Singular Moduli

Sarth Chavan

Euler Circle IRPW

July 17, 2023

Aims of the talk

1. Background & History
2. Introduce Elliptic curves
3. The j-invariant
4. Hilbert class polynomials

Hilbert's 9th and 12th problems

Figure: David Hilbert

- Find the general reciprocity law for any number field.

Hilbert's 9th and 12th problems

Figure: David Hilbert

- Find the general reciprocity law for any number field.
- Extend the Kronecker-Weber theorem to any number field.

What are Elliptic Curves?

Definition (Elliptic curves)

An **elliptic curve** is a plane curve defined by an equation of the form

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

for some constants a and b.

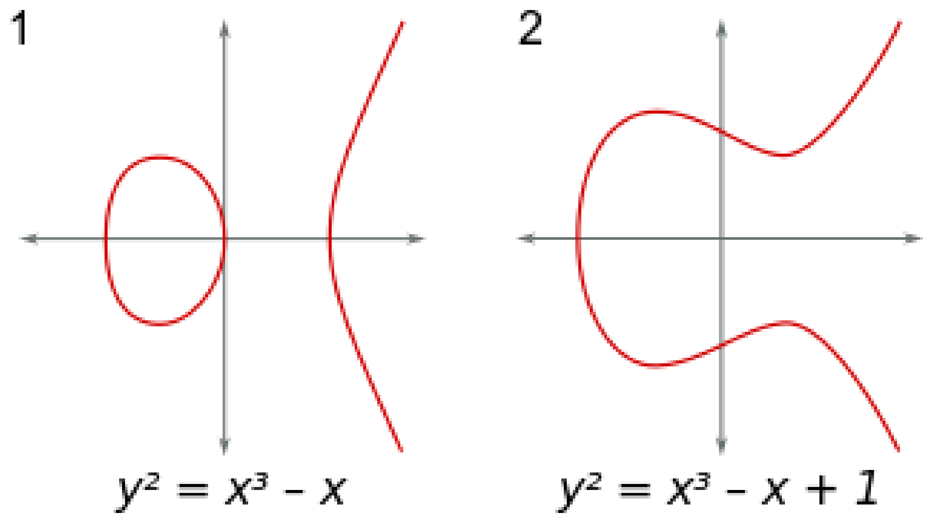
What are Elliptic Curves?

Definition (Elliptic curves)

An **elliptic curve** is a plane curve defined by an equation of the form

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

for some constants a and b.



Elliptic curves over $\mathbb{C}$

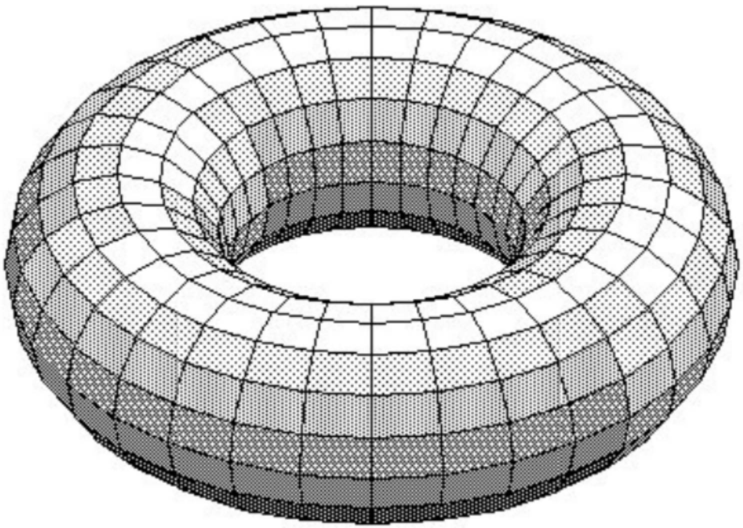


Figure: An elliptic curve over $\mathbb{C}$ is a compact manifold of the form $\mathbb{C}/L$, where $L = \mathbb{Z} + i\mathbb{Z}$ is a lattice in the complex plane.

Weierstrass Normal Form

Theorem

The equation of any cubic curve with a rational point can be written in the form

$$y^2 = 4x^3 - -\mathfrak{g}_2 x - \mathfrak{g}_3,$$

where a rational point is a point with rational coordinates.

Lattices and Curves

There is a bijective correspondence between lattices and complex elliptic curves.

Lattices and Curves

A **lattice** is defined to be an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$.

Lattices and Curves

A **lattice** is defined to be an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$. We find that

$$\mathfrak{g}_2(L) = 60 \sum_{L^*} \frac{1}{\omega^4}, \quad \mathfrak{g}_3(L) = 140 \sum_{L^*} \frac{1}{\omega^6},$$

where L^* is L without the element 0.

Singular moduli

Definition

The *j-invariant* of an elliptic curve E is defined as the quantity

$$j(E) = \frac{1728\mathfrak{g}_2^3}{\mathfrak{g}_2^3 - 27\mathfrak{g}_3^2} := \frac{1728\mathfrak{g}_2^3}{\Delta(E)},$$

where

$$\mathfrak{g}_2 = 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau+n)^4}, \quad \mathfrak{g}_3 = 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau+n)^6},$$

are multiples of the standard Eisenstein series on the upper half-plane $\mathbb{H}$.

Singular moduli

Definition

Let $j(z)$ be the classical modular function for $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$j(z) := \frac{1}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3$$
$$= q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$$

where $q = e^{2\pi \imath z}$ and $\sigma_a(n) = \sum_{k|n} k^a$.

Singular moduli

Definition

Let $j(z)$ be the classical modular function for $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$j\,(z) := \frac{1}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3$$
$$= q^{-1} + 744 + 196884q + 21493760q^2 + \ldots,$$

where $q = e^{2\pi\imath z}$ and $\sigma_a(n) = \sum_{k|n} k^a$.

Singular moduli is the classical name for the values assumed by $j(z)$ at imaginary quadratic arguments in the upper half of the complex plane.

Arithmetic nature

Let K be an imaginary quadratic number field with order $\mathcal{O}$.

Theorem

Let E be an elliptic curve with CM by $\mathcal{O}$. Then, $j(E)$ is an algebraic number.

Computing the singular moduli

Plug τ into the q-expansion of $j(\tau)$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots.$$

Computing the singular moduli

Plug τ into the q-expansion of $j(\tau)$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots .$$

This q-expansion can be computed via the q-expansions of $g_2(\tau)$ and $g_3(\tau)$,

$$g_2(\tau) = \frac{(2\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \quad g_3(\tau) = \frac{(2\pi)^6}{216}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)$$

Computing the singular moduli

Plug τ into the q-expansion of $j(\tau)$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots .$$

This q-expansion can be computed via the q-expansions of $g_2(\tau)$ and $g_3(\tau)$,

$$g_2(\tau) = \frac{(2\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \quad g_3(\tau) = \frac{(2\pi)^6}{216}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)$$

Can be computed using PARI-GP software.

Example

Example

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163 + 1728.$$

Example

Example

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163 + 1728.$$

Example

$$j\left(\frac{1+\sqrt{163}}{2}\right) = -(2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3.$$

Example

Example

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^6\cdot 3^6\cdot 7^2\cdot 11^2\cdot 19^2\cdot 127^2\cdot 163 + 1728.$$

Example

$$j\left(\frac{1+\sqrt{163}}{2}\right) = -(2^6\cdot 3\cdot 5\cdot 23\cdot 29)^3.$$

Example

$$j\left(\frac{1+\sqrt{-15}}{2}\right) = -\frac{-191025-85995\sqrt{5}}{2}.$$

Integrality of $j(\tau)$

Theorem

Let $\tau \in \mathbb{H}$. Then, $j(\tau)$ is an algebraic integer.

Gross-Zagier Theorem

Determined the prime factorization of the norm of the difference between two singular moduli.

Theorem

We have

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \pmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right),$$

where

$$J(d_1, d_2) = \left(\prod_{i=1}^{h_1} \prod_{k=1}^{h_2} (j(\mathfrak{a}_i) - j(\mathfrak{b}_k))\right)^{4/w_1 w_2}.$$

Hilbert class polynomials

Definition

The **Hilbert class polynomial** H_n is defined by

$$H_n(x) := \prod_{j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j(E)),$$

where $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E/\mathbb{C}) : \mathrm{End}(E) \cong \mathcal{O}\}$ is the set of j-invariants of elliptic curves $E/\mathbb{C}$ with CM by the imaginary order $\mathcal{O}$ with discriminant $-n = \mathrm{disc}(\mathcal{O})$.

Hilbert class polynomials

Definition

The **Hilbert class polynomial** H_n is defined by

$$H_n(x) := \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j(E)),$$

where $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E/\mathbb{C}) : \mathrm{End}(E) \cong \mathcal{O}\}$ is the set of j-invariants of elliptic curves $E/\mathbb{C}$ with CM by the imaginary order $\mathcal{O}$ with discriminant $-n = \mathrm{disc}(\mathcal{O})$.

Theorem

Hilbert class polynomials have integer coefficients, i.e., $H_n \in \mathbb{Z}[x]$.

Hilbert class polynomial

Problem. Given a monic irreducible polynomial $H \in \mathbb{Z}[X]$, determine whether H is an Hilbert class polynomial.

Hilbert class polynomial

Problem. Given a monic irreducible polynomial $H \in \mathbb{Z}[X]$, determine whether H is an Hilbert class polynomial.

Proposition

Let $H(X) \in \mathbb{Z}[X]$ be a polynomial of degree h with exactly h^+ real roots. If H is a Hilbert class polynomial then the following hold:

1. $h^+ \mid h$;
2. h^+ *is a power of* 2;
3. $h^+ \equiv h \pmod 2$; *that is,* $h^+ = 1$ *if and only if* h *is odd.*

Importance of singular moduli

- Generates ring class field extensions of imaginary quadratic fields.

Importance of singular moduli

- Generates ring class field extensions of imaginary quadratic fields.
- Distinguishes the isomorphism classes of elliptic curves with CM.