# PART 2: Selmer group heuristiss

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

$$\mathbb{Q}_v = \begin{cases} \mathbb{R} & \text{if } v = \infty \\ \mathbb{Q}_p & \text{if } v = p \end{cases}$$

$$\mathbb{A} := \prod_v{}' (\mathbb{Q}_v, \mathbb{Z}_v) = \left\{ (a_v) \in \prod \mathbb{Q}_v : a_v \in \mathbb{Z}_v \text{ for all but finitely many } v \right\}$$

---

$E$ ell. curve $/\mathbb{Q}$

<u>Mordell's theorem</u>: $E(\mathbb{Q})$ is f.g.

"Only" known proof:
- $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite for some $n \geq 2$
- height functions

$$
\begin{tikzcd}
0 \arrow[r] & E[n] \arrow[r] & E \arrow[r, "n"] \arrow[d, phantom, "\parallel" description] & E \arrow[r] & 0 \\
 & & E(\overline{\mathbb{Q}}) & &
\end{tikzcd}
$$

G-invariants

$$
\begin{tikzcd}
0 \arrow[r] & E[n](\mathbb{Q}) \arrow[r] & E(\mathbb{Q}) \arrow[r, "n"] & E(\mathbb{Q}) \arrow[dll, out=0, in=180] \\
 & H^1(\mathbb{Q}, E[n]) \arrow[r] & \underbrace{H^1(\mathbb{Q}, E)}_{H^1(G,\, E(\overline{\mathbb{Q}}))} \arrow[r, "n"] & H^1(\mathbb{Q}, E)
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & & \mathrm{Sel}_n E \arrow[d, phantom, "\subseteq" rotate=-90] & \\
0 \arrow[r] & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \arrow[r] \arrow[d] & H^1(\mathbb{Q}, E[n]) \arrow[r] \arrow[d, "\beta"] & H^1(\mathbb{Q}, E) \arrow[d, "\gamma"] \\
0 \arrow[r] & \prod_v' \dfrac{E(\mathbb{Q}_v)}{nE(\mathbb{Q}_v)} \arrow[r, "\alpha"] \arrow[d, phantom, "\parallel"] & \prod_v' H^1(\mathbb{Q}_v, E[n]) \arrow[r] \arrow[d, phantom, "\parallel"] & \prod_v' H^1(\mathbb{Q}_v, E) \arrow[d, phantom, "\parallel"] \\
 & \dfrac{E(\mathbb{A})}{nE(\mathbb{A})} & H^1(\mathbb{A}, E[n]) & H^1(\mathbb{A}, E)
\end{tikzcd}
$$

$\mathrm{Sel}_n E := \beta^{-1}(\operatorname{im} \alpha)$ $\qquad$ $Ш := \ker \gamma$

upper bound for $\dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})}$

finite, computable

---

$h(E) := \max(|A|^3, |B|^2)$ where $E$ is $y^2 = x^3 + Ax + B$

in $\mathbb{Z}$, minimal

$\mathcal{E} := \{\text{ell. curves}/\mathbb{Q}\}$

$\mathcal{E}_{<X} := \{E \in \mathcal{E} : h(E) < X\}$

<u>Def.</u> If $S \subset \mathcal{E}$, $\mathrm{Prob}(S) := \lim\limits_{X \to \infty} \dfrac{\# S \cap \mathcal{E}_{<X}}{\# \mathcal{E}_{<X}}$.

Given $p$, and $s$, what is

$$\mathrm{Prob}(\dim \mathrm{Sel}_p E = s)\ ?$$

# Maximal isotropic subspaces

$$\left.\begin{aligned} V &= \mathbb{F}_p^{2n} \\ Q(x_1,\dots,x_n,y_1,\dots,y_n) &:= x_1y_1+\dots+x_ny_n \end{aligned}\right\}\text{hyperbolic quadratic space}$$

$Q \rightsquigarrow$ symm. bilinear ~~form~~ pairing

$$\langle\, ,\, \rangle : V \times V \to \mathbb{F}_p$$

$$\langle v, w\rangle := Q(v+w) - Q(v) - Q(w)$$

Given $\underset{\text{subspace}}{Z \leq V}$, $Z^\perp := \{ v \in V : \langle v, z\rangle = 0 \text{ for all } z \in Z\}$

$Z$ is <u>isotropic</u> if $Q|_Z = 0$.

$Z$ is <u>maximal isotropic</u> if $Q|_Z = 0$ and $Z = Z^\perp$

(Then $\dim Z = n$.)

<u>Example</u>: $\{(x_1, \dots, x_n, 0, \dots, 0) : x_i \in \mathbb{F}_p\}$

is max isot.

$$OGr_n(\mathbb{F}_p) := \{\text{max. isot. } Z \leq V\}.$$

Choose $Z, W \in OGr_n(\mathbb{F}_p)$ at random;

get random variable $\dim_{\mathbb{F}_p}(Z \cap W)$.

<u>Conj.</u> (P., Rains 2012): For each $s \in \mathbb{Z}_{\geq 0}$

$$\operatorname*{Prob}_{E \in \mathcal{E}}(\dim \mathrm{Sel}_p E = s) = \lim_{n \to \infty} \mathrm{Prob}(\dim(Z \cap W) = s)$$

<u>Goal</u>: $\mathrm{Sel}_p E$ <u>is</u> an intersection of max. isot. subspaces in an <u>infinite-dim.</u> quadratic space.

Assume $p$ is odd. (for simplicity)

$$Q \longleftrightarrow \langle\ ,\ \rangle$$

$$Q(v) := \frac{1}{2}\langle v,v\rangle \longmapsfrom \langle\ ,\ \rangle$$

# Local fields

$E / \mathbb{Q}_v$

$$V_v := H^1(\mathbb{Q}_v, E[p])$$

finite-dim $\mathbb{F}_p$-v.s.

The Weil pairing

$$e : E[p] \times E[p] \longrightarrow \underset{\overline{\mathbb{Q}}_v^{\times}}{\overset{\parallel}{\mathbb{G}_m}}$$

induces

$$\langle\ ,\ \rangle_v : V_v \times V_v \xrightarrow{\cup} H^2(\mathbb{Q}_v, E[p] \otimes E[p]) \xrightarrow{e} H^2(\mathbb{Q}_v, \mathbb{G}_m) = \mathrm{Br}\,\mathbb{Q}_v \hookrightarrow \frac{\mathbb{Q}}{\mathbb{Z}} \hookrightarrow \frac{\mathbb{R}}{\mathbb{Z}}$$

$$\updownarrow$$

$$Q_v : V_v \to \mathbb{R}/\mathbb{Z}$$

Define $W_v := \mathrm{im}\left( \frac{E(\mathbb{Q}_v)}{pE(\mathbb{Q}_v)} \longrightarrow \underset{V_v}{\overset{\parallel}{H^1(\mathbb{Q}_v, E[p])}} \right)$

O'Neil: Tate local duality $\Longrightarrow$ $W_v$ is max. isot. in $V_v$

## Global field

$E/\mathbb{Q}$

For each $v$, let $V_v = H^1(\mathbb{Q}_v, E[p])$

$$V := \prod{}'(V_v, W_v) \simeq H^1(\mathbb{A}, E[p])$$

$$Q := \sum q_v : V \to \mathbb{R}/\mathbb{Z}$$

$$\begin{tikzcd}
 & H^1(\mathbb{Q}, E[p]) \arrow[d, "\beta"] & \\
\dfrac{E(\mathbb{A})}{pE(\mathbb{A})} \arrow[r, "\alpha"] & H^1(\mathbb{A}, E[p]) \arrow[dr, equal] & \\
 & & V
\end{tikzcd}$$

Theorem: (a) $\operatorname{im}(\alpha)$, $\operatorname{im}(\beta)$ are max. isot.

(b) $\beta$ is injective

(c) $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta) = \beta(\operatorname{Sel}_p E) \simeq \operatorname{Sel}_p E$

## Ingredients of proof:

(a) $\mathrm{im}(\alpha) = \prod W_v$

max istropic

$\mathrm{im}(\beta)$ is max. isot. by

9-term Poitou-Tate exact seq;

(b) Chebotarev density theorem

+ Sylow $p$-subgp of $GL_2(\mathbb{F}_p)$ is cyclic

(c) By (a), (b), and def. of $\mathrm{Sel}_p$.