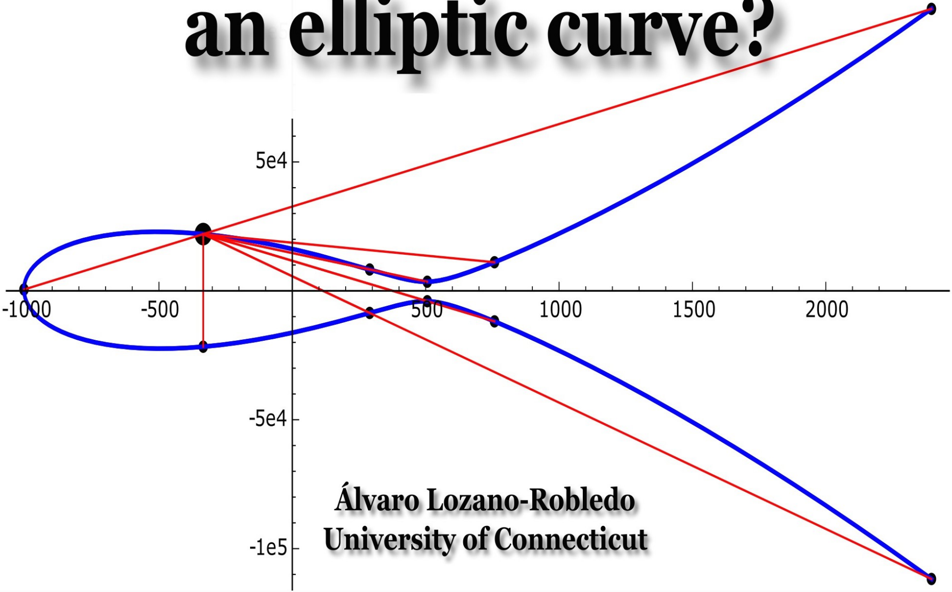
What is... an elliptic curve?

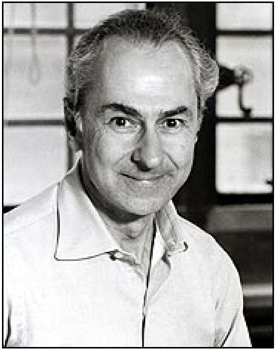


Álvaro Lozano-Robledo
University of Connecticut

The curve $y^2 + xy = x^3 - 749461x + 263897441$ as in the title screen is an example of an *elliptic curve*.

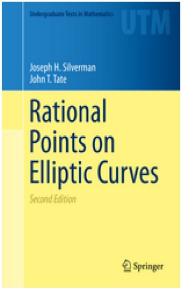
“It is possible to write endlessly on elliptic curves. (This is not a threat.)”

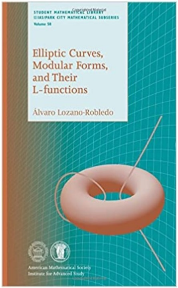
– Serge Lang, from *Elliptic Curves: Diophantine Analysis*

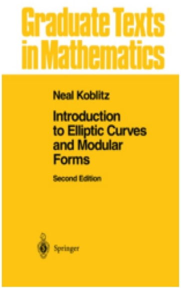


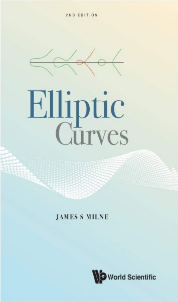
Foreword

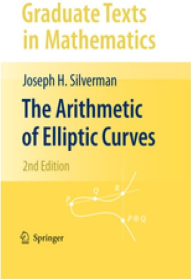
It is possible to write endlessly on elliptic curves. (This is not a threat.) We deal here with diophantine problems, and we lay the foundations, especially for the theory of integral points. We review briefly the analytic theory of the Weierstrass function, and then deal with the arithmetic aspects 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.

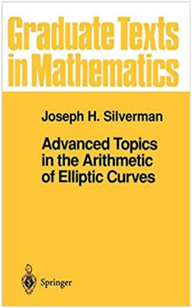

Undergraduate Texts in Mathematics
UTM
Joseph H. Silverman
John T. Tate
Rational Points on Elliptic Curves
Second Edition
Springer

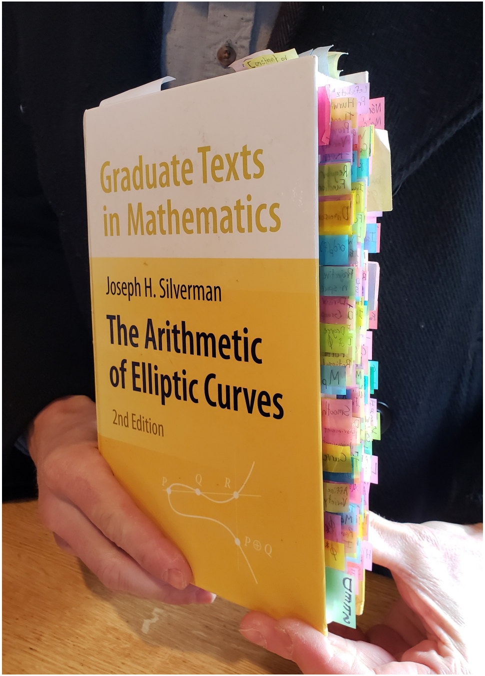

STUDENT MATHEMATICAL LIBRARY
IAS/PARK CITY MATHEMATICAL SUBSERIES
Volume 58
Elliptic Curves, Modular Forms, and Their L-functions
Álvaro Lozano-Robledo
American Mathematical Society
Institute for Advanced Study


Graduate Texts in Mathematics
Neal Koblitz
Introduction to Elliptic Curves and Modular Forms
Second Edition
Springer

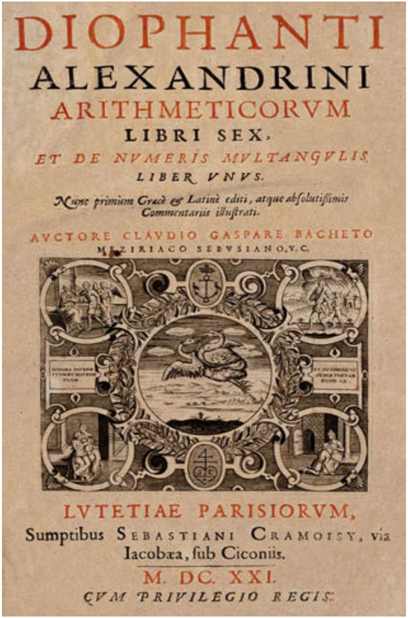

2ND EDITION
Elliptic Curves
JAMES S MILNE
World Scientific


Graduate Texts in Mathematics
Joseph H. Silverman
The Arithmetic of Elliptic Curves
2nd Edition
Springer


Graduate Texts in Mathematics
Joseph H. Silverman
Advanced Topics in the Arithmetic of Elliptic Curves
Springer


Graduate Texts in Mathematics
Joseph H. Silverman
The Arithmetic of Elliptic Curves
2nd Edition
P
Q
R
P⊕Q

What is an elliptic curve?


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis
Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

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 $\mathbb{Z}$? (**Davis, Matiyasevich, Putnam, Robinson: No**)

Examples of diophantine equations and rational points:

- $3x + 5y = 1$, a line on the plane

$$(-3, 2) \text{ is a point on the line.}$$

- $x^2 + y^2 = z^2$, pythagorean triples

$$(3, 4, 5) \text{ is a pythagorean triple.}$$

- $x^3 + y^3 + z^3 = 42$, expressions of 42 as the sum of three cubes

  $(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$

  is an expression recently found by A. Booker and D. Sutherland.

- $Y^4 + 5X^4 - 6X^2Y^2 + 6X^3Z + 26X^2YZ + 10XY^2Z - 10Y^3Z - 32X^2Z^2 - 40XYZ^2 + 24Y^2Z^2 + 32XZ^3 - 16YZ^3 = 0$,
  the *cursed curve* (the modular curve $X_s(13)$).

$$(1, 1, 2) \text{ is a (CM) point on the cursed curve.}$$

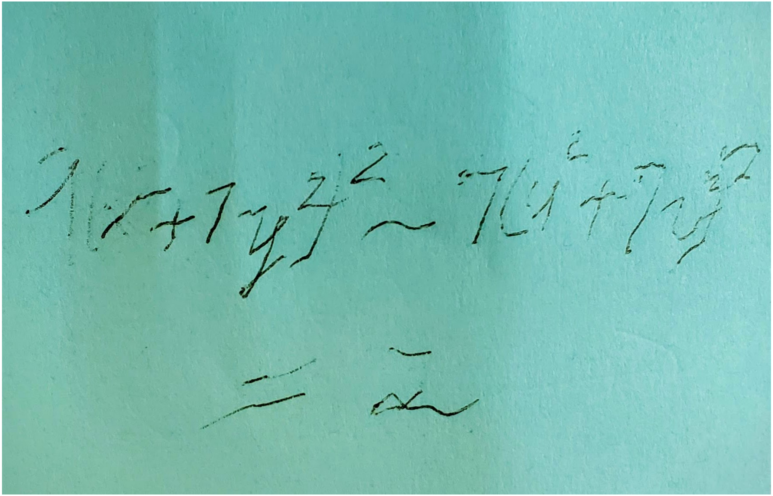
Annals of Mathematics **189** (2019), 885–944
https://doi.org/10.4007/annals.2019.189.3.6

Explicit Chabauty–Kim for the split Cartan modular curve of level 13

By Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk

Abstract

We extend the explicit quadratic Chabauty methods developed in previous work by the first two authors to the case of non-hyperelliptic curves. This results in a method to compute a finite set of p-adic points, containing the rational points, on a curve of genus $g \geq 2$ over the rationals whose Jacobian has Mordell–Weil rank g and Picard number greater than one, and which satisfies some additional conditions. This is then applied to determine the rational points of the modular curve $X_{\mathrm{s}}(13)$, completing the classification of non-CM elliptic curves over $\mathbf{Q}$ with split Cartan level structure due to Bilu–Parent and Bilu–Parent–Rebolledo.



A gift from Martin Davis, the diophantine equation

$$9(x^2 + 7y^2)^2 - 7(u^2 + 7v^2)^2 = 2.$$

What diophantine equations can we solve?

- **Polynomials in one variable**, $f(x) = 0$, with integer coefficients:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

  Divisibility theory: if $x_0 = \frac{m}{n}$ is a root, then $m \mid a_0$ and $n \mid a_n$.

- **Polynomials in two variables, degree 1**:

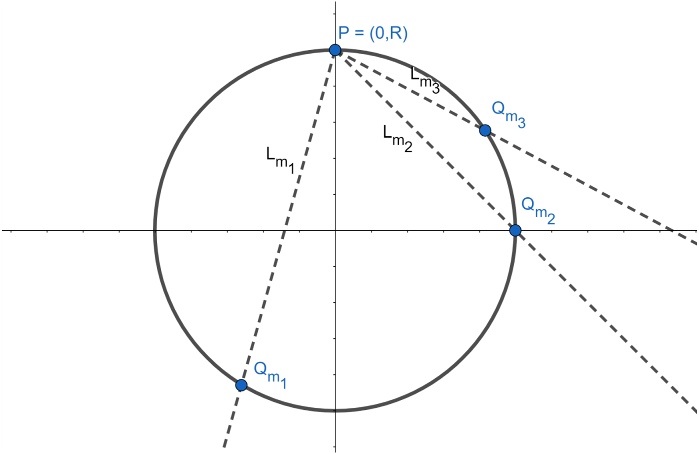
$$L : ax + by = c.$$

  Theory of greatest common divisors: there is an integral point on L if and only if $\gcd(a, b) \mid c$.

- **Polynomials in two variables, degree 2**:

$$C : ax^2 + by^2 + cxy + dx + ey + f = 0.$$

  Hasse–Minkowski (local-to-global) theory determines existence of one point. Stereographic projection finds the rest.



A parametrization via stereographic projection of the rational points on the circle $x^2 + y^2 = R^2$ of radius R is given by

$$Q_m = \left(-\frac{2Rm}{(m^2+1)}, \frac{R(m^2-1)}{(m^2+1)} \right).$$

$$C : f(x_1, x_2) = 0$$

When C is smooth (projectively!), of degree 3 (genus 1), we lack an algorithm that will determine whether there are **any** rational points on C, or, if one exists, an algorithm that will determine **all** the rational points on the curve C.

Definition

An elliptic curve E over a field F is a (projective) smooth cubic curve (genus one), with at least one point defined over F.

- **Fact:** every elliptic curve has a (Weierstrass) model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ for some } a_i \in F.$$

- We are interested in determining all F-rational points on E:

$$E(F) = \{(x_0, y_0) \in E : x_0, y_0 \in F\} \cup \{\mathcal{O} = [0 : 1 : 0]\}.$$

$$C : f(x_1, x_2) = 0$$

When C is smooth (projectively!), of degree 3 (genus 1), we lack an algorithm that will determine whether there are **any** rational points on C, or, if one exists, an algorithm that will determine **all** the rational points on the curve C.

Definition

An elliptic curve E over a field F is a (projective) smooth cubic curve (genus one), with at least one point defined over F.

Example

Let $E/\mathbb{Q}$ be the curve $y^2 = x^3 - x$. Then:

$$E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\},$$

where $\mathcal{O} = [0 : 1 : 0]$, in projective coordinates, in the "point at infinity."

$$C : f(x_1, x_2) = 0$$

When C is smooth (projectively!), of degree 3 (genus 1), we lack an algorithm that will determine whether there are **any** rational points on C, or, if one exists, an algorithm that will determine **all** the rational points on the curve C.

Definition

An elliptic curve E over a field F is a (projective) smooth cubic curve (genus one), with at least one point defined over F.

Example

Let $E/\mathbb{Q}$ be the curve $X^3 + Y^3 = 1$. Then, $E(\mathbb{Q})$ is in bijection with $E'(\mathbb{Q})$, where $E' : y^2 = x^3 - 432$ via $\psi\colon E \to E'$ given by

$$\psi((X, Y)) = \left(\frac{12}{X+Y}, \frac{36(X-Y)}{X+Y}\right), \ \psi^{-1}((x, y)) = \left(\frac{36+y}{6x}, \frac{36-y}{6x}\right).$$

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

- **Fermat's last theorem** was proved via the so-called Frey curve $Y^2 = X(X - A^n)(X + B^n)$, where $A^n + B^n = C^n$.
- The **congruent number problem** is connected 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.
- **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.
- **Elliptic curve cryptography** is widely used in internet applications (e.g., WhatsApp end-to-end encryption).

The Congruent Number Problem

Let $n \geq 1$ be a natural number. Is there a right triangle (a, b, c) with rational sides $a, b, c \in \mathbb{Q}$ whose area is precisely n?

Example

The number $n = 6$ is a congruent number because it is the area of the right triangle $(3, 4, 5)$.

Example

The right triangles are parametrized $(e^2 - f^2, 2ef, e^2 + f^2)$ for $e > f \geq 1$. Hence, $n = ef(e^2 - f^2)$ is a congruent number. For instance, $n = 30$ is the area of $(5, 12, 13)$.

The number $n = 1$ is *not* the area of a right triangle with rational sides (proved by Fermat). The number $n = 5$ is a congruent number, but it is not the area of a right triangle with *integer* side lengths.

In *Flos* (circa 1225), **Leonardo “Bigollo” Pisano (a.k.a. Fibonacci)** found a right triangle of area $n = 5$ in response to a challenge by the Roman Emperor Frederick II:

$$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right).$$

The connection between congruent numbers and elliptic curves:

Theorem (Congruent numbers $\leftrightarrow$ Points on elliptic curves)

There is a 1-1 correspondence between the sets

- $\{(a, b, c) : a^2 + b^2 = c^2,\ \frac{ab}{2} = n\}$ *and*
- $\{(x, y) : y^2 = x^3 - n^2 x,\ y \neq 0\}$,

given by

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \quad (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

Example

Fibonacci's triangle $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ of area $n = 5$ maps to the point

$$P = \left(\frac{25}{4}, \frac{75}{8}\right)$$

on the curve $y^2 = x^3 - 25x$. (And P maps to Fibonacci's triangle.)

The connection between congruent numbers and elliptic curves:

Theorem (Congruent numbers $\leftrightarrow$ Points on elliptic curves)

There is a 1-1 correspondence between the sets

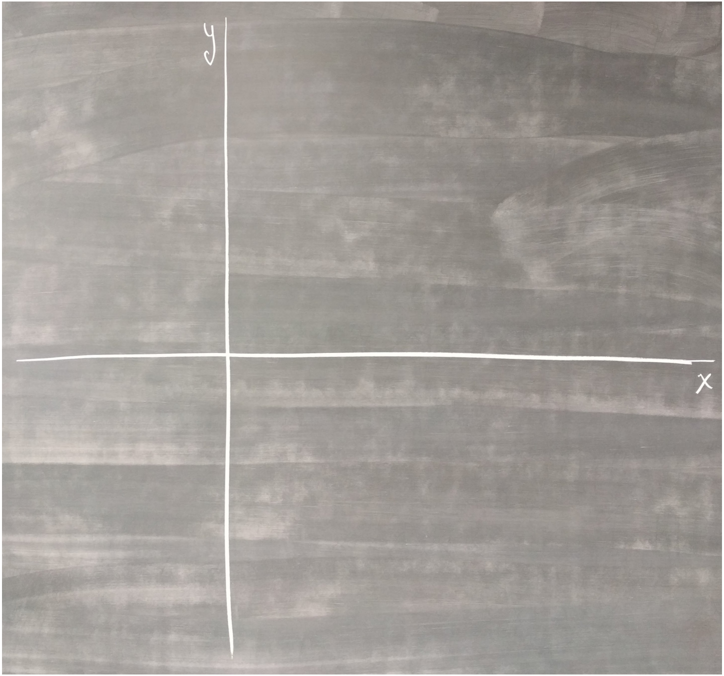
- $\{(a,b,c) : a^2+b^2=c^2,\ \frac{ab}{2}=n\}$ *and*
- $\{(x,y) : y^2=x^3-n^2x,\ y\neq 0\}$,

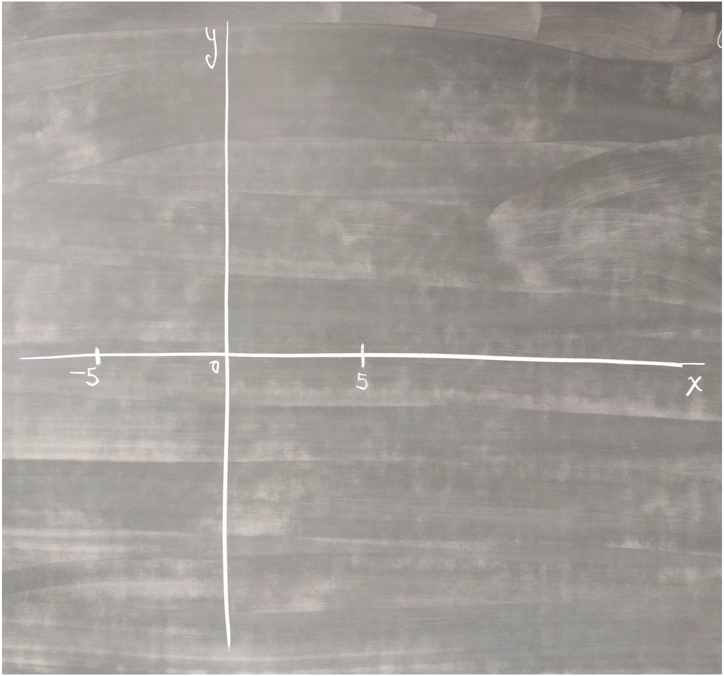
given by

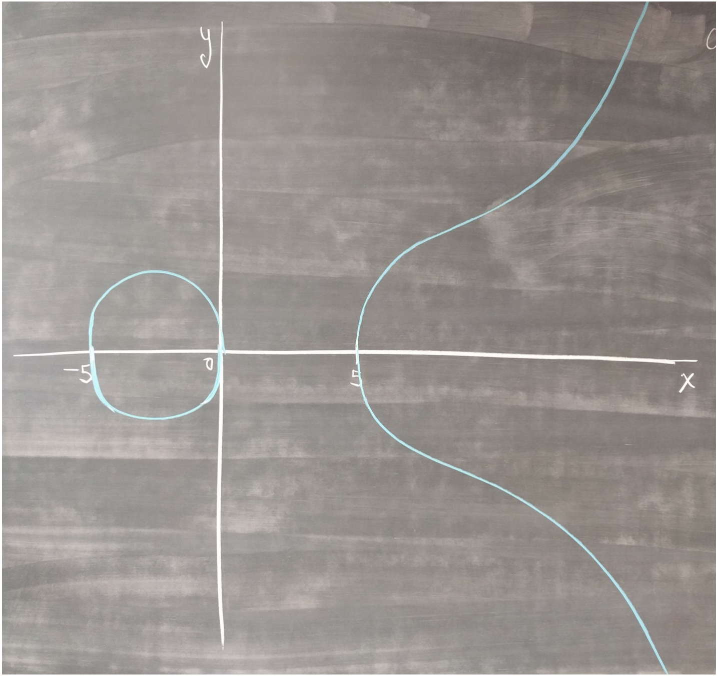
$$(a,b,c)\mapsto\left(\frac{nb}{c-a},\frac{2n^2}{c-a}\right),\ (x,y)\mapsto\left(\frac{x^2-n^2}{y},\frac{2nx}{y},\frac{x^2+n^2}{y}\right).$$

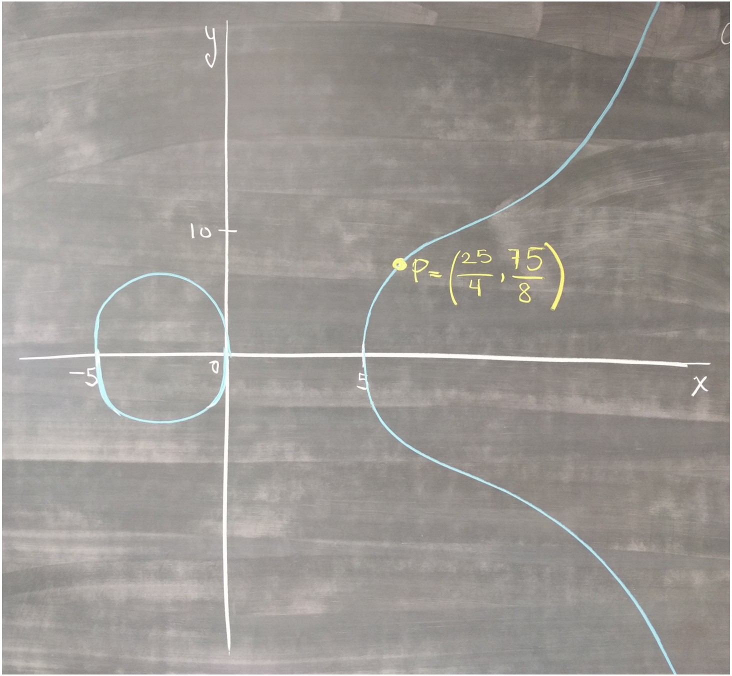
Via the previous correspondence, right triangles with area $n=5$ correspond to points on $y^2=x^3-25x$ with non-zero y-coordinate.

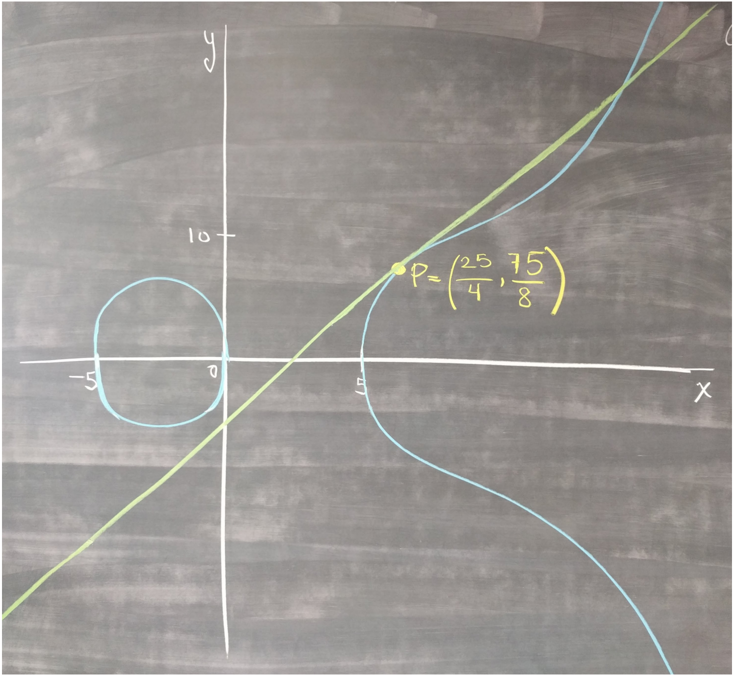
Let's **grab some chalk** and use the theory of elliptic curves to find another right triangle of area 5.

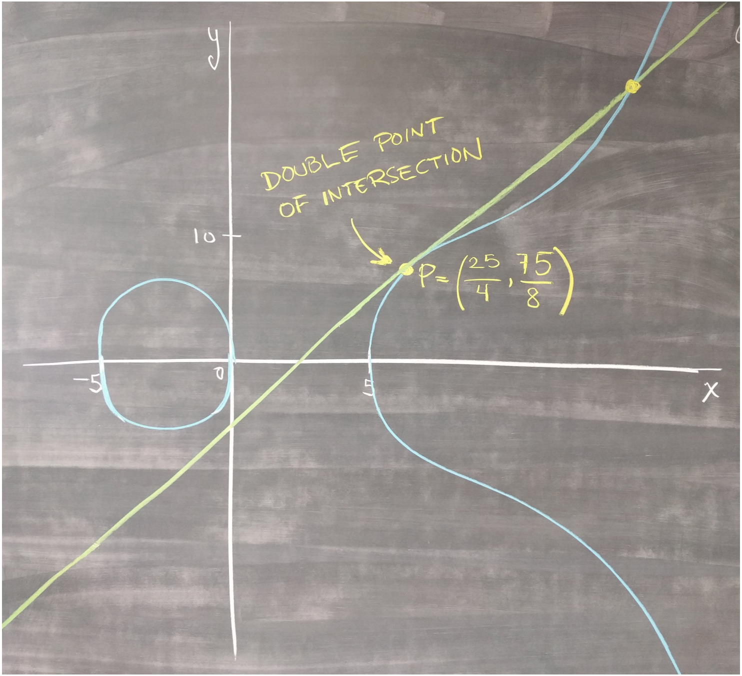

y
x

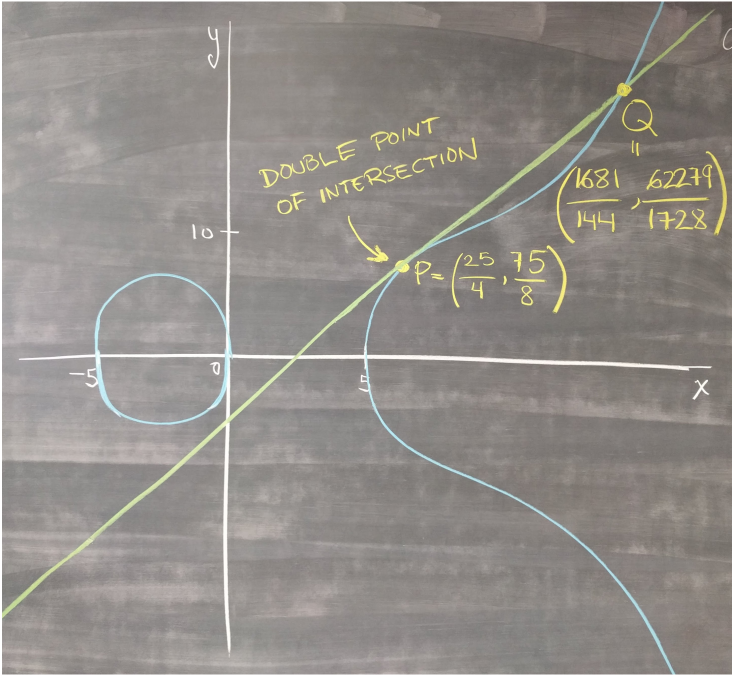

y
-5
0
5
x


y
-5
0
5
x


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


y
10
$P = \left(\frac{25}{4}, \frac{75}{8}\right)$
-5
0
5
x


y
10
-5
0
5
x
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)

Theorem

There is a 1-1 correspondence between the sets

- $\{(a, b, c) : a^2 + b^2 = c^2,\ \frac{ab}{2} = n\}$ *and*
- $\{(x, y) : y^2 = x^3 - n^2 x,\ y \neq 0\}$,

given by

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right),\ (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

Example

The point $P = (\frac{1681}{144}, \frac{62279}{1728})$ on the curve $y^2 = x^3 - 25x$ corresponds to the triangle

$$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348} \right)$$

of area 5.

For a fixed $n \geq 1$, the curve $y^2 = x^3 - n^2 x$ is an example of an elliptic curve.

Definition

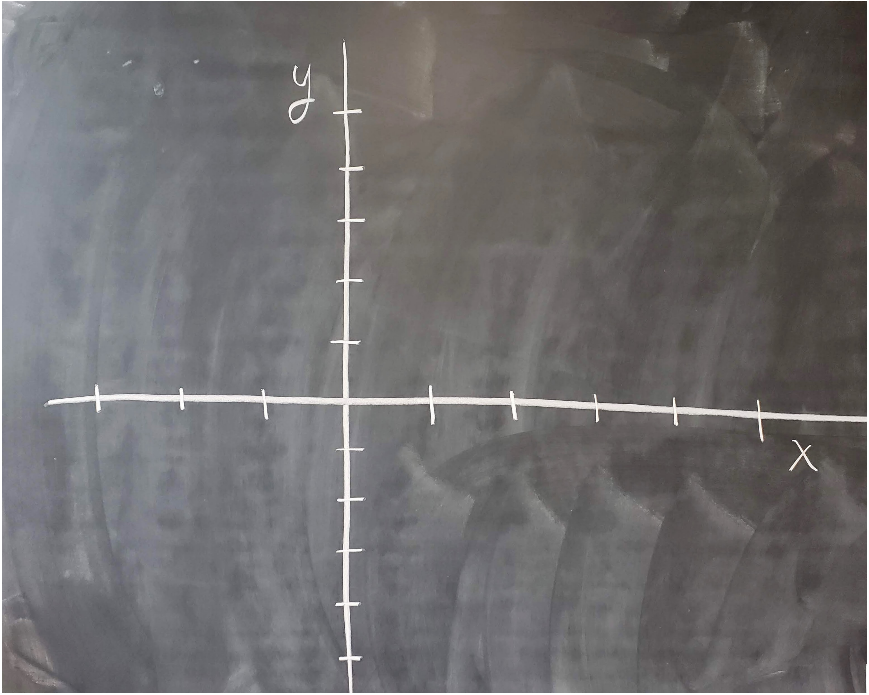
An elliptic curve E over a field F is a (projective) smooth cubic curve (genus one), with at least one point defined over F.

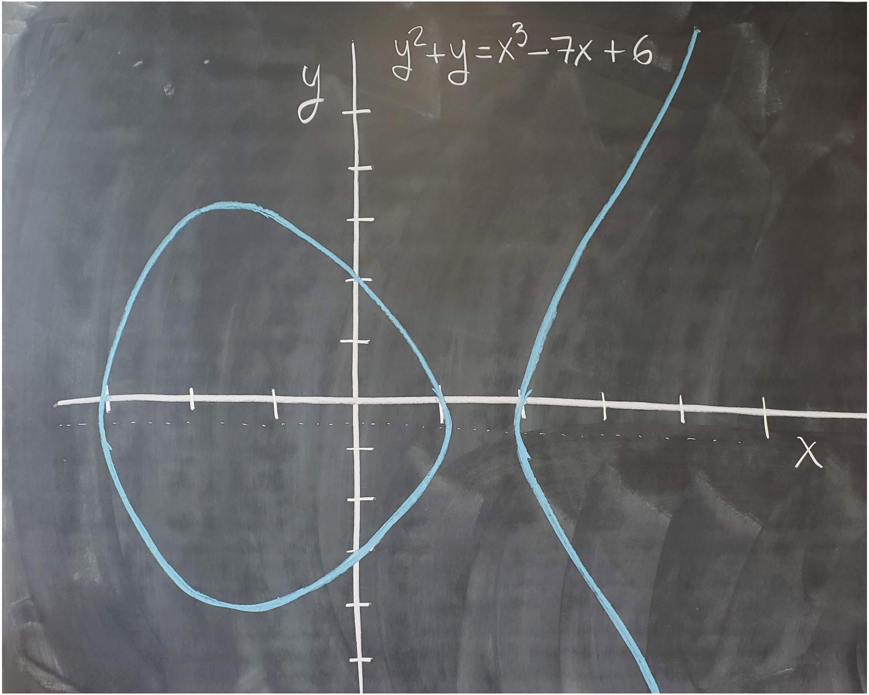
We are interested in determining all F-rational points on E:

$$E(F) = \{(x_0, y_0) \in E : x_0, y_0 \in F\} \cup \{\mathcal{O} = [0 : 1 : 0]\}.$$

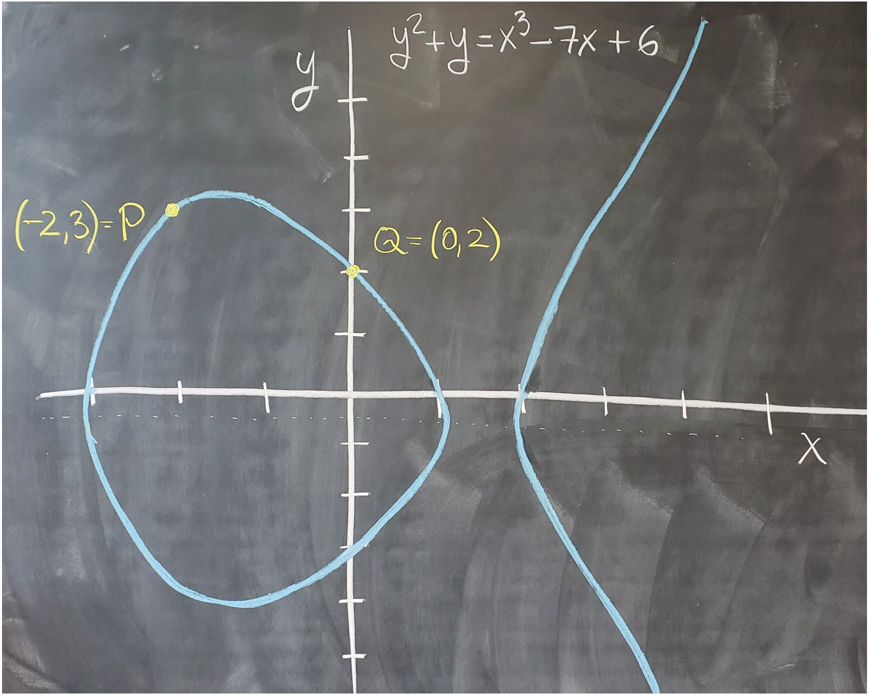
KEY FEATURE OF ELLIPTIC CURVES:

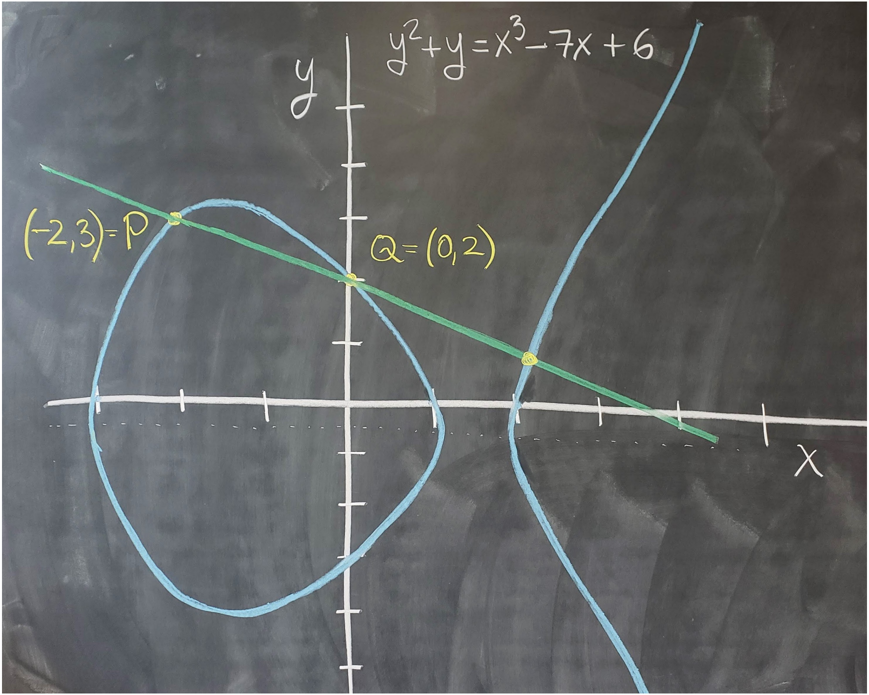
The set of F-rational points $E(F)$ of an elliptic curve E/F can be endowed with a group structure, defined geometrically (also algebraically through groups of divisors).


y
x

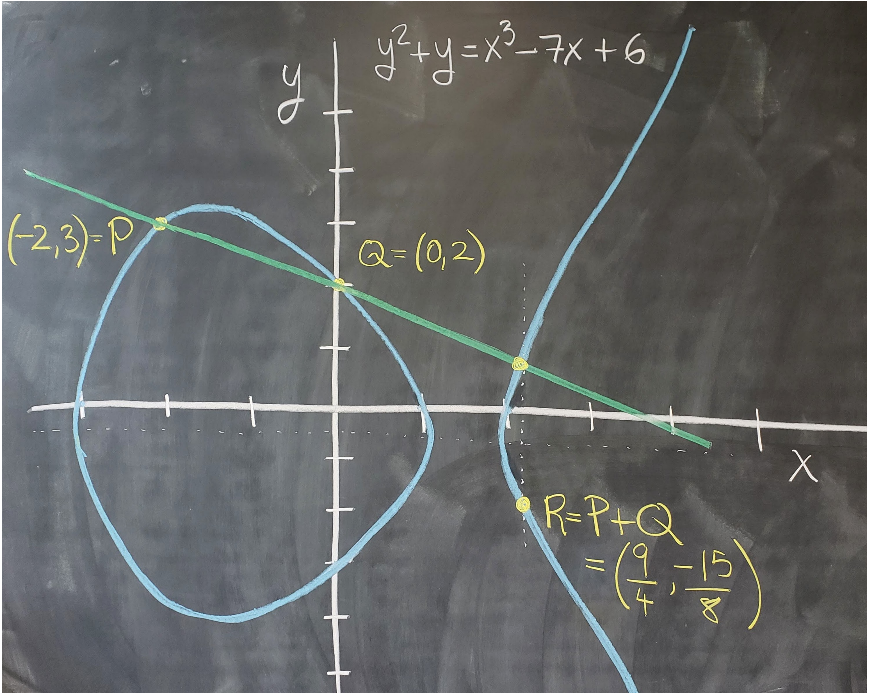


$y^2+y=x^3-7x+6$
y
x

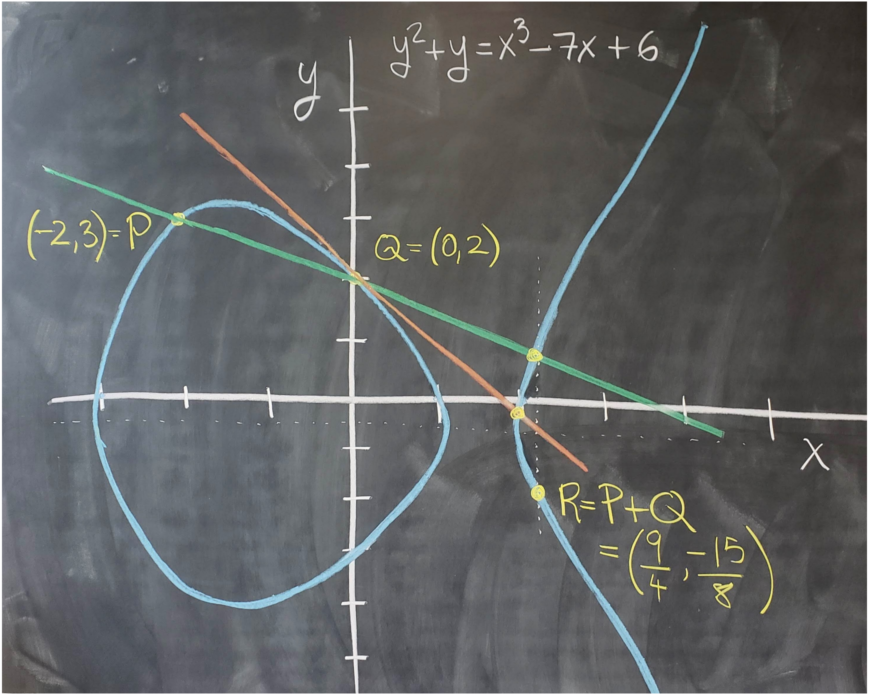

$y^2 + y = x^3 - 7x + 6$
y
x
$(-2,3) = P$
$Q = (0,2)$



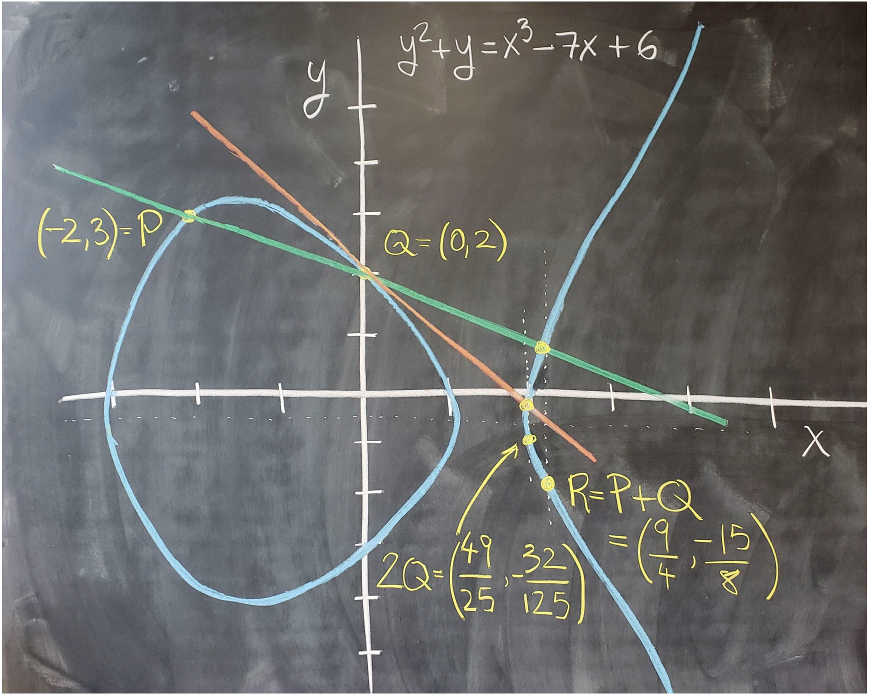
y²+y=x³−7x+6
y
(−2,3)=P
Q=(0,2)
x



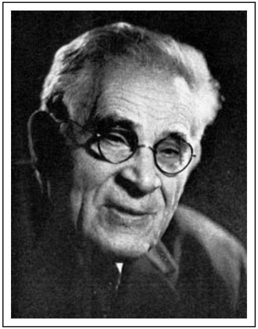
y² + y = x³ − 7x + 6
y
(−2,3) = P
Q = (0,2)
R = P + Q
= (9/4, −15/8)
x



$y^2+y=x^3-7x+6$
y
x
$(-2,3)=P$
$Q=(0,2)$
$R=P+Q$
$=\left(\frac{9}{4},\frac{-15}{8}\right)$



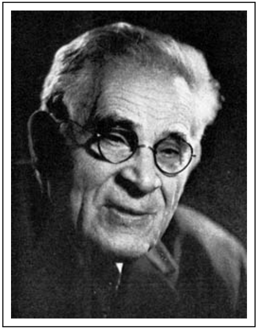
$y^2+y=x^3-7x+6$
y
x
$(-2,3)=P$
$Q=(0,2)$
$R=P+Q$
$=\left(\frac{9}{4},-\frac{15}{8}\right)$
$2Q=\left(\frac{49}{25},-\frac{32}{125}\right)$



Louis Mordell
1888 – 1972

Theorem (Mordell, 1922)

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



Louis Mordell
1888 – 1972

André Weil
1906 – 1998

Theorem (Mordell–Weil, 1928)

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

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:

$$E_2(\mathbb{Q}) = \{\mathcal{O}, (2, \pm 3), (0, \pm 1), (-1, 0)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

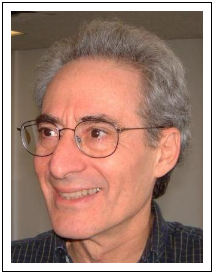
3. The curve $E_3/\mathbb{Q} : y^2 = x^3 - 2$ does not have any rational torsion points other than $\mathcal{O}$. However, $E_3(\mathbb{Q}) = \langle (3, 5) \rangle \cong \mathbb{Z}$.

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

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

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

What torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ are possible?



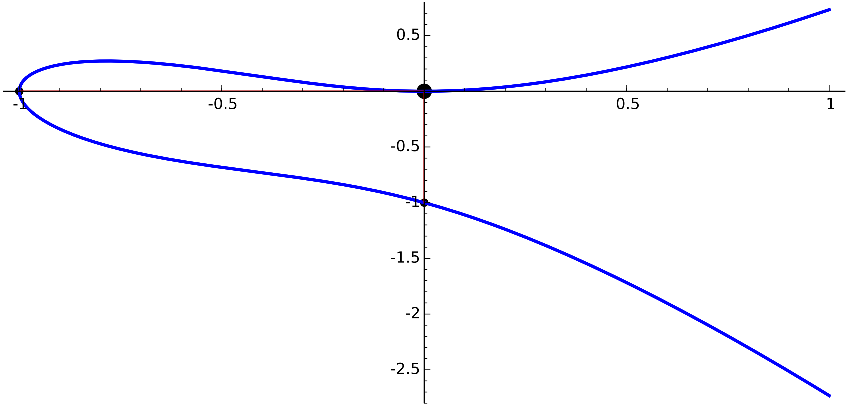
Barry Mazur

Theorem (Levi–Ogg Conjecture; Mazur, 1977)

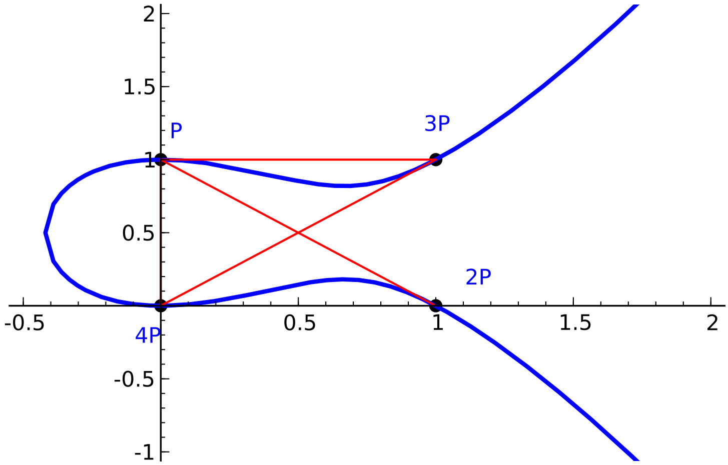
Let $E/\mathbb{Q}$ be an elliptic curve. Then

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

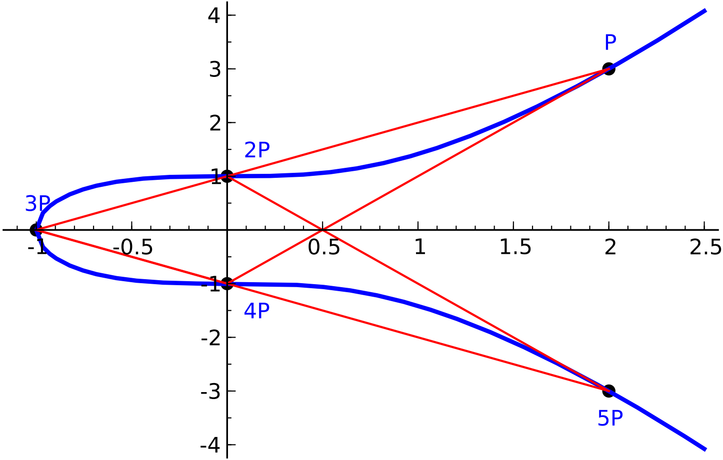
Moreover, each possible group appears infinitely many times.



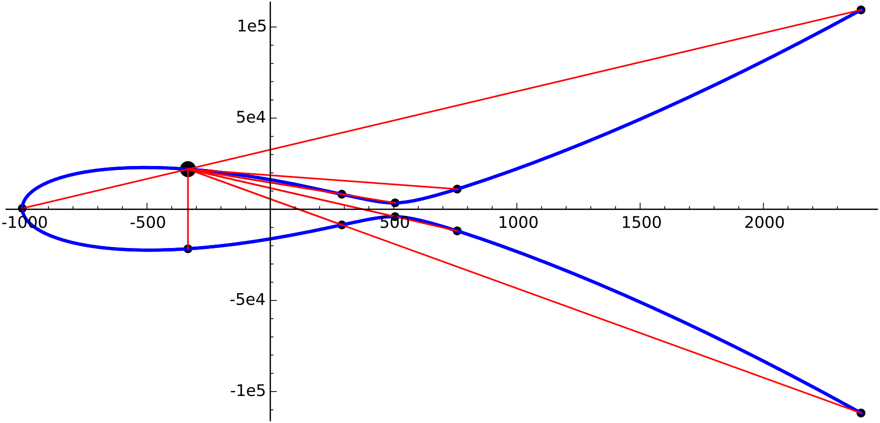
The elliptic curve $E/\mathbb{Q} : y^2 + xy + y = x^3 + x^2$
has a point $P = (0, 0)$ of order 4.



The curve $E/\mathbb{Q} : y^2 - y = x^3 - x^2$ has a point $P = (0, 1)$ of order 5.



The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + 1$ has a point $P = (2, 3)$ of order 6.



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

$$y^2 + xy = x^3 - 749461x + 263897441$$

“Torsion Groups and Galois Representations of Elliptic Curves”
Zagreb (Croatia), June 25-29, 2018.

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

What ranks $R_{E/\mathbb{Q}}$ of elliptic curves over $\mathbb{Q}$ are possible?

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?

Example (2006): Elkies' elliptic curve of rank ≥ 28 ($= 28$ under GRH!)

$$y^2 + xy + y = x^3 - x^2 - (20067762415575526585033208209338542750930230312178956502)x + (34481611795030556467032985690390720374855944359319180361266008296291939448732243429)$$

Independent points of infinite order:

Noam Elkies

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

$$P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$$

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

$$\vdots$$

$$
\begin{aligned}
P_4 =&[213913026013915666492982137,\\
&366395091714397292024214596929412975275311]\\
P_5 =&[153470676446712072388547733 7,\\
&854295853460176942890210328627810727995311]\\
P_6 =&[-273107948787567703334157506 3,\\
&2625218154843321916412840726239021433875311]\\
P_7 =&[277572626684457164970545853 7,\\
&128457554740140602488694876990826403699311]\\
P_8 =&[149438572932718895754183381 7,\\
&884866055277334059861164945140492334114511]\\
P_9 =&[186843822862088735850906525 7,\\
&592374032144377087127251403930593585891311]\\
P_{10} =&[200894510882574377486654253 7,\\
&476906778801255528821517507815414247115311]\\
P_{11} =&[234836054091802516965163293 7,\\
&174929300062005578573403324764488043635311]
\end{aligned}
$$

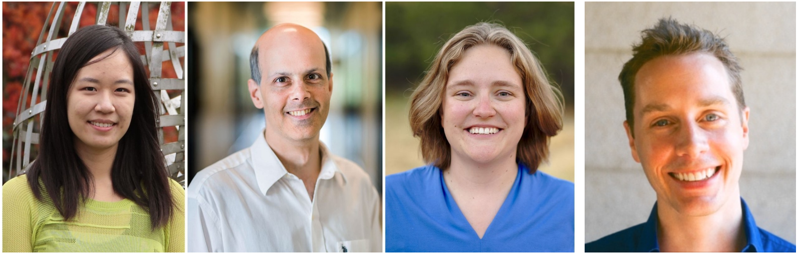
*P*12 = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]
P13 = [2924128607708061213363288937, 28350264431488878501488356474767375899531]
P14 = [5374993891066061893293934537, 286188908427263386451175031916479893731531]
P15 = [1709690768233354523334008557, 71898834974686089466159700529215980921631]
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]

Open Problem

Can the rank $R_{E/\mathbb{Q}}$ of an elliptic curve be arbitrarily large?

Conjectures and heuristic arguments for and against:

- Néron (1950), Honda (1960): Yes (bounded).
- Cassels (1966), Tate (1974), Mestre (1982), Silverman (1986, 2009), Brumer (1992), Ulmer (2002), Farmer–Gonek–Hughes (2007): No (unbounded).
- Rubin–Silverberg (2000), Granville (2006), Watkins (2015), Park–Poonen–Voight–Wood (2016): Yes (bounded).



Jennifer Park, Bjorn Poonen, Melanie Matchett Wood, John Voight.

Conjecture (Park, Poonen, Voight, Wood)

The ranks $R_{E/\mathbb{Q}}$ are bounded, and there are only finitely many rank values above 21.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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

Donald Anderson, first poster child.

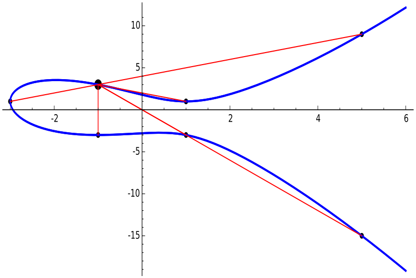
The torsion subgroups over $\mathbb{Q}$ are the "poster child" of what an arithmetic group should be like. Torsion subgroups are:

- Computable
- Classified
- Parametrized in families
- Statistically understood

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



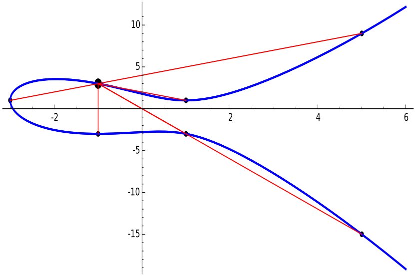
The curve $E : y^2 + xy + y = x^3 + x^2 - 4x + 5$ (`42.a5`) has torsion subgroup $\langle(-1, 3)\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

- **Computable**
  - Nagell–Lutz theorem.
  - Division polynomials.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E: y^2 + xy + y = x^3 + x^2 - 4x + 5$ (42.a5) has torsion subgroup $\langle(-1, 3)\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

- **Classified**
  - Mazur's theorem:

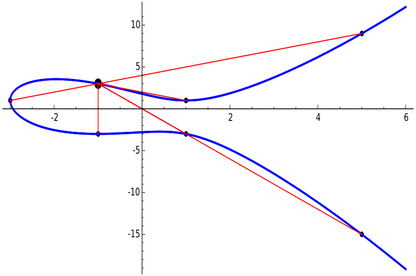
$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z}, & \text{or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \end{cases}$$

where $1 \leq M \leq 10$ or $M = 12$, and $1 \leq N \leq 4$.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E : y^2 + xy + y = x^3 + x^2 - 4x + 5$ (`42.a5`) has torsion subgroup $\langle(-1,3)\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

- **Parametrized in families**
  - Kubert et al.:

e.g.,
elliptic curves with $\mathbb{Z}/8\mathbb{Z}$ tors.:

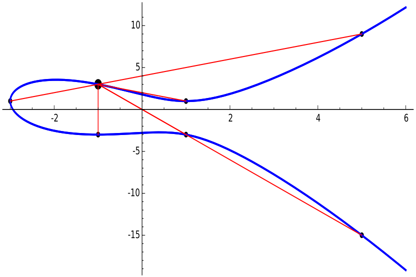
$$E : y^2+(1-a)xy-by^2 = x^3-bx^2$$

with $b = (2t-1)(t-1)$ and $a = b/t$, for any $t \neq 0, 1/2, 1$.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E' : y^2 + \frac{1}{3}xy - \frac{2}{9}y = x^3 - \frac{2}{9}x^2$ ($\cong_{\mathbb{Q}}$ `42.a5`) has torsion subgroup $\langle(-1,3)\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

- **Parametrized in families**
  - Kubert et al.:

  e.g.,
  elliptic curves with $\mathbb{Z}/8\mathbb{Z}$ tors.:

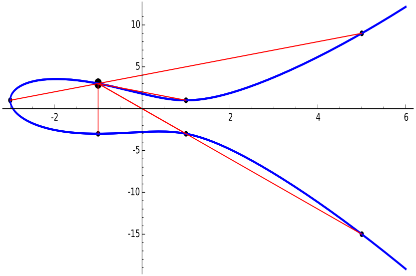
  $E : y^2+(1-a)xy-by^2 = x^3-bx^2$

  with $b = (2t-1)(t-1)$ and
  $a = b/t$, for any $t \neq 0, 1/2, 1$.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E : y^2 + xy + y = x^3 + x^2 - 4x + 5$ (`42.a5`) has torsion subgroup $\langle(-1,3)\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

- **Statistically understood**
  - Harron–Snowden (2013):

Let $N_G(X)$ be the number of elliptic curves $E/\mathbb{Q}$ with (naive) height $\leq X$ and $E(\mathbb{Q})_{\text{tors}} \cong G$. Then, there are positive constants $C_1, C_2, d(G)$ such that

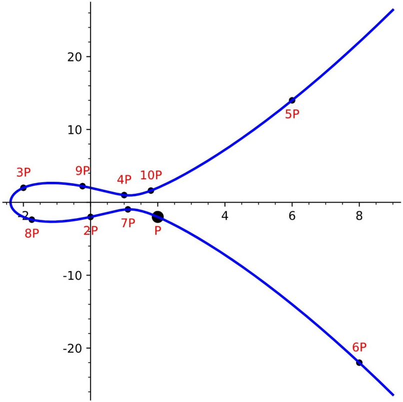
$$C_1 X^{d(G)} \leq N_G(X) \leq C_2 X^{d(G)}.$$

E.g., $d(\{0\}) = 5/6$ and $d(\mathbb{Z}/8\mathbb{Z}) = 1/12$.

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E : y^2 = x^3 - 4x + 4$ ($\texttt{88.a1}$) has trivial torsion subgroup and rank 1, with $E(\mathbb{Q}) = \langle (2, -2) \rangle \cong \mathbb{Z}$.

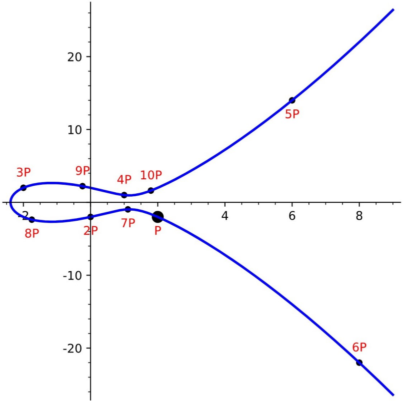
How about the rank?

- Computable?
- Classified?
- Parametrized in families?
- Statistically understood?

Goal

Our goal is to understand the possible structures of $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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



The curve $E : y^2 = x^3 - 4x + 4$ (`88.a1`) has trivial torsion subgroup and rank 1, with $E(\mathbb{Q}) = \langle (2, -2) \rangle \cong \mathbb{Z}$.

How about the rank?

~~· Computable?~~ Maybe

~~· Classified?~~ No

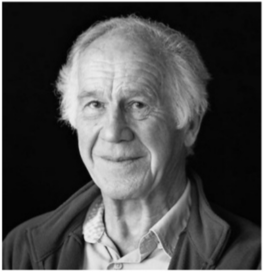
~~· Parametrized in families?~~ No

~~· Statistically understood?~~ No

Is the Rank Computable?

- **Analytically?** Yes*, if we assume B–S-D, the rank is the order of vanishing of the Hasse–Weil L-function $L(E, s)$ at $s = 1$.
  (*Computing values requires $\approx \sqrt{N_E}$ Fourier coefficients, and issues certifying zeroes numerically.)

The **Birch and Swinnerton-Dyer conjecture** is wide open, with only some special cases (rank ≤ 1) known to be true.



Bryan Birch

Sir Peter Swinnerton-Dyer

Is the Rank Computable?

- **Analytically?** Yes*, if we assume B–S-D, the rank is the order of vanishing of the Hasse–Weil L-function $L(E, s)$ at $s = 1$.
  (*Computing values requires $\approx \sqrt{N_E}$ Fourier coefficients, and issues certifying zeroes numerically.)

The **Birch and Swinnerton-Dyer conjecture** is wide open, with a one million dollar reward attached to it (it is one of the Millenium Problems proposed by the Clay Math Institute).

Is the Rank Computable?

- **Analytically?** Yes*, if we assume B–S-D, the rank is the order of vanishing of the Hasse–Weil L-function $L(E, s)$ at $s = 1$.
  (* Computing values requires $\approx \sqrt{N_E}$ Fourier coefficients, and issues certifying zeroes numerically.)

- **Algebraically?** Yes*, if we assume $\text{Ш}(E/\mathbb{Q})[p^\infty]$ is finite, for some prime p, then the method of p-descent determines $E(\mathbb{Q})$.

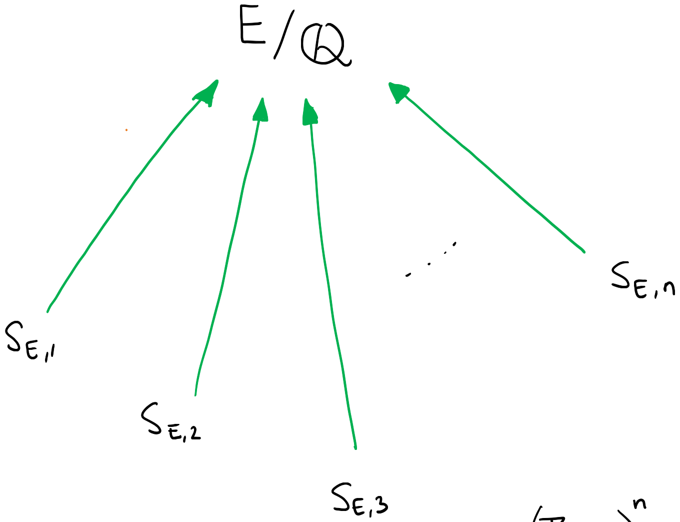
  (* Computing the rank may involve computing models for high p-descendants.)

  The method of descent is based on the following exact sequence:

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

  where $\mathrm{Sel}_{p^n}(E/\mathbb{Q})$ is a finite, computable, cohomological group defined by finitely many local conditions.

2-Descent



where $\mathrm{Sel}_2(E/\mathbb{Q}) = \langle S_{E,1}, S_{E,2}, \ldots, S_{E,n} \rangle \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^n$

2-Descent: Example

$$E/\mathbb{Q}$$

$$y^2 = x^3 - 105196x - 12970320$$

$S_{E,5}$

$$y^2 = -8x^4 + 306x^2 - 2312$$

$S_{E,1}$

$$y^2 = 289x^4 + 1020x^2 + 1156$$

$S_{E,4}$

$$y^2 = 8x^4 + 306x^2 + 2312$$

$S_{E,2}$

$$y^2 = 4x^4 - 2244x^2 + 289$$

$S_{E,3}$

$$y^2 = 289x^4 + 408x^3 + 1428x^2 + 816x + 1156$$

2-Descent: Example

$$E/\mathbb{Q}$$

$$y^2 = x^3 - 105196x - 12970320$$

$S_{E,5}$

$$y^2 = -8x^4 + 306x^2 - 2312$$

$(0,34) \in S_{E,1}$

$$y^2 = 289x^4 + 1020x^2 + 1156$$

$S_{E,4}$

$$y^2 = 8x^4 + 306x^2 + 2312$$

$(0,17) \in S_{E,2}$

$$y^2 = 4x^4 - 2244x^2 + 289$$

$(0,34) \in S_{E,3}$

$$y^2 = 289x^4 + 408x^3 + 1428x^2 + 816x + 1156$$

2-Descent: Example

$E/\mathbb{Q}$

$$y^2 = x^3 - 105196x - 12970320$$

$(-170, 0)$ $(374, 0)$ $(-202, 192)$

$S_{E,5}$

$y^2 = -8x^4 + 306x^2 - 2312$

$(0,34) \in S_{E,1}$

$y^2 = 289x^4 + 1020x^2 + 1156$

$S_{E,4}$

$y^2 = 8x^4 + 306x^2 + 2312$

$(0,17) \in S_{E,2}$

$y^2 = 4x^4 - 2244x^2 + 289$

$(0,34) \in S_{E,3}$

$y^2 = 289x^4 + 408x^3 + 1428x^2 + 816x + 1156$

2-Descent: Example

$$E/\mathbb{Q}$$

$$y^2 = x^3 - 105196x - 12970320$$

$(-170, 0)$ $(374, 0)$ $(-202, 192)$

$(0, 34) \in S_{E,1}$

$$y^2 = 289x^4 + 1020x^2 + 1156$$

$(0, 17) \in S_{E,2}$

$$y^2 = 4x^4 - 2244x^2 + 289$$

$(0, 34) \in S_{E,3}$

$$y^2 = 289x^4 + 408x^3 + 1428x^2 + 816x + 1156$$

$S_{E,4}$

$$y^2 = 8x^4 + 306x^2 + 2312$$

$S_{E,5}$

$$y^2 = -8x^4 + 306x^2 - 2312$$

$\in$ $\in$ $Ш(E/\mathbb{Q})[2]$

2-Descent: Example

$E/\mathbb{Q}$

$$y^2 = x^3 - 105196x - 12970320$$

$(-170, 0)$ $(374, 0)$ $(-202, 192)$

$(0,34) \in S_{E,1}$

$y^2 = 289x^4 + 1020x^2 + 1156$

$(0,17) \in S_{E,2}$

$y^2 = 4x^4 - 2244x^2 + 289$

$(0,34) \in S_{E,3}$

$y^2 = 289x^4 + 408x^3 + 1428x^2 + 816x + 1156$

$S_{E,4}$

$y^2 = 8x^4 + 306x^2 + 2312$

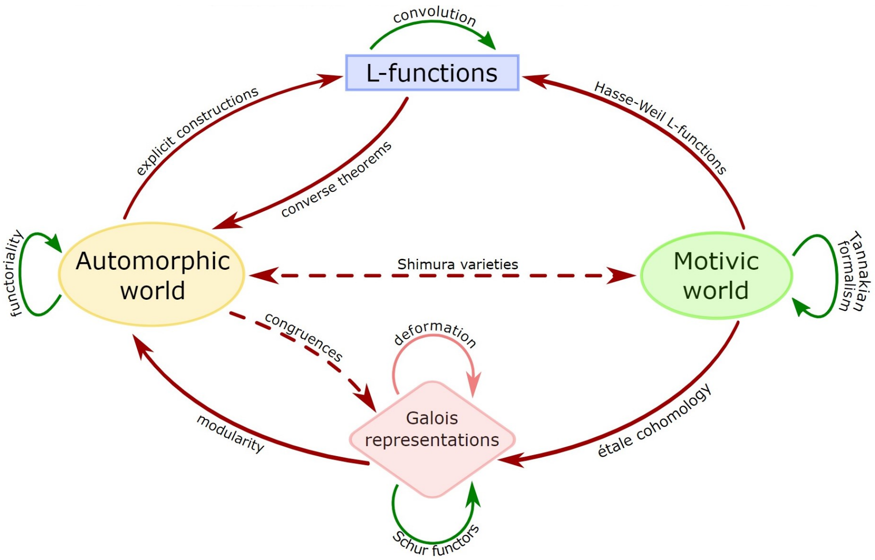
$S_{E,5}$

$y^2 = -8x^4 + 306x^2 - 2312$

$\in$ Ш$(E/\mathbb{Q})[2]$ $\ni$

$$\mathrm{Sel}_2(E/\mathbb{Q}) \cong \underbrace{(\mathbb{Z}/2\mathbb{Z})^2}_{\text{TORSION}} \oplus \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{MW RANK}} \oplus \underbrace{(\mathbb{Z}/2\mathbb{Z})^2}_{\text{SHA}}$$

The BIG Picture (the LMFDB universe)



THANK YOU

"*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 "Bigollo" Pisano, *Liber Abaci*.