Progress on Mazur's program B, Part III: Rational Points

David Zureick-Brown

Emory University
Slides available at `http://www.mathcs.emory.edu/~dzb/slides/`

Torsion groups and Galois representations of elliptic curves
Zagreb, Croatia

June 25, 2018

$$\rho_{E,n} \colon G_{\mathbb{Q}} \twoheadrightarrow H(n) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$G_{\mathbb{Q}} \left\{ \begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \left. \begin{array}{c} \overline{\mathbb{Q}}^{\ker \rho_{E,n}} = \mathbb{Q}(E[n]) \\ | \\ \mathbb{Q} \end{array} \right\} H(n) \end{array} \right.$$

Problem (Mazur's "program B")

Classify all possibilities for $H(n)$.

Rational Points on modular curves

Mazur's program B

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

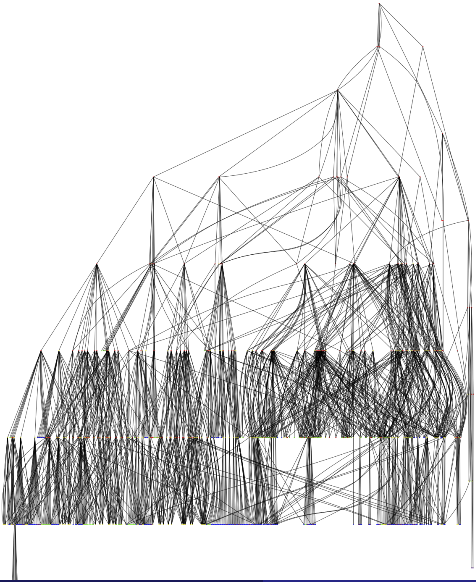
Remark

- 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).

Fact

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

Subgroups of $GL_2(\mathbb{Z}_2)$



Sample subgroup (Serre)

$$\begin{array}{ccccc} \ker\phi_2 & \subset & H(8) & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \\ & & \Big\downarrow{\scriptstyle \phi_2} & & \Big\downarrow \\ I + 2M_2(\mathbb{Z}/2\mathbb{Z}) & \subset & H(4) & = & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \\ & & \Big\downarrow{\scriptstyle \phi_1} & & \Big\downarrow \\ & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \end{array}$$

$\dim_{\mathbb{F}_2} \ker\phi_2 = 3$

$\dim_{\mathbb{F}_2} \ker\phi_1 = 4$

$$\chi\colon\ \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{F}_2^3.$$

$\chi = \mathrm{sgn} \times \det$

$H(8) := \chi^{-1}(G),\ G \subset \mathbb{F}_2^3.$

Sample subgroup (Dokchitser^2)

$$\begin{array}{ccccccc} \langle I + 2E_{1,1}, I + 2E_{2,2}\rangle & \subset & H(4) & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \\ & & \downarrow & & \downarrow \\ & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \end{array}$$

$\dim_{\mathbb{F}_2} \ker \phi_1 = 2$

$$H(2) = \left\langle \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \cong \mathbb{F}_3 \rtimes D_8.$$

$$\operatorname{im} \rho_{E,4} \subset H(4) \Leftrightarrow j(E) = -4t^3(t+8).$$

$$X_H \cong \mathbb{P}^1 \xrightarrow{j} X(1).$$

A typical subgroup

$$
\begin{tikzcd}
\ker \phi_4 & \subset & H(32) \arrow[d, "\phi_4"] & \subset & \mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z}) \arrow[d] & & \dim_{\mathbb{F}_2} \ker \phi_4 = 4 \\
\ker \phi_3 & \subset & H(16) \arrow[d, "\phi_3"] & \subset & \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}) \arrow[d] & & \dim_{\mathbb{F}_2} \ker \phi_3 = 3 \\
\ker \phi_2 & \subset & H(8) \arrow[d, "\phi_2"] & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \arrow[d] & & \dim_{\mathbb{F}_2} \ker \phi_2 = 2 \\
\ker \phi_1 & \subset & H(4) \arrow[d, "\phi_1"] & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \arrow[d] & & \dim_{\mathbb{F}_2} \ker \phi_1 = 3 \\
 & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) & &
\end{tikzcd}
$$

Non-abelian entanglements

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

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

$$\operatorname{im} \rho_{E,6} \subset H(6) \Leftrightarrow K(E[2]) \subset K(E[3])$$

Main conjecture

Conjecture (Serre)

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 37$, $\rho_{E,\ell}$ is surjective.

Serre's Open Image Theorem

Theorem (Serre, 1972)

Let E be an elliptic curve over K without CM. The image of ρ_E

$$\rho_E(G_K) \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

is open.

Note:

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$$

“Vertical” image conjecture

Conjecture

There exists a constant N such that for every $E/\mathbb{Q}$ without CM

$$\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})\right] \leq N.$$

Remark

This follows from the “$\ell > 37$” conjecture.

Problem

Assume the “$\ell > 37$” conjecture and compute N.

Main Theorems

Rouse, ZB (2-adic)

The index of $\rho_{E,2^\infty}(G_\mathbb{Q})$ divides 64 or 96; all such indices occur.

Zywina (mod ℓ)

Classifies $\rho_{E,\ell}(G_\mathbb{Q})$ (modulo some conjectures).

Zywina (all possible indices; modulo some conjectures)

The **index** of $\rho_{E,N}(G_\mathbb{Q})$ divides $220, 336, 360, 504, 864, 1152, 1200, 1296$ or 1536.

Zywina–Sutherland

Parametrizations in all **prime power** levels, $g = 0$ and $g = 1, r > 0$ cases.

Gonzalez–Jimenez, Lozano–Robledo

Classify $E/\mathbb{Q}$ with $\rho_{E,N}(G_\mathbb{Q})$ abelian.

Main Theorems continued

Morrow (composite level)

Classifies $\rho_{E,2^n\cdot\ell}(G_{\mathbb{Q}})$.

Camacho–Li–Morrow–Petok–ZB (composite level)

Classifies $\rho_{E,\ell_1^n\cdot\ell_2^m}(G_{\mathbb{Q}})$ (partially).

Brau–N. Jones, N. Jones–McMurdy (in progress)

Equations for X_H for entanglement groups H.

Rouse–ZB for other prime powers (in progress)

Partial progress; e.g. for $N = 3^n$.

Derickx–Etropolski–Morrow–van Hoejk–ZB (in progress)

Classify possibilities for cubic torsion.

Some applications and complements

Theorem (R. Jones, Rouse, ZB)

1. **Arithmetic dynamics**: *let* $P \in E(\mathbb{Q})$.
2. *How often is the order of* $\widetilde{P} \in E(\mathbb{F}_p)$ *odd?*
3. *Answer depends on* $\rho_{E,2^\infty}(G_\mathbb{Q})$.
4. *Examples:* $11/21$ *(generic),* $121/168$ *(maximal),* $1/28$ *(minimal)*

Theorem (Various authors)

Computation of $S_\mathbb{Q}(d)$ *and* $S(d)$ *for particular* d.

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

Classification of $E(\mathbb{Q}(3^\infty))_{\text{tors}}$

More applications

Theorem (Sporadic points)

Najman's example $X_1(21)^{(3)}(\mathbb{Q})$; "easy production" of other examples.

Theorem (Jack Thorne)

Elliptic curves over $\mathbb{Q}_\infty$ are modular.
(One step is to show $X_0(15)(\mathbb{Q}_\infty) = X_0(15)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.)

Theorem (Zywina)

Constants in the Lang–Trotter conjecture.

Cremona Database, 2-adic images

Index, # **of isogeny classes**

1 , 727995

2 , 7281

3 , 175042

4 , 1769

6 , 57500

8 , 577

12 , 29900

16 , 235

24 , 5482

32 , 20

48 , 1544

64 , 0 (two examples)

96 , 241 (first example - $X_0(15)$)

CM , 1613

Cremona Database

Index, $\#$ **of isogeny classes**

64 , 0

$j = -3 \cdot 2^{18} \cdot 5 \cdot 13^3 \cdot 41^3 \cdot 107^3 \cdot 17^{-16}$

$j = -2^{21} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13^3 \cdot 23^3 \cdot 41^3 \cdot 179^3 \cdot 409^3 \cdot 79^{-16}$

Rational points on $X_{ns}^{+}(16)$ (Heegner, Baran)

Fun 2-adic facts

1. All indices dividing 96 occur infinitely often; 64 occurs only twice.
2. The 2-adic image is determined by the mod 32 image
3. 1208 different images can occur for non-CM elliptic curves
4. There are 8 “sporadic” subgroups.

More fun 2-adic facts

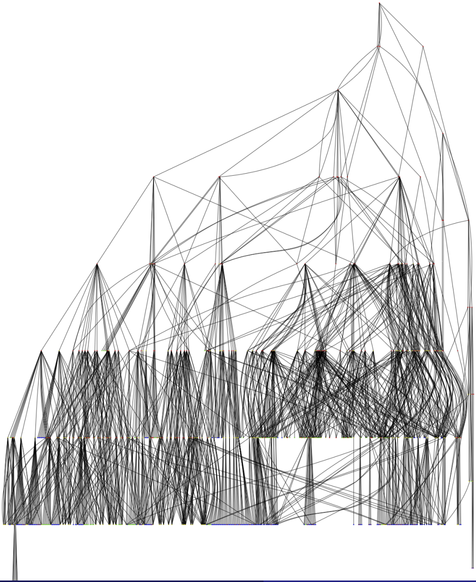
If $E/\mathbb{Q}$ is a non-CM elliptic curve whose mod 2 image has index

- 1, the 2-adic image can have index as large as 64.
- 2, the 2-adic image has index 2 or 4.
- 3, the 2-adic image can have index as large as 96.
- 6, the 2-adic image can have index as large as 96;
- (although some quadratic twist of E must have 2-adic image with index less than 96).

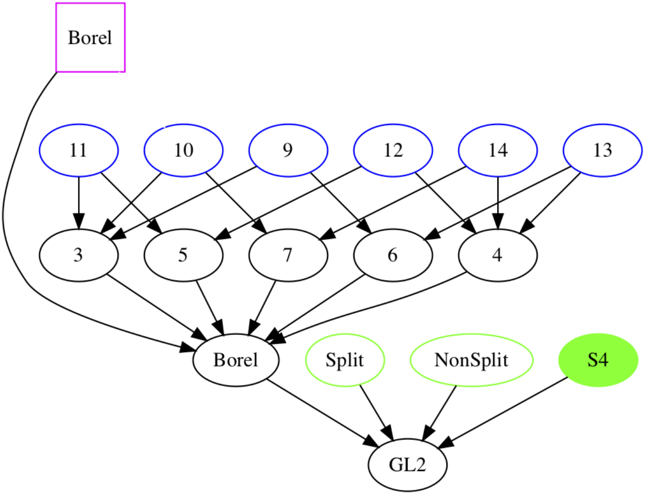
Template

1. Compute all arithmetically minimal $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$
2. Compute equations for each X_H
3. Find (with proof) all rational points on each X_H.

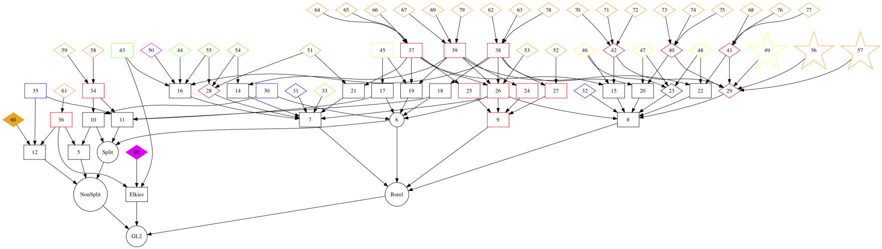
Subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$



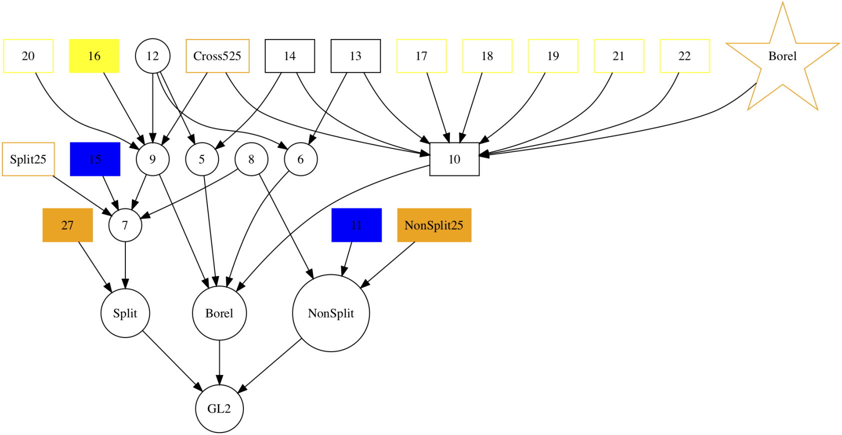
Subgroups of $\mathrm{GL}_2(\mathbb{Z}_{13})$



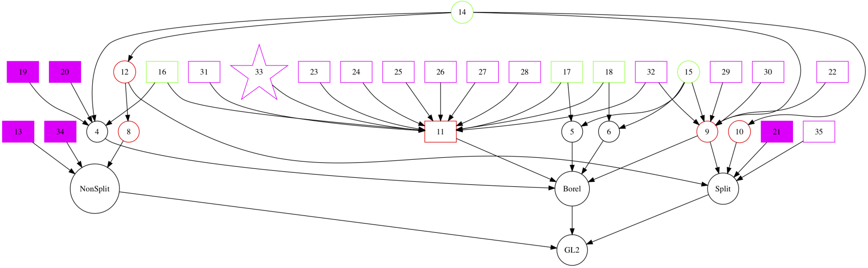
Subgroups of $GL_2(\mathbb{Z}_3)$



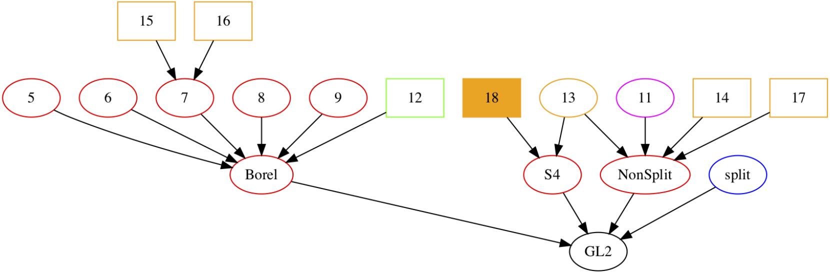
Subgroups of $GL_2(\mathbb{Z}_5)$



Subgroups of $GL_2(\mathbb{Z}_7)$



Subgroups of $GL_2(\mathbb{Z}_{11})$



Numerics, $\ell = 2$

318 curves X_H with $-I \in H$ (excluding pointless conics)

Genus	0	1	2	3	5	7
Number	175	52	57	18	20	4

Rational points rundown, $\ell = 2$

318 curves (excluding pointless conics)

Genus	0	1	2	3	5	7
Number	175	52	56	18	20	4
Rank of Jacobian						
0		25	46	–	–	??
1		27	3	9	10	??
2			7	–	–	??
3				9	–	??
4					–	??
5					10	??

More 2-adic facts

1. There are 8 "sporadic" subgroups
   1. Only one genus 2 curve has a sporadic point
   2. Six genus 3 curves each have a single sporadic point
   3. The genus 1, 5, and 7 curves have no sporadic points
2. Many accidental isomorphisms of $X_H \cong X_{H'}$.
3. There is one H such that $g(X_H) = 1$ and $X_H \in X_H(\mathbb{Q})$.

Rational Points rundown: $\ell = 3$

3	$g = 0$	Handled by Sutherland–Zywina
	$g = 1$	all rank zero
	$g = 4$	map to g = 1
	$g = 2$	Chabauty works
	$g = 4$	no 3-adic points
	$g = 3$	Picard curves; map to rank 0 AV
	$g = 4$	Admits étale triple cover
	$g = 6$	Admits étale triple cover
	$g = 12$	gonality ≤ 9, plane model, degree 121
	$g = 43$	New ideas needed

Rational Points rundown: $\ell = 5$

5	$g = 0$ (10 level 5, 3 level 25)	All level 5 curves are genus 0
	$g = 4$ (4 level 25)	No 5-adic points
	$g = 8, 22$	known (e.g., $X_{\text{ns}}(25)$)
	$g = 2$ (2 level 25)	Rank 2, A_5 mod 2 image
	$g = 4$ (3 level 25)	All isomorphic.
		Each has 5 rational points
		Each admits an order 5 aut
		Simple Jacobian
	$g = 14, 36$ (levels 25 and 125)	No models (or ideas, yet)

Rational Points rundown: $\ell = 7$

7	$g = 1, 3$	[Z, 4.4] handles these, $X_H(\mathbb{Q})$ is finite.
	$g = 19, 26$, level 49	Maps to one of the 6 above
	$g = 1$, level 49	[SZ] handles this one (rank 0)
	$g = 3, 19, 26$, level 49, 343	Map to curve on previous line
	$g = 12$, level 49	Handled by Greenberg–Rubin–Silverberg–Stoll
	$g = 94$	Known ($X_{\mathrm{ns}}(49)$)
	$g = 9, 12, 69$	No models (or ideas, yet)

Rational Points rundown: $\ell = 11$

11	all maximal are genus one	
	only positive rank is $X_{ns}(11)$	
	All but one are ruled out by Zywina	some have sporadic points;
		[Z, Theorem 1.6]
	$g = 5$, level 11	[Z, Lemma 4.5]
	$g = 5776$, level 121	"Challenge..."

Rational Points rundown: $\ell = 13$

Zywina handles all level 13 except for the cursed curve

13	$g = 2, 3$, level 13 (8 total)	
	$g = 8$, level 169	$X_0(13^2)$, handled by Kenku
	$X_{ns}(13)$	Cursed. Genus 3, rank 3. No torsion. Some points Probably has maximal mod 2 image Solved by Balakrishnan, Müller
	$X_{S_4}(13)$	Also cursed.

Rational Points: summary of remaining work.

3	$g = 12, 43$
5	$g = 2, 4, 14, 36$
7	$g = 9, 12, 69$
11	a single genus 5776 curve remains
13	$X_{S_4}(13)$

Explicit methods: highlight reel

- Local methods
- Chabauty
- Elliptic Chabauty
- Mordell–Weil sieve
- étale descent
- Pryms
- **Equationless descent via group theory.**
- **New techniques for computing** $\operatorname{Aut} C$.

Pryms (via Nils Bruin)

$$
\begin{tikzcd}
D \arrow[r, "\iota - \mathrm{id} - (\iota(P) - P)"] \arrow[d, "\mathrm{et}"'] \arrow[loop below, "\iota"] & \ker_0(J_D \to J_C) =: \mathrm{Prym}(D \to C) \\
C &
\end{tikzcd}
$$

$$C(\mathbb{Q}) = \bigcup_{\delta \in \{\pm 1, \pm 2\}} \operatorname{im} D_\delta(\mathbb{Q})$$

Pryms

$$\begin{tikzcd} D \arrow[r, "\iota - \mathrm{id} - (\iota(P) - P)"] \arrow[d, "\mathrm{et}"'] \arrow[loop below, "\iota"] & \ker_0(J_D \to J_C) =: \mathrm{Prym}(D \to C) \\ C \end{tikzcd}$$

Example (Genus $C = 3 \Rightarrow$ Genus $D = 5$)

- $C\colon Q(x, y, z) = 0$
- $Q = Q_1 Q_3 - Q_2^2$.

$$\begin{aligned} D_\delta\colon\ Q_1(x, y, z) &= \delta u^2 \\ Q_2(x, y, z) &= \delta uv \\ Q_3(x, y, z) &= \delta v^2 \end{aligned}$$

- $\mathrm{Prym}(D_\delta \to C) \cong \mathrm{Jac}_{H_\delta}$,
- $H_\delta\colon y^2 = -\delta \det(M_1 + 2xM_2 + x^2 M_3)$.

Thanks

Thank you!