

Final: Friday, May 23 1:30-4:30

Special office hours: this Thursday 9-12

Computing Torsion Group:

$$E(\mathbb{Q})_{\text{tors}} = \{P \in E(\mathbb{Q}) \mid \exists N > 0 \text{ with } NP = O\}$$

Thm: (Lutz-Nagell) $E: y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$ Let $D = a^2b^2 - 4a^3c - 4b^3 - 18abc - 27c^2$. Then if (α, β) is a torsion point, then α, β integers and $\beta^2 \mid D$, or $\beta = 0$.Algorithm for computing $E(\mathbb{Q})_{\text{tors}}$:

1. Change var. to put equation in form of L-N.
2. Compute square integers β^2 dividing D .
3. For each β , try to solve $\beta^2 = x^3 + ax^2 + bx + c$ with $x \in \mathbb{Z}$.
4. Compute N (each possible tors pt) for $1 \leq N \leq 10$ and $N=12$.
5. Identify group corresponding to $E(\mathbb{Q})_{\text{tors}}$.

Ex: $y^2 = x^2 + 4$

From last time, $\mathbb{Z}/(3)$ or $\mathbb{Z}/(9)$, and $\mathbb{Z}/(3)$ is correct.

Ex: $y^2 - y = x^3 - x^2$

Complete the square:

$$(y - \frac{1}{2})^2 = x^3 - x^2 + \frac{1}{4} \Rightarrow y^2 = x^3 - x^2 + \frac{1}{4}$$

$$\text{Let } x = \frac{1}{4}x, \quad y^2 = \frac{1}{4}x^3 - \frac{1}{4}x^2 + \frac{1}{4} \quad 4^2 y^2 = x^3 - 4x^2 + 16$$

$$y = 2^2 y, \quad y^2 = x^3 - 4x^2 + 16$$

$$D = 4^4(16) - 27(16)^2 = 16^2(-11) = 2^8(-11)$$

Possible values for β :

$$0, \pm 1, \pm 2, \pm 2^2, \pm 2^3, \pm 2^4$$

$$\beta = 0: \quad x^3 - 4x^2 + 16 = 0.$$

$$(x - \alpha)(x^2 + \gamma x + \delta) = x^3 - 4x^2 + 16.$$

$$-\alpha + \gamma = -4 \Rightarrow \gamma \in \mathbb{Z}, \quad -\alpha\gamma + \delta = 0 \Rightarrow \delta = \alpha\gamma$$

$$-\alpha\delta = 16 \Rightarrow -\alpha^2\gamma = 16. \Rightarrow \alpha = \pm 2, \pm 2^2$$

check w/ $-\alpha + \gamma = -4 \Rightarrow$ no solutions

$$\beta = \pm 1: \quad x^3 - 4x^2 + 15 = 0$$

$$(x - \alpha)(x^2 + \gamma x + \delta)$$

$$-\alpha + \gamma = -4 \quad -\alpha\gamma + \delta = 0 \quad -\alpha^2\gamma = 15 \Rightarrow \alpha = \pm 1 \Rightarrow \gamma = -15.$$

no solution.

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

Ex: $y^2 = x^3 - 4x$ $D = 4^4$.

Possible β : $\beta = 0, \pm 1, \pm 2, \pm 2^2, \pm 2^3, \pm 2^4$

$\beta = 0$: $0 = x(x-2)(x+2)$.

$(0,0)$ $(2,0)$ $(-2,0)$ all have order 2.

$\therefore E(\mathbb{Q})$ has one of $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$, $\mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$, $\mathbb{Z}/(2) \oplus \mathbb{Z}/(6)$, $\mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$

Reason: $\mathbb{Z}/(n)$ n even.

elts. $[m]$ s.t. $2[m] = 0 \Leftrightarrow n|2m \Leftrightarrow \frac{n}{2}|m$

$m \equiv \frac{n}{2} (n)$ or $m \equiv 0 (n)$.

A priori could be $\mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$.

$(1,0)$ $(0,2)$ $(1,2)$.

$(0,2) = 2(0,1) \Rightarrow$ one of our pts. is 2·P' w/ P' int coord.