^{2}3671^{2}4283^{2}10331^{2}12239^{2}13859^{2}$
31	$-3^{35}11^{4}31^{1}127^{2}179^{2}199^{4}863^{4}883^{2}$ $1171^{2}1511^{2}1531^{2}3547^{2}3943^{2}13879^{2}14923^{2}$
$15(b-1)^2$	$71^{3}127^{4}163^{8}251^{2}307^{4}359^{2}487^{4}523^{4}1063^{4}$ $1259^{2}1567^{4}2411^{2}2879^{2}21059^{2}26459^{2}$
$16(b-1)^2$	$19^{32}107^{4}127^{8}179^{4}251^{4}271^{4}307^{4}359^{4}631^{4}$
$24(b+2)$	$127^{4}271^{4}359^{4}487^{4}503^{2}631^{4}919^{4}2143^{4}2447^{2}$ $2591^{2}6047^{2}7559^{2}7919^{2}16487^{2}18287^{2}26711^{2}$
36	$7^{4}11^{2}19^{36}127^{8}199^{4}251^{4}271^{4}307^{4}431^{4}487^{4}503^{2}971^{2}$
$25(b+2)$	$107^{4}251^{2}503^{4}647^{4}1259^{2}1511^{2}3671^{2}4211^{2}9539^{2}$ $9791^{2}10331^{2}13499^{2}21599^{2}26711^{2}35999^{2}41399^{2}$
40	$3^{46}31^{2}107^{8}163^{4}199^{4}271^{4}307^{4}431^{4}467^{4}1871^{2}$ $2719^{2}2791^{2}3511^{2}7039^{2}15391^{2}50311^{2}$
$20(b-1)^2$	$19^{24}719^{4}971^{2}1871^{2}3779^{2}6011^{2}7559^{2}8171^{2}$ $9719^{2}29339^{2}30059^{2}30851^{2}32939^{2}55079^{2}$
$29(b+2)$	$19^{36}127^{4}179^{4}307^{4}379^{4}739^{4}1423^{4}2087^{2}2683^{4}3167^{2}$ $6427^{4}10151^{2}10331^{2}14327^{2}17387^{2}21599^{2}41399^{2}$
$33(b+2)$	$19^{36}107^{6}127^{4}359^{4}431^{4}503^{4}739^{4}1063^{4}5903^{2}7559^{2}8819^{2}9539^{2}$ $11483^{2}21599^{2}30203^{2}32507^{2}35999^{2}49499^{2}57527^{2}71711^{2}98207^{2}$

Table 6.4: $\mathrm{Gal}(F/\mathbb{Q})$-stable CM Points on the $(2,3,9)$ Triangle Group (Norms, $|N(d)| > 12000$, Numerators)

D	Denominator
23	$2^{54}5^{18}17^{27}53^{9}359^{9}$
$16(b+2)$	$2^{49}3^{18}17^{18}71^{3}$
24	$17^{9}89^{9}359^{9}$
$17(b+2)$	$2^{75}17^{18}251^{5}$
$12(b-1)^2$	$2^{63}5^{9}17^{27}53^{9}$
27	$2^{90}17^{27}107^{5}$
$20(b+2)$	$2^{84}5^{9}89^{9}269^{9}719^{9}$
$21(b+2)$	$2^{72}5^{9}17^{36}89^{9}719^{9}$
31	$2^{54}17^{27}53^{18}269^{9}$
$15(b-1)^2$	$2^{108}5^{9}11^{9}89^{9}179^{9}701^{9}$
$16(b-1)^2$	$2^{147}5^{9}53^{9}71^{10}431^{5}647^{9}$
$24(b+2)$	$2^{105}11^{9}71^{12}503^{7}971^{9}$
36	$2^{120}71^{3}107^{5}179^{5}863^{9}1511^{9}$
$25(b+2)$	$2^{120}5^{1}17^{36}71^{12}179^{5}$
40	$2^{124}17^{36}71^{10}359^{9}$
$20(b-1)^2$	$2^{42}11^{9}17^{18}71^{1}179^{5}359^{5}431^{9}1439^{9}$
$29(b+2)$	$2^{108}5^{18}53^{9}71^{6}107^{1}521^{9}683^{9}2141^{9}2267^{9}$
$33(b+2)$	$2^{219}17^{36}197^{9}233^{9}1097^{9}3527^{9}$

Table 6.4: $\mathrm{Gal}(F/\mathbb{Q})$-stable CM Points on the $(2,3,9)$ Triangle Group (Norms, $|N(d)| > 12000$, Denominators)

D	$\lvert N(D)\rvert$	g
$-5b^2+9b$	71	F
$-5b^2+b$	199	F
$8b^2-4b-27$	323	$x^2+(b^2-3)x-b^2+3$
$-3b^2+5b-3$	379	F
$7b^2+b-28$	503	$x^3+(-b^2+b+2)x+1$
$5b^2+2b-23$	523	F
$3b^2+b-16$	591	x^2-bx-1
$-8b^2+4b+1$	639	$x^2+(-b^2+b+3)x-b^2+1$
$-12b^2+16b+5$	699	$x^2+(-b^2+b+1)x-1$
$9b^2-3b-31$	739	F
$-4b^2+4b-3$	867	$x^2+(b^2-1)x+1$
b^2-12	971	$x^3+(b^2-1)x^2+(b^2-2)x-b^2+2$
$8b^2-31$	1007	$x^4+(-b^2+b+1)x^3+bx^2+(2b^2-4b-2)x-b^2+2b+1$
$-8b^2+12b$	1088	$x^4+(-b-1)x^3+(b^2+b-1)x^2+(-b^2-b+2)x+1$
$-4b-12$	1216	x^2-b
$-7b^2-3b-3$	1387	$x^2+(b^2-b-2)x-b+1$
$-4b^2+11b-10$	1791	$x^4+(b^2-b-1)x^3+(b^2-2b-2)x^2+(b^2-b-1)x+1$
$-11b^2+6b+1$	2179	$x^3+(b^2-b-2)x^2+(-b^2+2)x+b$
$-3b^2+4b-8$	2287	$x^3-x^2+(b^2-b-3)x-b^2+3$
$4b^2-23$	2719	$x^3+(-b^2+b+2)x^2+x-b$
$25b^2-12b-80$	3043	x^2-x-b
$-16b^2+24b+4$	3264	$x^4+(b-1)x^2+1$
$-b^2-7b-16$	3411	$x^4+(-3b^2+b+7)x^3+(-6b^2+2b+16)x^2$ $+(-4b^2+3b+15)x-2b^2-b+4$
$-3b^2+8b-12$	3583	$x^3+x^2+(-b^2+2)x-b-2$
$12b^2-4b-44$	3648	$x^4+(-b-1)x^2+1$
$-12b^2+8b$	4672	$x^4+(b^2+b-2)x^3+4x^2+(b^2+b-2)x+1$
$15b^2-11b-56$	4699	$x^4+(b^2+b)x^3+(-b^2+3b+8)x^2+(b^2+2b+1)x-b^2+b+4$
b^2-20	5779	$x^3+(-b^2+b+1)x^2+(b^2-2b-1)x+b$

Table 6.5: CM Points on the $(2,3,9)$ Triangle Group (Number Fields)

D	Numerator	Denominator
$-5b^2+9b$	$19^4 71^1$	2^{18}
$-5b^2+b$	$3^9 19^2 199^1$	2^{18}
$8b^2-4b-27$	$-19^6 107^2 163^4$	2^{45}
$-3b^2+5b-3$	$-3^9 19^4 127^2 379^1$	2^{45}
$7b^2+b-28$	$-19^6 107^2 127^6 271^2 307^2 503^1$	$2^{54} 17^9$
$5b^2+2b-23$	$-3^9 19^4 127^2 523^1$	17^9
$3b^2+b-16$	$19^8 107^2 251^2 359^2$	$2^{36} 17^9$
$-8b^2+4b+1$	$-19^8 71^2 107^2 179^2 251^2 431^2$	$2^{36} 17^9$
$-12b^2+16b+5$	$19^8 71^2 179^2 467^2$	2^{45}
$9b^2-3b-31$	$3^{15} 19^6 163^2 307^2 739^1$	$2^{45} 17^9$
$-4b^2+4b-3$	$-71^2 107^2 179^2 359^2 431^2 467^2$	$2^{45} 17^{10}$
b^2-12	$-19^{12} 127^2 179^2 199^2 251^2 271^2 487^4 971^1$	$2^{90} 17^9$
$8b^2-31$	$19^{12} 71^4 127^2 179^2 251^2 271^2 307^2 359^2 631^4$	$2^{72} 17^{18}$
$-8b^2+12b$	$-19^8 71^4 199^4 379^4 503^2 523^2 739^2$	$2^{63} 17^{18}$
$-4b-12$	$-3^{26} 19^2 71^2 199^4 379^2 523^2$	$2^{63} 17^9$
$-7b^2-3b-3$	$3^{26} 19^6 127^2 271^2 307^2$	$2^{45} 53^9$
$-4b^2+11b-10$	$19^8 71^2 107^2 163^4 431^2 467^2 683^2 719^2 1151^2 1187^2$	$2^{72} 17^9 53^9$
$-11b^2+6b+1$	$3^{33} 107^2 271^2 487^2 991^2 1063^2 2179^1$	$2^{45} 71^9$
$-3b^2+4b-8$	$-3^{33} 19^6 71^4 127^2 487^4 631^2 811^2 2287^1$	$2^{54} 17^{18} 53^9$
$4b^2-23$	$-3^{39} 19^{12} 163^2 179^2 631^2 1459^2 2719^1$	$2^{54} 17^9 53^9 71^5$
$25b^2-12b-80$	$3^{18} 19^8 71^2 127^2 163^2 179^2 251^2 271^2 631^2 811^2 1423^2 1783^2$	$2^{90} 53^9 89^9$
$-16b^2+24b+4$	$19^{16} 503^2 971^2 1619^2 1871^2 1907^2 2339^2 2591^2$	$2^{57} 17^9 53^9 71^1$
$-b^2-7b-16$	$19^{16} 251^4 359^2 467^2 1223^2 1259^2 1511^2 2087^2 2663^2$	$2^{45} 17^9 71^9 89^9$
$-3b^2+8b-12$	$3^{27} 19^{18} 199^2 271^2 487^2 1171^2 1531^2 2251^2 3583^1$	$2^{54} 17^9 53^{18} 71^5$
$12b^2-4b-44$	$19^{20} 71^4 127^4 503^4 971^2 1619^2 2447^2 2699^2 2843^2$	$2^{57} 3^9 17^{18} 53^9 89^9$
$-12b^2+8b$	$-3^4 619^8 379^4 523^2 739^2 2179^2 2503^2 2791^2$	$2^{63} 71^7 89^9 107^5$
$15b^2-11b-56$	$-3^{48} 7^6 19^8 107^4 127^2 179^6 199^2 631^2 1531^2$	$2^{90} 17^9 53^9 89^9$
b^2-20	$-3^{39} 19^{12} 107^2 307^2 359^2 1171^4 1279^2 3187^2 3331^2 5779^1$	$2^{45} 17^9 71^{18} 179^5$

Table 6.6: CM Points on the $(2,3,9)$ Triangle Group (Norms)

Bibliography

[1] Montserrat Alsina and Pilar Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM monograph series, vol. 22, AMS, Providence, 2004.

[2] George E. Andrews, Richard Askey, and Ranjan Roy, *Special functions*, Encyclopedia of mathematics and its applications, vol. 17, Cambridge University Press, Cambridge, 1999.

[3] Z.I. Borevich and I.R. Shafarevich, *Number theory*, Academic Press, New York, 1966.

[4] R.P. Brent and H.T. Kung, *Fast algorithms for manipulating formal power series*, J. ACM **25** (1978), no. 4, 581–595.

[5] J.A. Buchmann and H.W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260.

[6] J.W.S. Cassels and A. Fröhlich, eds., *Algebraic number theory*, Thompson Book Company, Washington, 1967.

[7] A.L. Chistov, *The complexity of the construction of the ring of integers of a global field*, Soviet Math. Dokl. **39** (1989), no. 3, 597–600.

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

[9] Henri Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[10] Henri Cohen, *Advanced topics in computational algebraic number theory*, Graduate texts in mathematics, vol. 193, Springer-Verlag, Berlin, 2000.

[11] 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.

[12] J.E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441.

[13] Harold Davenport, *Multiplicative number theory*, third ed., Graduate texts in mathematics, vol. 74, Springer-Verlag, New York, 2000.

[14] M. Eichler, *Über die Idealklassenzahl hypercomplexer Systeme*, Math. Z. **43** (1938), 481–494.

[15] Noam D. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 1–47.

[16] Noam D. Elkies, *Explicit modular towers*, Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997), T. Basar, A. Vardy, eds., 1998, 23–32, also available at `arXiV:math.NT/0103107`.

[17] Noam D. Elkies, *Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples*, preprint available at `arXiV:math.NT/0409020`.

[18] Lester R. Ford, *Automorphic functions*, McGraw-Hill, New York, 1929.

[19] Robert C. Forrey, *Computing the hypergeometric function*, J. Comp. Physics **137** (1997), 79–100.

[20] A. Fröhlich, *Local fields*, in *Algebraic number theory*, J.W.S. Cassels and A. Fröhlich, eds., Thompson Book Company, Washington, 1967, 1–41.

[21] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 2nd ed., Cambridge University Press, Cambridge, 2003.

[22] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[23] I.S. Gradshtein and I.M. Ryzhik, *Table of integrals, series, and products*, 6th ed., Alan Jeffrey ed., Academic Press, San Diego, 2000.

[24] Gábor Ivanyos and Lajos Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Comput. Complexity **3** (1993), 245–261.

[25] Robin Hartshorne, *Algebraic geometry*, Graduate texts in mathematics, vol. 52, Springer-Verlag, New York, 1977.

[26] Yasutaka Ihara, *Schwarzian equations*, J. Fac. Soc. Univ. Tokyo **21** (1974) 97–118.

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

[28] Gerald Janusz, *Algebraic number fields*, second ed., Graduate studies in mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[29] Stefan Johansson, *On fundamental domains of arithmetic Fuchsian groups*, Math. Comp **69** (2000), no. 229, 339–349.

[30] Svetlana Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.

[31] D. Kohel, Quaternion algebras, in *The MAGMA Handbook*, reference manual available at `http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.

[32] Stephen S. Kudla, Michael Rapoport, and Tonghai Yang, *Derivatives of Eisenstein series and Faltings heights*, Compos. Math. **140** (2004), no. 4, 887–951.

[33] T.Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate texts in mathematics, vol. 131, American Math. Soc., Providence, 2001.

[34] T.Y. Lam, *Introduction to quadratic forms over fields*, Graduate studies in mathematics, vol. 67, American Math. Soc., Providence, 2005.

[35] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate studies in mathematics, vol. 110, Berlin: Springer-Verlag, 1994.

[36] H.W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244.

[37] A.K. Lenstra, H.W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513–534.

[38] 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.

[39] C. MacLachlan and G. Rosenberger, *Two-generator arithmetic Fuchsian groups*, Math. Proc. Camb. Phil. Soc. **93** (1983), 383–391.

[40] C. MacLachlan and G. Rosenberger, *Two-generator arithmetic Fuchsian groups*, Math. Proc. Camb. Phil. Soc. **111** (1992), 7–24.

[41] M. Neher, *Improved validated bounds for Taylor coefficients and for Taylor remainder series*, J. Comp. Appl. Math. **152** (March 2003), no. 1, 393–404.

[42] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[43] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, 1997.

[44] William H. Press, et al., *Numerical recipes in C: the art of scientific computing*, 2nd ed., Cambridge University Press, Cambridge, 1992.

[45] I. Reiner, *Maximal orders*, Clarendon Press, Oxford, 2003.

[46] David Peter Roberts, *Shimura curves analogous to $X_0(N)$*, Harvard Ph.D. thesis, 1989.

[47] Lajos Rónyai, *Zero divisors in quaternion algebras*, J. Algorithms **9** (1988), 494–506.

[48] Lajos Rónyai, *Algorithmic properties of maximal orders in semisimple algebras over $\mathbb{Q}$*, Comput. Complexity **2** (1992), no. 3, 225–243.

[49] Lajor Rónyai, *Computing the structure of finite algebras*, J. Symbolic Computation **9** (1990), 355–373.

[50] J. P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.

[51] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.

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

[53] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, to appear in Math. Comp.

[54] Lucy Joan Slater, *Generalized hypergeometric functions*, Cambridge University Press, Cambridge, 1966.

[55] Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.

[56] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo **24** (1977) 201–212.

[57] Tikao Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. **21** (1951), 163–178.

[58] Joris van der Hoeven, *Relax, but don't be too lazy*, J. Symbolic Comput. **34** (2002), no. 6, 479–542.

[59] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.

[60] Helmut Völklein, *Rigid generators of classical groups*, Math. Ann. **311** (1998), 421–438.

[61] Helmut Völklein, *Groups as Galois groups: an introduction*, Cambridge studies in advanced mathematics, vol. 53, Cambridge University Press, New York, 1996.

[62] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[63] André Weil, *Basic number theory*, 3rd ed., Springer-Verlag, Berlin, 1974.

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

[65] Christiaan van de Woestijne, *Solving diagonal equations over finite fields*, Ph.D. thesis, Universiteit Leiden, in preparation.

[66] Shou-Wu Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290.