PREVIOUSLY...

MORDELL-WEIL (over $\mathbb{Q}$) { WEAK MORDELL-WEIL /K; DESCENT THEOREM; HEIGHTS (over $\mathbb{Q}$) }

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

RANK OF $E(\mathbb{Q})$

TORSION SUBGROUP

"FREE PART"

TODAY: TORSION POINTS

and then canonical heights.

(VII.3.4) ⇒ **Thm.** Let K be a number field, E/K an ell. curve.

w/ $y^2 + a_1 xy + a_3 y = \cdots$ LONG WEIERS. !

such that $a_i \in \mathcal{O}_K$. Let $P \in E(K)$ be a pt of finite order $m \geq 2$.

(a) If m is not a power of a prime, then $x(P), y(P) \in \mathcal{O}_K$. $(= R)$.

(b) If $m = p^n$, then $\forall\, v \in M_K^0$, let $r_v = \left\lfloor \frac{\mathrm{ord}_v(P)}{p^n - p^{n-1}} \right\rfloor$,

then $\mathrm{ord}_v(x(P)) \geq -2 r_v$

$\mathrm{ord}_v(y(P)) \geq -3 r_v$

In particular, $x(P), y(P)$ are integral if $\mathrm{ord}_v(p) = 0$.

Recall Over $\mathbb{Q}$: $r_q = \left\lfloor \frac{\mathrm{ord}_q(p)}{p^n - p^{n-1}} \right\rfloor = \begin{cases} 0 & \text{if } q \neq p. \\ 0 & \text{any } n \text{ if } p = q > 2 \\ 1 & p = 2, n = 1 \end{cases}$

Cor. (Nagell-Lutz theorem)

$E/\mathbb{Q}: y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.

Suppose $P \in E(\mathbb{Q})$ is a non-zero torsion point. Then:

(a) $x(P), y(P) \in \mathbb{Z}$.

(b) Either $2P = \mathcal{O}$ or else $y(P)^2 \mid (4A^3 + 27B^2)$.

example $E: y^2 = x^3 - 2$

- $E[2]$ $x^3 - 2 = 0$ is irreducible over $\mathbb{Q}$ $\Rightarrow$ no two torsion $/\mathbb{Q}$.

$P \notin E[2]$, $\underbrace{y(P)^2}_{\mathbb{Z}} \mid 4A^3 + 27B^2 = 27 \cdot 4$

$\Rightarrow y \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$

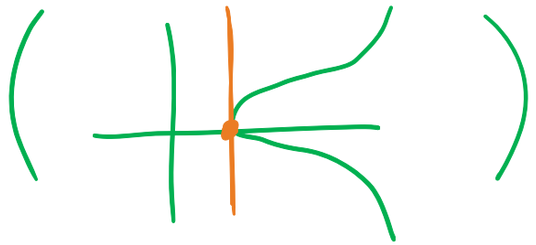
$\Rightarrow x^3 = y^2 + 2 \in \{3, 6, 11, 38\} \cap \square = \emptyset$

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

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

Pf. (Nagell-Lutz) → FOR SHORT WEIERSTRASS EQN'S !!!

(a) If $m=2$, $y(P)=0$



$\Rightarrow$ $x(P)$ is a root of $X^3+AX+B=0$, $A,B\in\mathbb{Z}$ $\rightarrow$ $x(P)\in \mathcal{O}_{\bar{\mathbb{Q}}}$ (algebraic integer)

$\rightarrow$ if $x(P)$ in $\mathbb{Q}$, then $x(P)$ is in $\mathbb{Z}$.

$\hookrightarrow$ $x(P)\in \mathcal{O}_{\bar{\mathbb{Q}}}\cap\mathbb{Q}=\mathbb{Z}$.

This shows that

if $P\in E[2](\mathbb{Q})\rightarrow x(P), y(P)\in\mathbb{Z}$.

If $m>2$, it follows from the Thm. $r_v=0$, and $x(P), y(P)\in\mathbb{Z}$.

(b) Assume $[2]P \neq \mathcal{O}$, $y(P) \neq 0$.

Then by (a), $x(P), y(P), x(2P) \in \mathbb{Z}$.

Duplication formula: $$x(2P) = \frac{\phi(x(P))}{4\psi(x(P)}$$