Arithmetic statistics for elliptic curves

Master's thesis presentation

David Kurniadi Angdinata

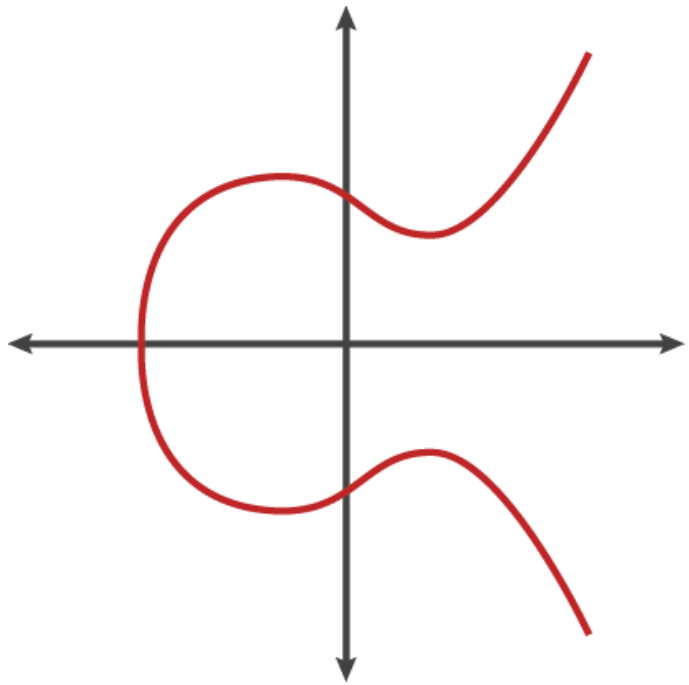
Imperial College London

Monday, 22 June 2020

Some motivation

What are elliptic curves?

- Solutions to $y^2 = x^3 + ax + b$ for rational numbers a and b.



What are they used for?

- Number theory.
- Cryptography.

Some motivation

What do we know?

- It is a group.
- It has a rank.

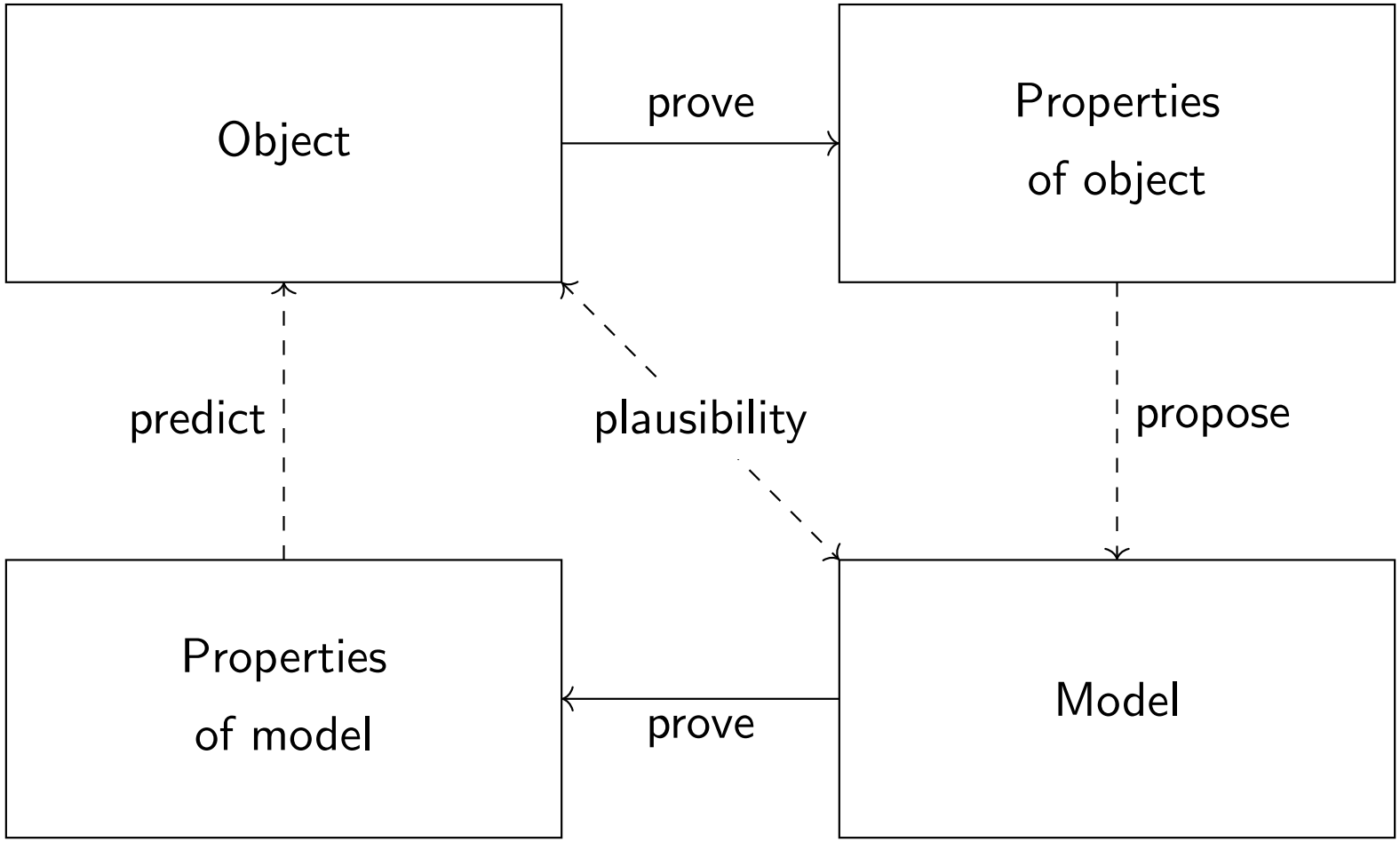
What do we not know?

- What is the average rank?
  - Probably $\frac{1}{2}$.
- How large can the rank be?
  - At least 28.
- Is the rank bounded?
  - Maybe?

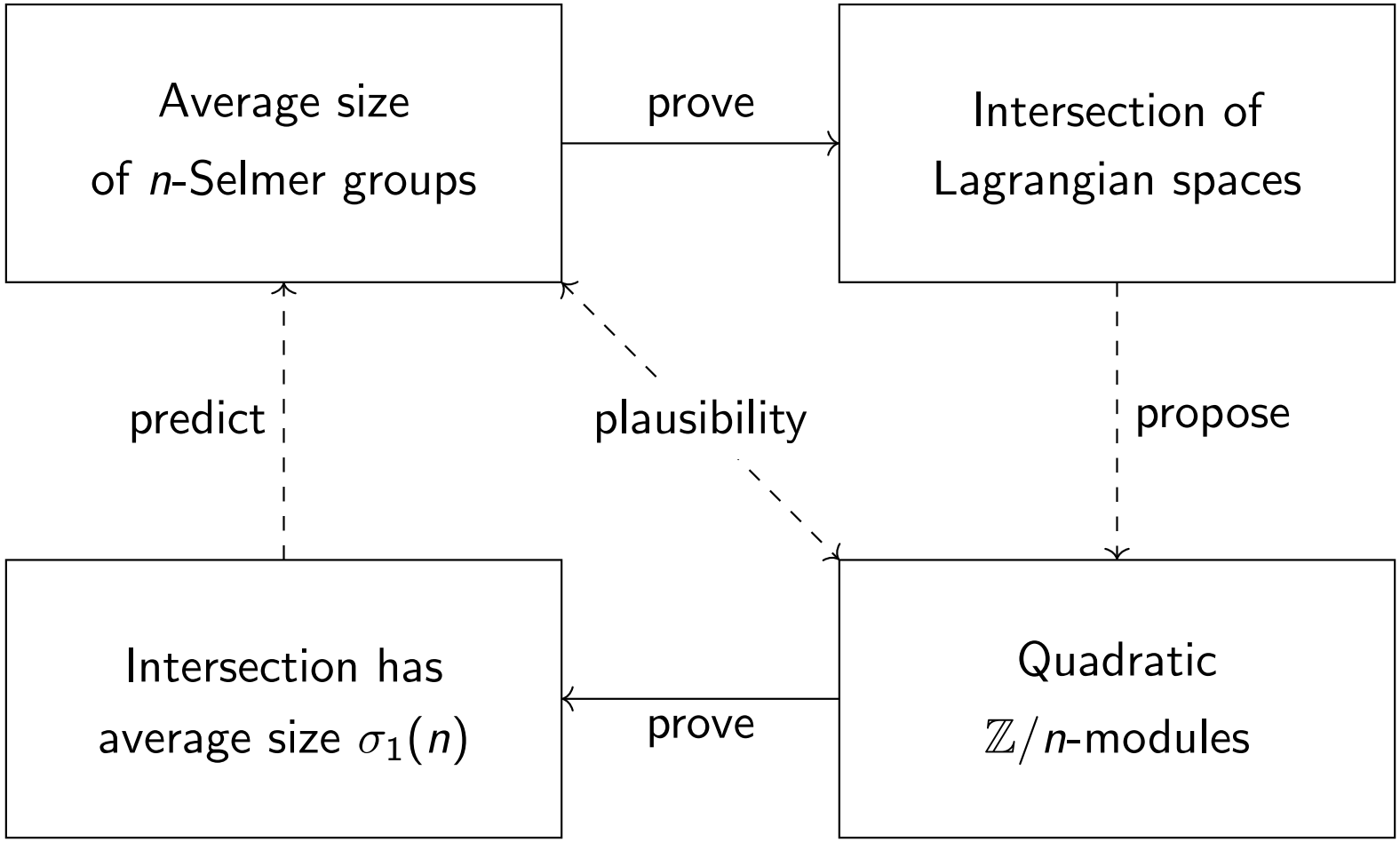
What can we do?

- Study Selmer groups and Tate–Shafarevich groups.
- Neither are easy to study.
- Study models for them instead.

Framework and overview



Framework and overview



Framework and overview

"Modelling the Selmer group, the Tate–Shafarevich group, and the Mordell–Weil rank of elliptic curves over number fields"

Theorem (1) (idea)

The n-Selmer group is usually the intersection of two Lagrangian spaces.

Theorem (2) (idea)

The intersection of two Lagrangian spaces should have average size $\sigma_1(n)$.

"All but finitely many rational elliptic curves have rank at most 21"

Preliminary background

Let E be an *elliptic curve* defined over a *number field* K.

- K is a finite extension of $\mathbb{Q}$ with a fixed algebraic closure $\overline{K}$.
- $E = E(\overline{K})$ is a smooth projective plane curve of genus one with a distinguished point $\mathcal{O} \in E(K)$.
- $\mathrm{Gal}(\overline{K}/K)$ acts on E with invariants $E(K)$.

Theorem (Mordell–Weil)

$E(K)$ is a finitely generated abelian group.

There is an isomorphism

$$E(K) \cong \mathrm{tor}(E/K) \times \mathbb{Z}^{\mathrm{rk}(E/K)}.$$

The **Mordell–Weil rank** is $\mathrm{rk}(E/K)$.

Preliminary background

Let E be an elliptic curve defined over a number field K.

Multiplying by $n \in \mathbb{N}^+$,

$$0 \to E[n] \to E \xrightarrow{[n]} E \to 0.$$

Applying $\mathrm{Gal}(\overline{K}/K)$ cohomology,

$$0 \longrightarrow E(K)[n] \longrightarrow E(K) \longrightarrow E(K) \xrightarrow{\delta} H^1(K, E[n]) \to H^1(K, E) \to H^1(K, E) \to \dots.$$

Truncating at $H^1(K, E[n])$,

$$0 \longrightarrow E(K)/n \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0.$$

Preliminary background

Let E be an elliptic curve defined over a number field K.

There is a short exact sequence

$$0 \to E(K)/n \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0.$$

Let K_v be a *completion* of K with respect to a norm $|\cdot|_v$. Similarly,

$$0 \to \prod_v E(K_v)/n \to \prod_v H^1(K_v, E[n]) \to \prod_v H^1(K_v, E)[n] \to 0.$$

There is a row-exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/n & \longrightarrow & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \lambda} & \overset{\sigma}{\searrow} & \downarrow{\scriptstyle \tau[n]} & & \\
0 & \to & \prod_v E(K_v)/n & \xrightarrow{\kappa} & \prod_v H^1(K_v, E[n]) & \to & \prod_v H^1(K_v, E)[n] & \to & 0.
\end{array}$$

Preliminary background

Let E be an elliptic curve defined over a number field K.

The n-**Selmer group** is

$$\mathrm{Sel}_n(K,E) = \ker(\sigma : H^1(K, E[n]) \to \textstyle\prod_v H^1(K_v, E)[n]).$$

By the first isomorphism theorem,

$$\mathrm{Sel}_n(K,E)/\ker\lambda \xrightarrow{\sim} \mathrm{im}\,\kappa \cap \mathrm{im}\,\lambda.$$

The **Tate–Shafarevich group** is

$$Ш(K,E) = \ker(\tau : H^1(K,E) \to \textstyle\prod_v H^1(K_v, E)).$$

There is an exact sequence

$$0 \to E(K)/n \to \mathrm{Sel}_n(K,E) \to Ш(K,E)[n] \to 0.$$

Arithmetic of Selmer groups

Theorem (1)

For almost all elliptic curves defined over a number field, the p^e-Selmer group is the intersection of two Lagrangian direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

- *Almost all*: limiting proportion when ordered by height.
- *Quadratic* module M: has a quadratic form $\omega : M \to \mathbb{Q}/\mathbb{Z}$.
- *Non-degenerate* M: $M \cong M^\star$.
- *Lagrangian* submodule N: $\omega(N) = 0$ and $N^\perp = N$.
- *Infinite rank*: in terms of generators.

Think of $M = (\mathbb{Z}/p^e)^{2n}$, equipped with hyperbolic quadratic form

$$(x_1, \ldots, x_n, y_1, \ldots, y_n) \mapsto \sum_{i=1}^{n} x_i y_i,$$

with Lagrangian submodule $N = (\mathbb{Z}/p^e)^n \oplus 0^n$.

Arithmetic of Selmer groups

Theorem (1)

For almost all elliptic curves defined over a number field, the p^e-Selmer group is the intersection of two Lagrangian direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

References:

- Colliot-Thélène, Skorobogatov, Swinnerton-Dyer (1998): $p^e = 2$ and finite-dimensional construction. [1]
- Bhargava, Kane, Lenstra, Poonen, Rains (2015): general p^e, infinite-rank construction, and generalisations to abelian varieties with arbitrary isogenies over arbitrary global fields. [2]

[1] J.-L. Colliot-Thelene, A. Skorobogatov and P. Swinnerton-Dyer. 'Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points'. In: Invent. Math. 134 (1998)

[2] M. Bhargava, D. Kane, H. Lenstra, B. Poonen and E. Rains. 'Modelling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves'. In: Camb. J. Math. 3 (2015)

Arithmetic of Selmer groups

Theorem (1)

For almost all elliptic curves defined over a number field, the p^e-Selmer group is the intersection of two Lagrangian direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

Sketch of proof.

Recall that $\mathrm{Sel}_n(K,E)/\ker\lambda \cong \mathrm{im}\,\kappa \cap \mathrm{im}\,\lambda$.

1. Construct the local non-degenerate quadratic module.
   - Construct Θ such that $0 \to \overline{K_v}^\times \to \Theta \to E[n] \to 0$.
   - Define $\mathrm{Ob}_{K_v} : H^1(K_v, E[n]) \to \mathrm{Br}(K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$.
   - Prove $\langle \cdot,\cdot \rangle_{\mathrm{Ob}_{K_v}} = [\cdot,\cdot] \circ \cup$, and deduce Ob_{K_v} is a quadratic form.
   - Show non-degeneracy using local duality.
2. Prove $\mathrm{im}\,\kappa$ and $\mathrm{im}\,\lambda$ are Lagrangian.
   - Prove basic properties of Brauer–Severi diagrams to redefine Ob_{K_v}.
   - Define $M = \overline{\prod_v} H^1(K_v, E[n])$ and $\mathfrak{q} = \sum_v \mathrm{inv}_{K_v} \circ \mathrm{Ob}_{K_v} : M \to \mathbb{Q}/\mathbb{Z}$.
   - Show $\mathrm{im}\,\kappa$ is Lagrangian using B–S diagrams and local duality.
   - Show $\mathrm{im}\,\lambda$ is Lagrangian using class field theory and global duality.

Arithmetic of Selmer groups

Theorem (1)

For almost all elliptic curves defined over a number field, the p^e-Selmer group is the intersection of two Lagrangian direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

Sketch of proof.

Recall that $\mathrm{Sel}_n(K,E)/\ker\lambda \cong \mathrm{im}\,\kappa \cap \mathrm{im}\,\lambda$.

1. Construct the local non-degenerate quadratic module.
2. Prove $\mathrm{im}\,\kappa$ and $\mathrm{im}\,\lambda$ are Lagrangian.
3. Prove $\mathrm{im}\,\kappa$ and $\mathrm{im}\,\lambda$ are direct summands.
   - Use infinite abelian group theory to characterise direct summands in terms of divisibility-preserving maps and apply global duality.
4. Attain good criterion for $\ker\lambda = 0$ when $n = p^e$.
   - Use Chebotarev's density theorem to reduce to $H^1_c(\mathrm{im}\,\rho_{E[n]}, E[n])$ and apply inflation-restriction repeatedly to reduce to $\mathrm{SL}_2(\mathbb{Z}/n)$.
   - Extract assumption $\mathrm{SL}_2(\mathbb{Z}/n) \leq \mathrm{im}\,\rho_{E[n]}$ and justify its ubiquity using Hilbert's irreducibility theorem and division polynomials. □

Model for Selmer groups

Theorem (2)

The average size of the intersection of two Lagrangian direct summands of the quadratic $\mathbb{Z}/p^e$-module $(\mathbb{Z}/p^e)^{2n}$ chosen uniformly at random tends to the sum of divisors σ_1 of p^e as $n \to \infty$.

- Theorem (1): the p^e-Selmer group is the intersections of two Lagrangian direct summands in $\overline{\prod_v} H^1(K_v, E[p^e])$.
- Theorem (2): the size of the intersection of two Lagrangian direct summands in $(\mathbb{Z}/p^e)^\infty$ has first moment $\sigma_1(p^e)$.
- On the other hand, $(\mathbb{Z}/p^e)^\infty$ is always free, while $\overline{\prod_v} H^1(K_v, E[p^e])$ is almost never free, by Hilbert's irreducibility theorem.

Reference:

- Poonen, Rains (2012): $e = 1$. [3]

[3] B. Poonen and E. Rains. 'Random maximal isotropic subspaces and Selmer groups'. In: J. Amer. Math. Soc 25 (2012)

Model for Selmer groups

Theorem (2)

The average size of the intersection of two Lagrangian direct summands of the quadratic $\mathbb{Z}/p^e$-module $(\mathbb{Z}/p^e)^{2n}$ chosen uniformly at random tends to the sum of divisors σ_1 of p^e as $n \to \infty$.

Sketch of proof.

1. Linear algebra of $(\mathbb{Z}/p^e)^{2n}$.
   - Show correspondence theorem for direct summands.
   - Count number of direct summands of fixed rank.
   - Obtain linear algebra for Lagrangian direct summands.
2. Lagrangian direct summands of $(\mathbb{Z}/p^e)^{2n}$.
   - Compute result for $n = 1$ explicitly.
   - Count fibres of $L \mapsto (L \cap N^{\perp} + N)/N$.
   - Extract rank one free submodule and apply induction.
3. Average size of $L_1 \cap L_2$.
   - Count number of injections $\mathbb{Z}/p^e \hookrightarrow L_1$.
   - Compute probability that L_2 contains image of $\mathbb{Z}/p^e \hookrightarrow L_1$.
   - Deduce result by telescoping argument. $\square$

Heuristic consequences

A model for n-Selmer groups.

- For almost all elliptic curves E defined over a number field K,

$$\mathrm{Sel}_n(K,E)[p^e] \cong \mathrm{Sel}_{p^e}(K,E), \qquad p^e \mid n.$$

- Derive linear algebra for $\mathbb{Z}/n$ and consider $(L_1 \cap L_2)[p^e]$.

A model for Mordell–Weil ranks and Tate–Shafarevich groups.

- Use

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \varinjlim_e \mathrm{Sel}_{p^e}(K,E) \to Ш(K,E)[p^\infty] \to 0.$$

- Consider

$$0 \to (L_1 \cap L_2) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to (L_1 \otimes \mathbb{Q}_p/\mathbb{Z}_p) \cap (L_2 \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to T \to 0.$$