Elliptic curves

Lecture 2

19th April 2024

Recall: Diophantine equation

$$C : f(x_1, \ldots, x_r) = 0 \qquad (*)$$

$$f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r], \quad \deg f = n$$

Goal: Understand $C(R) = \{(x_1, \ldots, x_r) \in R^r \mid (*)\}$

$R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$

$r = 1$, any n: easy (finite check)

$r = 2$, $n = 1$: $\mathbb{Q}$ trivial, $\mathbb{Z}$: Bezout's lemma

$r = 2$, $n = 2$: Conics

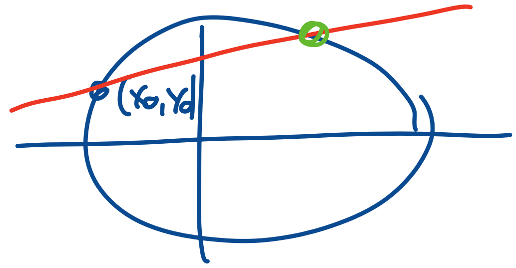
$C(\mathbb{Q}) \neq \emptyset$? local-to-global princible

If $(x_0, y_0) \in C(\mathbb{Q})$ we can find all points in $C(\mathbb{Q})$.

(HW 1, Ex 2)

<u>Idea</u>: If $f(x_0, y_0) = 0$ consider a line through (x_0, y_0) with slope $t \in \mathbb{Q}$

This meets the conic in another point.



$y = t \cdot (x - x_0) + y_0$

Consider $f(x, t(x-x_0)+y_0)$ and factor it $\overset{\parallel}{(x-x_0)(a(t)x+b(t))}$.

Then $\left(-\frac{b(t)}{a(t)}, t\left(\frac{-b(t)}{a(t)} - x_0\right) + y_0\right) \in C(\mathbb{Q})$.

Notice: $a(t), b(t) \in \mathbb{Q}$

(vertical lines need to be considered seperately)

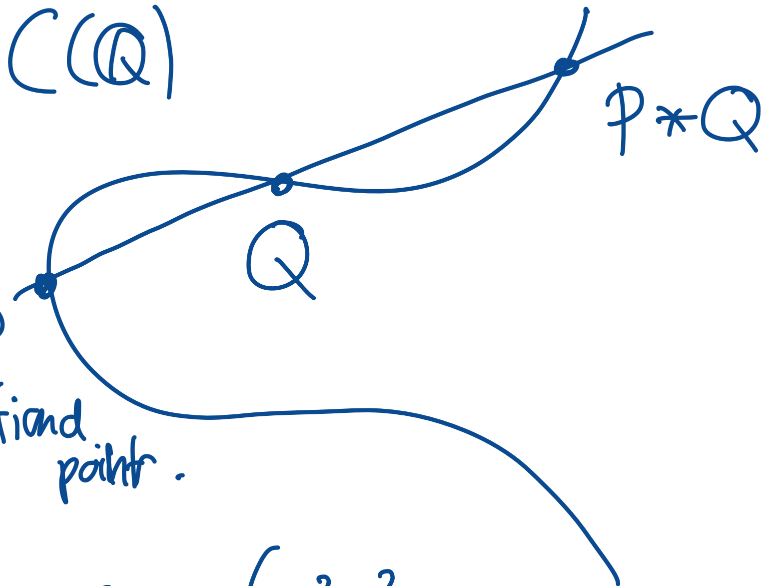
This gives indeed all points in $C(\mathbb{Q})$, since for any $(x_1, y_1) \in C(\mathbb{Q})$ the line between (x_0, y_0) and (x_1, y_1) has a rational slope (or $x_0 = x_1$).

$r=2,\ n=3$: cubic curves

C:

$$f(x,y) = ax^3 + bx^2y + \dots + hx + iy + j = 0$$

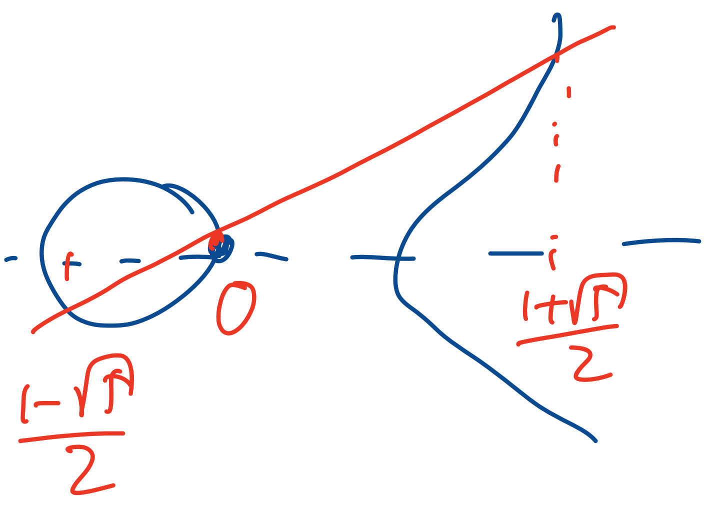
Having one $(x_0, y_0) \in C(\mathbb{Q})$ is now not enough to create new rational points.



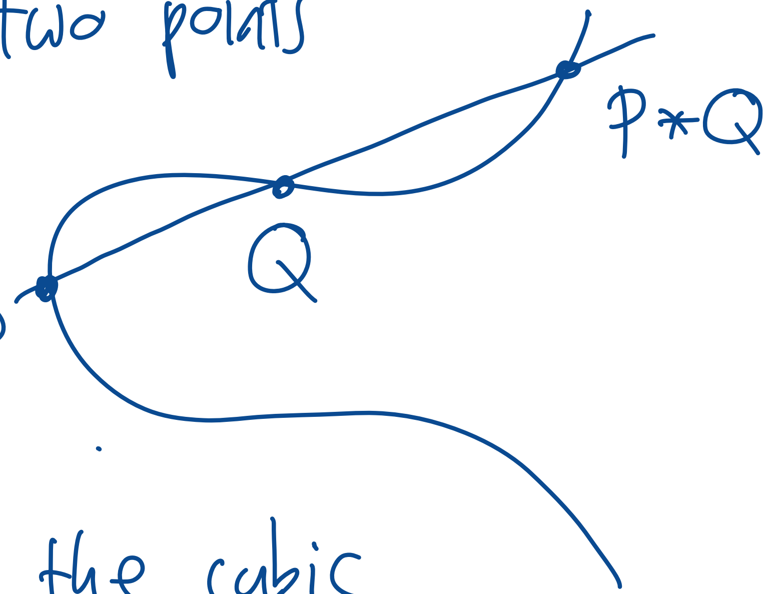
Example: C: $y = x^3 - x$ $\left(x^2 = x^3 - x \iff x=0 \vee x^2-x-1=0 \right)$

$(0,0) \in C(\mathbb{Q})$. The line $y=x$ intersects the curve in $\left(\frac{1-\sqrt{5}}{2}, \dots\right)$ $\mathbb{Q} \not\ni$

and $\left(\frac{1+\sqrt{5}}{2}, \dots\right)$

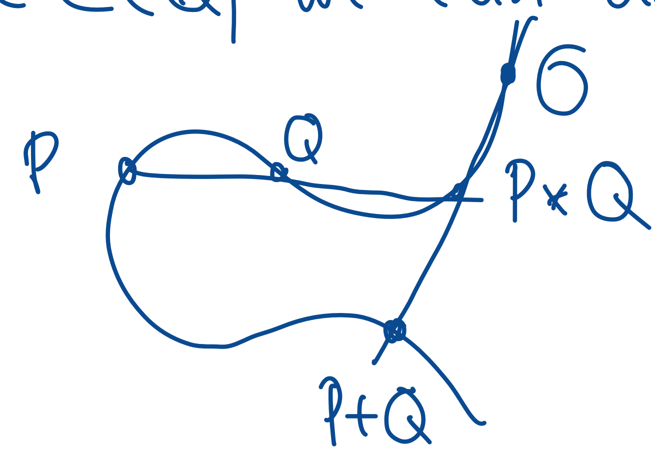


But if one has two points $P, Q \in C(\mathbb{Q})$ then the line between them has a rational slope and intersects the cubic in another point $P * Q$.



product? No neutral element.

But if $\exists\, O \in C(\mathbb{Q})$ we can define $P+Q$ as $O * (P * Q)$



Elliptic curve: non-singular (projective-) plane cubic curve with at least one $\mathbb{Q}$-pt. O

$\rightsquigarrow$ can always bring it in the form $y^2 = x^3 + Ax + B$

Higher cases?

We can also consider the curves over $\mathbb{C}$

$$C/\mathbb{R} \qquad C/\mathbb{C}$$

$\uparrow$ curve $\qquad$ $\uparrow$ surface over $\mathbb{R}$

genus of surface $C(\mathbb{C})$: $r=2$, deg $1,2$

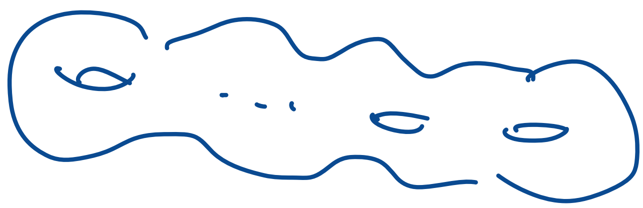
genus=0

$r=2$, deg $n=3,(4)$

genus=1

$n\geq 4$

higher genus



Thm (Faltings)

A curve C of genus ≥ 2 has only finitely many $\mathbb{Q}$-pts.

Back to elliptic curves:

Example of explicit addition

Consider the curve

$$E: y^2 = x^3 + c \qquad c \in \mathbb{Z}$$

You can check by direct calculation that if $(x,y) \in E(\mathbb{Q})$ then

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^2} \right) \in E(\mathbb{Q})$$

(Bachet's duplication formula)

For example, $c = -2$, $E: y^2 = x^3 - 2$

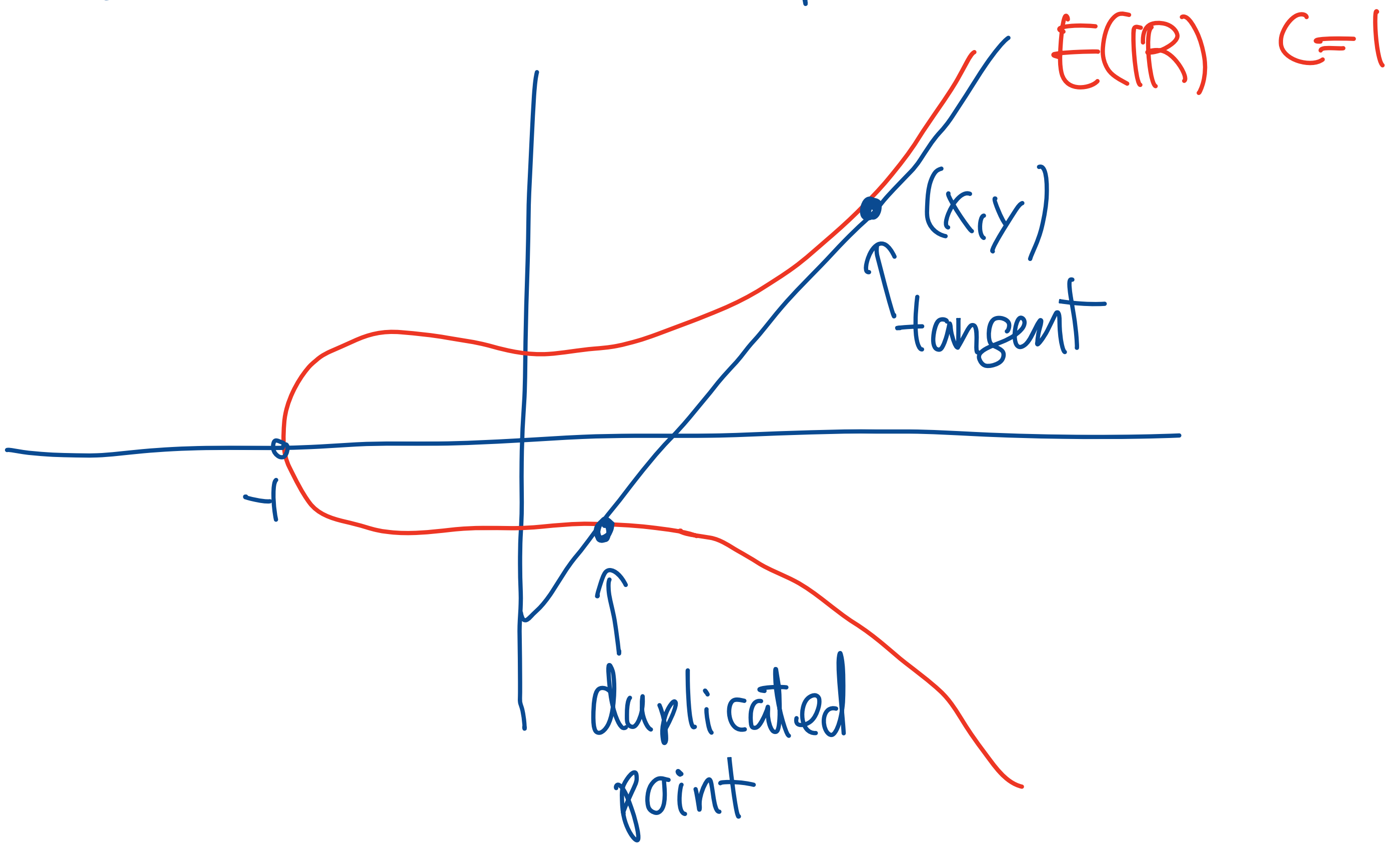
then $(3, \pm 5) \in E(\mathbb{Q})$

actually only integer solution

(for any c just finitely many)

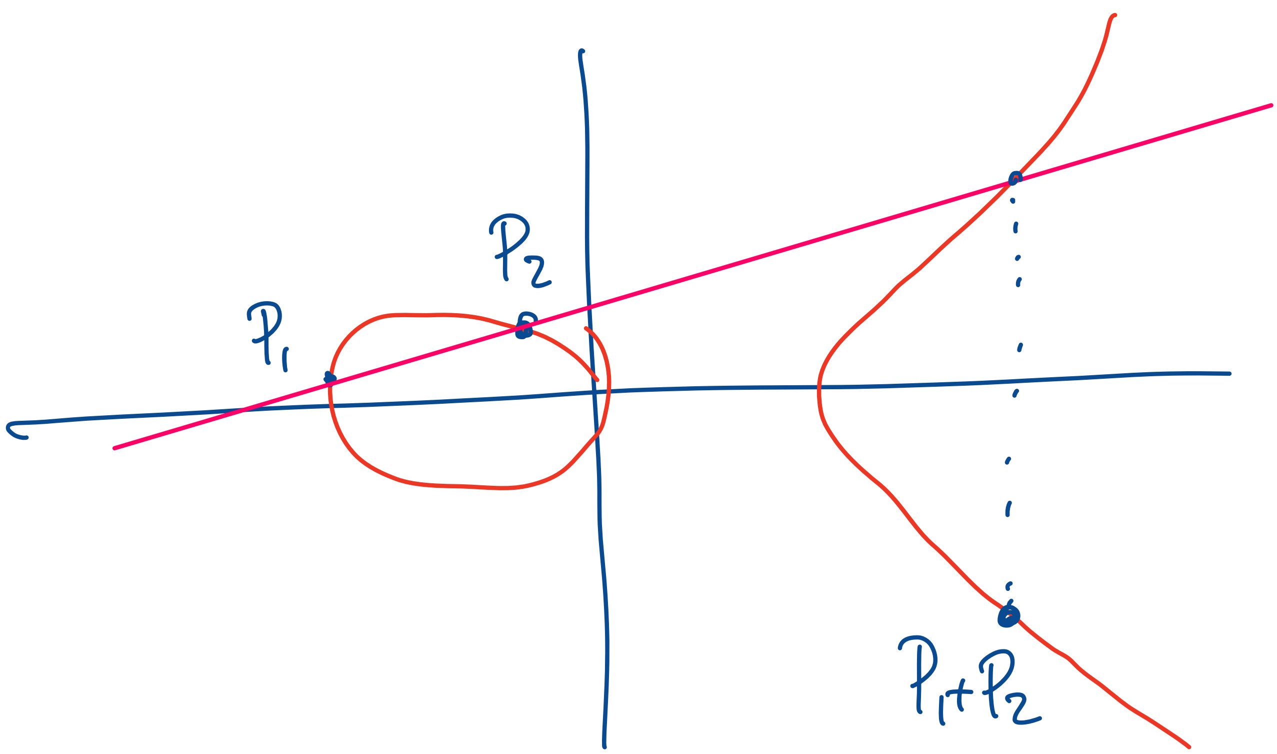
$$\rightsquigarrow \left(\frac{129}{10^2}, -\frac{383}{10^3} \right)$$

The duplication formula has a geometric interpretation:



This is just a special case of the group structure of an elliptic curve. In general we can take two points $P_1, P_2 \in E(\mathbb{Q})$ and consider the line between these two (In the special case $P_1 = P_2$ this line is the tangent).

This line intersects the curve in a third point (possibly the point at infinity). We then define $P_1 + P_2$ as this third point mirrored at the x-axis.



We will show: If $P_1, P_2 \in E(\mathbb{Q})$ then $P_1 + P_2 \in E(\mathbb{Q})$ and $E(\mathbb{Q})$ is a group with "+" and neutral element $\mathcal{O}$ = point at infinity.

One of the main goals is to show the following:

<u>Theorem</u> (Mordell 1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

$$\Rightarrow \quad E(\mathbb{Q}) = \underbrace{\overset{\text{elements of finite order}}{E(\mathbb{Q})_{\text{torsion}}}}_{\text{understood}} \oplus \mathbb{Z}^{\overset{\text{rank of } E}{r}}$$

not understood

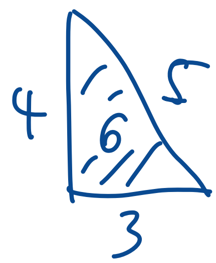
Birch & Swinnerton-Dyer conjecture

Congruent number problem

$n \geq 1$ is called a congruent number if there exists a right triangle with rational sides and whose area equals n.

Q: Which numbers n are congruent?

6 is congruent



<u>Proposition</u> $n \geq 0$ is congruent iff the curve E $y^2 = x^3 - n^2 x$ has a point (x,y) with $x, y \in E(\mathbb{Q})$ and $y \neq 0$.

One can show: If $(x,0) \in E(\mathbb{Q})$ then $(x,0)$ is a torsion pt.

$\Longrightarrow$ $(x,y) \in E(\mathbb{Q})$ with $y \neq 0 \Longleftrightarrow$ rank of $E > 0$

Conjecture (Birch & Swinnerton-Dyer) (BSD Conj)

"rank of elliptic curve"

$\parallel$

"order of zero of Hasse-Weil L-function $L(E,s)$ at $s=1$"

Roughly Let $N_p = \# E(\mathbb{Z}/p\mathbb{Z})$ and set $a_p = p+1-N_p$

$$L(E,s) \underset{\text{not exact}}{\overset{\text{"}\,\text{"}}{=}} \prod_p \frac{1}{1-a_p p^{-s}+p\,p^{-2s}}$$

Theorem (Tunnell) (n odd)

(odd) even

n is a congruent number

$$\Longleftrightarrow 2\underbrace{\#\{(x,y,z)\in\mathbb{Z}^3 \mid n = \overset{8}{2x^2} + \overset{2}{y^2} + \overset{64}{32z^2}\}}_{A_n}$$

$\Uparrow$ BSD Conj.

$\parallel$

$$\underbrace{\#\{(x,y,z)\in\mathbb{Z}^3 \mid n = \overset{8}{2x^2} + \overset{2}{y^2} + \overset{16}{8z^2}\}}_{B_n}$$

Example: $2A_5 = B_5 = 0$