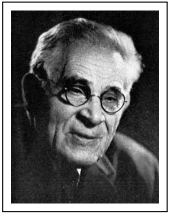
Ranks of Elliptic Curves

Why Ranks are (Almost Certainly) Bounded

Syracuse University Algebra Seminar

Caleb McWhorter
Syracuse University

March 22, 2019



1888 – 1972

"Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."

– L.J. Mordell, 1922

Definition (Elliptic Curve)

An elliptic curve is...

(i) a smooth projective curve of genus 1 (with $\mathcal{O}$).

(ii) a compact Riemann surface of genus 1.

(iii) an abelian variety of dimension one.

(iv) a nonempty smooth variety $V(F)$, where $\deg F = 3$.

(v) for fixed A, B with $-16(4A^3 + 27B^2) \neq 0$, the set

$$E_{A,B} := \{(x,y) \colon y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

with an addition law $\oplus$.

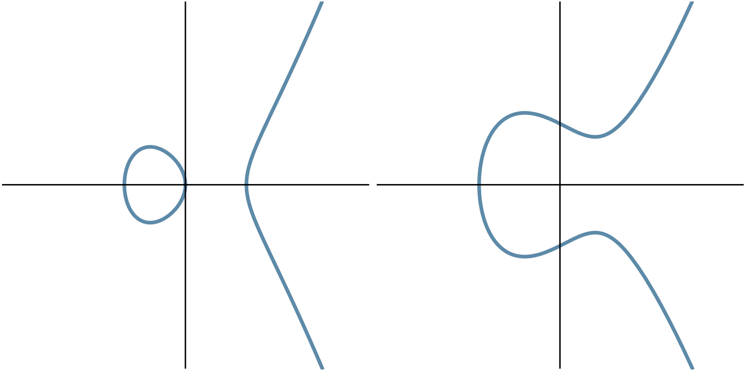
Given an elliptic curve

$$E_{A,B} : y^2 = x^3 + Ax + B$$

We also define…

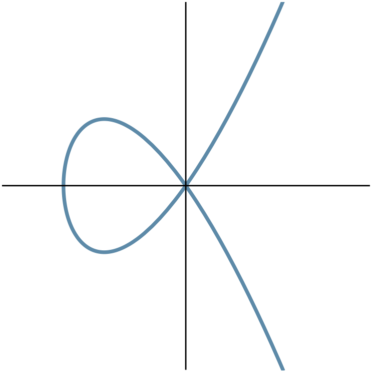
- Discriminant: $\Delta := -16(4A^3 + 27B^2)$
- j-Invariant: $j := -1728 \, \dfrac{(4A)^3}{\Delta}$

Examples

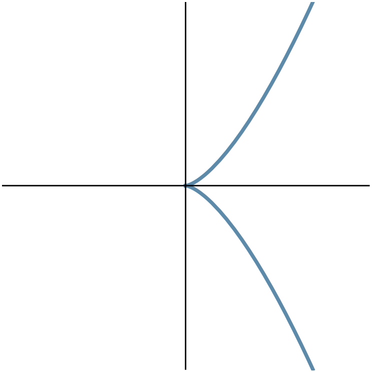


(a) $y^2 = x(x^2 + 1)$

(b) $y^2 = x^3 - x + 1$

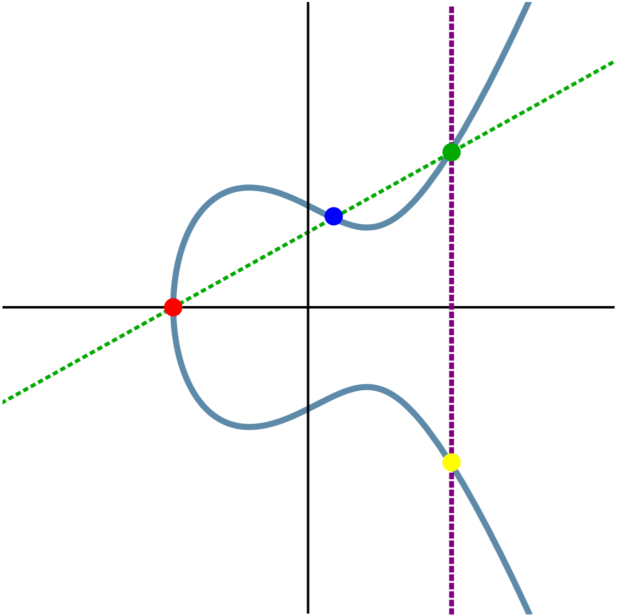


(c) $y^2 = x^2(x+2)$



(d) $y^2 = x^3$

Addition Law (Geometric Version)

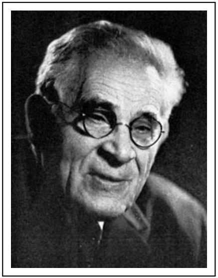


Theorem (Mordell, 1922)

Let $E/\mathbf{Q}$ be an elliptic curve. Then the group of rational points on E, denoted $E(\mathbf{Q})$ is a finitely generated abelian group. In particular,

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{tors}$$

where $r \geq 0$ is the rank and $E(\mathbf{Q})_{tors}$ is the set of points with finite order.



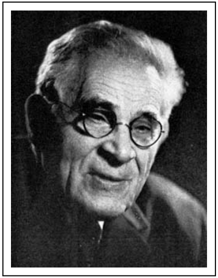
Louis J. Mordell
1888 – 1972

Theorem (Mordell–Weil, 1928)

Let K be a number field and A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbf{Z}^{r_{A/K}} \oplus A(K)_{tors}$$

where $r_{A/K} \geq 0$ is the rank and $A(K)_{tors}$ is the set of points with finite order.



Louis J. Mordell
1888 – 1972

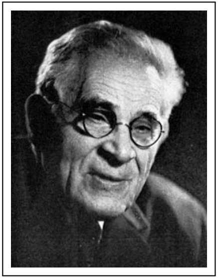
André Weil
1906 – 1998

Theorem (Mordell–Weil–Néron, 1952)

Let K be a field that is finitely generated over its prime field and A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbf{Z}^{r_{A/K}} \oplus A(K)_{tors}$$

where $r_{A/K} \geq 0$ is the rank and $A(K)_{tors}$ is the set of points with finite order.



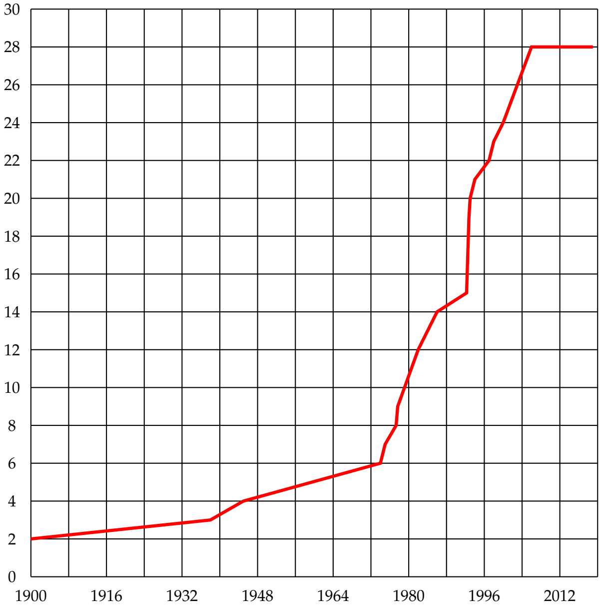
Louis J. Mordell
1888 – 1972

André Weil
1906 – 1998

André Néron
1922 – 1985

What are the possible ranks of elliptic curves $E/\mathbf{Q}$?

Rank	*Year*	*Due To*
3	1938	Billing
4	1945	Wiman
6	1974	Penney/Pomerance
7	1975	Penney/Pomerance
8	1977	Grunewald/Zimmert
9	1977	Brumer/Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao/Kouya
22	1997	Fermigier
23	1998	Martin/McMillen
24	2000	Martin/McMillen
28	2006	Elkies


30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
1900
1916
1932
1948
1964
1980
1996
2012

Are the ranks of elliptic curves $E/\mathbf{Q}$ unbounded?

What is the 'average' rank of elliptic curves $E/\mathbf{Q}$?

What does ‘average’ mean here?

Probabilities with Infinite Sets

Probabilities with Infinite Discrete Sets

$\mathcal{A}$:= Some property
S_n := set of objects up to size n.
A_n := set of objects in S with property $\mathcal{A}$ in S_n.

$$P(\mathcal{A}) = \lim_{n\to\infty} \frac{|A_n|}{|S_n|}$$

Example (*Probability that positive integer is even*)

Example (*Probability that positive integer is even*)

We expect $P(\text{Even}) = \frac{1}{2}$.

Example (*Probability that positive integer is even*)

We expect $P(\text{Even}) = \frac{1}{2}$.

$\mathcal{A} = \text{Integer even}$
$S_n := \{1, 2, \ldots, n\}$
$A_n := \{2, 4, \ldots\}$

Consider the counting numbers up to $n > 2$. We have n counting numbers and $n/2 - \epsilon_n$ of them are even.

Example (*Probability that positive integer is even*)

We expect $P(\text{Even}) = \frac{1}{2}$.

$\mathcal{A} = \text{Integer even}$
$S_n := \{1, 2, \ldots, n\}$
$A_n := \{2, 4, \ldots\}$

Consider the counting numbers up to $n > 2$. We have n counting numbers and $n/2 - \epsilon_n$ of them are even.

$$P(\text{Even}) = \lim_{n \to \infty} \frac{|A_n|}{|S_n|} = \lim_{n \to \infty} \frac{n/2 - \epsilon_n}{n} = \lim_{n \to \infty} \left(\frac{1}{2} - \frac{\epsilon_n}{n} \right) = \frac{1}{2}$$

Example (*Probability positive integer is prime*)

Example (*Probability positive integer is prime*)

$\mathcal{A}$ = Integer prime
$S_n := \{1, 2, \ldots, n\}$
$A_n := \{2, 3, \ldots\}$

By the Prime Number Theorem: $\pi(n) \sim \frac{n}{\log n}$.

Example (*Probability positive integer is prime*)

$\mathcal{A}$ = Integer prime
$S_n := \{1, 2, \ldots, n\}$
$A_n := \{2, 3, \ldots\}$

By the Prime Number Theorem: $\pi(n) \sim \frac{n}{\log n}$.

$$P(\text{Prime}) = \lim_{n\to\infty} \frac{|A_n|}{|S_n|} = \lim_{n\to\infty} \frac{\pi(n)}{n} \approx \lim_{n\to\infty} \frac{1}{\log n} = 0$$

Example (*Probability positive integer is prime*)

$\mathcal{A} =$ Integer prime
$S_n := \{1, 2, \ldots, n\}$
$A_n := \{2, 3, \ldots\}$

By the Prime Number Theorem: $\pi(n) \sim \frac{n}{\log n}$.

$$P(\text{Prime}) = \lim_{n\to\infty} \frac{|A_n|}{|S_n|} = \lim_{n\to\infty} \frac{\pi(n)}{n} \approx \lim_{n\to\infty} \frac{1}{\log n} = 0$$

Remark. For infinite sets $P(A) = 0$ does not mean A cannot occur.

Challenge: What is the probability that two random positive integers are coprime?

We proceed the same way for average size.

Example (*Average size of a positive integer*)

Example (*Average size of a positive integer*)

$$\lim_{n\to\infty} \frac{1+2+\cdots+n}{n} = \lim_{n\to\infty} \frac{n(n-1)/2}{n} = \lim_{n\to\infty} \frac{n-1}{2} = \infty$$

Frivolous Theorem of Arithmetic

Theorem (Steinbach, 1990)

Almost all natural numbers are very, very, very large.

We need two things:

- A notion of ‘size’ for elliptic curves.
- A way of counting the number of elliptic curves up to a given ‘size.’

Fact. Any elliptic curve $E/\mathbf{Q}$ is isomorphic to an elliptic curve of the form

$$E_{A,B} \colon y^2 = x^3 + Ax + B.$$

where $A, B \in \mathbf{Z}$.

Fact. Any elliptic curve $E/\mathbf{Q}$ is isomorphic to an elliptic curve of the form

$$E_{A,B}\colon y^2 = x^3 + Ax + B.$$

where $A, B \in \mathbf{Z}$.

In fact, $E/\mathbf{Q}$ is isomorphic to a unique $E_{A,B}$ if we require that if $p^4 \mid A$ then $p^6 \nmid B$.

There are many notions of ‘size’ (a.k.a. complexity) of an elliptic curve $E_{A,B} := y^2 = x^3 + Ax + B$:

- Naïve Height: $H(E_{A,B}) := \max\{|A|^3, |B|^2\}$

- Falting’s Height

- Discriminant, Δ_E: $\Delta(E_{A,B}) := -16(4A^3 + 27B^2)$

- Conductor, $N_E := \prod_{p \text{ prime}} p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & E \text{ has good reduction at } p \\ 1, & E \text{ has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p \end{cases}$$

Fun Aside

Conjecture (Szpiro)

For every $\epsilon > 0$, there exists a κ_ϵ such that for all elliptic curves $E/\mathbf{Q}$

$$|\Delta_E| \leq \kappa_\epsilon N_E^{6+\epsilon}.$$

Fun Aside

Conjecture (Szpiro)

For every $\epsilon > 0$, there exists a κ_ϵ such that for all elliptic curves $E/\mathbf{Q}$

$$|\Delta_E| \leq \kappa_\epsilon N_E^{6+\epsilon}.$$

Conjecture (ABC Conjecture, Masser–Oesterlé)

For every $\epsilon > 0$, there exists a constant κ_ϵ such that for all positive coprime integers a, b, c satisfying $a + b = c$, then

$$c \leq \kappa_\epsilon \mathrm{rad}(abc)^{1+\epsilon}$$

Fun Aside

Fact. The *ABC* Conjecture implies Szpiro's conjecture, and if Szpiro's conjecture is true, then the *ABC* conjecture is true with exponent $3/2$.

Naïve Height

$$E_{A,B}\colon y^2 = x^3 + Ax + B$$

The naïve height of $E_{A,B}$ is

$$H(E_{A,B}) := \max\{|A|^3, |B|^2\}.$$

The naïve height can also be defined as $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$.

The advantage of the naïve height is that is we know how many elliptic curves there are up to a given height.

Let $\mathcal{E}_{H \leq X}$ denote the set of isomorphism classes of elliptic curves of height at most X.

Let $\mathcal{E}_{H \leq X}$ denote the set of isomorphism classes of elliptic curves of height at most X.

$$\#\mathcal{E}_{H \leq X} = 4\zeta(10)^{-1} X^{5/6} + O(X^{1/2})$$

Let $\mathcal{E}_{H\leq X}$ denote the set of isomorphism classes of elliptic curves of height at most X.

$$\#\mathcal{E}_{H\leq X} = 4\zeta(10)^{-1}X^{5/6} + O(X^{1/2})$$

This essentially comes from the fact that there are $X^{1/3}$ choices for A and $X^{1/2}$ choices for B.

Let $\mathcal{E}_{H \leq X}$ denote the set of isomorphism classes of elliptic curves of height at most X.

$$\#\mathcal{E}_{H \leq X} = 4\zeta(10)^{-1}X^{5/6} + O(X^{1/2})$$

This essentially comes from the fact that there are $X^{1/3}$ choices for A and $X^{1/2}$ choices for B.

It is conjectured that all the measures of heights give the same order of magnitude for all but a 'small' proportion of elliptic curves.

Conjecture (Goldfeld, Katz–Sarnak)

When ordered by height, the average rank of elliptic curves $E/\mathbf{Q}$ is $\frac{1}{2}$. More precisely, 50% of curves should have rank 0 and 50% of curves should have rank 1.

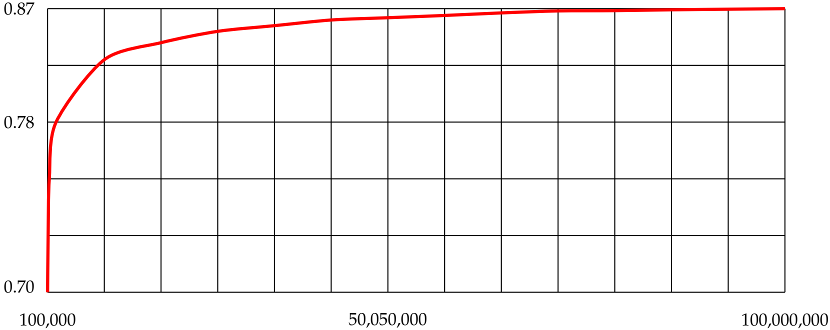
Dorian Goldfeld

Nick Katz

Peter Sarnak

Prior to the conjecture, the average rank was not even known to be finite!

Computations of Brumer, McGuinness, Bektemirov, Stein, Watkins



Average rank of elliptic curves of conductor $\leq 10^8$. The average turns out to be $0.8664\ldots$.

Two Important Conjectures

Riemann Hypothesis (RH)

The Riemann Zeta Function, $\zeta(s)$, is defined as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}.$$

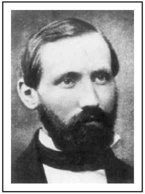
Riemann Hypothesis (RH)

The Riemann Zeta Function, $\zeta(s)$, is defined as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}.$$

Conjecture (Riemann Hypothesis, 1859)

If $s \in \mathbf{C}$ is a nontrivial zeros of $\zeta(s)$, then $\Re(s) = 1/2$



Bernhard Riemann
1826 – 1866

Generalized Riemann Hypothesis (GRH)

Let χ be a Dirichlet character, i.e. an arithmetic function $\chi : \mathbf{Z} \to \mathbf{C}$ that is both periodic and totally multiplicative. Then the Dirichlet L-function is

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Conjecture (Generalized Riemann Hypothesis)

If $s \in \mathbf{C}$ is a nontrivial zeros of $L(\chi, s)$, then $\Re(s) = 1/2$

Bernhard Riemann
1826 – 1866

Hasse Principle: $|p+1-\#E(\mathbf{F}_p)| \leq 2\sqrt{p}$. We define 'error terms' $a_p := p+1-\#E(\mathbf{F}_p)$.

Hasse Principle: $|p+1-\#E(\mathbf{F}_p)| \leq 2\sqrt{p}$. We define 'error terms' $a_p := p+1-\#E(\mathbf{F}_p)$.

$$L(E,s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Modularity Theorem

Theorem (Wiles, Taylor, Brueil, Conrad, Diamond)

$L(E,s)$ can be analytically continued to $\mathbf{C}$.

Andrew Wiles

Richard Taylor

Christophe Breuil

Brian Conrad

Fred Diamond

In particular, $L(E, s)$ has a Taylor expansion about $s = 1$:

$$L(E, s) = c_0 + c_1(s - 1) + c_2(s - 1)^2 + \cdots$$

In particular, $L(E, s)$ has a Taylor expansion about $s = 1$:

$$L(E, s) = c_0 + c_1(s - 1) + c_2(s - 1)^2 + \cdots$$

Define the analytic rank r_{an} of E to be the order of vanishing of $L(E, s)$ at $s = 1$,

$$L(E, s) = c_{r_{an}}(s - 1)^{r_{an}} + \cdots$$

Birch and Swinnerton-Dyer Conjecture (BSD)

Conjecture

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Birch and Swinnerton-Dyer Conjecture (BSD)

Conjecture

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Due to work of Gross, Zagier, Kolyvagin, if $r_{an} \leq 1$, then $r_{\text{anal}} = r_{alg}$. If BSD is true, there is an algorithm to compute the rank of an elliptic curve.

Birch and Swinnerton-Dyer Conjecture (BSD)

Conjecture

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Due to work of Gross, Zagier, Kolyvagin, if $r_{an} \leq 1$, then $r_{\text{anal}} = r_{alg}$. If BSD is true, there is an algorithm to compute the rank of an elliptic curve.

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \ \mathrm{Reg}(E)\, \#Ш(E/\mathbf{Q}) \ \prod_p c_p}{\#E(\mathbf{Q})^2_{tors}}$$

Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

2004: Heath-Brown (assuming BSD, GRH) improved this average rank to ≤ 2.0

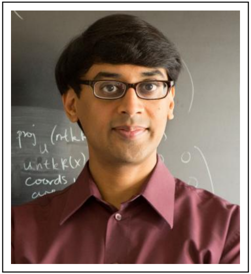
Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

2004: Heath-Brown (assuming BSD, GRH) improved this average rank to ≤ 2.0

2009: Young (assuming BSD, GRH) improved this to $\leq 25/14 \approx 1.786$.

Is there a proof of boundedness (with an estimate) without assuming BSD, GRH?



Manjul Bhargava

Arul Shankar

Idea of Bhargava-Shankar

We do not know how to compute $E(\mathbf{Q})$, so we study the 'simpler' group $E(\mathbf{Q})/nE(\mathbf{Q})$.

Idea of Bhargava-Shankar

We do not know how to compute $E(\mathbf{Q})$, so we study the 'simpler' group $E(\mathbf{Q})/nE(\mathbf{Q})$.

By the Mordell-Weil Theorem, we know that

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$$

Idea of Bhargava-Shankar

We do not know how to compute $E(\mathbf{Q})$, so we study the 'simpler' group $E(\mathbf{Q})/nE(\mathbf{Q})$.

By the Mordell-Weil Theorem, we know that

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$$

Then we must have

$$E(\mathbf{Q})/nE(\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^r \oplus E(\mathbf{Q})_{\text{tors}}/nE(\mathbf{Q})_{\text{tors}}$$

Idea of Bhargava-Shankar

If we knew $E(\mathbf{Q})/nE(\mathbf{Q})$ and $E(\mathbf{Q})_{\text{tors}}$, we could compute r.

Idea of Bhargava-Shankar

If we knew $E(\mathbf{Q})/nE(\mathbf{Q})$ and $E(\mathbf{Q})_{\text{tors}}$, we could compute r.

Example. If $n = p$, then

$$\dim_{\mathbf{F}_p} E(\mathbf{Q})/pE(\mathbf{Q}) = \dim_{\mathbf{F}_p} E(\mathbf{Q})[p] + \operatorname{rank} E(\mathbf{Q})$$

Selmer & Shafarevich-Tate Groups

Define a computable group $S^n(E)$, called the Selmer group, containing $E(\mathbf{Q})/nE(\mathbf{Q})$.

Selmer & Shafarevich-Tate Groups

Define a computable group $S^n(E)$, called the Selmer group, containing $E(\mathbf{Q})/nE(\mathbf{Q})$.

Approximate $E(\mathbf{Q})/nE(\mathbf{Q})$ by $S^{(n)}(E)$. We define an 'error term' $Ш(E)$, called the Shafarevich-Tate group.

$$0 \to E(\mathbf{Q})/nE(\mathbf{Q}) \to S^{(n)}(E) \to Ш[n] \to 0$$

Definition

Let $\varphi : E/K \to E'/K$ be an isogeny. The φ-Selmer group E/K is the subgroup of $H^1(G_{\overline{K}/K}, E[\varphi])$ defined by

$$S^{(\varphi)}(E/K) := \ker \left\{ H^1(G_{\overline{K}/K}, E[\varphi]) \to \prod_{v \in M_K} \mathrm{WC}(E/K_v) \right\}$$

The Shafarevich-Tate group of E/K is the subgroup of $\mathrm{WC}(E/K)$ defined by

$$\text{Ш}(E/K) := \ker \left\{ \mathrm{WC}(E/K) \to \prod_{v \in M_K} \mathrm{WC}(E/K_v) \right\}.$$

Idea of Bhargava-Shankar

$$0 \to E(\mathbf{Q})/nE(\mathbf{Q}) \to S^{(n)}(E) \to Ш[n] \to 0$$

If $E(\mathbf{Q})[n] = \{\mathcal{O}\}$, then

$$n^{\operatorname{rank} E} \leq |S^{(n)}(E)|.$$

Idea of Bhargava-Shankar

$$0 \to E(\mathbf{Q})/nE(\mathbf{Q}) \to S^{(n)}(E) \to Ш[n] \to 0$$

If $E(\mathbf{Q})[n] = \{\mathcal{O}\}$, then

$$n^{\operatorname{rank} E} \leq |S^{(n)}(E)|.$$

To prove boundedness of average rank, it is enough to show that the average size of $|S^{(n)}(E)|$ for any $n > 1$.

Outline of the Proof

1. For $n \leq 5$, construct a representation V of an algebraic group G defined over $\mathbf{Z}$ related to A, B.
2. Count the elements under the action of G on V with bounded A, B.
3. Sieve to count the elements of $S^{(n)}(E_{A,B})$ 'in' the representation.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Corollary

Let $n = 1, 2, 3, 4, 5$. When ordered by height, the average size of the n-Selmer group for elliptic curves $E/\mathbf{Q}$ is $\sigma(n)$.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Corollary

Let $n = 1, 2, 3, 4, 5$. When ordered by height, the average size of the n-Selmer group for elliptic curves $E/\mathbf{Q}$ is $\sigma(n)$.

Conjecture (Bhargava–Shankar)

Let $n \geq 1$. When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average size of the n-Selmer group is $\sigma(n)$.

Proposition (Bhargava–Shankar)

If the previous conjecture is true for all n, then when elliptic curves are ordered by height, a density of 100% of elliptic curves have rank 0 or 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average rank is bounded (by $0.885 < 1$).

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, the average rank is bounded (by $0.885 < 1$).

Corollary

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have rank 0.

Corollary

When elliptic curves $E/\mathbf{Q}$ are ordered by height, more than 80% have rank 0 or 1.

What about lower bounds?

Theorem (Bhargava, Shankar, Skinner)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have rank 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Corollary

A positive proportion of elliptic curves satisfy the BSD conjecture.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbf{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Corollary

A positive proportion of elliptic curves satisfy the BSD conjecture.

Theorem (Bhargava–Shankar–Zhang)

More than 66% of elliptic curves have analytic rank 0 or 1, and thus satisfy BSD.

The average rank is bounded. But what about ranks generally?

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbf{Z}_p$.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbf{Z}_p$.

The model predicts…

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbf{Z}_p$.

The model predicts…

- rank $E(\mathbf{Q})$ is 0 or 1 each with density 50%.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbf{Z}_p$.

The model predicts…

- rank $E(\mathbf{Q})$ is 0 or 1 each with density 50%.
- rank $E(\mathbf{Q}) \geq 2$ with density 0%.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbf{Z}_p$.

The model predicts…

- rank $E(\mathbf{Q})$ is 0 or 1 each with density 50%.
- rank $E(\mathbf{Q}) \geq 2$ with density 0%.
- Only finitely many elliptic curves over $\mathbf{Q}$ have rank ≥ 22.

Questions?