Sporadic Cubic Torsion

David Zureick-Brown

Amherst College

arXiv:2007.13929

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

AMS Special Session on
Arithmetic Geometry with a View toward Computation

January 6, 2024

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

Mazur's Theorem

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups.

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

Via geometry, let

- $Y_1(N)$ be the curve paramaterizing (E, P), where P is a point of exact order N on E, and let
- $Y_1(M, N)$ (with $M \mid N$) be the curve paramaterizing E/K such that $E(K)_{\text{tors}}$ contains $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

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

Modular curves via Tate normal form

Example ($N = 9$)

$E(K) \cong \mathbb{Z}/9\mathbb{Z}$ 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 ($N = 11$)

$E(K) \cong \mathbb{Z}/11\mathbb{Z}$ correspond to $a, b \in K$ 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 $-b + 1$.

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

Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. We can restate the results of Mazur's Theorem as follows.

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

So, in a sense, the simplest thing that could happen does happen for these modular curves.

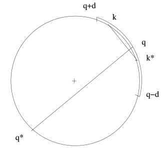
Higher Degree Torsion Points

Theorem (Merel, 1996)

For every integer $d \geq 1$, there is a constant $N(d)$ such that for all $K/\mathbb{Q}$ of degree at most d and all E/K,

$$\#E(K)_{tors} \leq N(d).$$

Expository reference: Darmon, Rebellodo (Clay summer school, 2006)



Problem

Fix $d \geq 1$. Classify all groups which can occur as $E(K)_{tors}$ for $K/\mathbb{Q}$ of degree d. Which of these occur infinitely often?

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.

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

In particular, the corresponding curves $X_1(M,N)$ all have $g \leq 2$, which guarantees that they have 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

- 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 arise in the fashion. We call outliers **isolated**
- When X is a modular curve, cusps and CM points give rise to many isolated points; we call an isolated point **sporadic** 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.

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

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 $X \to \mathbb{P}^1$; ot*
- *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* $X \to \mathbb{P}^1$*; ot*
- 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.

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

Theorem (Najman, 2014)

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

Remark

Parent showed that 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

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

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

Modular curves

Definition

- $X(N)(K) := \{(E/K, P, Q) : E[N] = \langle P, Q\rangle\} \cup \{\text{cusps}\}$
- $X(N)(K) \quad \ni \quad (E/K, P, Q) \Leftrightarrow \rho_{E,N}(G_K) = \{I\}$

Definition

$\Gamma(N) \subset H \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ (finite index)

- $X_H := X(N)/H$
- $X_H(K) \ni (E/K, \iota) \Leftrightarrow H(N) \subset H \mod N$

Stacky disclaimer

This is only true up to twist; there are some subtleties if

1. $j(E) \in \{0, 12^3\}$ (plus some minor group theoretic conditions), or
2. if $-I \in H$.

Example - torsion on an elliptic curve

If E has a K-rational **torsion point** $P \in E(K)[n]$ (of exact order n) then:

$$H(n) \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= \quad P \\ \sigma(Q) &= \quad a_\sigma P \quad + \quad b_\sigma Q \end{aligned}$$

Example - Isogenies

If E has a K-rational, **cyclic isogeny** $\phi\colon E \to E'$ with $\ker\phi = \langle P \rangle$ then:

$$H(n) \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= \quad a_\sigma P \\ \sigma(Q) &= \quad b_\sigma P \quad + \quad c_\sigma Q \end{aligned}$$

Example - other maximal subgroups

Normalizer of a split Cartan:

$$N_{\mathrm{sp}} = \left\langle \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

$H(n) \subset N_{\mathrm{sp}}$ and $H(n) \not\subset C_{\mathrm{sp}}$ iff

- there exists an unordered pair $\{\phi_1, \phi_2\}$ of cyclic isogenies,
- whose kernels intersect trivially,
- neither of which is defined over K,
- but which are both defined over some quadratic extension of K,
- and which are Galois conjugate.

Example - other maximal subgroups

Normalizer of a non-split Cartan:

$$C_{\mathsf{ns}} = \mathrm{im}\left(\mathbb{F}_{p^2}^* \to \mathrm{GL}_2(\mathbb{F}_p)\right) \subset N_{\mathsf{ns}}$$

$H(n) \subset N_{\mathsf{ns}}$ and $H(n) \not\subset C_{\mathsf{ns}}$ iff

E admits a “necklace” (Rebolledo, Wuthrich)

A typical subgroup (from Rouse–ZB)

"Jenga"

$$\begin{array}{ccccccc}
\ker\phi_4 & \subset & H(32) & \subset & \mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_4 = 4 \\
 & & \downarrow{\scriptstyle \phi_4} & & \downarrow & & \\
\ker\phi_3 & \subset & H(16) & \subset & \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_3 = 3 \\
 & & \downarrow{\scriptstyle \phi_3} & & \downarrow & & \\
\ker\phi_2 & \subset & H(8) & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_2 = 2 \\
 & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\
\ker\phi_1 & \subset & H(4) & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_1 = 3 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow & & \\
 & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) & &
\end{array}$$

$$\ker\phi_i \subset I + \ell^i M_2(\mathbb{F}_\ell) \cong \mathbb{F}_\ell^4$$

Non-abelian entanglements

(from Brau–Jones)

There exists a surjection $\theta\colon\ \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

$$\begin{tikzcd}
 & H(6) := \Gamma_\theta \arrow[ddl, two heads] \arrow[ddr, two heads] \arrow[d, phantom, "\cap"] & \\
 & \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \arrow[dl, two heads] \arrow[dr, two heads] & \\
\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})
\end{tikzcd}$$

$$\operatorname{im}\rho_{E,6} \subset H(6) \Leftrightarrow j(E) = 2^{10}3^3t^3(1-4t^3) \Rightarrow K(E[2]) \subset K(E[3])$$
$$X_H \cong \mathbb{P}^1 \xrightarrow{j} X(1)$$

Rational Points on modular curves

Mazur's program B

Compute $X_H^{(d)}(\mathbb{Q})$ for all H.

Remark

- *Sometimes* $X_H \cong \mathbb{P}^1$ *or elliptic with rank* $X_H(\mathbb{Q}) > 0$.
- *Some* X_H *have sporadic points.*
- *Can compute* $g(X_H)$ *group theoretically (via Riemann–Hurwitz).*
- *Can compute* $\#X_H(\mathbb{F}_q)$ *via moduli and enumeration [Sutherland].*

Fact

$$g(X_H), \gamma(X_H) \to \infty \text{ as } \left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H\right] \to \infty.$$

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 $H' \subset \left\langle \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix} \right) \right\rangle$
- Thus we have a degree 3 map

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

and an induced map

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

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	v	N	g	v	N	g	v
$\leqq 10$	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			

CM j-invariants

Zywina, Silverman AEC II

j-invariant	D	f	Elliptic curve $E_{D,f}$	N
0	3	1	$y^2 = x^3 + 16$	3^3
$2^4 3^3 5^3$		2	$y^2 = x^3 - 15x + 22$	$2^2 3^2$
$-2^{15} 3 \cdot 5^3$		3	$y^2 = x^3 - 480x + 4048$	3^3
$2^6 3^3 = 1728$	4	1	$y^2 = x^3 + x$	2^6
$2^3 3^3 11^3$		2	$y^2 = x^3 - 11x + 14$	2^5
$-3^3 5^3$	7	1	$y^2 = x^3 - 1715x + 33614$	7^2
$3^3 5^3 17^3$		2	$y^2 = x^3 - 29155x + 1915998$	7^2
$2^6 5^3$	8	1	$y^2 = x^3 - 4320x + 96768$	2^8
-2^{15}	11	1	$y^2 = x^3 - 9504x + 365904$	11^2
$-2^{15} 3^3$	19	1	$y^2 = x^3 - 608x + 5776$	19^2
$-2^{18} 3^3 5^3$	43	1	$y^2 = x^3 - 13760x + 621264$	43^2
$-2^{15} 3^3 5^3 11^3$	67	1	$y^2 = x^3 - 117920x + 15585808$	67^2
$-2^{18} 3^3 5^3 23^3 29^3$	163	1	$y^2 = x^3 - 34790720x + 78984748304$	163^2

Sporadic points on $X_H(\ell)$, $H \subset \mathrm{GL}_2(\mathbb{F}_\ell)$

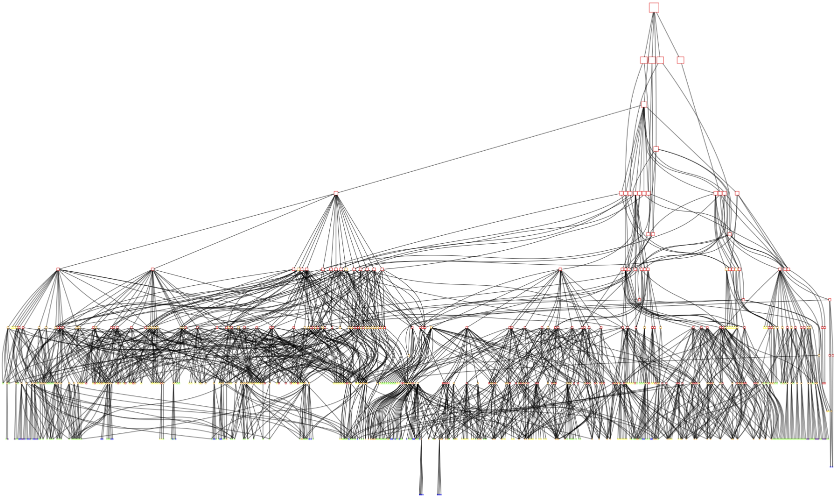
Zywina, "On the Possible Images of the Mod ℓ Representations Associated to…"

7	$3^3 \cdot 5 \cdot 7^5/2^7$	$H \subsetneq N_{ns}(7)$	Sutherland 2012
11	-11^2	$\left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \begin{pmatrix}2^2&0\\0&2^9\end{pmatrix} \right\rangle$	$g(X_0(11)) = 1$
	$-11 \cdot 131^3$	$\left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \begin{pmatrix}2^4&0\\0&2^7\end{pmatrix} \right\rangle$	
13	$\frac{2^4 \cdot 5 \cdot 13^4 \cdot 17^3}{3^{13}}$	$\widetilde{H} \subset S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$	BDMTV
	$-\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}}$		Annals 2019
	$\frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}}$		$g = r = 3$
17	$-17 \cdot 373^3/2^{17}$, $-17^2 \cdot 101^3/2$	$H_i \subsetneq B(17)$	$g(X_0(17)) = 1$
37	$-7 \cdot 11^3$, $-7 \cdot 137^3 \cdot 2083^3$	$H_i \subsetneq B(37)$	$\exists\, \iota \neq w_{37}$

2-adic sporadic points; $H \subset \mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z})$, index 96 or 64

j-invariant	level of H	Generators of image	
2^{11}	16	$\begin{bmatrix}7 & 14\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 5\\6 & 11\end{bmatrix}, \begin{bmatrix}3 & 0\\0 & 7\end{bmatrix}$	hyperelliptic
$2^4 \cdot 17^3$	16	$\begin{bmatrix}7 & 0\\0 & 3\end{bmatrix}, \begin{bmatrix}3 & 5\\14 & 7\end{bmatrix}, \begin{bmatrix}7 & 7\\2 & 1\end{bmatrix}$	genus 3
$\frac{4097^3}{2^4}$	16	$\begin{bmatrix}3 & 5\\6 & 3\end{bmatrix}, \begin{bmatrix}3 & 5\\14 & 7\end{bmatrix}, \begin{bmatrix}7 & 7\\2 & 1\end{bmatrix}$	rank 1
$\frac{257^3}{2^8}$	16	$\begin{bmatrix}7 & 14\\0 & 1\end{bmatrix}, \begin{bmatrix}5 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 5\\6 & 3\end{bmatrix}$	
$-\frac{857985^3}{62^8}$	32	$\begin{bmatrix}25 & 18\\2 & 7\end{bmatrix}, \begin{bmatrix}25 & 25\\2 & 7\end{bmatrix}, \begin{bmatrix}1 & 0\\8 & 1\end{bmatrix}, \begin{bmatrix}25 & 11\\2 & 7\end{bmatrix}$	not hyperelliptic
$\frac{919425^3}{496^4}$	32	$\begin{bmatrix}29 & 0\\4 & 1\end{bmatrix}, \begin{bmatrix}31 & 27\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 4\\0 & 1\end{bmatrix}, \begin{bmatrix}31 & 31\\2 & 1\end{bmatrix}$	genus 3, rank 3
$-\frac{3\cdot 18249920^3}{17^{16}}$ $-\frac{7\cdot 1723187806080^3}{79^{16}}$	16	$\begin{bmatrix}4 & 7\\15 & 12\end{bmatrix}, \begin{bmatrix}7 & 14\\7 & 9\end{bmatrix}, \begin{bmatrix}2 & 1\\11 & 9\end{bmatrix}$	$g(X_{ns}(16)) = 2$ rank 2

Subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$



Sporadic points on X_H, $H \subset \mathrm{GL}_2(\mathbb{Z}_\ell), \ell > 2$

Rouse–Sutherland–Zureick-Brown, in progress

- Probably no sporadic rational points for $\ell = 3$.
- Some sporadic points for $\ell = 5$.
- Still working on the bookkeeping for $\ell = 7, 11$.

See Jeremy Rouse's CNTA talk, linked here

Bourdon–Gill–Rouse–Watson, 2020

(Application) Classification of all odd degree isolated points on $X_1(N)$ with rational j-invariant:

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

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.

(Morrow) $H_1 \times H_2 \subset \mathrm{GL}_2(\mathbb{Z}/2^m\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

$$\emptyset$$

Camacho-Navarro–Li–Morrow–Petok–Zureick-Brown

$H_1 \times H_2 \subset \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/q^n\mathbb{Z})$ (Genus 1)

$3B^0-3a$	$4A^0-4a$	109503/64, -35937/4
$3B^0-3a$	$4D^0-4a$	-35937/4, 109503/64
$3B^0-3a$	$5A^0-5a$	-316368, 432
$3B^0-3a$	$5B^0-5a$	-25/2, -349938025/8, -121945/32, 46969655/32768
$3B^0-3a$	$7B^0-7a$	3375/2, -189613868625/128 -140625/8, -1159088625/2097152
$3C^0-3a$	$4A^0-4a$	3375/64
$3C^0-3a$	$5B^0-5a$	1331/8, -1680914269/32768
$4A^0-4a$	$5B^0-5a$	-1723025/4, 1026895/1024

Camacho-Navarro–Li–Morrow–Petok–Zureick-Brown

$H_1 \times H_2 \subset \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/q^n\mathbb{Z})$ (Genus ≥ 2)

label 1	label 2	sporadic j-invariants
4A0-4a	7B0-7a	$-38575685889/16384$, $351/4$
4D0-4a	5A0-5a	-36, $-64278657/1024$
5B0-5a	9A0-9a	-23788477376, 64.
5E0-5a	2A0-8a	-5000
4A0-4a	5E0-5a	(genus 3)

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

d \ N	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		∞																												

ICERM project: higher degree sporadic points on $X_0(N)$

Bilgin, Giusti, Korde, Manes, Morrison, Sankar, Triantafillou, Viray, Zureick-Brown

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

Formal immersions

Previous work

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

Main technique

- If N is large, then there are no elliptic curves mod small $\ell \nmid 2N$ with an N torsion point (e.g., by the Hasse bound).
- Thus a non cuspidal point of $X_1(N)$ reduces mod ℓ to a cusp.
- Fiddle with conditions on ℓ, N so that the formal immersion criterion works. (E.g., need to worry about cusps splitting.)

Put table from our paper here

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. $\operatorname{rank} J_1(2, 2N)(\mathbb{Q})$ *if and only if* $N \in S_1$.

The Mordell–Weil Sieve

For a finite set S of primes of good reduction, we have the following commutative diagram.

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

Compare the images of α and β.

Thanks!

Thank you!