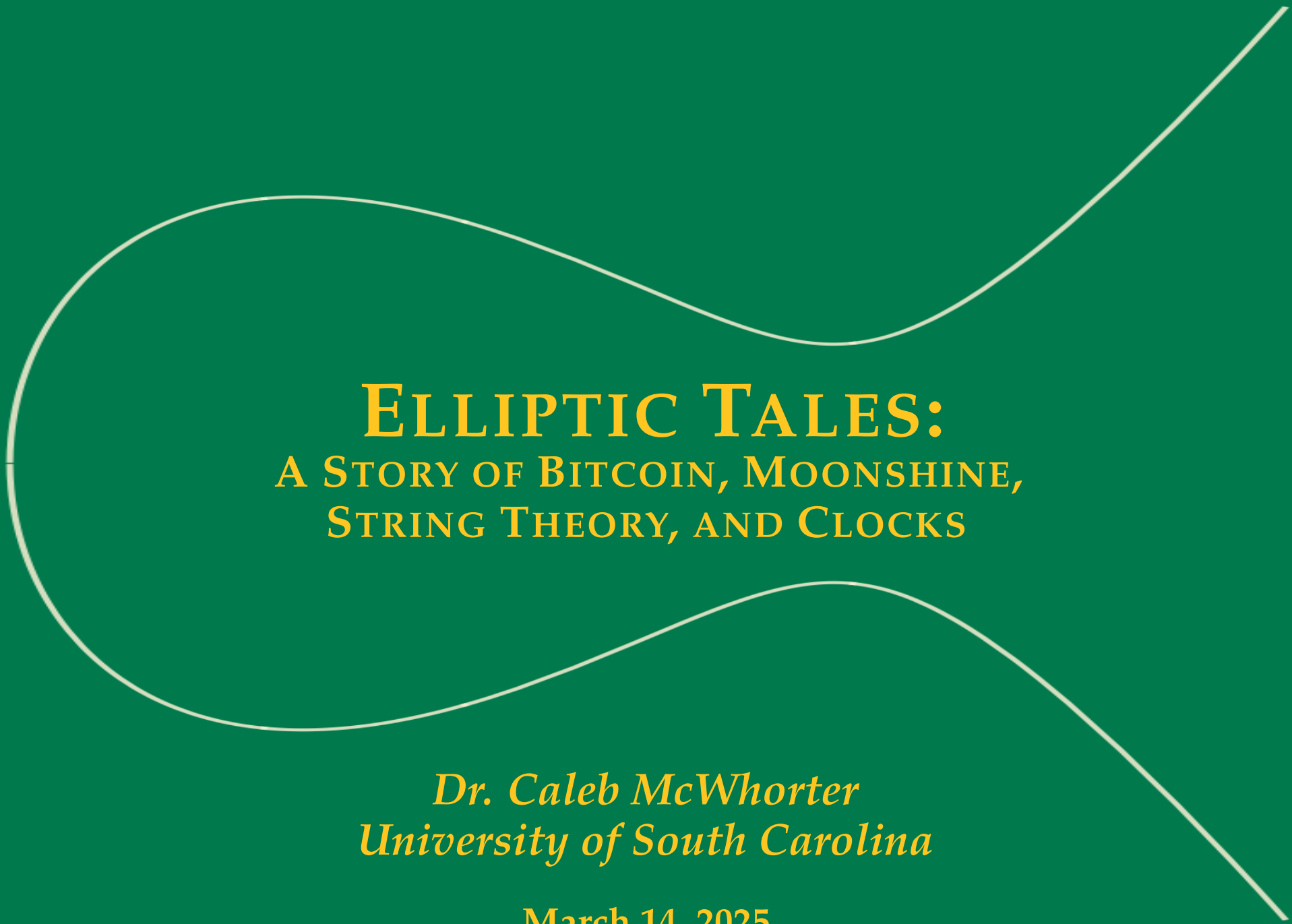


Elliptic Tales:
A Story of Bitcoin, Moonshine, String Theory, and Clocks

Dr. Caleb McWhorter
University of South Carolina

March 14, 2025

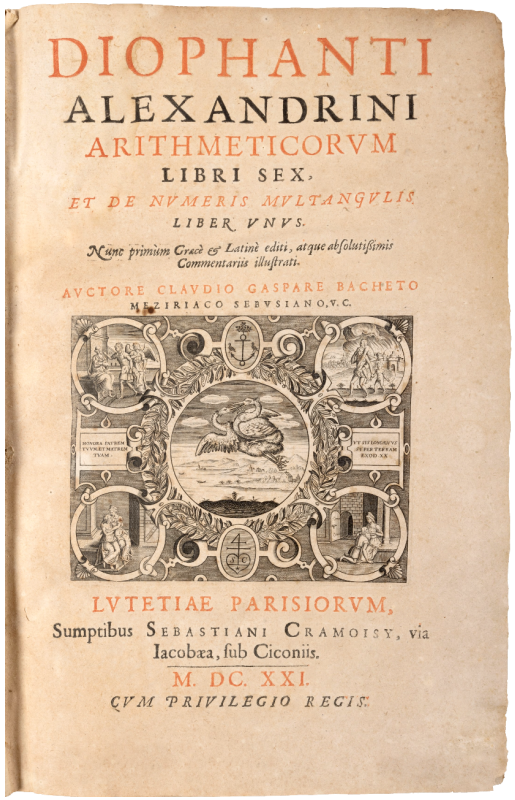
What is Arithmetic Geometry?

Arithmetic Geometry ≈ Diophantine Equations

Arithmetic Geometry is approximately the study of Diophantine equations. These are named after Diophantus of Alexandria (born ≈ A.D. 200), who wrote a thirteen volume set called the *Arithmetica* of which six survive.

Definition (Diophantine Equation)

A Diophantine equation is a polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$ with integer coefficients. One may consider the coefficients to come from other rings.


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.

We can ask number of questions:

- Can we determine if there are integer, rational, etc. solutions?
- If there are solutions, can we determine if there finitely or infinitely many?
- Can we find such solutions?
- Can we describe all the solutions?
- Is there an algorithm to do this generally?

Polynomial Equations in One Variable

Consider the equation $f(x) = 0$, where $f(x)$ is a polynomial.

Question: Can we determine if there are 'nice' solutions to a polynomial equation and, if so, determine what those solutions are?

Example

- $2x + 1 = 5 \quad \Longrightarrow \quad x = 2$ — 1 'nice' solution
- $x^2 = 6 - x \quad \Longrightarrow \quad x = -3, 2$ — 2 'nice' solutions
- $x^2 - 2x - 4 = 0 \quad \Longrightarrow \quad x = 1 \pm \sqrt{5}$ — 2 'not nice' solutions
- $x^2 + 1 = 0 \quad \Longrightarrow \quad x = \pm i$ — No solutions?

The Case of One Variable Polynomials

The case of one variable is finding the roots of a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$.

Theorem (Rational Roots Theorem)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, where $a_i \in \mathbb{Z}$ and $a_0, a_n \neq 0$. Then the only rational solutions to $f(x) = 0$ have $x = p/q$, where p is an integer factor of a_0 and q is an integer factor of a_n.

- We can determine if there are integer or rational solutions.
- There are always at most n solutions.
- We can find all the integer or rational solutions.
- The Rational Roots Theorem describes all the solutions.
- The Rational Roots Theorem describes an algorithm to do this generally.

Equations in Two Variables (Degree 1)

What if we considered the equation $f(x, y) = 0$, where $f(x, y)$ is a polynomial of 'degree 1' in two variables?

Question: Can we determine if there are 'nice' solutions to a polynomial equation and, if so, determine what those solutions are?

Example

- If $2x + 3y - 1 = 0$, i.e. $2x + 3y = 1$, there are infinitely many solutions. For example, $(x, y) = (-1, 1), (2, -1), (-4, 3), \ldots$. The solutions all have the form $(x, y) = (-1 - 3k, 1 + 2k)$, where k is an integer.
- If $2x - 4y - 5 = 0$, i.e. $2x - 4y = 5$, there are no (integer solutions). However, there are rational solutions, e.g. $(\frac{5}{2}, 0)$ and $(0, -\frac{5}{4})$. In fact, all the solutions are rational (but not integer) and have the form $(k, \frac{4k+5}{2})$, where k is an integer.

Two Variable Linear Equations

The case of two variable linear equations is finding integer (or rational) solutions to $ax + by = c$. This already involves a beautiful results from elementary number theory. Working modulo n for some integer n leads to the Chinese Remainder Theorem.

Theorem (Linear Diophantine Equations in Two Variables)

Let a, b, c be integers with $a, b \neq 0$ and let $d = \gcd(a, b)$. The equation $ax + by = c$ has integer solutions if and only if $d \mid c$. If so, the equation has infinitely many solutions and all solutions have the form...

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k,$$

where (x_0, y_0) is a solution and k is an integer.

- We can determine if and when there are integer solutions.
- If there are integer solutions, there are infinitely many and we can parametrize them.
- There are always infinitely many rational solutions and we can parametrize the solutions.
- There is an algorithm in both the integer and rational case.

What about higher degree equations?

Higher Degree Equations

What about equations in two variables with higher degree?

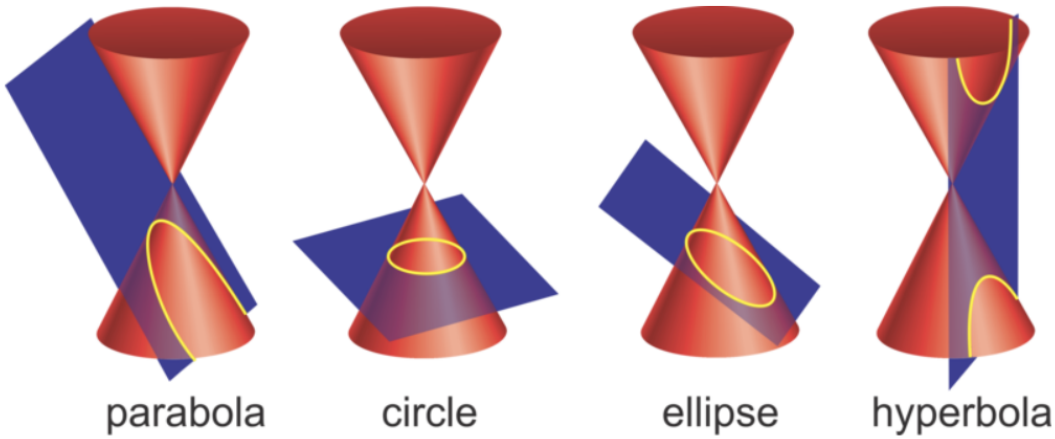
Example

- The equation $y^2 + 108 = x^3$ has no solutions.
- The equation $y^2 = x^3 - 2$ only has the solutions $(x, y) = (3, \pm 5)$.
- The equation $x^2 + y^2 = 4$ has infinitely many solutions.
- The equation $x^2 - 1141y^2 = 1$ has solutions but the 'simplest' solution, i.e. 'first' integer solution, is...

$$x = 1036782394157223963237125215$$
$$y = 30693385322765657197397208$$

Quadratic Diophantine Equations — Conics

The case of two variable, quadratic Diophantine equations is the study of 'nice' points on various conic sections, i.e. the set of zeros for a polynomial $F(x,y) = ax^2 + bxy + cy^2 + ex + fy + h \in \mathbb{Q}[x,y]$.

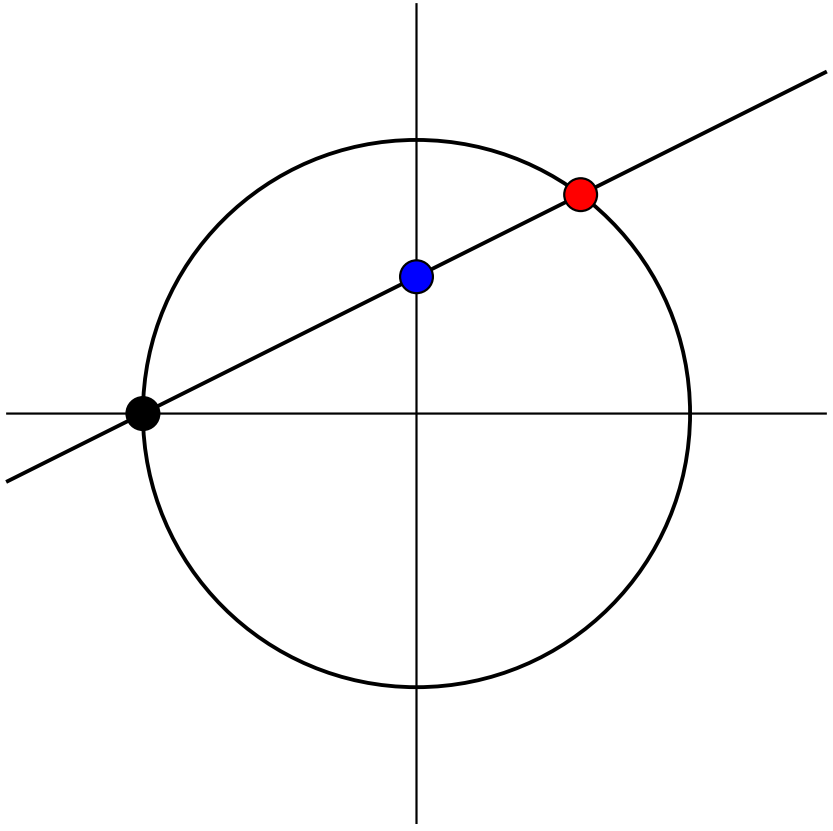


- The set of real solutions to these polynomials are circles, ellipses, parabolas, hyperbolas, and degenerate cases like a point or pair of lines. Therefore, we seek 'nice' points on these surfaces.
- We want our curves to be smooth, i.e. there is no solution (over $\mathbb{C}^2$) to

$$F(x,y) = \frac{\partial F}{\partial x}(x,y) = \frac{\partial F}{\partial y}(x,y) = 0$$

Finding Rational Points on Conics

$$x^2 + y^2 = 1$$



$$C(\mathbb{Q}) = \{(-1,0)\} \cup \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}$$

Local-Global Principles

The 'projection' method does not always work—we need a rational point at the start. For example, the following circle has no rational point:

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

Transforming this into an integer equation, one can work modulo 4 and show there is no solution, which implies there is no rational solution. In fact, all conics that do not have a rational point fail some type of congruence condition.

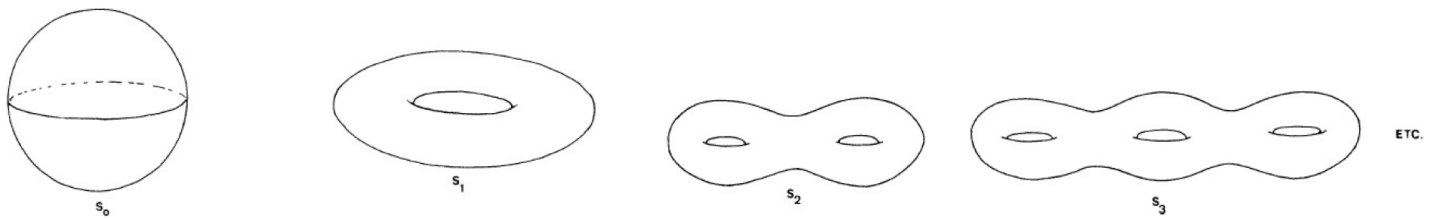
Principle (Hasse, Local-Global Principle)

A collection of equations has a solution 'if and only if' it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all p.

The Case of Higher Degree Equations

Theorem (Mordell, 1922, Faltings, 1983)

If C is a curve over $\mathbb{Q}$ of genus g at least 2, then C has at most finitely many rational points.



Remark

If C is a nonsingular, projective plane curve of degree d is given by...

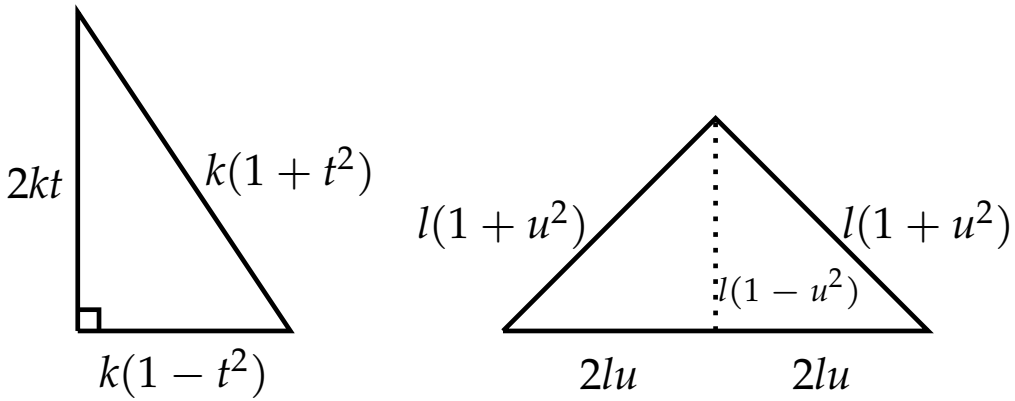
$$g = \frac{(d-1)(d-2)}{2}$$

For a non-singular hypersurface H of degree d in $\mathbb{P}^n$, we have $g = \binom{d-1}{n}$. Topologically, the genus is the number of 'holes.'

Isosceles Triangle Problem

Does there exist a rational right triangle and a rational isosceles triangle that have the same area and the same perimeter?

If yes, we can find $t, u \in \mathbb{Q}$, $0 < t < 1$, $0 < u < 1$, and $k > 0$.



With even more algebra, this is the same as finding a rational solution (x, y) to

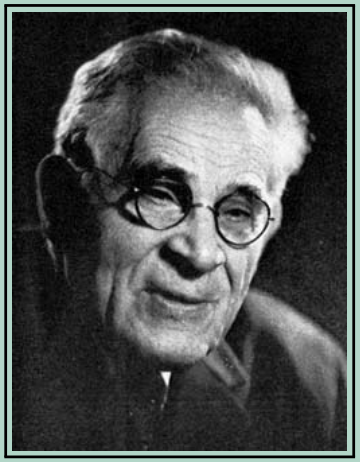
$$y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$$

Theorem (Hirakawa, Matsumura 2018)

Up to similitude, there exists a unique pair of rational right triangles and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with side $(377, 135, 352)$. *and isosceles triangle with sides* $(366, 366, 132)$.

This leaves the ‘sweet spot’ of cubic equations

Elliptic Curves



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…

- A nonsingular projective curve of genus 1.
- An abelian variety of dimension 1.
- A nonempty smooth variety, $V(F)$, with $\deg F = 3$.
- A compact Riemann surface of genus 1.
- The set of solutions to…

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

along with a specified 'distinguished point ∞' and an addition law given by the chord-tangent law.

Elliptic Curves — Short Weierstrass Form

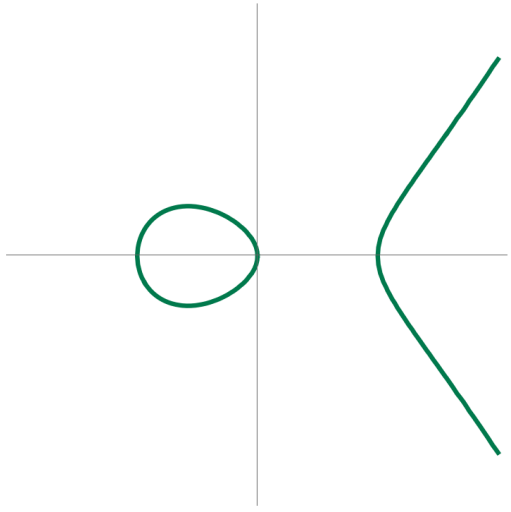
Starting with...

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

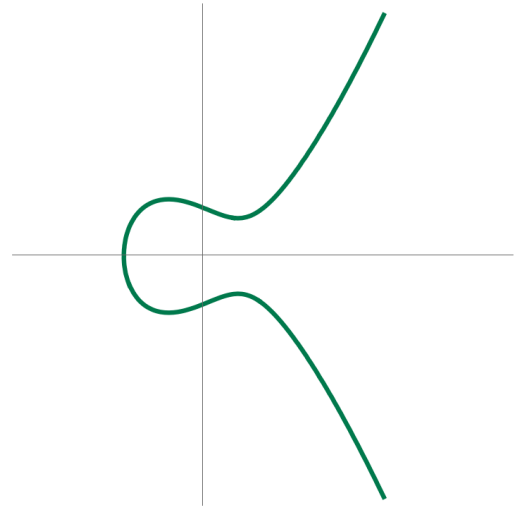
After a series of transformations, we obtain the form of an elliptic curve that we want. So, an elliptic curve is...

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

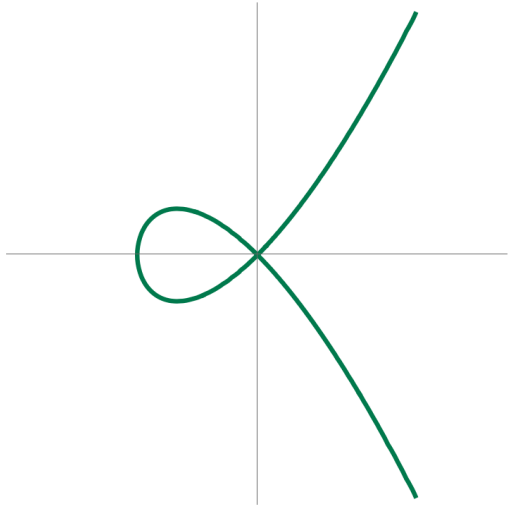
- Require $\Delta = -16(4A^3 + 27B^2) \neq 0$.
- $C(\mathbb{Q})$ could be empty, finite, or infinite.



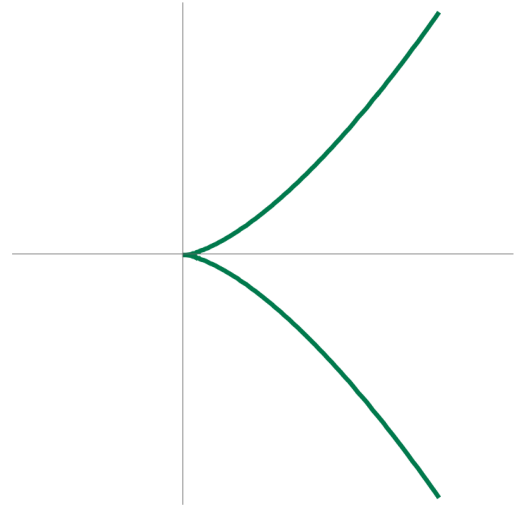
$y^2 = x(x+1)(x-1)$



$y^2 = x^3 - x + 1$

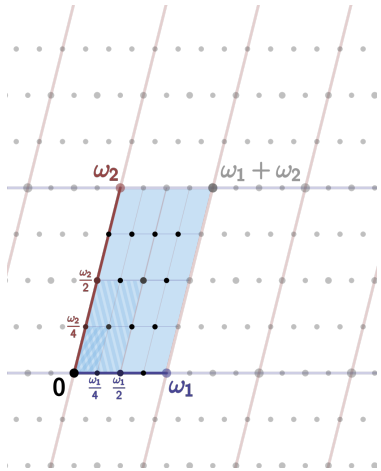


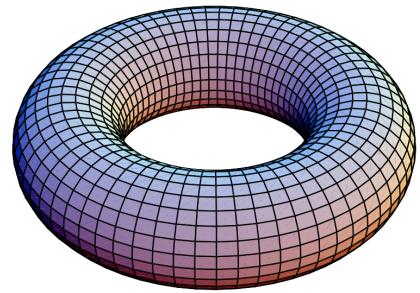
$y^2 = x^2(x+1)$



$y^2 = x^3$

In fact, if one considers the complex solutions to these equations, one can show that $E(\mathbb{C})$ is isomorphic to a torus!





(a) The Möbius strip.

(b) The idea of the embedding.

(c) Topology is delicious!

S. Derbyshire, *Lattice torsion points*. CC BY-SA 3.0

Groups & Fields

What is a Group?

Definition (Group)

A group, G, is a set with a binary operation, $\star$, such that...

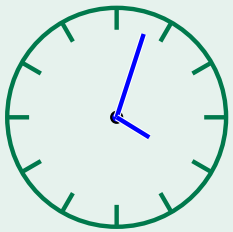
(a) (Associativity) $g \star (h \star k) = (g \star h) \star k$ for all $g, h, k \in G$.

(b) (Identity) There exists $e \in G$ such that $e \star g = g \star e = g$ for all $g \in G$.

(c) (Inverses) For every $g \in G$, there exists $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} \star g = e$.

Example

(i) The integers under addition modulo n form a group, i.e. 'clock arithmetic.'



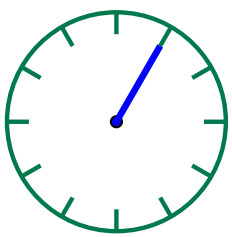
(ii) The integers, $\mathbb{Z}$, under addition form a group, i.e. an 'infinite clock.'

Torsion Subgroups

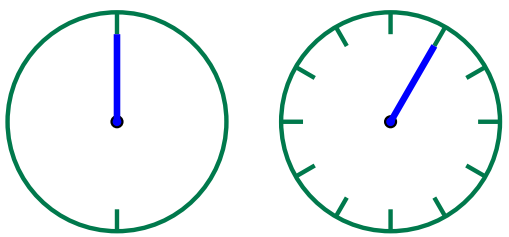
Definition (Torsion)

A group element which when operated on itself a finite number of times returns to the identity is called a *torsion* element. The torsion subgroup of a group is the collection of all its torsion elements.

From now on, when you hear n-torsion, think a clock with n numbers on it, which we will denote $\mathbb{Z}/n\mathbb{Z}$. If there is a '$\oplus$' symbol between them, just imagine two of these types of clocks next to each other—ticking away.



'$=$' $\mathbb{Z}/12\mathbb{Z}$



'$=$' $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$

We will denote an 'infinite clock', i.e. a clock with the numbers $1, 2, \ldots$ on it, by $\mathbb{Z}$. If we write $\mathbb{Z}^r$, we just mean r of these types of clocks next to each other—ticking away.

What is a (Galois) Field?

Definition ('Field')

A field is a collection of 'numbers' where one can perform addition, subtraction, multiplication, and (nonzero) division and these operations are 'nice.'

Example

(i) The rational numbers, $\mathbb{Q}$, are a field with the usual $+, -, \times, \div$.

(ii) Number fields (extensions of $\mathbb{Q}$) are also fields. For example, consider $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$,

$$(5 - 3\sqrt{2}) + (-4 + 6\sqrt{2}) = 1 + 3\sqrt{2}$$

$$(6 - 7\sqrt{2}) \cdot (6 + 7\sqrt{2}) = -62 + 0\sqrt{2}$$

$$\frac{1 + 3\sqrt{2}}{1 + \sqrt{2}} = 5 - 2\sqrt{2}$$

The dimension of a number field as a $\mathbb{Q}$-vector space, i.e. number of 'pieces' in these numbers, is called the *degree* of the extension.

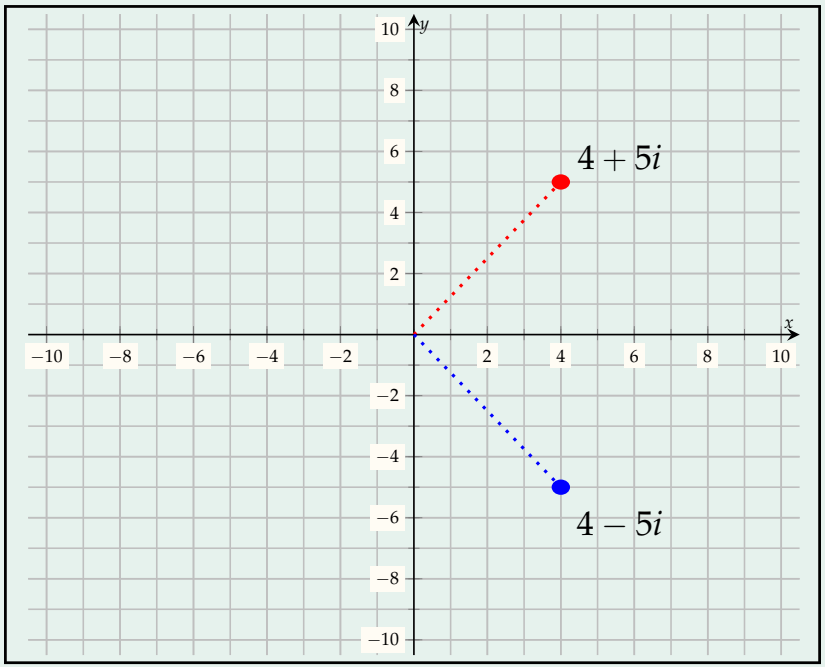
Galois Fields

Definition (Galois Field)

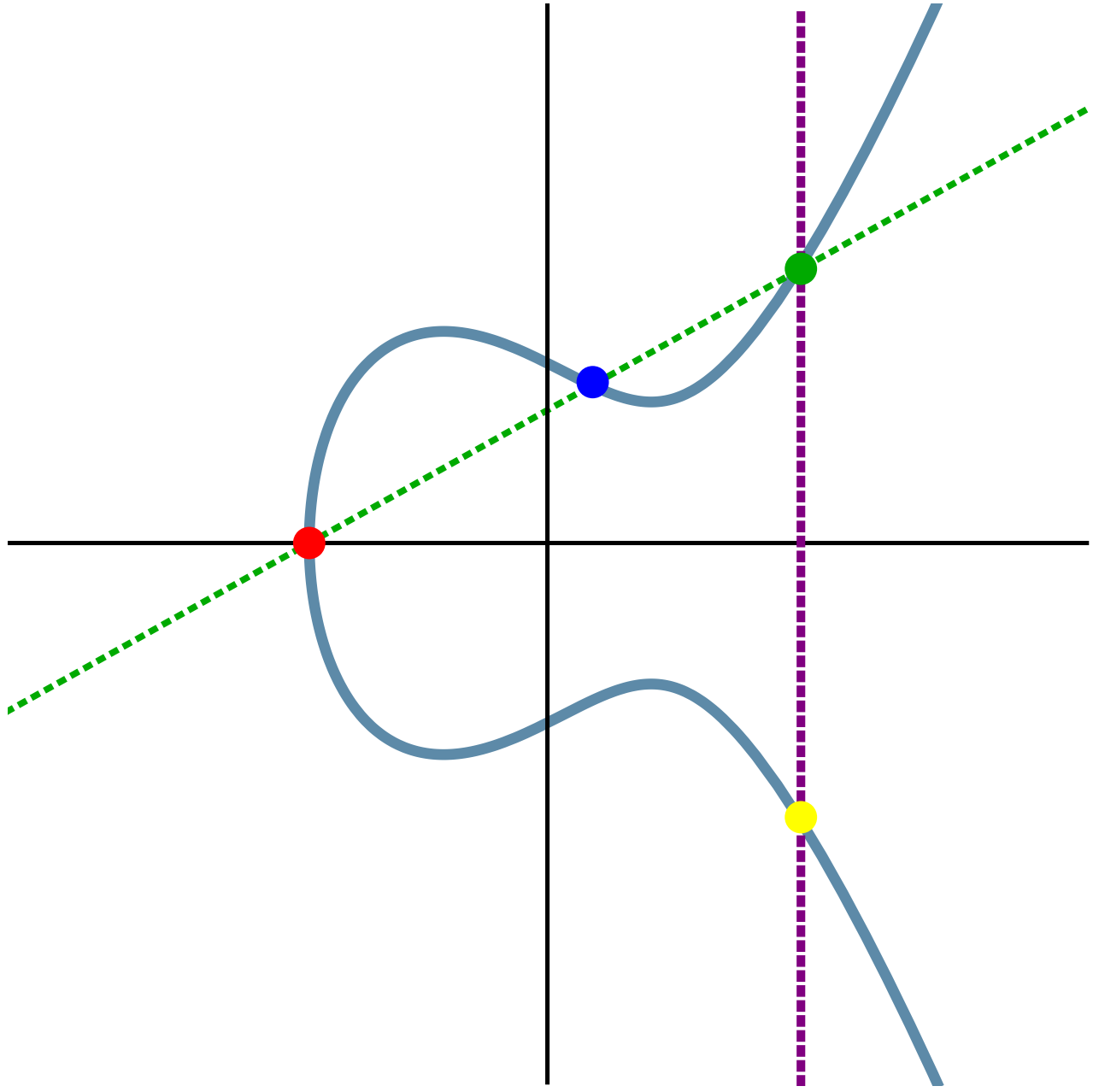
A Galois field is a 'number field' whose numbers satisfy extra symmetries.

Example

Consider the number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, i.e. "complex numbers with only rational parts." We can add, subtract, multiply, and divide these numbers. But they also have an extra symmetry given by conjugation, $\overline{a + bi} = a - bi$.



The Group Law: Addition on Elliptic Curves



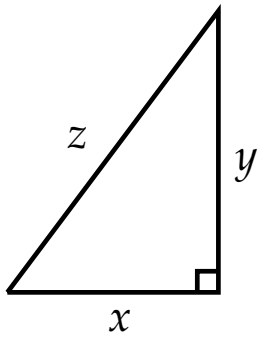
Why Elliptic Curves?

Congruent Number Problem

An integer is a *congruent number* if it is the area of a rational right triangle.

This is equivalent to finding a rational triplet (x, y, z) with...

$$x^2 + y^2 = z^2 \quad \text{and} \quad n = \frac{xy}{2}.$$



Example

- 6 is congruent: $3^2 + 4^2 = 5^2$ and $\frac{3\cdot 4}{2} = 6$
- 5 is congruent: $\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2$ and $\frac{1}{2}\left(\frac{3}{2}\cdot\frac{20}{3}\right) = 5$
- 1 is *not* congruent (due to Fermat)
- 157 is congruent (due to Don Zagier):

$$x = \frac{411340519227716149383203}{21666555693714761309610}, y = \frac{6803298487826435051217540}{411340519227716149383203}, z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

This problem is 'equivalent' to finding rational points (x, y) on the elliptic curve...

$$y^2 = x^3 - n^2 x$$

Fermat's Last Theorem

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

Theorem (Fermat's Last Theorem; Wiles, 1994; Taylor-Wiles, 1995)

There are no nontrivial integer solutions to the equation $x^n + y^n = z^n$ *whenever* $n > 2$.

Andrew Wiles

Richard Taylor

What integers are the sums of cubes?

What integers n are the sum of three cubes?

$$x^3 + y^3 + z^3 = n$$

What integers are the sums of cubes?

$$x^3 + y^3 + z^3 = N$$

- From 1955 – 2016, it was known that all integers 1–100 that were not 4 or 5 modulo 9 were the sum of three cubes except 33, 42, 74.

- After the release of a Numberphile video, Huisman 2016 found the following:

$$(66\,229\,832\,190\,556)^3 + (28\,3450\,105\,697\,727)^3 + (-284\,650\,292\,555\,885)^3 = 74$$

- In 2019, Booker found the following:

$$(-2\,736\,111\,468\,807\,040)^3 + (-8\,778\,405\,442\,862\,239)^3 + (8\,866\,128\,975\,287\,528)^3 = 33$$

- Finally, shortly thereafter in 2019, Sutherland and Booker (using 1.3 million hours of computing time)

$$(12\,602\,123\,297\,335\,631)^3 + (80\,435\,758\,145\,817\,515)^3 + (-80\,538\,738\,812\,075\,974)^3 = 42$$

ECDH, Playstation 3, & Bitcoin

Elliptic curves are the basis for ECDH (Elliptic-Curve Diffie-Hellman) encryption, which is the backbone of most modern encryption (for now…).

PlayStation 3 hack – how it happened and what it means

A group of coders claims the PS3 has been hacked, opening the doors to software piracy. We look into the implications

The PS3 has been hacked. But how – and why? Photograph: Kevork Djansezian/AP

BIZ & IT —

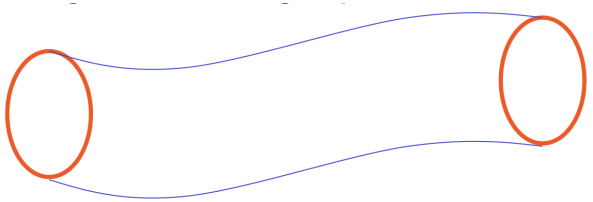
Google confirms critical Android crypto flaw used in $5,700 Bitcoin heist

Java Crypto weakness could affect security in hundreds of thousands of apps.

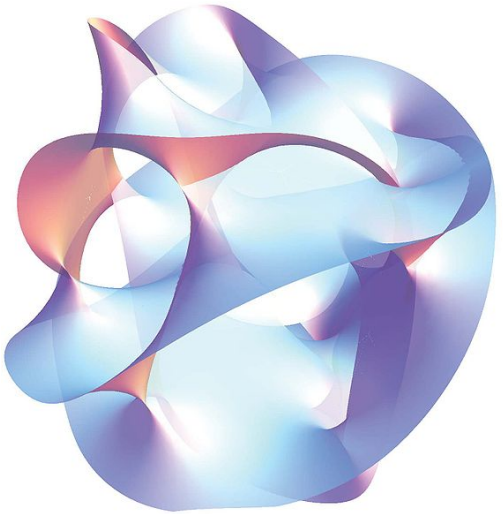
DAN GOODIN - 8/14/2013, 9:15 PM

String Theory

In String Theory, the idea of point-like particles are replaced by curve-like strings of some higher dimension, e.g. 6-dimensional or 23-dimensional. A single string which 'moves about' and eventually returns to its start traces out a surface—specifically a torus! So paths of single strings 'look like' elliptic curves!



Furthermore, in Quantum Physics, physicists often need to compute averages over all possible paths. So when considering this type of computation in String Theory, one would then be integrating over the space of all elliptic curves!

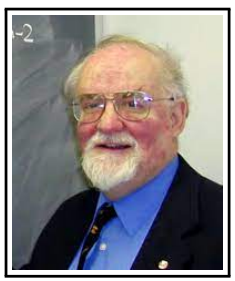


Monstrous Moonshine

An elliptic curve can be uniquely identified (over $\mathbb{C}$) by its j-invariant. The j-invariant is given by the modular j-invariant function,

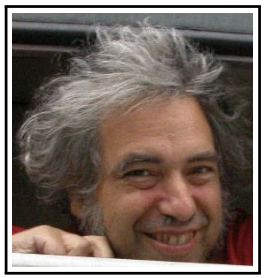
$$j(\tau) = \frac{1}{q} + 744 + 196884q + 214937609q^2 + \cdots$$

where $q = e^{2\pi i\tau}$ and τ is given by the elliptic curve.



John McKay

John Conway



Simon Norton

Richard Borcherd

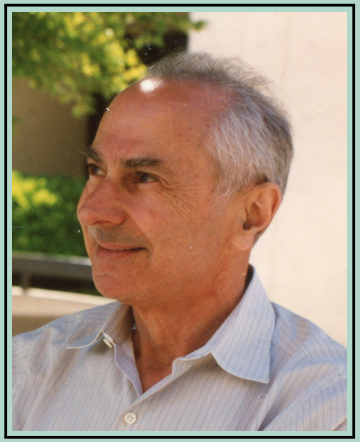
Beginning In 1978, John McKay, Conway-Norton, and Borcherds discovered that the coefficients in the modular j-invariant are sums of linear combinations of the dimensions of the irreducible representations of the monster group, M, which is the largest of the sporadic groups. These appear in the classification of all finite simple groups. In fact, Borcherd's work won a Field's Medal.

This is also related to the fact that...

$$e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925007\ldots$$

Art

Lenstra & de Smit were recently able to finish an incomplete piece of M.C. Escher using elliptic curves:



1927 – 2005

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

– Serge Lang, *Elliptic Curves: Diophantine Analysis*

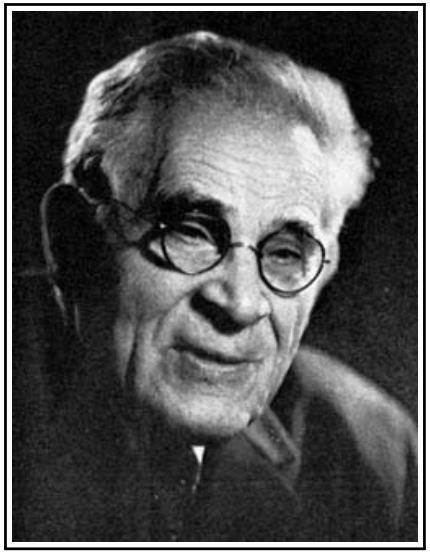
Elliptic Curve Structure

Theorem (Mordell-Weil-Néron, 1952)

Let K be a field that is finitely generated over its prime field, and let 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,

$$A(K) \cong \mathbb{Z}^{r_K} \oplus A(K)_{tors},$$

where $r_K \geq 0$ is the rank and $A(K)_{tors}$ is the torsion subgroup.



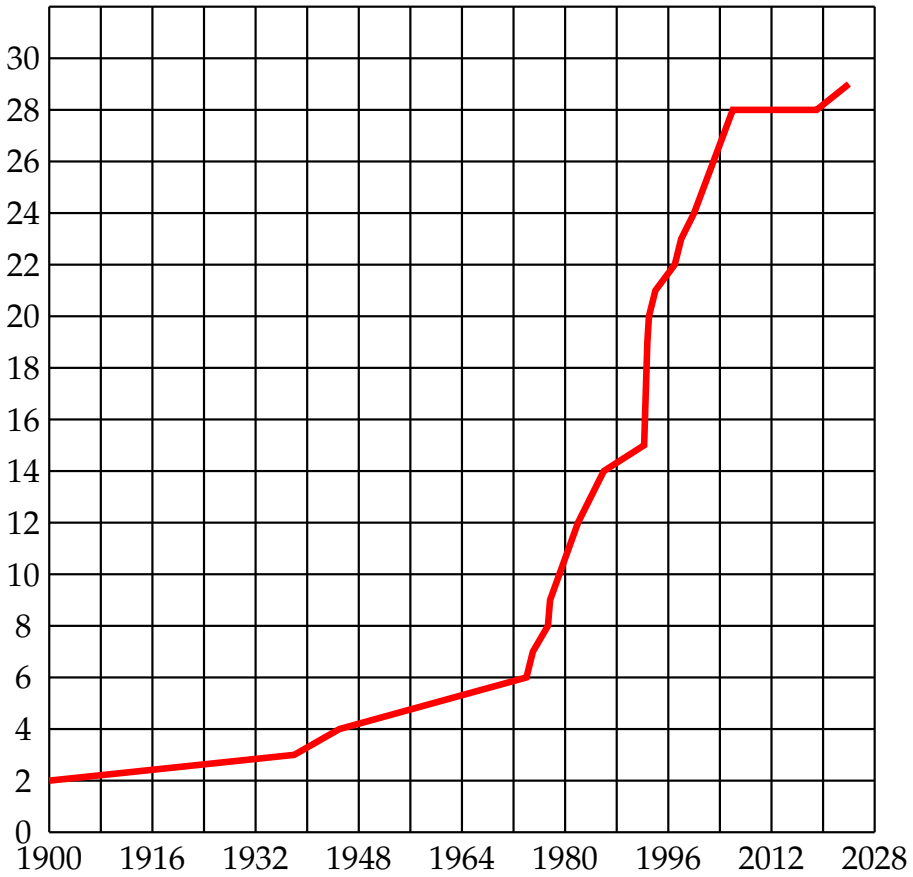
Louis J. Mordell

André Weil

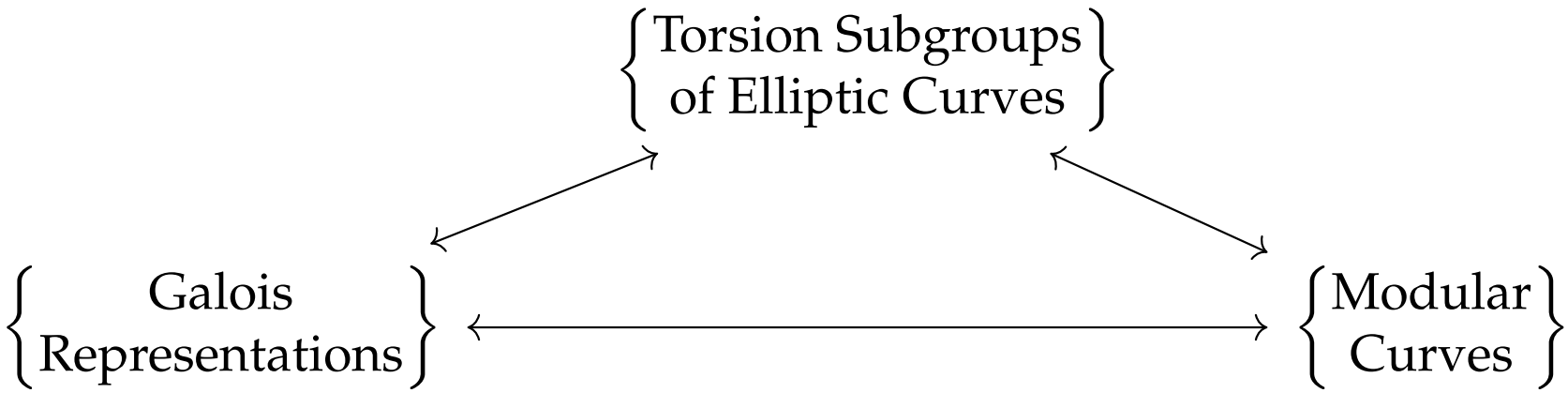
André Néron

Ranks of Elliptic Curves (over $\mathbb{Q}$)

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
29	2024	Elkies, Klagsbrun



Torsion Subgroups of Elliptic Curves



Theorem (Levi-Ogg Conjecture; Mazur, 1977)

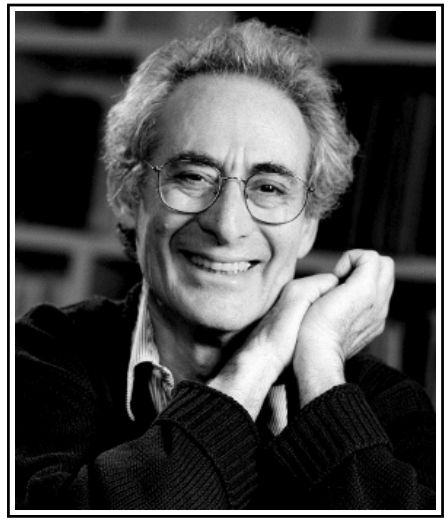
If $E/\mathbb{Q}$ is a rational elliptic curve, then the possible torsion subgroups $E(\mathbb{Q})_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 4 \end{cases}$$

Furthermore, each possibility occurs infinitely often.

Beppo Levi

Andrew Ogg



Barry Mazur

Theorem (Najman, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quadratic number field. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 15, 16 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{cases}$$

Each such possibility occurs for infinitely many elliptic curves except for $\mathbb{Z}/15\mathbb{Z}$, which occurs only for the elliptic curves `50b1` and `50a3` over $\mathbb{Q}(\sqrt{5})$ and the elliptic curves `50b2` and `450b4` over $\mathbb{Q}(\sqrt{-15})$.

Filip Najman

Theorem (Najman, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic number field. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7 \end{cases}$$

Each such possibility occurs for infinitely many elliptic curves except for $\mathbb{Z}/21\mathbb{Z}$, which only occurs for the elliptic curve `162b1` over $\mathbb{Q}(\zeta_9)^+$.

Filip Najman

Theorem (Chou, 2015; González-Jimenez, Lozano-Robledo, 2016; González-Jimenez, Najman, 2016)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quartic number field. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 15, 16, 20, 24 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Each such possibility occurs for infinitely many elliptic curves except for $\mathbb{Z}/15\mathbb{Z}$, which occurs only for the elliptic curves with $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$ over some quartic field.

Michael Chou

Enrique González-Jiménez

Álvaro Lozano-Robledo

Filip Najman

Theorem (González-Jimenez, 2016)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quintic number field. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 12, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \end{cases}$$

Each of these possibilities occurs infinitely many times except for $\mathbb{Z}/11\mathbb{Z}$ which occurs for the elliptic curves `121a2`, `121c2`, and `121b1` over some quintic field.

Enrique González-Jiménez

Theorem (Daniels, González-Jimenez, 2018; Gužvić, 2019)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a sextic number field. Then the possible torsion subgroups $E(K)_{tors}$ are among:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 21, 30, n \neq 11 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 7, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 6^* \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 3 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Each such possibility occurs for infinitely many elliptic curves except for $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, and possibly $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.

Harris Daniels

Enrique González-Jiménez

Tomislav Gužvić

Theorem (González-Jimenez, Najman, 2016)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a number field whose smallest prime divisor is at least 7, then the only possible torsion subgroups $E(\mathbb{Q})_{tors}$ are those from Mazur's list, namely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \end{cases}$$

Each such possibility occurs for infinitely many elliptic curves. In fact, if the largest prime divisor is at least 11, then $E(K)_{tors} = E(\mathbb{Q})_{tors}$.

Enrique González-Jiménez

Filip Najman

Classification over Odd Degree Galois Fields

Theorem (M.)

The set $\Phi_{\mathbb{Q}}^{\mathrm{Gal},odd}(d^\infty)$ *is finite, and if* $E(K)_{tors} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal},odd}(d^\infty)$, *then* $E(K)_{tors}$ *is precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 14, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7. \end{cases}$$

Moreover, each such possibility occurs.

$$\Phi_{\mathbb{Q}}^{\mathrm{Gal,odd}}(d^\infty) := \bigcup_{\substack{d \in \mathbb{N} \\ d \text{ odd}}} \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$$

$F(d)^+$	$\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$	$F(d)^+$	$\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$
$(0,0,0^+,0^+)$	$\Phi(1)$	$(2,0,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$
$(0,1,0^+,0^+)$	$\Phi_{\mathbb{Q}}(5)$	$(2,1^+,0,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}$
$(1,0,0,0)$	$\Phi_{\mathbb{Q}}(3)$	$(2,1^+,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$
$(1,0,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/11\mathbb{Z}\}$	$(2,1^+,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$
$(1,0,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/43\mathbb{Z}\}$	$(2,1^+,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$
$(1,0,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$	$(4^+,0,0,0)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(1,1^+,0,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5)$	$(4,0,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(1,1^+,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/67\mathbb{Z}\}$	$(4,0,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/47\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(1,1^+,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/43\mathbb{Z}\}$	$(4,0,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(1,1^+,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$	$(4,1^+,0,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(2,0,0,0)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}$	$(4,1^+,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(2,0,0,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$	$(4,1^+,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$
$(2,0,1^+,0)$	$\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$	$(4^+,1^+,1^+,1^+)$	$\Phi_{\mathbb{Q}}(3) \cup \Phi(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$

Classification over Nonic Galois Fields

Theorem (Chou, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quartic Galois number field. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 15, 16 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{cases}$$

Michael Chou

Outline of the Classification

1. Determine the possible prime orders.
2. Bound the p-Sylow Subgroups.
3. Create a finite list of possibilities.
4. Find examples and eliminate cases.

Step 1. Determine the Possible Prime Orders

Theorem (Lozano-Robledo, 2013)

Let $S_{\mathbb{Q}}(d)$ be the set of primes such that there exists an elliptic curve $E/\mathbb{Q}$ with a point of order p defined in an extension $K/\mathbb{Q}$ of degree at most d. Then $S_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$.

Álvaro Lozano-Robledo

Remark

Lozano-Robledo computes $S_{\mathbb{Q}}(d)$ for $1 \leq d \leq 21$ and gives a conjectural formula for $d \geq 1$, which is valid for $1 \leq d \leq 42$, which would follow from a positive answer to Serre's uniformity question.

Proposition (González-Jiménez, Najman, 2016)

(i) $11 \in R_{\mathbb{Q}}(d)$ *if and only if* $5 \mid d$.

(ii) $17 \in R_{\mathbb{Q}}(d)$ *if and only if* $8 \mid d$.

Enrique González-Jiménez

Filip Najman

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. If $P \in E(K)$ is a point of prime order p, then $p \in \{2, 3, 5, 7, 13, 19\}$.

Step 2. Bound the Size of the Sylow Subgroups

Theorem (González-Jiménez, Lozano-Robledo)

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values:

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad \text{or} \quad -\frac{7 \cdot 17231878060 80^3}{79^{16}}$$

in which case $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this is best possible in that there are one-parameter families $E_{s,N}(t)$ of elliptic curves over $\mathbb{Q}$ such that for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ such that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is equal to the bound given above.

Lemma (2-Sylow Bound)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Lemma (Odd Torsion)

Let $K/\mathbb{Q}$ be an odd degree number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain full p-torsion for all odd primes.

Proof. By the existence of the Weil-pairing, if $E(K)$ contains full p-torsion, then $\mathbb{Q}(\zeta_p) \subseteq K$. But for $p > 2$, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p)$ is even, a contradiction. $\square$

Lemma (Galois Isogeny)

Let $K/\mathbb{Q}$ be a Galois extension, and let $E/\mathbb{Q}$ be a rational elliptic curve. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then E has a rational n-isogeny.

Lemma (Galois Isogeny)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a Galois extension. If $E(K)_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then E has a rational n-isogeny.

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

Let $N \geq 2$ be such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point. Then

(i) *$N \leq 10$ or $N = 12, 13, 16, 18$, or 25. In this case, $X_0(N)$ is a curve of genus 0, and the $\mathbb{Q}$ rational points on $X_0(N)$ form an infinite 1-parameter family, or*

(ii) *$N = 11, 14, 15, 17, 19, 21$, or 27, i.e. $X_0(N)$ is a rational elliptic curve (in each case $X_0(N)(\mathbb{Q})$ is finite, or*

(iii) *$N = 37, 43, 67$, or 163. In this case, $X_0(N)$ is a curve of genus ≥ 2 and by Faltings' Theorem has only finitely many $\mathbb{Q}$-rational points.*

In particular, a rational elliptic curve may only have a rational cyclic n-isogeny for $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. Furthermore, if E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Lemma (p-Sylow bounds)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then

$$E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$
$$E(K)[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z}$$
$$E(K)[5^\infty] \subseteq \mathbb{Z}/25\mathbb{Z}$$
$$E(K)[7^\infty] \subseteq \mathbb{Z}/7\mathbb{Z}$$
$$E(K)[13^\infty] \subseteq \mathbb{Z}/13\mathbb{Z}$$
$$E(K)[19^\infty] \subseteq \mathbb{Z}/19\mathbb{Z}$$

Step 3. Create a Finite List of Possibilities

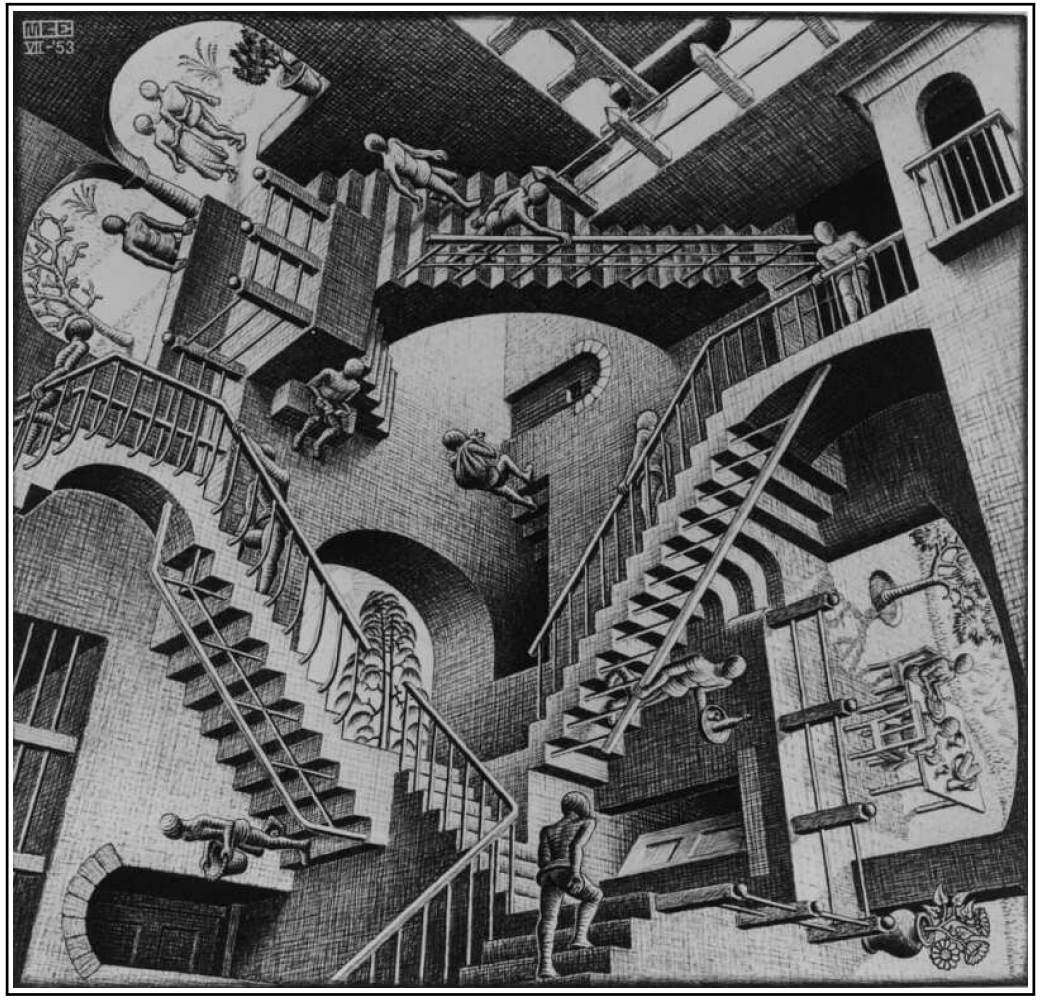
Lemma

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ is isomorphic to one of the following (although not all cases need occur):

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, \ldots, 7, 9, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27 \end{cases}$$

Step 4. Find Examples & Eliminate Cases

Upstairs/Downstairs Games



M.C. Escher's Relativity

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $F/\mathbb{Q}$ be a cubic Galois field. Then there exists a nonic Galois field K such that $E(K)_{tors} \cong E(F)_{tors}$.

Proof.

- If F_1, F_2 are distinct cubic Galois fields, then F_1F_2 is a nonic Galois extension. It suffices to prove there are infinitely many distinct cubic Galois fields.
- For a chosen integer k, define $a := k^2 + k + 7$.
- The field $K_a := \mathbb{Q}(x^3 - ax + a)$ is a cubic Galois field. For each distinct a, the fields K_a are distinct. □

Corollary

$\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(3) \subseteq \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$

Examples of torsion subgroups $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$.

Torsion Subgroup	Elliptic Curve	Galois Cubic Field
$\mathbb{Z}/13\mathbb{Z}$	147b1	$\mathbb{Q}(\zeta_7)^+$
$\mathbb{Z}/14\mathbb{Z}$	49a3	$\mathbb{Q}(\zeta_7)^+$
$\mathbb{Z}/18\mathbb{Z}$	14a4	$\mathbb{Q}(\zeta_7)^+$
$\mathbb{Z}/21\mathbb{Z}$	162b1	$\mathbb{Q}(\zeta_9)^+$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$	1922c1	$\mathbb{Q}(x^3 - x^2 - 10x + 8)$

Examples of $E(K)$ with 19 and 27-torsion over nonic fields.

$E(K)_{\text{tors}}$	$E(\mathbb{Q})_{\text{tors}}$	E	K
$\mathbb{Z}/19\mathbb{Z}$	$\{\mathcal{O}\}$	361a1	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/27\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	27a4	$\mathbb{Q}(\zeta_{27})^+$

This leaves the following list of torsion subgroups whose existence or non-existence we have yet to prove.

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 15, 25 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 5, 6, 9, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27 \end{cases}$$

Lemma (Najman, 2015)

Let p, q be distinct odd primes, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$ and E/F_1 an elliptic curve with no p-torsion over F_1. Then if q does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.

Lemma (Najman, 2015)

Let p be an odd prime number, q a prime not dividing p, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, E/F_1 an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/p\mathbb{Z}$, $E(F_1) \not\supset \mathbb{Z}/p^2\mathbb{Z}$, and $\zeta_p \notin F_2$. Then $E(F_2) \not\supset \mathbb{Z}/p^2\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Suppose $P \in E(K)_{tors}$ is a point of order p. Then

(i) *if $p \in \{3, 5\}$, then P is defined over $\mathbb{Q}$, i.e. $P \in E(\mathbb{Q})[p]$.*

(ii) *if $p = 13$, then there is a cubic field $F \subseteq K$ with $P \in E(F)[p]$.*

(iii) *if $p \in \{2, 7\}$, then P is defined over $\mathbb{Q}$, i.e. $P \in E(\mathbb{Q})[p]$, or there is a cubic field $F \subseteq K$ with $P \in E(F)[p]$.*

Lemma

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Proof.

- By our previous result, we know that $E(K)[5^\infty] = E(\mathbb{Q})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$.
- Choosing a model $E : y^2 = x^3 + Ax + B$, we know the x-coordinates of points of order 2 correspond to roots of $x^3 + Ax + B$.
- As $E(K)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, K contains a splitting field for $x^3 + Ax + B$, which has degree 1, 3, or 6.
- Degree 6 is not possible as $K/\mathbb{Q}$ has odd degree. Then $\mathbb{Q}(E(K)[2^\infty])$ is defined over at most a cubic field.
- But then either $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or there is a cubic field, F, with $E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, contradicting the classification of either $\Phi(1)$ or $\Phi_{\mathbb{Q}}(3)$. □

Theorem (M.)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 19, 21, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Examples of each possible $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$.

$E(K)_{\text{tors}}$	Cremona Label	$E(\mathbb{Q})_{\text{tors}}$	K
$\{\mathcal{O}\}$	11a2	$\{\mathcal{O}\}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z}$	14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/3\mathbb{Z}$	19a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/4\mathbb{Z}$	15a7	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/5\mathbb{Z}$	11a1	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/6\mathbb{Z}$	14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/7\mathbb{Z}$	26b1	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/8\mathbb{Z}$	15a4	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/9\mathbb{Z}$	54b3	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/10\mathbb{Z}$	66c1	$\mathbb{Z}/10\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/12\mathbb{Z}$	90c3	$\mathbb{Z}/12\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/13\mathbb{Z}$	147b1	$\{\mathcal{O}\}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/14\mathbb{Z}$	49a4	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/18\mathbb{Z}$	260610o2	$\mathbb{Z}/6\mathbb{Z}$	9.9.80646091894081.1
$\mathbb{Z}/19\mathbb{Z}$	361a1	$\{\mathcal{O}\}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/21\mathbb{Z}$	162b1	$\mathbb{Z}/3\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/27\mathbb{Z}$	27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}(\zeta_{27})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	15a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	15a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	30a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	210e2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	1922c1	$\{\mathcal{O}\}$	9.9.10441392056596 9.1

Conjecture

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic field. Then $E(K)_{\text{tors}}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 19, 21, 26, 27, 28, 36, 42 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7, 9 \end{cases}$$

Moreover, each such possibility occurs.

Torsion Growth over Nonic Galois Fields

$E(K)_{\text{tors}}$ \ $E(\mathbb{Q})_{\text{tors}}$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$	$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_8$
$\mathcal{C}_1$	✓														
$\mathcal{C}_2$		✓													
$\mathcal{C}_3$			✓												
$\mathcal{C}_4$				✓											
$\mathcal{C}_5$					✓										
$\mathcal{C}_6$						✓									
$\mathcal{C}_7$	✓						✓								
$\mathcal{C}_8$								✓							
$\mathcal{C}_9$			✓						✓						
$\mathcal{C}_{10}$										✓					
$\mathcal{C}_{12}$											✓				
$\mathcal{C}_{13}$	✓														
$\mathcal{C}_{14}$		✓													
$\mathcal{C}_{18}$						✓									
$\mathcal{C}_{19}$	✓														
$\mathcal{C}_{21}$			✓												
$\mathcal{C}_{27}$			✓												
$\mathcal{C}_2 \times \mathcal{C}_2$	✓											✓			
$\mathcal{C}_2 \times \mathcal{C}_4$													✓		
$\mathcal{C}_2 \times \mathcal{C}_6$			✓											✓	
$\mathcal{C}_2 \times \mathcal{C}_8$															✓
$\mathcal{C}_2 \times \mathcal{C}_{14}$	✓														

Bicyclic Nonic Galois Fields

Theorem (M.)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic bicyclic Galois field, i.e. a nonic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then $E(K)_{tors}$ is precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Examples of torsion subgroups $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\mathcal{C}_3 \times \mathcal{C}_3}(9)$.

$E(K)_{\text{tors}}$	Cremona Label	$E(\mathbb{Q})_{\text{tors}}$	K
$\{\mathcal{O}\}$	11a2	$\{\mathcal{O}\}$	9.9.62523502209.1
$\mathbb{Z}/2\mathbb{Z}$	14a5	$\mathbb{Z}/2\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/3\mathbb{Z}$	19a1	$\mathbb{Z}/3\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/4\mathbb{Z}$	15a7	$\mathbb{Z}/4\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/5\mathbb{Z}$	11a1	$\mathbb{Z}/5\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/6\mathbb{Z}$	14a2	$\mathbb{Z}/6\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/7\mathbb{Z}$	26b1	$\mathbb{Z}/7\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/8\mathbb{Z}$	15a4	$\mathbb{Z}/8\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/9\mathbb{Z}$	54b3	$\mathbb{Z}/9\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/10\mathbb{Z}$	66c1	$\mathbb{Z}/10\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/12\mathbb{Z}$	90c3	$\mathbb{Z}/12\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/13\mathbb{Z}$	147b1	$\{\mathcal{O}\}$	9.9.62523502209.1
$\mathbb{Z}/14\mathbb{Z}$	49a4	$\mathbb{Z}/2\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/18\mathbb{Z}$	14a4	$\mathbb{Z}/6\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/21\mathbb{Z}$	162b1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}(\zeta_{27})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	15a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	15a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	30a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	210e2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	1922c1	$\{\mathcal{O}\}$	9.9.10441920565969.1

Cyclic Nonic Galois Fields

Theorem (M.)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic cyclic Galois field, i.e. a nonic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Then $E(K)_{tors}$ is precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4 \end{cases}$$

Examples of torsion subgroups $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$.

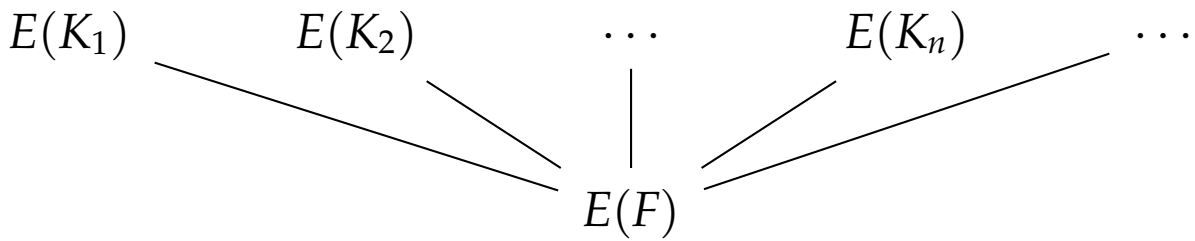
$E(K)_{\text{tors}}$	Cremona Label	$E(\mathbb{Q})_{\text{tors}}$	K
$\{\mathcal{O}\}$	11a2	$\{\mathcal{O}\}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z}$	14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/3\mathbb{Z}$	19a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/4\mathbb{Z}$	15a7	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/5\mathbb{Z}$	11a1	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/6\mathbb{Z}$	14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/7\mathbb{Z}$	26b1	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/8\mathbb{Z}$	15a4	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/9\mathbb{Z}$	54b3	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/10\mathbb{Z}$	66c1	$\mathbb{Z}/10\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/12\mathbb{Z}$	90c3	$\mathbb{Z}/12\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/13\mathbb{Z}$	147b1	$\{\mathcal{O}\}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/18\mathbb{Z}$	260610o2	$\mathbb{Z}/6\mathbb{Z}$	9.9.80646091894081.1
$\mathbb{Z}/21\mathbb{Z}$	162b1	$\mathbb{Z}/3\mathbb{Z}$	9.9.62523502209.1
$\mathbb{Z}/27\mathbb{Z}$	27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}(\zeta_{27})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	15a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	15a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	30a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	210e2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}(\zeta_{19})^+$

Questions?

The Numerous Problem Variations

There are numerous questions you can ask about elliptic curves, e.g.

- Fix an elliptic curve, vary the extensions.



- Fix a field, K, and vary the elliptic curves:

$$E_1(K) \qquad E_2(K) \qquad E_3(K) \qquad E_4(K) \qquad E_5(K) \qquad \cdots$$

- Vary both the curves and the fields:

$$\begin{array}{cccc} E_1(K_1) & E_1(K_2) & E_1(K_3) & \cdots \\ E_2(K_1) & E_2(K_2) & E_2(K_3) & \cdots \\ E_3(K_1) & E_3(K_2) & E_3(K_3) & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Hilbert's 10th Problem

We discussed a method for finding rational points on conics, but this involved starting with a rational point. How do we even know there is such a point? You can ask this question generally, can we decide if a Diophantine equation has a point over some ring. This is Hilbert's 10th Problem. Below is a table for what is known about whether this holds over certain rings, ordered by their arithmetic complexity (the complexity of their absolute Galois group).

Ring	Hilbert's 10th
$\mathbb{C}$	✓
$\mathbb{R}$	✓
$\mathbb{F}_q$	✓
p-adic fields	✓
$\mathbb{F}_q((t))$	?
Number Fields	?
$\mathbb{Q}$	?
Global Function Fields	✗
$\mathbb{F}_q(t)$	✗
$\mathbb{C}(t)$	?
$\mathbb{C}(t_1, \ldots, t_n)$	✗
$\mathbb{R}(t)$	✗
$\mathcal{O}_K$	$\approx$?
$\mathbb{Z}$	✗

Additional Elliptic Curve Terms

Definition (Isogeny)

Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. If $|\ker \phi| = n$, we say ϕ is an n-isogeny.

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

j-INVARIANT

Take an elliptic curve $y^2 = x^3 + Ax + B$. The transformations which preserve this equations are: $x = \mu^2 x$ and $y = \mu^3 y$ for $\mu \in \overline{K}^\times$. We then define the j-invariant

$$j = 1728 \frac{4A^3}{4A^4 + 27B^2}$$

These classify elliptic curves up to isomorphism over $\overline{K}$.

Remark

The j-invariant does not classify elliptic curves over K:

$$y^2 = x^3 - 25x$$
$$y^2 = x^3 - 4x$$

Both have j-invariant 1728 but are not isomorphic over $K = \mathbb{Q}$ (but are over $K = \mathbb{Q}(\sqrt{10})$). So the j-invariant only classifies elliptic curves 'up to twisting'.

Endomorphism Ring & CM Elliptic Curves

Considering the multiplication by n-map: $P \mapsto nP$

$$\operatorname{End} E \supseteq \mathbb{Z}$$

Generally, $\operatorname{End} E$ is one of the following:

- $\mathbb{Z}$
- an order in an imaginary quadratic field
- an order in a quaternion algebra (not if char $K = 0$)

Example

$$y^2 = x^3 + B$$
$$(x, y) \mapsto (\zeta_3 x, -y)$$
$$y^2 = x^3 + Ax$$
$$(x, y) \mapsto (-x, iy)$$

Definition (CM Elliptic Curve)

An elliptic curve E is said to have complex multiplication (CM) or be a CM elliptic curve (an elliptic curve with complex multiplication) if $\operatorname{End} E \supsetneq \mathbb{Z}$.

Division Polynomials

Consider an elliptic curve $y^2 = x^3 + Ax + B$ and define

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-2}\psi_{n+1}^3 \\
\psi_{2n} &= \left(\frac{\psi_n}{2y}\right)(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)
\end{aligned}$$

The polynomial ψ_n is called the nth division polynomial. The roots of ψ_n give the x-coordinates of the p-torsion points.

Weil Pairing

There is a pairing $e_n : E[n] \times E[n] \to \mathbb{Q}(\zeta_n)$, called the Weil pairing, satisfying

(i) e_n is bilinear

(ii) e_n is non-degenerate

(iii) $e_n(P, P) = 1$

(iv) $e_n(P, Q) = e_n(Q, P)^{-1}$

(v) $e_n(P^\sigma, Q^\sigma) = \sigma e_n(P, Q)$ for all automorphisms of $\overline{K}$ which fix A, B.

Remark

Using the Weil pairing, it is routine to verify that if $E[n] \subseteq K^2$, then $\mathbb{Q}(\zeta_n) \subseteq K$.

Definition (Weakly Modular Form of Weight k)

Let k be an integer. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is weakly modular form of weight k if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \tau \in \mathcal{H}$$

Definition (Modular Form of Weight k)

Let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is modular form of weight k if

(i) f is holomorphic on $\mathcal{H}$,

(ii) f is weakly modular of weight k,

(iii) f is holomorphic at ∞.

Define the modular form, called the Weierstrass $\wp$-function,

$$\wp(z) = \wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

and define the Eisenstein series of weight k

$$G_{k,\Lambda} = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-k}$$

$\wp(z)$ satisfies the following:

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

Now define an elliptic curve

$$\begin{aligned} y^2 &= 4x^3 - g_2x - g_3 \\ g_2 &= 60G_4 \\ g_3 &= 140G_6 \end{aligned}$$

Theorem

Let Λ be a lattice, and let E be the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. Then

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto \infty \end{aligned}$$

is an isomorphism of groups.

To go the other direction, write E as

$$y^2 = 4x^3 - g_2 x - g_3 = 4(x - e_1)(x - e_2)(x - e_3); \quad e_1 < e_2 < e_3$$

Then define

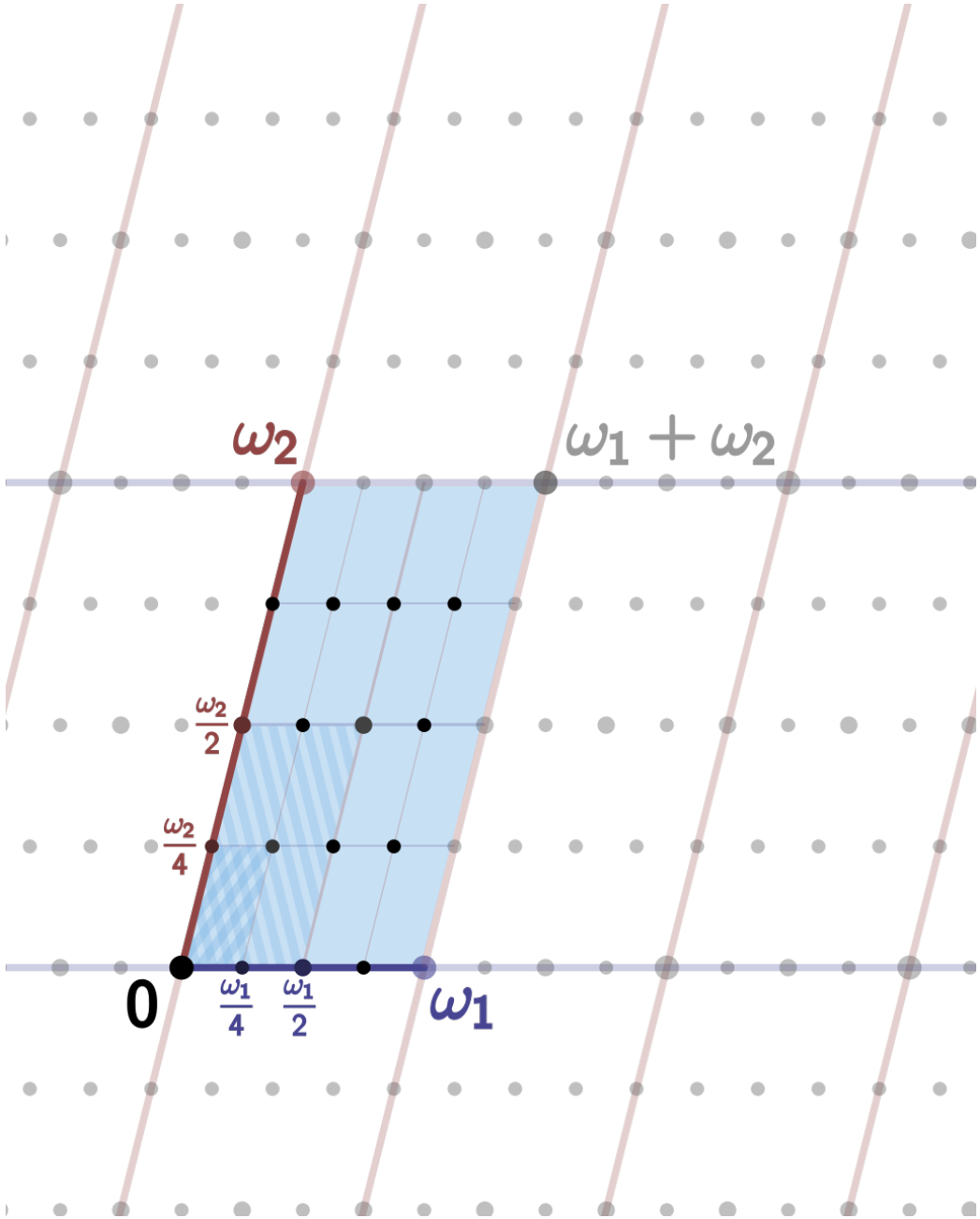
$$\omega_1 = \frac{2i}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}} \int_1^{1/k} \frac{dt}{\sqrt{(t^2 - 1)(1 - k^2 t^2)}}$$

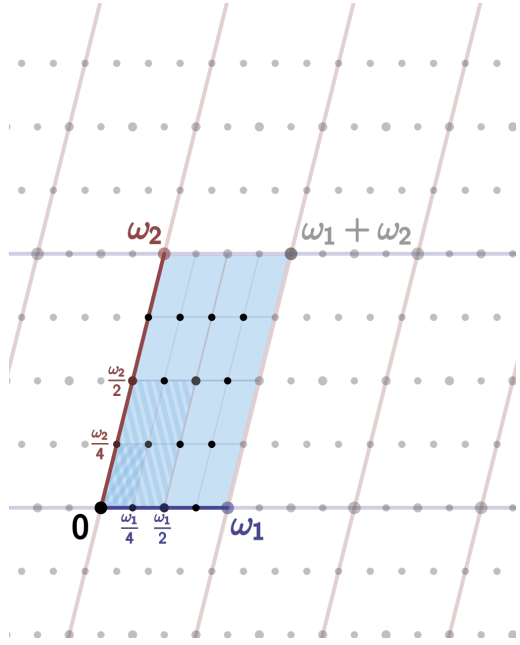
$$\omega_2 = \frac{2}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}} \int_{-1}^{1} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 t^2)}}$$

where

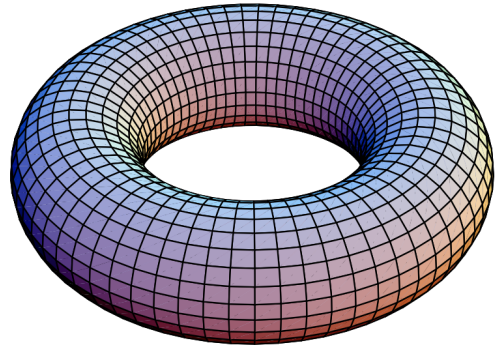
$$k = \frac{\sqrt{e_3 - e_1} - \sqrt{e_3 - e_2}}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}}$$

Then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.





- This shows: $E[n] := \{P \in E : nP = \mathcal{O}\} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
- $E(\mathbb{C})$ is isomorphic to a torus



Structure of the Torsion Subgroup

$$E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$$

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

Galois Representations

- Let $G_K := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.
- G_K acts on $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
- Fix a basis of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, then we have a representation

$$\rho_{E,n} : G_K \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

  the so-called mod n Galois representation.
- One also forms the ℓ-adic Tate module: $T_\ell(E) := \varprojlim_n E[\ell^n]$ and the ℓ-adic representation $\rho_\ell : G_K \to \mathrm{Aut}(T_\ell(E))$.

Theorem (Serre)

Let K be a number field, and let E/K be an elliptic curve without CM. Then for all but finitely many primes ℓ, $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective.

L-FUNCTIONS

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

Then we define the Hasse-Weil L-function of E to be

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

We can also write

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where a_n are the Fourier coefficients given by

$$a_p = \begin{cases} p+1-N_p, & \text{if } E \text{ has good reduction at } p \\ 1, & \text{if } E \text{ has split multiplicative reduction at } p \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0, & \text{if } E \text{ has additive reduction at } p \end{cases}$$

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

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

Andrew Wiles

Richard Taylor

Christophe Breuil

Brian Conrad

Fred Diamond

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

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

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

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

Conjecture (BSD)

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.

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^{r_E}} = \frac{\Omega_E \ \text{Reg}(E) \ \#Ш(E/\mathbb{Q}) \ \prod_p c_p}{\#E(\mathbb{Q})^2_{tors}}$$

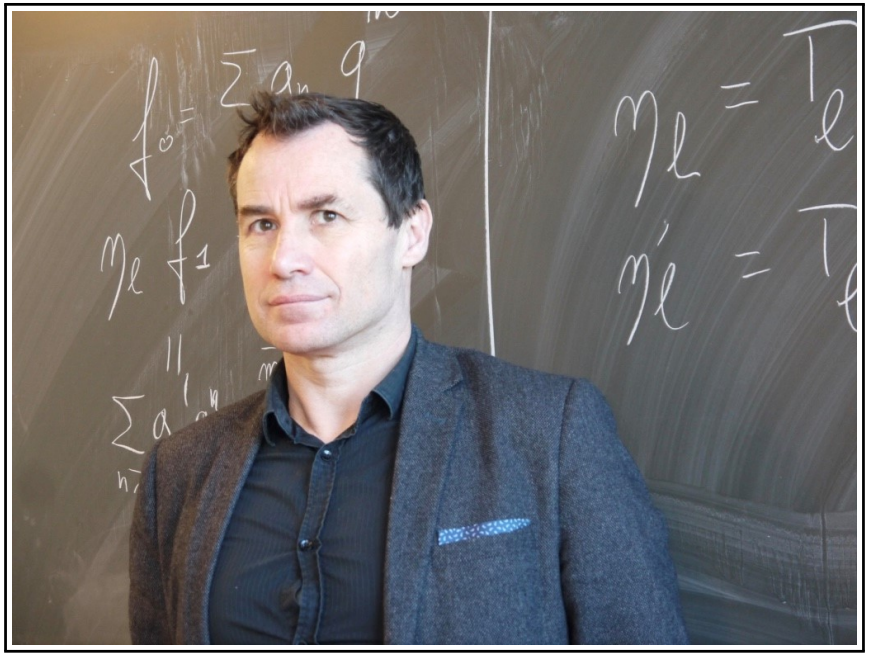
Boundedness

Boundedness of Torsion

One should ask why there should be finitely many possible torsion subgroups at all. The boundedness of the size of the torsion subgroup is a result of several individuals, originating with Merel in 1996.

Theorem (Merel,1996)

Let K be a number field of degree $[K : \mathbb{Q}] = d > 1$. There is a number $B(d) > 0$ such that $|E(K)_{tors}| \leq B(d)$ for all elliptic curves E/K.



Loïc Merel

Theorem (Merel, 1996; Parent, 1999)

Let K be a number field of degree $d > 1$. Then

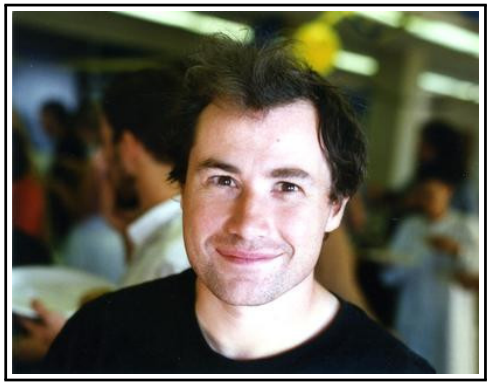
(i) *(Merel) Let E/K be an elliptic curve. If $E(K)$ contains a point of exact prime order p, then $\ell \leq d^{3d^2}$.*

(ii) *(Parent) If P is a point of exact prime power order ℓ^n, then*

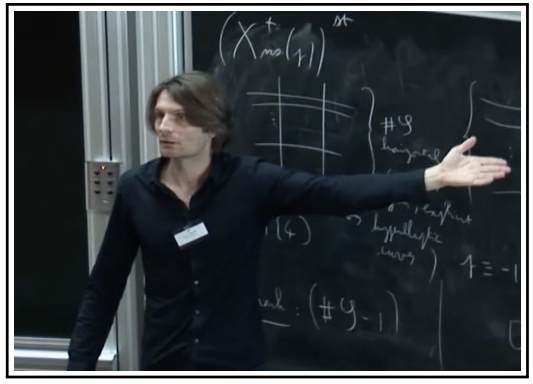
- (a) $\ell^n \leq 65(3^d - 1)(2d)^6$, *if* $\ell \geq 5$
- (b) $\ell^n \leq 65(5^d - 1)(2d)^6$, *if* $\ell = 3$
- (c) $\ell^n \leq 129(3^d - 1)(3d)^6$, *if* $\ell = 2$

In particular, $\ell^p \leq 129(5^d - 1)(3d)^6$ for all primes ℓ.

(iii) *(Oesterlé) If $p \in S(d)$, then $p \leq (1 + 3^{d/2})^2$.*



Loïc Merel



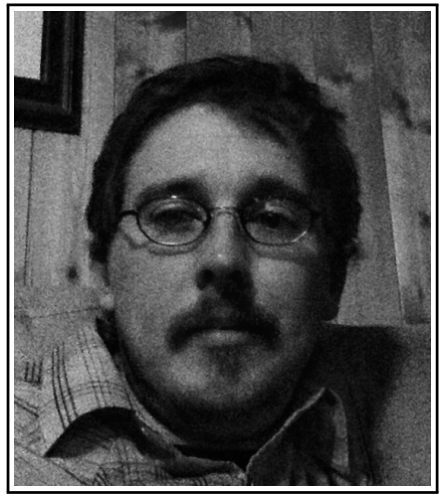
Pierre Parent

Joseph Oesterlé

Conjecture (Clark, Cook, Stakewicz)

There is a constant C such that $B(d) \leq C\, d \log\log d$ for all $d \geq 3$.

Pete Clark



Brian Cook

James Stankewicz

Theorem (Hindry, Silverman, 1999)

Let K be a field of degree $d \geq 2$ and E/K be an elliptic curve such that $j(E)$ is an algebraic integer. Then we have

$$|E(K)_{tors}| \leq 1\,977\,404 \cdot d \log d$$

Marc Hindry

Joseph Silverman

Theorem (Clark, Pollack, 2015)

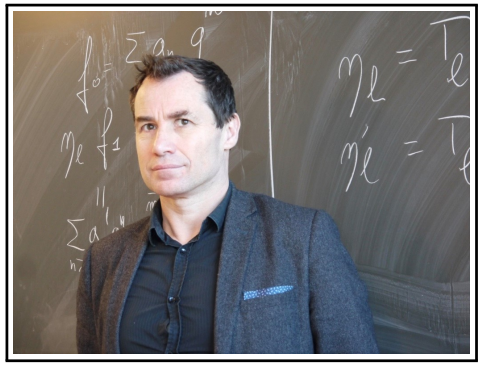
There is an absolute, effective constant C such that for all number fields K of degree $d \geq 3$ and all elliptic curves E/K with CM, we have $|E(K)_{tors}| \leq C\, d \log\log d$.

Pete Clark

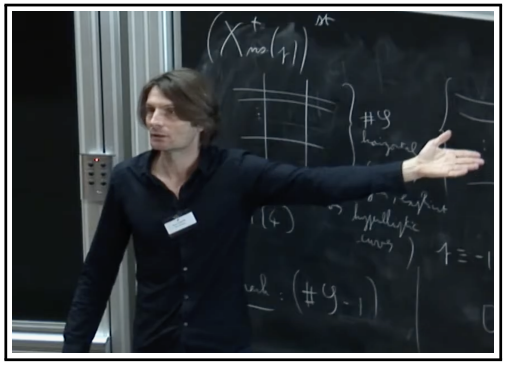
Paul Pollack

Theorem (Merel, 1996)

Let $F/\mathbb{Q}$ be a number field of degree d. If $P \in E(F)$ is a point of exact prime power p^n, then $p \leq 3^{3d^2}$.



Loïc Merel



Pierre Parent

Remark

In 1999, Parent improved this to $p^n \leq 129(5^d - 1)(3d)^6$.

Theorem (Lozano-Robledo, 2013)

Let $K/\mathbb{Q}$ be a number field of degree d and suppose there is an elliptic curve E/K with CM by a full order with a point of order p^n, then

$$\varphi(p^n) \leq 24\, e_{\max}(p, K/\mathbb{Q}) \leq 24\, d$$

Álvaro Lozano-Robledo

Torsion over General Number Fields

Theorem (Kenku, Momose, 1988; Kamienny, 1992)

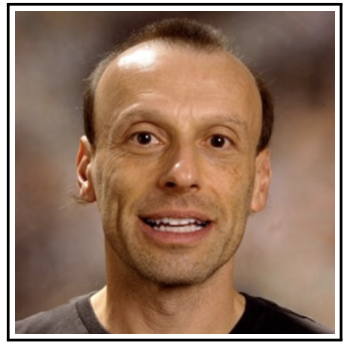
Let $K/\mathbb{Q}$ be a quadratic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{cases}$$

Moreover, each possibility occurs infinitely often.

Monsur Kenku

Fumiyuki Momose



Sheldon Kamienny

Theorem (Jeon,Kim,Schweizer, 2004; Etropolski,Morrow,Zureick Brown; Derickx, 2016; Derickx,Etropolski,van Hoeij,Morrow,Zureick-Brown, 2020)

Let $K/\mathbb{Q}$ be a cubic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 20, 21 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 7 \end{cases}$$

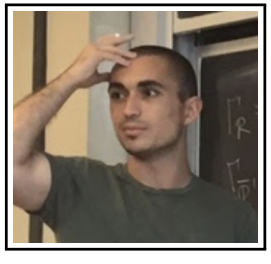
Each of these possibilities occurs infinitely many times except for $\mathbb{Z}/21\mathbb{Z}$ which occurs only for the elliptic curve `162b1` over $\mathbb{Q}(\zeta_9)^+$.

Jeon

Kim

Schweizer

Etropolski



Morrow

Zureick-Brown

Derickx

van Hoeij

Theorem (Jeon, Kim, Park, 2006)

Let $K/\mathbb{Q}$ be a quartic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 18, 20, 21, 22 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Daeyeol Jeon

Chang Kim

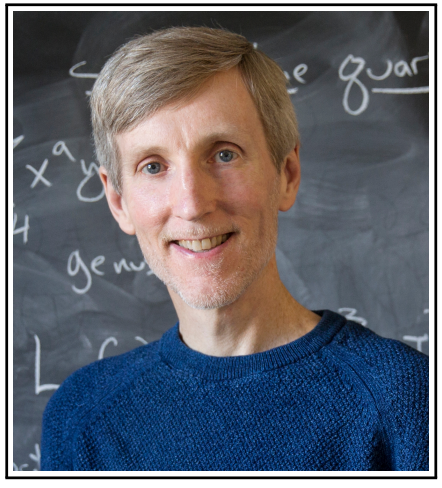
Eui-Sung Park

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a quintic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, \ldots, 22, 24, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 8 \end{cases}$$

Maarten Derickx



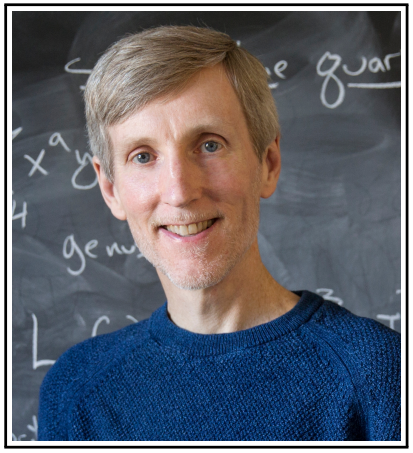
Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a sextic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, \ldots, 30; n \neq 23, 25, 29 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 10 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, \ldots, 4 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Maarten Derickx



Drew Sutherland

Theorem (Clark, Corn, Rice, Stankewicz; 2013)

Let K be a number field of degree $d = 1, 2, \ldots, 13$ and E/K be an elliptic curve with CM. Then all possible torsion subgroups are given, and an algorithm to compute the list.

Pete Clark

Patrick Corn

Alex Rice

James Stankewicz

Theorem (Bourdon, Clark, Stankewicz, 2015)

Let F be a number field of odd degree, let E/F be a K-CM elliptic curve, and let $T = E(F)_{tors}$. Then

(a) *One of the following occurs:*

- (i) *T is isomorphic to the trivial group $\mathcal{O}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;*
- (ii) *$T \cong \mathbb{Z}/\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \mod 8$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$;*
- (iii) *$T \cong \mathbb{Z}/2\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \mod 4$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$.*

(b) *If $E(F)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta = -4$.*

(c) *If $E(F)_{tors} \cong \mathbb{Z}/4\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta \in \{-4, -16\}$.*

(d) *Each of the groups listed in part (a) arises up to isomorphism as the torsion subgroup $E(F)$ of a CM elliptic curve E defined over an odd degree number field F.*

Abbey Bourdon

Pete Clark

James Stankewicz

Theorem (Bourdon, Pollack; 2018)

Let K be an odd degree number field and E/K be an elliptic curve with CM. Then the torsion subgroups $E(K)_{tors}$ are computable.

Abbey Bourdon

Paul Pollack

Theorem (Bourdon, Chaos; 2022)

Let F be a number field of degree $2p$ for $p > 5$ prime, and let E/F be an elliptic curve with CM by the order of discriminant Δ. Then $E(F)_{tors}$ is new if and only if one of the following occurs:

(i) $\Delta = -115$, $p = 11$, *and* $E(F)_{tors} \cong \mathbb{Z}/23\mathbb{Z}$, *or*

(ii) $\Delta = -235$, $p = 23$, *and* $E(F)_{tors} \cong \mathbb{Z}/47\mathbb{Z}$, *or*

(iii) $\Delta = \in \{-11, -19, -27, -43, -67, -163\}$, p *is a Germain prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{tors} \cong \mathbb{Z}/(2p+1)\mathbb{Z}$, *or*

(iv) $\Delta \in \{-8, -12, -16, -28\}$, p *is a Germain prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{tors} \cong \mathbb{Z}/2(2p+1)\mathbb{Z}$, *or*

(v) $\Delta = -7$, p *is a Germain prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}2(2p+1)\mathbb{Z}$, *or*

(vi) $\Delta = -3$, $p = 7$, *and* $E(F)_{tors} \cong \mathbb{Z}/49\mathbb{Z}$, *or*

(vii) $\Delta = -3$, $6p+1$ *is prime, and* $E(F)_{tors} \cong \mathbb{Z}/(6p+1)\mathbb{Z}$, *or*

(viii) $\Delta = -4$, $4p+1$ *is prime, and* $E(F)_{tors} \cong \mathbb{Z}/2(4p+1)\mathbb{Z}$.

In particular, any new torsion subgroup arises on one of only finitely many CM elliptic curves, and all but $\Delta = -115$ and -235 correspond to imaginary quadratic orders of class number 1.

Abbey Bourdon

Holly Paige Chaos

Torsion over Infinite Extensions

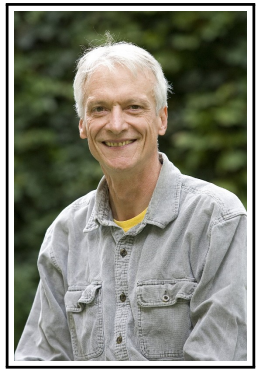
Theorem (Laska, Lorenz, 1985; Fujita, 2005)

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $\mathbb{Q}(2^\infty)$ be the maximal abelian 2-extension of $\mathbb{Q}$. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 15 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, & \text{or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 3, 4 \end{cases}$$

and each such possibility occurs.

Michael Laska



Martin Lorenz

Yasutsugu Fujita

Theorem (Daniels, Lozano-Robledo, Najman, Sutherland, 2017)

Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the torsion subgroup $E(\mathbb{Q}(3^\infty))_{tors}$ is finite and is isomorphic to precisely one of the following groups:

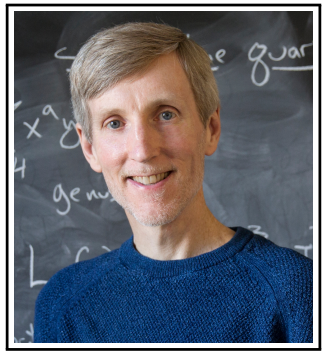
$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 4, 5, 7, 8, 13 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 4, 7 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & \text{with } n = 1, 2, 3, 5, 7 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 4, 6, 7, 9. \end{cases}$$

All but four of the torsion subgroups, T, listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. For $T \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, there are only 2, 2, 4, and 1 (respectively) $\overline{\mathbb{Q}}$-isomorphism classes of $E/\mathbb{Q}$ for which $E(\mathbb{Q}(3^\infty))_{tors} \cong T$.

Harris Daniels

Álvaro Lozano-Robledo

Filip Najman



Andrew Sutherland

Theorem (Daniels, 2017)

Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}(D_4^\infty))$ is finite and isomorphic to one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 13, 15 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 5 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 6, 8 \text{ or} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 5, 16. \end{cases}$$

All but 3 of the 24 torsion structures listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. The torsion structures that occur finitely often are $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$, and $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, which occur for 4, 2, and 1 $\overline{\mathbb{Q}}$-isomorphism classes, respectively.

Harris Daniels

Theorem (Daniels, Derickx, Hatley, 2019)

Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(A_4^\infty))_{tors}$ is finite and isomorphic to one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 13, 15, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7 \text{ or} \\ \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 6, 8. \end{cases}$$

All but 4 of the 26 torsion structures listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. The torsion structures that occur finitely often are $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/15$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, which occur for 4, 2, 2, and 1 $\overline{\mathbb{Q}}$-isomorphism classes, respectively.

Harris Daniels

Maarten Derickx

Jeffrey Hatley

Theorem (Chou, 2019)

Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}^{ab})_{tors}$ is finite, and is isomorphic to precisely one of the following groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 9 \text{ or} \\ \mathbb{Z}3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 5, 6, 8. \end{cases}$$

Each of the listed groups appears as a torsion subgroup for $E(\mathbb{Q}^{ab})_{tors}$ for some elliptic curve over $\mathbb{Q}$.

Michael Chou

Theorem (Chou, Daniels, Krijan, Najman, 2018)

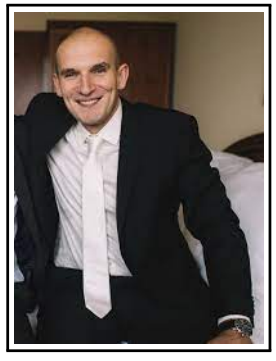
Let p be a prime, and let $E/\mathbb{Q}$ be an elliptic curve. Then if $p = 2, 3$, then $E(\mathbb{Q}_{\infty,p})_{tors}$ is one of the following groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 21^*, 27^* \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, \end{cases}$$

where the starred cases can only occur if $p = 3$. If $p \neq 2, 3$, then $E(\mathbb{Q}_{\infty,p})_{tors} = E(\mathbb{Q})_{tors}$. Each of the groups listed above appears as a torsion subgroup for $E(\mathbb{Q}_{\infty,p})_{tors}$ for some $E/\mathbb{Q}$ and each p possible.

Michael Chou

Harris Daniels



Ivan Krijan

Filip Najman

Theorem (Gužvić, Vukorepa, 2022)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors} \in \Phi(1)$ or is one of $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and $E(\mathbb{Q}(\zeta_{27}))_{tors} \in \Phi(1)$ or is one of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}$ with $n = 1, 2, 3$, $\mathbb{Z}/21\mathbb{Z}$, or $\mathbb{Z}/27\mathbb{Z}$. Furthermore, let $p \in \{5, 7, 11\}$. Then either $E(\mathbb{Q}(\zeta_p))_{tors} \in \Phi(1)$ or is one of $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, or $\mathbb{Z}/16\mathbb{Z}$, if $p = 5$, or $\mathbb{Z}/n\mathbb{Z}$ with $n = 13, 14, 18$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ with $n = 7, 9$, if $p = 7$, or $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/25\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, if $p = 11$.

Theorem (Gužvić, Krijan, 2020)

Let $\mathcal{K} = \prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}$ and $\mathcal{K}_{\geq p} = \prod_{q \text{ prime}, q \geq p}$, and let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathcal{K}_{\geq 5})_{tors} = E(\mathbb{Q})_{tors}$ and $E(\mathcal{K})_{tors}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 21, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

Moreover, each such group above occurs for some elliptic curve $E/\mathbb{Q}$.

Tomislav Gužvić

Ivan Krijan

Borna Vukorepa

Theorem (Rouse,Zureick-Brown, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve without CM. Then the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/Q))$ divides 64 or 96, and all such indices occur. Furthermore, the image of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_2)$ of the image of $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

Jeremy Rouse

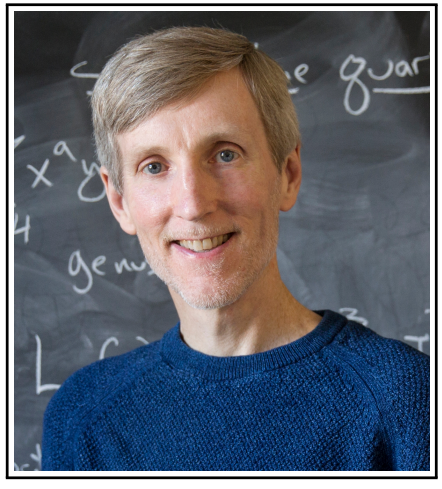
David Zureick-Brown

Remark

They also enumerate all 1,208 possibilities and find their rational points.

Theorem (Sutherland, Zywina, 2016)

Up to conjugacy, there are 248 open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ *of prime power level satisfying* $-I \in G$ *and* $\det G = \hat{\mathbb{Z}}^\times$ *for which* X_G *has infinitely many rational points. Of these 248 groups, there are 220 of genus 0 and 28 of genus 1.*



Drew Sutherland

David Zywina

Possible Prime Divisors

Theorem (Mazur, Parent, Derickx, Kammienny, Stein, Stoll, Lozano-Robledo, et al.)

$$
\begin{aligned}
S_{\mathbb{Q}}(\{1,2\}) &= \{2,3,5,7\} \\
S_{\mathbb{Q}}(\{3,4\}) &= \{2,3,5,7,13\} \\
S_{\mathbb{Q}}(\{5,6,7\}) &= \{2,3,5,7,11,13\} \\
S_{\mathbb{Q}}(8) &= \{2,3,5,7,11,13\} \\
S_{\mathbb{Q}}(\{9,10,11\}) &= \{2,3,5,7,11,13,17,19\} \\
S_{\mathbb{Q}}(\{12,\ldots,20\}) &= \{2,3,5,7,11,13,17,19,37\} \\
S_{\mathbb{Q}}(21) &= \{2,3,5,7,11,13,17,19,37,43\}
\end{aligned}
$$

Remark

Lozano-Robledo computes $S_{\mathbb{Q}}(d)$ for $1 \leq d \leq 21$, and gives a conjecturally formula valid for all $1 \leq d \leq 42$, following from a positive answer to Serre's uniformity question.

Álvaro Lozano-Robledo

Remark

Furthermore, Enrique González-Jiménez and Filip Najman determine all possible prime orders of a point $P \in E(K)_{\text{tors}}$, where $[K : \mathbb{Q}] = d$ for all $d \leq 3\,342\,296$.

Theorem (González-Jiménez, Lozano-Robledo, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values:

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad \text{or} \quad -\frac{7 \cdot 17231878060 80^3}{79^{16}}$$

in which case $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this is best possible in that there are one-parameter families $E_{s,N}(t)$ of elliptic curves over $\mathbb{Q}$ such that for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ such that $[\mathbb{Q}(T_{s,N}):\mathbb{Q}]$ is equal to the bound given above.

Torsion over Function Fields

Theorem (McDonald, 2017)

Let $K = \mathbb{F}_q(T)$, where $q = p^n$. Let E/K be non-isotrivial. If $p \nmid E(K)_{tors}$, then $E(K)_{tors}$ is one of the following:
$0, \mathbb{Z}/2\mathbb{Z}, \ldots, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.
If $p \mid \#E(K)_{tors}$, then $p \leq 11$, and $E(K)_{tors}$ is one of

$$\begin{cases} \mathbb{Z}/p\mathbb{Z}, & p = 2, 3, 5, 7, 11 \\ \mathbb{Z}/2p\mathbb{Z}, & p = 2, 3, 5, 7 \\ \mathbb{Z}/3p\mathbb{Z}, & p = 2, 3, 5 \\ \mathbb{Z}/4p\mathbb{Z}, & p = 2, 3 \\ \mathbb{Z}/5p\mathbb{Z}, & p = 2, 3 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & p = 2 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, & p = 3 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & p = 5 \end{cases}$$

Robert McDonald