Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups

John Voight

Magma Group
Department of Mathematics and Statistics
University of Sydney, NSW 2006, Australia
jvoight@gmail.com

Abstract. Let $\Gamma \subset PSL_2(\mathbb{R})$ be a cocompact arithmetic triangle group, i.e. a Fuchsian triangle group that arises from the unit group of a quaternion algebra over a totally real number field. The group Γ acts on the upper half-plane $\mathfrak{H}$; the quotient $X_{\mathbb{C}} = \Gamma \backslash \mathfrak{H}$ is a Shimura curve, and there is a map $j : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. We algorithmically apply the Shimura reciprocity law to compute CM points $j(z_D) \in \mathbb{P}^1_{\mathbb{C}}$ and their Galois conjugates so as to recognize them as purported algebraic numbers. We conclude by giving some examples of how this method works in practice.

To motivate what follows, we begin with a description of the classical situation. The subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ of matrices which are upper triangular modulo $N \in \mathbb{Z}_{>0}$ acts on the completed upper half-plane $\mathfrak{H}^*$ by linear fractional transformations; the quotient $X_0(N)_{\mathbb{C}} = \Gamma_0(N) \setminus \mathfrak{H}^*$ can be given the structure of a compact Riemann surface. The complex curve $X_0(N)_{\mathbb{C}}$ itself is a moduli space for (generalized) elliptic curves equipped with a cyclic subgroup of order N, and consequently it has a model $X_0(N)_{\mathbb{Q}}$ defined over $\mathbb{Q}$. There exist "special" points on $X_0(N)_{\mathbb{Q}}$, known as *CM points*, where the corresponding elliptic curves have complex multiplication by quadratic imaginary fields K. CM points are defined over abelian extensions H of K, and the *Shimura reciprocity law* explicitly describes the action of the Galois group $\mathrm{Gal}(H/K)$ on them. The image of a CM point under the elliptic modular j-function is known as a *singular modulus*. Gross and Zagier give a formula for the norm of the difference of two singular moduli [6]; the traces of singular moduli arise as the coefficients of modular forms (see e.g. [18]).

In this article, we generalize this situation by replacing the modular curve $X_0(N)$ by a *Shimura curve* $X_0(\mathfrak{N})$, associated to a quaternion algebra defined over a totally real number field F. The curves $X_0(\mathfrak{N})$ we will consider similarly come equipped with a map $j : X_0(\mathfrak{N}) \to \mathbb{P}^1$ as well as CM points defined over abelian extensions H of totally imaginary extensions K of F. Developing ideas of Elkies [5], we can compute these points to high precision as complex numbers, and we generalize his methods by using the Shimura reciprocity law to recognize them as putative algebraic numbers by also computing their conjugates under $\mathrm{Gal}(H/K)$. We may then compute the norms, traces, and other information

about these CM points, with a view towards a generalized Gross-Zagier formula in this setting.

In §§1–2, we introduce the basic facts about quaternion algebras, Fuchsian groups and Shimura curves that we will use in the sequel. In §3, we outline numerical methods for computing the value of the map j to high precision—this can safely be skipped for the reader willing to accept Proposition 3.2. In §4, we treat the problem of principalization of ideals in maximal orders of quaternion algebras, and in Algorithm 4.4 we solve this problem under hypotheses that hold in our situation. In §5, we define CM points and show in Algorithm 5.2 how to compute these points as putative algebraic numbers using the Shimura reciprocity law. In §6, we briefly discuss relevant Galois descent. Finally, in §7, we give examples of how these algorithms work in practice, and in §8 we tabulate some of our results.

1 Quaternion algebras

In this section, we introduce quaternion algebras and describe some of their basic properties. A reference for the material in this section is [15]. Throughout, let F be a field with $\operatorname{char} F \neq 2$.

A *quaternion algebra* A over F is a central simple algebra of dimension 4 over F, or equivalently, an F-algebra with generators $\alpha, \beta \in A$ such that

$$\alpha^2 = a, \quad \beta^2 = b, \quad \alpha\beta = -\beta\alpha \tag{1}$$

with $a, b \in F^*$.

Example 1.1. The matrix ring $M_2(F)$ is a quaternion algebra over any field F, as is the division ring $\mathbb{H}$ of Hamiltonians over $\mathbb{R}$.

Let A be a quaternion algebra over F. Then A has a unique involution $^- : A \to A$ called *conjugation* such that $\theta + \overline{\theta}, \theta\overline{\theta} \in F$ for all $\theta \in A$, and we define the *reduced trace* and *reduced norm* of θ to be respectively $\operatorname{trd}(\theta) = \theta + \overline{\theta}$ and $\operatorname{nrd}(\theta) = \theta\overline{\theta}$. For A as in (1) and $\theta = x + y\alpha + z\beta + w\alpha\beta \in A$, we have

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

Let $K \supset F$ be a field containing F. Then $A_K = A \otimes_F K$ is a quaternion algebra over K, and we say K *splits* A if $A_K \cong M_2(K)$. If $[K : F] = 2$, then K splits A if and only if there exists an F-embedding $K \hookrightarrow A$.

Now let F denote a number field with ring of integers $\mathbb{Z}_F$. Let v be a non-complex place of F, and let F_v denote the completion of F at v. Then there is a unique quaternion algebra over F_v which is a division ring, up to isomorphism. We say A is *unramified* at v if F_v splits A otherwise say A is *ramified* at v. The algebra A is ramified at only finitely many places v, and we define the *discriminant* of A to be the ideal of $\mathbb{Z}_F$ given by the product of all finite ramified places of A.

A $\mathbb{Z}_F$-*lattice* of A is a finitely generated $\mathbb{Z}_F$-submodule I of A such 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.

2 Shimura curves arising from triangle groups

In this section we introduce Shimura curves and triangle groups; basic references are [7] and [5].

Let $\mathfrak{H}$ be the complex upper-half plane, equipped with the hyperbolic metric d. The group $PSL_2(\mathbb{R})$ isometrically acts on $\mathfrak{H}$ by linear fractional transformation. Let Γ be a *Fuchsian group*, a discrete subgroup of $PSL_2(\mathbb{R})$ such that the orbit space $X_{\mathbb{C}} = \Gamma\backslash\mathfrak{H}$ has finite hyperbolic area. The quotient space $X_{\mathbb{C}}$ can be given the structure of a Riemann surface of genus g.

The stabilizer $\Gamma_z = \{\gamma \in \Gamma : \gamma(z) = z\}$ of a point $z \in \mathfrak{H}$ is finite and cyclic; 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*. The set of Γ-orbits with nontrivial stabilizer is finite and in bijective correspondence with the set of elliptic cycles up to conjugation. Choosing a point $z_0 \in \mathfrak{H}$ not fixed by any element of $\Gamma \setminus \{1\}$, we obtain a fundamental domain for Γ given by

$$D = \{z \in \mathfrak{H} : d(z, z_0) \leq d(z, \gamma(z_0)) \text{ for all } \gamma \in \Gamma\}. \tag{2}$$

The domain D is a hyperbolic polygon, a connected, closed hyperbolically convex region bounded by a union of geodesics.

Now let F be a totally real number field with $[F : \mathbb{Q}] = n$ and let A be a quaternion algebra over F such that $A \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \times \mathbb{H}^{n-1}$. We fix the unique real place of F at which A is unramified and identify F as a subfield of $\mathbb{R}$ by this embedding; we also fix an isomorphism $\iota_\infty : A \otimes_F \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$. Let $\mathcal{O}$ be a maximal order in A (unique up to conjugation in A) and define the subgroup

$$\Gamma^*(1) = \{\iota_\infty(\gamma) : \gamma \in A,\ \gamma\mathcal{O} = \mathcal{O}\gamma,\ \mathrm{nrd}(\gamma) \text{ totally positive}\}/\{\pm 1\} \subset PSL_2(\mathbb{R}).$$

The group $\Gamma^*(1)$ is an *arithmetic* Fuchsian group, and as above it gives rise to a Riemann surface $X^*(1)_{\mathbb{C}} = \Gamma^*(1)\backslash\mathfrak{H}$.

An example of this situation is the modular group $\Gamma^*(1) = PSL_2(\mathbb{Z})$ with the usual fundamental domain, which corresponds to $F = \mathbb{Q}$ and $A = M_2(\mathbb{Q})$. We will exclude this well-studied case and assume from now on that A is a division ring, and thus the fundamental domain D and $X^*(1)_{\mathbb{C}}$ are compact.

Suppose that Γ has t elliptic cycles of order $m_1, \ldots, m_t$. Then the group Γ is freely generated by elements $a_1, b_1, \ldots, a_g, b_g, s_1, \ldots, s_t$ subject to the relations

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

where $[a, b] = aba^{-1}b^{-1}$; the group Γ is said to have *signature* $(g; m_1, \ldots, m_t)$. We further make the assumption that $\Gamma^*(1)$ is a *triangle group*, a Fuchsian group of signature $(0; p, q, r)$ with $p, q, r \in \mathbb{Z}_{\geq 2}$. Therefore we have a presentation

$$\Gamma^*(1) = \langle s_p, s_q, s_r | s_p^p = s_q^q = s_r^r = s_p s_q s_r = 1 \rangle. \tag{3}$$

The fundamental domain D is the union of a *fundamental triangle*, a hyperbolic triangle with angles $\pi/p, \pi/q, \pi/r$ and vertices z_p, z_q, z_r at the fixed points of the

generators s_p, s_q, s_r, respectively, together with its image in the reflection in the geodesic connecting any two of the vertices.

By assumption we have $g = 0$ and hence we have a map $j : X^*(1)_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, which is uniquely defined once we assert that the images of the elliptic points z_p, z_q, z_r be $0, 1, \infty$, respectively.

By [13], there are exactly 18 quaternion algebras A (up to isomorphism), defined over one of 13 totally real fields F, that give rise to such a cocompact arithmetic triangle group $\Gamma^*(1)$. (As pointed out in [5, p. 3], already these contain a number of highly interesting curves.) We note that each such F is Galois over $\mathbb{Q}$ and has class number 1; the fields $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\cos \pi/12)$, and $\mathbb{Q}(\cos \pi/15)$, arising from the classes IV, V, IX, XV, XVI, and XVII, have strict class number 2, the rest have strict class number 1.

3 Computing hypergeometric series

We continue notation from §§1–2. In this section, we address the following problem.

Problem 3.1. Given $z \in \mathfrak{H}$, compute the value $j(z) \in \mathbb{P}^1(\mathbb{C})$.

In other words, in Problem 3.1 we wish to compute the parametrization $j : \Gamma^*(1)\backslash\mathfrak{H} \to X^*(1)$ to large precision over $\mathbb{C}$. The reader who is uninterested in these numerical concerns may safely accept the following proposition and proceed to the next section.

Proposition 3.2. *There exists an explicit algorithm to solve Problem 3.1.*

For the details, we refer the reader to [5] and [17, §5.2].

We provide an outline of the proof of Proposition 3.2. In the first step, we reduce the problem to one in a neighborhood of an elliptic point. 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 then find $z' \in D$ in the Γ-orbit of z as follows.

Algorithm 3.3. For $z \in \mathfrak{H}$, this algorithm returns an element $z' \in D$ in the Γ-orbit of z.

1. Let z'_q be the image of z_q in the reflection of the geodesic $z_p z_r$.
2. Apply s_r to z until z is in the region R bounded by the geodesics $z_r z_q$ and $z_r z'_q$.
3. 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 2.

Proof. For the proof, we map $\mathfrak{H}$ conformally to the unit disc $\mathfrak{D}$ by the map $z \mapsto (z - z_r)/(z - \overline{z_r})$, which maps $z_r \mapsto 0$. The element s_r now acts by rotation on $\mathfrak{D}$ by $2\pi/r$ about the origin, and the image of R is a sector $S \subset \mathfrak{D}$ with central angle $2\pi/r$.

Since the center of rotation of s_p lies away from the origin, for $z \in S$ as in Step 3 we have $z \in D$ if and only if $|s_p^i z| \geq |z|$ for all $0 < i \leq p$. Thus we see that the algorithm terminates correctly, because we obtain in this way a Γ-orbit with strictly decreasing absolute value, and yet the group Γ acts discontinuously so this orbit is finite.

Since $j(z') = j(z)$, we replace z by z'. Now the point z is near to at least one elliptic point τ of Γ. We apply the linear fractional transformation

$$z \mapsto w = \frac{z - \tau}{z - \overline{\tau}}$$

which maps the upper half-plane $\mathfrak{H}$ to the open unit disc $\mathfrak{D}$ and maps $\tau \mapsto 0$. One easily recovers z from w as

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

Next, 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 the elliptic point τ of order s, there exists a Puiseux series $\phi_\tau(t) \in t^{1/s}\mathbb{C}[[t]]$ given as an explicit quotient of two hypergeometric series, 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 $w = \phi_\tau(t)$.

4 Principalization of ideals

In this section, we exhibit in Algorithm 4.4 a way to compute a generator for a principal (right) ideal of a maximal order $\mathcal{O}$ for a certain class of quaternion algebras A. Already, computing the class group and unit group of a number field appears to be a difficult task; consequently, we will be content to provide an effective algorithm that seems to work well in practice, as we are unable to prove any rigorous time bounds. We refer the reader to [15, §III.5] for the background relevant to this section.

Let A be a quaternion algebra defined over a number field F, and let $\mathcal{O} \subset A$ be a maximal order. Let I, J be right ideals of $\mathcal{O}$. We say that I and J are in the same *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 $\mathcal{O}$. Since A is non-commutative, the set of ideal classes may not form a group; however, the number h of ideal classes is finite and is independent of $\mathcal{O}$.

We are led to the following problem.

Problem 4.1. Given a right ideal $I \subset \mathcal{O}$, determine if I is a principal ideal and, if so, compute an an element α such that $I = \alpha\mathcal{O}$.

For applications to the situation of Shimura curves, we may assume that 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 4.2 ([9, Corollary 34.21], [15, 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* $\mathrm{Cl}\,\mathbb{Z}_F$.

In view of Proposition 4.2, the task identifying principal ideals in $\mathcal{O}$ is computationally equivalent to the analogous problem for F. From now on, suppose that F is a totally real field with $[F : \mathbb{Q}] = n$ and that A satisfies the Eichler condition.

Lemma 4.3. *Let $I \subset \mathcal{O}$ be a right ideal, and let $\xi \in I$. Then ξ generates I if and only if* $\mathrm{nrd}(\xi)\mathbb{Z}_F = \mathrm{nrd}(I)$*, which holds if and only if* $|N_{F/\mathbb{Q}}(\mathrm{nrd}(\xi))| = N_{F/\mathbb{Q}}(\mathrm{nrd}(I))$.

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 $\mathcal{O}/I$ as a $\mathcal{O}$-module (see [9, 24.1]), 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 [9, Theorem 24.11]. The second statement follows in the same way, now in the much easier context of Dedekind domains.

The following algorithm then gives a solution to Problem 4.1 under these hypotheses.

Algorithm 4.4 (Principal ideal testing). Let $I \subset \mathcal{O}$ be a right ideal. This algorithm determines if I is principal and outputs a generator for I if one exists.

1. Compute $\mathrm{nrd}(I) \subset \mathbb{Z}_F$. Test if $\mathrm{nrd}(I) \subset \mathbb{Z}_F$ is principal by [3, §6.5.10]. If not, output a message indicating that I is not principal and terminate the algorithm. Otherwise, let $q = N_{F/\mathbb{Q}}(\mathrm{nrd}(I))$.
2. Find a $\mathbb{Z}$-generating set for I and write these elements in a $\mathbb{Z}$-basis for $\mathcal{O}$. Using the MLLL algorithm [3, 2.6.8], find a $\mathbb{Z}$-basis $B = \gamma_1, \ldots, \gamma_{4n}$ for I.
3. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct real embeddings $F \hookrightarrow \mathbb{R}$. Embed $I \hookrightarrow \mathbb{R}^{4n}$ as a lattice L via the embedding

$$\mu \mapsto (\sigma_i(\mu_j))_{\substack{i=1,\ldots,n \\ j=1,\ldots,4}}$$

   where we write $\mu = \mu_1 + \mu_2\alpha + \mu_3\beta + \mu_4\alpha\beta$ for α, β as in (1). Compute an LLL-reduced basis L' of this lattice with respect to the ordinary inner product on $\mathbb{R}^{4n}$, 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. For each μ in the $\mathbb{Z}$-linear span of B', compute $\mathrm{nrd}(\mu)$. If $|N_{F/\mathbb{Q}}(\mathrm{nrd}(\mu))| = q$, output μ and terminate the algorithm.

The algorithm terminates correctly by Proposition 4.2 if I is not principal and by Lemma 4.3 (and sheer enumeration) if I is principal.

Remark 4.5. The LLL-step proves experimentally to be crucial. We can see this more precisely by the following statement: 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 satisfies

$$|N_{F/\mathbb{Q}}(\mathrm{nrd}(\gamma))| \leq C|N_{F/\mathbb{Q}}(\mathrm{nrd}(I))|.$$

Since any generator $\xi \in I$ has $N_{F/\mathbb{Q}}(\mathrm{nrd}(I)) = |N_{F/\mathbb{Q}}(\mathrm{nrd}(\xi))|$, we conclude that the algorithm produces elements which are very close to being generators. We refer the reader to [17, Proposition 4.4.9] for the proof and a discussion.

5 CM points and Shimura reciprocity

In this section, we define CM points and give methods for explicitly computing them. We continue notation from §§1–2.

We first classify quadratic orders over $\mathbb{Z}_F$. The quadratic extensions K of F are classified by Kummer theory as the fields $K = F(\sqrt{D})$ for $D \in F^*/F^{*2}$. 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. In our situation, F has class number 1, hence each such quadratic order is equal as a $\mathbb{Z}_F$-module to $\mathbb{Z}_F \oplus \mathbb{Z}_F\delta$ for some $\delta \in \mathbb{Z}_K$; the discriminant $D \in \mathbb{Z}_F$ of a minimal polynomial for δ is independent of the choice 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 $D \in \mathbb{Z}_F$ by O_D. Each such order is contained in a unique maximal order of discriminant d, known as the *fundamental discriminant*, with $D = df^2$ and $f \in \mathbb{Z}_F$ (unique up to $\mathbb{Z}_F^*$). We say that a quadratic order O_D is *totally imaginary* if D is totally negative.

Let O_D be a totally imaginary quadratic order of discriminant $D = df^2$ with field of fractions $K = F(\sqrt{d})$. Suppose that K is a splitting field for 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. We further assume that the embedding is *optimal*, so that $\iota_K(K) \cap \mathcal{O} = O_D$ (see [4]). Let $z = z_D$ be the fixed point of $\iota_K(\mu)$ in $\mathfrak{H}$; we then say z is a *CM point* on $\mathfrak{H}$, and $j(z)$ is a *CM point* on $\mathbb{P}^1(\mathbb{C})$.

Let H_D be the ring class field of K of conductor f. By class field theory, we have the Artin isomorphism

$$\begin{aligned} \mathrm{Cl}(O_D) &\xrightarrow{\sim} \mathrm{Gal}(H_D/K) \\ [\mathfrak{p}] &\mapsto \mathrm{Frob}_{\mathfrak{p}} \end{aligned}$$

for all primes $\mathfrak{p}$ of K unramified in H_D, where $\mathrm{Cl}(O_D)$ is the group of invertible fractional ideals of O_D modulo principal fractional ideals. For any fractional ideal $\mathfrak{c}$ of K with $\mathfrak{c} \leftrightarrow \sigma$ under the Artin map, by Proposition 4.2 there exists $\xi \in A$ such that

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

which describes the action of $\mathrm{Gal}(H_D/K)$ on $j(z)$ as indicated in the following theorem known as the *Shimura reciprocity law*.

Theorem 5.1 ([11, p. 59]). *We have $j(z) \in \mathbb{P}^1(H_D)$ and*

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

We may now compute the conjugates of $j(z)$ under $\mathrm{Gal}(H_D/K)$.

Algorithm 5.2. This algorithm computes the set

$$\{j(z)^\sigma : \sigma \in \mathrm{Gal}(H_D/K)\} \subset \mathbb{C}. \tag{4}$$

1. Compute a set G of ideals in bijection with the ring class group $\mathrm{Cl}\, O_D$.
2. Using Algorithm 4.4, for each ideal $\mathfrak{c} \in G$, compute an element $\xi \in \mathcal{O}$ such that $\mathfrak{c}\mathcal{O} = \xi\mathcal{O}$.
3. For each ξ from Step 2, compute $j(\iota_\infty(\xi^{-1})(z))$ according to Proposition 3.2, and output this set.

Remark 5.3. One can compute the set G in step 1 by the natural exact sequence

$$1 \to \frac{(\mathbb{Z}_K/f\mathbb{Z}_K)^*}{\mathbb{Z}_K^*(\mathbb{Z}_F/f\mathbb{Z}_F)^*} \to \mathrm{Cl}\, O_D \to \mathrm{Cl}\, \mathbb{Z}_K \to 1;$$

a representative set of elements of $\mathrm{Cl}\, O_D$ can be obtained as cosets of $\mathrm{Cl}\, \mathbb{Z}_K$.

Given a complete set of conjugates t^σ of a purported algebraic number t, we then 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 [3, §2.7.2]).

6 Galois descent

In this section, we discuss the Galois descent properties of CM points z. The computationally-minded reader may proceed to the next section, since these results will not affect the output. We continue notation from §2 and §5.

According to Theorem 5.1, a CM point $j(z)$ of discriminant D is defined over the ring class field H_D of $K = F(\sqrt{D})$. However, the set of conjugates of $j(z)$ may descend to a smaller field.

Proposition 6.1. *Let S be a full set of $\mathrm{Gal}(H_D/K)$-conjugates of $j(z)$ as in (4). Then S is in fact a full set of $\mathrm{Gal}(H_D/F)$-conjugates.*

Suppose that $\sigma(D)/D \in \mathbb{Z}_F^{*2}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Then H_D is Galois over $\mathbb{Q}$, and S is a full set of $\mathrm{Gal}(H_D/\mathbb{Q})$-conjugates.

The first statement is due to Shimura [12, §9.2]. Unfortunately, the proof of the second statement is too detailed to appear in these pages. For some discussion, see [17, Propositions 5.1.2, 5.4.1], though the proof there is incomplete. We now give a sketch of the proof of Proposition 6.1.

Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$, and define

$$\Gamma(\mathfrak{N}) = \{\iota_\infty(\gamma) : \gamma \in \mathcal{O}^*,\ \mathrm{nrd}(\gamma) = 1,\ \gamma \equiv 1 \pmod{\mathfrak{N}}\}. \tag{5}$$

We define $X(\mathfrak{N})_{\mathbb{C}} = \Gamma(\mathfrak{N})\backslash\mathfrak{H}$. Denote by $H(\mathfrak{N})$ the ray class field of F of conductor $\mathfrak{N}$.

The curve $X(\mathfrak{N})$ has an interpretation as a moduli space for a certain class of abelian varieties equipped with level structure, and as a result it has a canonical model defined over a number field. The following is due to Shimura.

Theorem 6.2 ([11, Main Theorem I (3.2)]). *There exists a projective, non-singular curve $X(\mathfrak{N})_{H(\mathfrak{N})}$ defined over $H(\mathfrak{N})$ and a holomorphic map $j_{\mathfrak{N}} : \mathfrak{H} \to X(\mathfrak{N})_{\mathbb{C}}$, such that the map $j_{\mathfrak{N}}$ yields an analytic isomorphism*

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

As with the case of modular curves, with additional restrictions on the moduli interpretation, one obtains a curve $X(\mathfrak{N})_F$ defined over F.

Claim. If $\sigma(\mathfrak{N}) = \mathfrak{N}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, then $X(\mathfrak{N})_F$ has a model $X(\mathfrak{N})_{\mathbb{Q}}$ defined over $\mathbb{Q}$.

Let S be the set of ramified places of A. For $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, let A^σ be the quaternion algebra which is ramified at the set $\sigma(S)$, let $\Gamma^*(1)^\sigma$ be the group associated to this data as in §2, and let $\Gamma(\mathfrak{N})^\sigma$ be defined as in (5) for the ideal $\sigma(\mathfrak{N})$. By functoriality, we see that the Galois-conjugate curve $X(\mathfrak{N})^\sigma$ corresponds exactly to the Shimura curve associated to the quaternion algebra A^σ and ideal $\sigma(\mathfrak{N})$.

It is well-known that any two triangle groups of the same type (i.e. having the same signature) are conjugate under $PSL_2(\mathbb{R})$. From the basic theory of Shimura curves, we see that the groups $\Gamma^*(1)$ and $\Gamma^*(1)^\sigma$ have the same type. So let $\delta \in PSL_2(\mathbb{R})$ be such that $\delta\Gamma^*(1)\delta^{-1} = \Gamma^*(1)^\sigma \subset PSL_2(\mathbb{R})$. Now using that $\sigma(N) = \mathfrak{N}$, we show that $\delta\Gamma(\mathfrak{N})\delta^{-1} = \Gamma(\mathfrak{N})^\sigma$. It follows that δ gives an isomorphism of Riemann surfaces $X(\mathfrak{N})_{\mathbb{C}} \xrightarrow{\sim} X(\mathfrak{N})^\sigma_{\mathbb{C}}$, which in fact yields an isomorphism $\phi_\sigma : X(\mathfrak{N})_F \xrightarrow{\sim} X(\mathfrak{N})^\sigma_F$ defined over F. The map ϕ_σ lies over $\mathbb{P}^1_F$ since it must pair up the elliptic points which by the classification we note have distinct orders, and hence must act by the identity. The maps ϕ_σ then give the data necessary for Galois descent to $\mathbb{Q}$ (see [16]).

Now suppose that $\mathfrak{N}$ is prime to the discriminant of A. Then we have an isomorphism $\iota_{\mathfrak{N}} : \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \xrightarrow{\sim} M_2(\mathbb{Z}_{F,\mathfrak{N}})$, unique up to conjugation by an element of $GL_2(\mathbb{Z}_{F,\mathfrak{N}})$, where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$. We then define the subgroup

$$\Gamma_0(\mathfrak{N}) = \{\iota_\infty(\gamma) : \gamma \in \mathcal{O}^*,\ \mathrm{nrd}(\gamma) = 1,\ \iota_{\mathfrak{N}}(\gamma) \text{ upper triangular modulo } \mathfrak{N}\}.$$

We let $\Gamma_0(\mathfrak{N})\backslash\mathfrak{H} = X_0(\mathfrak{N})_{\mathbb{C}}$. The quotient $X(\mathfrak{N})_{\mathbb{Q}}/H \xrightarrow{\sim} X_0(\mathfrak{N})$ by the (Borel) subgroup H is stabilized by the action of the Galois group on the automorphism group of $X(\mathfrak{N})_{\mathbb{Q}}/X^*(1)_{\mathbb{Q}}$, and hence the quotient morphism is defined over $\mathbb{Q}$ and we have a model $X_0(\mathfrak{N})_{\mathbb{Q}}$ for $X_0(\mathfrak{N})_{\mathbb{C}}$.

For each $\mathfrak{N}$, there exists an element $w_{\mathfrak{N}} \in \mathrm{Aut}(\Gamma_0(\mathfrak{N}))$, known by analogy as an *Atkin-Lehner involution*, defined to be a normalizing element $w_{\mathfrak{N}} \in \mathcal{O}$ with $\mathrm{trd}(w_{\mathfrak{N}}) = 0$ and $\mathrm{nrd}(w_{\mathfrak{N}})\mathbb{Z}_{F,\mathfrak{N}} = \mathfrak{N}$. Putting together the functions $j(z), j(w_{\mathfrak{N}}(z))$, we obtain a birational map of $X_0(\mathfrak{N})$ to an irreducible closed subvariety of $\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$ of dimension 1, described by a polynomial $\Phi_{\mathfrak{N}}(x, y)$ in the affine open $(\mathbb{P}^1_{\mathbb{C}} \setminus \{\infty\})^2 = \mathbb{A}^2_{\mathbb{C}}$. By the claim above, the polynomial $\Phi_{\mathfrak{N}}(x, y)$ has coefficients in $\mathbb{Q}$.

To conclude the proof of the proposition, let D be as in Proposition 6.1, and 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 $\omega_N \in O_D$ of trace zero and norm $4N$; its image $\omega_N = \iota_K(\mu) \in \mathcal{O}$ is an Atkin-Lehner involution on $X_0(N)$. Obviously μ commutes with ω_N, so $z = \omega_N(z)$, and hence $j(z) = j(\omega_N z)$. Therefore $j(z)$ is a root of the polynomial $\Phi_N(x, x)$, and since this is true of each of the conjugates of $j(z)$ as well, we obtain Proposition 6.1.

7 Examples and applications

We now give examples of the above algorithms for the class XI of Takeuchi [14]. 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 $b = -(\zeta_9 + 1/\zeta_9)$ satisfies $b^3 - 3b - 1 = 0$. We have $\mathrm{disc}(F/\mathbb{Q}) = 3^4$ and F has strict class number 1.

We choose the unique real place σ for which $\sigma(b) > 0$, and we take A to be the quaternion algebra which is ramified at the other two real places and is unramified at all other places. By Takeuchi [14, Proposition 2], we easily compute that A is isomorphic to the algebra as in (1) with $\alpha^2 = -3$, $\beta^2 = b$.

We fix the isomorphism $\iota_\infty : A \otimes_F \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$, given explicitly as

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

We next 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. 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 an integral element

$\zeta \in A$ satisfying $\zeta^9 = 1$. Extending this to a maximal order (a naïve approach suffices here, or see [17, §4.3]), we have $\mathcal{O} = \mathbb{Z}_F \oplus \mathbb{Z}_F\zeta \oplus \mathbb{Z}_F\eta \oplus \mathbb{Z}_F\omega$, where

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

These elements have minimal polynomials

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

From Takeuchi [14, Table (3)], we know that $\Gamma^*(1)$ 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 $s_p, s_q, s_r \in \mathcal{O}_1^*$, satisfying the relations

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

hence the elliptic elements s_p, s_q, s_r generate $\mathcal{O}_1^*$. 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 Fig. 1: any shaded (or unshaded) triangle is a fundamental triangle for $\Gamma^*(1)$, and the union of any shaded and unshaded triangle forms a fundamental domain for $\Gamma^*(1)$.

By exhaustively listing elements of $\mathcal{O}$, we enumerate (optimal) embeddings $\iota_D : O_D \hookrightarrow \mathcal{O}$ for orders with discriminant D of small norm. Using Algorithm 5.2, we compute the CM points for these orders, and the results are listed in Tables 1–4 in §8. This follows in the spirit of the extended history of computing such tables for values of the elliptic j-function (see e.g. [6, pp. 193–194]).

Example 7.1. The field $K = F(\sqrt{-7})$ has class number 1. The element

$$\mu = (-b^2 - b + 2) + (-b^2 + 2b + 5)\zeta + (2b^2 - 2b - 8)\omega + (3b + 6)\eta \in \mathcal{O}$$

has minimal polynomial $x^2 - x + 2$ hence $\mathbb{Z}_F[\mu] = \mathbb{Z}_K = O_{-7}$. 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 we compute that $j(z) = -9594.703125000\ldots$, which agrees with

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

to the precision computed (100 digits).

Example 7.2. Now take $K = F(\sqrt{-2})$, with class number 3. We find $\mu \in \mathcal{O}$ satisfying $\mu^2 + 2 = 0$, so $\mathbb{Z}_f[\mu] = \mathbb{Z}_K = O_{-8}$; explicitly,

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

We obtain the CM point $j(z) = 17137.9737\ldots$ as well as its Galois conjugates $0.5834\ldots \pm 0.4516\ldots i$. 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 (200 digits); 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 Gross-Zagier formula as in [6], 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 [5, p. 42]. The work in this direction concerning the Arakelov geometry of Shimura curves has dealt with either quaternion algebras over $\mathbb{Q}$ (such as [10], [19], [8]) or $M_2(F)$ with F real quadratic, the case of Hilbert modular forms (see [2]). A nice formulation for the case of cocompact arithmetic triangle groups seems to be in order. It is hoped that the data computed here will be useful in proving such a formula.

8 Tables and figures

In the following tables, we list the results from the extended example in §7 concerning the $(2, 3, 9)$ triangle group.

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 $K = F(\sqrt{D})$ is Galois over $\mathbb{Q}$ and contains an order O_D of discriminant D. We list in Table 1 for each such small D a polynomial g which is a minimal polynomial for the ring class field H_D of K of conductor $f\mathbb{Z}_F$, where $D = df^2$. In Table 2, we list factorizations of the norms of the CM point $j(z_D) \in \mathbb{P}^1(H_D)$.

In Tables 3–4, we repeat the above without assuming that D is Galois-stable.

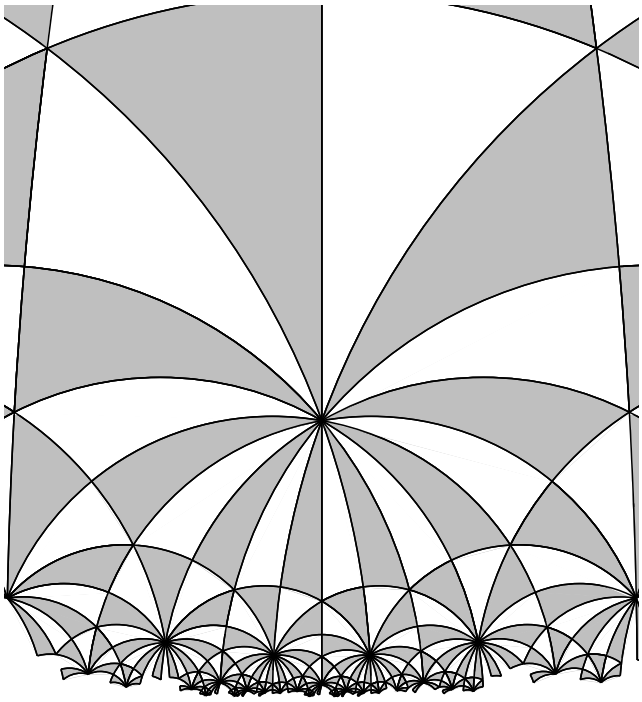

Fig. 1. The translates of a fundamental triangle for $\Gamma^*(1)$

$-D$	$\lvert N(D)\rvert$	g
$b+2$	3	$\mathbb{Q}$
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 1. Gal($F/\mathbb{Q}$)-stable CM Points: Ring class fields

$-D$	Numerator	Denominator
$b+2$	1	0
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 2. Gal($F/\mathbb{Q}$)-stable CM Points: Norms

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	$x^4+(b-1)x^2+1$

Table 3. CM Points: Ring class 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	$-19^{12} 127^2 179^2 199^2 251^2 271^2 487^4 971^1$	$2^{90}17^9$
$8b^2-31$	$19^{12} 71^4 127^2 179^2 251^2 271^2 307^2 359^2 631^4$	$2^{72}17^{18}$
$-8b^2+12b$	$-19^8 71^4 199^4 379^4 503^2 523^2 739^2$	$2^{63}17^{18}$
$-4b-12$	$-3^{26} 19^2 71^2 199^4 379^2 523^2$	$2^{63}17^9$
$-7b^2-3b-3$	$3^{26} 19^6 127^2 271^2 307^2$	$2^{45}53^9$
$-4b^2+11b-10$	$19^8 71^2 107^2 163^4 431^2 467^2 683^2 719^2 1151^2 1187^2$	$2^{72}17^9 53^9$
$-11b^2+6b+1$	$3^{33} 107^2 271^2 487^2 991^2 1063^2 2179^1$	$2^{45}71^9$
$-3b^2+4b-8$	$-3^{33} 19^6 71^4 127^2 487^4 631^2 811^2 2287^1$	$2^{54}17^{18}53^9$
$4b^2-23$	$-3^{39} 19^{12} 163^2 179^2 631^2 1459^2 2719^1$	$2^{54}17^9 53^9 71^5$
$25b^2-12b-80$	$3^{18} 19^8 71^2 127^2 163^2 179^2 251^2 271^2 631^2 811^2 1423^2 1783^2$	$2^{90}53^9 89^9$
$-16b^2+24b+4$	$19^{16} 503^2 971^2 1619^2 1871^2 1907^2 2339^2 2591^2$	$2^{57}17^9 53^9 71^1$

Table 4. CM Points: Norms

References

1. Montserrat Alsina and Pilar Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM monograph series, vol. 22, American Mathematical Society, Providence, 2004.
2. Jan Hendrik Bruinier, *Infinite products in number theory and geometry*, Jahresber. Deutsch. Math.-Verein. **106** (2004), no. 4, 151–184.
3. Henri Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
4. M. Eichler, *Über die Idealklassenzahl hypercomplexer Systeme*, Math. Z. **43** (1938), 481–494.
5. Noam D. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 1–47.
6. Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.
7. Svetlana Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.
8. Stephen S. Kudla, Michael Rapoport, and Tonghai Yang, *Derivatives of Eisenstein series and Faltings heights*, Compos. Math. **140** (2004), no. 4, 887–951.
9. I. Reiner, *Maximal orders*, Clarendon Press, Oxford, 2003.
10. David Peter Roberts, *Shimura curves analogous to* $X_0(N)$, Harvard Ph.D. thesis, 1989.
11. Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.
12. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô memorial lectures, Princeton University Press, Princeton, 1994.
13. Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.
14. Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo **24** (1977) 201–212.
15. Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.
16. Helmut Völklein, *Groups as Galois groups: an introduction*, Cambridge studies in advanced mathematics, vol. 53, Cambridge University Press, New York, 1996.
17. John Voight, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.
18. D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., 2002, Int. Press, Somerville, MA, 211–244.
19. Shou-Wu Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290.