18.783 Elliptic Curves
Lecture 18

Andrew Sutherland

November 14, 2023

The CM torsor

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

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

is a torsor for the ideal class group $\mathrm{cl}(\mathcal{O})$, 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

$$\phi_{\mathfrak{a}} \colon E_{\mathfrak{b}} \to \mathfrak{a}E_{\mathfrak{b}}$$

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

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

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 Γ-orbits of $\mathcal{H}$)

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

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

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

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

so to construct a space on which Γ 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 τ 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 τ;
- $\tau = \infty$: all sets of the form $\{\tau \in \mathcal{H} : \operatorname{im} \tau > r\}$ for any $r > 0$.

Definition

The modular curve $X(1)$ is the quotient $\mathcal{H}^*/\Gamma$ (the Γ-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* τ_1, τ_2 *such that*

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

for $\gamma \in \Gamma$. *Each* $\tau \in \mathcal{H}^*$ *has an open neighborhood in which it has no* Γ*-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 $\psi_i \colon U_i \to \mathbb{C}$ with open images.

Homeomorphisms ψ_i and ψ_j are compatible if whenever $U_i \cap U_j \neq \emptyset$ the transition map

$$\psi_j \circ \psi_i^{-1} \colon \; \psi_i(U_i \cap U_j) \to \psi_j(U_i \cap U_j)$$

is holomorphic. The ψ_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 $\pi\colon \mathbb{C} \to \mathbb{C}/L$ 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 disc of radius r about z. Then $\pi_{|_{U_z}}$ defines a homemomorphism and we may take $\{\pi(U_z)\}$ as our open cover, the maps $\pi^{-1}\colon \pi(U_z) \to U_z$ as our charts, and the identity map as transition maps.

This defines a complex structure on the torus $\mathbb{C}/L$, and it is connected 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 $X(1)$

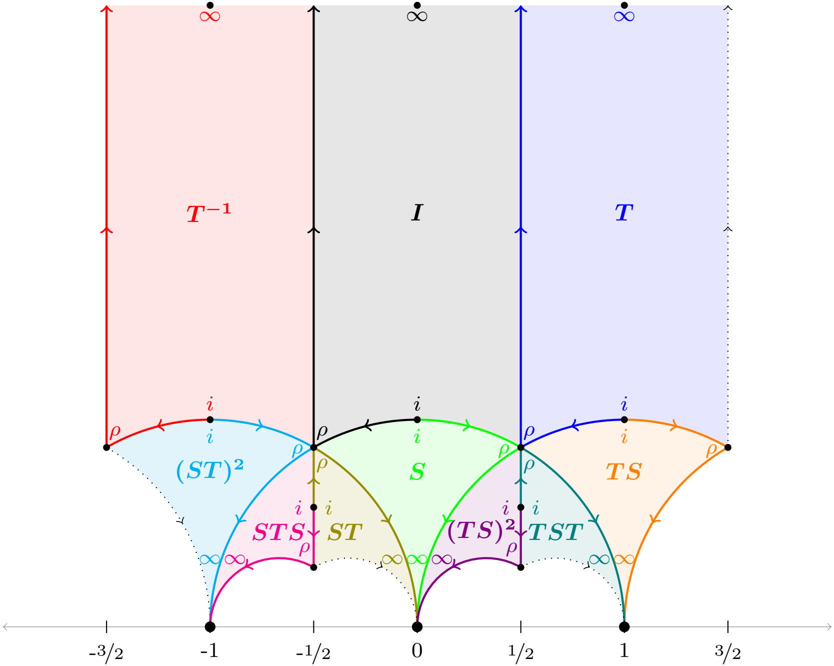
To define a complex structure of $X(1)$ we can restrict attention to $\mathcal{F}^*$. There are three points that complicate matters: $i, \rho := e^{2\pi i/3}, \infty$.

Lemma

Let G_τ be the stabilizer of $\tau \in \mathcal{F}^*$ in Γ. Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then

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

Proof: See Problem Set 8.



∞
∞
∞
T^{-1}
I
T
i
ρ
$(ST)^2$
S
TS
STS
ST
$(TS)^2$
TST
-3/2
-1
-1/2
0
1/2
1
3/2

A complex structure for $X(1)$

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

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

$$\delta_x\colon \mathcal{H} \to \mathcal{D}$$
$$\tau \mapsto \frac{\tau - \tau_x}{\tau - \bar{\tau}_x}$$

Note that $\operatorname{im}\tau > 0$ and $\operatorname{im}\bar{\tau}_x < 0$ so $\delta_x(\tau)$ is defined and nonzero for all $\tau \in \mathcal{H}$. The map δ_x extends to a map on $\mathcal{H}^*$ sending ∞ 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 $|G_x| > 2$ we instead define $\psi_x(x) := \delta_x(\pi^{-1}(x))^n$, where $n := |G_x|/2$ is the size of the Γ-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 $\varphi\colon \mathcal{H} \to \mathcal{H}$ be a holomorphic function fixing τ_x whose n-fold composition with itself is the identity, with n minimal. Then for some primitive nth root of unity ζ, we have $\delta_x(\varphi(\tau)) = \zeta\delta_x(\tau)$ for all $\tau \in \mathcal{H}$.

Proof: See notes.

For $x = \infty$ we have $G_x = \simeq \mathbb{Z}$, define $\delta_\infty(z) := e^{2\pi i z}$ 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 with a complex structure, hence a compact Riemann surface. To show that it has genus 0, we triangulate by connecting the points i, ρ, and ∞, 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.

More modular curves

Definition

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

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

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

$$\Gamma_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N \right\};$$
$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N \right\}.$$

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

We now define the modular curves

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

all of which are compact Riemann surfaces.