The geometric average size of Selmer groups

Aaron Landesman

Stanford University

AMS Special Session on Stability in Topology, Arithmetic, and Representation Theory
The Ether

Ranks of elliptic curves

Theorem (Mordell-Weil)

Let E be an elliptic curve over a global field K (such as $\mathbb{Q}$ or $\mathbb{F}_q(t)$). Then the group of K-rational points $E(K)$ is a finitely generated abelian group.

For E an elliptic curve over K, write $E(K) \simeq \mathbb{Z}^r \oplus T$ for T a finite group. Then, r is the **rank** of E.

Question

What is the average rank of an elliptic curve?

Motivation

Conjecture (Minimalist Conjecture)

The average rank of elliptic curves is $1/2$. Moreover,

- 50% of curves have rank 0,
- 50% have rank 1,
- 0% have rank more than 1.

Goal

Explain why this holds, in an appropriate large q limit.

Definition of Selmer group

Let $K = \mathbb{F}_q(t)$, let E an elliptic curve over K, let $\mathscr{E}^0$ be the identity component of the Néron model for E over $\mathbb{P}^1_{\mathbb{F}_q}$ and let $\mathscr{E}^0[n]$ denote the n-torsion of $\mathscr{E}$.

Definition (non-standard)

The n-**Selmer** group of E is

$$\mathrm{Sel}_n(E) := H^1(\mathbb{P}^1_{\mathbb{F}_q}, \mathscr{E}^0[n])$$

Selmer group and rank

Lemma

The $\mathbb{Z}/n$ *rank of* $\mathrm{Sel}_n(E) = H^1(\mathbb{P}^1_{\mathbb{F}_q}, \mathscr{E}^0[n])$ *is an upper bound for the rank of* E*.*

Proof.

From the definition of Néron model, the rank of $H^0(\mathbb{P}^1, \mathscr{E}^0)$ as an abelian group agrees with the rank of E.

□

Average size of Selmer groups

Say $E/\mathbb{F}_q(t)$ is in minimal Weierstrass form given by

$$y^2z = x^3 + A(s,t)xz^2 + B(s,t)z^3,$$

(so $\operatorname{char}\mathbb{F}_q > 3$,) where there exists d so that $A(s,t)$ and $B(s,t)$ are homogeneous polynomials in $\mathbb{F}_q[s,t]$ of degrees $4d$ and $6d$. The **height** of E is

$$h(E) := d.$$

Definition

The **average size** of the n-Selmer group of height up to d is

$$\operatorname{Average}^{\leq d}(\#\operatorname{Sel}_n/\mathbb{F}_q(t)) := \frac{\sum_{E/\mathbb{F}_q(t),h(E)\leq d}\#\operatorname{Sel}_n(E)}{\#\{E/\mathbb{F}_q(t)\colon h(E)\leq d\}},$$

where the sum runs over isomorphism classes of elliptic curves $E/\mathbb{F}_q(t)$, having $h(E)\leq d$.

Conjecture on the average size of Selmer groups

Conjecture (Bhargava–Shankar and Poonen–Rains)

When all elliptic curves are ordered by height,

$$\lim_{q\to\infty}\lim_{d\to\infty} \text{Average}^{\leq d}(\#\,\text{Sel}_n\,/\mathbb{F}_q(t)) = \sum_{s|n} s.$$

Remark

- An analogous statement over $\mathbb{Q}$ (without a limit in q) was shown for $n = 2, 3, 4, 5$ by Bhargava and Shankar.
- The upper bound was shown for $n = 3$ over $\mathbb{F}_q(t)$ by de Jong.
- This was shown for $n = 2$ more generally over function fields by Ho, Le Hung, and Ngo.

Main result

We can try to approach the conjecture by reversing the limits.

Conjecture:
$$\lim_{q\to\infty} \lim_{d\to\infty} \frac{\sum_{E/\mathbb{F}_q, h(E)\le d} \# \operatorname{Sel}_n(E)}{\# \{E : h(E) \le d\}} = \sum_{s|n} s.$$

Limits reversed:
$$\frac{\sum_{E/\mathbb{F}_q, h(E)\le d} \# \operatorname{Sel}_n(E)}{\# \{E : h(E) \le d\}} = \sum_{s|n} s.$$

Theorem (L.)

For $n \geq 1$ and $d \geq 2$,

$$\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \operatorname{Average}^{\le d}(\# \operatorname{Sel}_n / \mathbb{F}_q(t)) = \sum_{s|n} s.$$

The Distribution of Selmer groups

Theorem (L.)

For $n \geq 1$ and $d \geq 2$,

$$\lim_{\substack{q \to \infty \\ \gcd(q,2n)=1}} \text{Average}^{\leq d}(\#\,\mathrm{Sel}_n\,/\mathbb{F}_q(t)) = \sum_{s|n} s.$$

Remark

More generally, Bhargava, Kane, Lenstra, Poonen, and Rains have conjectures predicting the full distribution. With Tony Feng and Eric Rains, we have proven their predictions in the large q limit as above.

In particular, we recover the minimalist conjecture (that the average rank of elliptic curves is $1/2$) in the large q limit.

Proof overview

Theorem (L)

For $n \geq 1$ and $d \geq 2$,

$$\lim_{\substack{q \to \infty \\ \gcd(q,2n)=1}} \text{Average}^{\leq d}(\# \, \text{Sel}_n \, / \mathbb{F}_q(t)) = \sum_{s|n} s.$$

Proof overview:

(1) Construct a space $\mathrm{Sel}_{n,k}^d$ parameterizing n-Selmer elements of elliptic curves of height d over k.

(2) By Lang-Weil, the average size of the n-Selmer group is the number of components of $\mathrm{Sel}_{n,k}^d$

(3) Compute the number of components of $\mathrm{Sel}_{n,k}^d$ by viewing it as a finite cover of the moduli of height d elliptic curves, and computing the monodromy.

Proof sketch

For k a finite field, construct a space $\mathrm{Sel}_{n,k}^{d}$ parameterizing pairs (E, X), where E is an elliptic curve over $k(t)$ and X is an n-Selmer element of E. Let $\mathscr{W}_k^d$ denote a parameter space for Weierstrass equations of elliptic curves $E/k(t)$ of height d.

The total number of Selmer elements over varying elliptic curves over $k(t)$ is $\mathrm{Sel}_{n,k}^{d}(k)$, so we are reduced to computing

$$\frac{\#\mathrm{Sel}_{n,k}^{d}(k')}{\#\mathscr{W}_k^d(k')}$$

for large finite extensions k' of k.

Proof sketch, continued

We want to compute

$$\frac{\#\mathrm{Sel}^d_{n,k}(k')}{\#\mathscr{W}^d_k(k')}.$$

Theorem (Lang-Weil)

For X a finite type space over $\mathbb{F}_p$ with r geometrically irreducible components, $\lim_{q\to\infty} X(\mathbb{F}_q) = rq^{\dim X} + O(q^{\dim X - 1/2})$*.*

So,

$$\begin{aligned}\frac{\#\mathrm{Sel}^d_{n,k}(k')}{\#\mathscr{W}^d_k(k')} &= \frac{\#\text{components of } \mathrm{Sel}^d_{n,k}}{\#\text{components of } \mathscr{W}^d_k} \\ &= \frac{\#\text{components of } \mathrm{Sel}^d_{n,k}}{1} \\ &= \#\text{components of } \mathrm{Sel}^d_{n,k}.\end{aligned}$$

Proof sketch, continued

To complete the proof, we want to show

$$\#\text{components of } \mathrm{Sel}^d_{n,k} = \sum_{s|n} s.$$

Let ${\mathscr{W}^\circ}^d_k \subset \mathscr{W}^d_k$ be the dense open parameterizing smooth Weierstrass models. Set up the fiber square

$$\begin{array}{ccc} {\mathrm{Sel}^\circ}^d_{n,k} & \longrightarrow & \mathrm{Sel}^d_{n,k} \\ \big\downarrow{\scriptstyle \pi^\circ} & & \big\downarrow{\scriptstyle \pi} \\ {\mathscr{W}^\circ}^d_k & \longrightarrow & \mathscr{W}^d_k. \end{array}$$

The resulting map π° is finite étale. Hence, we obtain a monodromy representation

$$\rho^d_k(n) : \pi_1^{\text{ét}}({\mathscr{W}^\circ}^d_k) \to \mathrm{GL}(V^d_{n,k}).$$

Proof sketch, continued

Recall we are trying to compute #components of $\mathrm{Sel}^{\circ d}_{n,k}$, which is a finite étale cover of $\mathscr{W}^{\circ d}_{k}$ with monodromy representation

$$\rho^d_k(n) : \pi_1^{\text{ét}}(\mathscr{W}^{\circ d}_{k}) \to \mathsf{GL}(V^d_{n,k}).$$

Therefore, the number of components is the number of orbits of $\operatorname{im} \rho^d_k(n)$.

Proof sketch, continued

Recall we are trying to compute #components of $\mathrm{Sel}^{\circ d}_{n,k}$, which is a finite étale cover of $\mathscr{W}^{\circ d}_{k}$ with monodromy representation

$$\rho^d_k(n) : \pi_1^{\text{ét}}(\mathscr{W}^{\circ d}_k) \to \mathrm{GL}(V^d_{n,k}).$$

Therefore, the number of components is the number of orbits of $\operatorname{im} \rho^d_k(n)$.

Theorem

For n prime, there is a quadratic form q^d_n on $V^d_{n,k}$ so that, up to index 2, $\operatorname{im} \rho^d_k(n) = O(q^d_n)$.

For n is prime, there are $n+1$ orbits of $O(q^d_n)$, corresponding to the n level sets of q^d_n, along with the 0 vector. We find that for n prime,

$$\#\text{components of } \mathrm{Sel}^{\circ d}_{n,k} = \#\text{orbits of } O(q^d_n) = n+1 = \sum_{s \mid n} s.$$