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

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

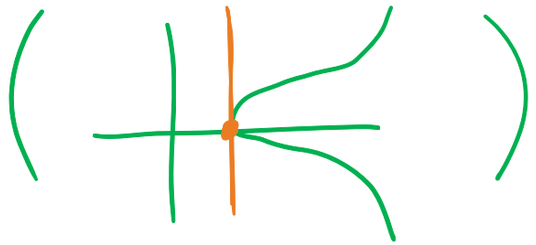
$\Rightarrow x^3 = y^2 + 2 \in \{3, 6, 11, 38\} \cap \square = \emptyset$

$\Rightarrow$ 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 $[2]P \neq O$, $y(P) \neq 0$.

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

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

where $\phi(X) = X^4 - 2AX^2 - 8BX + A^2$, $\psi(X) = X^3 + AX + B$.

Lemma $\Rightarrow$ $$\underbrace{(3X^2 + 4A)}_{f(X)}\phi(X) - \underbrace{(3X^3 - 5AX - 27B)}_{g(X)}\psi(X) = 4A^3 + 27B^2$$

- $\phi(x(P)) = x(2P) \cdot 4\psi(x(P))$, $\psi(x(P)) = y(P)^2$ ↗ plug in.

$$\Rightarrow y(P)^2 \cdot \left(4f(x(P)) \cdot x(2P) - g(x(P))\right) = 4A^3 + 27B^2$$

An eqn of integers! $\Rightarrow$ $y(P)^2 \mid 4A^3 + 27B^2$ ▨

Thm (Mazur, 1977 - Conjectured: Levi, Ogg)

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

Recall: Weil pairing $\rightarrow$ if $E[m] \subseteq E(k)$, then $\mu_m \subseteq K$.

Fact: Every subgp in Mazur's list occurs for ∞'ly many j-invariants over $\mathbb{Q}$.

example Ell. curves $/\mathbb{Q}$ w/ $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/7\mathbb{Z}$ belong to a 1-parameter family:

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

with $P = (0,0) \in E[7]$, $d \in \mathbb{Q}$, $(\Delta \neq 0)$.

Reference: Weston's "The modular curves $X_0(11)$ and $X_1(11)$" $X_1(7)$

Canonical Heights

$H : \mathbb{Q} \to \mathbb{R}$, $H(p/q) = \max\{|p|, |q|\}$

$h_x : E(\mathbb{Q}) \to \mathbb{R}$, $h_x(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O}. \end{cases}$

In general, if f is an even function on $E(\mathbb{Q})$,

define $h_f(P) = \begin{cases} \log H(f(P)) & \text{if } P \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O}. \end{cases}$ } also a height!

Thm $E/\mathbb{Q}$, $f \in \mathbb{Q}(E)$ is even ($f(P) = f(-P)$). Then (constant depends only on E and f.)

- $\forall P, Q \in E(\mathbb{Q})$: $h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$

  (i.e., h_f is "almost" a quad. form)

- $f, g \in \mathbb{Q}(E)$ are even, then $(\deg g) h_f = (\deg f) h_g + O(1)$

Prop $E/\mathbb{Q}$, $f \in \mathbb{Q}(E)$ even, $P \in E(\mathbb{Q})$. Then the limit:

$$\frac{1}{\deg f} \lim_{N \to \infty} \frac{h_f([2^N]P)}{4^N}$$ exists and it's independent of f.

Pf. • Show that seq. is Cauchy.

(b) heights $\left(h_f(2P) \geq 4h_f(P) - C_2\right) \Rightarrow \exists\, C.\ \forall Q \in E(\mathbb{Q})\ \ |h_f([2]Q) - 4h_f(Q)| \leq C$

Let $N \geq M \geq 0$ be integers,

$$\left| \frac{h_f([2^N]P)}{4^N} - \frac{h_f([2^M]P)}{4^M} \right| = \left| \sum_{n=M}^{N-1} \frac{h_f([2^{n+1}]P)}{4^{n+1}} - \frac{h_f([2^n]P)}{4^n} \right|$$

$$\leq \sum_{n=M}^{N-1} \frac{|h_f([2^{n+1}]P) - 4h_f([2^n]P)|}{4^{n+1}} \overset{Q=[2^n]P}{\leq} \sum_{n=M}^{N-1} \frac{C}{4^{n+1}} \leq \frac{C}{3 \cdot 4^M} \to 0 \text{ as } N \geq M \geq 0,\ M \to \infty$$

$\Rightarrow$ Cauchy!

Ind.) If g is also even, $(\deg g)\, h_f = (\deg f)\, h_g + O(1)$

$$\frac{1}{\deg g \deg f}\left((\deg g)\,\frac{h_f([2^N]P)}{4^N} - (\deg f)\,\frac{h_g([2^N]P)}{4^N}\right) = \frac{1}{\deg g \cdot \deg f}\,\frac{O(1)}{4^N} \longrightarrow 0 \quad \text{as } N\to\infty.$$

$$\lim \frac{1}{\deg f}\,\frac{h_f}{4^N} \;-\; \lim \frac{1}{\deg g}\,\frac{h_g}{4^N} = 0$$

so limits coincide regardless of even fn. ▨

Def. The canonical Néron–Tate height on $E(\bar{\mathbb{Q}})$ is

$$\hat{h} : E(\bar{\mathbb{Q}}) \to \mathbb{R}, \quad \hat{h}(P) = \frac{1}{\deg f} \lim_{N\to\infty} \frac{h_f([2^N]P)}{4^N}$$

where f is an arbitrary even fn. (NOTE: $\hat{h}(O) = 0$.)

Thm $E/\mathbb{Q}$, with can. height $\hat{h}$.

(a) $f \in \mathbb{Q}(E)$ even, then $(\deg f)\cdot \hat{h} = h_f + \overbrace{O(1)}^{\text{constant that depends only on } E, f}$.

(a) $\forall P, Q \in E(\mathbb{Q})$

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \quad \text{("parallelogram law")}$$

(b) $\forall P \in E(\mathbb{Q}), m \in \mathbb{Z}$, $\hat{h}([m]P) = m^2 \hat{h}(P)$.

(c) $\hat{h}$ is a quad. form on E, i.e., $\hat{h}$ is even and

$$\langle , \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

$$(P, Q) \longmapsto \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \text{ is bilinear.}$$

(d) $P \in E(\mathbb{Q})$, $\hat{h}(P) \geq 0$ and $\hat{h}(P) = 0 \iff P$ is torsion. (!)

If $\hat{h}'$ satisfies (a) and (b) for any $m \geq 2$, then $\hat{h}' = \hat{h}$.