Heuristics for the arithmetic of elliptic curves

Bjorn Poonen

(based on joint papers with Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra jr., Jennifer Park, Eric Rains, John Voight, and Melanie Matchett Wood)

VaNTAGe on September 1, 2020

An elliptic curve E over $\mathbb{Q}$ is the closure in $\mathbb{P}^2$ of a smooth curve

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Q}$. (Smoothness amounts to $4A^3 + 27B^2 \neq 0$.)

An elliptic curve E over $\mathbb{Q}$ is the closure in $\mathbb{P}^2$ of a smooth curve

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Q}$. (Smoothness amounts to $4A^3 + 27B^2 \neq 0$.)

Who cares?

An elliptic curve E over $\mathbb{Q}$ is the closure in $\mathbb{P}^2$ of a smooth curve

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Q}$. (Smoothness amounts to $4A^3 + 27B^2 \neq 0$.)

Who cares?

I care, because they're

- the simplest varieties whose $\mathbb{Q}$-points are not fully understood,
- the simplest projective algebraic groups of dimension ≥ 1.

$E(\mathbb{Q})$ is an abelian group.

Rational points on elliptic curves

Theorem (Mordell 1922)

The abelian group $E(\mathbb{Q})$ is finitely generated.

Thus $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ for some $r \geq 0$ and finite abelian group T.

Theorem (Mazur 1977)

The possibilities for the torsion subgroup T are

- $\mathbb{Z}/m\mathbb{Z}$ *for* $m \leq 12$ *excluding* 11, *and*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *for* $n \leq 4$.

What about the rank $r := \operatorname{rk} E(\mathbb{Q})$?

Is the rank bounded?

Poincaré 1901: What are the possibilities for the rank?

Question

Is $\operatorname{rk} E(\mathbb{Q})$ *bounded as* E *varies over all elliptic curves over* $\mathbb{Q}$*?*

- Early authors conjectured YES: Néron 1950, Honda 1960.
- Later, most conjectured NO: Cassels 1966, Tate 1974, Mestre 1982, Silverman 1986, 2009, Brumer 1992, Ulmer 2002, Farmer–Gonek–Hughes 2007.
- Recent heuristics for YES: Rubin and Silverberg 2000, Granville 2006, Watkins 2015.

We will present a different heuristic, which models ranks, Selmer groups, and Shafarevich–Tate groups simultaneously and predicts that $\operatorname{rk} E(\mathbb{Q}) \leq 21$ for all but finitely many E (Granville/Watkins also suggested 21).

Each E is isomorphic to a unique one given by

$$y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ such that there is no prime p with $p^4 | A$ and $p^6 | B$.

- $\mathscr{E}$:= the set of such elliptic curves.
- all but finitely many E means all but finitely many $E \in \mathscr{E}$.
- height E := $\max(|4A^3|, |27B^2|)$ for each $E \in \mathscr{E}$.
- $\mathscr{E}_{\leq H} := \{E \in \mathscr{E} : \text{height } E \leq H\}$.

Proposition

$\#\mathscr{E}_{\leq H} \sim H^{5/6}$, ignoring constants.

Sketch of proof:

About $H^{1/3}$ choices for A, and about $H^{1/2}$ choices for B.

Selmer group

Let $n \geq 2$. Taking Galois cohomology of

$$0 \longrightarrow E[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

yields

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \xrightarrow{\text{global}} \mathrm{H}^1(\mathbb{Q}, E[n])$$

im(global)? Too hard.

Selmer group

Let $n \geq 2$. Taking Galois cohomology of

$$0 \longrightarrow E[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

yields

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \arrow[r, "\text{global}"] \arrow[d] & \mathrm{H}^1(\mathbb{Q}, E[n]) \arrow[d] \\
0 \arrow[r] & \dfrac{E(\mathbb{Q}_p)}{nE(\mathbb{Q}_p)} \arrow[r, "\text{local}"] & \mathrm{H}^1(\mathbb{Q}_p, E[n])
\end{tikzcd}$$

im(global)? Too hard.
im(local)? Easier.

Selmer group

Let $n \geq 2$. Taking Galois cohomology of

$$0 \longrightarrow E[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

yields

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \arrow[r, "\text{global}"] \arrow[d] & \mathrm{H}^1(\mathbb{Q}, E[n]) \arrow[d] \\
0 \arrow[r] & \displaystyle\prod_{p \leq \infty} \frac{E(\mathbb{Q}_p)}{nE(\mathbb{Q}_p)} \arrow[r, "\text{local}"] & \displaystyle\prod_{p \leq \infty} \mathrm{H}^1(\mathbb{Q}_p, E[n])
\end{tikzcd}$$

im(global)? Too hard.
im(local)? Easier.

Selmer group

Let $n \geq 2$. Taking Galois cohomology of

$$0 \longrightarrow E[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

yields

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \arrow[r, "\text{global}"] \arrow[d] & \mathrm{H}^1(\mathbb{Q}, E[n]) \arrow[d, "\beta"'] \\
0 \arrow[r] & \prod_{p \leq \infty} \dfrac{E(\mathbb{Q}_p)}{nE(\mathbb{Q}_p)} \arrow[r, "\text{local}"] & \prod_{p \leq \infty} \mathrm{H}^1(\mathbb{Q}_p, E[n])
\end{tikzcd}$$

im(global)? Too hard.
im(local)? Easier.
$\mathrm{Sel}_n\, E := \{c : \beta(c) \in \mathrm{im}(\text{local})\}$ is an upper bound for $\dfrac{E(\mathbb{Q})}{nE(\mathbb{Q})}$.

Selmer groups and Shafarevich–Tate groups

For each E, one has

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \underbrace{\operatorname{Sel}_n E}_{n\text{-Selmer group}} \longrightarrow \underbrace{\text{Ш}[n]}_{\substack{n\text{-torsion of the} \\ \text{Shafarevich–Tate group}}} \longrightarrow 0.$$

Setting $n = p^e$ and taking $\varinjlim_e$ yields

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \operatorname{Sel}_{p^\infty} E \longrightarrow \text{Ш}[p^\infty] \longrightarrow 0.$$

We will model these sequences.

Model for $\mathrm{Sel}_p\, E$

Equip $V_n := \mathbb{F}_p^{2n}$ with the quadratic form

$$Q(x_1, \ldots, x_n, y_1, \ldots, y_n) := x_1 y_1 + \cdots + x_n y_n.$$

Call a subspace $Z \subseteq V_n$ maximal isotropic if $Q|_Z = 0$ and $Z^\perp = Z$.

Conjecture (P.–Rains 2012)

The distribution of $\dim \mathrm{Sel}_p\, E$ *as* E *ranges over* $\mathscr{E}$ *equals*
$\lim_{n\to\infty}$ *of the distribution of* $\dim(Z \cap W)$
for random maximal isotropic subspaces Z, W *of* V_n.

Lots of reasons to believe this:

- A variant for many quadratic twist families is proved for $p = 2$ (Heath-Brown 1994, Swinnerton-Dyer 2008, Kane 2013).
- $\mathrm{Sel}_p\, E$ is an intersection of two maximal isotropic subgroups (P.–Rains 2012).
- Compatible with de Jong 2002 and Bhargava–Shankar 2015– theorems on Average($\#\,\mathrm{Sel}_n$).
- "Large q limit" function field variant proved (Feng–Landesman–Rains 2020$^+$).

From Sel_p to Sel_{p^e} and Sel_{p^∞}

BKLPR 2015: Generalizing leads to

- a conjectural distribution for $\mathrm{Sel}_{p^e} E$;
- a conjectural distribution for the whole sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0;$$

- for each $r \geq 0$, a conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$, in terms of $\mathrm{coker}(A)_{\mathrm{tors}}$ for a random matrix $A \in \mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ conditioned on $\mathrm{rk}(\ker A) = r$.

Reasons to believe these:

- Compatible with conjectures of Delaunay & Jouhet 2000–2014.
- A variant for many quadratic twist families is proved for $p = 2$ (Alexander Smith 2020^+).

From Sel_p to Sel_{p^e} and Sel_{p^∞}

BKLPR 2015: Generalizing leads to

- a conjectural distribution for $\mathrm{Sel}_{p^e} E$;
- a conjectural distribution for the whole sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0;$$

- for each $r \geq 0$, a conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$, in terms of $\operatorname{coker}(A)_{\mathrm{tors}}$ for a random matrix $A \in \mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ conditioned on $\operatorname{rk}(\ker A) = r$.

Reasons to believe these:

- Compatible with conjectures of Delaunay & Jouhet 2000–2014.
- A variant for many quadratic twist families is proved for $p = 2$ (Alexander Smith 2020$^+$).

How to model an elliptic curve E of height H

Using growing functions $\eta(H)$ and $X(H)$ to be specified later,

1. Choose $n \in \mathbb{Z}_{>0}$ of size about $\eta(H)$ of random parity.
2. Choose random $A_E \in \mathrm{M}_n(\mathbb{Z})_{\mathrm{alt}}$ with $|\text{entries}| \leq X(H)$.
3. Define random variables

$$Ш'_E := (\operatorname{coker} A)_{\mathrm{tors}} \quad \text{and} \quad \mathrm{rk}'_E := \mathrm{rk}_{\mathbb{Z}}(\ker A).$$

These are supposed to model $Ш(E)$ and $\mathrm{rk}\, E(\mathbb{Q})$.

The functions $\eta(H)$ and $X(H)$ are chosen so that

$$X(H)^{\eta(H)} = H^{1/12+o(1)};$$

it turns out that this ensures that for rank 0 curves, the averages of $Ш'_E$ and $Ш(E)$ match (conditionally on standard conjectures).

Consequences of the model

Theorem (Park–P.–Voight–Wood 2019)

The following hold with probability 1*:*

$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E = 0\} = H^{20/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E = 1\} = H^{20/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 2\} = H^{19/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 3\} = H^{18/24+o(1)}$$
$$\vdots$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 20\} = H^{1/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 21\} \leq H^{o(1)},$$
$$\#\{E \in \mathscr{E} : \mathrm{rk}'_E > 21\} \text{ is finite.}$$

For comparison: Elkies found

- infinitely many elliptic curves of rank at least 19, and
- one elliptic curve of rank at least 28.

Elliptic curves with prescribed torsion subgroup

torsion subgroup	# curves	our rank bound	known example
trivial	$H^{5/6}$	21	19
$\mathbb{Z}/2\mathbb{Z}$	$H^{1/2}$	13	11
$\mathbb{Z}/3\mathbb{Z}$	$H^{1/3}$	9	7
$\mathbb{Z}/4\mathbb{Z}$	$H^{1/4}$	7	6
$\mathbb{Z}/5\mathbb{Z}$	$H^{1/6}$	5	4
$\mathbb{Z}/6\mathbb{Z}$	$H^{1/6}$	5	5
$\mathbb{Z}/7\mathbb{Z}$	$H^{1/12}$	3	2
$\mathbb{Z}/8\mathbb{Z}$	$H^{1/12}$	3	3
$\mathbb{Z}/9\mathbb{Z}$	$H^{1/18}$	2	1
$\mathbb{Z}/10\mathbb{Z}$	$H^{1/18}$	2	1
$\mathbb{Z}/12\mathbb{Z}$	$H^{1/24}$	2	1
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$H^{1/3}$	9	8
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$H^{1/6}$	5	5
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$H^{1/12}$	3	3
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$H^{1/24}$	2	1

Summary

- Heuristics for Selmer groups led to a model for the complete package consisting of ranks, Selmer groups, and Shafarevich–Tate groups.
- Many aspects of the model are supported by theorems.
- In the model, the pseudo-ranks of all but finitely many elliptic curves over $\mathbb{Q}$ are bounded by 21.
- This suggests that $\operatorname{rk} E(\mathbb{Q})$ is uniformly bounded as E varies.

Also,

- Similar heuristics may apply to elliptic curves over global fields, after excluding curves definable over proper subfields.
- Similar heuristics may apply to abelian varieties of fixed dimension over a fixed number field.

Elliptic curves over global fields: heuristics

- K: a global field
- $\mathscr{E}_K$: a set of representatives for the isomorphism classes of elliptic curves over K
- $B_K := \limsup_{E \in \mathscr{E}_K} \operatorname{rk} E(K)$.

Example

Our heuristic predicts $20 \leq B_{\mathbb{Q}} \leq 21$.

A naive adaptation of our heuristic would suggest that

$$20 \leq B_K \leq 21 \text{ for every global field } K.$$

Question

How does this compare with reality?

Not well...

Elliptic curves over global fields: reality

Theorem (Tate–Shafarevich 1967, Ulmer 2002)

If K is a global function field, then $B_K = \infty$.

Even for number fields, B_K can be arbitrarily large
(but maybe still always finite):

Theorem (Park–P.–Voight–Wood)

There exist number fields K of arbitrarily high degree such that $B_K \geq [K : \mathbb{Q}]$.

Number fields for which B_K is large include

- number fields in anticyclotomic towers and
- certain multiquadratic fields.

Elliptic curves over global fields: reconciliation

Question

How do we explain the differences between our heuristic and reality?

The elliptic curves of high rank used to prove that B_K is large for some K are special in that they are definable over a proper subfield of K. Exclude them!

- $\mathscr{E}_K^\circ$: the set of $E \in \mathscr{E}_K$ such that
  E is not a base change of a curve from a proper subfield.
- $B_K^\circ := \limsup_{E \in \mathscr{E}_K^\circ} \operatorname{rk} E(K)$.

Speculation

It is possible that $B_K^\circ < \infty$ for every global field K.

On the other hand, it is not true that $B_K^\circ \leq 21$ for all number fields: Shioda's rank 68 elliptic curve $y^2 = x^3 + t^{360} + 1$ over $\mathbb{C}(t)$ specializes to show that $B_K^\circ \geq 68$ for many number fields K.

Abelian varieties

Question

For abelian varieties A over number fields K, is there a bound on $\operatorname{rk} A(K)$ depending only on $\dim A$ and $[K:\mathbb{Q}]$?

- Fix g. By restriction of scalars and Zarhin's trick, one reduces to considering one algebraic family $\mathcal{F}_g$ of principally polarized abelian varieties over $\mathbb{Q}$.
- Define the height of $A \in \mathcal{F}_g$ in terms of coefficients of defining polynomials.
- The number of abelian varieties in $\mathcal{F}_g$ of height $\leq H$ is bounded by a polynomial in H.
- If, as for elliptic curves, there is a model involving a pseudo-rank rk'_A such that $\operatorname{Prob}(\operatorname{rk}'_A \geq r)$ gets divided by at least a fixed fractional power of H each time r is incremented by 1, then the pseudo-ranks are bounded with probability 1.
- Thus maybe actual ranks are bounded too.

Guess: YES!