Modular Curves as Moduli Spaces

Math 285M Final Presentation

December 17, 2025

Outline

The Modular Group and the Upper Half-Plane

- The Upper Half-Plane ($\mathbb{H}$): $\{z \in \mathbb{C} | \text{Im}(z) > 0\}$. A model of hyperbolic geometry.
- The Modular Group $SL_2(\mathbb{Z})$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.
- Action: The group acts on $\mathbb{H}$ by fractional linear transformations: $z \mapsto \frac{az+b}{cz+d}$.
- Fundamental Domain: A region in $\mathbb{H}$ that contains exactly one representative from each orbit.
- Extended upper half-plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{QP}^1$ adds a line at infinity. This will "compactify" the modular curve.

Congruence Subgroups

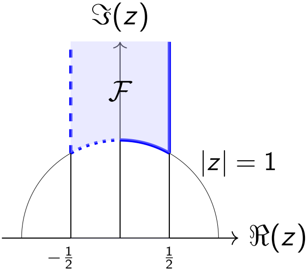
- $\Gamma_0(N)$: Matrices
$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
with $c \equiv 0 \pmod{N}$.
- $\Gamma_1(N)$: Matrices with $a, d \equiv 1 \pmod{N}$ and $c \equiv 0 \pmod{N}$.

Modular Curves

We have modular curves

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

Visualize as fundamental domains.



For $\Gamma = SL_2(\mathbb{Z})$, the modular curve is topologically equivalent to a sphere.

Visualizing Modular Curves

In the Poincaré disk, the fundamental domains for $SL_2(\mathbb{Z})$ and $\Gamma_0(11)$ are:

The modular curve $X_0(11)$ has genus 1.

More Fundamental Domains

(a) $X_1(5)$

(b) $X_1(11)$

History of Modular Curves as Moduli Spaces

- The study of modular curves has roots in the 19th century (Gauss, Dedekind, Klein, Poincaré).
- Hecke, Siegel, and Shimura connected modular curves to the arithmetic of elliptic curves.
- The modern perspective, viewing modular curves as moduli spaces, was crystallized in Grothendieck's school in the 1960s.

Moduli Spaces

Definition (Rough)

A moduli space is a geometric space whose points represent (isomorphism classes of) algebro-geometric objects of some fixed kind.

- $\mathbb{R}_{>0}$ is a moduli space for the problem of classifying circles in $\mathbb{R}^2$ up to congruence.
- $\mathbb{RP}^1$ is the moduli space for lines in $\mathbb{R}^2$ passing through the origin.
- $\mathbb{RP}^2$ is the moduli space for lines in $\mathbb{R}^3$ passing though the origin.

Why Moduli Spaces?

$$\text{Moduli Spaces} \quad \Longleftrightarrow \quad \text{“solution spaces”}$$

Example

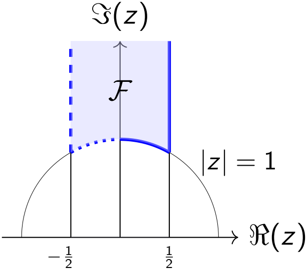
Circles in $\mathbb{R}^2$ inherit a notion of closeness from the moduli space $\mathbb{R}_{>0}$.

Modular Curves as Moduli Spaces

Theorem (Uniformization)

Each point $\tau \in \mathbb{H}$ gives an elliptic curve $E_\tau \cong \mathbb{C}/\Lambda_\tau$ and this classifies all elliptic curves.

$Y(1) = \mathbb{H}/\Gamma$ is the moduli space for elliptic curves.



Modular Curves as Moduli Spaces

We can generalize this:

- $Y_1(N) \quad \Longleftrightarrow \quad (E, P)$, where $|P| = N$.
- $Y_0(N) \quad \Longleftrightarrow \quad (E, C)$, where $C \subset E$ cyclic, $|C| = N$.

Proof Sketch

Let E be an elliptic curve, and $P \in E(\mathbb{C})$ have order N.

- $E \cong \mathbb{C}/\Lambda_\tau$
- $P = (c\tau + d)/N + \Lambda_\tau$ HW!!
- Use $\mathrm{SL}_2(\mathbb{Z})$ to send $\frac{c\tau+d}{N} \to \frac{1}{N}$.
- $\Gamma_1(N)$ fixes $\frac{1}{N} + \Lambda_\tau$.
- Thus, consider τ as an element of $Y_1(N) \cong \mathbb{H}/\Gamma_1(N)$.

Proof Sketch

Conversely:

- Suppose $(E_\tau, P) \cong (E_{\tau'}, P')$, where $E_\tau = \mathbb{C}/\Gamma_\tau$, $P \cong \frac{1}{N} + \Lambda_\tau$.
- There exists some $\gamma \in \Gamma_1(N)$ sending $\tau \to \tau'$.

Modular Curves as Riemann Surfaces

- $Y_1(N) \cong \mathbb{H}/\Gamma_1(N)$ is the moduli space for enhanced elliptic curves (E, P), where $P \in E(\mathbb{C})$ is a point of order N.
- $X_1(N)$ is the compactification.
- The cusps do NOT correspond to elliptic curves.

Question

Why do we compactify $Y_1(N)$ to obtain $X_1(N)$?

Modular Curves as Riemann Surfaces

Answer

$X_*(N)$ may be described as an algebraic curve.

In fact, $X_0(N)$ and $X_1(N)$ can be described using polynomials with *rational* coefficients.

Key Idea

Rational points on $X_1(N)$ correspond to elliptic curves $E/\mathbb{Q}$ with a point $P \in E(\mathbb{Q})$ of order N.

Why there are no 11-torsion points

$X_1(11)$ is parametrized by $E_{11} : y^2 - y = x^3 - x^2$.

- All the rational points are cusps, so NO elliptic curves over $\mathbb{Q}$ with 11-torsion.

On the other hand, $X_1(5)$ can be parametrized by $x = y$.

- Has infinitely many rational points, hence there are infinitely many elliptic curves over $\mathbb{Q}$ with points of order 5.

When are points of order 11 possible?

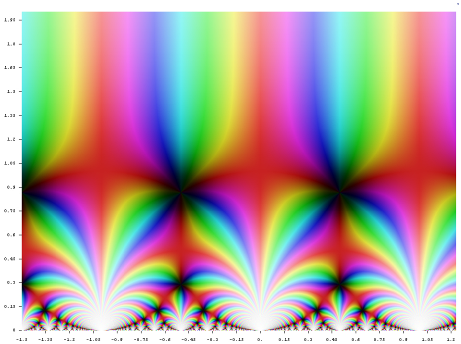
Key Idea

More generally, points in K on $X_1(N)$ correspond to elliptic curves E/K with points of order N.

- Let $K = \mathbb{Q}(\sqrt{2})$.
- Then $P = (\frac{1}{2}, \frac{1}{4}\sqrt{2} + \frac{1}{2}) \in E_{11}(K)$
- P has infinite order!
- Conclusion: infinitely many elliptic curves over K with points of order 11

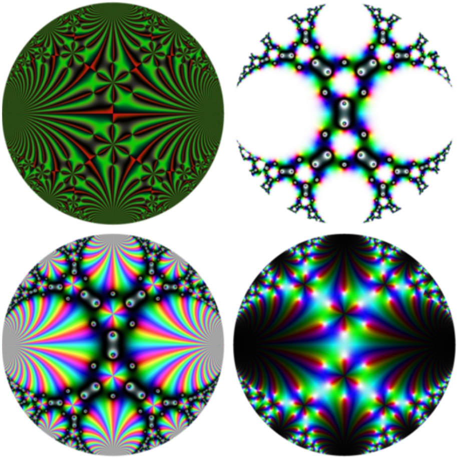
The j-invariant

For each elliptic curve $E = E_\tau$, we can associate a complex number $j(\tau)$ called the j-invariant, which uniquely determines E up to isomorphism. The function $j(\tau)$ is a modular function!



The j-invariant

In the Poincaré disk, it looks like:



What does $X_0(11)$ look like?

The functions $j(11\tau)$ and $j(\tau)$ generate $\mathcal{M}(\Gamma_0(11))$.

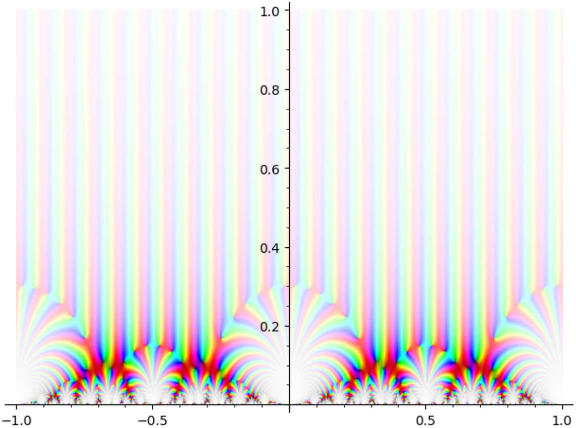


Figure: The modular form $(j(11\tau) + j(\tau))/1728$

Another view of $X_0(11)$

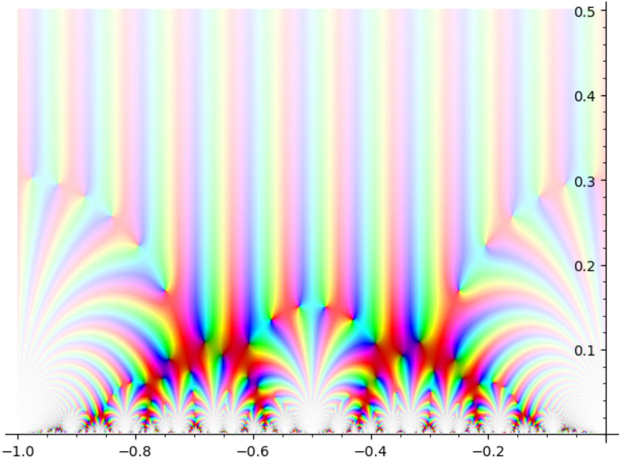


Figure: The modular form $(j(11\tau) + j(\tau))/1728$

References

- Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* (2nd ed.). Springer.
- Lowry Duda, D. (2021). Visualizing Modular Forms. In *Arithmetic geometry, number theory, and computation*, 537-557. Springer.
- Lowry Duda, D. (2022). *Visualizing Modular Curves*. davidlowryduda.com
- Baaziz, H. (2010). Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. Math. Comput., 79, 2371-2386.
- Stéphane Laurent. (2023). The pretty Klein j-invariant function. R-bloggers. r-bloggers.com
- The LMFDB Collaboration, The L-functions and modular forms database, lmfdb.org