CTNT 2024

Connecticut Summer School in Number Theory

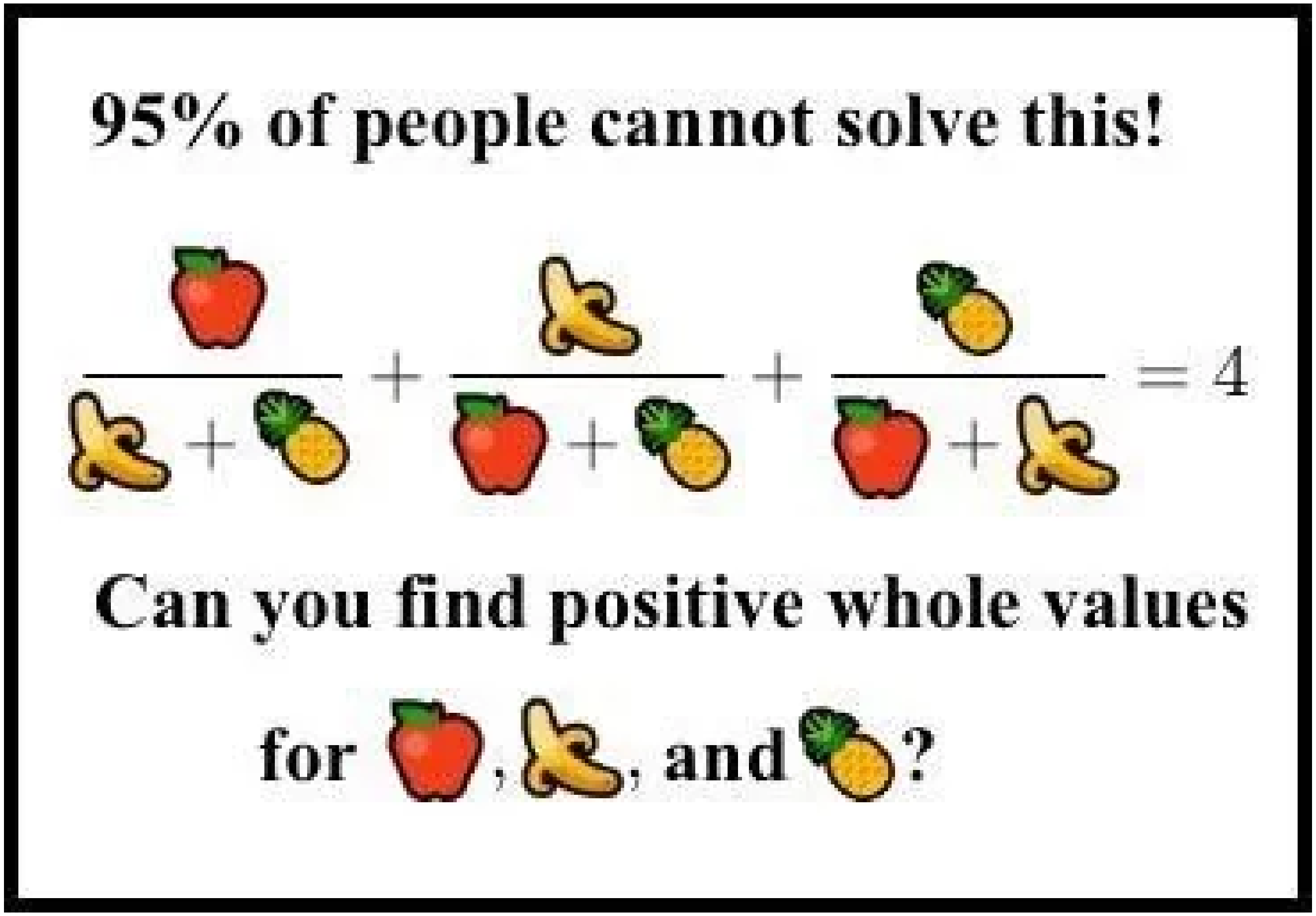
Introduction to Elliptic Curves

Álvaro Lozano-Robledo
(University of Connecticut)

Lecture 2

Models for Elliptic Curves

My goal: make you part of the 5%!



Not Easy!

Here is the simplest solution:

apple = 154476802108746166441951315019919837485664325669565431700026634898253202035277999

banana = 36875131794129999827197811565225474825492979968971970996283137471637224634055579

pineapple = 4373612677928697257861252602371390152816537558161613618621437993378423467772036

$$\begin{cases} x = \text{Apples} \\ y = \text{Bananas} \\ z = \text{Pineapples} \end{cases}$$

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$$

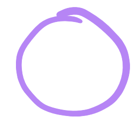
$$\Rightarrow \quad x(x+y)(x+z) + y(x+y)(y+z)$$
$$+ z(x+z)(y+z) = 4(x+y)(x+z)(y+z)$$

Q. Is this an elliptic curve??

DEFINITION

An elliptic curve over a field F is a smooth projective curve of genus 1 with at least one point defined over F.

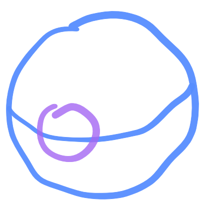
"F-rational"



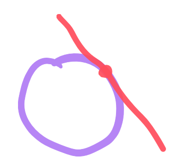
EX. affine: $x^2+y^2=1$

projective: $X^2+Y^2=Z^2$

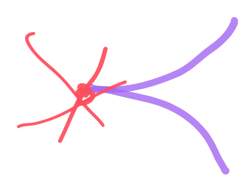
$$\begin{cases} x = \dfrac{X}{Z} \\ y = \dfrac{Y}{Z} \end{cases}$$



EX smooth: $x^2+y^2=1$



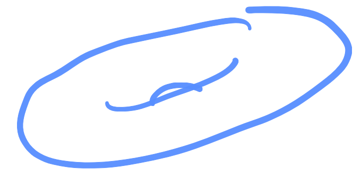
singular: $y^2=x^3$



EX genus 0 : $x^2+y^2=1$

genus 1 : $y^2=x^3+1$

$y^2=x^4+1$



EX no points over $\mathbb{Q}$: $x^2+y^2=-1$

points over $\mathbb{Q}$: $x^2+y^2=1$

GOOD NEWS/FACT:

A (projective) smooth cubic curve w/ at least one point is an elliptic curve!

Ex. $X(X+Y)(X+Z) + Y(X+Y)(Y+Z)$

$+ Z(X+Z)(Y+Z) = 4(X+Y)(X+Z)(Y+Z)$

$x = \frac{X}{Z}$

$y = \frac{Y}{Z}$

Affine: $x(x+y)(x+1) + y(x+y)(y+1)$

$+ (x+1)(y+1) = 4(x+y)(x+1)(y+1)$

- is a non-singular cubic (projectively!)
- it has a $\mathbb{Q}$-rational point! (FIND ONE!)

$\mathbb{Q}$-point

$[1, -1, 1]$

it's an elliptic curve!

Ex. $x^3+y^3=1$ $\qquad$ $x^3+y^3=1729$

$$y^2=x^3+1$$

$$y^2=x(x+1)(x+2)$$

are also examples of elliptic curves.

MORE GOOD NEWS:

PROPOSITION. Let F be a field and let E/F be an elliptic curve, given by $f(u,v)=0$. Then, there is an invertible change of variables such that E can be given by an equation of the form:

Weierstrass model.

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

for some $a_i\in F$. Moreover, if $\mathrm{char}(F)\neq 2,3$, then a model can be found of the form:

$$E:\ y^2=x^3+Ax+B,\qquad A,B\in F.$$

Short W-model

NOTE.

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

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

$$y^2 = x^3 + Ax + B$$

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

and $\mathcal{O} = [0,1,0]$ belongs to the (proj) curve.

Ex. Let $d \neq 0$.

$$u^3 + v^3 = d \quad \leftrightsquigarrow \quad y^2 + 9dy = x^3 - 27d^2$$

$$\psi(u,v) = \left(\frac{3d}{u+v} \, , \, -\frac{9dv}{u+v} \right)$$

Ex.

$$x(x+y)(x+1) + y(x+y)(y+1)$$
$$+ (x+1)(y+1) = 4(x+y)(x+1)(y+1)$$

$$y^2 + xy + y = x^3 - 234x + 1352$$

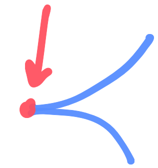
$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

(a Weierstrass model)

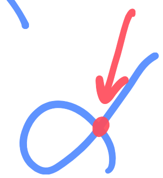
$E: y^2 = x^3 + Ax + B$

(a (short) Weierstrass model)

$y^2 = x^3$



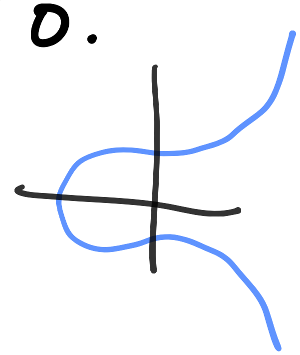
$y^2 = x^3 + x^2$
$= x^2(x-1)$

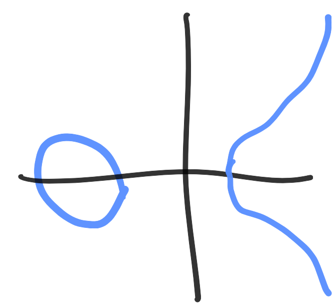


Even more good news: Let

$$\Delta_E = -16(4A^3 + 27B^2)$$ (the discriminant)

Then E is non-singular $\iff \Delta_E \neq 0$.





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

Let $j(E) = -1728 \dfrac{(4A)^3}{\Delta_E}$ (the j-invariant)

then $E \cong_{\bar{F}} E'$ if and only if

$$j(E) = j(E').$$

$y^2 = x^3 + 1 \ /\mathbb{Q}$

$y^2 = x^3 + 5^3 \ /\mathbb{Q}$

$\cong_{\mathbb{Q}(\sqrt{5})}$

(i.e., the j-invariant classifies elliptic curves up to isomorphism)

Note. There is an elliptic curve with $j(E) = j_0$ for <u>any</u> $j_0 \in F$.

- $j_0 = 0$, $y^2 + y = x^3$, $\Delta = -27$
- $j_0 = 1728$, $y^2 = x^3 + x$, $\Delta = -64$
- $j_0 \neq 0, 1728$

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3}$$

Note. We are interested in:

E/F any field!

$E/\mathbb{Q}$ $E/F(t)$

$E/\mathbb{C}$ $\vdots$

$E/\mathbb{F}_p$ $E/\mathbb{F}_p(t)$

Shafarevich

$E/\mathbb{F}_q$

$E/\mathbb{C}$

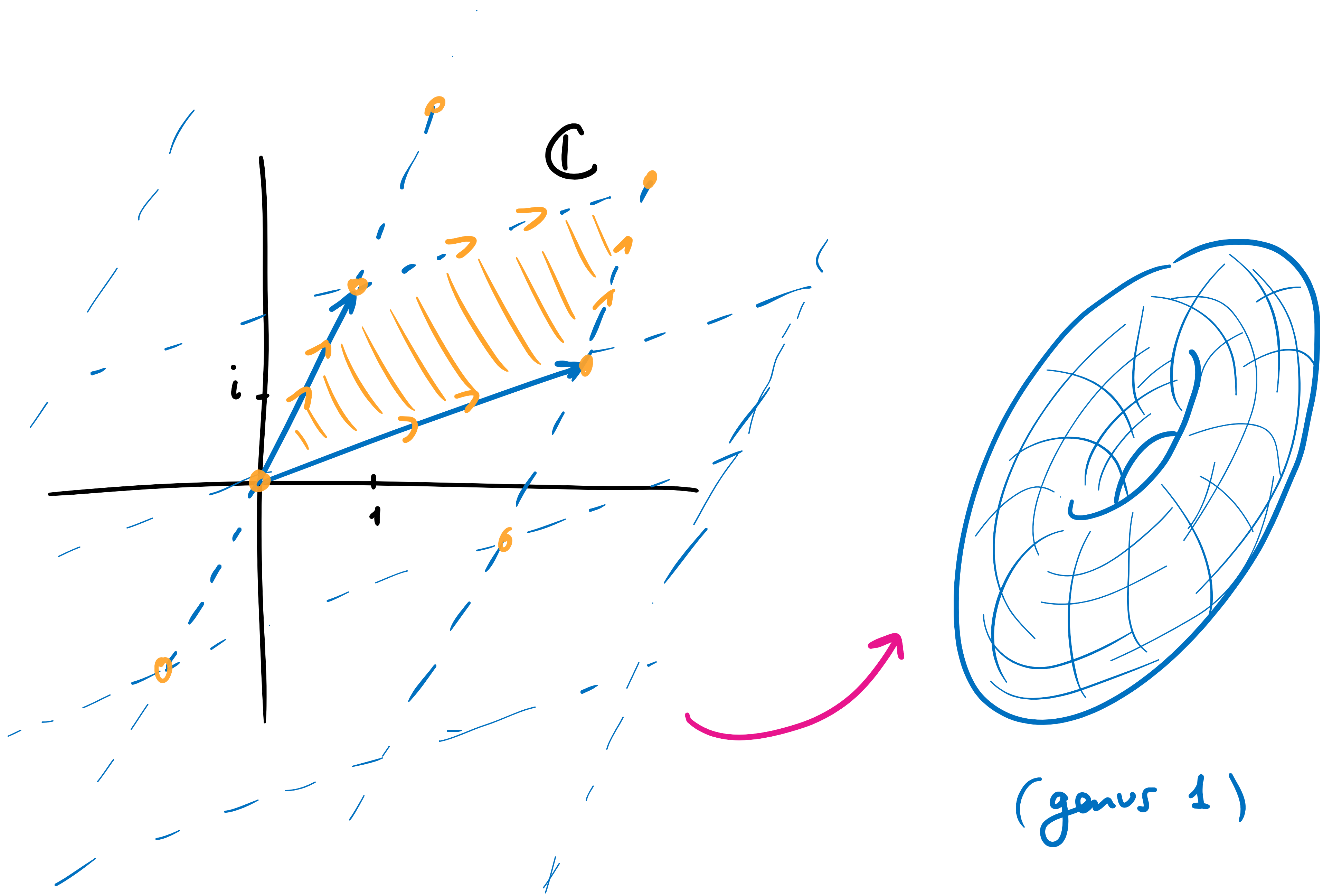
Theorem. Let $E/\mathbb{C}$ be an elliptic curve. Then there is a lattice $\Lambda \subseteq \mathbb{C}$ s.t.

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$$

$[p)$ $[p]$ $\rightsquigarrow E[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$

and, viceversa, if $\Lambda \subseteq \mathbb{C}$ is a lattice, there is $E/\mathbb{C}$ ell. cur. s.t. $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

$j(\Lambda)$ $E_{j(\Lambda)}$


ℂ
i
1
(genus 1)

Points on Elliptic Curves

Ex.

$$x(x+y)(x+1) + y(x+y)(y+1) + (x+1)(y+1) = 4(x+y)(x+1)(y+1)$$

$$y^2 + xy + y = x^3 - 234x + 1352$$

Rational points ??

Ex.

$$x(x+y)(x+1) + y(x+y)(y+1) + (x+1)(y+1) = 4(x+y)(x+1)(y+1)$$

$$y^2 + xy + y = x^3 - 234x + 1352$$

$(-11, -4)$

$(8, -8)$

$$\begin{cases} x = \text{Apples} \\ y = \text{Bananas} \\ z = \text{Pineapples} \end{cases}$$

$$\frac{-11}{-3} + \frac{-4}{-10} + \frac{1}{-15} = 4$$

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$$

$x = -11$, $y = -4$, $z = 1$

Works!

About $\mathbb{Z}$-points:

Theorem (Siegel)

Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2 = x^3 + Ax + B \quad \text{w/ } A, B \in \mathbb{Z}.$$

Then $\underbrace{E(\mathbb{Z})}_{\substack{\text{POINTS ON} \\ E \text{ W/ } \mathbb{Z}\text{-COORDS.}}}$ is finite.

+ BAKER: If $(x_0, y_0) \in E(\mathbb{Z})$, then

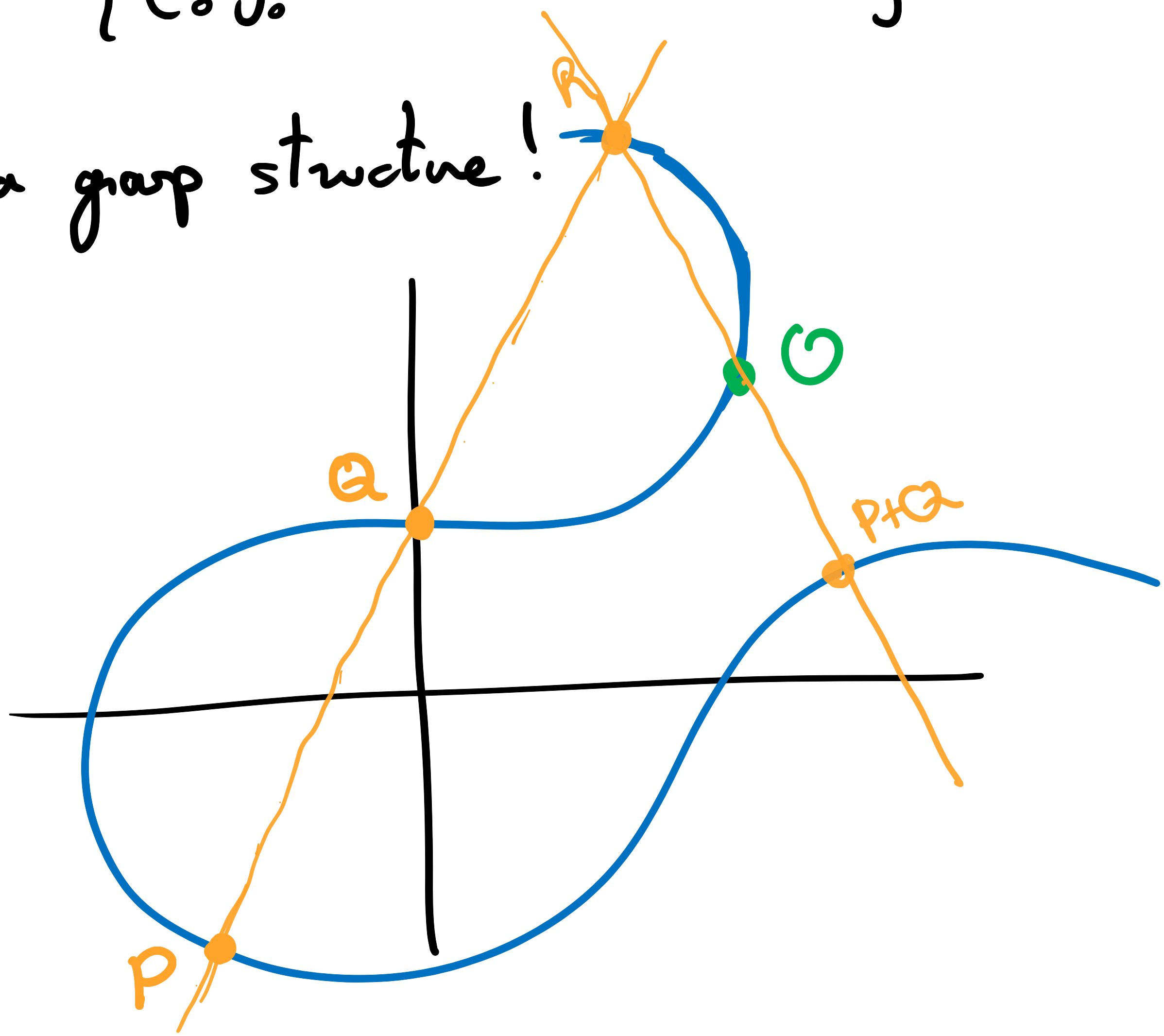
$$\max(|x_0|, |y_0|) < e^{10^6 \cdot \max(|A|, |B|)^{10^6}}.$$

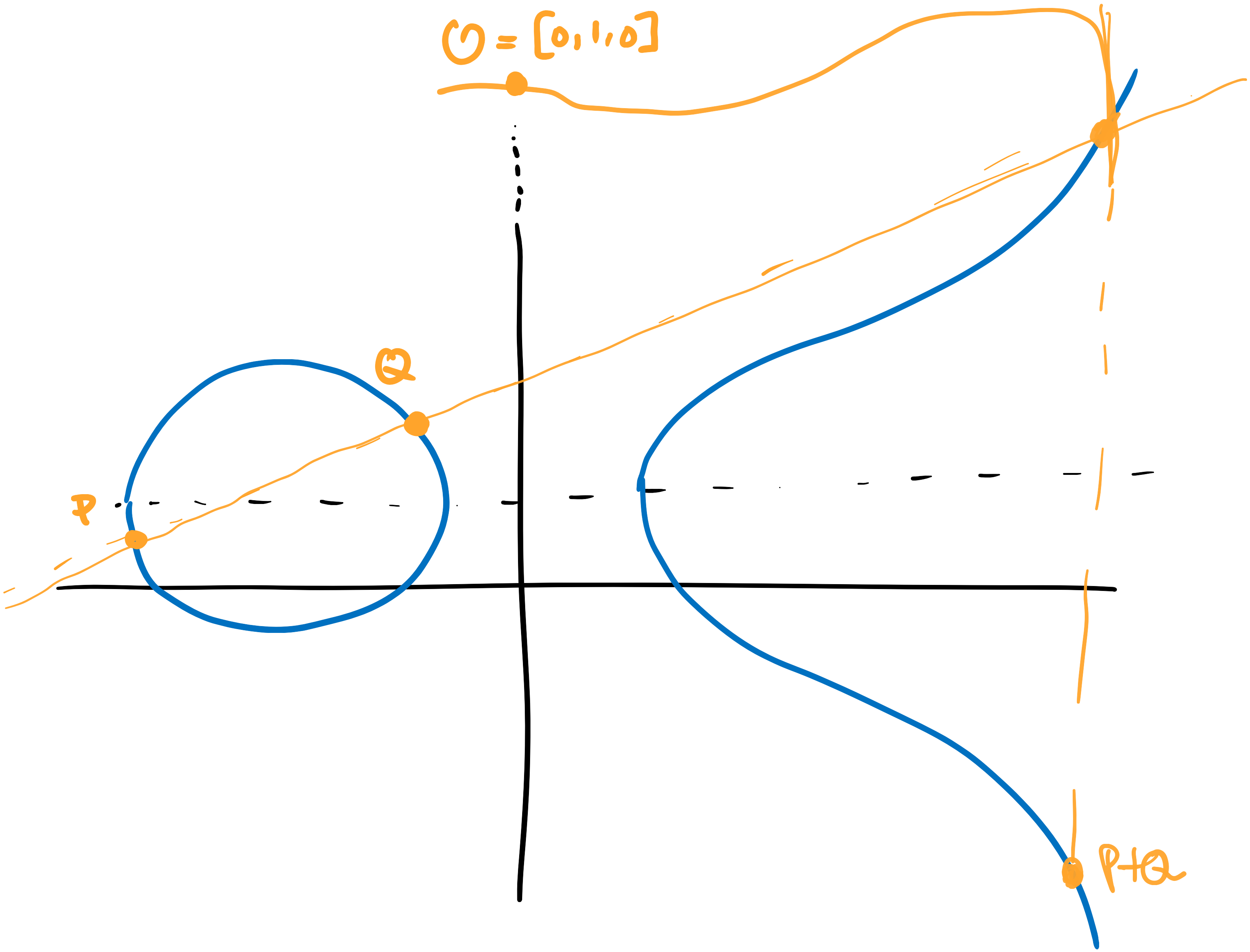
The $\mathbb{Q}$-rational points

$[0,1,0]$

$$E(\mathbb{Q}) = \{(x_0, y_0) \in E : x_0, y_0 \in \mathbb{Q}\} \cup \{\mathcal{O}\}$$

enjoy a group structure!





O = [0,1,0]
Q
P
P+Q

EXERCISE.

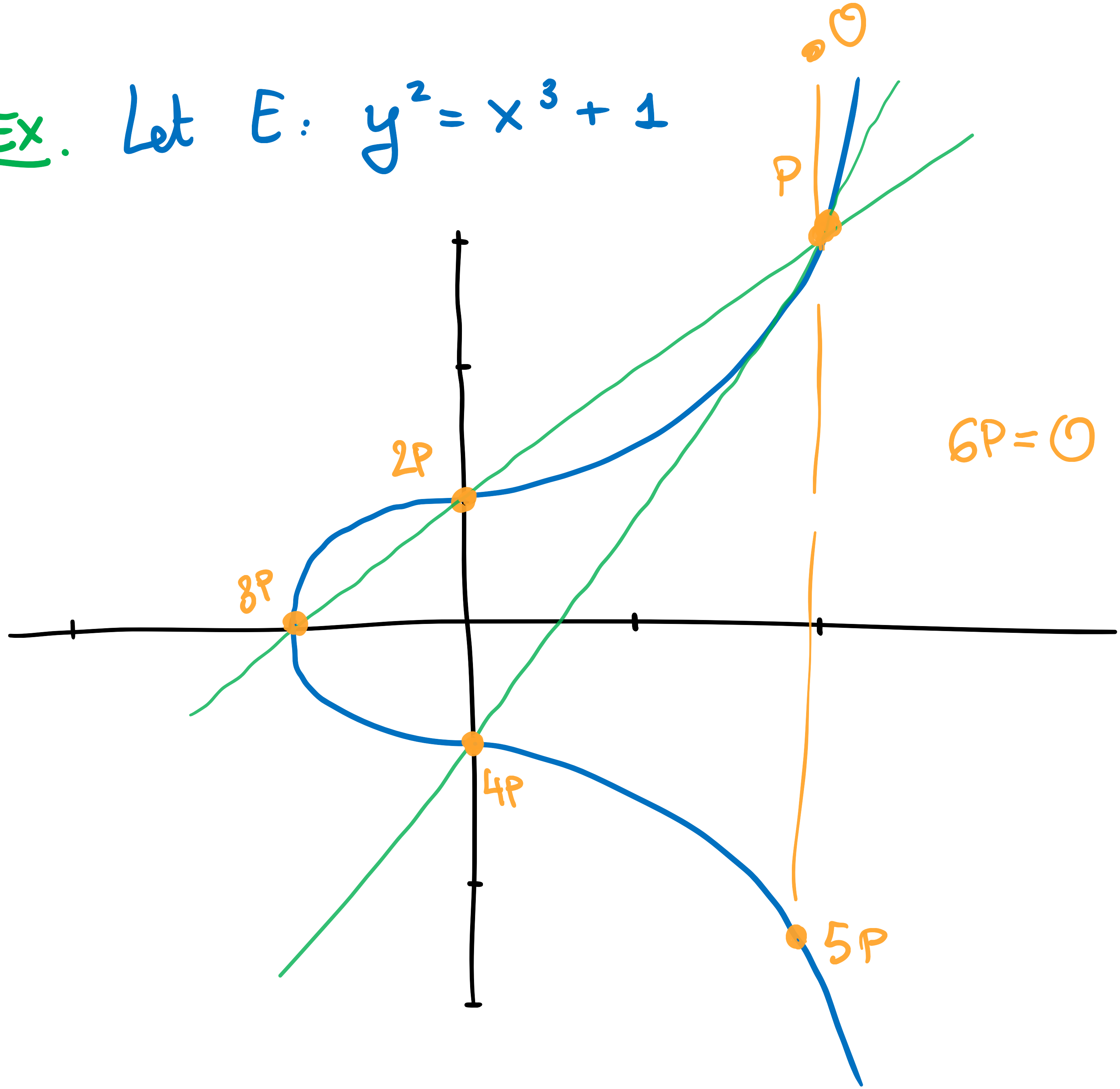
Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve.

Show that if $L: x = k$ is a vertical line, then

$$E \cap L \text{ contains } \mathcal{O} = [0,1,0].$$

HINT: WORK IN PROJECTIVE COORDINATES.

Ex. Let $E: y^2 = x^3 + 1$



Ex. Let $E: y^2 = x^3 - 25x$, and let $P = (5,0)$, $Q = (-4,6)$.

$\boxed{P+Q}$

$$\begin{cases} y^2 = x^3 - 25x \\ y = -\frac{2}{3}(x-5) \end{cases}$$

$L = \overline{PQ}$

$$x^3 - \frac{4}{9}x^2 - \frac{185}{9}x - \frac{100}{9} = 0$$

$$\shortparallel$$

$$(x-5)(x+4)(x+5/9)$$

$$L \cap E = \{P, Q, (-5/9, \tfrac{100}{27})\} \Rightarrow P+Q = \left(-5/9, -\frac{100}{27}\right)$$

Ex. Let $E: y^2 = x^3 - 25x$, and let

$P = (5,0)$, $Q = (-4,6)$.

$\boxed{2Q}$

$$\begin{cases} y^2 = x^3 - 25x \\ y = \frac{23}{12}(x+4) + 6 \end{cases}$$

tangent at Q

$$x^3 - \frac{529}{144}x^2 - \frac{1393}{18}x - \frac{1681}{9} = 0$$

$$\parallel$$

$$(x+4)^2\left(x - \frac{1681}{144}\right)$$

$$L \cap E = \left\{Q, \left(\frac{1681}{144}, \frac{62279}{1728}\right)\right\} \Rightarrow 2Q = \left(\frac{1681}{144}, -\frac{62279}{1728}\right)$$

Ex $E: y^2 = x^3 + 1 \;/\; \mathbb{F}_{11}$

$P = (7,5) \in E(\mathbb{F}_{11})$

b/c $\underset{\overset{\text{III}}{344}}{7^3} + 1 \equiv 5^2 \mod 11$

$2P = (2,8)$

$3P = (5,7)$

$4P = (0,10)$

$5P = (9,9)$

$6P = (10,0)$

$7P = (9,2)$

$8P = (0,1)$

$9P = (5,4)$

$10P = (2,3)$

$11P = (7,6)$

$12P = \mathcal{O} = [0,1,0]$

$E(\mathbb{F}_{11}) = \langle (7,5) \rangle \cong \mathbb{Z}/12\mathbb{Z}$

Ex.

$$y^2 + xy + y = x^3 - 234x + 1352$$

$$P = (8, -8)$$

$$2P = \left(\frac{610}{49}, -\frac{9281}{343} \right)$$

$$x = -8784, \quad y = 5165, \quad z = 9499$$

Ex.

$$y^2 + xy + y = x^3 - 234x + 1352$$

$$Q = (23, -103)$$

$$\underbrace{X = -1}_{:(}\ , \quad Y = 1\ , \quad Z = 1$$

$$2Q = (10, -12)$$

$$X = 1\ , \quad \underbrace{Y = 0}_{:(}\ , \quad Z = 1$$

("positive whole values")