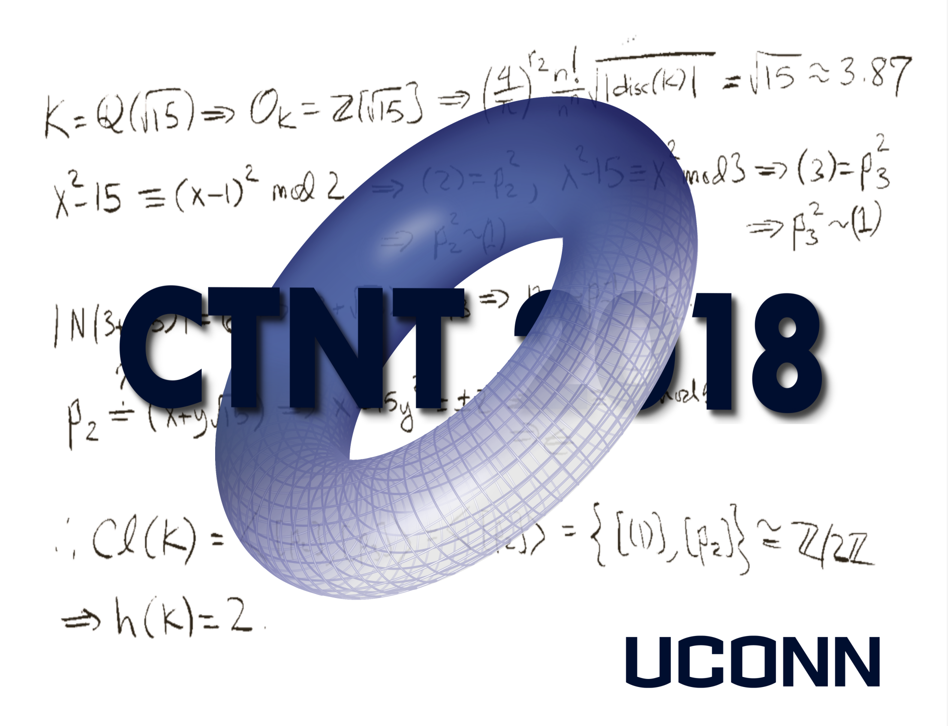

CTNT 2018
UCONN

Arithmetic Statistics
Lecture 4

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

May 28$^{\text{th}}$

CTNT 2018
Connecticut Summer School
in Number Theory

PREVIOUSLY...

We can define an **action of** $\mathrm{SL}(2, \mathbb{Z})$ **on Binary Quadratic Forms (BQFs)** by

$$M \cdot f\left(\left(\begin{array}{c} x \\ y \end{array}\right)\right) = f\left(M \cdot \left(\begin{array}{c} x \\ y \end{array}\right)\right) \quad \text{for any } M \in \mathrm{SL}(2, \mathbb{Z})$$

PREVIOUSLY...

We can define an **action of** $\mathrm{SL}(2,\mathbb{Z})$ **on Binary Quadratic Forms (BQFs)** by

$$M \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(M \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right) \quad \text{for any } M \in \mathrm{SL}(2,\mathbb{Z})$$

Associative?

PREVIOUSLY...

We can define an **action of** $\mathrm{SL}(2,\mathbb{Z})$ **on Binary Quadratic Forms (BQFs)** by

$$M \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(M \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right) \quad \text{for any } M \in \mathrm{SL}(2,\mathbb{Z})$$

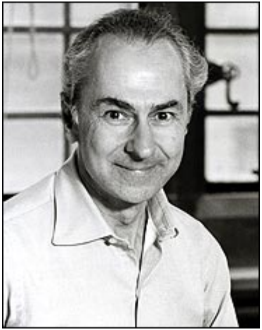
Associative? It is **not** associative when defined like this. Let us define a group action instead by $M \cdot f(v) = f(M^{-1}v)$, and suppose $f(x,y) = \begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}$. Then:

$$\begin{aligned}
N \cdot \left(M \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)\right) &= N \cdot \left(\begin{pmatrix} x & y \end{pmatrix} (M^{-1})^t \cdot A \cdot M^{-1} \begin{pmatrix} x \\ y \end{pmatrix}\right) \\
&= \begin{pmatrix} x & y \end{pmatrix} (N^{-1})^t \cdot ((M^{-1})^t \cdot A \cdot M^{-1}) \cdot N^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} x & y \end{pmatrix} ((NM)^{-1})^t \cdot A \cdot (NM)^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= (NM) \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)
\end{aligned}$$

Elliptic Curves

Elliptic Curves

e.g., $y^2 = x^3 - 25x$.

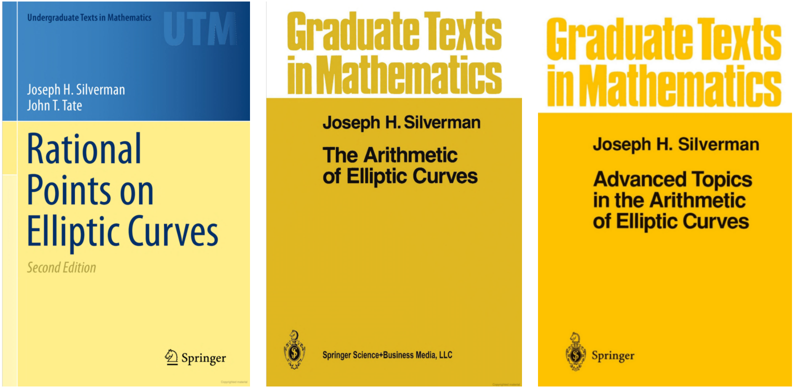


Foreword

It is possible to write endlessly on elliptic curves. (This is not a threat.) We deal here with diophantine problems, and we lay the foundations, especially for the theory of integral points. We review briefly the analytic theory of the Weierstrass function, and then deal with the arithmetic aspects of the addition formula, over complete fields and over number fields, giving rise to the theory of the height and its quadraticity. We apply this to integral points, covering the inequalities of diophantine approximation both on the multiplicative group and on the elliptic curve directly. Thus the book splits naturally in two parts.

From Serge Lang’s “Elliptic Curves: Diophantine Analysis”:

It is possible to write endlessly on elliptic curves. (This is not a threat.)

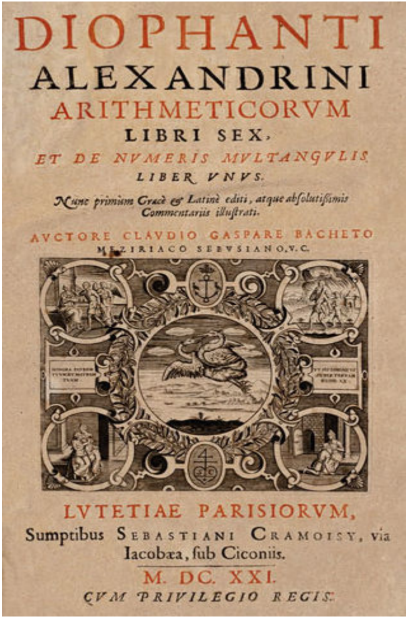


Joseph Silverman’s books on elliptic curves.

What is an elliptic curve?

What is an elliptic curve,... and WHY elliptic curves?

What is an elliptic curve,... and WHY elliptic curves?



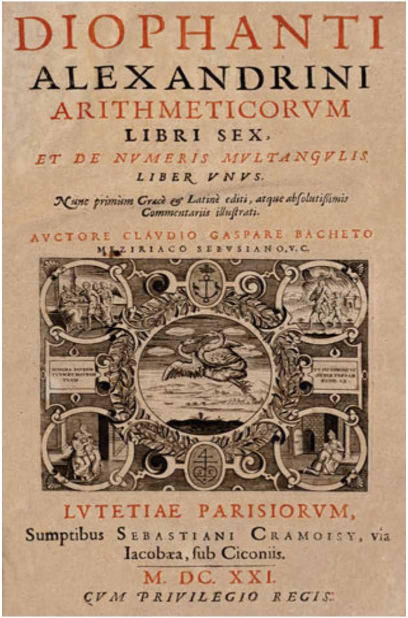
Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?

What is an elliptic curve,... and WHY elliptic curves?



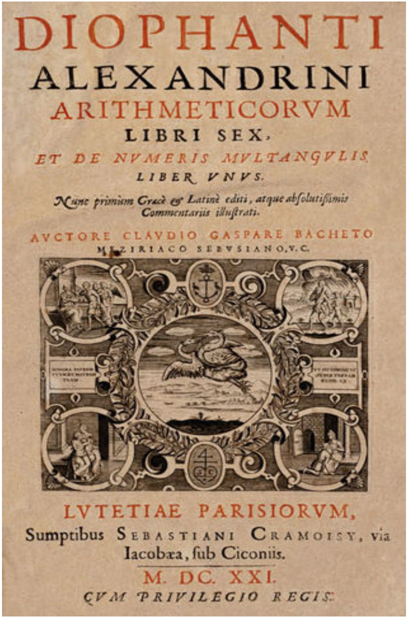
Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over** $\mathbb{Z}$) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$?

What is an elliptic curve,... and WHY elliptic curves?



Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over $\mathbb{Z}$**) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$? (David, Matiyasevich, Putnam, Robinson: No)

What is an elliptic curve,... and WHY elliptic curves?

Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over** $\mathbb{Z}$) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$? (David, Matiyasevich, Putnam, Robinson: No)

What is an elliptic curve,... and WHY elliptic curves?

Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over** $\mathbb{Z}$) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$? (David, Matiyasevich, Putnam, Robinson: No)

When $C : f(x, y) = 0$ is smooth (projective), of degree 3 (or genus 1), we already lack an algorithm that will determine whether there are rational points on C, or, if one exists, an algorithm that will determine *all* the rational points on C.

What is an elliptic curve,... and WHY elliptic curves?

Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over** $\mathbb{Z}$) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$? (David, Matiyasevich, Putnam, Robinson: No)

When $C : f(x, y) = 0$ is smooth (projective), of degree 3 (or genus 1), we already lack an algorithm that will determine whether there are rational points on C, or, if one exists, an algorithm that will determine *all* the rational points on C.

An **elliptic curve** defined over a field F, denoted by E/F, is a smooth projective curve, of genus 1, with at least one rational point defined over F.

What is an elliptic curve,... and WHY elliptic curves?

Given a polynomial equation

$$f(x_1, x_2, \ldots, x_r) = 0$$

with integer coefficients (i.e., a **diophantine equation**), we can ask three basic questions:

1. Can we determine if there are rational or integral solutions?
2. In the affirmative case, can we *find* such a solution?
3. Can we describe *all* such solutions?
4. (**Hilbert's Tenth Problem over** $\mathbb{Z}$) Is there a Turing machine to decide if $f = 0$ has solutions in $\mathbb{Z}$? (David, Matiyasevich, Putnam, Robinson: No)

When $C : f(x, y) = 0$ is smooth (projective), of degree 3 (or genus 1), we already lack an algorithm that will determine whether there are rational points on C, or, if one exists, an algorithm that will determine *all* the rational points on C.

An **elliptic curve** defined over a field F, denoted by E/F, is a smooth projective curve, of genus 1, with at least one rational point defined over F. Given by

$$Y^2 = X^3 + AX + B$$

What is an elliptic curve,... and WHY elliptic curves?

Some examples of diophantine equations, or problems that are connected to elliptic curves:

What is an elliptic curve,... and WHY elliptic curves?

Some examples of diophantine equations, or problems that are connected to elliptic curves:

- **Fermat's equation** $A^n + B^n = C^n$ leads to the so-called Frey curve $Y^2 = X(X - A^n)(X + B^n)$.

What is an elliptic curve,... and WHY elliptic curves?

Some examples of diophantine equations, or problems that are connected to elliptic curves:

- **Fermat's equation** $A^n + B^n = C^n$ leads to the so-called Frey curve $Y^2 = X(X - A^n)(X + B^n)$.
- The **congruent number problem** leads to $Y^2 = X^3 - n^2X$.

What is an elliptic curve,... and WHY elliptic curves?

Some examples of diophantine equations, or problems that are connected to elliptic curves:

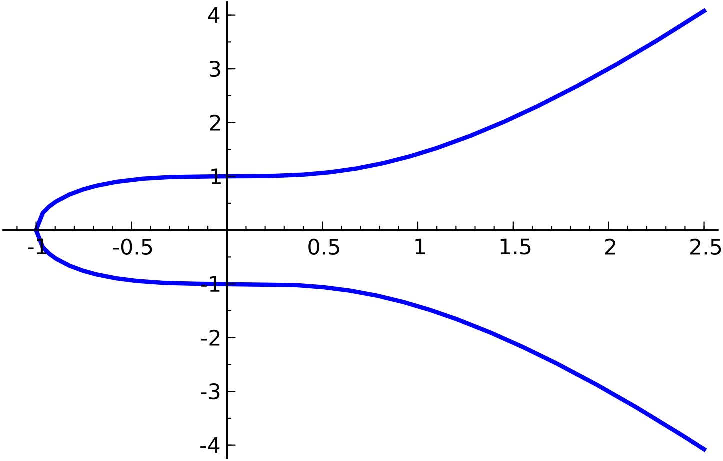
- **Fermat's equation** $A^n + B^n = C^n$ leads to the so-called Frey curve $Y^2 = X(X - A^n)(X + B^n)$.
- The **congruent number problem** leads to $Y^2 = X^3 - n^2X$.
- The **ABC conjecture** is logically equivalent to specific upper bounds on an integral solution (x_0, y_0) to Mordell's equation $Y^2 = X^3 + k$ in terms of the parameter k.

What is an elliptic curve,... and WHY elliptic curves?

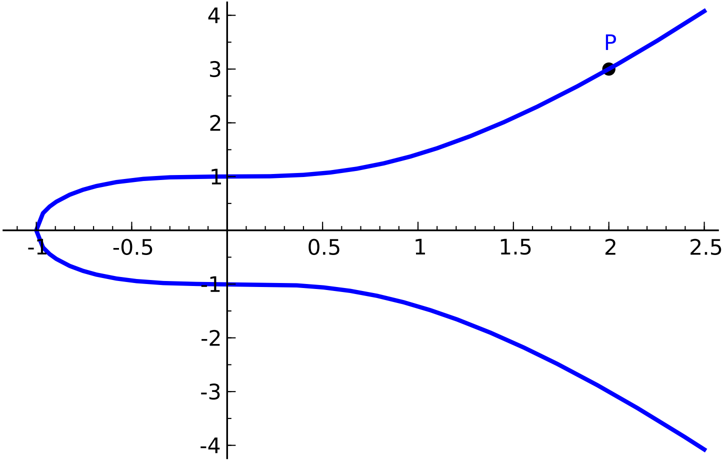
Some examples of diophantine equations, or problems that are connected to elliptic curves:

- **Fermat's equation** $A^n + B^n = C^n$ leads to the so-called Frey curve $Y^2 = X(X - A^n)(X + B^n)$.
- The **congruent number problem** leads to $Y^2 = X^3 - n^2 X$.
- The **ABC conjecture** is logically equivalent to specific upper bounds on an integral solution (x_0, y_0) to Mordell's equation $Y^2 = X^3 + k$ in terms of the parameter k.
- **Hilbert's Tenth Problem** over a ring of integers of a number field F can be shown to be undecidable if a well-known conjecture (finiteness of Sha) holds for elliptic curves over F.

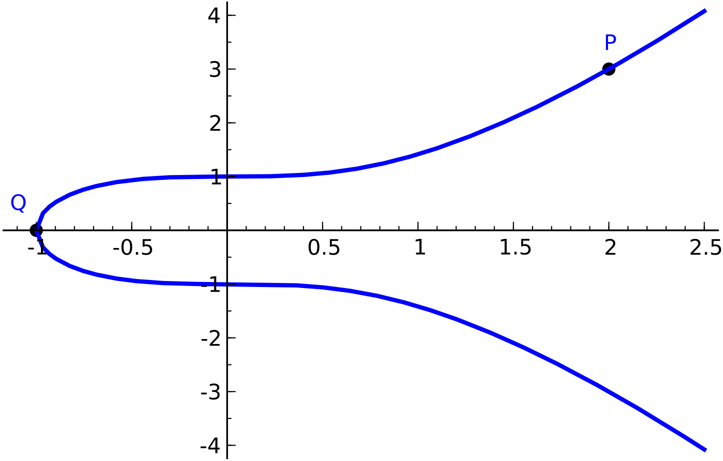
Example: the elliptic curve $y^2 = x^3 + 1$



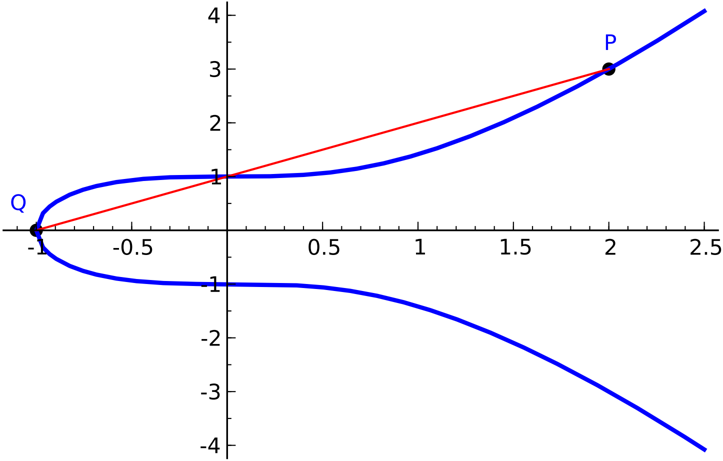
The addition of rational points on an elliptic curve



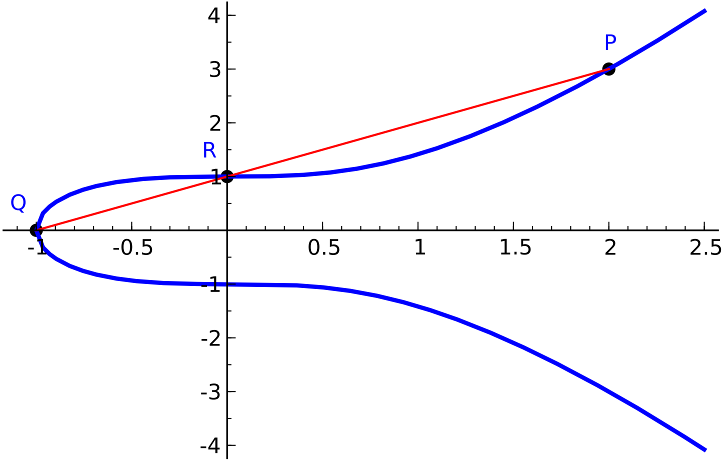
The addition of rational points on an elliptic curve



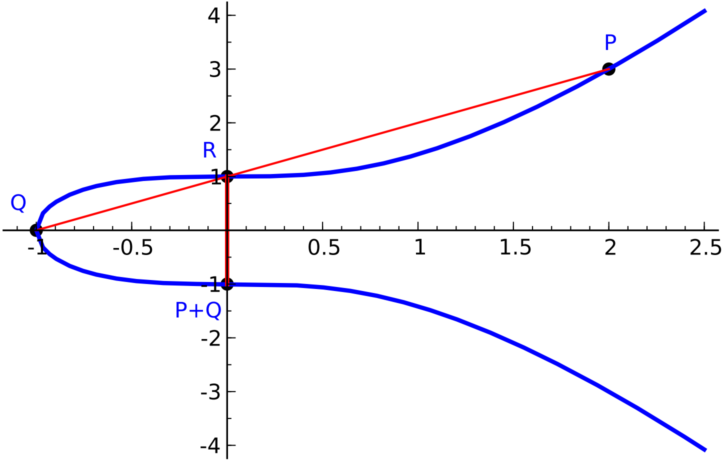
The addition of rational points on an elliptic curve

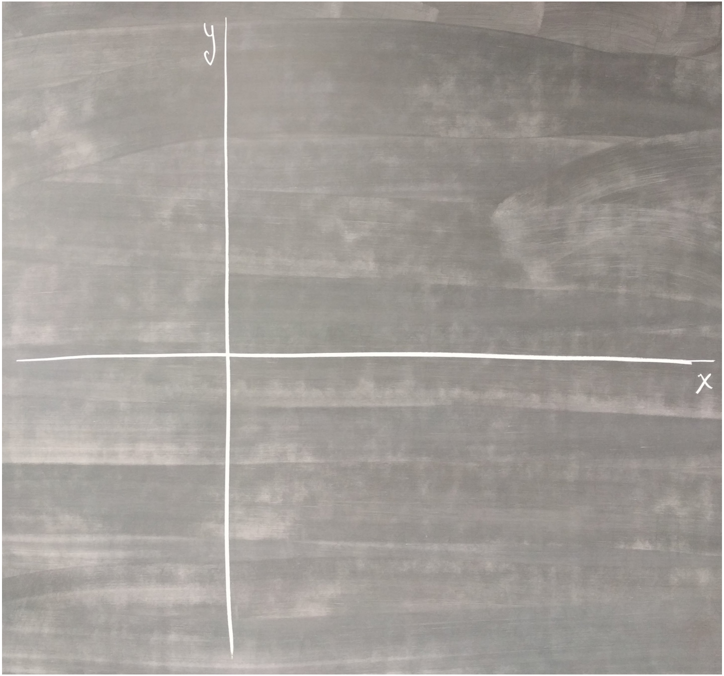


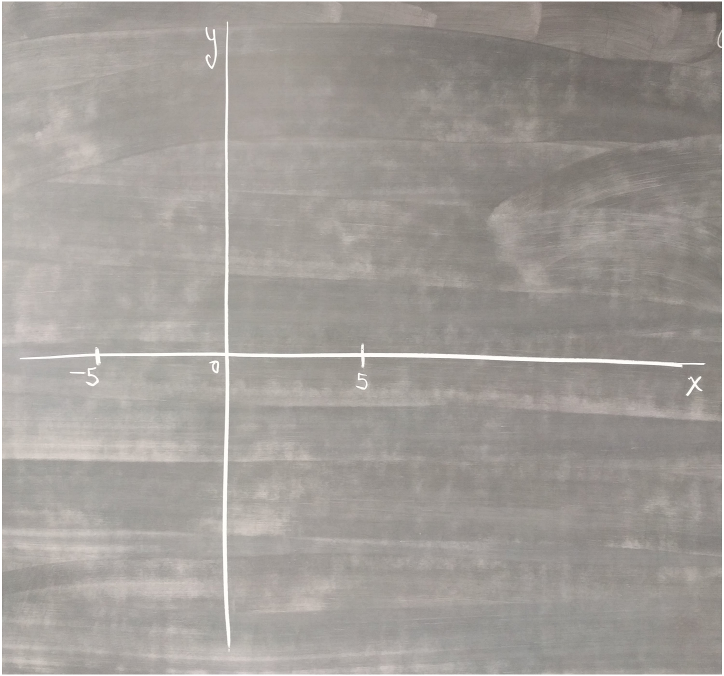
The addition of rational points on an elliptic curve

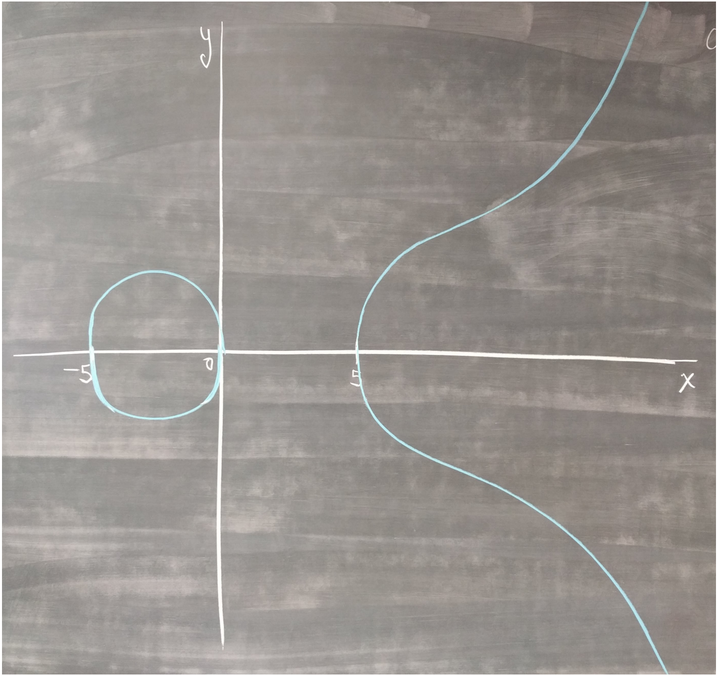


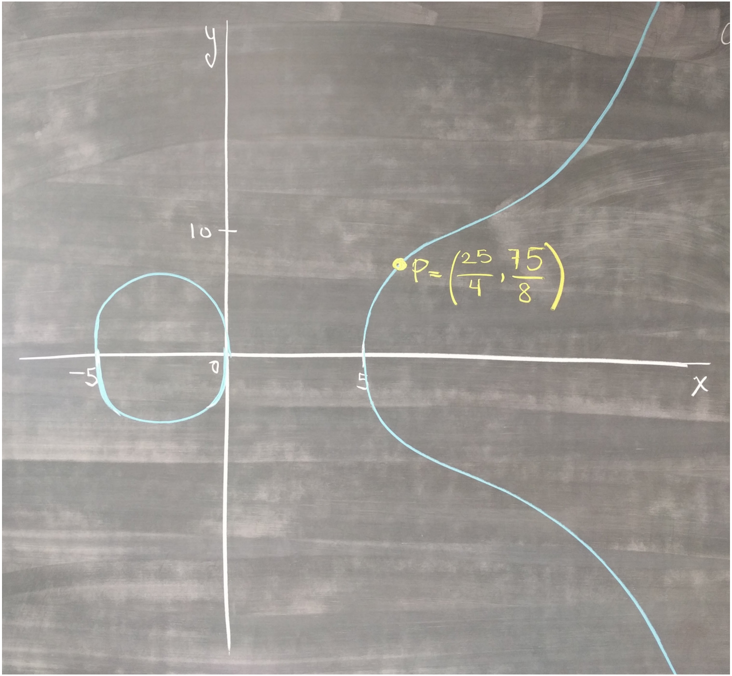
The addition of rational points on an elliptic curve

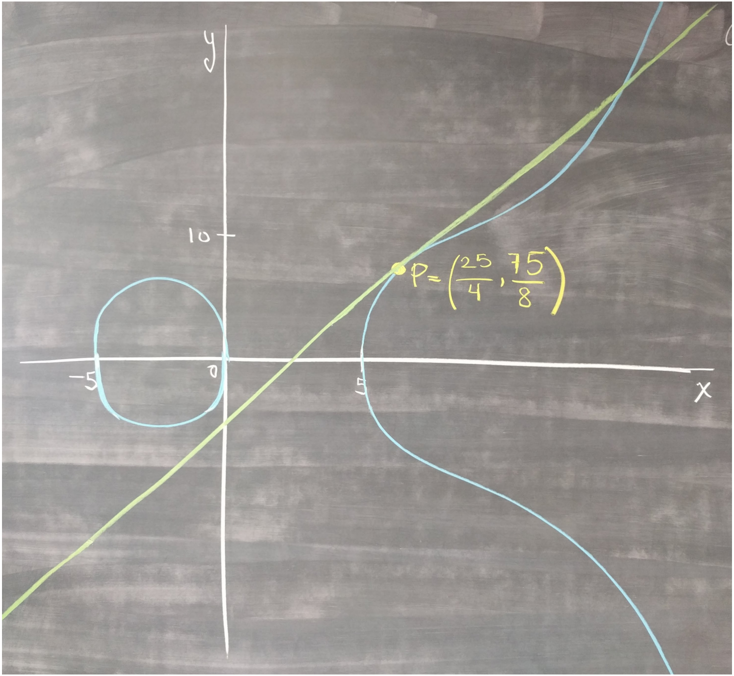


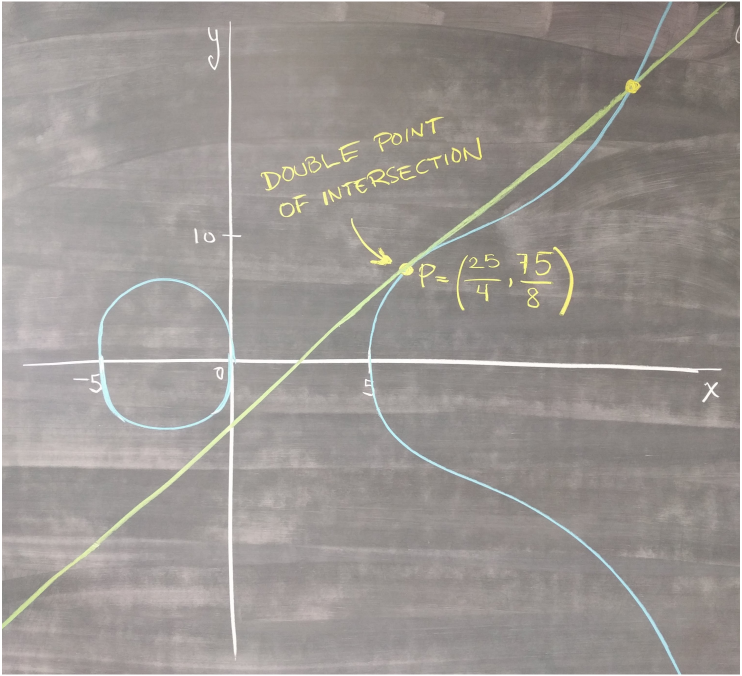

y
x

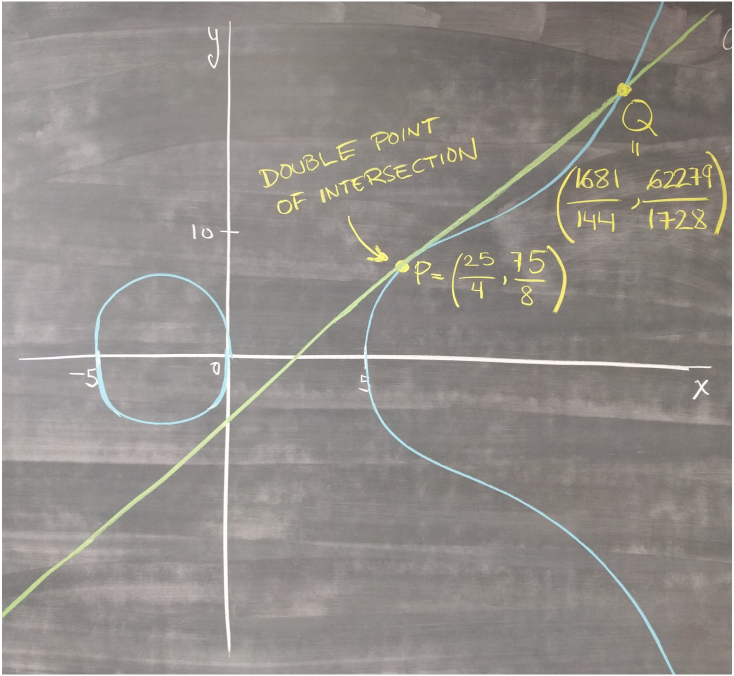

y
-5
0
5
x


y
x
-5
0
5

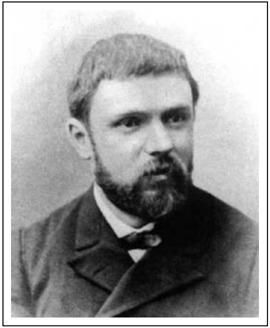

y
10
-5
0
5
x
P = (25/4, 75/8)


y
10
−5
0
5
x
P = (25/4, 75/8)

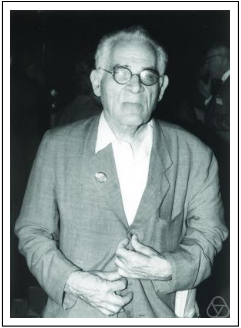

y
x
10
-5
0
5
DOUBLE POINT OF INTERSECTION
P = (25/4, 75/8)



y
10
-5
0
5
x
DOUBLE POINT OF INTERSECTION
P = (25/4, 75/8)
Q
=
(1681/144, 62279/1728)

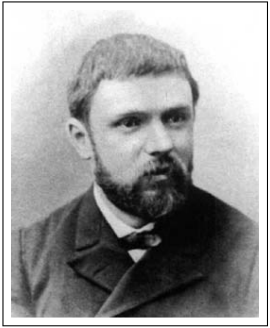


J. H. Poincaré
1854 – 1912

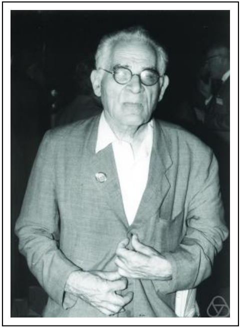


Louis Mordell
1888 – 1972

André Weil
1906 – 1998



J. H. Poincaré
1854 – 1912

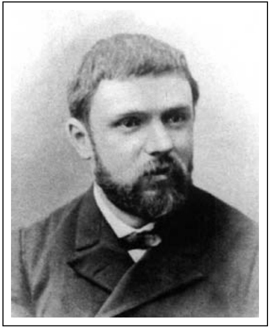


Louis Mordell
1888 – 1972

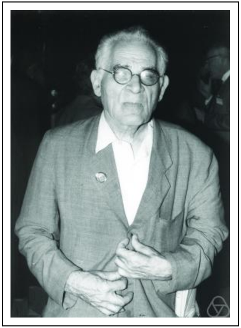
André Weil
1906 – 1998

Theorem (Mordell-Weil)

Let F be a number field, and let E/F be an elliptic curve. Then, the group of F-rational points on E, denoted by $E(F)$, is a finitely generated abelian group.



J. H. Poincaré
1854 – 1912



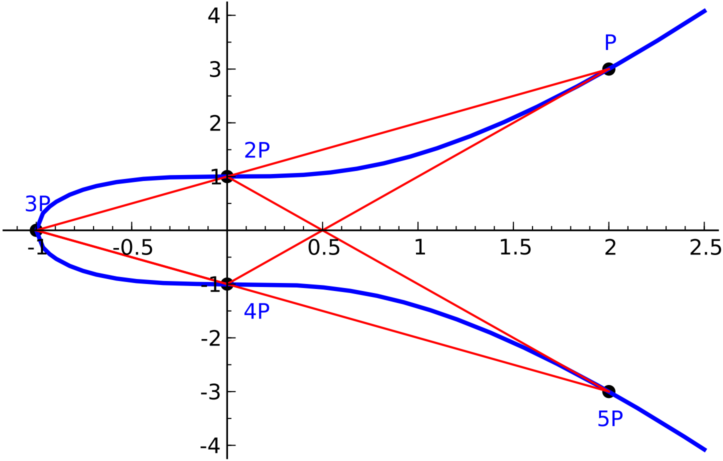
Louis Mordell
1888 – 1972

André Weil
1906 – 1998

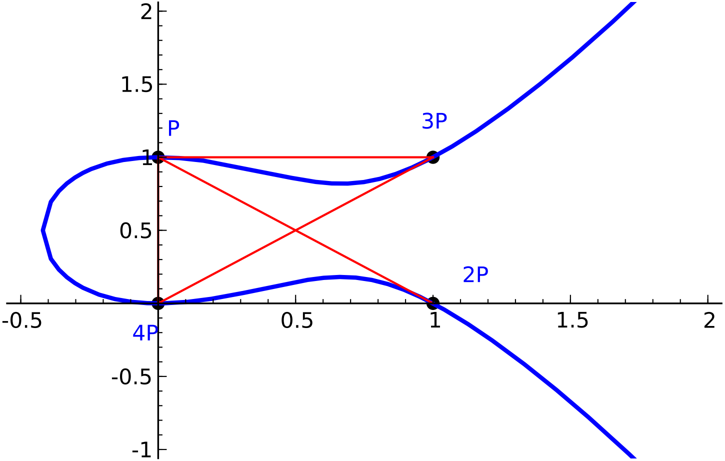
Theorem (Mordell-Weil)

Let F be a number field, and let E/F be an elliptic curve. Then, the group of F-rational points on E, denoted by $E(F)$, is a finitely generated abelian group. In particular, $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}$ where $E(F)_{tors}$ is a finite subgroup, and $R_{E/F} \geq 0$.

Torsion points: $P = (2, 3)$ has order 6 in $y^2 = x^3 + 1$



Torsion points: $(0, 1)$ has order 5 in $y^2 - y = x^3 - x^2$



The following are some examples of elliptic curves and their Mordell-Weil groups:

The following are some examples of elliptic curves and their Mordell-Weil groups:

1. The curve $E_1/\mathbb{Q} : y^2 = x^3 + 6$ satisfies $E_1(\mathbb{Q}) = \{\mathcal{O}\}$.

The following are some examples of elliptic curves and their Mordell-Weil groups:

1. The curve $E_1/\mathbb{Q} : y^2 = x^3 + 6$ satisfies $E_1(\mathbb{Q}) = \{\mathcal{O}\}$.
2. The curve $E_2/\mathbb{Q} : y^2 = x^3 + 1$ has only 6 rational points. Therefore $E_2(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ is an isomorphism of groups, and

$$E_2(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\}.$$

The following are some examples of elliptic curves and their Mordell-Weil groups:

1. The curve $E_1/\mathbb{Q} : y^2 = x^3 + 6$ satisfies $E_1(\mathbb{Q}) = \{\mathcal{O}\}$.
2. The curve $E_2/\mathbb{Q} : y^2 = x^3 + 1$ has only 6 rational points. Therefore $E_2(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ is an isomorphism of groups, and

$$E_2(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\}.$$

3. The curve $E_3/\mathbb{Q} : y^2 = x^3 - 2$ does not have any rational torsion points other than $\mathcal{O}$. However, the point $P = (3, 5)$ is a rational point. Thus, P must be a point of infinite order. In fact,

$$E_3(\mathbb{Q}) = \{nP : n \in \mathbb{Z}\} \quad \text{and} \quad E_3(\mathbb{Q}) \cong \mathbb{Z}.$$

The following are some examples of elliptic curves and their Mordell-Weil groups:

1. The curve $E_1/\mathbb{Q} : y^2 = x^3 + 6$ satisfies $E_1(\mathbb{Q}) = \{\mathcal{O}\}$.
2. The curve $E_2/\mathbb{Q} : y^2 = x^3 + 1$ has only 6 rational points. Therefore $E_2(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ is an isomorphism of groups, and

$$E_2(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\}.$$

3. The curve $E_3/\mathbb{Q} : y^2 = x^3 - 2$ does not have any rational torsion points other than $\mathcal{O}$. However, the point $P = (3, 5)$ is a rational point. Thus, P must be a point of infinite order. In fact,

$$E_3(\mathbb{Q}) = \{nP : n \in \mathbb{Z}\} \quad \text{and} \quad E_3(\mathbb{Q}) \cong \mathbb{Z}.$$

4. The elliptic curve $E_4/\mathbb{Q} : y^2 = x^3 + 7105x^2 + 1327104x$ features both torsion and infinite order points. In fact, $E_4(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$. The torsion subgroup is generated by the point of order 4 $T = (1152, 111744)$. The free part is generated by

$$P_1 = (-6912, 6912), P_2 = (-5832, 188568), P_3 = (-5400, 206280).$$

Variations of the problem

Theorem (Mordell-Weil)

$E(F)$ is finitely generated. In particular, $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}$.

Variations of the problem

Theorem (Mordell-Weil)

$E(F)$ is finitely generated. In particular, $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}$.

Variations:

Variations of the problem

Theorem (Mordell-Weil)

$E(F)$ is finitely generated. In particular, $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}$.

Variations: **torsion subgroups**

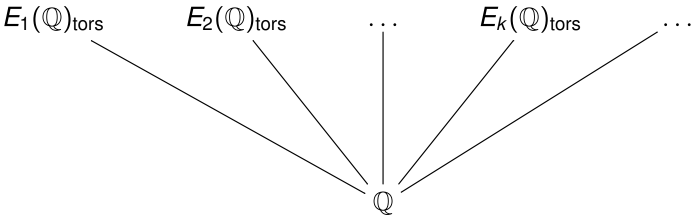
$$\begin{tikzcd}
E_1(F)_{\text{tors}} & E_2(F)_{\text{tors}} & \cdots & E_k(F)_{\text{tors}} & \cdots \\
 & & F \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

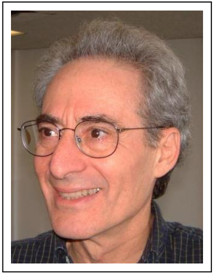
where $E_1, E_2, \ldots, E_k, \ldots$ is some family of (perhaps all) elliptic curves over a fixed field F.

Torsion subgroups of elliptic curves over $\mathbb{Q}$

$$\begin{tikzcd}[column sep=small]
E_1(\mathbb{Q})_{\text{tors}} \arrow[drr, dash] & E_2(\mathbb{Q})_{\text{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E_k(\mathbb{Q})_{\text{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Torsion subgroups of elliptic curves over $\mathbb{Q}$





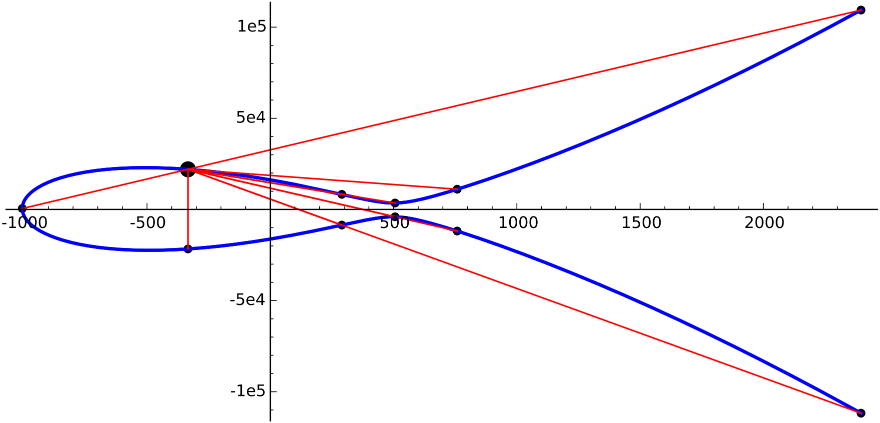
Barry Mazur

Theorem (Levi–Ogg Conjecture; Mazur, 1977)

Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4. \end{cases}$$

Moreover, each possible group appears infinitely many times.



The elliptic curve `30030bt1` has a point of order 12.

Question

Can we “count” how many elliptic curves are there with each torsion subgroup?

- We will consider elliptic curves (up to isomorphism over $\mathbb{Q}$) given by a minimal short Weierstrass model over $\mathbb{Z}$, that is,

$$\mathcal{E} = \{E/\mathbb{Q} : y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z}\},$$

with $4A^3 + 27B^2 \neq 0$, and such that if $d^4|A$ and $d^6|B$, then $d = \pm 1$.

Question

Can we “count” how many elliptic curves are there with each torsion subgroup?

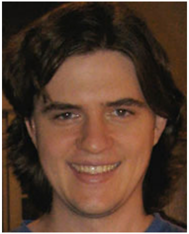
- We will consider elliptic curves (up to isomorphism over $\mathbb{Q}$) given by a minimal short Weierstrass model over $\mathbb{Z}$, that is,

$$\mathcal{E} = \{E/\mathbb{Q} : y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z}\},$$

  with $4A^3 + 27B^2 \neq 0$, and such that if $d^4|A$ and $d^6|B$, then $d = \pm 1$.
- The naive height of $E \in \mathcal{E}$ is defined by

$$\mathrm{ht}(E) = \max\{4|A|^3, 27B^2\}.$$

- $\mathcal{E}(X) = \{E \in \mathcal{E} : \mathrm{ht}(E) \leq X\}$, all elliptic curves up to height X.
- $\pi_{\mathcal{E}}(X) = \#\mathcal{E}(X)$.

Theorem (Harron, Snowden, 2013)

Let G be one of the groups in Mazur's list. We let $N_G(X)$ be the number of (isomorphism classes of) elliptic curves $E/\mathbb{Q}$ of height at most X for which $E(\mathbb{Q})_{tors} \cong G$. Then, there is an explicit constant $d(G)$ such that

$$\lim_{X\to\infty} \frac{\log N_G(X)}{\log X} = \frac{1}{d(G)}.$$

E.g., $d(0) = 6/5$, $d(\mathbb{Z}/2\mathbb{Z}) = 2$, $d(\mathbb{Z}/3\mathbb{Z}) = 3$, $d(\mathbb{Z}/5\mathbb{Z}) = 6$, and $d(\mathbb{Z}/7\mathbb{Z}) = 12$.

In particular, *almost all* elliptic curves over $\mathbb{Q}$ have trivial torsion.

Variations of the problem

Theorem (Mordell-Weil)

$E(F)$ is finitely generated. In particular, $E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}$.

Variations: **ranks**

$$\begin{tikzcd}
R_{E_1/F} & R_{E_2/F} & \cdots & R_{E_k/F} & \cdots \\
 & & F \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

where $E_1, E_2, \ldots, E_k, \ldots$ is some family of (perhaps all) elliptic curves over a fixed field F.

Variations of the problem: ranks over $\mathbb{Q}$

$$\begin{tikzcd}
R_{E_1/\mathbb{Q}} & R_{E_2/\mathbb{Q}} & \cdots & R_{E_k/\mathbb{Q}} & \cdots \\
& & \mathbb{Q} \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

where $E_1, E_2, \ldots, E_k, \ldots$ is a family of elliptic curves over $\mathbb{Q}$:

- All elliptic curves over $\mathbb{Q}$.
- Family of quadratic twists of a given curve: $y^2 = x^3 + Ad^2x + Bd^3$, for fixed $A, B \in \mathbb{Q}$, and any $d \neq 0$.
- Other 1-parameter families of elliptic curves.

Variations of the problem: ranks over $\mathbb{Q}$

$$\begin{tikzcd} R_{E_1/\mathbb{Q}} & R_{E_2/\mathbb{Q}} & \cdots & R_{E_k/\mathbb{Q}} & \cdots \\ & & \mathbb{Q} \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & & \end{tikzcd}$$

where $E_1, E_2, \ldots, E_k, \ldots$ is a family of elliptic curves over $\mathbb{Q}$:

- All elliptic curves over $\mathbb{Q}$.
- Family of quadratic twists of a given curve: $y^2 = x^3 + Ad^2x + Bd^3$, for fixed $A, B \in \mathbb{Q}$, and any $d \neq 0$.
- Other 1-parameter families of elliptic curves.

Open Problem

What values can $R_{E/\mathbb{Q}}$ take? In particular, can $R_{E/\mathbb{Q}}$ be arbitrarily large, or is it uniformly bounded?

Elkies' elliptic curve of rank ≥ 28

$$y^2 + xy + y = x^3 - x^2 - (20067762415575526585033208209338542750930230312178956502)x + (344816117950305564670329856903907203748559443593191803612660082962919394487322434 29)$$

Independent points of infinite order:

Noam Elkies

$$P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$$

$$P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$$

$$P_3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$$

$$\vdots$$

Elkies' elliptic curve of rank ≥ 28

$$
\begin{aligned}
P_4 =& [2139130260139156666492982137,\\
& 36639509171439729202421459692941297527531]\\
P_5 =& [1534706764467120723885477337,\\
& 85429585346017694289021032862781072799531]\\
P_6 =& [-2731079487875677033341575063,\\
& 262521815484332191641284072623902143387531]\\
P_7 =& [2775726266844571649705458537,\\
& 12845755474014060248869487699082640369931]\\
P_8 =& [1494385729327188957541833817,\\
& 88486605527733405986116494514049233411451]\\
P_9 =& [1868438228620887358509065257,\\
& 59237403214437708712725140393059358589131]\\
P_{10} =& [2008945108825743774866542537,\\
& 47690677880125552882151750781541424711531]\\
P_{11} =& [2348360540918025169651632937,\\
& 17492930006200557857340332476448804363531]
\end{aligned}
$$

Elkies' elliptic curve of rank ≥ 28

$P12$ = [-14720840070904811744700086663, 246643450653503714199947441549759798469131]
P13 = [2924128607708061213363288937, 28350264431488878501488356474767375899531]
P14 = [5374993891066061893293934537, 286188908427263386451175031916479893731531]
P15 = [1709690768233354523334008557, 71898834974686089466159700529215980921631]
P16 = [2450954011353593144072595187, 4445228173532634357049262550610714736531]
P17 = [2969254709273559167464674937, 32766893075366270801333682543160469687531]
P18 = [2711914934941692601332882937, 2068436612778381698650413981506590613531]
P19 = [20078586077996854528778328937, 2779608541137806604656051725624624030091531]
P20 = [2158082450240734774317810697, 34994373401964026809969662241800901254731]
P21 = [2004645458247059022403224937, 48049329780704645522439866999888475467531]
P22 = [2975749450947996264947091337, 33398989826075322320208934410104857869131]
P23 = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]
P24 = [311583179915063034902194537, 168104385229980603540109472915660153473931]
P25 = [2773931008341865231443771817, 12632162834649921002414116273769275813451]
P26 = [2156581188143768409363461387, 35125092964022908897004150516375178087331]
P27 = [3866330499872412508815659137, 121197755655944226293036926715025847322531]
P28 = [2230868289773576023778678737, 28558760030597485663387020600768640028531]

For current rank records, visit Andrej Dujella's website:

https://web.math.pmf.unizg.hr/~duje/tors/tors.html

The Rank

For each $r \geq 0$, we define the set of curves of rank r up to height X:

$$\mathcal{R}_r(X) = \{E \in \mathcal{E}(X) : \mathrm{rank}(E(\mathbb{Q})) = r\}, \quad \pi_{\mathcal{R}_r}(X) = \#\mathcal{R}_r(X).$$

The Rank

For each $r \geq 0$, we define the set of curves of rank r up to height X:

$$\mathcal{R}_r(X) = \{E \in \mathcal{E}(X) : \text{rank}(E(\mathbb{Q})) = r\}, \quad \pi_{\mathcal{R}_r}(X) = \#\mathcal{R}_r(X).$$

Some conjectures and heuristics:

The Rank

For each $r \geq 0$, we define the set of curves of rank r up to height X:

$$\mathcal{R}_r(X) = \{E \in \mathcal{E}(X) : \mathrm{rank}(E(\mathbb{Q})) = r\}, \quad \pi_{\mathcal{R}_r}(X) = \#\mathcal{R}_r(X).$$

Some conjectures and heuristics:

- (50% $-$ 50% Conjecture, Goldfeld, Katz–Sarnak) Fix a global field k. Asymtotically, 50% of elliptic curves over k have rank 0, and 50% have rank 1. Moreover, the average rank is $1/2$, that is

$$\mathrm{AveRank}_{\mathcal{E}}(X) = \frac{\sum_{E \in \mathcal{E}(X)} \mathrm{rank}(E(\mathbb{Q}))}{\pi_{\mathcal{E}}(X)} \to \frac{1}{2} \quad \text{as } X \to \infty.$$

Data

- The BHKSSW (Balakrishnan, Ho, Kaplan, Spicer, Stein, Weigandt) database covers all 238,764,310 elliptic curves up to height 26,998,673,868 $\approx 2.7 \cdot 10^{10}$.
  - Also six large-height data sets of 100,000 curves with height $\sim 10^k$ for $k = 11, 12, 13, 14, 15, 16$.

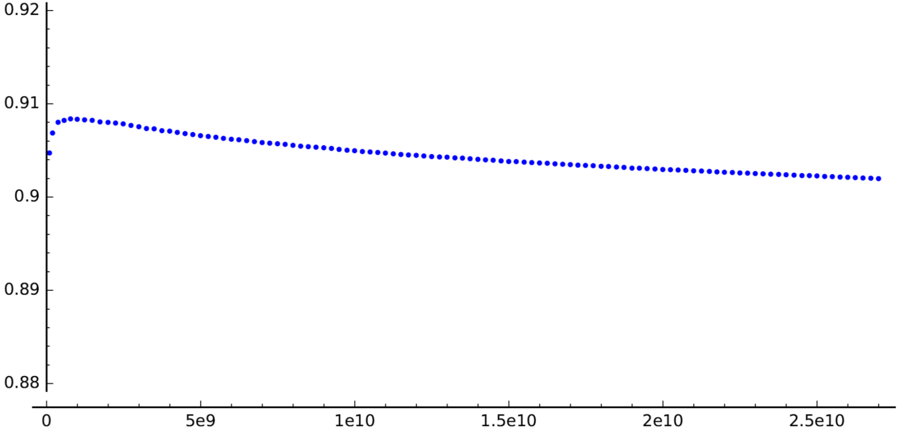


Figure: Values of $\mathrm{AveRank}_{\mathcal{E}}(X)$ from the BHKSSW database (blue dots). The local max happens at about $6 \cdot 10^8$. At $X = 2.7 \cdot 10^{10}$ value is $0.90197580\ldots$.

Theorem (Skinner, Bhargava-Shankar)

$0.216 \leq \lim_{X\to\infty} \mathrm{AveRank}_{\mathcal{E}}(X) \leq 0.885.$

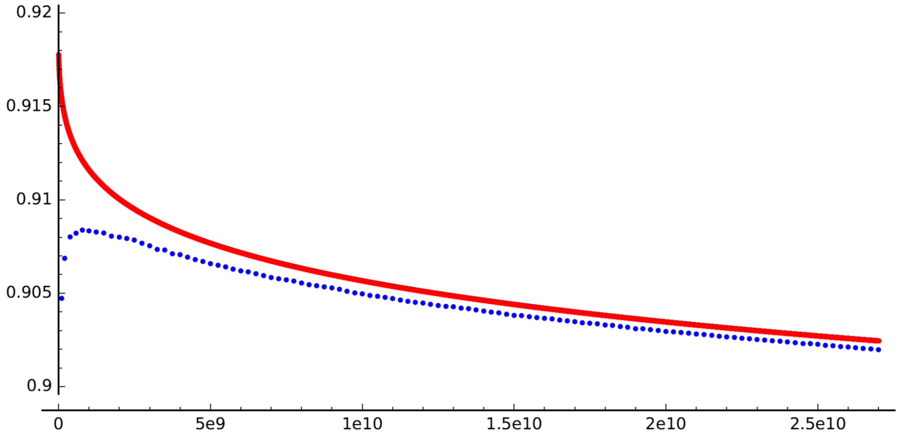


Figure: Values of $\text{AveRank}_{\mathcal{E}}(X)$ from the BHKSSW database (blue dots), and numerical integration of the approximation given by our model (in red).

According to the database, we have $\text{AveRank}_{\mathcal{E}}(2.7 \cdot 10^{10}) = 0.90197580$ while our approximation gives 0.90244770. Thus, the absolute error is 0.00047189 (note $(2.7 \cdot 10^{10})^{-1/3} \approx 0.0003$), which is a 0.0523% of the value.

X	AveRank(X)	X	AveRank(X)
10^{10}	0.905665	10^{50}	0.548880
10^{15}	0.846828	10^{75}	0.512531
10^{20}	0.766868	10^{100}	0.503256
10^{30}	0.649901	10^{150}	0.500215
10^{40}	0.585108	10^{200}	0.500006

Table: Conjectural approximate values of AveRank(X) obtained using our models.

How do we compute ranks?

We use **Selmer groups**: a cohomological-defined group where we can embed the (weak) Mordell-Weil group of an elliptic curve. Recall the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

How do we compute ranks?

We use **Selmer groups**: a cohomological-defined group where we can embed the (weak) Mordell-Weil group of an elliptic curve. Recall the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

Good news: Selmer groups are computable because they are defined locally. The elements of $\mathrm{Sel}_2(E/\mathbb{Q})$ can be interpreted as quartics that are everywhere locally solvable (solutions over $\mathbb{Q}_p$ for every $2 \leq p \leq \infty$).

How do we compute ranks?

We use **Selmer groups**: a cohomological-defined group where we can embed the (weak) Mordell-Weil group of an elliptic curve. Recall the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

Good news: Selmer groups are computable because they are defined locally. The elements of $\mathrm{Sel}_2(E/\mathbb{Q})$ can be interpreted as quartics that are everywhere locally solvable (solutions over $\mathbb{Q}_p$ for every $2 \leq p \leq \infty$).

Bad news: The Tate-Shafarevich group $Ш(E/\mathbb{Q})$ measures the failure of the local-to-global principle, and it is **hard** to compute. The elements of $Ш(E/\mathbb{Q})[2]$ can be interpreted as quartics that are everywhere locally solvable but not globally solvable (solutions over $\mathbb{Q}_p$ for every $2 \leq p \leq \infty$ but not over $\mathbb{Q}$).

How do we compute ranks?

We use **Selmer groups**: a cohomological-defined group where we can embed the (weak) Mordell-Weil group of an elliptic curve. Recall the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

Good news: Selmer groups are computable because they are defined locally. The elements of $\mathrm{Sel}_2(E/\mathbb{Q})$ can be interpreted as quartics that are everywhere locally solvable (solutions over $\mathbb{Q}_p$ for every $2 \leq p \leq \infty$).

Bad news: The Tate-Shafarevich group $Ш(E/\mathbb{Q})$ measures the failure of the local-to-global principle, and it is **hard** to compute. The elements of $Ш(E/\mathbb{Q})[2]$ can be interpreted as quartics that are everywhere locally solvable but not globally solvable (solutions over $\mathbb{Q}_p$ for every $2 \leq p \leq \infty$ but not over $\mathbb{Q}$).

We define the (2-)Selmer rank of $E(\mathbb{Q})$ by

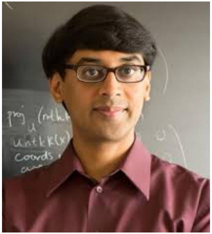
$$\text{selrank}(E(\mathbb{Q})) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2].$$

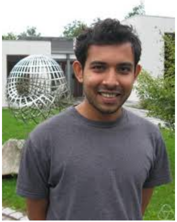
Then, $\text{rank}(E(\mathbb{Q})) \leq \text{selrank}(E(\mathbb{Q}))$.

We define the (2-)Selmer rank of $E(\mathbb{Q})$ by

$$\text{selrank}(E(\mathbb{Q})) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2].$$

Then, $\text{rank}(E(\mathbb{Q})) \leq \text{selrank}(E(\mathbb{Q}))$.





Theorem (Bhargava, Shankar, 2010)

The average size of $\text{Sel}_2(E/\mathbb{Q})$ *in the family of all elliptic curves is* 3.

They also conjecture that the average size of $\text{Sel}_p(E/\mathbb{Q})$ is $p+1$.

We will write $\pi_{\mathcal{S}_n}(X)$ for the number of elliptic curves $E/\mathbb{Q}$ up to height X with $\operatorname{selrank}(E(\mathbb{Q})) = n$.

We will write $\pi_{\mathcal{S}_n}(X)$ for the number of elliptic curves $E/\mathbb{Q}$ up to height X with $\mathrm{selrank}(E(\mathbb{Q})) = n$. Following work on quadratic twists by Heath-Brown, Monsky, Kane, and Swinnerton-Dyer:

Conjecture (Poonen–Rains, for $p = 2$)

$$\begin{aligned} s_n &= \mathrm{Prob}(\mathrm{selrank}(E(\mathbb{Q})) = n) = \lim_{X\to\infty} \frac{\pi_{\mathcal{S}_n}(X)}{\pi_{\mathcal{E}}(X)} \\ &= \left(\prod_{j\geq 0} \frac{1}{1+2^{-j}}\right) \cdot \left(\prod_{k=1}^{n} \frac{2}{2^k - 1}\right). \end{aligned}$$

s_0	s_1	s_2	s_3	s_4	s_5
0.209711	0.419422	0.279614	0.079889	0.010651	0.000687

Table: Values of $s_n = \mathrm{Prob}(\mathrm{selrank}(E(\mathbb{Q})) = n)$

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Answer: **NO.**

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Answer: **NO.** Reason: there is a bilinear pairing (Cassels-Tate)

$$Ш(E/\mathbb{Q}) \times Ш(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

which, for instance, forces $\#Ш(E/\mathbb{Q})[p^\infty]$ to be a square (if finite!).

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Answer: **NO.** Reason: there is a bilinear pairing (Cassels-Tate)

$$Ш(E/\mathbb{Q}) \times Ш(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

which, for instance, forces $\#Ш(E/\mathbb{Q})[p^\infty]$ to be a square (if finite!).

Delaunay (2001): Assume $Ш(E/\mathbb{Q})[p^\infty]$ is a random finite abelian group G together with a non-degenerate alternating bilinear pairing β.

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Answer: **NO.** Reason: there is a bilinear pairing (Cassels-Tate)

$$Ш(E/\mathbb{Q}) \times Ш(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

which, for instance, forces $\#Ш(E/\mathbb{Q})[p^\infty]$ to be a square (if finite!).

Delaunay (2001): Assume $Ш(E/\mathbb{Q})[p^\infty]$ is a random finite abelian group G together with a non-degenerate alternating bilinear pairing β. Put a weight on each group $1/\#\,\mathrm{Aut}^\beta(G)$, where $\mathrm{Aut}^\beta(G)$ are the automorphisms that preserve β.

Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Question

Is $Ш(E/\mathbb{Q})[p^\infty]$ a "random" p-group?

Answer: **NO.** Reason: there is a bilinear pairing (Cassels-Tate)

$$Ш(E/\mathbb{Q}) \times Ш(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

which, for instance, forces $\#Ш(E/\mathbb{Q})[p^\infty]$ to be a square (if finite!).

Delaunay (2001): Assume $Ш(E/\mathbb{Q})[p^\infty]$ is a random finite abelian group G together with a non-degenerate alternating bilinear pairing β. Put a weight on each group $1/\#\,\mathrm{Aut}^\beta(G)$, where $\mathrm{Aut}^\beta(G)$ are the automorphisms that preserve β. Obtain (Cohen-Lenstra type) heuristics for the probability of each isomorphism type for $Ш[p^\infty]$.

Delaunay (2001): Assume $\text{Ш}(E/\mathbb{Q})[p^\infty]$ is a random finite abelian group G together with a non-degenerate alternating bilinear pairing β. Put a weight on each group $1/\#\,\mathrm{Aut}^\beta(G)$, where $\mathrm{Aut}^\beta(G)$ are the automorphisms that preserve β. Obtain (Cohen-Lenstra type) heuristics for the probability of each isomorphism type for $\text{Ш}[p^\infty]$.

Delaunay (2001): Assume $Ш(E/\mathbb{Q})[p^\infty]$ is a random finite abelian group G together with a non-degenerate alternating bilinear pairing β. Put a weight on each group $1/\#\operatorname{Aut}^\beta(G)$, where $\operatorname{Aut}^\beta(G)$ are the automorphisms that preserve β. Obtain (Cohen-Lenstra type) heuristics for the probability of each isomorphism type for $Ш[p^\infty]$.

For instance, if the rank of $E/\mathbb{Q}$ is 0, then the probability that p divides $\#Ш$ is given by

$$f_0(2) = 1 - \prod_{k=1}^{\infty}(1 - (1/p)^{2k-1}).$$

E.g., $f_0(2) = 0.58\ldots$, $f_0(3) = 0.36\ldots$, and $f_0(5) = 0.20\ldots$

Bhargava, Kane, Lenstra, Poonen, Rains:
Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[p] \to 0.$$

Bhargava, Kane, Lenstra, Poonen, Rains:
Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

$$0 \to E(\mathbb{Q})/p^nE(\mathbb{Q}) \to \mathrm{Sel}_{p^n}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^n] \to 0.$$

Bhargava, Kane, Lenstra, Poonen, Rains:
Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

$$0 \to E(\mathbb{Q})/p^nE(\mathbb{Q}) \to \mathrm{Sel}_{p^n}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^n] \to 0.$$

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

a short exact sequence of $\mathbb{Z}_p$-modules. Model $Ш(E/\mathbb{Q})[p^\infty]$, allegedly a finite p-group, by:

Bhargava, Kane, Lenstra, Poonen, Rains:
Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

$$0 \to E(\mathbb{Q})/p^nE(\mathbb{Q}) \to \mathrm{Sel}_{p^n}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^n] \to 0.$$

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

a short exact sequence of $\mathbb{Z}_p$-modules. Model $Ш(E/\mathbb{Q})[p^\infty]$, allegedly a finite p-group, by:

$$0 \to \operatorname{Ker} R \to \mathbb{Z}_p^n \to \mathbb{Z}_p^n \to \mathbb{Z}_p^n/\operatorname{Col}(R) \to 0.$$

and $Ш(E/\mathbb{Q})[p^\infty] \leftrightsquigarrow (\mathbb{Z}_p^n/\operatorname{Col}(R))_{\mathrm{tors}}$.

Bhargava, Kane, Lenstra, Poonen, Rains:
Let $p \geq 2$ be a prime. Then:

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

$$0 \to E(\mathbb{Q})/p^n E(\mathbb{Q}) \to \mathrm{Sel}_{p^n}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^n] \to 0.$$

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

a short exact sequence of $\mathbb{Z}_p$-modules. Model $Ш(E/\mathbb{Q})[p^\infty]$, allegedly a finite p-group, by:

$$0 \to \operatorname{Ker} R \to \mathbb{Z}_p^n \to \mathbb{Z}_p^n \to \mathbb{Z}_p^n/\operatorname{Col}(R) \to 0.$$

and $Ш(E/\mathbb{Q})[p^\infty] \leftrightsquigarrow (\mathbb{Z}_p^n/\operatorname{Col}(R))_{\mathrm{tors}}$.

- If we want to model elliptic curves of rank r, fix $\operatorname{rank}(\operatorname{Ker}(R)) = r$.
- Remember that $Ш(E/\mathbb{Q})[p^\infty]$ has a non-deg. alt. bil. pairing, so R needs to be alternating.

Theorem: The distribution of $(\mathbb{Z}_p^n/\operatorname{Col}(R))_{\mathrm{tors}}$ over all alternating matrices R with $\operatorname{rank}\operatorname{Ker}(R) = r$, converges to Delaunay's distribution for curves of rank r, as $n \to \infty$.

Park, Poonen, Voight, Wood:
Model elliptic curves of height H as follows:

Park, Poonen, Voight, Wood:
Model elliptic curves of height H as follows:

- Choose a height H.

Park, Poonen, Voight, Wood:
Model elliptic curves of height H as follows:

- Choose a height H.
- Choose $n \geq 1$ uniformly at random (from an interval that depends on H).

Park, Poonen, Voight, Wood:

Model elliptic curves of height H as follows:

- Choose a height H.
- Choose $n \geq 1$ uniformly at random (from an interval that depends on H).
- Choose an $n \times n$ alternating matrix R_E with integer coefficients, with entries bounded by $X = X(H)$, chosen uniformly at random.

Park, Poonen, Voight, Wood:
Model elliptic curves of height H as follows:

- Choose a height H.
- Choose $n \geq 1$ uniformly at random (from an interval that depends on H).
- Choose an $n \times n$ alternating matrix R_E with integer coefficients, with entries bounded by $X = X(H)$, chosen uniformly at random.

Then, Coker(R_E) models $\text{Ш}(E/\mathbb{Q})$ and rank(Ker(R_E)) models rank($E(\mathbb{Q})$).

Park, Poonen, Voight, Wood:
Model elliptic curves of height H as follows:

- Choose a height H.
- Choose $n \geq 1$ uniformly at random (from an interval that depends on H).
- Choose an $n \times n$ alternating matrix R_E with integer coefficients, with entries bounded by $X = X(H)$, chosen uniformly at random.

Then, Coker(R_E) models $\text{Ш}(E/\mathbb{Q})$ and rank(Ker(R_E)) models rank($E(\mathbb{Q})$).

Consequences:

(a) For $1 \leq r \leq 20$, we have $\sum_{k=r}^{\infty} \pi_{\mathcal{R}_k}(X) = X^{(21-r)/24+o(1)}$.

(b) All but finitely many elliptic curves satisfy rank($E(\mathbb{Q})$) ≤ 21.

A PROBABILISTIC MODEL FOR THE DISTRIBUTION OF RANKS OF ELLIPTIC CURVES OVER $\mathbb{Q}$

ÁLVARO LOZANO-ROBLEDO

Abstract. In this article, we propose a new probabilistic model for the distribution of ranks of elliptic curves in families of fixed Selmer rank, and compare the predictions of our model with previous results, and with the databases of curves over the rationals that we have at our disposal. In addition, we document a phenomenon we refer to as *Selmer bias* that seems to play an important role in the data and in our models.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. The Mordell–Weil theorem states that the group $E(\mathbb{Q})$ of rational points on E is finitely generated and, therefore, we have an isomorphism

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E},$$

where $E(\mathbb{Q})_{\text{tors}}$ is the (finite) subgroup of points of finite order, and $R_E = \text{rank}(E(\mathbb{Q})) \geq 0$ is the rank of the elliptic curve. The torsion subgroups that arise over $\mathbb{Q}$ are well understood: Mazur's theorem settles what groups are possible ([21], [22]), the parametrization of the corresponding modular curves are known ([20]), and we know the distribution of elliptic curves with a prescribed torsion subgroup ([15]) as a function of the height of the curve. However, the distribution of ranks of elliptic curves is unknown. Several conjectures can be found in the literature (e.g., on the average rank, see [24]), and also some heuristic models ([29], [23]), but the basic questions about the distribution of the ranks remain unanswered. For instance, it is not known whether the rank can be arbitrarily large (currently, the largest rank known is 28, due to Noam Elkies - see [11] for Elkies' example, and other current records).

In this article, we propose a new probabilistic model for the distribution of ranks of elliptic curves (in families of fixed 2-Selmer rank) and explore its possible consequences. The model itself is built on a probability space of *test elliptic curves* and *test Selmer elements* in the spirit of Cramér's model for the prime numbers (see [6], [13]). As such, our model is a collection $\mathbf{T}$ of all possible sequences of (finite) sets of test elliptic curves of each height (with certain growth conditions as the height grows). The sequence of ordinary elliptic curves $\mathcal{E}$ over $\mathbb{Q}$ belongs to this class, and we make predictions about $\mathcal{E}$ from the asymptotic average behavior from sequences in $\mathbf{T}$ under the assumption of certain probabilistic hypotheses (see Sections 1.3, 5, and 7 for more details). We use the largest database of elliptic curves at our disposal ([1], which we will refer to as the BHKSSW database) in order to

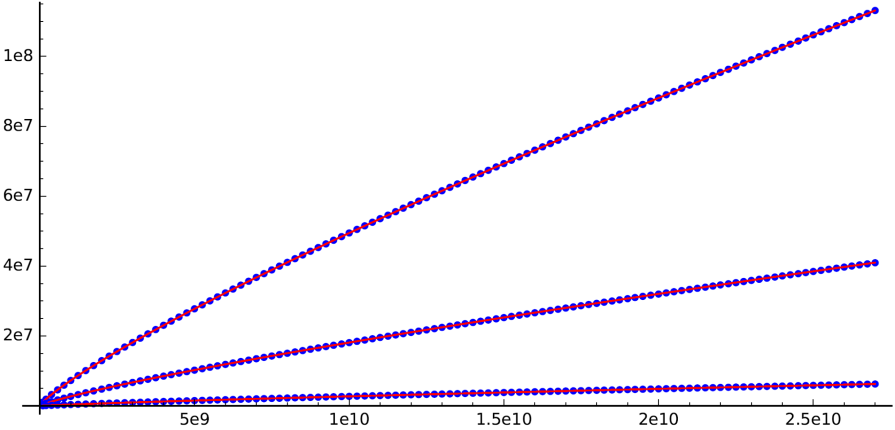


Figure: Values of $\pi_{\mathcal{R}_r}(X)$ from the BHKSSW database (blue dots) for $r = 1, 2, 3$, and the approximations predicted by our models (in red).

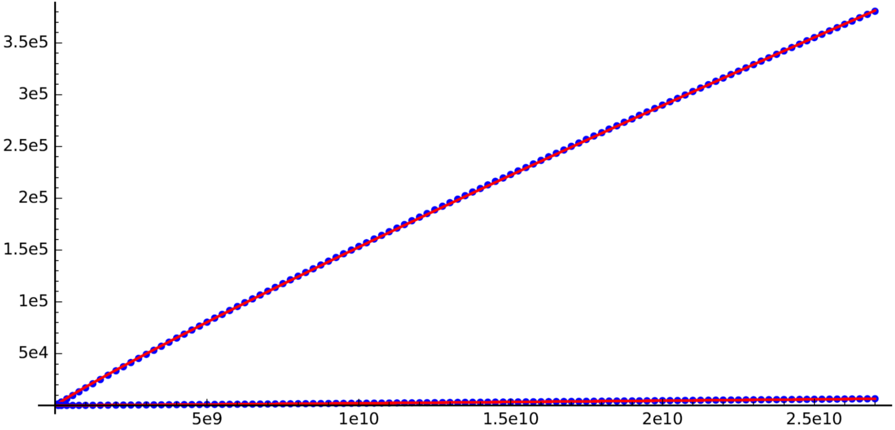


Figure: Values of $\pi_{\mathcal{R}_r}(X)$ from the BHKSSW database (blue dots) for $r = 4, 5$, and the approximations predicted by our models (in red).

	$r = 1$	2	3	4	5
$\pi_{\mathcal{R}_r}(2.7 \cdot 10^{10})$	113128929	40949289	6259157	380519	6481
Approx. value	113133971	41005107	6273138	381272	6438
$\lvert\text{Error}\rvert$	5042	55818	13981	753	43
Error %	0.004456	0.136310	0.223368	0.197887	0.663477
$\approx s_r \cdot X^{1/2}$	68848.72	45942.96	13112.47	1749.97	111.73

Table: Values of $\pi_{\mathcal{R}_r}(2.7 \cdot 10^{10})$ from the BHKSWW database, the approximate values (rounded to the closest integer) given by numerical integration of the formulas predicted by the models, the absolute error, the error as a percentage of the actual value of $\pi_{\mathcal{R}_r}$, and the size of the predicted error $s_r \cdot (2.7 \cdot 10^{10})^{1/2}$.

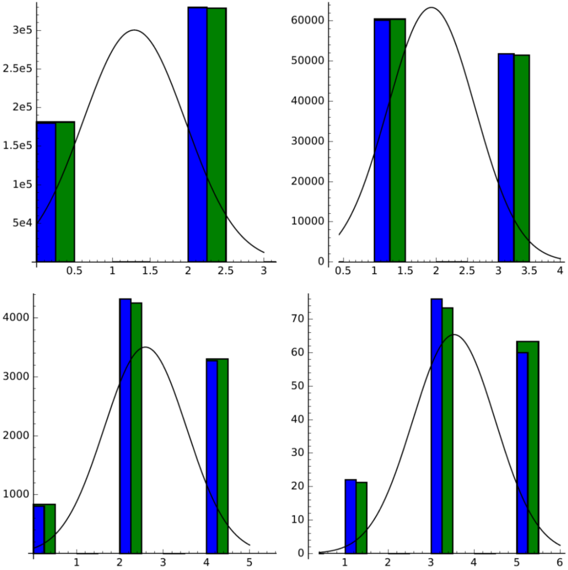


Figure: Distribution of Mordell–Weil ranks (in blue) among elliptic curves in $\mathcal{E}([2 \cdot 10^{10}, 2.025 \cdot 10^{10}])$ by Selmer rank $n = 2, 3, 4, 5$, and compared to the predicted M–W ranks (in green) that we would expect from the models.

n	$\pi_{\mathcal{S}_n}(I)$	M–W ranks observed in $\mathcal{S}_n$	M–W ranks predicted
2	509,845	$[180128, 0, 329717, 0, 0, 0]$	$[181246.58, 0, 328598.41, 0, 0, 0]$
3	111,926	$[0, 60149, 0, 51777, 0, 0]$	$[0, 60455.09, 0, 51470.90, 0, 0]$
4	8399	$[803, 0, 4321, 0, 3275, 0]$	$[836.68, 0, 4256.52, 0, 3305.78, 0]$
5	158	$[0, 22, 0, 76, 0, 60]$	$[0, 21.24, 0, 73.38, 0, 63.36]$

Table: Mordell–Weil ranks observed in the interval height interval $I = [2 \cdot 10^{10}, 2.025 \cdot 10^{10}]$ and the ranks predicted by the models.

THANK YOU

alvaro.lozano-robledo@uconn.edu

http://alozano.clas.uconn.edu/

"*If by chance I have omitted anything*
more or less proper or necessary,
I beg forgiveness,
since there is no one who is without fault
and circumspect in all matters."

Leonardo Pisano (Fibonacci), *Liber Abaci*.