

Shimura curve computations

John Voight

University of Sydney

University of Minnesota (2006–2007)

University of Vermont (2007–)

Clay Mathematics Institute Summer School

Georg-August-Universität, Göttingen

2 August 2006

Introduction

In this talk, we give some concrete examples of Shimura curves and do some explicit computations with them.

“[W]ithout the security blanket of your evidence, I would never have dared a proof. . . . The fun of the subject seems to me to be in the examples.” —Gross to Birch, 1982

- Quaternion algebras.
- Shimura curves as Riemann surfaces.
- Shimura curves as moduli spaces.
- Example: Discriminant 6.
- Triangle groups.
- Second example: $(2, 3, 9)$ -triangle group.

Motivation: 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

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

This group acts on the completed upper half-plane \mathfrak{H}^* 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} .

Quaternion algebras: Definition

Now we seek to generalize this set-up coming from modular curves.

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 $\text{char } F \neq 2$. 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 $\alpha, \beta \in A$ which generate B such that

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

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

Example. Of course, $M_2(F) \cong \left(\frac{1, 1}{F}\right)$. And we have 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 .

Quaternion algebras: Properties

The quaternion algebra B has a unique involution $\bar{} : B \rightarrow B$, called *conjugation*, with the property that $\alpha\bar{\alpha} \in F$ for all $\alpha \in B$. The map $\text{nrd}(\alpha) = \alpha\bar{\alpha}$ 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

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

Now assume that F is 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* $\text{disc}(B)$ of B .

Let \mathbb{Z}_F denote the ring of integers of F . An *order* of B is a subring $\mathcal{O} \subset B$ 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 in our situation, they will be unique up to conjugation in B .

Shimura curves as Riemann surfaces

Let $\mathcal{O} \subset B$ be a maximal order. Then we may define the group analogous to $SL_2(\mathbb{Z})$, namely $\mathcal{O}_1^* = \{\gamma \in \mathcal{O} : \text{nrd}(\gamma) = 1\}$.

In order to obtain a discrete subgroup of $PSL_2(\mathbb{R})$, we need that F is a totally real field and that B is split at exactly one real place, so that

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

where \mathbb{H} is the ring of Hamiltonians. 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.

We now assume that $B \not\cong M_2(\mathbb{Q})$ (the case of modular curves), and hence B is a division ring and $X^B(1)_{\mathbb{C}}$ is compact.

Example: Discriminant 6

We now make this theory concrete!

We take $F = \mathbb{Q}$ and we consider the quaternion algebra B over \mathbb{Q} with $\text{disc}(B) = 6$, i.e. B is ramified at the primes 2 and 3. We have $B = \left(\frac{-1, 3}{\mathbb{Q}} \right)$, so that $\alpha, \beta \in B$ satisfy

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

We find the maximal order

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\delta$$

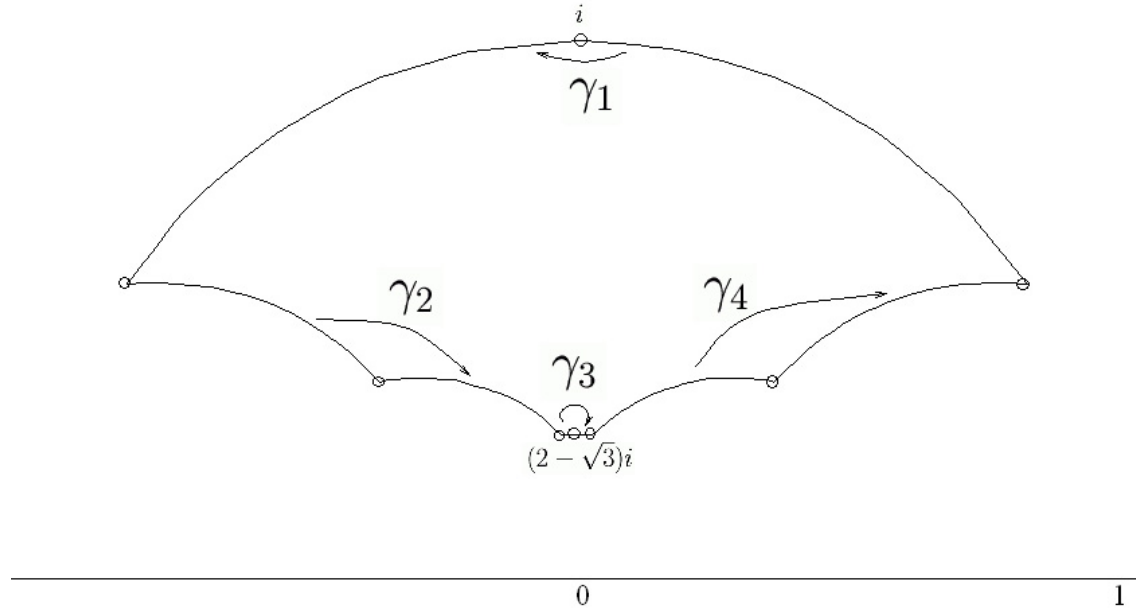
where $\delta = (1 + \alpha + \beta + \alpha\beta)/2$, and we have an embedding

$$\iota_\infty : A \rightarrow M_2(\mathbb{R})$$

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

Example: Fundamental domain

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.



The elements

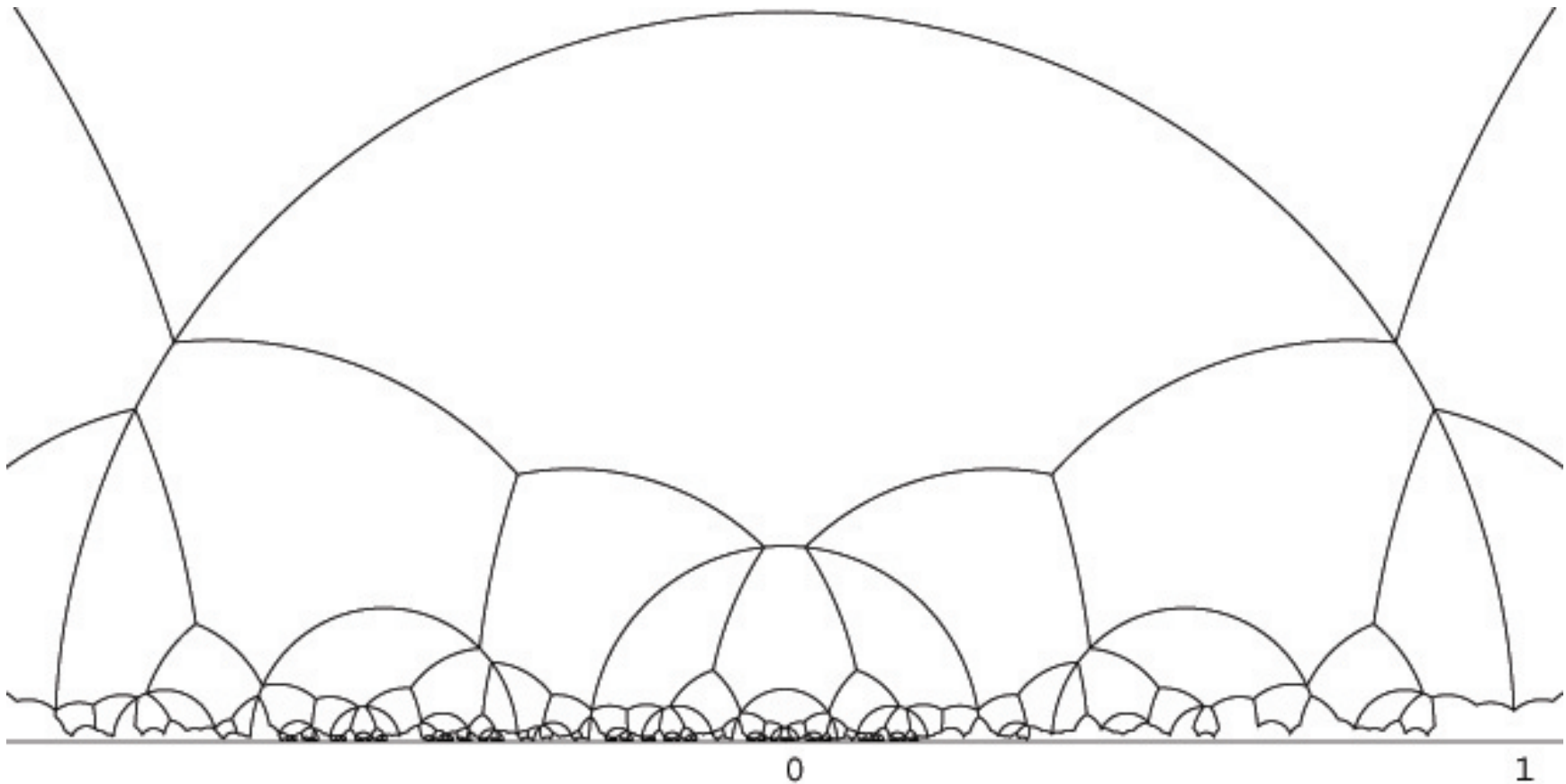
$$\gamma_1 = \alpha, \quad \gamma_2 = \alpha + \delta, \quad \gamma_3 = 2\alpha + \alpha\beta, \quad \gamma_4 = 1 + \alpha - \beta + \delta$$

are known as *side-pairing elements*. This yields the presentation

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

Example: Tessellation

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



(The algorithm for drawing hyperbolic polygons is due to Helena Verrill.)

Example: Signature and genus

One can compute the area of the above fundamental domain D by triangulation, but we also have the formula

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

The genus g can then 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

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

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

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

Thus we have a map $X^B(1)_{\mathbb{C}} \rightarrow \mathbb{P}_{\mathbb{C}}^1$.

Shimura curves as moduli spaces

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

To simplify the exposition, we now assume that the totally real field F has narrow class number 1 (written $h^+(F) = 1$); for example, we may take $F = \mathbb{Q}$.

Under this hypothesis, the curve $X^B(1)$ is the coarse moduli space for pairs (A, ι) , where:

- A is an abelian variety of dimension $2[F : \mathbb{Q}] = 2n$, and
- $\iota : \mathcal{O} \hookrightarrow \text{End}(A)$ is an embedding of involutive algebras.

We say that such an A has *QM by* \mathcal{O} .

It follows from this moduli description that there exists a *canonical model* $X^B(1)_F$ for $X^B(1)_{\mathbb{C}}$ defined over F (Shimura, Deligne).

Example: Models

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

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

This identification can be made quite explicit (Baba-Granath). 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 $f : \mathfrak{H} \rightarrow \mathbb{C}$ 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 a 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 $X^B(1)_{\mathbb{C}} \rightarrow X^B(1)_{\mathbb{Q}}$.

CM points

On the modular curves $X_0(N)$, we have *CM points* which correspond to isogenies between elliptic curves with extra endomorphisms, namely, those elliptic curves which have CM by an imaginary quadratic field K . CM points are defined over ring class extensions H of K and the Shimura reciprocity law describes explicitly the action of $\text{Gal}(H/K)$ 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. $B \otimes_F K \cong M_2(K)$. CM points on $X^B(1)$ correspond to abelian varieties A of dimension $2[F : \mathbb{Q}] = 2n$ with endomorphism algebra $\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M_2(K)$.

K splits B if and only if there exists an embedding $\iota_K : K \hookrightarrow B$; the map ι_K is concretely given by an element $\mu \in \mathcal{O}$ such that $\mathbb{Z}_F[\mu] = \mathbb{Z}_K$, where \mathbb{Z}_F and \mathbb{Z}_K denote the respective rings of integers. Let $z = z_D$ be the fixed point of $\iota_\infty(\mu)$ in \mathfrak{H} ; we then say z is a *CM point* on $X^B(1)_{\mathbb{C}}$.

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.

Example: CM points

We return to our example with $F = \mathbb{Q}$ and $\text{disc}(B) = 6$.

The following computation is due to Elkies and Baba-Granath.

Let $K = \mathbb{Q}(\sqrt{-19})$, and $\mathbb{Z}_K = \mathbb{Z}[(1 + \sqrt{-19})/2]$. We have $\# \text{Cl}(\mathbb{Z}_K) = 1$, 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 $\text{End}(J(C)) \cong M_2(\mathbb{Z}_K)$. 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 $\text{Aut}(C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

Atkin-Lehner involutions

Recall that $X^B(1)$ parametrizes pairs (A, ι) , where A is an abelian variety (over \mathbb{C} , say) with QM by \mathcal{O} specified by $\iota : \mathcal{O} \hookrightarrow \text{End}(A)$. But there may be more than one such embedding ι , even up to isomorphism!

For each prime divisor $\mathfrak{m} \mid \text{disc}(B)$, there is an *Atkin-Lehner involution*

$$w_{\mathfrak{p}} : X^B(1)_F \rightarrow X^B(1)_F$$

$$(A, \iota) \mapsto (A, \iota^{\mathfrak{m}})$$

where $\iota^{\mathfrak{m}}$ is corresponding *twist* of ι . These involutions generate a subgroup W of $\text{Aut}(X^B(1)_F)$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^e$, where e is the number of prime divisors of $\text{disc}(B)$.

All such twists arise in this way, and therefore the quotient $X^{B^*}(1)_F$ by all 2^e such Atkin-Lehner involutions parametrizes abelian varieties with QM by \mathcal{O} without a particular choice of embedding ι .

Looking at this in another way, the group

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

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

Example: Atkin-Lehner quotient

In our running example, we have $X = X^B(1) : x^2 + 3y^2 + z^2 = 0$.

The two Atkin-Lehner involutions w_2, w_3 act by

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

The quotients are therefore

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

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

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

under our normalization.

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

The $(2, 4, 6)$ -triangle group

Recall that the group

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

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

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

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

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

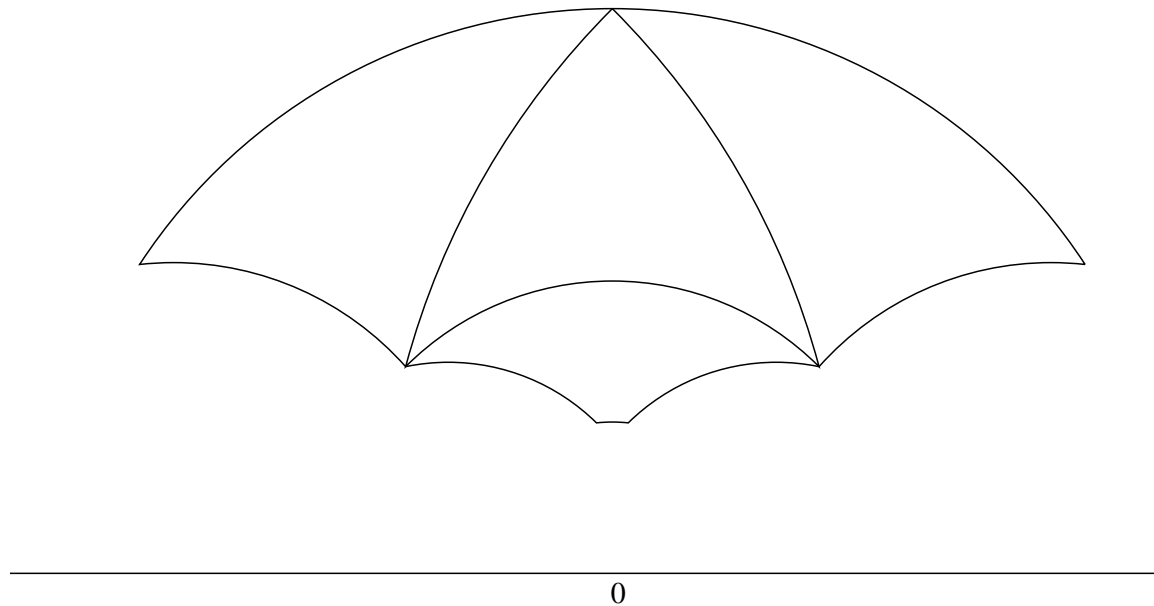
$$\Gamma^{B^*}(1) \cong \langle s_2, s_4, s_6 \mid s_2^2 = s_4^4 = s_6^6 = s_6 s_4 s_2 = 1 \rangle$$

where $s_2 = -1 + 2\alpha - \beta + 2\delta$, $s_4 = -1 + \alpha$, $s_6 = -2 + \alpha + \delta$ have $\text{nrd}(s_2) = 6$, $\text{nrd}(s_4) = 2$, $\text{nrd}(s_6) = 3$.

This group 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.

The $(2, 4, 6)$ -triangle group: Fundamental domain

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



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

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

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* $\Gamma^{B^*}(1)$. Already these contain a number of highly interesting curves! In this light, we consider $SL_2(\mathbb{Z})$ 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 $j : X^{B^*}(1) \rightarrow \mathbb{P}_{\mathbb{C}}^1$. (In fact, the canonical model for $X^{B^*}(1)_{\mathbb{C}}$ over F is already \mathbb{P}_F^1 .) 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 $0, 1, \infty$.

Explicit computation of CM points

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

Theorem (V). *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 $\text{Gal}(H/K)$.*

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

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 $B \cong \left(\frac{-3, b}{F} \right)$, i.e. B is generated by α, β with

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

Here, we have $\text{disc}(B) = \mathbb{Z}_F$, 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

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

Second example

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

$$\zeta = -\frac{1}{2}b + \frac{1}{6}(2b^2 - b - 4)\alpha$$

$$\eta = -\frac{1}{2}b\beta + \frac{1}{6}(2b^2 - b - 4)\alpha\beta$$

$$\omega = -b + \frac{1}{3}(b^2 - 1)\alpha - b\beta + \frac{1}{3}(b^2 - 1)\alpha\beta.$$

By work of Takeuchi, 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

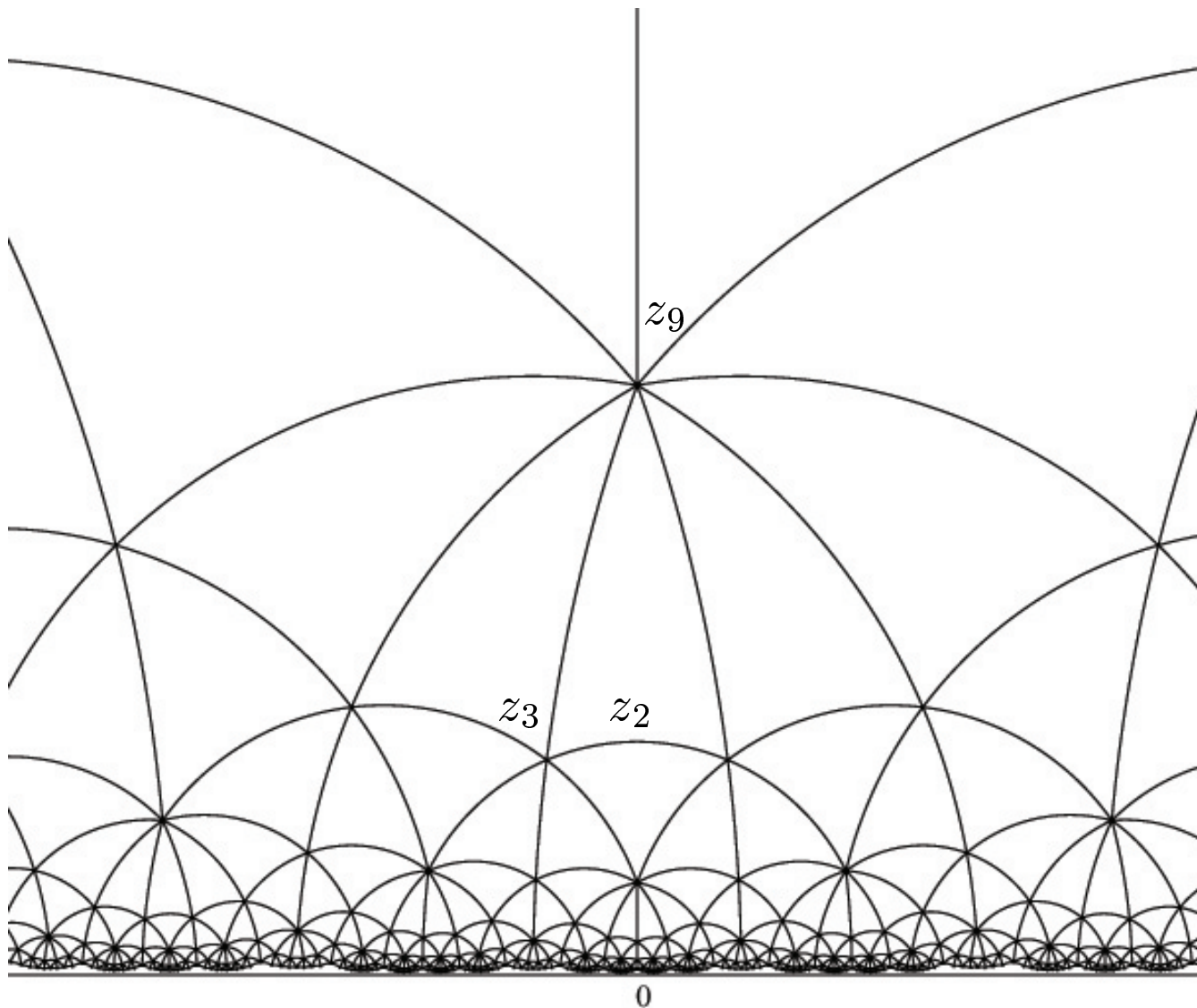
$$s_2^2 = s_3^3 = s_9^9 = s_2 s_3 s_9 = 1.$$

The fixed points of these elements are

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

and they form the vertices of a fundamental triangle.

Second example: Fundamental triangles



Each such triangle is the union of two fundamental triangles.

Second example: CM points

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 $j(z) = 17137.9737\dots$ as well as its Galois conjugates $0.5834\dots \pm 0.4516\dots i$, which yields the minimal polynomial for $j = j(z)$

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

to the precision computed (300 digits). Note that

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

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

Second example: CM points

Large examples can be computed, including over ring class extensions!

Consider the field $K = F(\sqrt{-5})$ with discriminant $\text{disc}(K/F) = -20$. 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 $14 = \#\text{Cl}(\mathbb{Z}_{K,f})$, 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

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

Conclusion

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 from to the setting of Shimura curves. These curves, which although at first are only abstractly defined, can also be made very concrete.

Shimura curves arise from generalizing constructions from $M_2(\mathbb{Q})$ to certain quaternion algebras over totally real fields F . Shimura curves admit a description as a Riemann surface, and from a fundamental domain we can “see” what the curve looks like over \mathbb{C} . Shimura curves also admit a description as a moduli space, which gives an equation for this curve over F . In analogy with modular curves they come equipped with CM points.

There exist algorithms to do explicit computations with the simplest Shimura curves, and from these examples we can already see some of the “fun of the subject”.