

Fermat's Last Theorem

Lecture I

Nuno Freitas

Second Portuguese number theory meeting

4 – 8 Sep 2023

Motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \quad a, b, c \in \mathbb{Z}, \quad n \geq 3$$

satisfy $abc = 0$.

Theorem (Wiles, Taylor–Wiles)

All semistable elliptic curves over \mathbb{Q} are modular.

Fields to keep in mind

- ▶ The complex numbers \mathbb{C} and the real numbers $\mathbb{R} \subset \mathbb{C}$.
- ▶ $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ satisfies a monic polynomial } f \in \mathbb{Q}[x]\}$
- ▶ $\overline{\mathbb{Q}}$ is a field called the **algebraic closure** of \mathbb{Q} .
- ▶ A **number field** K is a subfield of $\overline{\mathbb{Q}}$, which is finite dimensional as a \mathbb{Q} vector space.
- ▶ For example : $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$
- ▶ The p -adic fields \mathbb{Q}_p for all primes p
- ▶ The finite fields $\mathbb{F}_p \subset \overline{\mathbb{F}}_p$ for all primes p
- ▶ We denote $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_K := \text{Gal}(\overline{\mathbb{Q}}/K)$
- ▶ We denote $G_{\mathbb{Q}_p} := \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \simeq D_p \subset G_{\mathbb{Q}}$.

Rational points

Projective plane curves

Let $F \in K[X, Y, Z]$ be a homogeneous polynomial of degree d :

$$F(X, Y, Z) = \sum_{\substack{0 \leq i, j, k \leq d \\ i+j+k=d}} c_{ijk} X^i Y^j Z^k.$$

Then, we see that

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z), \quad \forall \lambda \in K.$$

Hence, $F(a, b, c) = 0$ implies that $F(\lambda a, \lambda b, \lambda c) = 0$. Therefore the following set is well-defined:

$$\mathcal{C} := \left\{ [a : b : c] \in \mathbf{P}^2(\overline{K}) : F(a, b, c) = 0 \right\},$$

where \overline{K} is a fixed algebraic closure of K .

We call \mathcal{C} the **projective plane curve** defined by F over K .

Projective plane curves

Example

(a) The line $L : 3x + y + 1 = 0$ becomes

$$\mathcal{L} : 3X + Y + Z = 0.$$

(b) The parabola $C : y - x^2 = 0$ becomes

$$\mathcal{C} : ZY - X^2 = 0.$$

(c) The plane cubic $C : y^2 = x^3 + ax + b$ becomes

$$\mathcal{C} : ZY^2 = X^3 + aXZ^2 + bZ^3.$$

(d) The Fermat curve $C_n : x^n + y^n = 1$ becomes

$$\mathcal{C}_n : X^n + Y^n = Z^n.$$

Rational points on curves

Definition

Let K be a field. Let $f \in K[x, y]$ define the **plane curve**

$$C : f(x, y) = 0.$$

For $a, b \in K$, we say that $P = (a, b)$ is a **rational point** on C if

$$f(a, b) = 0.$$

The set of all rational points on C is denoted by $C(K)$.

Given a field $F \supset K$ we are often interested in the set $C(F)$ of F -rational points.

Similarly, let $\mathcal{C} : F(x, y, z) = 0$ be a projective curve. Then, we say that $P = [a : b : c]$ is a **rational point** on \mathcal{C} if $F(a, b, c) = 0$. We denote the set of all K -rational points on \mathcal{C} by $\mathcal{C}(K)$.

Rational points on curves

Problem:

Let $C : f(x, y) = 0$ be a plane curve over \mathbb{Q} .

(a) **Does C have any rational point?** That is, is $C(\mathbb{Q}) \neq \emptyset$?

(b) If $C(\mathbb{Q}) \neq \emptyset$, can we **describe this set?**

We can also state this problem using projective plane curves.

Example

The curve $X^2 + Y^2 + Z^2 = 0$ has no points on \mathbb{Q} nor \mathbb{R} .

Rational points on curves

Example

We will show the curve $C : x^2 + y^2 = 3$ has no rational points.

A rational point on C is equivalent to a rational point (with $Z = 1$) on the homogenised curve

$$\mathcal{C} : X^2 + Y^2 = 3Z^2.$$

For a contradiction, assume that $[a : b : c] \in \mathcal{C}$ is rational, *i.e.*, $a^2 + b^2 = 3c^2$ with $a, b, c \in \mathbb{Q}$ **not** all zero.

WLOG we can assume that $a, b, c \in \mathbb{Z}$ are coprime.

By reducing modulo 4, we would have:

$$a^2, b^2, c^2 \equiv 0, 1 \pmod{4}$$

Therefore

$$a^2 + b^2 \equiv 0, 1, 2 \pmod{4} \quad \text{and} \quad 3c^2 \equiv 0, 3 \pmod{4}$$

thus a, b, c must all be even, contradiction with $\gcd(a, b, c) = 1$.

Rational points on curves

FLT can also be stated in terms of rational points.

Theorem (Wiles)

Let $n \geq 3$ be a natural number. A triple (a, b, c) , with $a, b, c \in \mathbb{Z}$, satisfies the equation $a^n + b^n = c^n$ if and only if $abc = 0$.

Without loss of generality, can assume that $c \neq 0$.

Set $x = a/c$ and $y = b/c$ in \mathbb{Q} (dehomogenization).

FLT: For $n \geq 3$, the curve $C_n : x^n + y^n = 1$ has **no** rational points, except for $(0, \pm 1), (\pm 1, 0)$ for n **even**, and $(0, 1), (1, 0)$ for n **odd**.

FLT only became a theorem in 1995 thanks to the British mathematician Andrew Wiles, and it was an open problem for around 350 years!

Finding rational points on curves is often a very hard problem!

Rational points on curves

The Fermat curve for $n = 2$ is the circle $C_2 : x^2 + y^2 = 1$.

We can parameterise rational points on C_2 by

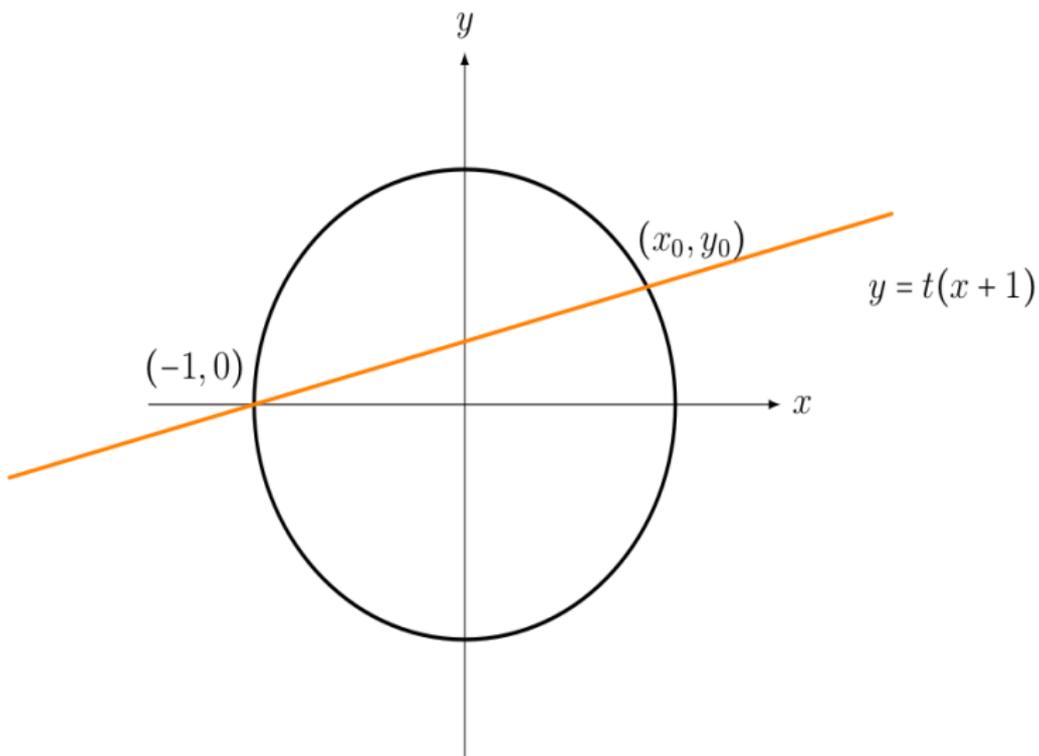
$$\begin{aligned} \mathbb{Q} &\rightarrow C_2(\mathbb{Q}) \setminus \{(-1, 0)\} \\ t &\mapsto (x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \end{aligned}$$

This is a bijection whose inverse is given by

$$(x, y) \mapsto t := \frac{y}{1 + x}.$$

The equation $x^2 + y^2 = z^2$ (Pythagorean theorem) has **infinitely** many solutions, contrasting with Fermat's Last Theorem.

Rational points on curves



Bachet-Mordell equation

Let $c \in \mathbb{Z}$ be non-zero, and consider the equation

$$y^2 - x^3 = c.$$

Bachet discovered that if $P = (x, y)$ is a rational point on the previous curve then so is

$$P' = \left(\frac{x^4 - 8cx}{4y^2}, \frac{x^6 + 20cx^3 - 8c^2}{8y^3} \right).$$

Brachet-Mordell equation

Example

Let $c = -2$ and consider

$$y^2 - x^3 = -2.$$

This curve contains the point $P = (3, 5)$.

$$P = (3, 5) \mapsto P' = \left(\frac{129}{100}, \frac{383}{1000} \right) \mapsto$$
$$P'' = \left(\frac{2340922881}{(7660)^2}, \frac{-113259286337279}{(7660)^3} \right) \mapsto \text{etc}$$

Fact: The sequence P, P', P'', \dots never repeats. Hence, for $c = -2$, the Bachet-Mordell equation has infinitely many rational solutions.

Bachet-Mordell equation

A natural question is, where does this construction come from?

Again from geometry!

Let $P = (x, y)$ be a point on $C : y^2 - x^3 = c$.

Then the tangent to C at P has slope $\frac{3x^2}{2y}$ so has equation

$$Y = y + \frac{3x^2}{2y}(X - x)$$

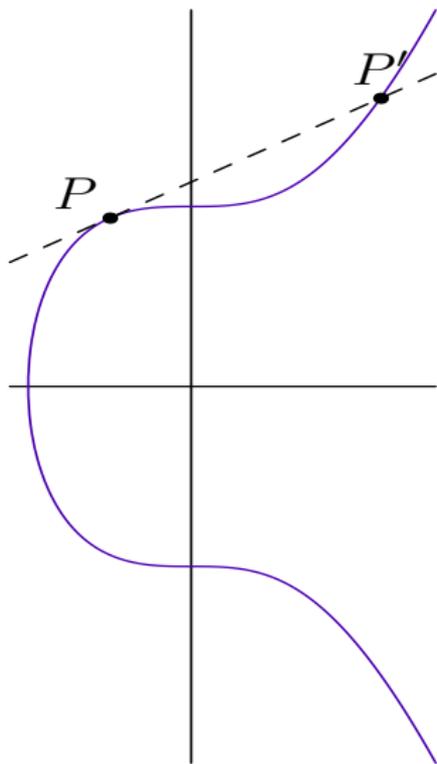
.

This tangent line L intersects C where

$$\left(y + \frac{3x^2}{2y}(X - x) \right)^2 - X^3 = c,$$

which is a cubic in X .

Bachet-Mordell equation



Bachet-Mordell equation

By expansion, one gets

$$X^3 - \frac{9x^4}{4y^2}X^2 + \text{lower terms} = 0.$$

This has x as a double root and the sum of the roots equals $\frac{9x^4}{4y^2}$. So the third root is given by

$$x' = \frac{9x^4}{4y^2} - 2x = \frac{9x^4 - 8xy^2}{4y^2} = \frac{x^4 + 8x(x^3 - y^2)}{4y^2} = \frac{x^4 - 8cx}{4y^2}$$

Now $P' = (x', y')$ where $y' = y + \frac{3x^2}{2y}(x' - y)$, hence

$$P' = \left(\frac{x^4 - 8cx}{4y^2}, \frac{x^6 + 20cx^3 - 8c^2}{8y^3} \right).$$

Bachet knew this construction in 1621!

Bachet-Mordell equation

Question: For which non-zero $c \in \mathbb{Z}$ does $C : y^2 - x^3 = c$ has infinitely many rational solutions?

Mordell proved this is the case for all $c \neq 1, 432$.

We will see that the set of rational points form a group.

For example,

$c = -2 \rightsquigarrow$ infinite cyclic group generated by $(3, 5)$ and $P' = -2P$

$c = 1 \rightsquigarrow C_6$

$c = 432 \rightsquigarrow C_3$

$c = 1358556 \rightsquigarrow \mathbb{Z}^6$ (Womack 2000)

The record in 2009 was \mathbb{Z}^{12} again by Womack.

Now it is \mathbb{Z}^{15} for a massive number c .

Bachet-Mordell equation

For $c = 432$, the Bachet-Mordell equation only has finitely many solutions. Here is a good reason for this :

Given a \mathbb{Q} -point (x, y) in $y^2 = x^3 - 432$ write

$$x = 12 \frac{c}{a+b} \quad y = 36 \frac{a-b}{a+b}$$

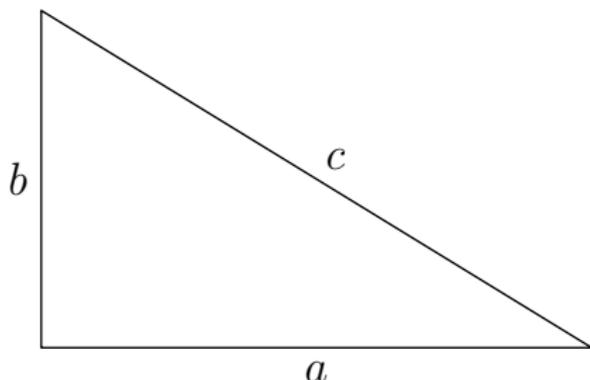
then we get $a^3 + b^3 = c^3$.

Conversely, setting $a = 36 + y$, $b = 36 - y$ and $c = 6x$ and dividing by 216, we recover the $y^2 = x^3 - 432$.

And so solving the FLT for $n = 3$ is equivalent to finding rational points on this plane cubic curve.

Congruent number curves

Is there a right triangle with **rational** sides and area 5?



For this, we need:

$$\frac{ab}{2} = 5 \quad \text{and} \quad a^2 + b^2 = c^2,$$

Congruent number curves

We need:

$$\frac{ab}{2} = 5 \quad \text{and} \quad a^2 + b^2 = c^2,$$

which implies that

$$ab = 10$$

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2 + 20}{4} = \left(\frac{c}{2}\right)^2 + 5$$

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \frac{c^2 - 20}{4} = \left(\frac{c}{2}\right)^2 - 5.$$

Let $x = \left(\frac{c}{2}\right)^2 \in \mathbb{Q}$. Then $x - 5$, x and $x + 5$ are three squares in arithmetic progression and $(x - 5)x(x + 5) = y^2$ with $y \in \mathbb{Q}$.

So (x, y) is a rational point on the curve

$$E_5 : y^2 = x^3 - 25x.$$

Congruent number curves

Definition

We say that n is a **congruent number** if a solution to the right triangle problem exists.

More generally, for $n \in \mathbb{N}$, let $E_n : y^2 = x^3 - n^2x$.

If n is a congruent number then there exists a point $(x, y) \in E_n(\mathbb{Q})$ such that $x = (\frac{c}{2})^2$ and $y \neq 0$.

Conversely, if $P = (x, y) \in E_n(\mathbb{Q})$, such that $y \neq 0$, it turns out that the x -coordinate of $2P$ is a square.

It turns out that n is a congruent number if and only if E_n has a \mathbb{Q} -rational point (x, y) with $y \neq 0$.

Congruent number curves

Let $E_5 : y^2 = x^3 - 25x$. The group of solutions is isomorphic to

$$E_5(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \simeq \langle(0, 0)\rangle \times \langle(5, 0)\rangle \times \langle(-4, 6)\rangle$$

Take $P = (-4, 6)$, then

$$2P = \left(\left(\frac{41}{12} \right)^2, \frac{-62279}{1728} \right).$$

Let $x = \left(\frac{41}{12}\right)^2$, then $x - 5 = \left(\frac{31}{12}\right)^2$ and $x + 5 = \left(\frac{49}{12}\right)^2$. Thus

$$c = \frac{41}{6}, \quad a + b = \frac{49}{6}, \quad a - b = \frac{31}{6},$$

which gives $a = \frac{20}{3}$ and $b = \frac{3}{2}$. We have $\frac{ab}{2} = \frac{60}{12} = 5$ as expected.

Bezout's theorem

Curves in the projective plane

Definition

Let $F \in K[X, Y, Z]$ be a homogeneous polynomial of degree d .
The **projective plane curve defined by F** is given by

$$\mathcal{C} := \{[x : y : z] \in \mathbf{P}^2(\overline{K}) : F(x, y, z) = 0\}.$$

In order to study \mathcal{C} sometimes need to move it under a linear change of coordinates to an isomorphic curve \mathcal{C}' which is better to work with. These transformations preserve lines.

Example

We already saw the following examples

- ▶ $L : 3X + Y + Z = 0$ (line).
- ▶ $\mathcal{C} : ZY - X^2 = 0$ (conic).
- ▶ $\mathcal{C} : Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$ (cubic).
- ▶ $\mathcal{C}_n : X^n + Y^n - Z^n = 0$ (the Fermat curve).

Bezout's theorem

Theorem (Weak Bezout)

Let K be an **infinite** field, and $F, G \in K[X, Y, Z]$ be two homogeneous polynomials of degree m and n respectively, **without** a common irreducible factor; and let

$$\mathcal{C}_F = \{[x : y : z] \in \mathbf{P}^2(K) : F(x, y, z) = 0\},$$

$$\mathcal{C}_G = \{[x : y : z] \in \mathbf{P}^2(K) : G(x, y, z) = 0\}.$$

Then the set $\mathcal{C}_F \cap \mathcal{C}_G$ is **finite**, and contains at most mn points.

Remark: The **bound** mn in the conclusion of Bezout's theorem is due to the fact that a polynomial of degree d in $K[x]$ **has at most** d **roots**. To obtain an **equality**, we must work over an **algebraically closed field** K and **count** all roots with **multiplicity**.

Bezout's theorem

Theorem (Strong Bezout)

Let K be an algebraically closed field, and $F, G \in K[X, Y, Z]$ two homogeneous polynomials of degree m and n respectively, **without** a common irreducible factor; and let

$$\mathcal{C}_F = \{[x : y : z] \in \mathbf{P}^2(K) : F(x, y, z) = 0\},$$

$$\mathcal{C}_G = \{[x : y : z] \in \mathbf{P}^2(K) : G(x, y, z) = 0\}.$$

Then the set $\mathcal{C}_F \cap \mathcal{C}_G$ is **finite**, and we have

$$\sum_{P \in \mathcal{C}_F \cap \mathcal{C}_G} I(P; \mathcal{C}_F, \mathcal{C}_G) = mn.$$

Corollary

The intersection of a **line** with a **cubic** contains three points with coordinates in \overline{K} counting multiplicities.

Elliptic curves

Singular curves

Definition

Let \mathcal{C}/K be a projective curve and P be a point on $\mathcal{C}(\overline{K})$.

We say that P is **singular** if

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Otherwise, we say that P is **non-singular** or **smooth**.

Example

The curve $Y^2Z - X^3 + X^2Z = 0$ has derivatives

$$\frac{\partial F}{\partial X} = -3X^2 - 2XZ, \quad \frac{\partial F}{\partial Y} = 2YZ, \quad \frac{\partial F}{\partial Z} = Y^2 + X^2$$

that all vanish at the point $P = [0 : 0 : 1]$. So P is a singular point.

Singular curves

Example

Consider the curve

$$\mathcal{C} : Y^2Z - X^3 + 2XZ^2 + 2Z^3 = 0.$$

$$\frac{\partial F}{\partial X} = -3X^2 + 2Z^2, \quad \frac{\partial F}{\partial Y} = 2YZ$$

$$\frac{\partial F}{\partial Z} = Y^2 + 4XZ + 6Z^2.$$

We saw the only point at infinity on this curve is $P = [0 : 1 : 0]$, which is non-singular since $\frac{\partial F}{\partial Z}(P) \neq 0$.

So if $P = [x : y : z] \neq [0 : 1 : 0]$ is singular, then $y = 0$ and $z \neq 0$. In this case, $\partial F / \partial Z = 2z(2x + 3z) = 0$, which implies that $2x = -3z \neq 0$. Hence $\partial F / \partial X \neq 0$, which is a contradiction.

So the curve is non-singular.

Weierstrass equations

Elliptic curves are a special kind of plane cubic curves, which are commonly described using Weierstrass equations.

Definition

An **elliptic curve** E defined over a field K is a **non-singular** plane cubic given by an equation of the form

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

where $a_1, a_2, a_3, a_4, a_6 \in K$. This is a **Weierstrass equation**.

The homogenisation of E is

$$Y^2Z + a_1XYZ + a_3YZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and its **unique** point at infinity is $\infty = [0 : 1 : 0]$.

Weierstrass equations

Example

(a) Bachet-Mordell equation: $E : y^2 = x^3 + c$, where $c \neq 0$

(b) The congruent number curve: $E_n : y^2 = x^3 - n^2x$, $n > 0$.

When $\text{char}(K) \neq 2, 3$ we can use a simplified Weierstrass model. Indeed, in this case we will assume E/K is given in the form

$$y^2 = x^3 + ax^2 + bx + c \quad \text{or}$$

$$y^2 = x^3 + Ax + B \quad (\text{short Weierstrass model})$$

where $a, b, c, A, B \in K$.

Weierstrass equations

We need a criterion for a Weierstrass model to be non-singular.

Let $f(x) = x^3 + ax^2 + bx + c$ with $a, b, c \in K$.

The **discriminant of f** is given by

$$\begin{aligned}\Delta_f &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\ &= [(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)]^2,\end{aligned}$$

where e_1, e_2, e_3 are the roots of f .

Definition

Let $E : y^2 = f(x)$ be a Weierstrass model, where

$$f(x) = x^3 + ax^2 + bx + c.$$

The **discriminant Δ_E** of E is defined $\Delta_E := 16\Delta_f$.

Weierstrass equations

Proposition

Let $E : y^2 = f(x)$ where $f(x) = x^3 + ax^2 + bx + c$, $a, b, c \in K$.
Then E is an elliptic curve if and only if $\Delta_E \neq 0$.

Proof.

Let $g(x, y) = y^2 - f(x)$, and $P = (x, y)$ be a point in $E(\overline{K})$.
Recall that $\text{char}(K) \neq 2$. Then, by definition

$$E \text{ is singular at } P \iff \begin{cases} \frac{\partial g}{\partial x} = -f'(x) = 0 \\ \frac{\partial g}{\partial y} = 2y = 0 \end{cases} \iff f(x) = f'(x) = 0.$$
$$\iff f \text{ has a double root} \iff \Delta_E = 16\Delta_f = 0.$$

□

Corollary

A short Weierstrass equation $E : y^2 = x^3 + ax + b$ is an elliptic curve $\iff \Delta_E = 16(-4a^3 - 27b^2) \neq 0$.

Weierstrass equations

Let E be an elliptic curve over K given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6.$$

Let K' be a field containing K and let $E(K')$ be the set of (projective) K' -**rational points** of E .

We know there is only one point at infinity $\infty = [0, 1, 0]$, therefore we can write $E(K')$ as the union

$$\{(x, y) \in K'^2 : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}.$$

Example

Let $E : y^2 = x^3 - 2$. The set of \mathbb{Q} -rational points $E(\mathbb{Q})$ contains $P = (3, 5)$. We have the natural inclusions

$$\{P, \infty\} \subset E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C}).$$

Elliptic curves over \mathbb{R}

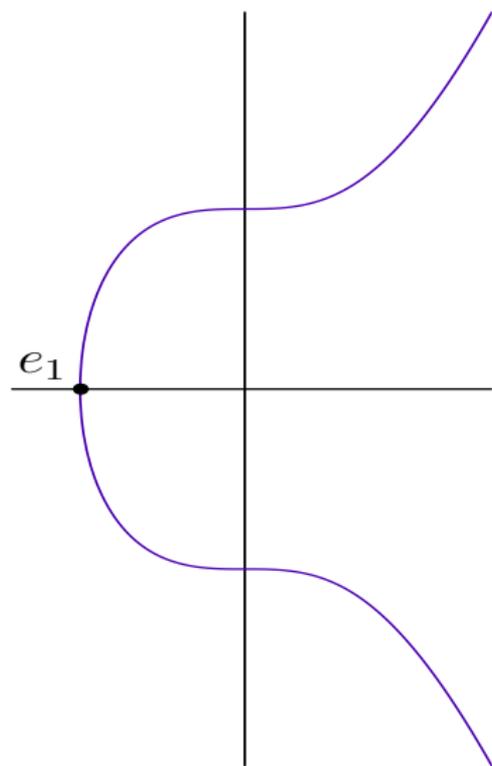


Figure: Case 1: $K \subset \mathbb{R}$, and $\Delta_E < 0 \Leftrightarrow e_1$ is real, $e_2 = \bar{e}_3 \notin \mathbb{R}$.

Elliptic curves over \mathbb{R}

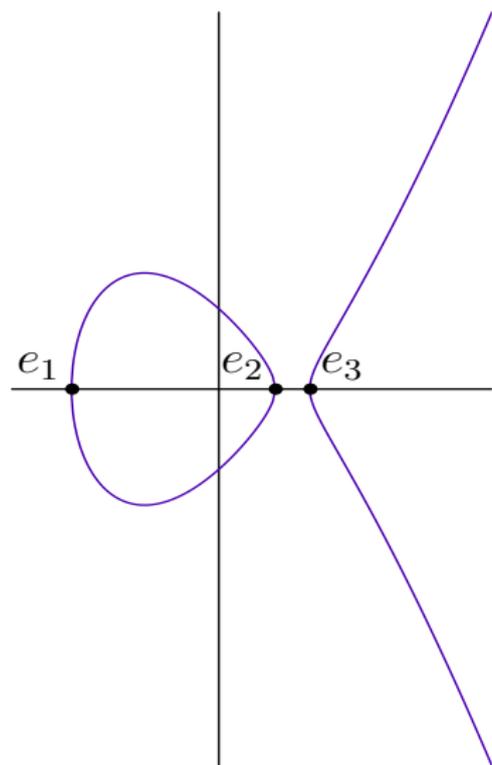


Figure: Case 2: $K \subset \mathbb{R}$, and $\Delta_E > 0 \Leftrightarrow e_1, e_2, e_3 \in \mathbb{R}$.

The group law

To define the group structure, we need the set of \overline{K} -rational points:

$$E(\overline{K}) = \{(x, y) \in \overline{K}^2 : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}.$$

Bezout's Theorem: L be a line in $\mathbf{P}^2(\overline{K}) \implies L \cap E$ has **three** points P, Q and R **counted with multiplicity**.

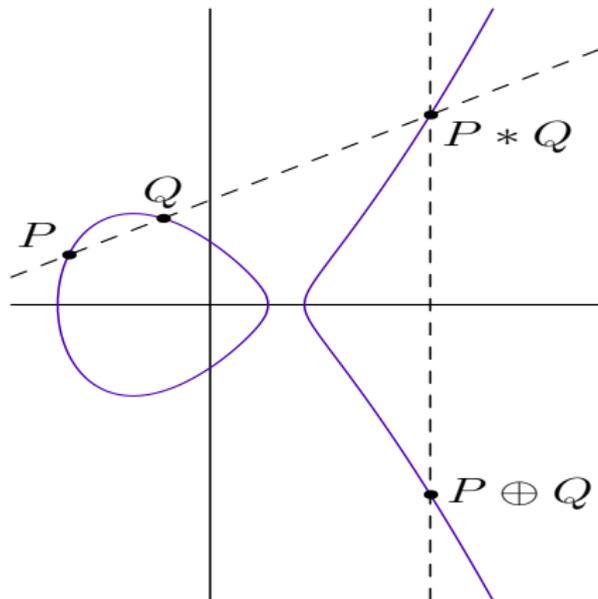
Definition

(1) Given $P, Q \in E(\overline{K})$, we denote **third** point of intersection of the line \overline{PQ} with E by $P * Q$.

(2) The **addition law** \oplus on $E(\overline{K})$ is defined as follows: For $P, Q \in E(\overline{K})$, set:

$$P \oplus Q = (P * Q) * \infty.$$

The group law

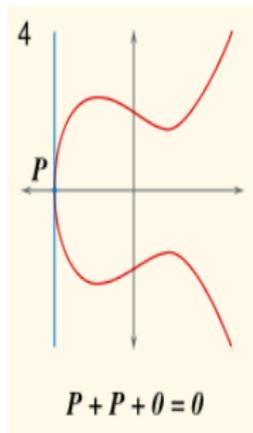
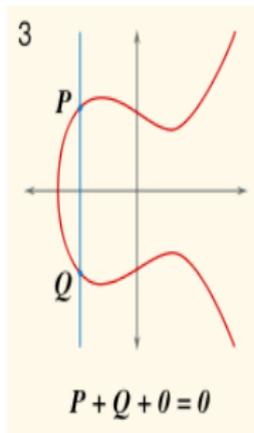
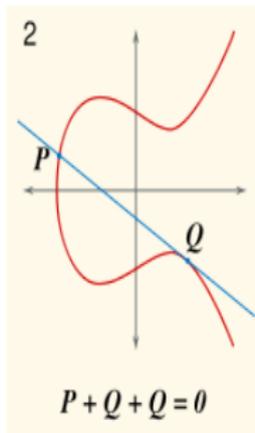
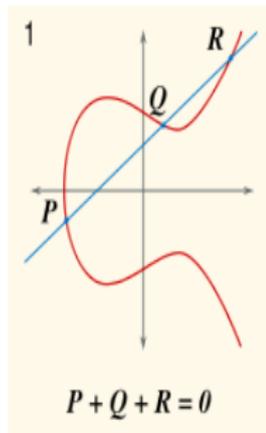


Theorem

Let E be an elliptic curve defined over a field K . Then, $E(\overline{K})$ is an abelian group under the operation \oplus , with identity $\infty = [0 : 1 : 0]$.

Alternative definition of the group law

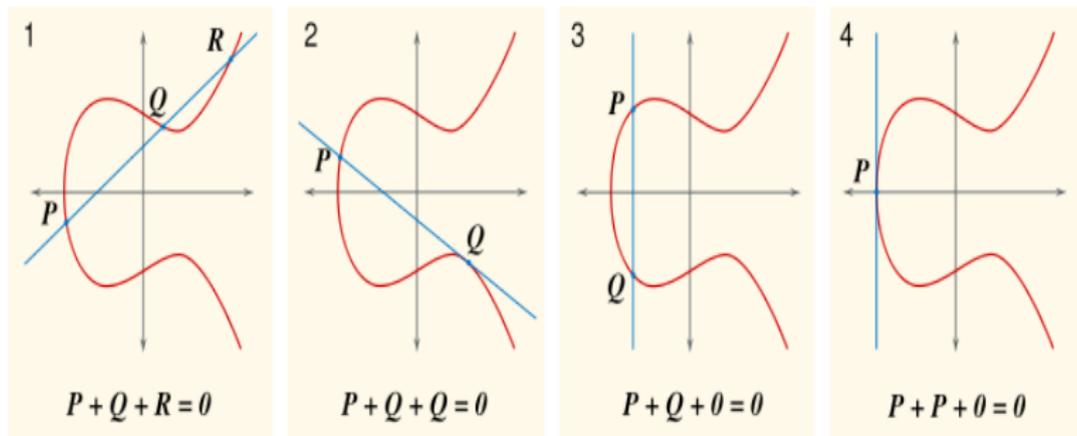
$P \oplus Q \oplus R = 0 (= \infty) \iff P, Q, R$ are the three points of intersection of a line L with E (counted with multiplicities).



Definition of the group law

Proposition (Points of order 2)

Let $E : y^2 = x^3 + ax + b = f(x)$ be an elliptic curve over K . Then $P = (x, y)$ is a point of order 2, i.e., $P \neq \infty$ and $P \oplus P = \infty$, if and only if x is a root of the cubic $f(x)$.



Computing with the group law

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over K .

Given $P_1, P_2 \in E(\overline{K})$, how do we compute $P_1 \oplus P_2$ **explicitly**?

(1) If $P_1 = \infty$ then $P_1 \oplus P_2 = P_2$; if $P_2 = \infty$, then $P_1 \oplus P_2 = P_1$.

Assume that $P_1, P_2 \neq \infty$, and write $P_i = (x_i, y_i)$.

(2) If $x_1 = x_2$ and $y_1 = -y_2$ then $P_1 \oplus P_2 = \infty$.

(3) In all other cases, we have

$$P_1 \oplus P_2 = (x_3, y_3) = (m^2 - x_1 - x_2, -y_1 - m(x_3 - x_1)).$$

where m (the slope) is given by

$$m = \begin{cases} \frac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2 \text{ and } y_i \neq 0 \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{otherwise.} \end{cases}$$

Corollary

If $K \subseteq K' \subseteq \overline{K}$ is a subfield, then $E(K')$ is a subgroup of $E(\overline{K})$.

The Mordell-Weil theorem

The Mordell-Weil theorem

Theorem (Mordell-Weil)

Let E/\mathbb{Q} be an elliptic curve.

Then the abelian group $E(\mathbb{Q})$ is finitely generated, i.e.,

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}},$$

where $r \geq 0$ is the **rank** of $E(\mathbb{Q})$, and $E(\mathbb{Q})_{\text{tors}}$ is finite.

Question: Does this mean that in practice we can determine $E(\mathbb{Q})$? By “determine” we mean find the abstract group structure, i.e. find the structure of $E(\mathbb{Q})_{\text{tors}}$ and r .

We will start by studying the torsion part $E(\mathbb{Q})_{\text{tors}}$.

Points of finite order

Points of finite order

Let $n > 0$ be an integer.

Let K be a field such that $\text{char}(K) = 0$ or $\text{char}(K) = p$ and $p \nmid n$.

Let E be an elliptic curve defined over K .

The multiplication-by- n map

$$\begin{aligned} [n] : E(\overline{K}) &\rightarrow E(\overline{K}) \\ P &\mapsto nP \end{aligned}$$

is a surjective homomorphism. The **n -torsion subgroup** of E is

$$E[n] := \ker([n]) = \{P \in E(\overline{K}) : nP = 0\}.$$

Proposition

Assume $\text{char}(K) = 0$ or $\text{char}(K) = p$ and $p \nmid n$. Then

$$\#E[n] = \#\ker([n]) = n^2$$

and

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Points of finite order

Remark

In the definition of $E[n]$ we use the **algebraic closure** \overline{K} of K .

Otherwise, $[n]$ would **no longer be surjective**, and conclusion of the Proposition would be **wrong**.

If $K \subseteq K' \subseteq \overline{K}$ (subfields), write $E(K')[n]$ for the subset of $E[n]$ which consists of the n -torsion points with coordinates in K' .

$E(K')[n]$ is a subgroup of $E[n]$.

Points of finite order

Given E/\mathbb{Q} we can view E as an elliptic curve over \mathbb{C} .

The structure of the abelian group $E(\mathbb{C})$ is particularly simple.

Indeed, there is a discrete lattice $\Lambda \subset \mathbb{C}$ of rank 2 (that is, as an abelian group $\Lambda \simeq \mathbb{Z}^2$) depending on E , and an isomorphism

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda.$$

By the n -torsion of $E(\mathbb{C})$ we mean the subgroup

$$E[n] = \{Q \in E(\mathbb{C}) : nQ = 0\}.$$

It follows that

$$E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2,$$

which can be viewed as 2-dimensional $\mathbb{Z}/n\mathbb{Z}$ -module.

We are left with showing that the points in $E[n]$ all have coordinates in $\overline{\mathbb{Q}}$ since E is defined over \mathbb{Q} .

Points of finite order

Example

Assume $\text{char}(K) \neq 2$, and let E be given by an equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_i \in \overline{K}.$$

From the proposition we have

$$E[2] = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

and we know that 2-torsion points have $y = 0$, therefore

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

In particular, writing $T_i = (e_i, 0)$ we have $T_3 = T_1 + T_2$.

Points of finite order

Example

Assume that $\text{char}(K) \neq 2, 3$, and let E be given by

$$E : y^2 = x^3 + Ax + B.$$

Let $P = (x, y) \in E(\overline{K})$. Then

$$\begin{aligned} P \text{ has order } 3 &\Leftrightarrow 3P = 0 \Leftrightarrow 2P = -P \\ &\Rightarrow x(2P) = x(-P) = x(P) = x \\ &\Rightarrow 3x^4 + 6Ax^2 + 12Bx - A^2 = 0, \end{aligned}$$

which has a non-zero discriminant, hence no repeated roots. Therefore $\#E[3] = 9$ (each root gives two opposite points in $E(\overline{K})$, plus the zero element) which is consistent with

$$E[3] = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$$

as predicted by the proposition.

Points of finite order

Example

(a) The curve $E_1 : y^2 = x^3 - 2$ has no 2-torsion point defined over \mathbb{Q} since $x^3 = 2$ has no solutions in \mathbb{Q} , so $E_1(\mathbb{Q})[2] = \{\infty\}$.

(b) For the curve $E_2 : y^2 = x(x^2 + 1)$, we have

$$E_2(\mathbb{Q})[2] = \{\infty, (0, 0)\}$$

and

$$E(\mathbb{Q}(i))[2] = \{\infty, (0, 0), (\pm i, 0)\}.$$

(c) The congruent number curves $E_n : y^2 = x(x^2 - n^2)$ have all the 2-torsion points defined over \mathbb{Q} :

$$E(\mathbb{Q})[2] = \{\infty, (0, 0), (n, 0), (-n, 0)\}.$$

Torsion subgroup over \mathbb{Q}

Torsion subgroup: The Lutz-Nagell Theorem

We have an easy process to compute points of order 2.

How about points of finite order > 2 ?

Theorem (Lutz-Nagell)

Let E over \mathbb{Q} be an elliptic curve given by an **integral** short Weierstrass equation

$$Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Z}, \quad \Delta = -4A^3 - 27B^2$$

If $P = (x, y) \in E(\mathbb{Q})$ has **finite order**, then

1. the coordinates $x, y \in \mathbb{Z}$, and
2. either $y = 0$ or $y^2 \mid \Delta_E$.

Corollary

The torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is finite.

Torsion subgroup: The Lutz-Nagell Theorem

The Batchet-Mordell equation provides an example of a point with integer coordinates and infinite order :

$$E : Y^2 = X^3 - 2 \quad P = (3, 5)$$

$$2P = \left(\frac{3 \cdot 43}{2^2 \cdot 5^2}, -\frac{383}{2^3 \cdot 5^3} \right),$$

$$3P = \left(\frac{73 \cdot 2251}{3^4 \cdot 19^2}, -\frac{5 \cdot 43 \cdot 71 \cdot 4339}{3^6 \cdot 19^3} \right),$$

$$4P = \left(\frac{3 \cdot 11 \cdot 43 \cdot 59 \cdot 27961}{2^4 \cdot 5^2 \cdot 383^2}, \frac{23 \cdot 911 \cdot 48383 \cdot 111721}{2^6 \cdot 5^3 \cdot 383^3} \right),$$

$$5P = \left(\frac{3 \cdot 241 \cdot 49681 \cdot 8556001}{29^2 \cdot 211^2 \cdot 2069^2}, \frac{5^2 \cdot 179 \cdot 269 \cdot 39239 \cdot 63901 \cdot 1510679}{29^3 \cdot 211^3 \cdot 2069^3} \right),$$

One can show that $2P, 3P, 4P, \dots$ have **denominators** more and more **highly divisible by p** .

Torsion subgroup: The Lutz-Nagell Theorem

Example

Consider $E : Y^2 = X^3 + 4$ satisfying $\Delta = -27(4)^2 = -3(12)^2$.

If $P = (x, y)$ has finite order then, either $y = 0$ or $|y| \mid 12$, hence

$$y \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

$ y $	0	1	2	3	4	6	12
y^2	0	1	4	9	16	36	144
$y^2 - 4$	-4	-3	0	5	12	32	140
x	-	-	0	-	-	-	-

So the only two possibilities are $P = (0, 2)$ or $-P = (0, -2)$.

One checks $2P = -P$ so P has order 3 (the line $y = 2$ intersects E at P with multiplicity 3, so $P + P + P = 0$).

Torsion subgroup: The Lutz-Nagell theorem

Example

Let E be given by $Y^2 = X^3 + 8$, with $\Delta = -27 \cdot 8^2 = -3(24)^2$.

If $P = (x, y)$ has finite order then $y = 0$ or $|y| \mid 24$.

$ y $	0	1	2	3	4	6	12	24
y^2	0	1	4	9	16	36	144	576
$y^2 - 8$	-8	-7	-4	1	8	28	136	568
x	-2	-	-	1	2	-	-	-

For $y = 0$, one gets $T = (-2, 0)$ which has order 2.

For $y = 3$, we get $P = (1, 3)$ satisfying $2P = (-7/4, -13/8)$.

Since $2P$ is **not** integral, it **cannot** have finite order.

For $y = 4$, we get $Q = (2, 4)$ yielding $2Q = (-7/4, 13/8) = -2P$, hence Q is **not** of finite order..