Introduction to Shimura Curves

Alyson Deines

Today

1 Motivation

In class this quarter we spent a considerable amount of time studying the curves $X(N) = \Gamma(N) \setminus \mathcal{H}^*$, $X_0(N) = \Gamma_0(N) \setminus \mathcal{H}^*$, $X_1(N)\Gamma_1(N) \setminus \mathcal{H}^*$, where $\mathcal{H}$ is the upper half of the complex plain and $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ and and $\Gamma(N)$, $\Gamma_0(N)$, and $\Gamma_1(N)$ are the usual congruence subgroups of $SL_2(\mathbb{Z})$. These curves are closely related to modular forms and elliptic curves. They have been extensively studied and are rich in theory.

A reasonable question to ask is how to generalize the classical congruence subgroups of $SL_2(\mathbb{R})$ and the modular curves associated to them. Are their other subgroups of $SL_2(\mathbb{Z})$ that give us curves and modular forms besides $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$? Can we generalize these subgroups of $SL_2(\mathbb{R})$ to number fields? That is, instead of working with $SL_2(\mathbb{Z})$, is it reasonable to work with $SL_2(\mathbb{Z}_F)$ where F is a number field? One way is to work with groups arising from quaternion algebras over totally real number fields. Let $\mathbb{H}$ denote the Hamiltonians. By working over a totally real number field F of degree n we can pick quaternion algebras that have an embedding of $B \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow M_2(\mathbb{R})^r \oplus \mathbb{H}^{n-r}$. We can restrict the elements of B further, to get subgroups $\Gamma \subset B$ which embed in $SL_2(\mathbb{R})^r$ and thus act on $\mathcal{H}^r$. This construction gives us *Shimura varieties*. If we restrict ourselves to examing embeddings of $B \oplus \mathbb{R} \hookrightarrow M_2(\mathbb{R})$, we get *Shimura curves*.

Why study Shimura curves? Shimura curves are close analogues of the traditional modular curves. Modular curves even arise as examples of Shimura curves over $\mathbb{Q}$. Modular curves parameterize elliptic curves with some other structure. Shimura curves parameterize abelian varieties in a similar way. Using the explicit formulas for elliptic curves and for the maps between them we are able to write down models for the first few curves $X_1(N)$ parameterizing an elliptic curve and an N torsion point. Similarly, we can obtain explicit models for Shimura curves over number fields.

This is not the only way in which the theory generalizes. From the subgroups Γ of $SL_2(\mathbb{R})$ we get from these quaternion algebras, we also have quaternionic modular forms, i.e., modular forms acted on by Γ. Interested parties should know that in the Shimura variety case, some of these groups are the ones we associate with Hilbert modular forms.

Shimura curves are also studied because they provide interesting examples of low genus curves and maps between them. Some of the buzz words where are error-correcting code, Drinfeld-Vladut upper bound, and arithmetic triangle groups. And recently, some interesting Heegner point constructions have been studied via CM computations on Shimura curves.

2 Quaternion Algebras

A *quaternion algebra* B over a field F is a central simple algebra of dimension 4. A more concrete way to view B is as an F-algebra generated by elements i and j such that for some $a, b \in F^\times$,

$$i^2 = a, \quad j^2 = b, \quad \text{, and} \quad ji = -ij.$$

B is denoted by $B = \left(\frac{a,b}{F}\right)$. Two well known examples are the Hamiltonian quaternions, $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ and the 2×2 matrices $\left(\frac{1,1}{\mathbb{R}}\right) \cong M_2(\mathbb{R})$ via

$$i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Back to the general case to clear up some more preliminaries, let B a quaternion algebra over a field F. Let K be a field containing F. Tensoring we get a quaternion algebra over K: $B_K = B \otimes_F K$. We say K *splits* B if $B_K \cong M_2(K)$. Let v be a non-complex place of F and let F_v be the completion of F at v. Then $B_v = B \otimes_F F_v$ is either $M_2(F_v)$ or the unique division ring of dimension 4 over F_v. If F_v splits B, i.e., $B_v \cong M_2(F_v)$ we say that B is *unramified* or *split* at v. Otherwise we say that B is *ramified* at v.

It is a theorem that a quaternion algebra is ramified at an even (finit) number of places. Let B be a quaternion algebra over a number field F. Then *discriminant* of B is the ideal in $\mathbb{Z}_F$ which is the product of the ramified places of B.

Quaternion algebras over number fields have a structure somewhat analogous to the ring of integers of a number field. A $\mathbb{Z}_F$-*lattice* of B is a finitely generated $\mathbb{Z}_F$-submodule $\mathcal{O}$ such that $F\mathcal{O} = B$. If $\mathcal{O}$ is also a subring of B then we say $\mathcal{O}$ is an order of B and a *maximal order* is an order that is not contained in any other order of B. The somewhat above is due to the fact that in general maximal orders of quaternion algebras fail to be unique. For example, if $\mathcal{O}$ is a maximal order of a quaternion algebra B and $x \in B$, then $x^{-1}\mathcal{O}x$ is another maximal order of B.

Let's have a working example. Let F be a totally real number field. Say $B = \left(\frac{1,1}{F}\right)$. Then $M_2(F) \cong B$ under the same isomorphism as before,

$$i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then $\mathcal{O} \cong M_2(\mathbb{Z}_F)$ is a maximal order of B. If we take all the invertible elements of $\mathcal{O}^\times \cong GL_2(\mathbb{Z}_F)$. But how do we get to $SL_2(\mathbb{Z}_F)$?

Conjugation is the unique involution $\ : B \to F$ such that for $x \in B$, $x\overline{x} \in F$. This gives us the *reduced norm*, or $nrd(x) = x\overline{x}$. For $B = \left(\frac{a,b}{F}\right)$ and $x \in B$, $x = u + vi + zj + wij$:

$$\overline{x} = u - vi - zi - wij \quad \text{ and } \quad nrd(x) = u^2 - av^2 - bz^2 + abw^2,$$

and because we'll want it later, the *reduced trace* is defined to be

$$\mathrm{trd}(x) = x + \overline{x} = 2u.$$

Looking again at our example, If we restrict to units of$\mathcal{O}$ reduced norm one:

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

So $\mathcal{O}_1^\times \cong SL_2(\mathbb{Z}_F)$.

This works in even more generality. Let F be a totally real number field of degree n and let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over F that splits at exactly one real place. This gives us the following map via the image of B under each embedding of $F \hookrightarrow \mathbb{R}$:

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

Let $\iota_\infty : B \to M_2(\mathbb{R})$ be the projection of B onto $M_2(\mathbb{R})$.

Then as before let $\mathcal{O}$ be a maximal order and

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

We now get our generalization of Γ:

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

To get our first example of a Shimura curve, we take the quotient $X^B(1)_{\mathbb{C}} = \Gamma^B(1) \setminus \mathcal{H}$.

Examples: First, we can see that over $\mathbb{Q}$ we can get back Let $B = \left(\frac{1,1}{\mathbb{Q}}\right)$, with generators i and j, $i^2 = 1 = j^2$ $ij = -ji$. Then $B \cong M_2(\mathbb{Q})$ via

$$i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We can take $\mathcal{O} = M_2(\mathbb{Z})$. Then $\mathcal{O}_1^\times = SL_2(\mathbb{Z})$ and $\Gamma^B(1) \cong PSL_2(\mathbb{R})$. Notice that this gives us the classical case of modular curves, $X^B(1) = X(1)$.

Notice that if we take $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ then $B \oplus_{\mathbb{Q}} \mathbb{R} = \mathbb{H}$ is an un-example.

What else can we get? Now let $B = \left(\frac{-1,3}{\mathbb{Q}}\right)$. Take $\alpha^2 = -1$ and $\beta^2 = 3$. Then ι_∞ takes

$$\alpha \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } \beta \mapsto \begin{bmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{bmatrix}.$$

So $B \hookrightarrow M_2(\mathbb{Q}(\sqrt{3}))$. Let $\delta = (1+\alpha+\beta+\alpha\beta)/2$ so we can pick maximal order $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\delta$. The Shimura curve that arises from this maximal order is one that does not appear in the classical setting.

3 Level Structures

We've seen how to get $\Gamma(1)$, but what about any of the congruences subgroups we studied all quarter? What if we want level structure? What we are looking for now are non-maximal orders. An easy way to get a non-maximal order is to take the intersection of two maximal orders. The resulting order is called an *Eichler order*.

Take $\gamma_1, ..., \gamma_4 \in B$, B a quaternion algebra. Define the discriminant of $\gamma_1, ..., \gamma_4$ to be $\operatorname{disc}(\gamma_1, ..., \gamma_4) = \det(\operatorname{trd}(\gamma_k\gamma_n))_{k,n=1,2,3,4}$. Let $\mathcal{O}$ be an order of a quaternion algebra B. This allows us to define the *discriminant* of $\mathcal{O}$,

$$\operatorname{disc}(\mathcal{O}) = \{\operatorname{disc}(\gamma_1, ..., \gamma_4) : \gamma_k \in \mathcal{O}\}.$$

The level of $\mathcal{O}$ is coprime to $\operatorname{disc}(B)$.

It is easy to create Eichler orders of a prescribed level. Now let B be a quaternion algebra over F and let $\mathcal{O}$ be a maximal order of B. Pick an ideal $\mathfrak{N}$ of $\mathbb{Z}_F$ coprime to $\operatorname{disc}(B)$. Letting $\mathbb{Z}_{F,\mathfrak{N}}$ be the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$, we have the embedding $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$. Then an Eichler order of level $\mathfrak{N}$ is

$$\mathcal{O}(\mathfrak{N}) = \{\gamma \in \mathcal{O} : \iota_{\mathfrak{N}}(\gamma) \text{ is upper triangular mod } \mathfrak{N}\}.$$

Further, by conjugating we get all Eichler orders.

Let B be a quaternion algebra over a number field F and let $\mathcal{O}$ be an Eichler order. The level of an Eichler order $\mathcal{O}$ is the ideal $\mathfrak{N} \subset \mathbb{Z}_F$ such that $\operatorname{disc}(\mathcal{O}) = \mathfrak{N}\operatorname{disc}(B)$. So we see that Eichler orders give us our level structure.

For example, over $M_2(\mathbb{Q})$ we have maximal orders

$$\begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} \text{ and } \begin{pmatrix} \mathbb{Z} & N^{-1}\mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{pmatrix}$$

which are conjuate via

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}.$$

The intersection of these two ideas is

$$\mathcal{O}(N) = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{pmatrix}$$

an Eichler order of level N. Then $\Gamma^B(\mathcal{O}(N)) = \Gamma_0(N)$ and $X(\mathcal{O}(N)) = X_0(N)$.