CTNT 2024

Connecticut Summer School in Number Theory

Introduction to Elliptic Curves

Álvaro Lozano-Robledo
(University of Connecticut)

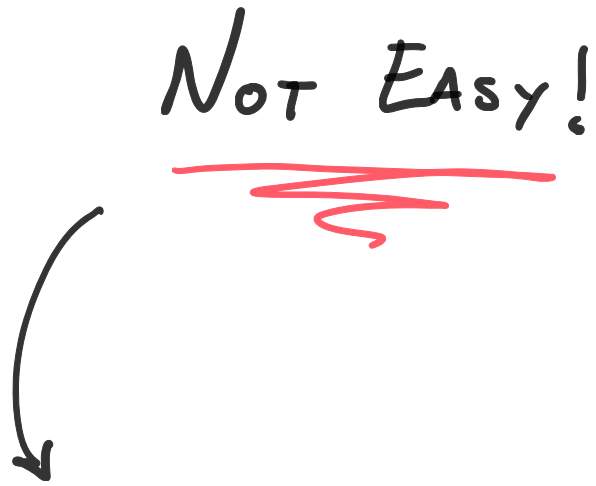
Lecture 3

The Mordell-Weil Group of an Elliptic Curve

My goal: make you part of the 5%!

95% of people cannot solve this!

Can you find positive whole values for 🍎, 🍌, and 🍍?



Here is the simplest solution:

apple = 1544768021087461664419513150199198374856643256695654317000266348982532020352779999

banana = 3687513179412999982719781156522547482549297996897197099628313747163722463405557 9

pineapple = 437361267792869725786125260237139015281653755816161361862143799337842346777203 6

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

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

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

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

Q. Is this an elliptic curve??

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.

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

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

$(-11, -4)$

$(8, -8)$

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

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

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

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

Works!

Ex.

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

$Q = (23, -103)$

$\rightarrow X = -1, Y = 1, Z = 1$

☹

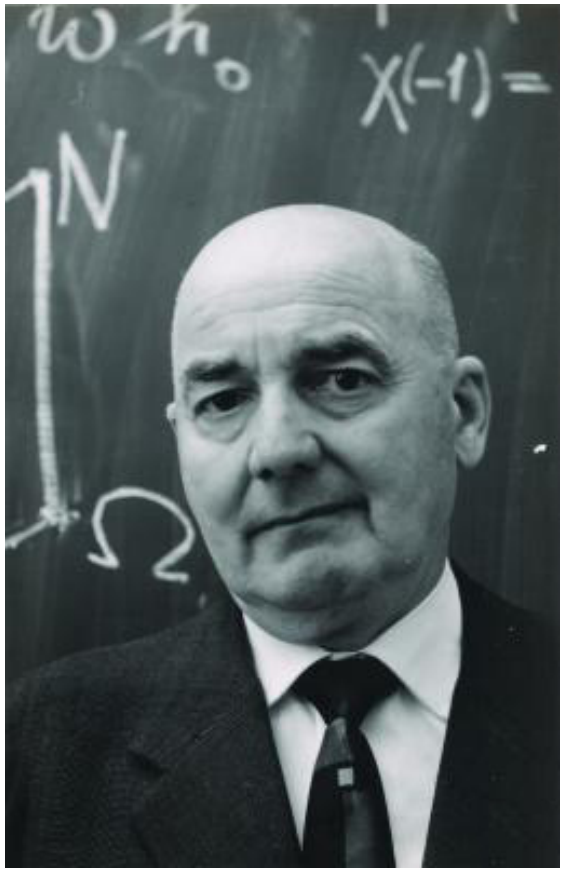
$2Q = (10, -12)$

$\rightarrow X = 1, Y = 0, Z = 1$

☹

("positive whole values")

We need to know more about F-rational points!



THEOREM (HASSE)

Let $\mathbb{F}_q$ be a finite field with q elements and let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$q+1-2\sqrt{q} < \#E(\mathbb{F}_q) < q+1+2\sqrt{q}$$

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

$\mathbb{F}_5 \cong \mathbb{Z}/5\mathbb{Z}$

$$E(\mathbb{F}_5) = \{O, (1,2), (1,3), (2,1), (2,4), (3,0)\}$$

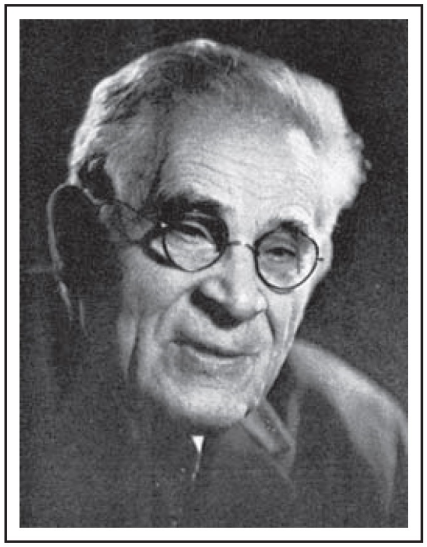
$$1.52\ldots = 5+1-2\sqrt{5} < 6 < 5+1+2\sqrt{5} = 10.47\ldots$$ ✓

EXERCISE. Find $E_1/\mathbb{F}_p$ s.t. $\#E_1(\mathbb{F}_p) = \lfloor p+1+2\sqrt{p} \rfloor$

$E_2/\mathbb{F}_p$ s.t. $\#E_2(\mathbb{F}_p) = \lfloor p+1-2\sqrt{p} \rfloor + 1$

What about $\mathbb{Q}$ or a # field ?

$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, ...



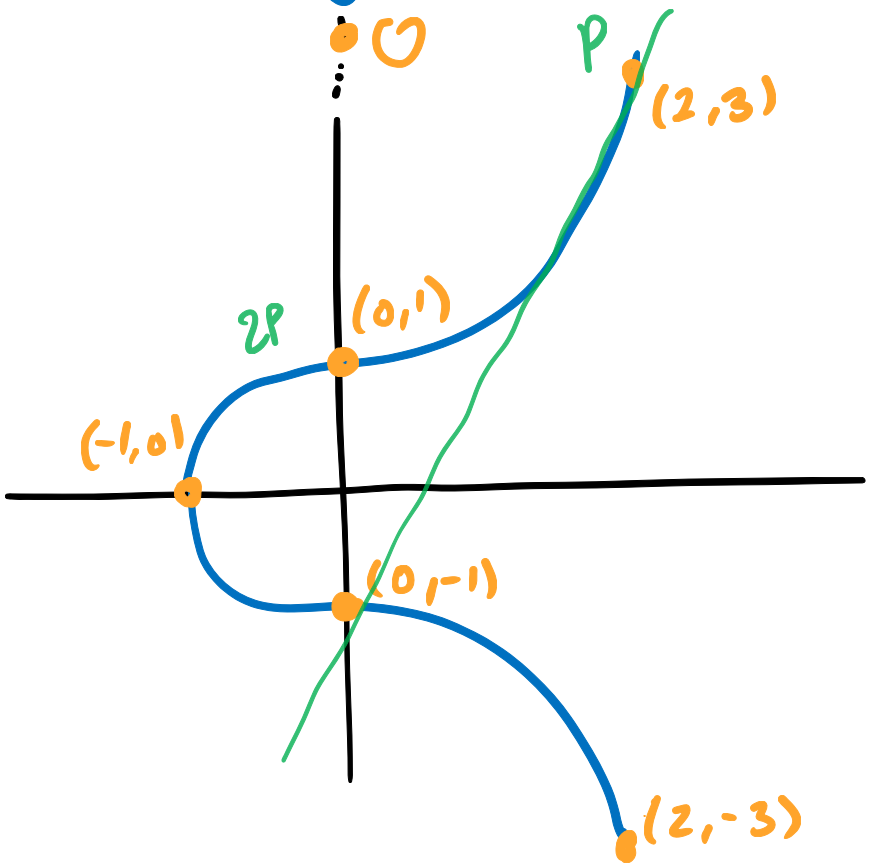
Louis Mordell
1888 – 1972

André Weil
1906 – 1998

Theorem (Mordell–Weil, 1928)

Let F be a number field, and let A/F be an abelian variety. Then, the group of F-rational points on A, denoted by $A(F)$, is a finitely generated abelian group. In particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ where $A(F)_{tors}$ is a finite subgroup, and $R_{A/F} \geq 0$.

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



$$E(\mathbb{Q}) = \{O, (0,\pm 1), (-1,0), (2,\pm 3)\}$$

$$E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors}$$

$$R_{E/\mathbb{Q}} = 0.$$

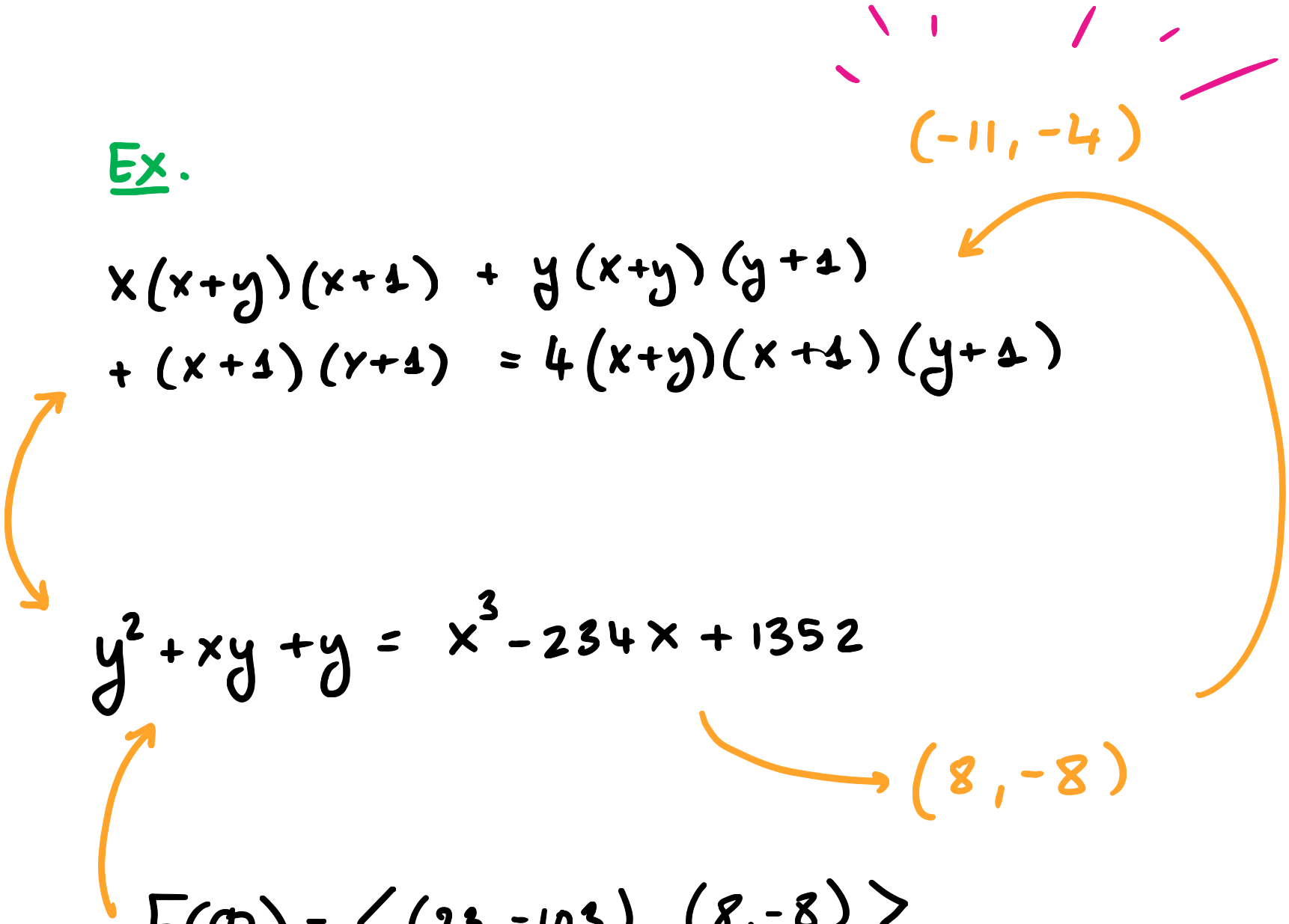
Ex $E: y^2 + y = x^3 - 7x + 6$

$$E(\mathbb{Q}) = \langle (1,0), (2,0), (0,-3) \rangle$$

$$\cong \mathbb{Z}^3$$

$$E(\mathbb{Q})_{tors} = \{O\}$$

$$R_{E/\mathbb{Q}} = 3$$


(-11, -4)
Ex.
x(x+y)(x+1) + y(x+y)(y+1)
+ (x+1)(y+1) = 4(x+y)(x+1)(y+1)
$y^2 + xy + y = x^3 - 234x + 1352$
(8, -8)
$E(\mathbb{Q}) = \langle (23, -103), (8, -8) \rangle$
$\cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$

Thus, every $R \in E(\mathbb{Q})$ is of the form:

$$R = n \cdot P + m \cdot Q$$

where $P = (23, -103)$, $0 \leq n < 6$,

$Q = (8, -8)$, $m \in \mathbb{Z}$.

$$R = n \cdot P + m \cdot Q$$

where $P = (23, -103)$, $0 \le n < 6$,

$Q = (8, -8)$, $m \in \mathbb{Z}$.

$R = 0 \cdot P + 9 \cdot Q$ leads to solution!

Here is the simplest solution:

X = apple = 154476802108746166441951315019919837485664325669565431700026634898253202035277999

Y = banana = 368751317941299998271978115652254748254929799689719709962831374716372246340555 79

Z = pineapple = 437361267792869725786125260237139015281653755816161361862143799337842346777 2036

Mordell-Weil Theorem for $E/\mathbb{Q}$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$$

Let's talk about torsion!

Ex

- $E_1 : y^2 = x^3 - 2$
- $E_2 : y^2 = x^3 + 8$
- $E_3 : y^2 = x^3 + 4$
- $E_4 : y^2 = x^3 + 4x$
- $E_5 : y^2 - y = x^3 - x^2$
- $E_6 : y^2 = x^3 + 1$

$E(\mathbb{Q})_{tors}$

$\{O\}$

$\mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/3$

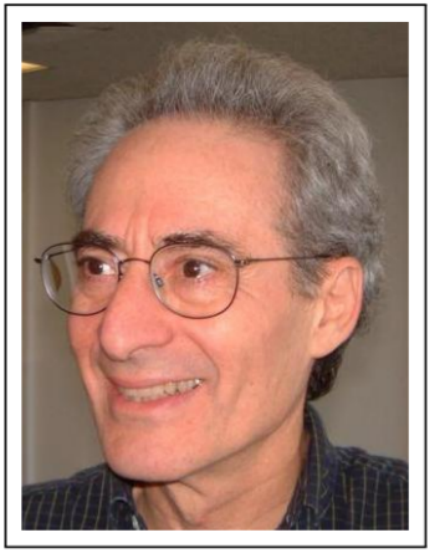
$\mathbb{Z}/4$

$\mathbb{Z}/5$

$\mathbb{Z}/6$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$$

What torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ are possible?



Barry Mazur

Theorem (Levi–Ogg Conjecture; Mazur, 1977)

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

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4. \end{cases}$$

Moreover, each possible group appears infinitely many times.

M=11 ?? $X_1(11)$ Weston's "The mod curves $X_0(11)$, $X_1(11)$"

Curve	Torsion	Generators
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(2,0)}{(0,0)}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(3,6)}{(0,0)}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(-3,18)}{(2,-2)}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(30,-90)}{(-40,400)}$

Figure 16.4. Examples of each of the possible torsion subgroups over $\mathbb{Q}$.

Note. Over $\mathbb{Q}$, elliptic curves with a given torsion subgroup belong to 1-parametric families.

Ex. Let $t \in \mathbb{Q}$ and

$$E_t : y^2 + (1-t)xy - ty = x^3 - tx^2$$

has $\mathbb{Z}/5\mathbb{Z} \subseteq E(\mathbb{Q})_{tors}$.

} Modular Curve $X_1(5)$

Conversely, if $A/\mathbb{Q}$ is an elliptic curve w/ $A(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$ then there is $t = t_A$ s.t.

$$E_{t_A} \underset{\mathbb{Q}}{\cong} A.$$

How do you compute torsion subgroups?

THEOREM (Nagell, Lutz)

Let $E/\mathbb{Q}$ be an elliptic curve with W. eq'n

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

Then, every torsion point $P \in E(\mathbb{Q})_{tors}$, $P \neq \mathcal{O}$:

(1) The coords. of P are integers: $x(P), y(P) \in \mathbb{Z}$.

(2) If P is of order $n \geq 3$, then $(y(P)^2) \mid (4A^3 + 27B^2)$.

(3) If P is of order 2, then $y(P) = 0$ and

$$x(P)^3 + A \cdot x(P) + B = 0.$$

Ex $E: y^2 = x^3 - 2$ ⟵ $(3,5)$

- $x^3 - 2$ has no $\mathbb{Q}$-roots $\Rightarrow$ no 2-torsion
- $4A^3 + 27B^2 = 27 \cdot 4$

$$y(P)^2 \mid 27 \cdot 4$$

$$\Rightarrow y(P) = \pm 1, \pm 2, \pm 3, \pm 6$$

$$\Rightarrow x(P)^3 = 3, 6, 11, \text{ or } 38$$ ✗

$\Rightarrow$ No torsion over $\mathbb{Q}$!

(but there is an $\mathbb{Z}$-point!)

Ex.

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

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

$$y^2 = x^3 - 302643x + 63998478$$

$$4A^3 + 27B^2 = -2929214360217 60$$
$$= 2^{10} \cdot 3^{12} \cdot 5 \cdot 7^2 \cdot 13^3$$

(!) LOTS OF WORK...

More on Elliptic Curves over Finite Fields.

$E/\mathbb{Q}$ → (reduce model mod p) → $E/\mathbb{F}_p$ elliptic curve ??

$E/\mathbb{Q}$: elliptic curve (w/ model $/\mathbb{Z}$)

Ex

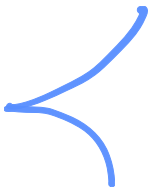
$y^2 = x^3 + 5/\mathbb{Q}$ → (mod 5) → $y^2 = x^3/\mathbb{F}_5$ singular !!

Possible Reductions Mod p

Ex

$y^2 = x^3 + 35x + 5 \;/\mathbb{Q}$

- mod 7 → $y^2 = x^3 + 5 \;/\mathbb{F}_7$ (smooth) — GOOD REDUCTION
- mod 5 → $y^2 = x^3 \;/\mathbb{F}_5$ (singular w/ cusp) — BAD ADDITIVE REDUCTION



$y^2 = x^3 - x^2 + 35 \;/\mathbb{Q}$

- mod 5 → $y^2 = x^3 - x^2 \;/\mathbb{F}_5$ — BAD SPLIT MULTIPLICATIVE REDUCTION

- mod 7 → $y^2 = x^3 - x^2 \;/\mathbb{F}_7$ — BAD NON-SPLIT MULTIPLICATIVE REDUCTION.

FACT. If p is of bad reduction, then

$$p \mid \Delta_E.$$

If Δ_E is minimal, then $p \mid \Delta_E \iff p$ is of bad red'n.

PROPOSITION Ex $y^2 = x^3 + 5^6 \underset{\mathbb{Q}}{\cong} y^2 = x^3 + 1$ $\quad (x,y) \mapsto \left(\frac{x}{5^2}, \frac{y}{5^3}\right)$

Let $E/\mathbb{Q}$ be an elliptic curve, p a prime number and $m \geq 1$ w/ $p \nmid m$. Suppose $E/\mathbb{Q}$ has good red'n mod p. Then the red'n mod p map

$$E(\mathbb{Q})[m] \longrightarrow \tilde{E}(\mathbb{F}_p)$$

is an inj. homomorphism. In particular $\#E(\mathbb{Q})[m] \mid \#\tilde{E}(\mathbb{F}_p)$

Ex

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

$$\Delta_E = 2^2 \cdot 5 \cdot 7^2 \cdot 13^3$$

- $p = 3$ is good and $\#\tilde{E}(\mathbb{F}_3) = 6$
- $p = 11$ is good and $\#\tilde{E}(\mathbb{F}_{11}) = 12$

exercise!

$\#E(\mathbb{Q})_{tors} \leq 6$ ($P = (23, -103)$ has order 6)

Complex Multiplication Interlude

E/F, $n \geq 1$, then:

$$[n] : E \longrightarrow E$$
$$P \longmapsto n \cdot P = P + \cdots + P$$

is an endomorphism of E, such that $[n] \circ [m] = [nm]$.

- $\mathrm{End}(E)$ is a ring under $+$ and $\circ$
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ (meaning $\{[n]\} \subseteq \mathrm{End}(E)$)

Q. Is $\mathrm{End}(E) = \mathbb{Z}$?

Ex $E: y^2 = x^3 - x$ $\boxed{j = 1728}$

$$[i]: E \longrightarrow E$$

$$P = (x_0, y_0) \longmapsto (-x_0, iy_0)$$

is an endomorphism.

Fact: $\mathrm{End}(E) = \{[n] + [i] \circ [m] : n, m \in \mathbb{Z}\}$

$$\cong \mathbb{Z}[i]$$

Why "complex multiplication"?

$E: y^2 = x^3 - x \qquad \mathbb{C}/\mathbb{Z}[i] \cong \mathbb{C}/\mathbb{Z}[i]$

$[n]: \mathbb{C}/\mathbb{Z}[i] \longrightarrow \mathbb{C}/\mathbb{Z}[i]$

$z \longmapsto n \cdot z$

$[i]: \mathbb{C}/\mathbb{Z}[i] \longrightarrow \mathbb{C}/\mathbb{Z}[i]$

$z \longmapsto i \cdot z$

EXERCISE

WELL DEFINED!

$[a+bi]: \quad z \longmapsto (a+bi) \cdot z$

Ex $E: y^2 = x^3 + 1$, $\rho^3 = 1$ $(\rho^2 + \rho + 1 = 0)$

$$[\rho] : E \longrightarrow E$$

$$(x_0, y_0) \longmapsto (\rho x_0, y_0)$$

is an endomorphism, and

$$\mathrm{End}(E) \cong \mathbb{Z}[\rho].$$

FACTS.

- E/F , F a # field

then $\mathrm{End}(E) \cong \mathbb{Z}$ OR $\mathcal{O}$

where $\mathcal{O} \subseteq \mathcal{O}_K$ is an order in an imaginary quadratic field.

- $E/\bar{\mathbb{Q}}$, $\mathrm{End}\, E \cong \mathcal{O}$

$\Rightarrow$ Class number of $\mathcal{O}$ is 1.

($\Rightarrow$ there are 13 j-invariants over $\bar{\mathbb{Q}}$ w/ CM)

$j = 0, 1728$

Back to Rank:

Ex. $E: y^2+y = x^3-7x+6 \;/\mathbb{Q}$

$$E(\mathbb{Q}) = \langle P, Q, R \rangle \cong \mathbb{Z}^3$$

$$P=(3,-4),\ Q=(2,-1),\ R=(1,-1)$$

This curve has lots of integral points:

[(-3 : 0 : 1), (-2 : -4 : 1), (-1 : -4 : 1), (0 : 2 : 1), (1 : 0 : 1), (2 : -1 : 1), (3 : 3 : 1), (4 : -7 : 1), (8 : 21 : 1), (11 : -36 : 1), (14 : 51 : 1), (21 : 95 : 1), (37 : -225 : 1), (52 : 374 : 1), (93 : 896 : 1), (342 : 6324 : 1), (406 : -8181 : 1), (816 : -23310 : 1)]

Q: $(1,0) = aP+bQ+cR$, find a,b,c.

Heights

Definition

- $h\left(\frac{m}{n}\right) = \log\left(\max(|m|, |n|)\right)$ if $\frac{m}{n} \in \mathbb{Q}$ lowest terms
- $E/\mathbb{Q}$, $P \in E(\mathbb{Q})$, $P = (x(P), y(P))$

$$H(P) = h(x(P))$$

- Néron-Tate Canonical Height

$$\hat{h}(P) = \frac{1}{2} \lim_{N \to \infty} \frac{H(2^N \cdot P)}{4^N}$$

PROPERTIES: $E/\mathbb{Q}$, $P \in E(\mathbb{Q})$, $m \geq 1$

- $\hat{h}(mP) = m^2 \hat{h}(P)$
- $\hat{h}(P) \geq 0$
- $\hat{h}(P) = 0 \iff P$ is a torsion pt
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$

  if $P, Q \in E(\mathbb{Q})$.
- $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$

  is a non-deg symmetric bilinear form.