

# 18.783 Elliptic Curves

## Lecture 18

Andrew Sutherland

November 13, 2025

## The CM torsor

Let  $\mathcal{O}$  be an order in an imaginary quadratic field with ideal class group  $\text{cl}(\mathcal{O})$ . The set

$$\text{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E) : E/\mathbb{C} \text{ with } \text{End}(E) = \mathcal{O}\}$$

is a **torsor** for the ideal class group  $\text{cl}(\mathcal{O})$ , where the action is induced by

$$\mathfrak{a}E_{\mathfrak{b}} := E_{\mathfrak{a}^{-1}\mathfrak{b}},$$

for proper  $\mathcal{O}$ -ideals  $\mathfrak{a}$  and  $\mathfrak{b}$ , where  $E_{\mathfrak{b}} \leftrightarrow \mathbb{C}/\mathfrak{b}$ , corresponding to the isogeny

$$\phi_{\mathfrak{a}}: E_{\mathfrak{b}} \rightarrow \mathfrak{a}E_{\mathfrak{b}}$$

of degree  $N\mathfrak{a} := [\mathcal{O} : \mathfrak{a}]$  induced by the inclusion  $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$  with kernel

$$E_{\mathfrak{b}}[\mathfrak{a}] := \{P \in E_{\mathfrak{b}}(\mathbb{C}) : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a} \subseteq \mathcal{O} \simeq \text{End}(E_{\mathfrak{b}})\}.$$

## The modular curve $Y(1)$

Recall that the modular group  $\Gamma := \mathrm{SL}_2(\mathbb{Z})$  acts on the upper half-plane  $\mathcal{H}$  via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d}.$$

### Definition

The modular curve  $Y(1)$  is the quotient  $\mathcal{H}/\Gamma$  (the  $\Gamma$ -orbits of  $\mathcal{H}$ )

The set  $Y(1)(\mathbb{C})$  may be identified with the fundamental region for  $\Gamma$ :

$$\mathcal{F} = \{z \in \mathcal{H} : \operatorname{re}(z) \in [-1/2, 1/2) \text{ and } |z| \geq 1, \text{ with } |z| > 1 \text{ if } \operatorname{re}(z) > 0\}.$$

The region  $\mathcal{F}$  is not compact. To make it compact we formally add  $\infty := i\infty$ . Now

$$\lim_{\operatorname{im} \tau \rightarrow \infty} \frac{a\tau + b}{c\tau + d} = \frac{a}{c},$$

so to construct a space on which  $\Gamma$  acts, we should also include  $\mathbb{Q}$ .

# The modular curve $Y(1)$

## Definition

The **extended upper half-plane** is the set

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

endowed with the topology determined by the following basic open sets

- $\tau \in \mathcal{H}$ : all open disks about  $\tau$  that lie in  $\mathcal{H}$ ;
- $\tau \in \mathbb{Q}$ : all sets  $\{\tau\} \cup D$ , where  $D \subseteq \mathcal{H}$  is an open disk tangent to  $\mathbb{R}$  at  $\tau$ ;
- $\tau = \infty$ : all sets  $\{\infty\} \cup \{\tau \in \mathcal{H} : \text{im } \tau > r\}$  with  $r > 0$ .

## Definition

The **modular curve**  $X(1)$  is the quotient  $\mathcal{H}^*/\Gamma$  (the  $\Gamma$ -orbits of  $\mathcal{H}^*$ ).

The set  $X(1)(\mathbb{C})$  may be identified with the fundamental region  $\mathcal{F}^* := \mathcal{F} \cup \{\infty\}$ .

## Topological properties of $X(1)$

### Lemma

*For any compact sets  $A, B \subseteq \mathcal{H}$  the set  $S = \{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$  is finite.*

**Proof:** To the board!

### Lemma

*For any  $\tau_1, \tau_2 \in \mathcal{H}^*$  there exist open neighborhoods  $U_1, U_2$  of  $\tau_1, \tau_2$  such that*

$$\gamma U_1 \cap U_2 \neq \emptyset \iff \gamma \tau_1 = \tau_2,$$

*for  $\gamma \in \Gamma$ . Each  $\tau \in \mathcal{H}^*$  has an open neighborhood in which it has no  $\Gamma$ -equivalents.*

**Proof:** To the board!

### Theorem

*$X(1)$  is a connected compact Hausdorff space.*

**Proof:** To the board!

# Riemann surfaces

## Definition

A **complex structure** on a topological space  $X$  is an open cover  $\{U_i\}$  of  $X$  together with a set of compatible homeomorphisms  $\psi_i: U_i \rightarrow \mathbb{C}$  with open images.

Homeomorphisms  $\psi_i$  and  $\psi_j$  are compatible if whenever  $U_i \cap U_j \neq \emptyset$  the **transition map**

$$\psi_j \circ \psi_i^{-1}: \psi_i(U_i \cap U_j) \rightarrow \psi_j(U_i \cap U_j)$$

is holomorphic. The  $\psi_i$  are called **charts** and the collection  $\{\psi_i\}$  is an **atlas**.

## Definition

A **Riemann surface** is a connected Hausdorff space with a complex structure (equivalently, it is a connected complex manifold of dimension one).

## Complex tori are Riemann surfaces

Let  $L$  be a lattice in  $\mathbb{C}$  and let  $\pi: \mathbb{C} \rightarrow \mathbb{C}/L$  be the quotient map, and choose  $r > 0$  less than half the length of the shortest vector in  $L$ .

For each  $z$  in a fundamental region for  $L$ , let  $U_z$  be the open disk of radius  $r$  about  $z$ . Then  $\pi|_{U_z}$  defines a homeomorphism and we may take  $\{\pi(U_z)\}$  as our open cover, the maps  $\pi^{-1}: \pi(U_z) \rightarrow U_z$  as our charts, and the identity maps as transition maps.

This defines a complex structure on the torus  $\mathbb{C}/L$ ; it is connected and Hausdorff, hence a Riemann surface. In fact it is a compact Riemann surface. To compute its genus we can apply Euler's formula

$$V - E + F = 2 - 2g$$

to any triangulation of a fundamental parallelogram:  $1 - 3 + 2 = 2 - 2g$ , so  $g = 1$ .

## A complex structure for $X(1)$

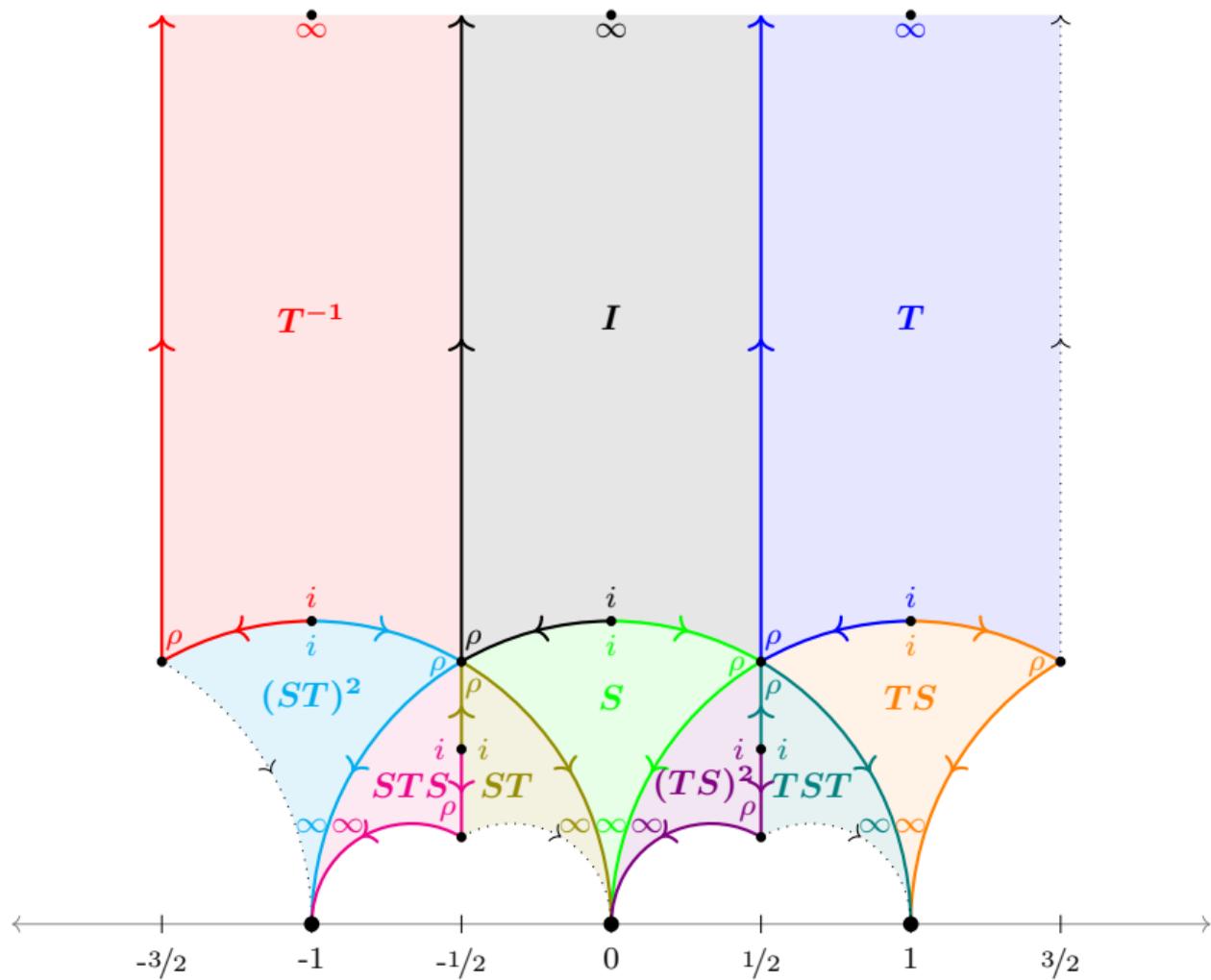
To define a complex structure on  $X(1)$  we can restrict attention to  $\mathcal{F}^*$ . There are three points that complicate matters:  $i, \rho := e^{2\pi i/3}, \infty$ .

### Lemma

Let  $G_\tau$  be the stabilizer of  $\tau \in \mathcal{F}^*$  in  $\Gamma$ . Let  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Then

$$G_\tau = \begin{cases} \{\pm I\} \simeq \mathbb{Z}/2\mathbb{Z} & \text{if } \tau \notin \{i, \rho, \infty\}; \\ \langle S \rangle \simeq \mathbb{Z}/4\mathbb{Z} & \text{if } \tau = i; \\ \langle ST \rangle \simeq \mathbb{Z}/6\mathbb{Z} & \text{if } \tau = \rho \\ \langle \pm T \rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} & \text{if } \tau = \infty. \end{cases}$$

**Proof:** See Problem Set 8.



## A complex structure for $X(1)$

Let  $\pi: \mathcal{H}^* \rightarrow X(1)$  be the quotient map, and for  $x \in X(1)$  let  $\tau_x$  be the unique point in  $\mathcal{F}^*$  with  $\pi(\tau_x) = x$ , and let  $G_x := G_{\tau_x}$  be its stabilizer in  $\Gamma$ .

For each  $\tau_x \in \mathcal{F}^*$  pick a neighborhood  $U_x$  such that  $\gamma U_x \cap U_x$  is empty for all  $\gamma \notin G_x$ . The sets  $\pi(U_x)$  are an open cover of  $X(1)$ .

For  $x \neq \infty$  we map  $U_x$  to the unit disc  $\mathcal{D} := \{z \in \mathbb{C} : |z| < 1\}$  via the homeomorphism

$$\begin{aligned} \delta_x: \mathcal{H} &\rightarrow \mathcal{D} \\ \tau &\mapsto \frac{\tau - \tau_x}{\tau - \bar{\tau}_x} \end{aligned}$$

Note that  $\operatorname{im} \tau > 0$  and  $\operatorname{im} \bar{\tau}_x < 0$  so  $\delta_x(\tau)$  is defined on  $\mathcal{H}$ , and nonzero for  $\tau \neq \tau_x$ . The map  $\delta_x$  extends to a map on  $\mathcal{H}^*$  sending  $\infty$  to 1 and  $\mathbb{Q}$  to points on  $\partial\mathcal{D}$ .

## A complex structure for $X(1)$

For  $\tau_x \neq i, \rho, \infty$  we have  $G_x = \{\pm 1\}$ , which stabilizes every point in  $U_x$ , so  $\pi|_{U_x}$  is injective and  $U_x/\Gamma = U_x/G_x = U_x$ , and we define the chart  $\psi_x := \delta_x \circ \pi^{-1}$ .

For  $\tau_x = i, \rho$  we have  $|G_x| > 2$ , so we instead define  $\psi_x(x) := \delta_x(\pi^{-1}(x))^n$ , where  $n := |G_x|/2$  is the size of the  $\Gamma$ -orbits in  $U_x - \{\tau_x\}$ ; this also works for  $|G_x| = 2$ .

### Lemma

Let  $\tau_x \in \mathcal{H}$ , with  $\delta_x(\tau)$  as above, and let  $\varphi: \mathcal{H} \rightarrow \mathcal{H}$  be a holomorphic function fixing  $\tau_x$  whose  $n$ -fold composition with itself is the identity, with  $n$  minimal. Then for some primitive  $n$ th root of unity  $\zeta$ , we have  $\delta_x(\varphi(\tau)) = \zeta\delta_x(\tau)$  for all  $\tau \in \mathcal{H}$ .

**Proof:** See notes.

For  $x = \infty$  we have  $\overline{G}_x \simeq \mathbb{Z}$ , define  $\delta_\infty(z) := e^{2\pi iz}$  for  $z \neq \infty$  and  $\delta_\infty(\infty) := 0$ , and take the chart  $\psi_\infty := \delta_\infty \circ \pi^{-1}$ , so  $\delta_\infty(\tau + m) = \delta_\infty(\tau)$  for  $\tau \in U_\infty - \{\infty\}$  and  $m \in \mathbb{Z}$ .

## A complex structure for $X(1)$

### Theorem

The open cover  $\{U_x\}$  and atlas  $\{\psi_x\}$  define a complex structure on  $X(1)$ .

**Proof:** See notes.

### Theorem

The modular curve  $X(1)$  is a compact Riemann surface of genus 0.

**Proof:**  $X(1)$  is a connected compact Hausdorff space with a complex structure, hence a compact Riemann surface. To show that it has genus 0, we triangulate by connecting the points  $i$ ,  $\rho$ , and  $\infty$ , yielding two triangles. Applying Euler's formula

$$V - E + F = 2 - 2g$$

with  $V = 3$ ,  $E = 3$ , and  $F = 2$ , we see that  $g = 0$ .

$X(1)$  is homeomorphic to the Riemann sphere  $S = \mathbb{P}^1(\mathbb{C})$ .

The modular curve  $Y(1)$  is homeomorphic to the complex plane  $\mathbb{C}$  via the  $j$ -function. 12

## More modular curves

### Definition

The **principal congruence subgroup**  $\Gamma(N)$  is defined by

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

A **congruence subgroup** (of level  $N$ ) is a subgroup of  $\mathrm{SL}_2(\mathbb{Z})$  that contains  $\Gamma(N)$ , e.g.

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\};$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

A **classical modular curve** is a quotient of  $\mathcal{H}^*$  or  $\mathcal{H}$  by a congruence subgroup.

We now define the modular curves

$$X(N) := \mathcal{H}^*/\Gamma(N), \quad X_1(N) := \mathcal{H}^*/\Gamma_1(N), \quad X_0(N) := \mathcal{H}^*/\Gamma_0(N),$$

all of which are compact Riemann surfaces.

MIT OpenCourseWare

<https://ocw.mit.edu>

18.783 / 18.7831 Elliptic Curves

Fall 2025

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.