Elliptic Curves as Riemann Surfaces

Yuan Ze

Department of Mathematics
National University of Singapore

MA5253 presentation, Nov 2023

Table of Contents

Elliptic curves

An elliptic curve (E, O) is a nonsingular projective curve E of genus 1 with a base point O attached.

Weirestrass form:

Given elliptic curve (E, O), there are meromorphic functions x, y on E such that:

$$E \to \mathbb{CP}^2, \quad \text{by } \begin{cases} P \mapsto (x(P) : y(P) : 1) & P \neq O \\ P \mapsto (0 : 1 : 0) & P = O \end{cases}$$

maps E bihomorphically to an elliptic curve in form:

$$C : Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$$

where $g_2, g_3 \in \mathbb{C}$ such that $\Delta = g_2^3 - 27 g_3^2 \neq 0$.

Elliptic curves

Sketch of proof. In fact, E is compact as a closed subset of $\mathbb{CP}^2$. By the Riemann-Roch theorem:

$$\deg(D) \geq 2g - 1 \implies \dim \ell(D) = \deg(D)$$

hence for $n \in \mathbb{Z}^+$, we have $\dim \ell(nO) = \deg(nO) = n$, which means there exist $x, y \in \mathfrak{M}(E)$ such that:

$$\ell(O) = \mathrm{Span}_{\mathbb{C}}\{1\}, \quad \ell(2O) = \mathrm{Span}_{\mathbb{C}}\{1, x\}, \quad \ell(3O) = \mathrm{Span}_{\mathbb{C}}\{1, x, y\}$$

$$\ell(4O) = \mathrm{Span}_{\mathbb{C}}\{1, x, y, x^2\}, \quad \ell(5O) = \mathrm{Span}_{\mathbb{C}}\{1, x, y, x^2, xy\}$$

where x has a 2-pole at O only, and y has a 3-pole at O only.

Elliptic curves

On the other hand:

$$\ell(6O) = \mathrm{Span}_{\mathbb{C}}\{1, x, y, x^2, xy, x^3, y^2\}$$

by linear dependency (and normalizing x and y):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and finally by substitution:

$$(x, y) \mapsto \left(\frac{y}{2} + \frac{a_1x + a_3}{2}, x - \frac{a_1^2 + a_2}{4}\right) \implies y^2 = 4x^3 - g_2x - g_3$$

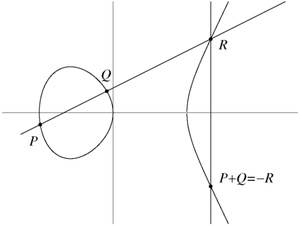
In particular, this is nonsingular.

The group law

Bézout's theorem:

Two coprime projective plane curves of degree m and n intersects at exactly mn points (counting multiplicity).

For elliptic curves over $\mathbb{R}$ with Weirestrass form ($O = (0 : 1 : 0)$):



Mordell-Weil theorem

The group of rational points on an elliptic curve is finitely generated.

Table of Contents

The Weierstrass $\wp$ function

Given lattice Λ on $\mathbb{C}$, functions:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \quad z \notin \Lambda$$

$$\wp'(z) = -\sum_{\omega \in \Lambda} \frac{2}{(z-\omega)^3}, \quad z \notin \Lambda$$

converging absolutely & uniformly on compact subsets of $\mathbb{C} \setminus \Lambda$, are Λ-periodic.

Proposition.

Functions $\wp$ and $\wp'$ satify the relation:

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Remark: $G_{2n}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2n}}$ is the Eisenstein series of weight $2n$.

The Weierstrass $\wp$ function

Proposition.

Functions $\wp$ and $\wp'$ satify the relation:

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Proof.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right)$$

$$= \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^{n+2}}$$

$$= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n} = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \mathcal{O}(z^6)$$

The Weierstrass $\wp$ function

Proposition.

Functions $\wp$ and $\wp'$ satify the relation:

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Proof.

$$\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \mathcal{O}(z^6)$$

$$\wp'(z) = -\frac{2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \mathcal{O}(z^5)$$

Direct calculation shows that:

$$(\wp'(z))^2 - \left(4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)\right) = \mathcal{O}(z^2)$$

is holomorphic at 0, and by Λ-periodicity is constantly 0.

The Weierstrass $\wp$ function

As a consequence, the point $(\wp(z), \wp'(z))$ satisfies the equation:

$$Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$

In fact, the RHS is a separable polynomial. Suppose $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, since $\wp'(z)$ is odd, by the Λ-periodicity we have:

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right) \implies \wp'\left(\frac{\omega_i}{2}\right) = 0, \quad i = 1, 2, 3$$

where $\omega_3 = \omega_1 + \omega_2$. Therefore $\wp(\omega_i/2)$ are roots of the polynomial $4X^3 - g_2(\Lambda)X - g_3(\Lambda)$. They are distinct since for each i:

$$\wp(z) - \wp(\omega_i/2)$$

has unique zero inside the fundamental domain D of Λ containing 0, by the fact that the only pole inside D is 0 of order 2, and $\omega_i/2$ is a zero of order 2.

Note. $\sum_{p\in D} \nu_p = 0$ by Λ-periodicity.

Elliptic curves as complex tori

Therefore we associated an elliptic curve $E(\Lambda)$ to a lattice Λ, by taking the projective completion $E(\Lambda)\colon Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$.

Proposition.

The map:

$$\varphi\colon \begin{cases} z+\Lambda \mapsto (\wp(z)\colon \wp'(z)\colon 1) & z \notin \Lambda \\ z+\Lambda \mapsto (0\colon 1\colon 0) & z \in \Lambda \end{cases}$$

gives an isomorphism from $\mathbb{C}/\Lambda$ to $E(\Lambda)$ as Riemann surfaces.

Proof of bijectivity. $z+\Lambda \mapsto \wp(z)$ surjects from $\mathbb{C}/\Lambda$ to $\hat{\mathbb{C}}$ as a non-constant holomorphic function. Any $w \in \mathbb{C}$ is taken twice by $\wp$ from two distinct points except the three double values $\wp(\omega_i/2+\Lambda)$. In this case, $w = \wp(\pm z+\Lambda)$ since $\wp$ is even, we have $\wp'(\pm z+\Lambda) = \pm\wp'(z+\Lambda) \neq 0$, hence φ is injective. It is also easy to see that φ is surjective.

Elliptic curves as complex tori

Proposition.

The map $\varphi\colon \mathbb{C}/\Lambda \to E(\Lambda)$ is a group isomorphism.

By properties of elliptic functions and examining Laurent expansion, we have the additive formula:

$$\wp(z) + \wp(z') + \wp(z + z') = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')}\right)^2$$

which coincides the explicit formula of x-coordinate in the group law.

The j-invariant

Recall. Any complex torus $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ for some $\tau \in \mathcal{H}$.

Denote $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$, the function:

$$j \colon \mathcal{H} \to \mathbb{C}, \quad j(\tau) = \frac{1728(g_2(\Lambda_\tau))^3}{(g_2(\Lambda_\tau))^3 - 27(g_3(\Lambda_\tau))^2}$$

is holomorphic and $\mathrm{SL}_2(\mathbb{Z})$-invariant. By expanding $g_2(\Lambda_\tau)$ and $g_3(\Lambda_\tau)$ to Fourier series, we deduce that:

$$j(\tau) = \frac{1}{q} + \cdots, \quad q = e^{2\pi i \tau}$$

hence j defines a non-constant holomorphic function $\mathrm{SL}_2(\mathbb{Z})/(\mathcal{H} \cup \{\infty\}) \to \hat{\mathbb{C}}$, which is surjective.

Remark. $G_k(\Lambda_\tau) = 2\zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$, $k > 2$ even.

The j-invariant

Recall. $\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\tau'}$ if and only if:

$$\tau' = \frac{a\tau + b}{c\tau + d} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

j is $\mathrm{SL}_2(\mathbb{Z})$-invariant, hence is well defined for isomorphic class of complex tori.

Proposition.

$\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$ if and only the values of j are the same.

Proof. If $j(\mathbb{C}/\Lambda) = j(\mathbb{C}/\Lambda')$, let $\lambda^4 = g_2(\Lambda)/g_2(\Lambda')$, by some algebra:

$$g_2(\Lambda') = g_2(\lambda\Lambda), \quad g_3(\Lambda') = g_3(\lambda\Lambda)$$

hence $\wp_{\Lambda'}(z) = \wp_{\lambda\Lambda}(z) \implies \Lambda' = \lambda\Lambda \implies \mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$.

Classification of elliptic curves over $\mathbb{C}$

The uniformization theorem for elliptic curves.

For any elliptic curve (E, O), there exists lattice Λ s.t. $(E, O) \simeq (\mathbb{C}/\Lambda, 0 + \Lambda)$.

Proof. Given $E\colon Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, choose $\tau \in \mathcal{H}$ such that:

$$j(\tau) = \frac{1728g_2^3}{g_2^2 - 27g_3^2} \implies \frac{g_2^3}{g_2(\Lambda_\tau)^3} = \frac{g_3^2}{g_3(\Lambda_\tau)^2}$$

Let $\omega_1^{-4} = g_2/g_2(\Lambda_\tau), \omega_2 = \tau\omega_1$, and $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, we have $g_2(\Lambda) = g_2$ and $g_3(\Lambda) = g_3$, hence $(E, O) \simeq (E(\Lambda), (0\colon 1\colon 0)) \simeq (\mathbb{C}/\Lambda, 0 + \Lambda)$.

Corollay.

We have the following correspondence:

$$\{\text{Elliptic curves over } \mathbb{C}\}/\simeq \;\longleftrightarrow\; \{\text{Complex tori}\}/\simeq \;\longleftrightarrow\; \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$$

Reference

1. Diamond, Fred, and Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. New York: Springer, 2005.
2. Milne, James S. *Elliptic curves*. World Scientific, 2020.
3. Silverman, Joseph H. *The arithmetic of elliptic curves*. Vol. 106. New York: Springer, 2009.