

18.781

9 May 2005

$$E: y^2 = x^3 - Ax - B \quad A, B \in \mathbb{Q}$$

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

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

Mazur's Thrm:  $E(\mathbb{Q})_{\text{tors}}$  is isomorphic to one of the following

•  $\{O\}$

•  $\mathbb{Z}/(n)$ ,  $2 \leq n \leq 10$   $n=12$

•  $\mathbb{Z}/(2) \oplus \mathbb{Z}/(n)$   $n=2, 4, 6, 8$

Goal: Algorithm for computing  $E(\mathbb{Q})_{\text{tors}}$ .

All of the groups in Mazur's thrm occur.

$$y^2 = x^3 - 2 \quad y^2 = x^3 + 8 \quad y^2 = x^3 + 4 \quad y^2 = x^3 + 4x \quad y^2 - y = x^3 - x^2$$

$$y^2 = x^3 + 1 \quad y^2 = x^3 - 43x + 166 \quad y^2 + 7xy = x^3 + 16x \quad y^2 + xy + y = x^3 - x^2 - 14x + 29$$

$$y^2 + xy = x^3 - 45x + 91 \quad y^2 + 43xy - 210y = x^3 - 210x^2 \quad y^2 = x^3 - 4x$$

$$y^2 = x^3 + 2x^2 - 3x \quad y^2 + 5xy - 6y = x^3 - 3x^2 \quad y^2 + 17xy - 120y = x^3 - 60x^2$$

Thrm: (Lutz-Nagell) Say  $E$  is given by  $y^2 = x^3 + ax^2 + bx + c$ ,  $a, b, c \in \mathbb{Z}$ .

Let  $D = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$  (discriminant)

If  $(\alpha, \beta) \in E(\mathbb{Q})_{\text{tors}}$  then  $\alpha, \beta \in \mathbb{Z}$  and either  $\beta = 0$  or  $\beta^2 \mid D$ .

Ex: Compute  $E(\mathbb{Q})_{\text{tors}}$  for  $y^2 = x^3 + 4$ .

$$D = -27 \cdot 4^3 = -3^3 \cdot 2^6$$

possibilities for  $\beta$ :  $\pm 3, \pm 2, \pm 4, \pm 6, \pm 12, \pm 1, 0$

$\beta = 0$ :  $0 = x^3 + 4$  no int. sol'n

$\beta = \pm 1$ :  $1 = x^3 + 4 \Rightarrow x^3 + 3 = 0$  no int. sol'n

$\beta = \pm 3$ :  $9 = x^3 + 4 \Rightarrow x^3 - 5 = 0$  no int. sol'n

$\beta = \pm 2$ :  $4 = x^3 + 4 \Rightarrow x^3 = 0 \Rightarrow x = 0$ .

$(0, 2)$   $(0, -2)$

$P = (0, 2)$   $2P: y^2 - x^3 - 4x^2 = 0$   $-P = (0, -2)$ .

tang. line  $(0) \cdot x + (4) \cdot y + (4 - 12)z = 0$   $4y - 8z = 0$   $4y - 8 = 0$ .

so 3<sup>rd</sup> pt. of intersection:  $4 = x^3 + 4 \Rightarrow x^3 = 0$   $(0, 2)$

so  $2P = (0, -2) \Rightarrow 2P = -P \Rightarrow 3P = O$ .

possibilities for  $E(\mathbb{Q})_{\text{tors}}$ :  $\mathbb{Z}$

(claim:  $\nexists P \neq O$  with  $2P = O$ .)

$$2P = O \Leftrightarrow P = -P \Leftrightarrow (\alpha, \beta) = (\alpha, -\beta) \Leftrightarrow \beta = 0$$

not  $\mathbb{Z}/(2) \oplus \mathbb{Z}/(n)$ .

can be  $\mathbb{Z}/(3)$  or  $\mathbb{Z}/(9)$ .

if  $E(\mathbb{Q})_{\text{tors}}$  were  $\mathbb{Z}/(a)$ ,  $\exists Q$  s.t.  $3Q = (0, 2)$ .