MODULI PROBLEMS OF ELLIPTIC CURVES
TERM 1 STUDY GROUP, 2023-24
Week 2 - Modular Curves and Elliptic Curves over $\mathbb{C}$

Edison Au-Yeung

We will first recall how to understand elliptic curves as complex lattices and the action of modular group on the upper half plane, then proceed to explore how the theory of elliptic curves can help us to interpret the quotient $SL_2(\mathbb{Z}) \setminus \mathbb{H}$. Finally, we will construct modular curves as quotients of the extended upper half plane.

(The materials from this document are mainly adapted from Siksek's notes on 'Explicit Arithmetic of Modular Curves' [2] and the book 'A First Course in Modular Forms' by Diamond and Shurman. [1])

1. Two quotients sets

A *complex elliptic curve* is a quotient of the complex plane by a lattice. Recall the Weierstrass $\wp$-function (relative to a complex lattice Λ), which is defined by the series

$$\wp(z) = \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

The functions $\wp$ and $\wp'$ satisfy Weierstrass's differential equation

$$\wp'(z)^2 = 4\wp^3 - g_2\wp(z) - g_3,$$

where g_2 and g_3 are constants depending on the lattice Λ.

The discriminant of the cubic polynomial on the right is non-zero, so we can use it to identify an elliptic curve $E/\mathbb{C}$ with $y^2 = 4x^3 - g_2x - g_3$. In particular, consider $\mathbb{C}/\Lambda$ as a quotient group and we know that points on an elliptic curve form a group structure, we have an isomorphism of abelian groups:

$$\begin{aligned} \Phi \colon \mathbb{C}/\Lambda &\to E_\Lambda(\mathbb{C}) \\ 0 &\to O \\ z &\mapsto \left(\wp(z), \frac{1}{2}\wp'(z) \right) \end{aligned}$$

Now moving on to examine the upper half plane

$$\mathbb{H} := \{x + iy \colon x, y \in \mathbb{R}, y > 0\}.$$

We know that $SL_2(\mathbb{Z})$ acts on the upper half (complex) plane by fractional linear (Mobius) transformations:

$$SL_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H};$$

$$(\gamma, \tau) \mapsto \frac{a\tau + b}{c\tau + d}, \text{ where } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$$

To study the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$, it suffices to consider its behaviour on the orbits of $\mathbb{H}$ under the action of $SL_2(\mathbb{Z})$. Roughly speaking, the fundamental domain of $SL_2(\mathbb{Z})$ serves as a represnetative region in the upper half plane $\mathbb{H}$. More precisely, it gives you a one-to-one correspondence between the orbits and points on $\mathbb{H}$ (i.e. any two points τ and τ' of the upper half plane are $SL_2(\mathbb{Z})$ – equivalent if and only if $\gamma(\tau) = \tau'$ for some $\gamma \in SL_2(\mathbb{Z})$.).

2. Connection between the two quotients

We now want to show that there is a bijection between the two quotient sets $\mathbb{C}/\Lambda$ and $SL_2(\mathbb{Z})\backslash\mathbb{H}$. That is, describing the equivalence classes of points in $\mathbb{H}$ under the action of $SL_2(\mathbb{C})$ by the isomorphism classes of complex elliptic curves.

From the previous section, for any given $\tau \in \mathbb{H}$, there is an elliptic curve $E_\tau/\mathbb{C}$ such that $E_\tau(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$. Recall that any two complex elliptic curves $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are holomorphically group-isomorphic if and only if $m\Lambda_\tau = \Lambda_{\tau'}$ for some $m \in \mathbb{C}$. Therefore, $E_\tau/\mathbb{C} \cong E_{\tau'}/\mathbb{C}$ if and only if $\tau = \gamma(\tau')$ for some $\gamma \in SL_2(\mathbb{Z})$. Therefore, we have a bijection (between upper half plane quotient and elliptic curves isomorphism classes):

$$SL_2(\mathbb{Z}) \setminus \mathbb{H} \longleftrightarrow \{\text{isomorphism classes of elliptic curves } E/\mathbb{C}\},$$
$$SL_2(\mathbb{Z}) \cdot \tau \mapsto [\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)].$$

In the bijection above, we are identifying E_τ with $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, with the square brackets denoting isomorphism classes. This has shown a correspondence between the points in the quotient $SL_2(\mathbb{Z}) \setminus \mathbb{H}$ and the isomorphism classes of complex elliptic curves.

More generally, we can consider the quotients of the upper half plane by various congruence subgroups, a certain type of subgroup of $SL_2(\mathbb{Z})$. Similar to how we constructed the bijection previously, they can be described by the sets of equivalence classes of elliptic cures with the addition of corresponding torsion data.

Definition 2.1 (Congruence subgroup)**.** *Let N be a positive integer, define*

$$\Gamma(N) = \{A \in SL_2(\mathbb{Z})\colon A \equiv I \pmod{N}\},$$

We say a subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is a congruence subgroup if there is some positive integer N such that

$$\Gamma(N) \subseteq \Gamma \subseteq SL_2(\mathbb{Z}).$$

*The least such N is called the **level of** Γ.*

$\Gamma(N)$ is also called the *principal congruence subgroup of level N*. In particular, there are two families of congruence subgroups of particular interest:

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})\colon c \equiv 0 \pmod{N}\};$$
$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})\colon a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N}\}.$$

Note that the action of these congruence subgroups on the upper half plane $\mathbb{H}$ is nothing more than restricting the action of $SL_2(\mathbb{Z})$ only.

Proposition 2.2. *Let N be a positive integer, E be an elliptic curve over $\mathbb{C}$.*

1. *Let P be a point of order N on $E/\mathbb{C}$ (that is, $NQ = 0$ but $nQ \neq 0$ for $0 < n < N$). Then*
   - *(a) There is an isomorphism $E/\mathbb{C} \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ (which depends on the choice of $\tau \in \mathbb{H}$) maps the point P to the coset $\frac{1}{N} + (\mathbb{Z} + \mathbb{Z}\tau) \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$.*
   - *(b) There is a bijection*

     $$\Gamma_1(N) \setminus \mathbb{H} \longleftrightarrow \{\text{isomorphism classes of pairs } (E/\mathbb{C}, P)\},$$

     $$\Gamma_1(N) \cdot \tau \mapsto \left[\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \frac{1}{N}\right],$$

     where $\frac{1}{N}$ denote the coset $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau) + \frac{1}{N}$.
2. *Let C be a cyclic subgroup of order N on $E/\mathbb{C}$. Then*
   - *(a) There is an isomorphism $E/\mathbb{C} \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ (which depends on the choice of $\tau \in \mathbb{H}$) maps the cyclic group C to $\left\langle \frac{1}{N} + (\mathbb{Z} + \mathbb{Z}\tau) \right\rangle \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$.*
   - *(b) There is a bijection*

     $$\Gamma_0(N) \setminus \mathbb{H} \longleftrightarrow \{\text{isomorphism classes of pairs } (E/\mathbb{C}, C)\},$$

     $$\Gamma_0(N) \cdot \tau \mapsto [\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \left\langle \frac{1}{N} \right\rangle].$$

Remark 2.3. *In the proposition above, we say two pairs $(E_1, P_1), (E_2, P_2)$ (resp. $(E_1, C_1), (E_2, C_2)$) are isomorphic if and only if there is an isomorphism $\phi : E_1 \to E_2$ such that $\phi(P_1) = P_2$ (resp. $\phi(C_1) = C_2$).*
Alternatively, if we accept the isomorphism in (a), this can also be written as 'any two pairs $(E_\tau, \frac{1}{N} + (\mathbb{Z} + \mathbb{Z}\tau)), (E_{\tau'}, \frac{1}{N} + (\mathbb{Z} + \mathbb{Z}\tau'))$ are isomorphic if and only $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$'.

Proof. For full proof of the above proposition, one can refer to Chapter 1.5 of '*A First Course in Modular Forms*' by Diamond and Shurman. [1] Here we will outline the proof for 1(a).

The goal here is to find a lattice Λ_τ such that $m\Lambda_\tau = \Lambda_{\tau'}$ for some $m \in \mathbb{C}$ to be determined, where we view $E/\mathbb{C} \cong \mathbb{C}/\Lambda_{\tau'}$.

1. Interpret the point P as an element of $\mathbb{C}/\Lambda_{\tau'}$ and write $P = \frac{c\tau'+d}{N} + \Lambda_{\tau'}$.
2. Since the order of P is precisely N, $\gcd(c, d, N) = 1$ and therefore we can use the fact that the map $SL_2(\mathbb{Z}) \mapsto SL_2(\mathbb{Z}_N)$ is surjective to claim that there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma \cdot \tau' = \tau$.
3. With some algebraic manipulation and let $m = c\tau' + d$, we can deduce that $m\Lambda_\tau = \Lambda_{\tau'}$ and therefore yielding

   $$m\left(\frac{1}{N} + \Lambda_\tau\right) = P.$$

The proof of 1(b) is some algebraic manipulations that mainly follow from (a), while 2 is similar to 1 and therefore omitted here. □

3. Modular curves

Definition 3.1 (Modular curve)**.** *For any congruence subgroup Γ of $SL_2(\mathbb{Z})$, acting on the upper half plane $\mathbb{H}$ from the left, the corresponding modular curve $Y(\Gamma)$ is defined as the quotient space of orbits under Γ,*

$$Y(\Gamma) = \Gamma \setminus \mathbb{H} = \{\Gamma\tau \colon \tau \in \mathbb{H}\}.$$

The modular curves for $SL_2(\mathbb{Z}) = \Gamma(1), \Gamma_0(N)$ and $\Gamma_1(N)$ are denoted

$$Y(1) = SL_2(\mathbb{Z}) \setminus \mathbb{H}, \qquad Y_1(N) = \Gamma(1) \setminus \mathbb{H}, \qquad Y_0(N) = \Gamma(0) \setminus \mathbb{H}.$$

In such way, we have constructed some Riemann surfaces. Notice that the fundamental domain of $SL_2(\mathbb{Z}) \setminus \mathbb{H}$ is unbounded along the positive imaginary axis, therefore none of the above is a compact set. If they were compact, we could have identified them as the set of complex points on an algebraic curve. To remedy this deficiency, we compactify $Y(\Gamma)$ by considering the extended upper half plane instead, defined by

$$\mathbb{H}^* \colon = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

The points in $\mathbb{H}^* \setminus \mathbb{H} = \mathbb{P}^1(\mathbb{Q})$ are called *cusps.*

Given that

$$\lim_{\mathrm{im}(\tau)\to\infty} \frac{a\tau + b}{c\tau + d} = \frac{a}{c},$$

it should be no surprise that we can extend the group action of $SL_2(\mathbb{Z})$ to $\mathbb{H}^*$.

Definition 3.2. *Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. The group action of $SL_2(\mathbb{Z})$ can be extended to $\mathbb{H}^*$ by defining as follows:*

$$SL_2(\mathbb{Z}) \times \mathbb{H}^* \to \mathbb{H}^*;$$

$$\gamma \cdot \tau = \begin{cases} \frac{a\tau+b}{c\tau+d}, & \tau \in \mathbb{H}^* \setminus \{-\frac{d}{c}, \infty\}, \\ \frac{a}{c}, & \tau = \infty, \\ \infty, & \tau = -\frac{d}{c} \end{cases}$$

Proposition 3.3. *The modular curve $SL_2(\mathbb{Z}) \setminus \mathbb{H}^*$ has one cusp.*

Proof. For $\tau \in \mathbb{Q}$, write $\tau = \frac{a}{c}$ for coprime integers a, c. Then there exists integers b and d such that $ad - bc = \gcd(a, c) = 1$. The matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

is such that $\gamma \cdot \infty = \tau$. Thus, the points in $\mathbb{P}^1(\mathbb{Q})$ form one orbit only under the action of $SL_2(\mathbb{Z})$ and the cusp point is then $SL_2(\mathbb{Z}) \setminus \mathbb{P}^1(\mathbb{Q}) = \{\infty\}$. □

Proposition 3.4. *For any congruence subgroup Γ of $SL_2(\mathbb{Z})$, the modular curve $\Gamma \setminus \mathbb{H}^*$ has finitely many cusps.*

Proof. We will use, without proof, the fact that for a congruence subgroup Γ, the index $[SL_2(\mathbb{Z})\colon \Gamma]$ is finite. From the previous proposition, we have shown that all the cusp points are $SL_2(\mathbb{Z})$–equivalent to the point $\{\infty\}$. Therefore, take $\tau \in \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \infty$, then there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\tau = \gamma \cdot \infty$.

For the modular curve $X(\Gamma)$, consider the set of cusps

$$\Gamma \setminus \mathbb{P}^1(\mathbb{Q}) = \{\Gamma \cdot \tau \colon \tau \in \mathbb{P}^1(\mathbb{Q})\}$$

But as discussed above, we have

$$\Gamma \cdot \tau = \Gamma \cdot (\gamma \cdot \infty) = (\Gamma\gamma) \cdot \infty.$$

Therefore, $\#\big(\Gamma \setminus \mathbb{P}^1(\mathbb{Q})\big) = [SL_2(\mathbb{Z})\colon \Gamma] < \infty$. □

This proposition tells us that to compactify the modular curves, we just need to add finite number of points to them (namely the cusp points). We denote the compactified modular curves for $SL_2(\mathbb{Z}) = \Gamma(1), \Gamma_0(N)$ and $\Gamma_1(N)$ by

$$X(1) = SL_2(\mathbb{Z}) \setminus \mathbb{H}^*, \qquad X_1(N) = \Gamma(1) \setminus \mathbb{H}^*, \qquad X_0(N) = \Gamma(0) \setminus \mathbb{H}^*.$$

References

[1] Diamond, F. & Shurman, J. *A First Course in Modular Forms.* Springer. (2005).

[2] Siksek, S. *Explicit arithmetic of modular curves.* CMI-HIMR Summer School, http://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf. (2019).