Clay Mathematics Proceedings
Volume 8, 2009

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

---

2000 *Mathematics Subject Classification.* Primary 11G18, Secondary 14G35.
Key words and phrases. Shimura curves, moduli spaces, triangle groups.

of a Shimura curve over $\mathbb{Q}$. In §4, we discuss the arithmetic of Shimura curves: 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 [**Vig80**] 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 by $B = \left(\dfrac{a,b}{F}\right)$.

Example. As examples of quaternion algebras, we have the ring of 2×2-matrices over F, or $M_2(F) \cong \left(\dfrac{1,1}{F}\right)$, and the division ring $\mathbb{H} = \left(\dfrac{-1,-1}{\mathbb{R}}\right)$ 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 $B = \left(\dfrac{a,b}{F}\right)$, 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 [**Kat92**, 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 [**Kat92**, §5.2] and is known as a *Shimura curve*.

From now on, we assume that $B \not\cong M_2(\mathbb{Q})$, 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 [**Kat92**, 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 $\operatorname{disc}(B) = 6$, i.e. B is ramified at the primes 2 and 3, and unramified at all other places, including ∞. Explicitly, we may take $B = \left(\dfrac{-1, 3}{\mathbb{Q}}\right)$, 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 [**AB04**, §5.5.2] or [**KV03**, §5.1].)