MA6201: Shimura varieties

Si Ying Lee

Spring 2026

Abstract

These are lecture notes to accompany MA6201 taught at NUS in Spring 2026. For comments or corrections, please send an email to `sylee@nus.edu.sg`.

Contents

1 Modular curves

Let

$$\mathbb{H} = \{\, z \in \mathbb{C} \mid \operatorname{Im} z > 0 \,\}.$$

There is a left action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ given as follows: for

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \quad \text{and} \quad z \in \mathbb{H},$$

define

$$g \cdot z := \frac{az+b}{cz+d}.$$

Note that this yields a surjection

$$\mathrm{SL}_2(\mathbb{R}) \twoheadrightarrow \mathrm{Aut}_{\mathrm{hol}}(\mathbb{H}),$$

where $\mathrm{Aut}_{\mathrm{hol}}(\mathbb{H})$ is the holomorphic automorphism group of $\mathbb{H}$. We are interested in certain discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ whose actions produce interesting quotients of $\mathbb{H}$.

Definition 1.1. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ is a *congruence subgroup* if it is a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subset \Gamma$ with finite index for some $N \geq 1$, where

$$\Gamma(N) = \left\{ g \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; g \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We will also usually assume that Γ is *small enough*, i.e., that $\Gamma \subset \Gamma(N)$ for some $N \geq 3$.

The group Γ (if small enough) acts freely and properly discontinuously on $\mathbb{H}$, and this implies that $\Gamma\backslash\mathbb{H}$ has a canonical complex manifold structure given by the complex structure on $\mathbb{H}$. Furthermore, the quotient map $\mathbb{H} \to \Gamma\backslash\mathbb{H}$ is the universal covering.

Definition 1.2. The complex manifold $\Gamma\backslash\mathbb{H}$ is called a *modular curve*.

Proposition 1.3. A modular curve $\Gamma\backslash\mathbb{H}$ has the following properties:

(a) $\Gamma\backslash\mathbb{H}$ has the canonical structure of an algebraic variety over $\mathbb{C}$, which is compatible with the complex manifold structure.

(b) $\Gamma\backslash\mathbb{H}$ is the moduli space of elliptic curves over $\mathbb{C}$ with "Γ-level structure".

(c) The moduli interpretation in (b) also makes sense over some number field E (depending on Γ; e.g., $E = \mathbb{Q}(\zeta_N)$ if $\Gamma = \Gamma(N)$). This moduli problem over E is represented by a quasi-projective E-scheme whose base change to $\mathbb{C}$ recovers $\Gamma\backslash\mathbb{H}$ as a $\mathbb{C}$-scheme. We say that $\Gamma\backslash\mathbb{H}$ has a *model* over E.

(d) This moduli interpretation even extends integrally over $\mathbb{Z}[\zeta_N, 1/N]$, to produce a smooth scheme.

(e) The $\mathbb{C}$-scheme $\Gamma\backslash\mathbb{H}$ has a canonical compactification obtained by adding certain "special points" (cusps), giving a proper algebraic curve.

We will now explain how to see (a)-(d).

Remark 1.4. To show (a), even after giving a structure of a complex manifold to $\Gamma\backslash\mathbb{H}$ one cannot appeal to the usual GAGA equivalence between smooth projective curves over $\mathbb{C}$ and compact Riemann surfaces, because $\Gamma\backslash\mathbb{H}$ is not compact. However, there is a canonical compactification of $\Gamma\backslash\mathbb{H}$ which is a compact Riemann surface (the Baily–Borel compactification).

1.1 Elliptic curves over $\mathbb{C}$

Definition 1.5. An elliptic curve E over $\mathbb{C}$ is a smooth projective algebraic group of dimension 1.

Over $\mathbb{C}$, every elliptic curve arises as a quotient $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. More precisely, given an elliptic curve E, there is a holomorphic group homomorphism $\exp : \mathrm{Lie}E \to E$ coming from Lie group theory. Here $\mathrm{Lie}E$ is the tangent space at the identity O, and is a 1-dimensional complex vector space. (Note that exp is not algebraic.) Then $\ker(\exp)$ is a lattice in $\mathrm{Lie}E$ and $(\mathrm{Lie}E)/\ker(\exp) \xrightarrow{\sim} E$ is an isomorphism of elliptic curves. Notice also that (non-canonically) the left hand side is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.

Remark 1.6. The map $\exp : \mathrm{Lie}E \to E$ is a universal covering. Hence we have the following canonical isomorphisms: $\ker(\exp) = \pi_1(E, O) = H^1(E, \mathbb{Z})$.

Suppose E and E' are elliptic curves. We have

$$\mathrm{Hom}(E, E') \cong \big\{ f : \mathrm{Lie}E \to \mathrm{Lie}E' \;\big|\; f \text{ is } \mathbb{C}\text{-linear and } f\big(H^1(E,\mathbb{Z})\big) \subset H^1(E',\mathbb{Z}) \big\}$$

where the assignment is given by $F \longmapsto dF\big|_{\mathrm{Lie}E}$. Combining the above facts, we have an equivalence of categories

$$\big((V,\Lambda),\ V \text{ a 1-dimensional } \mathbb{C}\text{-vector space and } \Lambda \subset V \text{ a } \mathbb{Z}\text{-lattice}\big) \xrightarrow{\sim} \big(\text{Elliptic curves}/\mathbb{C}\big)$$

given by

$$(V,\Lambda) \longmapsto V/\Lambda.$$

and the reverse map is given by

$$E \mapsto (\mathrm{Lie}E, H^1(E,\mathbb{Z})).$$

We first observe that two elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if there is a $\mathbb{C}$-linear holomorphic automorphism of $\mathbb{C}$ that takes Λ to Λ'. Every such holomorphic automorphism of $\mathbb{C}$ is given by multiplication by an element $\alpha \in \mathbb{C}^\times$. Indeed, any continuous group automorphism of a real vector space is necessarily an $\mathbb{R}$-linear map, and one checks that $\varphi(a+bi) = a\varphi(1) + b\varphi(i)$ is holomorphic if and only if $\varphi(i) = i\varphi(1)$. So $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ if and only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$. This gives us:

$$\{\text{Lattices inside } \mathbb{C}\}/\text{homothety} \xrightarrow{\sim} \{\text{Elliptic curves over} \mathbb{C}\}/\text{isomorphism}.$$

Now we orient $\mathbb{C}$, as real vector space, so that $(1, i)$ is a positive orientation. We let

$$\mathcal{Z} = \{\text{pairs } (\omega, \omega') \text{ of positively oriented } \mathbb{R}\text{-bases of } \mathbb{C}\}.$$

The group $\mathrm{SL}(2, \mathbb{Z})$ acts on $\mathcal{Z}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (\omega, \omega') = (a\omega + b\omega', c\omega + d\omega').$$

This action fixes the lattice $\mathbb{Z}\omega + \mathbb{Z}\omega' \subset \mathbb{C}$, and the quotient $\mathrm{SL}(2, \mathbb{Z})\backslash\mathcal{Z}$ is thus identified with the set of all lattices in $\mathbb{C}$. Thus we have a bijection

$$\mathrm{SL}(2, \mathbb{Z})\backslash\mathcal{Z}/\mathbb{C}^\times \xrightarrow{\sim} \{\text{Elliptic curves}\}/\text{isomorphism}.$$

where $\alpha \in \mathbb{C}^\times$ takes (ω, ω') to $(\alpha\omega, \alpha\omega')$, or equivalently takes the lattice Λ to $\alpha\Lambda$.

We further observe that

$$(\omega, \omega') \longmapsto \frac{\omega'}{\omega}$$

identifies $\mathcal{Z}/\mathbb{C}^\times$ with the upper half plane $\mathbb{H} \subset \mathbb{C}$:

$$\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}.$$

Thus, we have

$$\mathrm{SL}(2, \mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \{\text{Elliptic curves}\}/\text{isomorphism}.$$

Let $\mathbb{H}^\pm = \mathbb{C} \setminus \mathbb{R}$, the union of the upper and lower half planes. The group $\mathrm{GL}(2, \mathbb{Z})$ similarly acts by fractional linear transformations on $\mathbb{H}^\pm$ as above. Note that we further have an isomorphism

$$\mathrm{GL}(2, \mathbb{Z})\backslash\mathbb{H}^\pm \simeq \mathrm{SL}(2, \mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \{\text{Elliptic curves}\}/\text{isomorphism}.$$

Let us now give these sets some complex structures. Recall that we have an $\mathrm{SL}_2(\mathbb{Z})$-invariant holomorphic morphism $j : \mathbb{H}^+ \to \mathbb{C}$ inducing a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+ \xrightarrow{\sim} \mathbb{C}.$$

Here j corresponds to evaluating the classical j-invariant of an elliptic curve, which we recall is defined as follows:

Definition 1.7. Take an elliptic curve $E/\mathbb{C}$ and write it in Weierstrass form

$$y^2 = x^3 + ax + b.$$

The *j-invariant* is given by

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

We may use this map to identify the quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$ with $\mathbb{C}$ in order to give the former a complex manifold structure.

Note that $\mathbb{H}^+ \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$ is a holomorphic map, but not a local isomorphism. In other words, this is not a covering map; there is ramification over the images of i and $e^{\frac{2\pi i}{3}}$ with branching of order 2 and 3 respectively. This is related to the fact that the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathbb{H}^+$ is problematic in the following sense:

- $-I \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathbb{H}^+$. In particular, the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathbb{H}^+$ is not free.
- The naive solution is to now consider the action of $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ on $\mathbb{H}^+$. For this action, most points in $\mathbb{H}^+$ have trivial stabilizer, but points in the orbit of i and the orbit of $e^{\frac{2\pi i}{3}}$ have nontrivial stabilizers. So this is also not a solution.

This phenomenon exactly corresponds to the fact that for any elliptic curve E over $\mathbb{C}$ (or in fact any algebraically closed field of characteristic away from 2 or 3), the automorphism group of E is either:

1. $\mathbb{Z}/2\mathbb{Z}$, where the nontrivial automorphism is negation. This corresponds to the inclusion of $\{\pm I\}$ in all stabilizers.
2. $\mathbb{Z}/4\mathbb{Z}$. This automorphism group applies to a unique isomorphism class of elliptic curves.
3. $\mathbb{Z}/6\mathbb{Z}$. This automorphism group applies to a unique isomorphism class of elliptic curves.

Remark 1.8. The complex manifold structure we put on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$ (using j) is the unique one such that the projection $\mathbb{H}^+ \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$ is holomorphic.

Remark 1.9. It is "more correct", in some sense, to define the orbifold (or Deligne-Mumford stack) quotient of $\mathbb{H}^+$ by $\mathrm{SL}_2(\mathbb{Z})$. This allows us to still form something like a fine moduli space of elliptic curves that remembers the automorphisms (including the generic $\mathbb{Z}/2\mathbb{Z}$-automorphisms). We will discuss this in more detail when we talk about moduli spaces.

1.2 Alternative point of view: Hodge structures

In the previous subsection, we classified elliptic curves $\mathbb{C}/\Lambda$ up to isomorphism by morally fixing the complex vector space $\mathbb{C}$ and varying Λ. We now introduce a different way to think about the upper half plane with its complex structure which is more amenable to generalization to higher dimensions. We may fix an abstract $\mathbb{Z}$-module Λ, finite free of rank 2, and ask how we could vary the $\mathbb{C}$-structure.

As before, an elliptic curve is given by $E = (\mathrm{Lie}E)/H^1(E, \mathbb{Z})$. Also, we have a canonical isomorphism of 2-dimensional $\mathbb{R}$-vector spaces: $\mathrm{Lie}E \cong H^1(E, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$. Notice of course that $\mathrm{Lie}E$ also has a complex structure. Thus in order to reconstruct E, we need the abstract $\mathbb{Z}$-module $H^1(E, \mathbb{Z})$ together with a complex structure on the $\mathbb{R}$-vector space $H^1(E, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$. In general, to define a complex structure on an $\mathbb{R}$-vector space V, it suffices to define multiplication by i such that $i^2 = -1$. In other words, a complex structure on V is exactly an element $J \in \mathrm{End}_{\mathbb{R}}(V)$ such that $J^2 = -1$, and this element corresponds to scalar multiplication by i. Then, we extend this to all $\mathbb{C}$ by setting:

$$(x + iy) \cdot v \ = \ x \cdot v \ + \ y \cdot J(v)$$

for all real numbers x, y. However, we will give a slightly different definition here:

Definition 1.10. A complex structure on $\mathbb{R}^2$ is a homomorphism

$$h : \mathbb{C}^\times \to \mathrm{GL}(2, \mathbb{R}) = \mathrm{Aut}(\mathbb{R}^2)$$

such that the eigenvalues of $h(z) \in \mathbb{C}^\times$ on $\mathbb{R}^2$ are z and $\bar{z}$.

The equivalence between the two definitions can be seen by taking $J = h(i)$, and observing that the condition on the eigenvalues forces the characteristic polynomial of J to be $X^2 + 1$.

Choosing the base point $e_0 = (1, 0) \in \mathbb{R}^2$, we see that any complex structure h defines an isomorphism $i_h : \mathbb{R}^2 \to \mathbb{C}$ of complex vector spaces, via $i_h^{-1}(z) = h(z) \cdot e_0$.

Now, denote $V = \mathbb{R}^2$, and let $h : \mathbb{C}^\times \to \mathrm{Aut}(\mathbb{R}^2)$ be a complex structure. Then for any $z \in \mathbb{C}$, $z \notin \mathbb{R}$, $h(z)$ is diagonalizable and by definition has two eigenvalues on $V \otimes \mathbb{C}$, namely z and $\bar{z}$. For some $z \in \mathbb{C}^\times$, let $V^{-1,0} = V_h^{-1,0}$, resp. $V^{0,-1} = V_h^{0,-1}$, denote the z-eigenspace, resp. the $\bar{z}$-eigenspace, for $h(z)$ on $V_{\mathbb{C}}$. Observe that since h is a homomorphism, the subspaces $V^{-1,0}, V^{0,-1}$ are independent of the choice of $z \in \mathbb{C}^\times \backslash \mathbb{R}$.

Example 1.11. We can define a complex structure by the homomorphism

$$h_0 : \mathbb{C}^\times \to \mathrm{GL}(2, \mathbb{R}) \quad \text{such that} \quad h_0(x + iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix};$$

this obviously satisfies the hypothesis, and if we look at the eigenspaces for $z = i$, we get

$$V^{-1,0} = \mathbb{C} \cdot v_0, \qquad V^{0,-1} = \mathbb{C} \cdot v_0'$$

where

$$v_0 = \begin{pmatrix} -i \\ 1 \end{pmatrix}, \qquad v_0' = \begin{pmatrix} i \\ 1 \end{pmatrix}.$$

Proposition 1.12. Let $V^{-1,0}, V^{0,-1}$ as above. Then under the complex conjugation on $V \otimes \mathbb{R}$, we have

$$V^{-1,0} = \overline{V^{0,-1}}.$$

Proof. Let v, v' be the basis of $V \otimes \mathbb{C}$ such that $h(i)v = iv$, $h(i)v' = -iv'$. Thus $V^{-1,0} = \mathbb{C} \cdot v$, $V^{0,-1} = \mathbb{C} \cdot v'$. On the other hand, $h(i) \in \mathrm{Aut}(\mathbb{R}^2) = \mathrm{GL}(2, \mathbb{R})$ is a real matrix with eigenvalues i, $-i$, hence there is a real matrix γ such that

$$\gamma^{-1} h(i) \gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = h_0(i).$$

Then we see that, with v_0 and v_0' as above, we have $\gamma\mathbb{C}\cdot v_0 = V_h^{-1,0}$, resp. $\gamma\mathbb{C}\cdot v_0' = V_h^{0,-1}$. Now, we see that the claim is true for the complex structure h_0, since $\bar{v_0} = v_0'$. Thus, since γ is real, the claim follows. □

Now, we can relate the space of complex structures to $\mathbb{H}$ in the following way. Observe that $\mathrm{GL}(2,\mathbb{R})$ acts by fractional linear transformations on $\mathbb{H}^\pm$. The complex number $\tau_h = \gamma(i)$ then belongs to $\mathbb{H}^\pm$. Moreover we can define a map

$$\pi : \{\text{complex structures}\} \longrightarrow \mathbb{H}^\pm$$

by $\pi(h) = \tau_h$. This map may appear to depend on the choice of the matrix γ such that $h(i) = \gamma h_0(i)\gamma^{-1}$, but we have the following:

Proposition 1.13. The map π is well-defined.

Proof. We write $\tau_h(\gamma)$ to take provisional account of this dependence. Note first of all that h_0 and h both extend to algebra homomorphisms $\mathbb{C} \to M(2,\mathbb{R})$, and since i generates $\mathbb{C}$ as $\mathbb{R}$-algebra it follows that $\gamma h_0 \gamma^{-1} = h$. If γ' is another choice, then $k = \gamma'^{-1}\gamma$ belongs to the centralizer in $\mathrm{GL}(2,\mathbb{R})$ of h_0, i.e. to the centralizer of $h_0(\mathbb{C})$, which is just $h_0(\mathbb{C})$. Thus $k \in h_0(\mathbb{C})$, and if

$$k = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

we have $\tau_h(\gamma') = \gamma'(i) = \gamma(k(i))$. Since $k(i) = \dfrac{xi+y}{-yi+x} = i$, there is no dependence. □

In other words, letting $K_\infty = h_0(\mathbb{C}^\times) \subset \mathrm{GL}(2,\mathbb{R})$, there is a sequence of identifications

$$\{\text{complex structures}\} \simeq \mathrm{GL}(2,\mathbb{R})/K_\infty \simeq \mathbb{H}^\pm.$$

The significance of this is that the final term has an obvious complex structure, hence so do the first two terms. Moreover, this complex structure is $\mathrm{GL}(2,\mathbb{R})$-invariant.

We can expland on this a little bit more, to define the Borel embedding. The function associating the normalized vector $v' = v_h' \in V_h^{0,-1}$ to h is compatible with the complex structure. Now $V_h^{0,-1} \subset V_\mathbb{C}$ is a variable line in $V_\mathbb{C}$, hence defines a variable point $p_h \in \mathbb{P}(V_\mathbb{C}) = \mathbb{P}^1(\mathbb{C})$. If $\binom{\alpha}{\beta}$ is the homogeneous coordinate of a point in $\mathbb{P}^1$, we use the standard inhomogeneous coordinate α/β. Then the inhomogeneous coordinate of $V_h^{0,-1}$ is just τ_h. We thus have a holomorphic embedding

$$\{\text{complex structures}\} \simeq \mathrm{GL}(2,\mathbb{R})/K_\infty \hookrightarrow \mathbb{P}(V_\mathbb{C})$$

obtained by associating the subspace $V_h^{0,-1}$ to h.

Now, we define a family of elliptic curves $\mathcal{E}$ over $\mathbb{H}$ which was given, for each complex structure h, some elliptic curve E_h given as $\mathbb{C}/i_h(\mathbb{Z}^2)$. Recall the formula for $i_h : \mathbb{R}^2 \simeq \mathbb{C}$:

$$i_h\big(h(z)e_0\big) = z \cdot i_h(e_0).$$

The map i_h extends by linearity to a surjective homomorphism

$$\mathbb{R}^2 \otimes \mathbb{C} = V_{\mathbb{C}} \longrightarrow \mathbb{C}.$$

The left hand side is $V^{-1,0} \oplus V^{0,-1}$, and since the formula shows that i_h commutes with the action of $\mathbb{C}^\times$ on both sides, it follows that the map $V_{\mathbb{C}} \to \mathbb{C}$ is the projection

$$V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}/V^{0,-1}.$$

In other words, the $\mathbb{C}$ in the numerator is identified with $V^{-1,0}$, and we have the formula

$$E_h = (V_{\mathbb{C}}/V_h^{0,-1})/i_h(\mathbb{Z}^2).$$

We can further check that $i_h(\mathbb{Z}^2)$ is given by $\mathbb{Z} \oplus \mathbb{Z} \cdot \tau_h$.

1.3 Moduli interpretation

We have constructed a family of elliptic curves $\mathcal{E}$ over $\mathbb{H}$, but as we saw above, elliptic curves over $\mathbb{C}$ are parametrized by $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. We want to say that the family $\mathcal{E}/\mathbb{H}$ descends to this quotient. This would imply the existence of a universal family over $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, and hence this would imply that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ a fine moduli space. (We will discuss this notion rigorously later.)

However, we see that $\mathcal{E}$ does not admit a quotient by $\mathrm{GL}(2,\mathbb{Z})$. More precisely, there is an action of $\mathrm{GL}(2,\mathbb{Z})$ on the family $\mathcal{E}$ preserving the subgroup $i_h(\mathbb{Z}^2)$; we simply let $g \in \mathrm{GL}(2,\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}^2)$ act naturally on $i_h(\mathbb{Z}^2) \subset V_{\mathbb{C}}$. We run into the same issue as before: the element $-I_2 \in \mathrm{GL}(2,\mathbb{Z})$ acts as -1 on each $\mathcal{E}_h$ and the quotient is no longer a family of elliptic curves; and there are other elliptic fixed points in $\mathbb{H}$ (namely i and $e^{\frac{2\pi i}{3}}$) whose stabilizers define automorphisms of the corresponding elliptic curves.

Now, if we instead consider the group

$$\Gamma(N) = \{g \in \mathrm{GL}(2,\mathbb{Z}) \mid g \equiv I_2 \pmod{N}, \}$$

then there are no fixed points in $\mathbb{H}$ for any integer $N \geq 3$.

Proposition 1.14. For $N \geq 3$, $\Gamma(N)$ acts freely and properly discontinuously on $\mathbb{H}^+$.

Proof. We sketch the proof that the action is free. Suppose $\gamma \in \Gamma(N)$ has a fixed point in $\mathbb{H}^+$. Since the stabilizer of $i \in \mathbb{H}^+$ in $\mathrm{SL}_2(\mathbb{R})$ is $\mathrm{SO}_2(\mathbb{R})$ and since $\mathbb{H}^+$ is transitive under $\mathrm{SL}_2(\mathbb{R})$, we see that γ must lie in a $\mathrm{SL}_2(\mathbb{R})$-conjugate of $\mathrm{SO}_2(\mathbb{R})$. In particular γ must be semi-simple and its eigenvalues in $\mathbb{C}$ have absolute value 1. On the other hand, the characteristic polynomial of γ is monic with integer coefficients, so the eigenvalues of γ are algebraic integers. Combined with the previous fact, we see that the eigenvalues of γ must be roots of unity. In particular, we see that $\langle\gamma\rangle$ is a torsion subgroup of $\Gamma(N)$, but we can check that $\Gamma(N)$ is torsion free.

We omit the proof that $\Gamma(N)$ acts properly discontinuously. See [DS06, §2.1]. ∎

In particular, this implies that $\Gamma(N)\backslash\mathbb{H}^+$ has the natural structure of a Riemann surface and $\mathbb{H}^+ \to \Gamma(N)\backslash\mathbb{H}^+$ is a covering. Further, this is obviously the universal covering, since $\mathbb{H}^+$ is simply connected.

Definition 1.15. The *modular curve* $Y(N)$ is the complex manifold

$$Y(N) := \bigsqcup_{j\in(\mathbb{Z}/N\mathbb{Z})^*} \Gamma(N)\backslash\mathbb{H}.$$

It also follows that the quotient $\Gamma(N)\backslash\mathcal{E}$ is a family of elliptic curves over $\Gamma(N)\backslash\mathbb{H}$.

We can ask what this space classifies. Observe that $\Gamma(N)$ fixes the group $N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$, the basis of points of order N in $\mathcal{E}_h$ as defined by the generators

$$\begin{pmatrix}1\\0\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}0\\1\end{pmatrix}$$

modulo N is fixed for all $h \in \mathbb{H}$. Thus, we see that points of $\Gamma(N)\backslash\mathbb{H}$ carry more than the data of the elliptic curve E_h: we also have an isomorphism

$$\alpha_N : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N],$$

where

$$E[N] := \{z \in E \mid z + \cdots + z \text{ (N times) } = 0\}.$$

Recall that $E[N]$ is non-canonically isomorphic to $(\mathbb{Z}/\mathbb{Z})^2 = \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ as $\mathbb{Z}/N\mathbb{Z}$-modules.

Definition 1.16. A choice of an isomorphism $\gamma : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ is called a *level-N structure* on E. Equivalently, this is a choice of an ordered basis (P, Q) of $E[N]$ as a free $\mathbb{Z}/N\mathbb{Z}$-module.

Now, we consider the following: For each $j \in (\mathbb{Z}/N\mathbb{Z})^\times$, fix once and for all an element $g_j \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det(g_j) = j$. For instance, we may take $g_j = \begin{pmatrix} j & 0\\ 0 & 1\end{pmatrix}$.

For each $j \in (\mathbb{Z}/N\mathbb{Z})^\times$ and each $h \in \mathbb{H}^+$, we can define an elliptic curve together with a level-N structure: $(E_h, \gamma_h = g_j \circ \alpha_N : E_h[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2)$. Moreover, we say that two tuples (E, γ) and (E', γ') are isomorphic if we have an isomorphism $f : E \mapsto E'$ such that we have a commutative square

$$\begin{array}{ccc} E[N] & \xrightarrow{f} & E'[N] \\ \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\gamma'} \\ (\mathbb{Z}/N\mathbb{Z})^2 & = & (\mathbb{Z}/N\mathbb{Z})^2. \end{array}$$

Thus, we have a map

$$Y(N) \to \{\text{elliptic curves with level } N\text{-structure}\}/\text{isomorphism} \tag{1.3.1}$$

Proposition 1.17. The map (1.3.1) is a bijection.

Proof. We sketch here surjectivity: Let (E, γ) be an elliptic curve with level N structure. As before, we can identify E with a complex structure on given by some $h \in \mathbb{H}$ on $\Lambda = \mathbb{Z}^2$. Fix an isomorphism

$$u : \Lambda/N\Lambda \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2.$$

Observe that a level N structure on E induces an isomorphism (also denoted γ)

$$\gamma : \Lambda/N\Lambda \simeq (\mathbb{Z}/N\mathbb{Z})^2,$$

we compose u with some element of $\mathrm{GL}_2(\mathbb{Z})$ of determinant -1, and as a result we can always assume that $h \in \mathbb{H}^+$. Now let γ' be the composition

$$(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{u^{-1}} \Lambda/N\Lambda \xrightarrow{\gamma} (\mathbb{Z}/N\mathbb{Z})^2.$$

Then $\gamma' \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We note the following fact:

Fact. (Strong approximation for SL_2.) The natural map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

For a proof, see [DS06, Exercise 1.2.2]. Note that the statement is not true if we replace SL_2 by GL_2, since elements of $\mathrm{GL}_2(\mathbb{Z})$ all have determinants ± 1.

Let $j = \det(\gamma')$, so $\gamma' g_j^{-1} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. By the above fact, we can compose u with a suitable element of $\mathrm{SL}_2(\mathbb{Z})$ to arrange that $\gamma' = g_j$. When we do this the element h we found in the above will be moved by the element of $\mathrm{SL}_2(\mathbb{Z})$. The image of such h under the above map will hence be the isomorphism (E, γ). $\square$

Remark 1.18. Note that to make a distinguished choice of one connected component $\Gamma(N)\backslash\mathbb{H}$ in $Y_(N)$ amounts to choosing a primitive N-th root of unity. In particular, we see that $Y(N)$ is a more natural space to consider, since we are not required to make this choice. This difference will become important later when we want to define the canonical model of the modular curve.

It is natural to simply 'extend the moduli problem' to classify elliptic curves over arbitrary bases (at least away from primes dividing N), where we have $E[N]$ is (at least étale locally) isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. We will make this precise later.

References

[DS06] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, Springer New York, 2006.