Algebraic Geometry Lecture 12 – Elliptic Curves

Duc Khiem Huynh

Motivation: The simplest form of Diophantine equation is a polynomial in one variable:

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \qquad a_i \in \mathbb{Z}. \tag{1}$$

We may ask

(i) Are there solutions in integers?

(ii) Are there solutions in rational numbers?

(iii) Are there infinitely many solutions in integers?

(iv) Are there infinitely many solutions in rational numbers?

We know there are at most n solutions to the equation, and we know which rational numbers to check thanks to...

Gauss' lemma. *If p/q is a rational solution to (1) with p and q coprime then $q \mid a_n$ and $q \mid a_0$.*

Now consider Diophantine equations in two variables:

$$f(x,y) = 0. \tag{2}$$

The set of real solutions to (2) form a curve in the x-y plane called an algebraic curve. The difficulty of solving the equation increases with the degree of the polynomial involved.

Linear equations These can be written

$$ax + by + c = 0$$

for $a, b, c \in \mathbb{Z}$. Such an equation always has infinitely many rational solutions. Using Bézout's identity there are no integer solutions if $\mathrm{hcf}(a,b) \nmid c$, and infinitely many solutions otherwise.

Quadratic equations Graphs of these equations are conic sections (named as such since they are formed by intersecting a plane with a cone). If there is a rational solution then there are infinitely many. Complete sets of solutions can be described (very easily) using geometry.

The next hardest case is cubic equations. In contrast to linear and quadratic solutions the rational and integer solutions to cubics are not yet completely understood. We do have:

Siegel's theorem (1920)**.** *A cubic equation has only finitely many integer solutions.*

Baker–Coates theorem (1970s)**.** *There is an explicit upper bound for the largest solution in terms of the coefficients of the polynomial.*

Using a change of variables a general cubic equation in two variables can be written as

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

which is known as the general Weierstrass form. If the characteristic of the field we are working over is not 2 then this can be further simplified to

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

Such a curve is called an elliptic curve. The name comes from the fact that the arc length of an ellipse is computed using

$$y = \sqrt{f(x)}$$

for a cubic polynomial f.

More specifically an elliptic curve is a non-singular curve - i.e. it has three distinct roots. Equivalently the discriminant

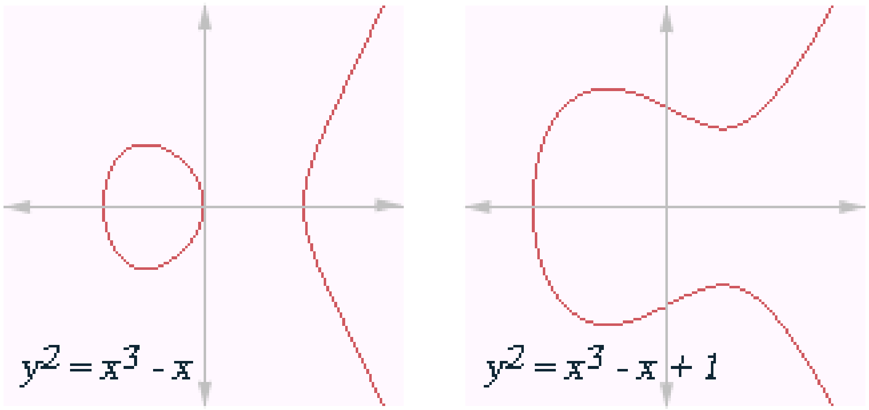
$$\Delta = -16(4b^3 + 27c^2)$$

is non-zero.

If the coefficients of $f(x) = x^3 + ax^2 + bx + c$ are rational numbers then f must have at least one real root by the intermediate value theorem. So we can write

$$f(x) = (x - \alpha)(x^2 + \beta x + \gamma).$$

If α is the only real root then f will only intersect the x-axis once, whereas if it has three real roots it will be made up of two parts. The curve on the right has one real root, while the one on the left has three:



Let $F(x,y) = y^2 - f(x)$. So

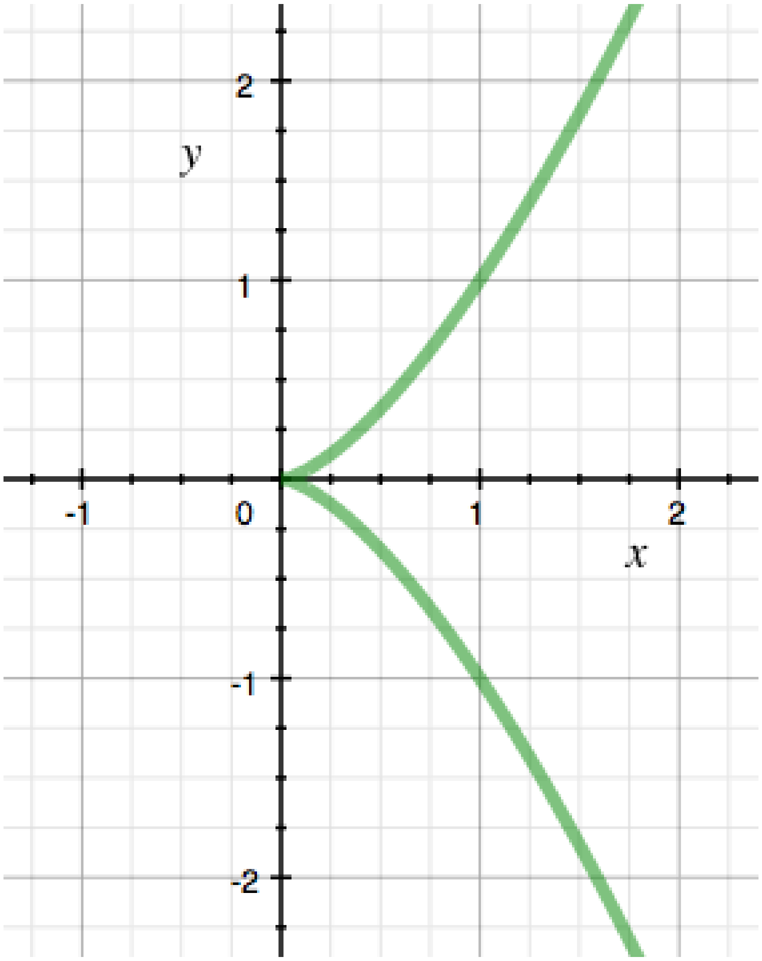
$$\frac{\partial F}{\partial x} = -f'(x) \qquad \frac{\partial F}{\partial y} = 2y.$$

The curve is singular if there exists a point (x_0, y_0) such that $F(x_0, y_0) = 0$ and both partial derivatives simultaneously vanish. So:

$$y_0 = 0, \quad f(x_0) = 0, \quad f'(x_0) = 0.$$

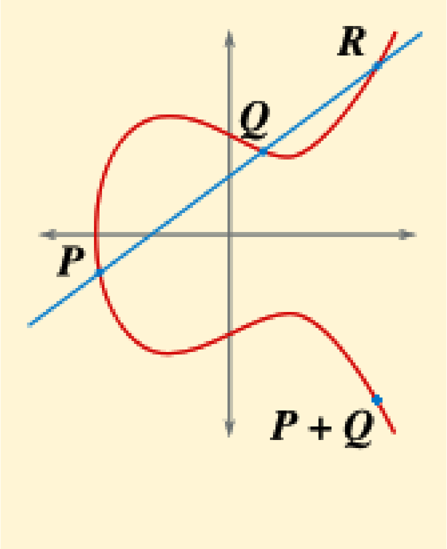
Thus f and f' have a common root x_0, so x_0 is a double root of f.

Conversely if f has a double root x_0 then $(x_0, 0)$ will be a singular point on C. If the root has multiplicity 2 then the curve will intersect itself, while if it has multiplicity 3 then the curve will have a cusp:



A cusp on $C : y^2 - x^3 = 0$.

Given a non-singular curve we can define the addition of two points on C geometrically:



Using this notion of addition on the rational points on C forms an abelian group denoted here as $\Gamma = C(\mathbb{Q})$.

Mordell's theorem. *The group of rational points on a non-singular cubic is finitely generated.*

Γ is isomorphic to a direct sum of infinite cyclic groups and finite cyclic groups of prime power orders:

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ times}} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{\nu_s}}$$

$$\cong \mathbb{Z}^r \oplus \mathcal{F}.$$

The number r is called the rank of C. $\mathcal{F}$ is the torsion group. Γ is finite if and only if its rank is zero.

Natural question: Given an elliptic curve how can we find its generating set? At present no one knows a procedure which is guaranteed to work for all curves.

To any elliptic curve E we can attach an L-function L. Then we have:

Birch–Swinnerton-Dyer conjecture.

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank}(E).$$

Height of a rational number

Let $x = p/q \in \mathbb{Q}$ with $(p, q) = 1$. Then the *height* of x is defined by

$$H(x) = \max\{|p|, |q|\}.$$

It can be thought of as a measurement of how “complicated” a rational number is. It is useful because we have:

The finiteness property of height: The set of all rational numbers whose height is less than some fixed number is finite.

Given an elliptic curve C and a point $P = (x, y) \in C(\mathbb{Q})$ we define

$$H(P) = H(x)$$
$$h(P) = \log H(P).$$

Descent theorem. *Let Γ be an abelian group and suppose that there is a function $h : \Gamma \to [0, \infty)$ with*

(i) for every $M \in \mathbb{R}$ the set $\{P \in \Gamma \mid h(P) \leqslant M\}$ is finite;

(ii) for every $P_0 \in \Gamma$ there is a constant K_0 such that

$$h(P + P_0) \leqslant 2h(P) + K_0$$

for every $P \in \Gamma$;

(iii) $h(2P) \geqslant 4h(P) - K$ for some constant K and every $P \in \Gamma$;

(iv) the subgroup 2Γ has finite index in Γ.

Then Γ is finitely generated.

Sketch proof. Take a representative for each coset of 2Γ in Γ. There are finitely many of them, say n. Denote them $Q_1, \dots, Q_n$. So for any $P \in \Gamma$ there is an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma.$$

So $P - Q_{i_1} = 2P_1$ for some $P_1 \in \Gamma$. Repeat this process with P_1 and so on:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m. \end{aligned}$$

The basic idea of the proof is that each P_i is more or less equal to $2P_{i+1}$ and the height $h(P_{i+1})$ is about $\frac{1}{4}h(P_i)$ by (ii). So the sequence of points $P_1, P_2, \dots$ should have decreasing height. Eventually they will end up in a set of points having bounded height, then by (i) the result follows. □

Mordell’s theorem is a corollary of the Descent theorem, all that is left to show is that the height function we defined satisfies all the hypotheses of the Descent theorem.