Progress on Mazur's program B

David Zureick-Brown

Emory University

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

JMM Special Session on Number Theory, Arithmetic Geometry, and Computation

January 19, 2019

Theorem 1 also fits into a general program:

B. Given a number field K and a subgroup H of $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\bar{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

Mazur - Rational points on modular curves (1977)

Background - Image of Galois

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

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

Problem (Mazur's "program B")

Classify all possibilities for $H(n)$.

Example - torsion on an ellitpic 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 $E(\overline{K})[n] \cong \langle P, Q \rangle$,

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

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 $E(\overline{K})[n] \cong \langle P, Q \rangle$,

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

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.

Modular curves

Definition

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

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 $-I \in H$.

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

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

Sample subgroup (Serre)

$$\begin{array}{ccccccc} \ker\phi_2 & \subset & H(8) & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_2 = 3 \\ & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\ I + 2M_2(\mathbb{Z}/2\mathbb{Z}) & \subset & H(4) & = & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) & & \dim_{\mathbb{F}_2}\ker\phi_1 = 4 \\ & & \downarrow{\scriptstyle \phi_1} & & \downarrow & & \\ & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) & & \end{array}$$

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

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

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

A typical subgroup

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

Non-abelian entanglements

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

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

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

Main conjecture

Conjecture (Serre)

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

In other words, conjecturally, $H(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell > 37$.

"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.

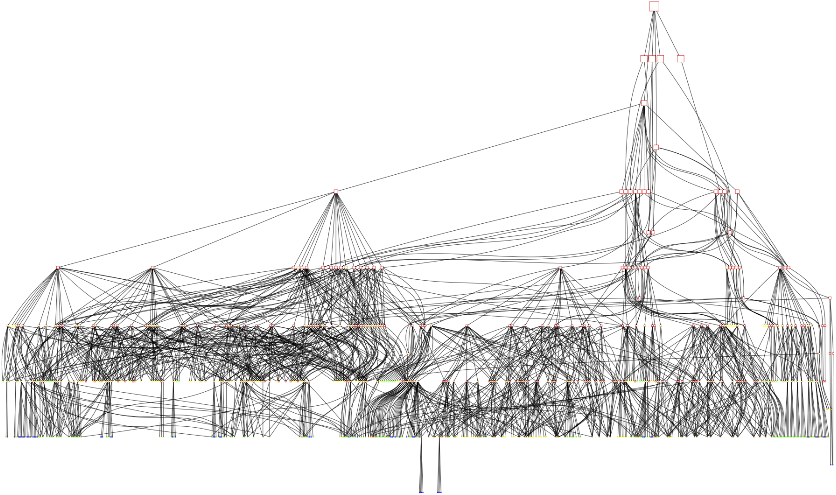
Main Theorem

Rouse, ZB (2-adic)

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

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.

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



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

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

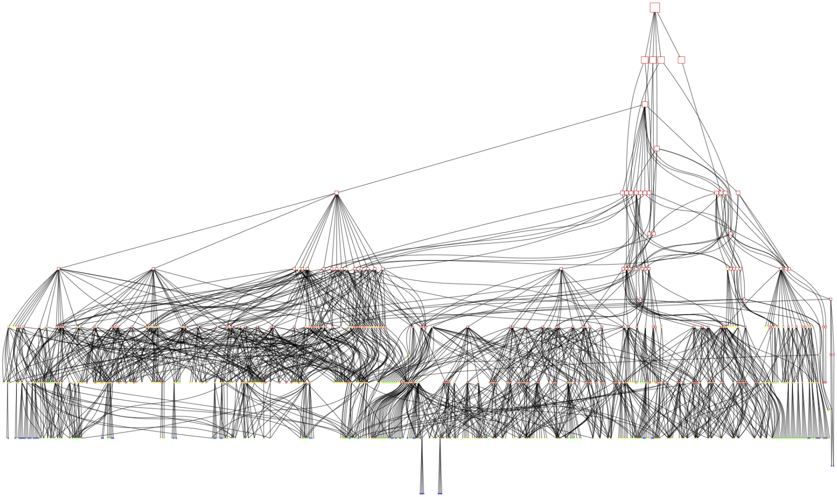
$j = -2^{21} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13^3 \cdot 23^3 \cdot 41^3 \cdot 179^3 \cdot 409^3 \cdot 79^{-16}$

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

Proof 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 $GL_2(\mathbb{Z}_2)$



Finding Equations – Basic idea

1. The canoncial map $C \hookrightarrow \mathbb{P}^{g-1}$ is given by $P \mapsto [\omega_1(P) : \cdots : \omega_g(P)]$.
2. For a general curve, this is an embedding, and the relations are quadratic.
3. For a modular curve,

$$M_k(H) \cong H^0(X_H, \Omega^1(\Delta)^{\otimes k/2})$$

given by

$$f(z) \mapsto f(z)\, dz^{\otimes k/2}.$$

Equations – Example: $X_1(17) \subset \mathbb{P}^4$

$$
\begin{aligned}
q - 11q^5 + 10q^7 + O(q^8) \\
q^2 - 7q^5 + 6q^7 + O(q^8) \\
q^3 - 4q^5 + 2q^7 + O(q^8) \\
q^4 - 2q^5 + O(q^8) \\
q^6 - 3q^7 + O(q^8)
\end{aligned}
$$

$$
\begin{aligned}
xu + 2xv - yz + yu - 3yv + z^2 - 4zu + 2u^2 + v^2 = 0 \\
xu + xv - yz + yu - 2yv + z^2 - 3zu + 2uv = 0 \\
2xz - 3xu + xv - 2y^2 + 3yz + 7yu - 4yv - 5z^2 - 3zu + 4zv = 0
\end{aligned}
$$

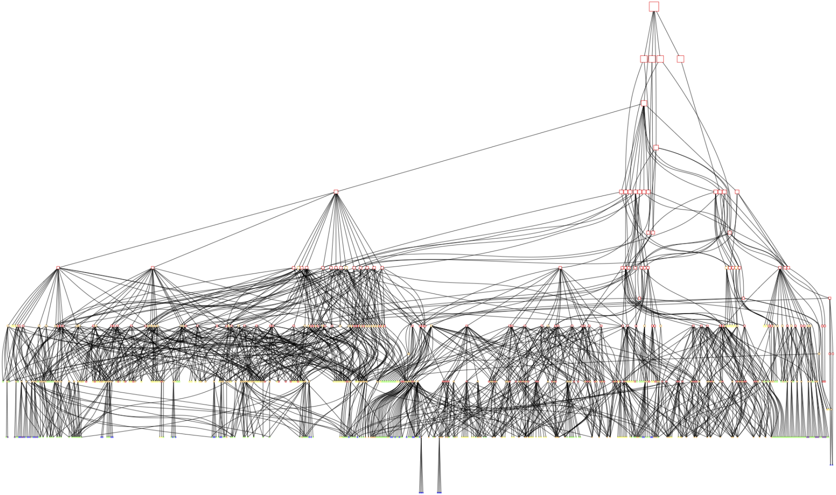
Equations – general

1. $H' \subset H$ of index 2, $X_{H'} \to X_H$ degree 2.
2. Given equations for X_H, compute equations for $X_{H'}$.
3. Compute a new modular form on H', compute (quadratic) relations between this and modular forms on H.
4. **Main technique** – if $X_{H'}$ has "new cusps", then write down Eisenstein series which vanish at "one new cusp, not others".

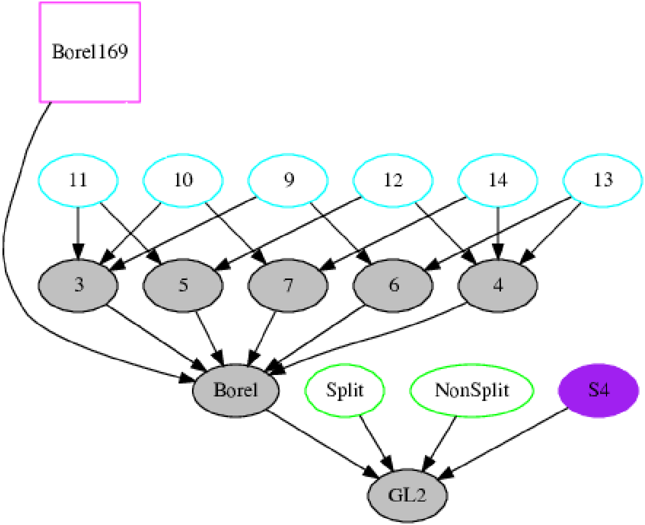
More 2-adic facts

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 $X_H \in X_H(\mathbb{Q})$.

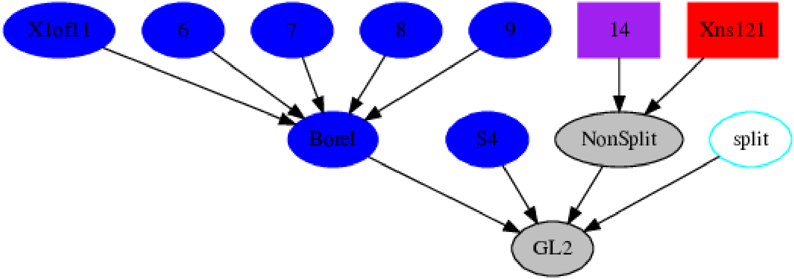
Subgroups of $GL_2(\mathbb{Z}_2)$



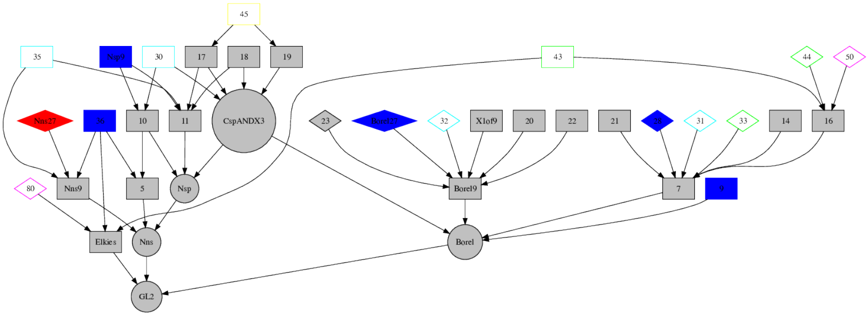
Subgroups of $GL_2(\mathbb{Z}_{13})$



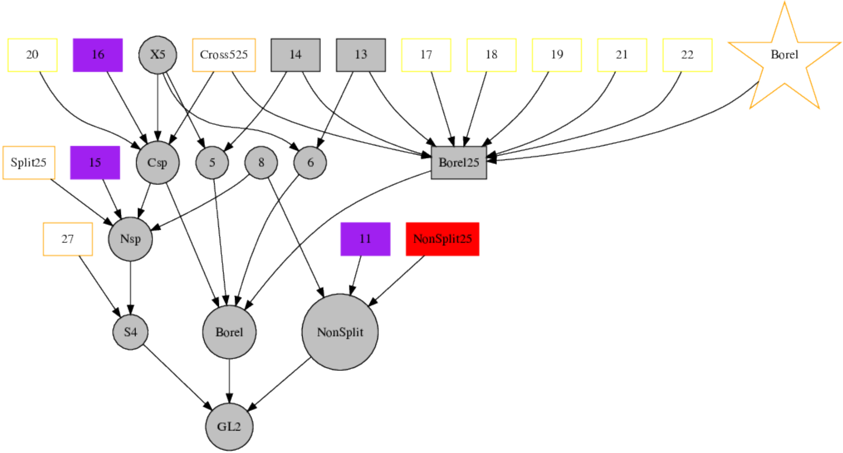
Subgroups of $GL_2(\mathbb{Z}_{11})$



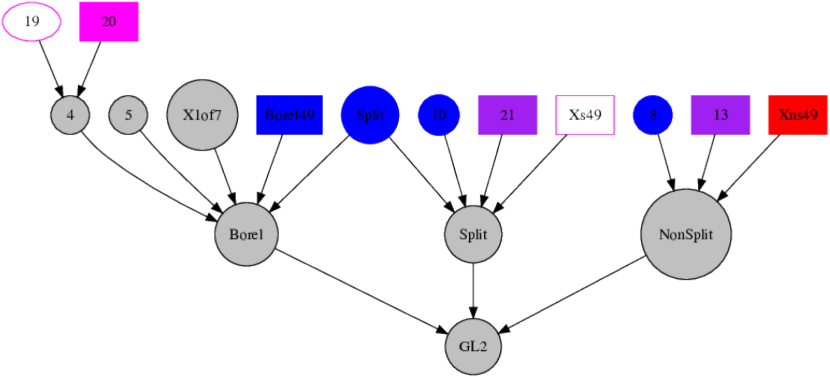
Subgroups of $GL_2(\mathbb{Z}_3)$



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



Subgroups of $\mathrm{GL}_2(\mathbb{Z}_7)$



Rational Points: summary of remaining work.

3	$g = 12$
5	$g = 2, 4, 14$
7	$g = 9, 12, 69$
11	$g = 41, 511$
13	$X_{S_4}(13)$ (genus 3)

Rational Points: summary of remaining work – more info.

The Untouchables	$X_{ns}^{+}(27), X_{ns}^{+}(25), X_{ns}^{+}(49), X_{ns}^{+}(121)$ $g = 12, 14, 69, 511$
Also probably untouchable ($r \geq g$)	X_{13}, X_{21}, X_{14} $g = 9, 9, 41$ level 7, 7, 11
Cautiously optimistic ($r \geq g$)	X_{11}, X_{15}, X_{16}, X_{S_4} $g = 2, 2, 4, 3$ level 5, 5, 5, 13
Optimistic ($r = 3 < g$)	$g = 12$, level 7

Explicit methods: highlight reel

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

Thanks

Thank you!