“Sporadic” torsion on elliptic curves

David Zureick-Brown

Amherst College

arXiv:2007.13929

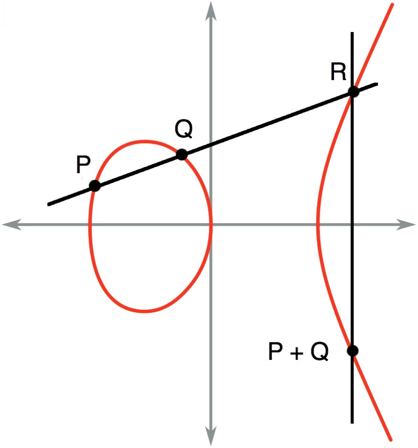
with Maarten Derickx,
Anastassia Etropolski,
Jackson S. Morrow,
and Mark van Hoeij

Connecticut Summer School in Number Theory

June 15, 2024

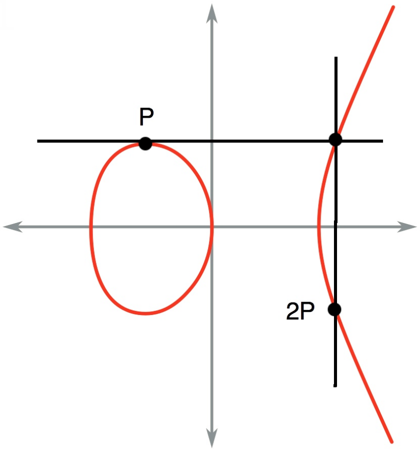
Slides available at `https://dmzb.github.io/`

Elliptic Curves – addition



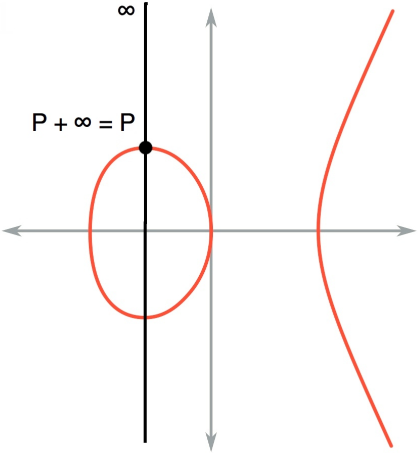
$$E\colon y^2 = x^3 + ax + b$$
$$P = (x_0, y_0)$$
$$Q = (x_1, y_1)$$
$$R = (x_2, y_2)$$
$$P + Q = (x_2, -y_2)$$

Elliptic Curves - duplication



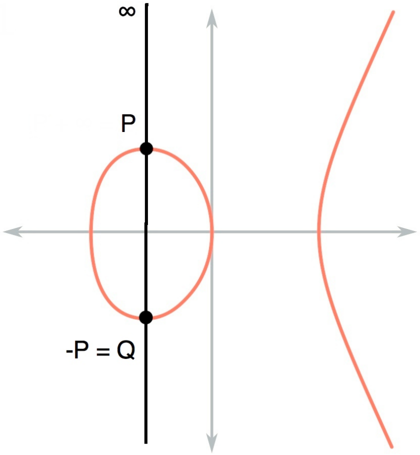
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0)$$
$$2P = (x_3, y_3)$$

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)

Elliptic Curves – torsion subgroup

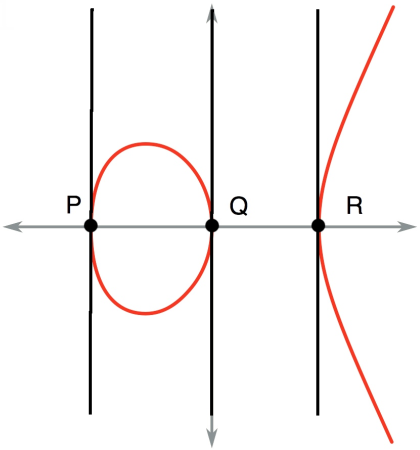
Let $n \in \mathbb{Z}$ be an integer.

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,

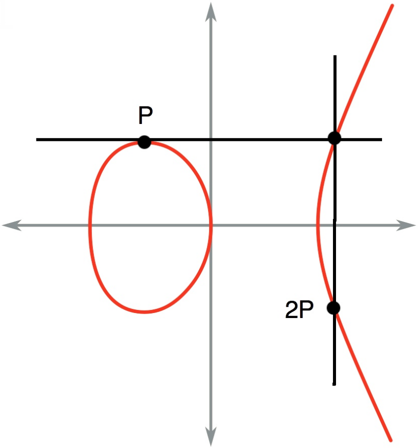
Elliptic Curves – structure of torsion

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.,

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

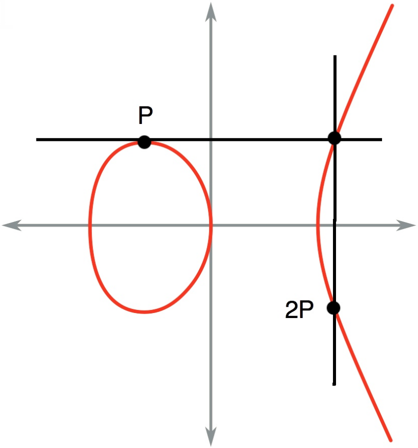
3-torsion and flexes



$$3P = 0$$

$$2P = -P$$

3-torsion and flexes



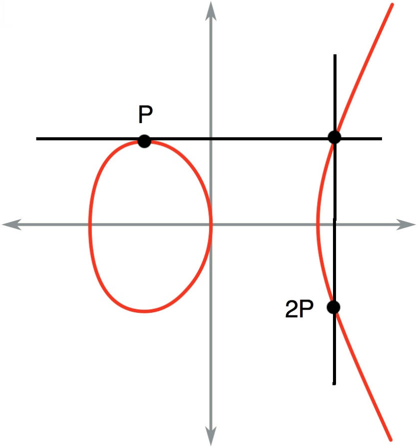
$$3P = 0$$

$$2P = -P$$

9 flexes

9 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.

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

Higher Degree Torsion

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

Theorem

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

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

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

$$a^2 + (b^2 + 1)a + b;$$

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.

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

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.

Higher Degree Torsion

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

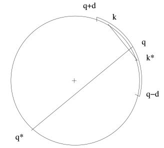
Theorem

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

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

Proof: **formal immersions** on $\mathrm{Sym}^{(d)} X_1(p)$.

Expository reference: Darmon, Rebellodo (Clay 2006)



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

Quadratic Torsion

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

Let E be an elliptic curve over a quadratic number field K. Then $E(K)_{\mathit{tors}}$ 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 $E(K)_{\mathit{tors}}$ infinitely often are exactly the following.

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

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 $E(K)_{\mathit{tors}}$ 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* $\mathbb{Q}(\zeta_9)^+$.

Najman's example

Theorem (Najman, 2014)

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

- Let $H := \rho_{E,21}(G_{\mathbb{Q}})$.
- Then H contains an index 3 subgroup H' such that $H' \subset \left\langle \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\rangle$
- Thus there is a degree 3 map

$$X_{H'} \to X_H$$

and an induced map

$$X_H \to \operatorname{Sym}^{(3)} X_{H'} \to \operatorname{Sym}^3 X_1(21)$$

Sporadic points on $X_1(N)$ with rational j-invariant

Bourdon–Gill–Rouse–Watson (2020)

The odd degree isolated points on $X_1(N)$ with rational j-invariant are

$$j = -3^2 \cdot 5^6/2^3, \text{ or } 3^3 \cdot 13/2^2$$

The first is the Najman cubic example, and the second corresponds to a degree 8 point on $X_1(28)$, found by Najman and González-Jiménez.

Bourdon–Hashimoto–Keller–Klagsbrun–Lowry-Duda–Morrison–Najman–Shukla, with Derickx–Van Hoeij (2023)

Strong evidence that the other other isolated $j \in \mathbb{Q}$ are

$$j = -7 \cdot 11^3 \text{ or } 7 \cdot 137^3 \cdot 2083^3 \qquad (\text{from } X_0(37)(\mathbb{Q})).$$

Rouse–Sutherland–Zureick-Brown–Voight

Conjectural classification of $X_H(\mathbb{Q})$ for prime power level.

See Jeremy Rouse's CNTA talk, linked here

Mazur - Rational Isogenies of Prime Degree (1978)

Let N be a positive integer. Examples of elliptic curves over $\mathbf{Q}$ possessing rational cyclic N-isogenies are known for the following values of N:

N	g	ν	N	g	ν	N	g	ν
$\leqq 10$	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

More Sporadic Points on $X_1(N)$, via Derickx–van Hoeij

d	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
20	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
19	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
18	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
17	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	12	∞	∞	∞
16	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	11	∞	∞	∞
15	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	10	∞
14	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	∞	∞
13	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	4	∞	1	∞	3	26
12	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	3	∞
11	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	3	∞	9	∞	1	∞				4
10	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	2	∞	1	∞	∞	∞	2	∞	1	3	1	2
9	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	1	8	1	4		∞			1	1
8	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞		∞	1	3	1	∞			1	1
7	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	∞	∞		∞			1			2				
6	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞	1	∞	∞	∞		∞							1			
5	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞		∞	∞			1		2										
4	∞	∞	∞	∞	∞	∞	∞	∞		∞	∞	∞		∞																
3	∞	∞	∞	∞	∞	∞		∞		∞	1																			
2	∞	∞	∞	∞	∞	∞		∞																						
1		∞																												

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* $\mathbb{Q}(\zeta_9)^+$.

Good fortune – many small level ranks are zero

Let

$$S_0 = \{1, \ldots, 36, 38, \ldots, 42, 44, \ldots, 52, 54, 55, 56, 59, 60, 62, 63, 64, 66, 68, 69, 70, 71, 72, 75, 76, 78, 80, 81, 84, 87, 90, 94, 95, 96, 98, 100, 104, 105, 108, 110, 119, 120, 126, 132, 140, 144, 150, 168, 180\},$$

$$S_1 = \{1, \ldots, 21, 24, 25, 26, 27, 30, 33, 35, 36, 42, 45\}.$$

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

1. $\operatorname{rank} J_0(N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_0$.
2. $\operatorname{rank} J_1(N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_0 - \{63, 80, 95, 104, 105, 126, 144\}$.
3. $\operatorname{rank} J_1(2, 2N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_1$.

Strategy

Previous work

- (Parent) handles $p > 13$ (via formal immersions).
- (Momose) $N = 27, 64$.
- (Wang) $N = 77, 91, 143, 169$
- (Bruin–Najman) $N = 40, 49, 55$

This leaves

- (rank 0) $N = 21, 22, 24, 25, 26, 28, 30, 32, 33, 35, 36, 39, 45$
- (rank 1) $N = 65, 121$

Rank 0

"Direct" analysis: $J(\mathbb{Q})$ is finite, and in principle it is a straightforward Riemann–Roch computation to compute the preimages of the Abel–Jacobi map:

$$X^{(d)}(\mathbb{Q}) \xrightarrow{\iota} J(\mathbb{Q})$$

Mordell–Weil Sieve: For a finite set S of primes of good reduction, we compare the images of α and β:

$$\begin{tikzcd}
X^{(d)}(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{p\in S} X^{(d)}(\mathbb{F}_q) \arrow[r, "\beta"] & \prod_{p\in S} J(\mathbb{F}_p)
\end{tikzcd}$$

Big obstacle: we need to know $J(\mathbb{Q})$!

Minutiae

Level	Genus	Method of proof	Genus of quotient
32	17	Maps to another curve in this table	$g(X_1(2,16)) = 5$
36	17	Maps to another curve in this table	$g(X_1(2,18)) = 7$
22	6	Local methods at $p = 3$ (§6.1)	N/A
25	12	Local methods at $p = 3$	N/A
21	5	Direct analysis over $\mathbb{Q}$ (§6.2)	N/A
26	10	Direct analysis over $\mathbb{F}_3$	N/A
30	9	Direct analysis over $\mathbb{Q}$ on $X_0(30)$ (§6.4)	$g(X_0(30)) = 3$
33	21	Direct analysis over $\mathbb{Q}$ on $X_0(33)$	$g(X_0(33)) = 3$
35	25	Direct analysis over $\mathbb{Q}$ on $X_0(35)$	$g(X_0(35)) = 3$
39	33	Direct analysis over $\mathbb{Q}$ on $X_0(39)$	$g(X_0(39)) = 3$
(2,16)	5	Hecke bound + direct analysis over $\mathbb{F}_3$ (§6.5)	N/A
(2,18)	7	Hecke bound + direct analysis over $\mathbb{F}_5$	N/A
28	10	Hecke bound + direct analysis over $\mathbb{F}_3$ (§6.6)	N/A
24	5	Hecke bound + additional argument (§4.13) + direct analysis over $\mathbb{F}_5$	N/A
45	41	Hecke bound + direct analysis over $\mathbb{Q}$ on $X_H(45)$ (§6.7)	$g(X_H(45)) = 5$
65	121	Formal immersion criteria (§7.3)	$g(X_0(65)) = 5$
121	526	Formal immersion criteria (§7.1)	$g(X_0(121)) = 6$

Formal immersions

- Classically, one takes p so large that any points of $X_1(p)^{(d)}(\mathbb{Q})$ reduces to a cusp mod 3
- (possible by the Hasse bound).
- *formal immersion criterion* $\Rightarrow$ the diagonal map is injective

$$\begin{tikzcd} X^{(d)}(\mathbb{Q}) \arrow[r, "\iota"] & J(\mathbb{Q}) \arrow[r] & A(\mathbb{Q}) \\ {]\infty[} \arrow[u] \arrow[urr] & & \end{tikzcd}$$

Maarten's insight

- This doesn't really have anything to do with modular forms
- (just differentials).
- For small N, if you understand what is going on well enough, you can modify the "criterion" to any individiual case you need.

Thank you!

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* $\mathbb{Q}(\zeta_9)^+$.

Rank 0

Well, $J(\mathbb{Q})$ is finite, and in principle it is a straightforward Riemann–Roch computation to compute the preimages of the Abel–Jacobi map:

$$X^{(d)}(\mathbb{Q}) \xrightarrow{\iota} J(\mathbb{Q})$$

Mordell–Weil Sieve: For a finite set S of primes of good reduction, we compare the images of α and β:

$$\begin{tikzcd} X^{(d)}(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\ \prod_{p \in S} X^{(d)}(\mathbb{F}_q) \arrow[r, "\beta"] & \prod_{p \in S} J(\mathbb{F}_p) \end{tikzcd}$$

Big obstacle: we need to know $J(\mathbb{Q})$!

Good fortune – many small level ranks are zero

Let

$$\begin{aligned} S_0 = \{&1, \ldots, 36, 38, \ldots, 42, 44, \ldots, 52, 54, 55, 56, 59, 60, 62, 63, 64, 66, 68, \\ &69, 70, 71, 72, 75, 76, 78, 80, 81, 84, 87, 90, 94, 95, 96, 98, 100, 104, 105, \\ &108, 110, 119, 120, 126, 132, 140, 144, 150, 168, 180\}, \end{aligned}$$

$$S_1 = \{1, \ldots, 21, 24, 25, 26, 27, 30, 33, 35, 36, 42, 45\}.$$

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

1. $\operatorname{rank} J_0(N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_0$.
2. $\operatorname{rank} J_1(N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_0 - \{63, 80, 95, 104, 105, 126, 144\}$.
3. $\operatorname{rank} J_1(2, 2N)(\mathbb{Q}) = 0$ *if and only if* $N \in S_1$.

More Sporadic Points on $X_1(N)$, via Derickx–van Hoeij