The j-invariant of an Elliptic Curve

Dylan Pentland

20 May 2018

An important question

Question. Given a polynomial $F(x, y) \in \mathbb{Q}[x, y]$, for which $p \in \mathbb{Q}^2$ is $F(p) = 0$?

It turns out a natural way to attack this problem is to attach a number g called the **genus** to F.

- $g = 0$. This is form conic sections, and these will either have no rational points or the rational points will be parameterized by $q \in \mathbb{Q}$ in an easy way.
- $g = 1$. These are cubic equations, and there can be finitely many rational points or infinitely many. The points have a nice group structure.
- $g \geq 2$. There are finitely many rational points (Falting's theorem).

What is an elliptic curve?

- An **elliptic curve** E is a curve of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

- With substitutions preserving rational points, these can be put in the **Weierstrass form** $y^2 = x^3 + ax + b$.
- E must also be **nonsingular**. Here, this means there are no self-intersections or cusps. We can check this by letting $F(x, y) = x^3 + ax^2 + bx + c - y^2$ and checking if

$$\nabla F = \vec{0},$$

at any point P where $F(P) = 0$, in which case E is singular.

The group structure of E

- Elliptic curves over $\mathbb{Q}$ come equipped with a group structure of the set of rational points $E(\mathbb{Q})$.
- We add $P, Q \in E(\mathbb{Q})$ to obtain a point $R = P \oplus Q$ by taking the third intersection R' of E and the line $\ell(P, Q)$ through P, Q. Flipping over the x axis, we obtain R.
- If $P = Q$, $\ell(P, Q)$ is the tangent to E. The identity is given by the point at infinity $\mathcal{O}$ – we say $P \oplus Q = \mathcal{O}$ if $\ell(P, Q)$ fails into intersect E in $\mathbb{R}^2$.

An illustration

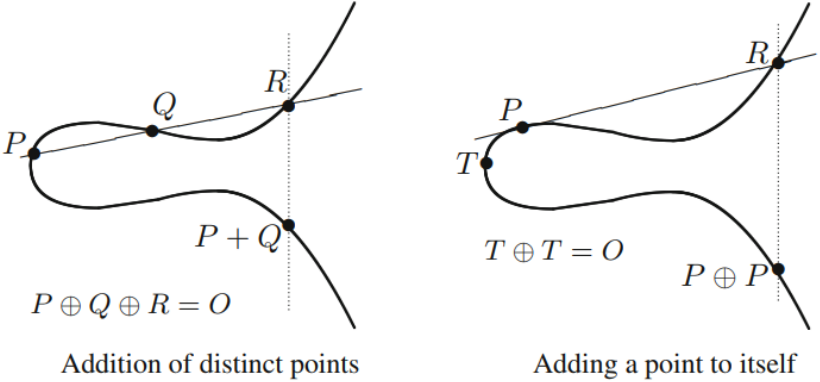

Figure 1: Elliptic curve addition (Image from [Sil09])

Elliptic curve isogenies

- An **isogeny** $\phi : E \to E'$ is a rational map which satisfies $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$, which reflects that ϕ induces a group homomorphism. The set of isogenies is denoted $\mathrm{Hom}(E, E')$. When $E = E'$, this is $\mathrm{End}(E)$.
- Over a field K, isogenies are maps $(x, y) \mapsto (f(x, y), g(x, y))$ where f, g are in $K(x, y)$.
- We say $E \cong E'$ if ϕ is an invertible map.
- **Example**: The map $[n] : E \to E$ sending $P \to nP$ is a member of $\mathrm{End}(E)$.

An isogeny invariant

Take an elliptic curve $E/\mathbb{Q}$ and write it in Weierstrass form $y^2 = x^3 + ax + b$. The j**-invariant** is given by

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Theorem

Let E, E' be elliptic curves over $\mathbb{Q}$. Then $E \cong E'$ over $\mathbb{C}$ if and only if $j(E) = j(E')$. In general, given a field K and elliptic curves E, E' over K then $E \cong E'$ over $\overline{K}$ if and only if $j(E) = j(E')$.

The $\wp$ function

In order to motivate $j(E)$, we need to reinterpret what an elliptic curve is. To do this, we look at **elliptic functions**, or doubly periodic meromorphic functions. The Weierstrass $\wp$ function describes these completely:

Theorem

Let $\Lambda \subset \mathbb{C}$ be a lattice, and let

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

The elliptic function field for $\mathbb{C}/\Lambda$ is given by $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.

Elliptic curves over $\mathbb{C}$ are complex tori

Theorem

Given a lattice $\Lambda \subset \mathbb{C}$, there is a corresponding elliptic curve E_Λ such that $\mathbb{C}/\Lambda \cong E_\Lambda(\mathbb{C})$ as groups. Given an elliptic curve E, there is a lattice Λ_E such that $E \cong \mathbb{C}/\Lambda_E$ as groups.

- The curve E_Λ is given by

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

  where $g_2(\Lambda) = 60\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-4}$, $g_3(\Lambda) = 140\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-6}$. The isomorphism is given by

$$z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)),$$

  when $z \notin \Lambda$ and $z \mapsto \mathcal{O}$ when $z \in \Lambda$.
- We can also take any elliptic curve E and obtain a lattice $\Lambda_E \cong \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ using integrals $\omega_1 = \int_\alpha \frac{dx}{y}$ and $\omega_2 = \int_\beta \frac{dx}{y}$ to obtain basis elements. Here, α, β generate $H_1(E(\mathbb{C}), \mathbb{Z})$.

Homothetic Lattices

We say Λ and Λ' are homothetic if $\Lambda = \omega\Lambda'$ for $\omega \in \mathbb{C}^\times$. We can equivalently characterize isomorphism classes of elliptic curves as follows:

Theorem

The complex tori $\mathbb{C}/\Lambda \cong E_\Lambda$ and $\mathbb{C}/\Lambda' \cong E_{\Lambda'}$ are isomorphic over $\mathbb{C}$ iff Λ and Λ' are homothetic.

Now it is very natural to consider the j**-invariant** from modular forms. This is defined by

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

where

$$g_2 = 60\sum_{(m,n)\neq(0,0)}(m+n\tau)^{-4}, g_3 = 140\sum_{(m,n)\neq(0,0)}(m+n\tau)^{-6}.$$

Why the j-invariant is a perfect fit

We want a homothety invariant $j(\Lambda)$ such that $j(\Lambda) = j(\Lambda')$ iff Λ, Λ' are homothetic. Suppose we have such a function:

- If j is a homothety invariant, $j([\omega_1, \omega_2]) = j([1, \omega_2/\omega_1])$.
- Consider $\tau, \tau' \in \mathbb{H}$. If $f(\tau) = f(\tau')$ precisely when the lattices $[1, \tau]$ and $[1, \tau']$ are the same then f should be a modular function as it is invariant under the natural action of $\mathrm{SL}(2, \mathbb{Z})$. The space of such functions is $\mathbb{C}(j)$, where $j = j(\tau)$ is the j-invariant.

As a result, we know we should base $j(\Lambda)$ off of $j(\tau)$. Noticing that g_2, g_3 sum over the lattice $[1, \tau]$, it is natural to define

$$j(E_\Lambda) = j(\Lambda) = 1728 \frac{g_2^3(\Lambda)}{g_2^3(\Lambda) - 27 g_3^2(\Lambda)},$$

where $g_2(\Lambda)$ and $g_3(\Lambda)$ are the coefficients of E_Λ.

- It remains to check that $j(\Lambda) = j(w\Lambda)$ – this is not too hard.

Conclusion

We can conclude the following about elliptic curves over $\mathbb{Q}$:

- If $j(E) \neq j(E')$, then certainly E and E' are not isomorphic.
- If $j(E) = j(E')$, they are isomorphic over $\mathbb{C}$ (more specifically, $\overline{\mathbb{Q}}$) but not necessarily over $\mathbb{Q}$. For example, take

$$E/\mathbb{Q} : y^2 = x^3 + x$$
$$E^7/\mathbb{Q} : y^2 = x^3 + 49x.$$

Here, $j(E) = j(E') = 1728$. However, $E(\mathbb{Q})$ is a finite group but $E^7(\mathbb{Q})$ is infinite, and hence not isomorphic to $E(\mathbb{Q})$. These curves are isomorphic over $\mathbb{Q}(\sqrt{7})$.

References

- Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.
- Joseph H Silverman and John Torrence Tate, *Rational points on elliptic curves*, vol. 9, Springer, 1992.