Elliptic Curves and Galois Theory

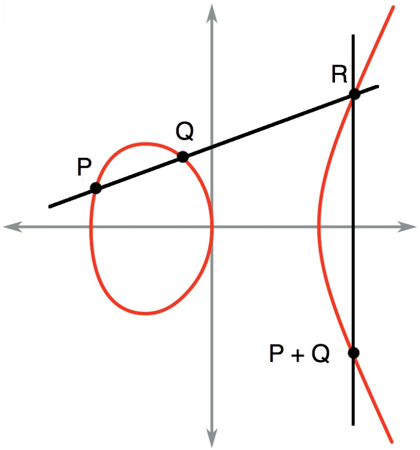
David Zureick-Brown
Amherst College

JHU–UMD Algebra and Number Theory Day

May 2, 2025

Slides available at https://dmzb.github.io/

Elliptic Curves – addition



$$E\colon y^2 = x^3 + ax + b$$
$$P = (x_0, y_0)$$
$$Q = (x_1, y_1)$$
$$R = (x_2, y_2)$$
$$P + Q = (x_2, -y_2)$$

Why are elliptic curves so interesting?

Elliptic curves are "just right":

- First interesting case after conics.
  [Apollonius of Perga (240-190BC)]
- Higher genus is "hyperbolic".
- A managable special or first case.

Connections

- Langlands, representation theory, Fermat's last theorem
- Arithmetics Dynamics
- Geometry (first moduli space; algebraic and Lie groups)
- Topology (elliptic cohomology, homotopy groups of spheres)
- Logic (Hilbert's Tenth Problem; definability)

Applications

- Cryptography
- Factorization
- More cryptography

Popular culture

Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m$ be polynomials with integer coefficients, e.g.,

$$\begin{aligned} x^2 + y^2 + 1 &= 0 \\ x^3 - y^2 - 2 &= 0 \\ 2y^2 + 17x^4 - 1 &= 0 \end{aligned}$$

Basic problem: solve polynomial equations

Describe the set

$$V(f_1, \ldots, f_m) = \left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i, f_i(a_1, \ldots, a_n) = 0 \right\},$$

i.e., the set of integer solutions to those polynomials

Fact

Solving Diophantine equations is difficult.

Hilbert's Tenth Problem

Theorem (Davis–Putnam–Robinson 1961, Matijasevič 1970)

There does not exist an algorithm solving the following problem:

***input**: integer polynomials* $f_1, \ldots, f_m$ *in variables* $x_1, \ldots, x_n$*;*

***output**:* $\mathrm{YES} \,/\, \mathrm{NO}$ *according to whether the set of solutions*

$$\left\{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}$$

is non-empty.

This is *known* to be true for many other cases (e.g., $\mathbb{C}, \mathbb{R}, \mathbb{F}_q, \mathbb{Q}_p, \mathbb{C}(t)$).

This is *still unknown* in many other cases (e.g., $\mathbb{Q}$).

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad \pm(0,1,1).$$

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad \pm(0,1,1).$$

This took 300 years to prove!

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

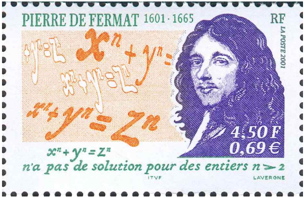
For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad \pm(0,1,1).$$

This took 300 years to prove!



Fermat’s Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

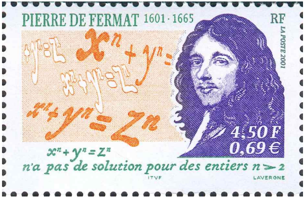
For primes $p \geq 3$ the only integer solutions to the equation

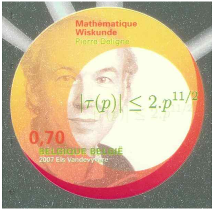
$$x^p + y^p = z^p$$

are integer multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad \pm(0,1,1).$$

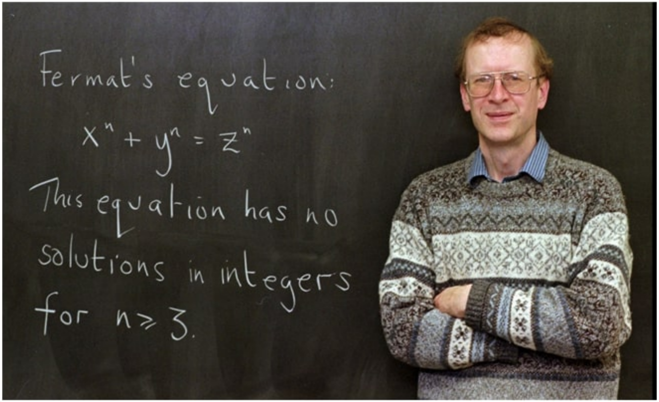
This took 300 years to prove!



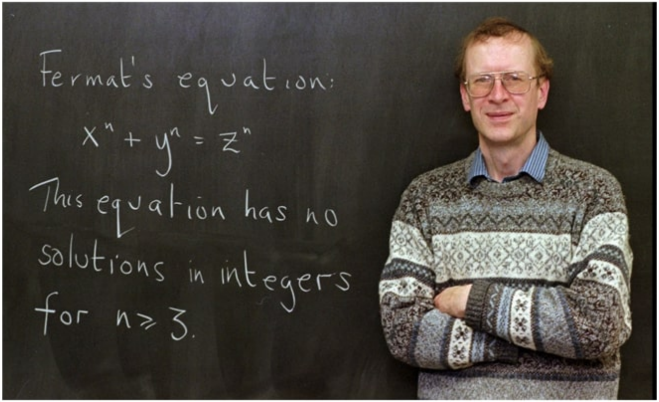


https://mathshistory.st-andrews.ac.uk/Miller/stamps/

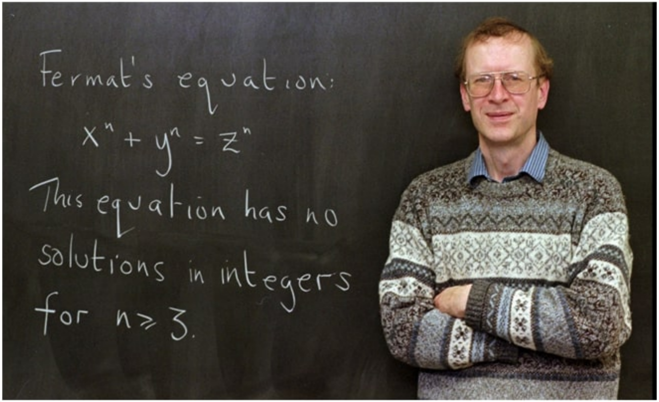
Fermat's Last Theorem - aftermath



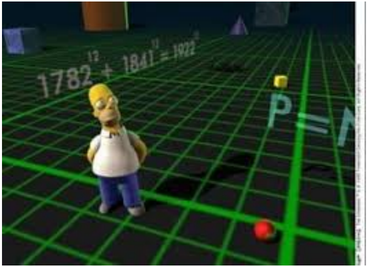
Fermat's Last Theorem - aftermath



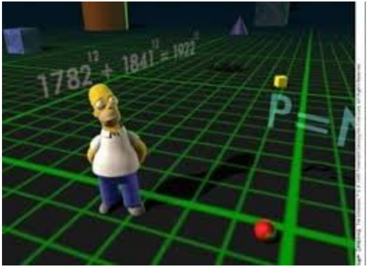
Fermat's Last Theorem - aftermath

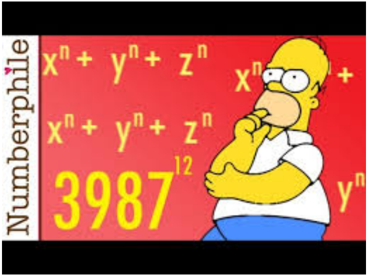


Fermat trolling



Fermat trolling



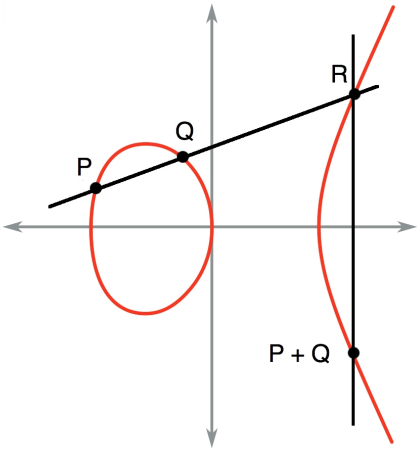


See https://youtu.be/ReOQ300AcSU?si=--fAdsdPttt4HR3N

Progressive Metal (2007)

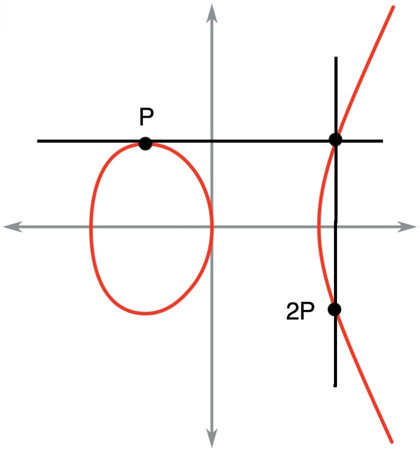
See Omnisdimensional Creator and Info Dump

Elliptic Curves – addition



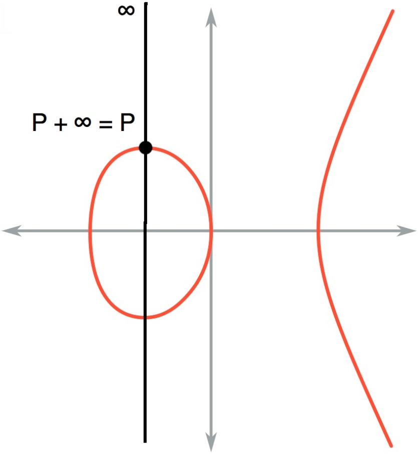
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0)$$
$$Q = (x_1, y_1)$$
$$R = (x_2, y_2)$$
$$P + Q = (x_2, -y_2)$$

Elliptic Curves - duplication



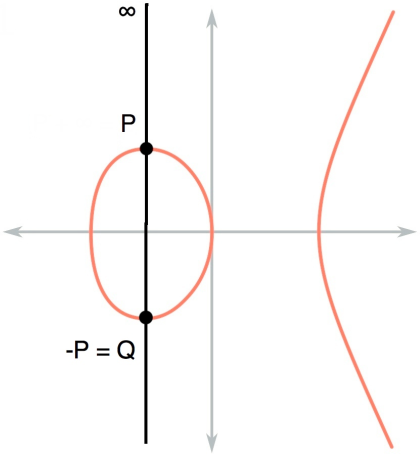
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0)$$
$$2P = (x_3, y_3)$$

Elliptic Curves – identity



$$E: y^2 = x^3 + ax + b$$

Elliptic Curves – inverses



$$E: y^2 = x^3 + ax + b$$

Guiding question

What are the possibilities for the abelian group $E(K)$?

$E(K)$ as K varies

Complete fields

- $E(\mathbb{C}) \cong S^1 \times S^1 \cong \mathbb{C}/\Lambda$ (a torus).
- $E(\mathbb{R}) \cong S^1$ or $S^1 \times \mathbb{Z}/2\mathbb{Z}$.
- $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \oplus T$

Mordell–Weil theorem

$E(\mathbb{Q})$ is finitely generated, thus isomorphic to $\mathbb{Z}^r \oplus T$

- r is the **rank** of $E(\mathbb{Q})$
- T is the **torsion subgroup** of $E(\mathbb{Q})$
- T is a finite abelian group (thus a product of cyclic groups)

Finite Fields

$E(\mathbb{F}_q)$ is finite, and $\#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$.

$E(K)$ as K varies

If $K \subset L$, then $E(K) \subset E(L)$ is a subgroup.

If K is a number field (e.g., $\mathbb{Q}(i)$), then

Mordell–Weil theorem

$E(K)$ is finitely generated, thus isomorphic to $\mathbb{Z}^r \oplus T$

- r is the **rank** of $E(K)$
- T is the **torsion subgroup** of $E(K)$
- T is a finite abelian group (thus a product of cyclic groups)

Rank you very much

Mordell–Weil theorem, for K a number field

$E(K) \cong \mathbb{Z}^r \oplus T$

r is the **rank** of $E(K)$

Rank and file

- r is unbounded as we vary K.
- r is conjecturally bounded if $K = \mathbb{Q}$.
- (2006 Elkies) there is an $E/\mathbb{Q}$ of rank 28
- (2024 Elkies–Klagsbrun) there is an $E/\mathbb{Q}$ of rank 29

Distribution of ranks

- $r = 0$ half the time, and $r = 1$ half the time (over $\mathbb{Q}$).
- $r = 2$ infinitely often (over $\mathbb{Q}$)
- (Alex Smith) true for quadratic twists

  and twisting is a “Markov process” on 2-power Selmer groups

Elliptic Curves – torsion subgroup

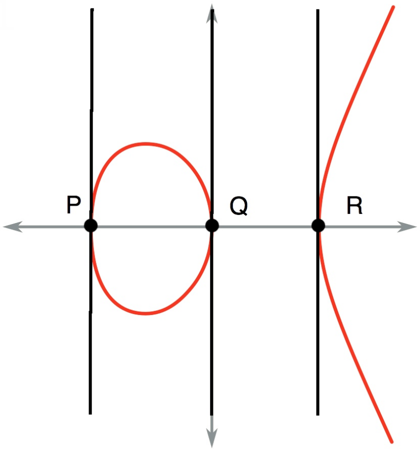
Let $n \in \mathbb{Z}$ be an integer.

Definition

The *n-torsion subgroup* $E[n]$ of E is defined to be

$$\ker\left(E \xrightarrow{[n]} E\right) := \{P \in E : nP := P + \ldots + P = \infty\}.$$

Elliptic Curves – two torsion



$$E: y^2 = x^3 + ax + b$$
$$2P = 2Q = 2R = \infty$$

Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- $E[n](\mathbb{Q})$ may be smaller,

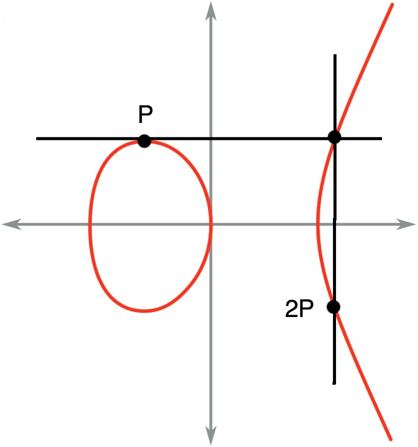
Elliptic Curves – structure of torsion

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- $E[n](\mathbb{Q})$ may be smaller, e.g.,

$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

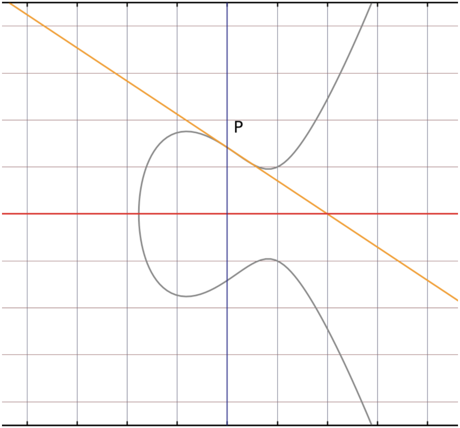
3-torsion and flexes



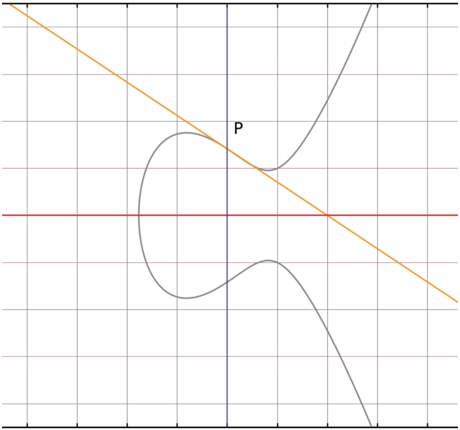
$$3P = 0$$

$$2P = -P$$

3-torsion and flexes



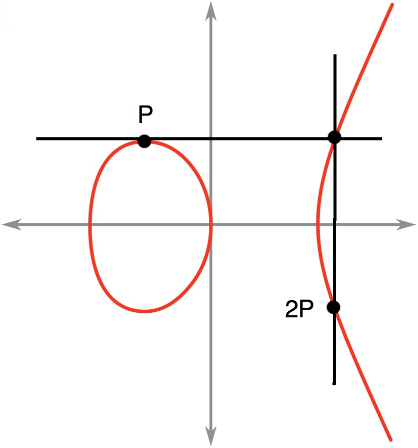
3-torsion and flexes



How many flexes?

How many flexes?

4 torsion



$$4P = 0$$

$$2P = -2P$$

Mazur's Theorem

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

Theorem (Mazur, 1978)

$E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups.

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 4. \end{array}$$

Quadratic Torsion

Theorem (Kamienny–Kenku–Momose, 1980's)

Let E be an elliptic curve over a quadratic number field K. Then $E(K)_{\text{tors}}$ is one of the following groups.

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 16 \text{ or } N = 18, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, & \text{for } 1 \leq N \leq 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

Higher Degree Torsion

Let $K/\mathbb{Q}$ have degree d.

Theorem

If $p \mid \#E(K)_{tors}$, then:

$$\begin{aligned} \textit{(Merel, 1996)} \quad & p \leq d^{3d^2} \\ \textit{(Oesterlé)} \quad & p \leq (3^{d/2}+1)^2 \ \textit{(if } p > 3\textit{)} \end{aligned}$$

Problem: Classify possibilities for $E(K)_{\text{tors}}$ for $K/\mathbb{Q}$ of degree d.

Modular curves

The curve $Y_1(N)$ parameterizes pairs (E, P), where P is a point of exact order N on E.

Let $M \mid N$.

The curve $Y_1(M, N)$ parameterizes E/K such that $E(K)_{\text{tors}}$ contains $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

Modular curves via Tate normal form

Move a given point P to $(0,0)$ and change coordinates to put E in the form

$$y^2 + axy + by = x^3 + bx^2$$

The point $P = (0,0)$ may or may not be a torsion point.

The condition that $nP = 0$ is an algebraic condition on a and b, and this gives you a curve.

Modular curves via Tate normal form

Example ($N = 9$)

$E(K) \supset \mathbb{Z}/9\mathbb{Z}$ if and only if there exists $t \in K$ such that E is isomorphic to

$$y^2 + (t - rt + 1)xy + (rt - r^2t)y = x^3 + (rt - r^2t)x^2$$

where r is $t^2 - t + 1$. The torsion point is $(0, 0)$.

Example ($N = 11$)

$E(K) \supset \mathbb{Z}/11\mathbb{Z}$ if and only if there exist $a, b \in K$ such that

$$a^2 + (b^2 + 1)a + b = 0$$

in which case E is isomorphic to

$$y^2 + (s - rs + 1)xy + (rs - r^2s)y = x^3 + (rs - r^2s)x^2$$

where r is $ba + 1$ and s is $-b + 1$.

Mazur's Theorem

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

Theorem (Mazur, 1978)

$E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups.

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 4. \end{array}$$

Modular curves:

- $Y_1(N)$ paramaterizes (E, P) with $P \in E[N]$ (of exact order N);
- $Y_1(M, N)$ paramaterizes containments $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \subset E(K)_{\text{tors}}$.

Mazur:

$Y_1(N)(\mathbb{Q}) \neq \varnothing$ and $Y_1(2, 2N)(\mathbb{Q}) \neq \varnothing$ iff N are as above.

Rational Points on $X_1(N)$ and $X_1(2, 2N)$

Let $X_1(N)$ and $X_1(M, N)$ be smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$.

We can restate Mazur's Theorem as follows.

Theorem (Mazur, 1978)

- *$X_1(N)$ and $X_1(2, 2N)$ have **genus 0** for **exactly** the N in Mazur's Theorem.*
- *In particular, there are **infinitely many** $E/\mathbb{Q}$ with such torsion structures.*
- *If $g(X)$ is **greater than** 0, then $X(\mathbb{Q})$ consists **only of cusps**.*

Minimalism

The *simplest* thing that could happen does for these modular curves.

Quadratic Torsion

Theorem (Kamienny–Kenku–Momose, 1980's)

Let E be an elliptic curve over a quadratic number field K. Then $E(K)_{tors}$ is one of the following groups.

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 16 \text{ or } N = 18, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, & \text{for } 1 \leq N \leq 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

- The corresponding modular curves all have $g(X) \leq 2$.
- Each admits a **degree 2 map** $X \to \mathbb{P}^1$.
- This guarantees that $\mathrm{Sym}^{(2)} X(\mathbb{Q})$ is infinite.
- i.e., each has infinitely many quadratic points.

Sporadic Points

Let $X/\mathbb{Q}$ be a curve and let $P \in \overline{\mathbb{Q}}$. The **degree** of P is $[\mathbb{Q}(P) : \mathbb{Q}]$.

The set of degree d points of X is infinite if (and only if)

- X admits a degree d map $X \to \mathbb{P}^1$;
- X admits a degree d map $X \to E$, where $\operatorname{rank} E(\mathbb{Q}) > 0$; or
- Jac_X contains a positive rank abelian subvariety such that ...

Most $\overline{\mathbb{Q}}$ points on curves arise in this fashion (by Riemann–Roch).

- We call outliers **isolated**.
- **Cusps and CM** points are often isolated on modular curves.
- An isolated point P on X is **sporadic** if there are only finitely points of X with the same degree as P.
- A sporadic point is **exceptional** if it is not cuspidal or CM.

See Bianca Viray's CNTA talk, linked here.

Cubic Torsion

Theorem (Jeon–Kim–Schweizer, 2004)

Let E be an elliptic curve over a cubic number field K. Then the subgroups which arise as $E(K)_{tors}$ infinitely often are exactly the following.

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 20,\ N \neq 17, 19, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 7. \end{array}$$

Minimalist conjecture

Conjecture

A modular curve X admits a non cuspidal, non CM point of degree d if and only if

- *X admits a degree d map $X \to \mathbb{P}^1$; or*
- *X admits a degree d map $X \to E$, where $\operatorname{rank} E(\mathbb{Q}) > 0$; or*
- *Jac_X contains a positive rank abelian subvariety such that...*

Minimalist conjecture

Conjecture

A modular curve X admits a non cuspidal, non CM point of degree d if and only if

- *X admits a degree d map $X \to \mathbb{P}^1$; or*
- *X admits a degree d map $X \to E$, where $\operatorname{rank} E(\mathbb{Q}) > 0$; or*
- *Jac_X contains a positive rank abelian subvariety such that...*

Cubic Torsion

Theorem (Jeon–Kim–Schweizer, 2004)

Let E be an elliptic curve over a cubic number field K. Then the subgroups which arise as $E(K)_{tors}$ infinitely often are exactly the following.

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 20,\ N \neq 17, 19, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 7. \end{array}$$

Theorem (Najman, 2014)

The elliptic curve `162b1` has a 21-torsion point over $\mathbb{Q}(\zeta_9)^+$.

Theorem (Parent)

The largest prime that can divide $E(K)_{tors}$ in the cubic case is $p = 13$.

Classification of Cubic Torsion

Theorem (Etropolski–Morrow–ZB–Derickx–van Hoeij)

The only torsion subgroups which appear for an elliptic curve over a cubic field are

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{for } 1 \leq N \leq 21,\ N \neq 17, 19, \text{ and} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & \text{for } 1 \leq N \leq 7. \end{array}$$

The only sporadic point is the elliptic curve `162b1` *over* $\mathbb{Q}(\zeta_9)^+$.

Galois theory: torsion fields

Definition

The n-torsion field of E/K is the field

$$K(E[n]) = \{x(P) : P \in E[n](\overline{K})\} \cup \{y(P) : P \in E[n](\overline{K})\}$$

i.e., the field obtained by adjoining the coordinates of the n-torsion points of E to K.

Remark

- *$K(E[n])$ is Galois over K.*
- *Indeed, if $\sigma \in G_K = \mathrm{Aut}_K \overline{K}$, then*

$$\sigma(nP) = n\sigma(P) = 0$$

(since the equations for $[n]$ have coefficients in K).

Example: $K(E[2])$

Let E be given by the equation $y^2 = f(x) = x^3 + ax + b$.

- $E[n](\mathbb{C}) = E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$.
- $E[n](\mathbb{Q})$ may be smaller, e.g.,

$$E[2](\mathbb{Q}) \cong \begin{cases} \{\infty\} & \text{if } f(x) \text{ has 0 rational roots} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } f(x) \text{ has 1 rational roots} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } f(x) \text{ has 3 rational roots} \end{cases}$$

  since $E[2](\mathbb{C}) = \{\infty\} \cup \{(e, 0) : f(e) = 0\}$
- $K(E[2])$ is thus the splitting field of f, and $\mathrm{Gal}(K(E[2])/K) \subseteq S_3$