Shimura curve computations

John Voight

Abstract. We introduce Shimura curves first as Riemann surfaces and then as moduli spaces for certain abelian varieties. We give concrete examples of these curves and do some explicit computations with them.

1. Introduction: modular curves

We motivate the introduction of Shimura curves by first recalling the definition of modular curves.

For each $N \in \mathbb{Z}_{>0}$, we define the subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\} \subset SL_2(\mathbb{Z}).$$

The group $\Gamma_0(N)$ acts on the completed upper half-plane $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{R})$ by linear fractional transformations, and the quotient $X_0(N)_{\mathbb{C}} = \Gamma_0(N) \backslash \mathfrak{H}^*$ can be given the structure of a compact Riemann surface. The curve $X_0(N)_{\mathbb{C}}$ parametrizes cyclic N-isogenies between (generalized) elliptic curves and therefore has a model $X_0(N)_{\mathbb{Q}}$ defined over $\mathbb{Q}$. On $X_0(N)_{\mathbb{Q}}$, we also have *CM points*, which correspond to isogenies between elliptic curves which have complex multiplication (CM) by an imaginary quadratic field K.

Shimura curves arise in generalizing this construction from the matrix ring $M_2(\mathbb{Q})$ to certain quaternion algebras over totally real fields F. A Shimura curve is the quotient of the upper half-plane $\mathfrak{H}$ by a discrete, "arithmetic" subgroup of $\mathrm{Aut}(\mathfrak{H}) = PSL_2(\mathbb{R})$. Such a curve also admits a description as a moduli space, yielding a model defined over a number field, and similarly comes equipped with CM points.

The study of the classical modular curves has long proved rewarding for mathematicians both theoretically and computationally, and an expanding list of conjectures have been naturally generalized to the setting of Shimura curves. These curves, which although at first are only abstractly defined, can also be made very concrete.

In §2, we briefly review the relevant theory of quaternion algebras and then define Shimura curves as Riemann surfaces. In §3, we provide a detailed example of a Shimura curve over $\mathbb{Q}$. In §4, we discuss the arithmetic of Shimura curves:

1991 *Mathematics Subject Classification.* Primary 11G18, 14G35.
Key words and phrases. Shimura curves, moduli spaces, triangle groups.

we explain their interpretation as moduli spaces, and define CM points, Atkin-Lehner quotients, and level structure. Finally, in §5, we illustrate these concepts by considering the case of Shimura curves arising from triangle groups, in some sense the "simplest" class, and do some explicit computations with them.

2. Quaternion algebras and complex Shimura curves

2.1. Quaternion algebras. We refer to [**Vi**] as a reference for this section.

As in the introduction, we look again at $SL_2(\mathbb{Z}) \subset M_2(\mathbb{Q})$: we have taken the group of elements of determinant 1 with integral entries in the $\mathbb{Q}$-algebra $M_2(\mathbb{Q})$. The algebras akin to $M_2(\mathbb{Q})$ are quaternion algebras.

Let F be a field with $\operatorname{char} F \neq 2$. A *quaternion algebra* over F is a central simple F-algebra of dimension 4. Equivalently, an F-algebra B is a quaternion algebra if and only if there exist $\alpha, \beta \in B$ which generate B as an F-algebra such that

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

for some $a, b \in F^*$. We denote this algebra $B = \left(\frac{a,b}{F}\right)$.

Example. As examples of quaternion algebras, we have the ring of 2×2-matrices over F, or $M_2(F) \cong \left(\frac{1,1}{F}\right)$, and the division ring $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ of Hamiltonians.

From now on, let B denote a quaternion algebra over F. There is a unique anti-involution $\overline{\ } : B \to B$, called *conjugation*, with the property that $\alpha\overline{\alpha} \in F$ for all $\alpha \in B$. The map $\operatorname{nrd}(\alpha) = \alpha\overline{\alpha}$ is known as the *reduced norm*.

Example. If $B = \left(\frac{a,b}{F}\right)$, and $\theta = x + y\alpha + z\beta + w\alpha\beta$, then

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

From now on, let F be a number field. Let v be a noncomplex place of F, and let F_v denote the completion of F at v. If $B_v = B \otimes_F F_v$ is a division ring, we say that B is *ramified* at v; otherwise $B_v \cong M_2(F_v)$ and we say B is *split* at v. The number of places v where B is ramified is finite and of even cardinality; their product is the *discriminant* $\operatorname{disc}(B)$ of B. Two quaternion algebras B, B' over F are isomorphic (as F-algebras) if and only if $\operatorname{disc}(B) = \operatorname{disc}(B')$.

Let $\mathbb{Z}_F$ denote the ring of integers of F. An *order* of B is a subring $\mathcal{O} \subset B$ (containing 1) which is a $\mathbb{Z}_F$-submodule satisfying $F\mathcal{O} = B$. A *maximal order* is an order which is maximal under inclusion. Maximal orders are not unique—but we mention that in our situation (where B has at least one unramified infinite place, see the next section), a maximal order in B is unique up to conjugation.

2.2. Shimura curves as Riemann surfaces. Let $\mathcal{O} \subset B$ be a maximal order. We then define the group analogous to $SL_2(\mathbb{Z})$, namely the group of units of $\mathcal{O}$ of norm 1:

$$\mathcal{O}_1^* = \{\gamma \in \mathcal{O} : \operatorname{nrd}(\gamma) = 1\}.$$

In order to obtain a discrete subgroup of $PSL_2(\mathbb{R})$ (see [**Ka**, Theorem 5.3.4]), we insist that F is a totally real (number) field and that B is split at exactly one real place, so that

$$B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \times \mathbb{H}^{[F:\mathbb{Q}]-1}.$$

We denote by $\iota_\infty : B \hookrightarrow M_2(\mathbb{R})$ the projection onto the first factor.

We then define the group

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

The quotient $X^B(1)_{\mathbb{C}} = \Gamma^B(1)\backslash\mathfrak{H}$ can be given the structure of a Riemann surface [**Ka**, §5.2] and is known as a *Shimura curve*.

From now on, we assume that $B \ncong M_2(\mathbb{Q})$, so that we avoid the (classical) case of modular curves; it then follows that B is a division ring and, unlike the case for modular curves, the Riemann surface $X^B(1)_{\mathbb{C}}$ is already compact [**Ka**, Theorem 5.4.1].

3. Example

We now make this theory concrete by considering an extended example.

We take $F = \mathbb{Q}$ and the quaternion algebra B over $\mathbb{Q}$ with $\mathrm{disc}(B) = 6$, i.e. B is ramified at the primes 2 and 3, and unramified at all other places, including ∞. Explicitly, we may take $B = \left(\frac{-1,3}{\mathbb{Q}}\right)$, so that $\alpha, \beta \in B$ satisfy

$$\alpha^2 = -1, \quad \beta^2 = 3, \quad \beta\alpha = -\alpha\beta.$$

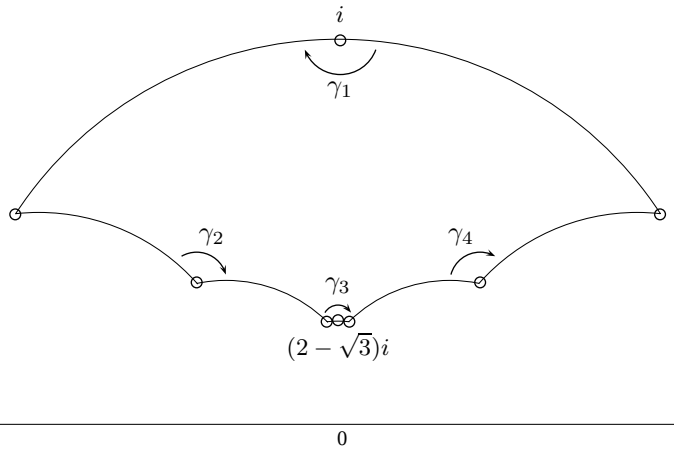
We find the maximal order

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\delta \text{ where } \delta = (1 + \alpha + \beta + \alpha\beta)/2,$$

and we have an embedding

$$\begin{aligned} \iota_\infty : B &\to M_2(\mathbb{R}) \\ \alpha, \beta &\mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}. \end{aligned}$$

With respect to this embedding, we compute a fundamental domain D for the action of $\Gamma^B(1) = \iota_\infty(\mathcal{O}_1^*/\{\pm 1\})$ as follows. (For an alternate presentation, see [**AB**, §5.5.2] or [**KV**, §5.1].)



The elements

$$\gamma_1 = \alpha, \ \gamma_2 = \alpha + \delta, \ \gamma_3 = 2\alpha + \alpha\beta, \ \gamma_4 = 1 + \alpha - \beta + \delta$$

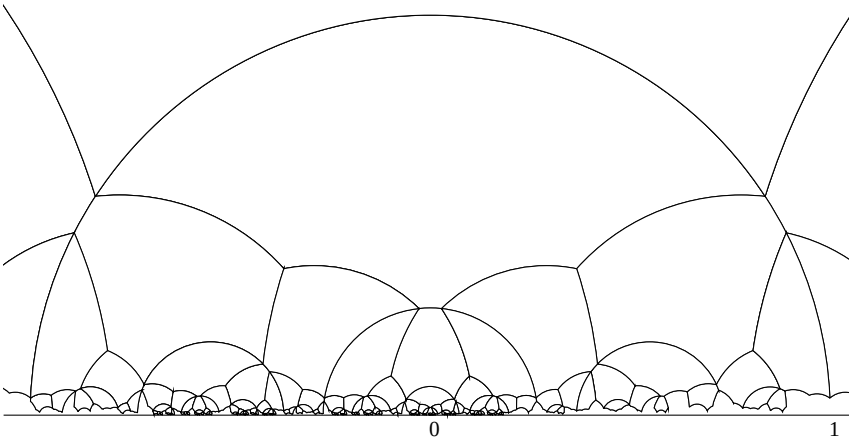
are known as *side-pairing elements*; they yield the presentation

$$\Gamma^B(1) \cong \langle \gamma_1, \dots \gamma_4 \mid \gamma_1^2 = \gamma_2^3 = \gamma_3^2 = \gamma_4^3 = \gamma_4\gamma_3\gamma_2\gamma_1 = 1 \rangle.$$

One can compute the area $\mu(D)$ of the above fundamental domain D by triangulation, but we also have the formula (see [**E**, §2.2])

$$\mu(D) = \mu(X^B(1)) = \frac{\pi}{3} \prod_{p|\mathrm{disc}(B)} (p-1) = \frac{2\pi}{3}.$$

The group $\Gamma^B(1)$ then tessellates $\mathfrak{H}$ as follows.



(The algorithm for drawing hyperbolic polygons is due to Verrill [**Ve**].)

The genus g of X can be computed by the Riemann-Hurwitz formula as

$$2g - 2 = \frac{\mu(X^B(1))}{2\pi} - \sum_q e_q \left(1 - \frac{1}{q}\right),$$

where e_q is the number of (conjugacy classes of) elliptic points of order q. From the presentation for $\Gamma^B(1)$ above, we can see directly that $e_2 = e_3 = 2$ and hence

$$2g - 2 = 1/3 - 2(1 - 1/2) - 2(1 - 1/3) = -2$$

so $g = 0$. Alternatively, we can compute the number of these elements by the formulas

$$e_2 = \prod_{p|\mathrm{disc}(B)} \left(1 - \left(\frac{-4}{p}\right)\right) = 2, \quad e_3 = \prod_{p|\mathrm{disc}(B)} \left(1 - \left(\frac{-3}{p}\right)\right) = 2.$$

Since the genus of X is zero, we have a map $X^B(1)_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$.

4. Arithmetic of Shimura curves

4.1. Shimura curves as moduli spaces. Just as with modular curves, Shimura curves are in fact moduli spaces, and this moduli description yields a model for $X^B(1)_{\mathbb{C}}$ which is defined over a number field.

In the case $F = \mathbb{Q}$, the curve $X^B(1)$ is a coarse moduli space for pairs (A, ι), where:

- A is an abelian surface, and
- $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is an embedding.

We say that such an A has *quaternionic multiplication* (QM) *by* $\mathcal{O}$. The involution $\overline{\ }$ on $\mathcal{O}$ induces via ι an involution on $\mathrm{End}(A)$, and there is a unique principal polarization on A which is compatible with this involution, then identified with the Rosati involution.

If $F \neq \mathbb{Q}$, the moduli description is more complicated: since B is then neither totally definite nor totally indefinite, it follows from the classification of endomorphism algebras of abelian varieties over $\mathbb{C}$ (see [**M**, Theorem 21.3]) that we cannot have $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B$. Instead, one must choose an imaginary quadratic extension K of F, as in [**Z**, §1.1.2], and consider a moduli problem over K. For simplicity, we assume from now on that F has narrow class number 1: under this hypothesis, we have a natural choice, namely $K = F(\sqrt{-d})$, where d is a totally positive generator for the discriminant $\mathrm{disc}(B)$. One may then think of the objects parametrized by a Shimura curve $X^B(1)_F$ as "abelian varieties with QM by $\mathcal{O}$"—the precise meaning of this phrase will be neglected here.

It then follows from this moduli description that there exists a *canonical model* $X^B(1)_F$ for $X^B(1)_{\mathbb{C}}$ defined over F, a theorem due to Shimura [**S**] and Deligne [**D**].

4.2. Example: Models. The model $X^B(1)_{\mathbb{Q}}$ over $\mathbb{Q}$ for our Shimura curve with $\mathrm{disc}(B) = 6$ is given by the conic

$$X^B(1)_{\mathbb{Q}} : x^2 + y^2 + 3z^2 = 0,$$

a result attributed to Ihara [**Ku**, p. 279].

This identification can be made quite explicit, a computation due to Baba-Granath [**BG**]. For $k \in \mathbb{Z}_{\geq 0}$, we denote by $M_k(\Gamma)$ the space of holomorphic weight k *modular forms* for the group $\Gamma = \Gamma^B(1)$, namely, the space of holomorphic maps $f : \mathfrak{H} \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Using an elementary formula due to Shimura, we compute the dimension of $M_k(\Gamma)$:

$$\dim_{\mathbb{C}} M_4(\Gamma) = \dim_{\mathbb{C}} M_6(\Gamma) = 1, \quad \dim_{\mathbb{C}} M_{12}(\Gamma) = 3.$$

From this, one can show that there exist normalized $h_k \in M_k(\Gamma)$ for $k = 4, 6, 12$ such that

$$h_{12}^2 + 3h_6^4 + h_4^6 = 0,$$

which realizes the map $X^B(1)_{\mathbb{C}} \to X^B(1)_{\mathbb{Q}}$.

4.3. CM points. On the modular curves $X_0(N)$, we have CM points arising from elliptic curves with extra endomorphisms. These points are defined over ring class extensions H of an imaginary quadratic field K, and the Shimura reciprocity law describes explicitly the action of $\mathrm{Gal}(H/K)$ on them. In a similar way, on the Shimura curve $X^B(1)$ we have *CM points* which correspond to abelian varieties with extra endomorphisms. Let $K \supset F$ be a totally imaginary quadratic extension which *splits* B, i.e. $B \otimes_F K \cong M_2(K)$; the field K splits B if and only if there exists an embedding $\iota_K : K \hookrightarrow B$, and the map ι_K is concretely given by an element $\mu \in \mathcal{O}$ such that $\mathbb{Z}_F[\mu] = \mathbb{Z}_K$. Let $z = z_D$ be the fixed point of $\iota_\infty(\mu)$ in $\mathfrak{H}$; we then

say z is a *CM point* on $X^B(1)_{\mathbb{C}}$. When $F = \mathbb{Q}$, CM points on $X^B(1)$ correspond to abelian surfaces A with endomorphism algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M_2(K)$; the interpretation is again more subtle when $F \neq \mathbb{Q}$, but there one may think of these points as similarly having "extra endomorphisms".

On the model $X^B(1)_F$, these points are defined over the Hilbert class field H of K (or more generally, ring class extensions), and one has also a Shimura reciprocity law; see [**S**] for a discussion and proof.

4.4. Example: CM points. The following computation can be found in Elkies [**E**, §3.4] and Baba-Granath [**BG**, §3.3].

We return to the example from §2, with $F = \mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{-19})$, and $\mathbb{Z}_K = \mathbb{Z}[(1+\sqrt{-19})/2]$. We have $\#\,\mathrm{Cl}(\mathbb{Z}_K) = 1$, and the elliptic curve $E = \mathbb{C}/\mathbb{Z}_K$ with CM by $\mathbb{Z}_K$ has j-invariant -96^3.

The genus 2 curve C defined by

$$C : y^2 = 2t^6 - 3(1+9\sqrt{-19})t^4 - 3(1-9\sqrt{-19})t^2 + 2$$

has Jacobian $J(C) \cong E \times E$, and $\mathrm{End}(J(C)) \cong M_2(\mathbb{Z}_K)$. This curve C "corresponds" to the moduli point $[C] = (32 : 27 : 13\sqrt{-19})$ on the Shimura curve $X^B(1) : x^2 + 3y^2 + z^2 = 0$. (The field of moduli of the point $[C]$ is $\mathbb{Q}$, but $\mathbb{Q}$ is not a field of definition for C; the automorphism group of C is $\mathrm{Aut}(C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

4.5. Atkin-Lehner involutions. Shimura curves also possess natural involutions, just like modular curves. The normalizer

$$N(\mathcal{O}) = \{\alpha \in B^*/F^* : \alpha\mathcal{O} = \mathcal{O}\alpha,\ \mathrm{nrd}(\alpha) \text{ is totally positive}\}$$

acts via ι_∞ as automorphisms of $X^B(1)_F$, and generates a subgroup

$$W \cong \prod_{\mathfrak{p} \mid \mathrm{disc}(B)} \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^e.$$

The elements of W are known as *Atkin-Lehner involutions*. Letting $\Gamma^{B*}(1) = \iota_\infty(N(\mathcal{O}))$, we see that the curve $X^{B*}(1) = \Gamma^{B*}(1)\backslash\mathfrak{H}$ is the quotient of $X^B(1)$ by W.

When $F = \mathbb{Q}$, these involutions have a natural moduli interpretation. Recall that the curve $X^B(1)$ parametrizes pairs (A, ι), where A is an abelian surface (over $\mathbb{C}$, say) with QM by $\mathcal{O}$ specified by an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$. But there may be more than one such embedding ι for a given A, even up to isomorphism: for each divisor $\mathfrak{m} \mid \mathrm{disc}(B)$, we can "twist" ι by $\mathfrak{m}$ to obtain a new pair $(A, \iota^{\mathfrak{m}})$. All such twists arise in this way (see [**R**, §3]), and therefore the quotient $X^{B*}(1)$ of $X^B(1)$ by W parametrizes abelian surfaces A which can be given the structure ι of QM by $\mathcal{O}$, without a particular choice of ι.

4.6. Example: Atkin-Lehner quotient. The two Atkin-Lehner involutions w_2, w_3 act on $X^B(1)_{\mathbb{Q}} : x^2 + y^2 + 3z^2 = 0$ by

$$w_2(x : y : z) = (x : -y : z), \quad w_3(x : y : z) = (-x : y : z).$$

The quotients are therefore

$$\begin{array}{ccc} X & \longrightarrow & X^{\langle w_2\rangle} = \mathbb{P}^1 \\ (x : y : z) & \longmapsto & (x : z) \end{array} \qquad \begin{array}{ccc} X & \longrightarrow & X^{\langle w_3\rangle} = \mathbb{P}^1 \\ (x : y : z) & \longmapsto & (y : z). \end{array}$$

and the quotient by the full group $W = \langle w_2, w_3 \rangle$ can be given by

$$\begin{aligned} j : X &\longrightarrow X^W = \mathbb{P}^1 \\ (x : y : z) &\longmapsto (16y^2 : 9x^2), \end{aligned}$$

under our normalization. Our moduli point $[C]$ corresponding to K with discriminant -19 was $[C] = (32 : 27 : 13\sqrt{-19})$, and so we find $j([C]) = 81/64 = 3^4/2^6$.

4.7. Level structure: congruence subgroups. Having introduced the group $\Gamma^B(1)$ which replaces $PSL_2(\mathbb{Z})$, we now introduce the curves analogous to the modular curves. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ that is coprime to the discriminant of B, and let $\mathbb{Z}_{F,\mathfrak{N}}$ be the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$; then there exists an embedding

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

We define

$$\Gamma_0^B(\mathfrak{N}) = \{\iota_\infty(\gamma) : \gamma \in \mathcal{O}_1^*,\ \iota_{\mathfrak{N}}(\gamma) \text{ is upper triangular modulo } \mathfrak{N}\}/\{\pm 1\}$$

and we again obtain a Riemann surface $X_0^B(\mathfrak{N})_{\mathbb{C}} = \Gamma_0^B(\mathfrak{N})\backslash\mathfrak{H}$.

In a similar way, for $F = \mathbb{Q}$, the curves $X_0^B(N)_{\mathbb{C}}$ parametrize cyclic N-isogenies between abelian surfaces with QM by $\mathcal{O}$. For any F, one can also show that the curve $X_0^B(\mathfrak{N})_{\mathbb{C}}$ admits a model over a number field.

5. Triangle groups

5.1. The $(2,4,6)$-triangle group. Recall from §4.5 that the group

$$\Gamma^{B*}(1) = \{\iota_\infty(\alpha) : \alpha \in B^*/F^*,\ \alpha\mathcal{O} = \mathcal{O}\alpha,\ \mathrm{nrd}(\alpha) \text{ is totally positive}\}$$

realizes the space $X^{B*}(1) = \Gamma^{B*}(1)\backslash\mathfrak{H}$. The quotient

$$\frac{\Gamma^{B*}(1)}{\Gamma^B(1)} \cong \prod_{p|\mathrm{disc}(B)} \mathbb{Z}/2\mathbb{Z},$$

arises from elements whose reduced norm divides $\mathrm{disc}(B) = 6$.

We can see the group $\Gamma^{B*}(1)$ again explicitly: it has a presentation

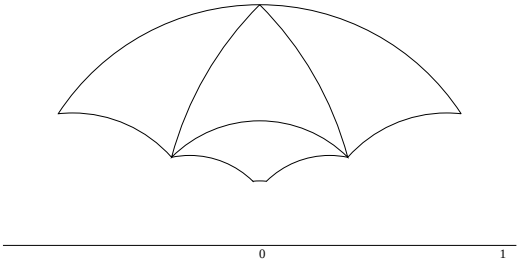
$$\Gamma^{B*}(1) \cong \langle s_2, s_4, s_6 \mid s_2^2 = s_4^4 = s_6^6 = s_6 s_4 s_2 = 1 \rangle$$

where

$$s_2 = -1 + 2\alpha - \beta + 2\delta,\ s_4 = -1 + \alpha,\ s_6 = -2 + \alpha + \delta$$

have $\mathrm{nrd}(s_2) = 6$, $\mathrm{nrd}(s_4) = 2$, $\mathrm{nrd}(s_6) = 3$, respectively. This group $\Gamma^{B*}(1)$ is known as a $(2,4,6)$-*triangle group*; a fundamental domain D for $\Gamma^{B*}(1)$ is the union of a *fundamental triangle*, a hyperbolic triangle with angles $\pi/2, \pi/4, \pi/6$ with vertices at the fixed points of s_2, s_4, s_6, respectively, together with its image in the reflection in the geodesic connecting any two of the vertices.

We can visualize the $(2,4,6)$-triangle group $\Gamma^{B*}(1)$ inside $\Gamma^B(1)$ as follows.



5.2. Cocompact arithmetic triangle groups. More generally, for $p, q, r \in \mathbb{Z}_{\geq 2}$ with $1/p + 1/q + 1/r < 1$, we may define the (p, q, r)-triangle group similarly as the group with presentation

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

By work of Takeuchi [**T**], there are exactly 18 quaternion algebras B (up to isomorphism), defined over one of 13 totally real fields F, that give rise to such a *cocompact arithmetic triangle group* $\Gamma^{B*}(1)$. Already these contain a number of curves worthwhile of study. (In this light, we could consider the classical $SL_2(\mathbb{Z})$ to be a $(2, 3, \infty)$-triangle group, though we still exclude this case in our discussion.)

Each of these "simplest" Shimura curves has genus zero, so we have a map $j : X^{B*}(1) \to \mathbb{P}^1_{\mathbb{C}}$. (In fact, one can show that the canonical model provided by Shimura and Deligne for $X^{B*}(1)_{\mathbb{C}}$ over F is already $\mathbb{P}^1_F$.) We normalize this map by taking the images of the elliptic fixed points z_p, z_q, z_r of s_p, s_q, s_r, respectively, to be $0, 1, \infty$.

5.3. Explicit computation of CM points. To summarize, from cocompact arithmetic triangle groups associated with certain quaternion algebras B over totally real fields F we obtain Riemann surfaces $X^{B*}(1)$ of genus 0 together with a map $j : X^{B*}(1) \to \mathbb{P}^1_{\mathbb{C}}$. There are CM points of arithmetic interest which we would like to compute.

THEOREM ([**Vo**]). *There exists an algorithm that, given a totally imaginary quadratic field $K \supset F$, computes the CM point $j(z) \in \mathbb{P}^1(\mathbb{C})$ associated to K to arbitrary precision, as well as all of its conjugates by the group* $\mathrm{Gal}(H/K)$.

One can then recognize the value j as an algebraic number by considering the polynomial defined by its conjugates.

5.4. Second example. We now give an example where $F \neq \mathbb{Q}$. Let F be the totally real subfield of $\mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive ninth root of unity. We have $\mathbb{Z}_F = \mathbb{Z}[b]$, where $b = -(\zeta_9 + 1/\zeta_9)$. We take $B = \left(\frac{-3, b}{F}\right)$, i.e. B is generated by α, β with

$$\alpha^2 = -3, \quad \beta^2 = b, \quad \beta\alpha = -\alpha\beta.$$

Here, we have $\mathrm{disc}(B) = \mathbb{Z}_F$, i.e. B is ramified at no finite place and at exactly two of the three real places. We fix the isomorphism $\iota_\infty : B \otimes_F \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$, 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 $\mathcal{O} = \mathbb{Z}_F \oplus \mathbb{Z}_F\zeta \oplus \mathbb{Z}_F\eta \oplus \mathbb{Z}_F\omega$, where

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

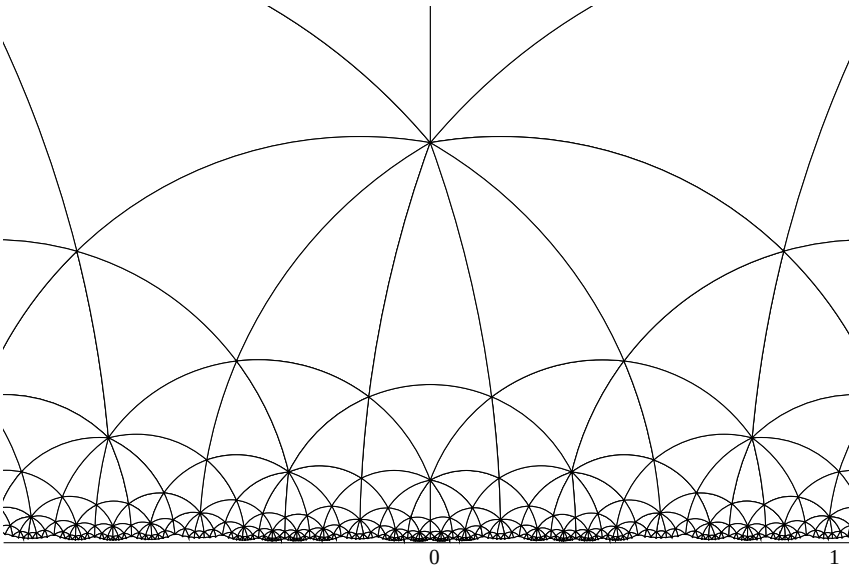
By work of Takeuchi [**T**], we know that $\Gamma^B(1) = \Gamma^{B*}(1)$ is a triangle group with signature $(p, q, r) = (2, 3, 9)$. Explicitly, we find the generators

$$s_2 = b + \omega - 2\eta, s_3 = -1 + (b^2 - 3)\zeta + (-2b^2 + 6)\omega + (b^2 + b - 3)\eta, s_9 = -\zeta$$

which satisfy the relations $s_2^2 = s_3^3 = s_9^9 = s_2 s_3 s_9 = 1$. The fixed points of these elements are

$$z_2 = 0.395526\ldots i,\ z_3 = -0.153515\ldots + 0.364518\ldots i,\ z_9 = i,$$

and they form the vertices of a fundamental triangle.



Each triangle in the above figure is a fundamental domain formed by the union of two such fundamental triangles.

5.5. CM points. As an example, we first take $K = F(\sqrt{-2})$ with class number 3. We find $\mu \in \mathcal{O}$ satisfying $\mu^2 + 2 = 0$, so $\mathbb{Z}_F[\mu] = \mathbb{Z}_K$ has discriminant -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 $0.5834\ldots \pm 0.4516\ldots i$, which yields the minimal polynomial for $j = j(z)$

$$j^3 - \tfrac{1096905}{64} j^2 + \tfrac{41938476081}{2097152} j - \tfrac{9781803409}{1048576} = 0$$

to the precision computed (300 digits). Note that

$$\tfrac{9781803409}{1048576} = \tfrac{7^2 71^2 199^2}{2^{20}}.$$

We verify that $K(j) = H = K(c)$, where $c^3 - 3c + 10 = 0$.

Larger examples can be computed, including over ring class extensions. Consider the field $K = F(\sqrt{-5})$ with discriminant $\mathrm{disc}(K/F) = -20$. We consider the order $\mathbb{Z}_{K,f} \subset K$ of conductor $f = b - 1$; note that $N_{F/\mathbb{Q}}(b-1) = 3$.

The CM point z has $j = j(z)$ which satisfies a polynomial of degree $14 = \#\,\mathrm{Cl}(\mathbb{Z}_{K,f})$, with $N(j)$ equal to

$$-\frac{71^8 127^8 163^4 179^2 487^4 971^2 1619^2 2591^2 2699^2 7451^2 10079^2 13859^2 17099^2}{2^{84} 5^9 89^9 269^9 719^9}.$$

The extension $K(j) = K(c)$ is generated by an element c which satisfies

$$c^{14} - c^{13} - 2c^{12} + 19c^{11} - 37c^{10} - 122c^9 + 251c^8 + 211c^7$$
$$- 589c^6 + 470c^5 - 41c^4 - 73c^3 + 22c^2 + 11c + 1 = 0.$$

References

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

[BG] Srinath Baba and Håkan Granath, Genus 2 curves with quaternionic multiplication, to appear in *Canadian J. Math.*, available at `http://www.mathnet.or.kr/preprint/mpip/2005-18.pdf`.

[D] Pierre Deligne, Travaux de Shimura, *Séminaire Bourbaki*, exp. no. 389, in *Lect. in Math.* **244**, Springer-Verlag, New York, 1971, 123–165.

[E] Noam D. Elkies, Shimura curve computations, *Algorithmic number theory (ANTS-III, Portland, OR, 1998)*, Lect. notes in comp. sci., vol. 1423, Springer, Berlin, 1998, 1–47.

[Ka] Svetlana Katok, *Fuchsian groups*, U. of Chicago Press, Chicago, 1992.

[KV] David R. Kohel and Helena A. Verrill, Fundamental domains for Shimura curves, *J. Théorie des Nombres de Bordeaux* **15** (2003), 205–222.

[Ku] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo* **25** (1979), 277–301.

[M] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, no. 5, Oxford University Press, London, 1970.

[R] Victor Rotger, Modular Shimura varieties and forgetful maps, *Trans. Amer. Math. Soc.* **356** (2004), 1535–1550.

[S] Goro Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. Math.* **85** (1967), 58–159.

[T] Kisao Takeuchi, Arithmetic triangle groups, *J. Math. Soc. Japan* **29** (1977), no. 1, 91–106.

[Ve] Subgroups of $PSL_2(\mathbb{R})$, *Handbook of Magma functions*, eds. John Cannon and Wieb Bosma, Sydney, July 2006, Chapter V.36, 1117–1138.

[Vi] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lect. notes in math., vol. 800, Springer, Berlin, 1980.

[Vo] John Voight, Computing CM points on Shimura curves arising from compact arithmetic triangle groups, *Algorithmic number theory (ANTS-VII, Berlin, 2006)*, Lect. notes in comp. sci., vol. 4076, Springer, Berlin, 2006, 406–420.

[Z] Shouwu Zhang, Heights of Heegner points on Shimura curves, *Ann. Math.* **153** (2001), 27–147.

Department of Mathematics and Statistics, University of Vermont, Burlington, VT 05401

E-mail address: `jvoight@gmail.com`