Rank heuristics for elliptic curves [1]

Part III Seminar Series

David Kurniadi Angdinata

University of Cambridge

Friday, 4 December 2020

[1] partially based on the VaNTAGe seminar on 'Heuristics for the arithmetic of elliptic curves' by Bjorn Poonen on 1 September 2020

Elliptic curves

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

Theorem (Mordell–Weil)

$E(K)$ is a finitely generated abelian group of the form

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

The **torsion subgroup** $\mathrm{tor}(E/K)$ is effectively computable.

Theorem (Lutz–Nagell)

If $(x, y) \in \mathrm{tor}(E/\mathbb{Q})$, then $y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid \Delta(E/\mathbb{Q})$.

Theorem (Mazur, Kamienny, Merel)

There are finitely many possibilities for $\mathrm{tor}(E/K)$.

Elliptic curves

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

Theorem (Mordell–Weil)

$E(K)$ is a finitely generated abelian group of the form

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

The **rank** $\mathrm{rk}(E/K)$ is computationally harder and more mysterious.

Conjecture (Birch–Swinnerton-Dyer)

If $K = \mathbb{Q}$, then $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rk}(E/\mathbb{Q})$.

Theorem (Kolyvagin)

BSD holds for modular elliptic curves with analytic rank zero and one.

Rank distribution conjecture

How is the rank distributed?

Consider the set $\mathcal{E}(\mathbb{Q})$ of unique minimal representatives of isomorphism classes of elliptic curves over $\mathbb{Q}$, ordered by the height function

$$H(E : y^2 = x^3 + Ax + B) = \max(4|A|^3, 27|B|^2).$$

Conjecture (Rank distribution)

The average rank of $\mathcal{E}(\mathbb{Q})$ is $\frac{1}{2}$.

Theorem (Bhargava–Shankar 2015)

The average rank of $\mathcal{E}(\mathbb{Q})$ is at most $\frac{7}{6}$.

Combining these shows that BSD holds for a positive proportion of $\mathcal{E}(\mathbb{Q})$ (Kolyvagin 1989, Breuil–Conrad–Diamond–Taylor 2001, Nekovář 2009, Dokchitser–Dokchitser 2010, Skinner–Urban 2015).

Rank boundedness conjecture

Is the rank bounded? Probably not...

Conjecture (Rank boundedness)

There are $E \in \mathcal{E}(\mathbb{Q})$ *of arbitrarily large rank.*

Theorem (Shafarevich–Tate 1967, Ulmer 2002)

There are $E \in \mathcal{E}(\mathbb{F}_p(T))$ *of arbitrarily large rank.*

Theorem (Elkies 2006)

There is $E \in \mathcal{E}(\mathbb{Q})$ *with rank at least* 28.

Theorem (Elkies–Klagsbrun 2020)

There is $E \in \mathcal{E}(\mathbb{Q})$ *with rank exactly* 20.

Many proponents (Cassels 1966, Tate 1974, Mestre 1982, Silverman 1986, Brumer 1992, Ulmer 2002, Farmer–Gonek–Hughes 2007).

Rank boundedness conjecture

Is the rank bounded? Probably!

Conjecture (Poonen et al [2] [3] [4])

There are finitely many $E \in \mathcal{E}(\mathbb{Q})$ with rank greater than 21.

- Model p^e-Selmer groups using intersection of quadratic submodules.
- Model Tate–Shafarevich groups using matrices with a fixed rank.
- Model the Mordell–Weil rank using matrices without fixing the rank.

A few others also predict boundedness (Néron 1950, Honda 1960, Rubin–Silverberg 2000, Granville 2006, Watkins 2015).

---

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

[3] 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)

[4] J. Park, B. Poonen, J. Voight and M. Wood. 'A heuristic for boundedness of ranks of elliptic curves'. In: J. Eur. Math. Soc (2019)

The Selmer and Tate–Shafarevich groups

Multiplication by $n \in \mathbb{N}^+$ gives

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

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

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

Truncating at $H^1(K, E[n])$ gives a short exact sequence

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

Similarly, there are short exact sequences

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

The Selmer and Tate–Shafarevich groups

There is a row-exact commutative diagram

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

The n-**Selmer group** is

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

The **Tate–Shafarevich group** is

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

There is an exact sequence

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

Modelling p^e-Selmer groups

Theorem

For almost all $E \in \mathcal{E}(K)$, the p^e-Selmer group $\mathrm{Sel}_{p^e}(E/K)$ is the intersection of two maximal totally isotropic direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

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

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

with two MTIDS's $(\mathbb{Z}/p^e)^n \oplus 0^n$ and $0^n \oplus (\mathbb{Z}/p^e)^n$.

The result was known for a finite-dimensional vector space over $\mathbb{F}_2$ (Colliot-Thélène–Skorobogatov–Swinnerton-Dyer 2002).

Modelling p^e-Selmer groups

By the first isomorphism theorem,

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

Theorem

For almost all $E \in \mathcal{E}(K)$, the p^e-Selmer group $\mathrm{Sel}_{p^e}(E/K)$ is the intersection of two maximal totally isotropic direct summands in a non-degenerate quadratic $\mathbb{Z}/p^e$-module of infinite rank.

Conjecture

The distribution of $\mathrm{Sel}_{p^e}(E/\mathbb{Q})$ coincides with the distribution of $S_1 \cap S_2$ for two randomly chosen MTIDS's $S_1, S_2 \subseteq (\mathbb{Z}/p^e)^{2n}$ as $n \to \infty$.

- Variant for function fields is known (Feng–Landesman–Rains 2020).
- Variant for quadratic twist families over $\mathbb{Q}$ is known for $p^e = 2$ (Heath-Brown 1994, Swinnerton-Dyer 2008, Kane 2013).
- Average of $\#(S_1 \cap S_2)$ is $\sigma_1(p^e)$, and average of $\#\,\mathrm{Sel}_{p^e}(E/\mathbb{Q})$ is $\sigma_1(p^e)$ for $p^e \leq 5$ (Bhargava–Shankar 2013-2015).

Modelling short exact sequences

Recall that

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

Setting $n = p^e$ and taking direct limits gives

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

Randomly choosing two MTIDS's $S_1, S_2 \subseteq (\mathbb{Z}_p)^{2n}$ gives

$$0 \to \mathcal{R} \to \mathcal{S} \to \mathcal{T} \to 0,$$

where $\mathcal{R} = (S_1 \cap S_2) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $\mathcal{S} = (S_1 \otimes \mathbb{Q}_p/\mathbb{Z}_p) \cap (S_2 \otimes \mathbb{Q}_p/\mathbb{Z}_p)$.

- Both $\varinjlim_e \mathrm{Sel}_{p^e}(E/K)$ and $\mathcal{S}$ are compatible with p^e-parts.
- Both $Ш(E/K)[p^\infty]$ and $\mathcal{T}$ are finite with an alternating pairing.
- Both $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $\mathcal{R}$ satisfy the rank distribution conjecture.
- Variant for quadratic twist families is known for $p = 2$ (Smith 2020).

Modelling Tate–Shafarevich groups

The rank distribution conjecture gives

$$\mathbb{P}(\mathrm{rk}_{\mathbb{Z}_p}(S_1 \cap S_2) = 0) = \mathbb{P}(\mathrm{rk}_{\mathbb{Z}_p}(S_1 \cap S_2) = 1) = \frac{1}{2}.$$

If $r \geq 2$, then

$$\{S_1, S_2 \subseteq \mathbb{Z}_p^{2n} : \mathrm{rk}_{\mathbb{Z}_p}(S_1 \cap S_2) = r\}$$

has measure zero as $n \to \infty$.

Instead choose M randomly from

$$\{M \in \mathrm{Mat}_n \mathbb{Z}_p : M^{\mathsf{T}} = -M,\ \mathrm{rk}_{\mathbb{Z}_p}(\ker M) = r\}, \qquad n \equiv r \mod 2,$$

and let $n \to \infty$. Use distribution of $\mathrm{tor}(\mathrm{coker}\, M)$ to model $\mathcal{T}$.

- Coincides with original $\mathbb{Z}_p^{2n}$ distribution for $\mathcal{T}$ for rank zero and one.
- Coincides with Delaunay's distribution for $Ш(E/\mathbb{Q})[p^\infty]$ (Delaunay–Jouhet 2000-2014).

Modelling ranks

How to model an elliptic curve E over $\mathbb{Q}$ of height h?

- Choose functions $X : \mathbb{N} \to \mathbb{R}$ and $Y : \mathbb{N} \to \mathbb{R}$ such that

$$X(x)^{Y(x)} = x^{\frac{1}{12}+o(1)}, \qquad x \to \infty.$$

- Choose n randomly from $\{\lceil Y(h) \rceil, \lceil Y(h) \rceil + 1\}$.
- Choose M randomly from

$$\{M \in \operatorname{Mat}_n \mathbb{Z} : M^\intercal = -M,\ M_{ij} \leq X(h)\}.$$

- Model $Ш(E/\mathbb{Q})$ by $\operatorname{tor}(\operatorname{coker} M)$ and $\operatorname{rk}(E/\mathbb{Q})$ by $\operatorname{rk}_{\mathbb{Z}}(\ker M)$.

Conditions are chosen such that the average size of

$$\# \operatorname{coker}_0' M = \begin{cases} \# \operatorname{tor}(\operatorname{coker} M) & \text{if } \operatorname{rk}_{\mathbb{Z}}(\ker M) = 0, \\ 0 & \text{if } \operatorname{rk}_{\mathbb{Z}}(\ker M) > 0, \end{cases}$$

is $h^{1/12+o(1)}$. The same is predicted for $Ш(E/\mathbb{Q})$ by strong BSD.

Modelling ranks

Denote the model for $\mathrm{rk}(E/\mathbb{Q})$ by $\mathrm{rk}'(E/\mathbb{Q})$.

Theorem (Poonen et al)

The following hold with probability 1.

$$\#\{E \in \mathcal{E}(\mathbb{Q}) : H(E) \leq h,\ \mathrm{rk}'(E/\mathbb{Q}) = 0\} = h^{20/24+o(1)}$$
$$\#\{E \in \mathcal{E}(\mathbb{Q}) : H(E) \leq h,\ \mathrm{rk}'(E/\mathbb{Q}) = 1\} = h^{20/24+o(1)}$$
$$\#\{E \in \mathcal{E}(\mathbb{Q}) : H(E) \leq h,\ \mathrm{rk}'(E/\mathbb{Q}) \geq 2\} = h^{19/24+o(1)}$$
$$\vdots$$
$$\#\{E \in \mathcal{E}(\mathbb{Q}) : H(E) \leq h,\ \mathrm{rk}'(E/\mathbb{Q}) \geq 20\} = h^{1/24+o(1)}$$
$$\#\{E \in \mathcal{E}(\mathbb{Q}) : H(E) \leq h,\ \mathrm{rk}'(E/\mathbb{Q}) \geq 21\} \leq h^{o(1)}$$
$$\#\{E \in \mathcal{E}(\mathbb{Q}) : \mathrm{rk}'(E/\mathbb{Q}) > 21\} \text{ is finite.}$$