THREE LECTURES ON SHIMURA CURVES

JOHN VOIGHT

Abstract. These notes are taken from a lecture series in three parts given at the University of Sydney in April 2006. In the first part, we introduce Shimura curves for the non-expert, avoiding technicalities. In the other two sections, we discuss the moduli interpretation of Shimura curves and treat some of the computational aspects.

Ever wondered what a Shimura curve is? They lie at the crossroads of many areas of mathematics: complex analysis, number theory, Diophantine equations, group theory, noncommutative algebra, algebraic geometry, Lie theory—even coding theory! The study of the first examples of these curves (the modular curves) can be traced back as far back as Gauss, and then later Klein and Fricke; recently, they have played an important role in the proof of Fermat's last theorem and in the solution of other number theoretic problems. In the first section, we introduce Shimura curves for the non-expert with an algebraic outlook and provide a brief exposition of their relationship to other areas of mathematics.

In the second section, we switch gears to treat a much more technically involved subject, intended for the reader who wishes to know more details. Over the complex numbers, a Shimura curve is simply a Riemann surface which is uniformized by an arithmetic Fuchsian group. Such curves in fact have a much richer structure: they are (coarse) moduli spaces for certain abelian varieties with "extra endomorphisms". We present an abbreviated account of this theory which will focus on the cases of curves over the rational numbers.

In the final section, we treat computational aspects of Shimura curves. The study of the classical modular curves has long proved rewarding for number theorists both theoretically and computationally, and an expanding list of conjectures have been naturally generalized from this setting to that of Shimura curves. Recently, computational aspects of these curves been explored in more depth and we discuss some of the central algorithmic problems in this area.

These notes are in rough form and are very underdeveloped, so comments and requests are welcome!

1. Survey of Shimura curves

In this section, we provide an extended and hopefully well-motivated introduction to Shimura curves. The expert reader should excuse a few white lies, which are made for the purposes of exposition. We will start at the very beginning and at each stage see how Shimura curves arise as a natural generalization.

1.1. The j-line.

The most "famous" Shimura curve is the j-line, which over the complex numbers $\mathbb{C}$ is just the complex plane, with coordinate j; by stereographic

Date: April 16, 2006.

projection, we see more properly that the j-line is the (punctured) Riemann sphere, so we add the point at ∞ to compactify. So what makes this sphere so special?

It all goes back to Gauss, who (in one formulation) was interested in quadratic *forms* $Q = Ax^2 + Bxy + Cy^2$ where $A, B, C \in \mathbb{Z}$ with $A > 0$ and discriminant $D = B^2 - 4AC < 0$. He was interested in the set of forms up to *equivalence*, i.e. up to the action of $SL_2(\mathbb{Z})$, where

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}, \quad \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

This action corresponds to an invertible change of variables in the quadratic form, so e.g. two equivalent forms represent the same primes, have the same discriminant, and so on. (We notice that $-1 \in SL_2(\mathbb{Z})$ acts trivially on the set of forms, so one should look at $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$; we will for the most part ignore this subtletly, and freely associate an element $\gamma \in SL_2(\mathbb{Z})$ with its class $\pm\gamma \in PSL_2(\mathbb{Z})$, and vice versa.)

Setting $y = 1$ in $Q = Ax^2 + Bxy + Cy^2$, we obtain the quadratic polynomial $Ax^2 + Bx + C$ which has two complex conjugate roots, hence a unique root τ in the upper half plane $\mathfrak{H} = \{x + yi \in \mathbb{C} : y > 0\}$. The action of the group $SL_2(\mathbb{Z})$ on the set of forms corresponds to an action on this root τ by

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

Thus, in order to choose a distinguished representative Q within an equivalence class of forms, we need to choose a distinguished $\tau \in \mathfrak{H}$ in the orbit of $SL_2(\mathbb{Z})$.

One then proves that in each $SL_2(\mathbb{Z})$-orbit, there is at least one τ such that $|\operatorname{Re}\tau| \leq 1/2$ and $|\tau| \geq 1$, and exactly one away from the boundary of this region, known as a *fundamental domain*. The element $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ identifies the circular arcs on either side of the fixed point i, and the element $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ identifies the vertical lines; and under these gluing relations, we obtain exactly a (punctured) Riemann sphere! (Near the points i and $\rho = e^{2\pi i/3}$, one has to take the appropriate neighborhoods to account for the nontrivial stabilizers, but we will sweep this under the rug for now.) It is known as the j-line for reasons we will discuss later.

That gives one solution to Gauss' problem. But what is really going on here? What more general phenomena are evident in this example?

1.2. **Fuchsian groups.** To begin with, the upper half-plane $\mathfrak{H}$ has geometry: it has a metric given by

$$ds^2 = \frac{dx^2 + dy^2}{y^2},$$

which gives a notion of distance and angle, and an area (or volume) given by $d\mu = (1/y^2)\,dx\,dy$. (This hyperbolic metric has been featured in the lithographs of M.C. Escher, where often he instead considers the Poincaré unit disc, to which one can map $\mathfrak{H}$ conformally.)

Given this metrized real topological space, we are then led to consider the group of orientation-preserving isometries of $\mathfrak{H}$, which is the group $PSL_2(\mathbb{R})$. In Gauss' problem we considered $PSL_2(\mathbb{Z}) \subset PSL_2(\mathbb{R})$, which is a *discrete* subgroup—indeed, the action of $PSL_2(\mathbb{R})$ on $\mathfrak{H}$ is transitive. But the group of one element is also discrete, so in fact we had something more. Stepping back, we had a discrete subgroup $\Gamma \subset PSL_2(\mathbb{R})$ such that the orbit space $X = \Gamma\backslash\mathfrak{H}$ has finite volume; such a group is known as a *Fuchsian group.*

So what are some other famous Fuchsian groups? It is natural to start by looking at subgroups of $SL_2(\mathbb{Z})$. For example, for each $N \in \mathbb{Z}_{>0}$, we have the subgroup

$$\Gamma(N) = \left\{\gamma \in SL_2(\mathbb{Z}) : \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}.$$

We again obtain quotients $X(N) = \Gamma(N)\backslash\mathfrak{H}$ (after compactification); a fundamental domain for the action of $\Gamma(N)$ is a union of $SL_2(\mathbb{Z})$-translates of the triangles from $PSL_2(\mathbb{Z})$. For $N = 1, 2, 3, 4, 5$ (and these values only), we obtain Riemann spheres; for $N = 3, 4, 5$, the triangular tesselations of the sphere yield the tetrahedron, the octahedron, and the icosahedron, respectively. (It is certainly reassuring that along our merry generalizing way, we encounter the classical Platonic solids!)

Similarly, the *congruence* subgroups

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

give the *modular curves* $X_0(N)$. Modular curves are quite famous in their own right, but they are also just examples of Shimura curves!

We have seen then to get interesting ("arithmetic") curves, we went from $PSL_2(\mathbb{R})$ all the way down to the subgroup $PSL_2(\mathbb{Z})$. There is certainly a lot of room in between! What about others? For any ring $\mathbb{Z} \subsetneq R \subset \mathbb{R}$, we might try $PSL_2(R)$, but this group is unfortunately never discrete. So we need to try something else.

We look again at the group $SL_2(\mathbb{Z})$; it generates the $\mathbb{Q}$-algebra $M_2(\mathbb{Q})$, and we recover $SL_2(\mathbb{Z})$ as the group of the elements of determinant 1 in $M_2(\mathbb{Q})$. So we should look for other algebras B which are similar to $M_2(\mathbb{Q})$.

1.3. **Quaternion algebras.** So what about the matrix ring is special? A ring theorist will tell you that $B = M_2(\mathbb{Q})$ is a *central simple algebra* over $\mathbb{Q}$: *central* because the center of B is $\mathbb{Q}$; *simple* because any B has no nontrivial two-sided ideals, so that any ring homomorphism $B \to C$ is either the zero map or injective, like for simple groups.

So let F be a field. We define a *quaternion algebra* over F to be a central simple F-algebra of dimension 4. Equivalently, if $\operatorname{char} F \neq 2$, an F-algebra B is a quaternion algebra if and only if there exist $\alpha, \beta \in B$ 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 $\left(\dfrac{a,b}{F}\right)$.

We recover the matrix ring $M_2(F) \cong \left(\dfrac{1,1}{F}\right)$, via $\alpha \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\beta \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Over the real numbers $\mathbb{R}$, we have the ring of *real Hamiltonians* $\mathbb{H} = \left(\dfrac{-1,-1}{\mathbb{R}}\right)$, more traditionally generated by elements i, j with $i^2 = j^2 = (ij)^2 = -1$. Over $\mathbb{R}$, there are only two quaternion algebras up to isomorphism, namely, $\mathbb{H}$ and $M_2(\mathbb{R})$. (In fact, $\mathbb{H}$ is the only (associative) noncommutative division algebra over $\mathbb{R}$, a fact which is originally due to Frobenius.)

Now let B be a quaternion algebra over a field F, and let $\sigma : F \hookrightarrow \mathbb{R}$ be an embedding. Then extending scalars, we obtain $B \otimes_F \mathbb{R}$ which is now a quaternion algebra over $\mathbb{R}$; we say B is *split* at σ if $B \otimes_F \mathbb{R} \cong M_2(\mathbb{R})$, and otherwise B is *ramified*.

For our considerations, there is no loss in restricting to fields F which are finite-dimensional over $\mathbb{Q}$, so let F be a number field. A quaternion algebra B over F has a *maximal order* $\mathcal{O} \subset B$, analogous to $\mathbb{Z} \subset \mathbb{Q}$ and $M_2(\mathbb{Z}) \subset M_2(\mathbb{Q})$. There exists also a multiplicative norm map $\operatorname{nrd} : B \to F$ which is analogous to the determinant $\det : M_2(\mathbb{Q}) \to \mathbb{Q}$.

1.4. **Finally, Shimura curves.** We then consider the group analogous to $SL_2(\mathbb{Z})$, namely the group of units of norm 1 in $\mathcal{O}$:

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

Suppose now that F has a real embedding $\sigma : F \hookrightarrow \mathbb{R}$, and that B is split at σ; then we have a map $\mathcal{O}_1^* \hookrightarrow SL_2(\mathbb{R})$; let $\Gamma^B(1)$ denote its image.

It turns out that the group $\Gamma^B(1)$ is a Fuchsian group if and only if F is *totally real* (i.e. every embedding of $F \hookrightarrow \mathbb{C}$ has image in $\mathbb{R}$) and B is ramified at all other real embeddings $\tau \neq \sigma$. (For F totally real, in the other cases we obtain varieties of higher-dimension.) A quaternion algebra B is said to be *indefinite* if B has a split real place.

We define an *arithmetic Fuchsian group* $\Gamma \subset PSL_2(\mathbb{R})$ to be any subgroup which is *commensurable* with a group $\Gamma^B(1)$ for some quaternion algebra B over a totally real field which is split at exactly one real place. (Groups G, G' are *commensurable* if $G \cap G'$ is of finite index in G, G'.)

Finally, a *Shimura curve* is a quotient $\Gamma \backslash \mathfrak{H}$ where Γ is an arithmetic Fuchsian group.

The 19th century pioneers who studied the congruence subgroups of $SL_2(\mathbb{Z})$ investigated these groups as enthusiastically as the regular modular curves. Some inroads proved much harder to pursue, however; see the sections that follow for some of the reasons why.

We now conclude this section with some examples and applications, with few details.

1.5. **More famous Shimura curves.** The next most "famous" Shimura curve is the Klein quartic C, given by the affine equation $y^7 = x^3 - x^2$, or more symmetrically by the projective equation $u^3v + v^3w + w^3u = 0$. It can be obtained in our setting in *two* different ways. We first have it as a modular curve $C \cong X(7)$. But C is also a Shimura curve X! We take the field $F = \mathbb{Q}(\theta)$, where $\theta = 2\cos(2\pi/7)$ (otherwise known as the the totally real subfield of $\mathbb{Q}(\zeta_7)$), the quaternion algebra $B = \left(\dfrac{\theta, \theta}{F}\right)$, and the group

$$\Gamma = \{\gamma \in \mathcal{O}_1^* : \gamma \equiv 1 \pmod{\mathfrak{p}_7}\}$$

where $\mathfrak{p}_7$ is the unique prime of the ring of integers $\mathbb{Z}_F$ of F above 7. Then $C \cong X(\Gamma)$.

In this case, we have an abstract presentation

$$\mathcal{O}_1^* \cong \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle$$

so that $\mathcal{O}_1^*$ is known as the $(2,3,7)$-*triangle group*. This name comes from the fact that a fundamental domain for $\mathcal{O}_1^*$ (embedded in $PSL_2(\mathbb{R})$) is the union of two hyperbolic triangles with angles $\pi/2, \pi/3, \pi/7$.

In fact, it is a theorem of Hurwitz that over a field of characteristic zero, a curve C of genus $g > 2$ has at most $84(g-1)$ automorphisms. Any curve that meets this upper bound is called a *Hurwitz curve*. The Klein curve C is such an example: It has automorphism group $PSL_2(\mathbb{F}_7)$ of order 168, the second smallest nonabelian simple group. In fact, it follows that a complex curve is a Hurwitz curve if and only if it is uniformized by a group commensurable with the $(2,3,7)$-triangle group. (This leads to many interesting questions in group theory!)

1.6. **Moduli spaces and Fermat's last theorem.** Shimura curves have found wide-ranging applications in number theory, including a dual role in the proof of Fermat's last theorem.

Recall we began with the j-line, $SL_2(\mathbb{Z})\backslash\mathfrak{H}$; this parametrizes elliptic curves over $\mathbb{C}$ by their j-invariant, hence the name. An elliptic curve $E = \mathbb{C}/\Lambda$ is a complex torus, where $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ is a lattice with $\tau \in \mathfrak{H}$; two elements $\tau, \tau' \in \mathfrak{H}$ give the same lattice (and hence the same elliptic curve) if and only if τ, τ' are in the same $SL_2(\mathbb{Z})$-orbit. In a similar way, the modular curves $X_0(N)$ and $X(N)$ parametrize elliptic curves equipped with a cyclic subgroup of order N and with full N-torsion, respectively.

It follows from this description as moduli spaces that these curves are not just Riemann surfaces—they actually arise as the complex points of a curve defined over $\mathbb{Q}$. Secretly, Shimura curves are also moduli spaces! Namely, they parametrize certain abelian varieties with endomorphism algebra B. (In §2, we will give a more precise formulation of these notions.) Shimura (and Deligne) proved that for every such quaternion algebra B over a totally real field F, there is a field F' called the *reflex field* such that the corresponding Shimura curve X is canonically defined over F'. For example, when F has narrow class number one, e.g. $F = \mathbb{Q}$, and $\Gamma = \Gamma^B(1)$, then $F' = F$.

The Shimura-Taniyama conjecture, now a theorem proved by Wiles et al., claims that every elliptic curve E over $\mathbb{Q}$ is modular, meaning there is a nonconstant morphism $\phi : X_0(N) \to E$ where N is the conductor of E. Ribet proved that this conjecture (in the semistable case) implies Fermat's last theorem. He does this by proving a particular case of the *epsilon conjecture* of Serre, interrelating the reductions of the Néron model of the Jacobian of a Shimura curve and a modular curve!

More generally, many theorems (and conjectures) for modular curves can be naturally generalized to the setting of Shimura curves.

1.7. **Other applications.** Meromorphic functions on $\mathfrak{H}$ which "transform well" under a Fuchsian group Γ are known as *automorphic functions*, or *modular functions* when Γ is commensurable with $SL_2(\mathbb{Z})$. For example, the j-function is a modular function since it is invariant under $SL_2(\mathbb{Z})$. Such functions which are holomorphic are called automorphic (or modular) *forms*.

The Langlands philosophy predicts that the L-functions obtained from Shimura curves should cover a very large and important class of the good (algebraic automorphic) L-functions. Higher dimensional analogues of Shimura curves, known as Shimura varieties, are used in the proof of the local Langlands conjecture for GL_n by Harris and Taylor.

Lie theorists arrive at the study of quaternion algebras and Shimura curves as well: after all, Fuchsian groups are discrete subgroups (hence a lattice) inside the semisimple Lie group $PSL_2(\mathbb{R})$.

Further careful analysis of the moduli interpretation for Shimura curves gives an integral model for these curves, so we can reduce a Shimura curve modulo a prime ideal of the ring of integers $\mathbb{Z}_F$ of F. This gives rise to prime powers q and towers of Shimura curves defined over $\mathbb{F}_q$ which have $(q-1+o(1))g$ points defined over $\mathbb{F}_{q^2}$, where the genus $g \to \infty$ in the tower. This is the largest possible number of points asymptotically, by a theorem of Drinfeld-Vlăduţ. Via a construction of Goppa this tower of curves gives rise to explicit error-correcting codes of surprisingly high quality, surpassing the so-called Varshamov-Gilbert bound.

The ramification data and Galois group G of a cover $X' \to X$ of Shimura curves can be determined from the arithmetic data; when $X \cong \mathbb{P}^1$, this gives rise to branched covers of the projective line. When X, X' are defined over $\mathbb{Q}$, by specialization, one may obtain infinitely many linearly disjoint extensions of $\mathbb{Q}$ with Galois group G, by a theorem of Hilbert. For example, this gives realizations of the group $PSL_2(\mathbb{F}_q)$ for certain prime powers q.

Finally, when X arises from a triangle group, then certain special points (*CM points*) give rise to triples of coprime $A, B, C \in \mathbb{Z}_F$ with many repeated factors and such that $A + B = C$. For example, for $F = \mathbb{Q}$, we obtain in a geometric way

$$107^2 + 2^{15} = 3^2 17^3.$$

There are many other surpising appearances and amusing applications of Shimura curves in mathematics!

2. Shimura curves as moduli spaces

We have seen in §1 a whirlwind survey of Shimura curevs. We started with the j-line, and at a certain moment we went from a Shimura curve, given just as Riemann surface, to a curve defined over a number field; we did that by claiming that the Shimura curve can be given a moduli interpretation. In this section, we explain bits of that claim; our attempt is to provide as "quick and dirty" an approach as possible: it surely is a long way to go, from $\mathbb{C}$ to a number field—and eventually, in theory, to a ring of integers—so we are contented just to give an overview, leaving the details to the many technical treatments in the literature.

2.1. Moduli over $\mathbb{C}$: Abelian surfaces.

The set of elliptic curves E over $\mathbb{C}$ up to isomorphism is in bijection with the set of lattices $\{\mathbb{Z} + \mathbb{Z}\tau : \tau \in \mathfrak{H}\}$ up to the action of $SL_2(\mathbb{Z})$, hence in bijection with the set $SL_2(\mathbb{Z})\backslash\mathfrak{H} = Y(1)_{\mathbb{C}}$, which can be given the structure of (compactified) Riemann surface. Similarly, for $N \in \mathbb{Z}_{>0}$,

$$\cong \backslash\{(E, C) : E/\mathbb{C} \text{ an elliptic curve, } C \subset E[N] \text{ cyclic of order } N\}$$

is in bijection with $\Gamma_0(N)\backslash\mathfrak{H} = Y_0(N)_{\mathbb{C}}$, and

$$\cong \backslash\{(E, \alpha) : E/\mathbb{C} \text{ an elliptic curve, } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]\}$$

is in bijection with $\Gamma(N)\backslash\mathfrak{H} = Y(N)_{\mathbb{C}}$.

In the next higher dimension, we encounter (principally polarized) abelian surfaces. Although every abelian surface $A/\mathbb{C}$ is given as $\mathbb{C}^2/\Lambda$ for $\Lambda \subset \mathbb{C}^2$ a lattice, the quotient must carry sufficiently many meromorphic functions, so not every lattice gives rise to an abelian surface. Therefore, we consider the *Siegel upper-half space*

$$\mathfrak{H}_2 = \{\tau \in M_2(\mathbb{C}) : \tau^t = \tau, \mathrm{Im}(\tau) > 0\},$$

and to any $\tau \in \mathfrak{H}_2$, we associate the lattice $\Lambda_\tau = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2 \subset \mathbb{C}^2$ and hence the surface $A_\tau = \mathbb{C}^2/\Lambda_\tau$. Every complex abliean surface arises in this way, and any two τ, τ' give rise to isomorphic abelian surfaces if and only if they are in the same orbit under the group

$$\mathrm{Sp}(2,\mathbb{Z}) = \{U \in M_4(\mathbb{Z}) : U^t J U = J\}, \quad \text{where } J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

where

$$\tau \mapsto (a\tau + b)(c\tau + d)^{-1} \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sp(2,\mathbb{Z}).$$

These are known as the *Riemann relations.*

(For the experts, we choose the principal polarization L_τ, which maps under the Chern class map to the Riemann form

$$E_\tau(\lambda, \mu) = \langle x_1, y_2 \rangle - \langle x_2, y_1 \rangle$$

for $\lambda = \tau x_1 + x_2$, $\mu = \tau y_1 + y_2$. This extends to an $\mathbb{R}$-bilinear form $\mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{R}$ by $E(i\lambda, i\mu) = E(\lambda, \mu)$, which gives a (Hermitian) Riemann form $H(\lambda, \mu) = E(i\lambda, \mu) + iE(\lambda, \mu)$.)

Therefore the parameter space for abelian surfaces is the quotient

$$\mathcal{A}_2 = Sp(2,\mathbb{Z})\backslash\mathfrak{H}_2;$$

the complex space $\mathcal{A}_2$ is a quasi-projective variety over $\mathbb{C}$ of dimension 3 known as *Igusa's threefold.* (The Satake compactification is a quotient of $\mathbb{P}^3$ by a finite group of order 46080.) Unlike the j-line of dimension 1, the new feature of $\mathcal{A}_2$ is that there are many subvarieties. In a similar way to elliptic curves, we can add level structure, but let us first cut down on the dimension!

2.2. **Special subvarieties over $\mathbb{C}$.** We look for certain special subvarieties of $\mathcal{A}_2$. For example, if $E/\mathbb{C}$ is an elliptic curve, then $A = E \times E$ is an abelian surface; together these give a subvariety

$$\cong \backslash \left\{ \begin{pmatrix} \tau & 0 \\ 0 & \tau \end{pmatrix} : \tau \in \mathfrak{H} \right\} \hookrightarrow \mathcal{A}_2$$

which is isomorphic to the complex affine line. Note that

$$\mathrm{End}(A) = M_2(\mathrm{End}(E)) \supset M_2(\mathbb{Z}).$$

Therefore, this subvariety is distinguished by the fact that the corresponding lattices have extra symmetries, or equivalently the abelian surfaces have extra endomorphisms. What possibilities may occur?

Theorem (Albert)**.** *Let A be a complex abelian surface. Then* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is one of the following:*

(i) $\mathbb{Q}$*;*
(ii) *A real quadratic field K;*
(iii) *An indefinite quaternion algebra B over $\mathbb{Q}$;*
(iv) *A quartic CM field K;*
(v) *$M_2(K)$, where K is an imaginary quadratic field.*

The dimension of the corresponding subvarieties of $\mathcal{A}_2$ is $3, 2, 1, 0, 0$, respectively. Notice that our embedded j-line corresponds to case (iii) with $B = M_2(\mathbb{Q})$.

Let B be an indefinite quaternion algebra over $\mathbb{Q}$. A complex abelian surface A as in (iii) is said to have *quaternionic multiplication (QM)* by B. There exists a unique maximal order $\mathcal{O} \subset B$ up to conjugation in B, and we have a map

$$\iota_\infty : B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}).$$

We define as in §1 the group $\mathcal{O}_1^* = \{\gamma \in \mathcal{O} : \operatorname{nrd}(\gamma) = 1\}$, and let

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

Now we consider the set

$$\cong \backslash\{(A, \iota) : A/\mathbb{C} \text{ an abelian surface}, \iota : \mathcal{O} \hookrightarrow \operatorname{End}(A)\}.$$

(The order $\mathcal{O}$ has a distinguished involution called conjugation; similarly, the ring $\operatorname{End}(A)$ has the Rosati involution. We therefore view the embedding ι as an embedding of *involutive rings*, so that ι respects the involution: Specifically, $\iota(\beta)^\circ = \iota(\overline{\beta})$.)

We now claim that this set can be made in natural bijection with $\Gamma^B(1)\backslash\mathfrak{H} = X^B(1)_{\mathbb{C}}$ as follows. We may extend ι_∞ to a map $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{C} \to M_2(\mathbb{C})$. To $\tau \in \mathfrak{H}$, we associate the lattice $\Lambda_\tau = \iota_\infty(\mathcal{O})\begin{pmatrix}\tau \\ 1\end{pmatrix} \subset \mathbb{C}^2$ (and the abelian surface $A_\tau = \mathbb{C}^2/\Lambda_\tau$); two such lattices, associated to τ, τ', yield isomorphic abelian varieties if and only if $\gamma\tau = \tau'$ for some $\gamma \in \mathcal{O}_1^*$.

The "forgetful" map which forgets the embedding ι gives a map of moduli from the above set to $\mathcal{A}_2$ which is not an embedding (due to the presence of isomorphisms); it is of degree 2 in all but finitely many cases. An explicit map $X^B(1)_{\mathbb{C}} \to \mathcal{A}_2$ depends on a choice of $\mu \in \mathcal{O}$ with $\mu^2 \in \mathbb{Z}_{<0}$, a fact we will see explained immediately below, as it corresponds to a choice of "complex structure" on the $\mathcal{O}$-module $\operatorname{End}(A)$.

The above moduli description for Shimura curves works well over $\mathbb{C}$, but we want models over $\mathbb{Q}$! There are two ways to precede from here, an adelic approach and an approach using representable functors.

2.3. **Adelic description.** To introduce the adelic description, we first give its derivation for the space $Y(1)_{\mathbb{C}}$. We have seen that $Y(1)_{\mathbb{C}}$ is in bijection with the set of lattices in $\mathbb{C}$ up to isomorphism, which we denote $\cong \backslash \operatorname{Lat}(\mathbb{C})$. But in fact a lattice in $\mathbb{C}$ is really a lattice in $\mathbb{R}^2$ together with a *complex structure* $\psi : \mathbb{C} \to \operatorname{End}_{\mathbb{R}}(\mathbb{R}^2)$, and these are in bijection with $\mathbb{C}\backslash\mathbb{R} = \mathfrak{H}^\pm$ as follows: choose $M = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in M_2(\mathbb{R})$ such that $M\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}M^{-1} = \psi(i)$; then we take $\tau = \dfrac{ai+b}{ci+d} \in \mathfrak{H}^\pm$. Therefore $Y(1)_{\mathbb{C}}$ is in bijection with

$$\cong \backslash(\mathfrak{H}^\pm \times \operatorname{Lat}(\mathbb{R}^2)) = GL_2(\mathbb{R})\backslash(\mathfrak{H}^\pm \times \operatorname{Lat}(\mathbb{R}^2)).$$

And for every lattice $\Lambda \in \operatorname{Lat}(\mathbb{R}^2)$, we can find an $M \in GL_2(\mathbb{R})$ such that $M\Lambda \subset \mathbb{Q}^2 \subset \mathbb{R}^2$, so this set is also in bijection with $GL_2(\mathbb{Q})\backslash(\mathfrak{H}^\pm \times \operatorname{Lat}(\mathbb{Q}^2))$.

Next, we introduce the adeles. For a $\mathbb{Z}$-module S, we define $\widehat{S} = S \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. We then see that the map

$$\begin{aligned}\mathrm{Lat}(\mathbb{Q}^2) &\to \mathrm{Lat}(\widehat{\mathbb{Q}}^2)\\ \Lambda &\mapsto \widehat{\Lambda}\end{aligned}$$

is a bijection, with inverse $\widehat{\Lambda} \mapsto \widehat{\Lambda} \cap \mathbb{Q}^2$. Now since $GL_2(\widehat{\mathbb{Q}})$ acts transitively on $\mathrm{Lat}(\widehat{\mathbb{Q}}^2)$, with stabilizer of a lattice $\widehat{\Lambda}$ given by $GL_2(\widehat{\mathbb{Z}})$, we have in sum a bijection

$$Y(1)(\mathbb{C}) \leftrightarrow GL_2(\mathbb{Q})\backslash(\mathfrak{H}^{\pm} \times GL_2(\widehat{\mathbb{Q}})/GL_2(\widehat{\mathbb{Z}})).$$

This gives a description for the quaternion algebra $B = M_2(\mathbb{Q})$. For any indefinite quaternion algebra B over $\mathbb{Q}$ with maximal order $\mathcal{O}$, we have in a similar way the set

$$B^*\backslash(\mathfrak{H}^{\pm} \times \widehat{B}^*/\widehat{\mathcal{O}}^*).$$

This description can be seen exactly as the set of (real) lattices inside $B \otimes_{\mathbb{Q}} \mathbb{R}$ together with a complex structure, up to isomorphism.

One then proves that this set has the structure of a complex manifold, and we have:

Theorem (Deligne). *There exists a curve $X^B_{\mathbb{Q}}$ defined over $\mathbb{Q}$, and an analytic isomorphism*

$$X^B_{\mathbb{Q}}(\mathbb{C}) \xrightarrow{\sim} B^*\backslash(\mathfrak{H}^{\pm} \times \widehat{B}^*/\widehat{\mathcal{O}}^*).$$

2.4. **Geometric description.** As a second approach, we attempt to extend the moduli description from $\mathbb{C}$ to other domains. This extension can be problematic: for example, every elliptic curves $E/\mathbb{Q}$ is distinguished up to isomorphism over $\overline{\mathbb{Q}}$ by its j-invariant, so $\mathbb{A}^1_{\mathbb{Q}}$ describes this moduli, but it fails when the isomorphisms are restricted over $\mathbb{Q}$, due to the presence of "twists". Moreover, when we add level structure, the curves $X_0(N)_{\mathbb{Q}}$ and $X(N)_{\mathbb{Q}}$ may have only finitely many $\mathbb{Q}$-rational points!

So we need something to allow us to describe elliptic curves not just over $\mathbb{Q}$, but over extensions of $\mathbb{Q}$, in families, in "deformation", etc. In other words, we need a notion of an elliptic curve over an arbitrary base S, which for us may be thought of as just a family of elliptic curves parametrized by S, or *S-family* for short. We also need a way to package together the isomorphism classes of elliptic curves over S, so we define a functor which associates to each $\mathbb{Q}$-scheme S the set of isomorphism classes of elliptic curves (perhaps with level structure) over S. Any scheme X over $\mathbb{Q}$ also defines a functor $S \mapsto \mathrm{Hom}(S, X)$, and we hope that the isomorphism classes of elliptic curves correspond as closely as possible to the points $X(S)$ of some variety X over $\mathbb{Q}$.

We now make this notion precise. Let $\mathsf{Sch}_{\mathbb{Q}}$ denote the category of schemes over $\mathbb{Q}$ with morphisms of schemes, and let Set denote the category of sets.

Definition. Let $F : \mathsf{Sch}_{\mathbb{Q}} \to \mathsf{Set}$ be a contravariant functor. Then $X \in \mathsf{Sch}_{\mathbb{Q}}$ is a *coarse moduli space* for F (or X *coarsely represents* F) if there exists a natural map $\Phi : F(-) \to \mathrm{Hom}(-, X)$ which satisfies:

(i) $\Phi : F(k) \xrightarrow{\sim} \mathrm{Hom}(k, X)$ is bijective if k is algebraically closed;

(ii) [Φ is *universal*] If (Z, Ψ) is any other such, then there is a unique commutative diagram

$$\begin{tikzcd}
F(-) \arrow[r] \arrow[dr] & \mathrm{Hom}(-, Z) \arrow[d, dashed, "\exists!"] \\
 & \mathrm{Hom}(-, X)
\end{tikzcd}$$

By Yoneda's lemma, condition (ii) is equivalent to a unique (commuting) morphism $X \to Z$.

$Y(N)$ are coarse moduli spaces for the functor $S \mapsto F_N(S)$ where $F_N(S)$ is the set of isomorphism classes of pairs (E, α) where E is an S-family of elliptic curves equipped with a map $\alpha : (\mathbb{Z}/N\mathbb{Z})^2_S \xrightarrow{\sim} E[N]$. If $N \geq 3$, then in fact $Y(N)$ is a *fine moduli space*, meaning that Φ is bijective for all S.

Now we return to our abelian surfaces. We define a functor $\mathcal{O} : \mathsf{Sch}_{\mathbb{Q}} \to \mathsf{Set}$ which associates to S the set of isomorphism classes of abelian schemes A over S (which can be thought of families of abelian surfaces parametrized by S) together with a map $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$.

Theorem (Shimura, Deligne). *The functor $F_{\mathcal{O}}$ is coarsely representable by a curve $X^B_{\mathbb{Q}}$ defined over $\mathbb{Q}$.*

By uniqueness and the solution to the moduli problem over $\mathbb{Q}$, we have a map $X^B_{\mathbb{Q}}(\mathbb{C}) \xrightarrow{\sim} \Gamma^B(1)\backslash\mathfrak{H}$ which is in fact an analytic isomorphism.

2.5. **Moduli of abelian varieties.** We are now prepared to make the leap to abelian varieties of arbitrary dimension. Let $[F : \mathbb{Q}] = h$ be a totally real field and B/F a quaternion algebra such that $B \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R}) \times \mathbb{H}^{h-1}$. (We saw in §1 that this describes the class of all quaternion algebras which give rise to Shimura curves.) We also choose a maximal order $\mathcal{O} \subset B$, which is again unique up to conjugation.

By general theory, if A is an abelian variety with $\dim(A) = g$ such that A has QM by B, then $4h \mid 2g$, so we take $g = 2h$. In other words, we must consider abelian varieties of twice the dimension of the ground field F.

With similar definitions, we have $\mathcal{A}_g = \mathrm{Sp}(2g, \mathbb{Z})\backslash\mathfrak{H}_g$ which is a quasiprojective complex variety of dimension $g(g+1)/2$. Now, $\mathrm{End}(A)$ does not come with the structure of a $\mathbb{Z}_F$-algebra, so we must now fix with our data the choice of an element $\mu \in \mathcal{O}$ such that $\mu^2 \in \mathbb{Z}_F$ is totally negative.

We define a functor which associates to a scheme S the set of isomorphism classes of (A, ι) where $A \to S$ is an S-family of abelian g-folds and $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ is an embedding which is compatible with our choice of μ in the sense that $\iota(\beta)^\circ = \iota(\mu^{-1}\overline{\beta}\mu)$. It is again a theorem of Shimura and Deligne that this functor is coarsely representable by a curve $X^B_{F^{(\infty)}}$ defined over $F^{(\infty)}$, where $F^{(\infty)}$ denotes the narrow Hilbert class field of F.

2.6. **CM points.** On the j-line, there are distinguished points which correspond to elliptic curves with extra endomorphisms. Let K be a quadratic imaginary field with $\mathrm{disc}(K) = d < 0$, and let $O_D \subset K$ be an order with $\mathrm{disc}(O_D) = D = df^2$ with $f \in \mathbb{Z}_{\geq 1}$. Then the set of elliptic curves $E/\mathbb{C}$ with CM by O_D up to isomorphism is a finite set of cardinality $\#\,\mathrm{Cl}(O_D)$, the size of the class group of O_D. From this description it follows that each such E is in fact defined over the ring class field R_f of K of conductor f.

In a similar way, on the one-dimensional shimura curve X^B we have points which correspond to abelian varieties with extra endomorphisms. Let K/F be a totally imaginary quadratic extension with $\operatorname{disc}(K) = \mathfrak{d}$, and let $O_{\mathfrak{D}} \subset K$ be an order with discriminant $\operatorname{disc}(O_{\mathfrak{D}}) = \mathfrak{D} = \mathfrak{d}\mathfrak{f}^2$. Now, the set of isomorphism classes of (A, ι) where $A/\mathbb{C}$ is an abelian g-fold and $\iota : M_2(O_{\mathfrak{D}}) \hookrightarrow \operatorname{End}(A)$ is again finite of cardinality $\#\operatorname{Cl}(O_{\mathfrak{D}})$, and each such A is defined over the ring class field $R_{\mathfrak{f}}$ of K. These points on X^B are known as *CM points*.

3. Computational aspects

In the previous sections, we have seen how Shimura curves come equipped with a description as moduli space, which allows them to be defined over number field in addition to their complex uniformization by a Fuchsian group. What is more, they come equipped a battery of CM points, which are defined over abelian extensions. In this section, we discuss the computational questions which arise from this theory.

3.1. The first example.

We begin by giving the "smallest" example of a Shimura curve which does not arise from a subgroup of $SL_2(\mathbb{Z})$. This example has been seen a great deal of treatment by various authors (Ihara, Alsina, Kohel, Elkies, etc.).

We take the quaternion algebra $B = \left(\dfrac{-1, 3}{\mathbb{Q}}\right)$ with $\operatorname{disc}(B) = 6$, and maximal order $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\delta$ where $\delta = (1 + \alpha + \beta + \alpha\beta)/2$. We then have a presentation

$$\mathcal{O}_1^*/\{\pm 1\} \cong \langle \gamma_1, \ldots \gamma_4 | \gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^3 = \gamma_1\gamma_2\gamma_3\gamma_4 = 1 \rangle$$

where

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

We then have the embedding

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

With respect to this embedding, we can define a fundamental domain for the action of $\Gamma^B(1) = \iota_\infty(\mathcal{O}_1^*/\{\pm 1\})$ as in Figure 1.

We again denote $X^B(1) = \Gamma^B(1)\backslash\mathfrak{H}$. The area of $X^B(1)$ is

$$\mu(X^B(1)) = (6-2)\pi - (1 + 1/4 + 2/3 + 1/2 + 2/3 + 1/4)\pi = 2\pi/3,$$

which can also be obtained by the formula

$$\mu(X^B(1)) = \frac{\pi}{3} \prod_{p | \operatorname{disc}(B)} (p-1);$$

hence the genus g of the corresponding Shimura curve is

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

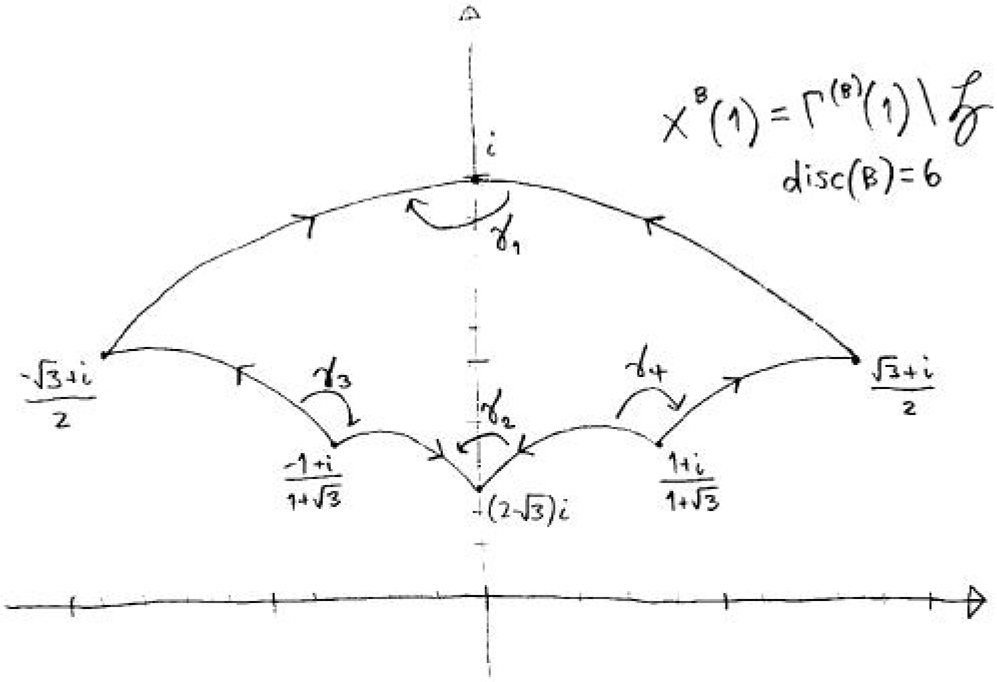

FIGURE 1. Fundamental domain for $X^B(1)$

where e_q is the number of (conjugacy classes of) elliptic points of order q; we see directly from the description of $\mathcal{O}_1^*$ that $e_2 = 2$ and $e_3 = 3$ (and indeed the elliptic vertices v_5, v_6 are conjugate to v_2) hence

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

so $g = 0$. Thus we have a map

$$X^B(1) = \Gamma^B(1) \setminus \mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}.$$

From the moduli description, we saw that $X^B(1)$ in fact has a model over $\mathbb{Q}$, and a result of Ihara is that $X^B(1)$ is the conic

$$X^B(1) : x^2 + y^2 + 3z^2 = 0,$$

and indeed, $X^B(1)(\mathbb{R}) = \emptyset$.

Alternately, we can add certain level structure (see Hashimoto and Murabashi), we obtain an (affine) curve

$$(X^B)' : 4s^2 - s^2 + t^2 + 2 = 0,$$

and then the *universal abelian surface* A with QM by B is the Jacobian of the curve

$$C^B : y^2 = x(x^4 + Px^3 + Qx^2 + Rx + 1)$$

over $(X^B)'$, where

$$P = 2s + 2t, R = 2s - 2t, Q = \frac{(1 + 2t^2)(11 - 28t^2 + 8t^4)}{3(1 - t^2)(1 - 4t^2)}.$$

3.2. **Computational problems for fundamental domains.** From now on, B will denote a quaternion algebra over a totally real field F of degree h which is split at exactly one real place with the embedding $B \hookrightarrow M_2(\mathbb{R})$, and $\mathcal{O} \subset B$ will denote a maximal order.

Given B, we can compute the hyperbolic volume by the formula

$$\frac{1}{2\pi}\mu(X^B(1)) = (-1)^h \frac{\zeta_F(-1)}{2^{h-2}} \prod_{\mathfrak{p} \mid \mathrm{disc}(B)} (N\mathfrak{p} - 1).$$

From the preceding example, we see that a first problem for Shimura curves is the following.

Problem ((FundDom))**.** *Given B, compute a fundamental domain for $\Gamma^B(1)$.*

We specify a fundamental domain by a convex hyperbolic polygon, given by an ordered set of vertices, including the gluing relations between the sides given by elements of $\mathcal{O}_1^*$.

From a fundamental domain, we should be able to compute the set of conjugacy classes of elliptic points and hence the genus.

Problem ((Units))**.** *Given $\mathcal{O}$, compute a minimal set of generators and relations for $\mathcal{O}_1^*$.*

Such a minimal set of generators is specified by the usual presentation for a Fuchsian group Γ, namely, if γ has signature $(g; e_1, \dots, e_r)$ then

$$\Gamma \cong \langle \alpha_1, \beta_1, \dots, \alpha_g, \beta_g, \gamma_1, \dots, \gamma_r | \gamma_1^{e_1} = \dots = \gamma_r^{e_r} = \gamma_1 \cdots \gamma_r [\alpha_1, \beta_1] \cdots [\alpha_r, \beta_r] = 1 \rangle$$

where $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ is the commutator.

A solution to (Units) should yield a solution to (FundDom), and vice versa, but we do not know of a result in this direction.

The work in this direction includes Alsina-Bayer and Kohel-Verrill over $\mathbb{Q}$, which do several examples, and Johansson who reduces the problem to a finite computation for any F.

3.3. **Level structure, tables.** We may also ask for a solution to these problems with *level structure*: given $\mathfrak{N} \subset \mathbb{Z}_F$ which is prime to $\mathrm{disc}(B)$, we have an embedding

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

where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the completion at the ideal $\mathfrak{N}$. Thus we can define $\Gamma_0(\mathfrak{N})$ to be the subgroup of $\mathcal{O}_1^*$ which map to upper triangular matrices modulo $\mathfrak{N}$, and thus we define $X_0^B(\mathfrak{N}) = \Gamma_0(\mathfrak{N})\backslash\mathfrak{H}$. We may similarly define $\Gamma_1(\mathfrak{N})$ and $\Gamma(N)$.

Problem ((BndGen))**.** *Given $h \in \mathbb{Z}_{\geq 1}$ and $g \in \mathbb{Z}_{\geq 0}$, list all pairs $(B/F, \mathfrak{N})$ where B/F is a quaternion algebra with $[F : \mathbb{Q}] \leq h$ and $\mathfrak{N}$ is an ideal of $\mathbb{Z}_F$, such that $g(X_0^B(\mathfrak{N})) \leq g$.*

It should be clear that this list will always be finite, but we have not seen an explicit result of this sort in the literature. For $F = \mathbb{Q}$ and $N = 1$, explicit formulas give $g(X^B(1)) = 0$ if and only if $\mathrm{disc}(B) = 6, 10, 22$, and $g(X^B(1)) = 1$ if and only if $\mathrm{disc}(B) = 14, 15, 21, 33, 34$. See Ihara (and others) for some other small examples, and Johansson for a solution to this problem with $h = 1, 2$ and $g = 2$.

Question. Is h bounded by g, in the sense the set of (BndGen) is still finite if we take $h = \infty$?

It seems likely that the answer to this question is yes, which would be very interesting: one could then list *all* Shimura curves of bounded genus. If the answer is no, this would also be very interesting!

Problem. *Given $X = X_0^B(\mathfrak{N})$ with genus "not too big", compute an equation for X.*

Problem. *Make a Cremona-like table of elliptic curves (or optimal quotients) of Jacobians $J(X)$.*

An application of this is to have tables of small examples of elliptic curves, which have found great utility for the modular group $SL_2(\mathbb{Z})$.

Problem. *If $\mathfrak{M} \mid \mathfrak{N}$, compute the map $X_0^B(\mathfrak{N}) \to X_0^B(\mathfrak{M})$.*

An application of this problem would be a solution to the inverse Galois problem.

Problem. *Compute an equation for the "universal curve" C over X.*

By reduction, from a solution to this problem we would obtain families of abelian varieties over finite fields with interesting endomorphism rings!

3.4. **Triangle groups.** We also have normalizers of these groups, which are analogs of Atkin-Lehner involutions.

Problem. *Given $X_0^B(\mathfrak{N})$ of genus $g \geq 2$, compute* $\operatorname{Aut}(X)$.

See very recent work of Aristides-Rotger for a partial answer over $\mathbb{Q}$.

For the example given above, the normalizer $N(\mathcal{O}_1^*)$ of $\mathcal{O}_1^*$ in A fits in an exact sequence

$$1 \to \mathcal{O}_1^* \to N(\mathcal{O}_1^*) \to (\mathbb{Z}/2\mathbb{Z})^2 \to 0$$

where $N(\mathcal{O}_1^*)/\mathcal{O}_1^*$ is generated by elements of norm $1, 2, 3, 6 \mid \operatorname{disc}(B)$. Now

$$N(\mathcal{O}_1^*) \cong \langle s_2, s_4, s_6 | s_2^2 = s_4^4 = s_6^6 = s_2 s_4 s_6 = 1\rangle$$

and so letting $X^{B*}(1) = \iota_\infty(N(\mathcal{O}_1^*))\backslash\mathfrak{H}$, we have $\mu(X^{B*}(1)) = \pi - (1/2 + 1/4 + 1/6)\pi = \pi/2$ so $g(X^{B*}(1)) = 0$. Now, $X^{B*}(1) \cong \mathbb{P}^1_{\mathbb{Q}}$, since the elliptic points are $\mathbb{Q}$-rational.

We can see this at work with the group $SL_2(\mathbb{Z})$ as well. The usual fundamental domain is the union of two hyperbolic triangles with angles $0, \pi/2, \pi/3$ reflected about the imaginary axis; the vertices i, ρ are elliptic points with stabilizers

$$\left\langle S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong \mathbb{Z}/2\mathbb{Z}$$

and

$$\left\langle ST = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \cong \mathbb{Z}/3\mathbb{Z}$$

and $SL_2(\mathbb{Z}) \cong \langle S, T | S^2 = (ST)^3 = 1\rangle$.

More generally, if $p, q, r \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ with $p \leq q \leq r$, we define the (p, q, r)-*triangle group*

$$\Gamma_{p,q,r} = \langle s_p, s_q, s_r | s_p^p = s_q^q = s_r^r = s_p s_q s_r = 1\rangle.$$

Thus $SL_2(\mathbb{Z})$ is a $(2, 3, \infty)$-triangle group. Now there exists a hyperbolic triangle with angles $\pi/p, \pi/q, \pi/r$ if and only if $1/p + 1/q + 1/r < 1$, and in this case we have

$$\Gamma_{p,q,r} \hookrightarrow \Gamma \subset PSL_2(\mathbb{R})$$

given by the reflections about the edges of this triangle. And similarly we have a map $j : \Gamma\backslash\mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$.

Proposition (Takeuchi). *$\Gamma_{p,q,r}$ is an arithmetic Fuchsian group if and only if (p,q,r) is one of 85 possibilities, if and only if $\Gamma_{p,q,r}$ is commensurable with $\Gamma^B(1)$ where B is one of 19 possibilities.*

One of these is $(p,q,r) = (2,3,\infty)$, which yields the triangle groups commensurable with $SL_2(\mathbb{Z})$. Triangle groups are the simplest class of Shimura curves and contain many interesting examples. For example, the Hurwitz curves arise from the $(2,3,7)$-triangle group. We assume from now on that $r \neq \infty$, so that $\Gamma_{p,q,r}$ is *cocompact*.

As a further example, we note from Takeuchi's list that the $(2,3,r)$-triangle group is arithmetic if and only if $r \in \{7,9,11\}$, and in this case $F = \mathbb{Q}(\zeta_r)^+$ and B is ramified at all but one real place and no finite place. Then $\mathcal{O}_1^* \cong \Gamma_{2,3,r}$.

By the theorem of Shimura and the fact that each such F has narrow class number 1, we have a map $j : \Gamma_{p,q,r}\backslash\mathfrak{H} \xrightarrow{\sim} \mathbb{P}^1_F$, which is unique if we take the images of the elliptic points of order p,q,r to be $0,1,\infty$.

3.5. CM points and modular forms.

We conclude with the computational problem of computing CM points.

Problem. *Given $X = X^B(\mathfrak{N})$ over F, a totally imaginary quadratic extension K/F and an order $O_{\mathfrak{D}} \subset K$, compute the set of CM points on X for O_D.*

See the work of Elkies and V for many computational examples. As an application, we can compute (nontorsion) CM points on elliptic curves over F, giving results in a direction of a generalized Gross-Zagier formula as well as ABC examples.

Finally:

Problem. *Given $\Gamma \subset PSL_2(\mathbb{R})$ a cocompact Fuchsian group and $k \in \mathbb{Z}_{\geq 0}$, "compute" the set of modular forms of weight k for Γ,*

$$M_k(\Gamma) = \{f : \mathfrak{H} \to \mathbb{C} : f(\gamma z) = \det(\gamma)^{-k} f(z) \text{ for all } \gamma \in \Gamma\}.$$

We may consider them by series expansion at an elliptic point or Fourier expansion along a geodesic (given say on a fundamental domain).

There are many other problems which naturally arise from this, but we end here!

Department of Mathematics and Statistics F07, University of Sydney, NSW 2006, Australia

E-mail address: voight@maths.usyd.edu.au