

# $\ell$ -adic images of Galois for elliptic curves over $\mathbb{Q}$

David Zureick-Brown (Amherst College)  
Jeremy Rouse (Wake Forest University)  
Drew Sutherland (MIT)

Western university algebra seminar

April 17, 2026

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

# Galois Representations

$$\begin{aligned}\mathbb{Q} &\subset K \subset \overline{\mathbb{Q}} \\ G_K &:= \text{Aut}(\overline{K}/K) \\ E[n](\overline{K}) &\cong (\mathbb{Z}/n\mathbb{Z})^2\end{aligned}$$

$$\begin{aligned}\rho_{E,n}: G_K &\rightarrow \text{Aut } E[n] \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \rho_{E,\ell^\infty}: G_K &\rightarrow \text{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \rho_E: G_K &\rightarrow \text{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim_n \text{GL}_2(\mathbb{Z}/n\mathbb{Z})\end{aligned}$$

# Serre's Open Image Theorem

## Theorem (Serre, 1972)

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

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

of  $\rho_E$  is open.

## Note:

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_{\ell})$$

Thus  $\rho_{E,\ell^\infty}$  is surjective for all but finitely many  $\ell$ .

For CM curves, see Lozano-Robledo's [paper](#) and work by Bourdon, Clark, and Pollack.

# Image of Galois

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

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

Problem (Mazur's "program B")

*Classify all possibilities for  $H(n)$ .*

# Mazur's Program B

As presented at Modular functions in one variable V in Bonn

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  $\text{Gal}(\bar{K}/K)$  into  $H \subset GL_2 \hat{\mathbb{Z}}$ .

Mazur - Rational points on modular curves (1977)

## 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  $Q \in E(\bar{K})[n]$  such that  $E(\bar{K})[n] \cong \langle P, Q \rangle$ ,

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

## Example - Isogenies

If  $E$  has a  $K$ -rational, **cyclic isogeny**  $\phi: E \rightarrow E'$  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:

$$N_{\text{sp}} = \left\langle \left( \begin{array}{cc} * & 0 \\ 0 & * \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right) \right\rangle$$

### $H(n) \subset N_{\text{sp}}$ and $H(n) \not\subset C_{\text{sp}}$ 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

$\mathbb{F}_{p^2}^*$  acts on  $\mathbb{F}_{p^2} \cong \mathbb{F}_p \times \mathbb{F}_p$

### Normalizer of a non-split Cartan:

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

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

$E$  admits a “necklace” (Rebolledo, Wuthrich)

# Image of Galois

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

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

Problem (Mazur's "program B")

*Classify all possibilities for  $H(n)$ .*

# Modular curves

## Definition

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

Let  $\Gamma(N) \subset H \subset \text{GL}_2(\widehat{\mathbb{Z}})$ . The minimal such  $N$  is the **level** of  $H$ .

## Definition

$X_H := X(N)/H(N)$  (where  $H(N)$  is the image of  $H$  in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ )

$X_H(K) \ni (E/K, \iota) \Leftrightarrow \rho_{E,N}(G_K) \subset H(N)$

## 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 **exceptional** points (i.e, non-cusp non-CM points).
- Can compute  $g(X_H)$  group theoretically (via Riemann–Hurwitz).

## Fact

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

# (Serre) Sample subgroup $H \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$

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

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

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

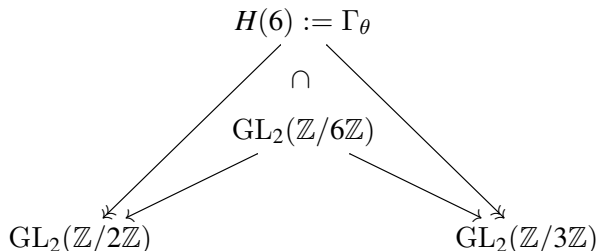
$$H(8) := \chi^{-1}(G), \quad G \subset \mathbb{F}_2^3.$$

# A typical subgroup $H \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$

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

## Non-abelian entanglements

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



## Brau–Jones

$$\mathrm{im} \rho_{E,6} \subset H(6) \Leftrightarrow j(E) = 2^{10}3^3t^3(1 - 4t^3) \Rightarrow K(E[2]) \subset K(E[3])$$

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

# 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,  $\rho_{E,\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$  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  $N$ .*

# Labeling subgroups of $GL_2(\widehat{\mathbb{Z}})$ up to conjugacy

## Definition

When  $\det(H) = \widehat{\mathbb{Z}}^\times$  these labels have the form  $N.i.g.n$ , where  $N$  is the level,  $i$  is the index,  $g$  is the genus, and  $n$  is a tiebreaker given by ordering the subgroups of  $GL_2(N)$ .

## Example

- The Borel subgroup  $B(13)$  has label  $13.14.0.1$ .
- The normalizer of the split Cartan  $N_{\text{sp}}(13)$  has label  $13.91.3.1$ .
- The normalizer of the nonsplit Cartan  $N_{\text{ns}}(13)$  has label  $13.78.3.1$ .
- The maximal  $S_4$  exceptional group  $S_4(13)$  has label  $13.91.3.2$ .

# Obligatory XKCD cartoon

## HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:  
THERE ARE  
14 COMPETING  
STANDARDS.

14?! RIDICULOUS!  
WE NEED TO DEVELOP  
ONE UNIVERSAL STANDARD  
THAT COVERS EVERYONE'S  
USE CASES.



SOON:

SITUATION:  
THERE ARE  
15 COMPETING  
STANDARDS.

# Obligatory XKCD cartoon

## HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:

~~14~~ THERE ARE  
COMPETING  
STANDARDS.

15

14?! RIDICULOUS!  
WE NEED TO DEVELOP  
ONE UNIVERSAL STANDARD  
THAT COVERS EVERYONE'S  
USE CASES.



~~SOON:~~

yesterday

SITUATION:

~~15~~ THERE ARE  
COMPETING  
STANDARDS.

16

# Main Theorem

## Definition

A point  $(E, \iota) \in X_H(K)$  is **exceptional** if  $X_H(K)$  is finite and  $\text{End } E = \mathbb{Z}$ .

## Theorem (Rouse–Sutherland–ZB 2021)

Let  $\ell$  prime,  $E/\mathbb{Q}$  be a non-CM elliptic curve, and  $H = \rho_{E, \ell^\infty}(G_{\mathbb{Q}})$ .

Then exactly one of the following is true:

- 1  $X_H(\mathbb{Q})$  is infinite and  $H$  is listed in (Sutherland–Zywina 2017);
- 2  $X_H$  has a rational exceptional point listed in Table 1;
- 3  $H \leq N_{\text{ns}}(3^3), N_{\text{ns}}(5^2), N_{\text{ns}}(7^2), N_{\text{ns}}(11^2)$ , or  $N_{\text{ns}}(\ell)$  for some  $\ell > 13$ ;
- 4  $H$  is a subgroup of  $49.179.9.1$  or  $49.196.9.1$ .

We conjecture that cases (3) and (4) never occur.

If they do, the exceptional points have **extraordinarily** large heights (e.g.  $10^{10^{200}}$  for  $X_{\text{ns}}^+(11^2)(\mathbb{Q})$ ).

label	level	notes	$j$ -invariants/models of exceptional points
16.64.2.1	2 <sup>4</sup>	$N_{\text{ns}}(16)$	$-2^{18} \cdot 3 \cdot 5^3 \cdot 13^3 \cdot 41^3 \cdot 107^3 / 17^{16}$ $-2^{21} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13^3 \cdot 23^3 \cdot 41^3 \cdot 179^3 \cdot 409^3 / 79^{16}$
16.96.3.335	2 <sup>4</sup>	$H(4) \subsetneq N_{\text{sp}}(4)$	$257^3 / 2^8$
16.96.3.343	2 <sup>4</sup>	$H(4) \subsetneq N_{\text{sp}}(4)$	$17^3 \cdot 241^3 / 2^4$
16.96.3.346	2 <sup>4</sup>	$H(4) \subsetneq N_{\text{sp}}(4)$	$2^4 \cdot 17^3$
16.96.3.338	2 <sup>4</sup>	$H(4) \subsetneq N_{\text{sp}}(4)$	$2^{11}$
32.96.3.230	2 <sup>5</sup>	$H(4) \subsetneq N_{\text{sp}}(4)$	$-3^3 \cdot 5^3 \cdot 47^3 \cdot 1217^3 / (2^8 \cdot 31^8)$
32.96.3.82	2 <sup>5</sup>	$H(8) \subsetneq N_{\text{sp}}(8)$	$3^3 \cdot 5^6 \cdot 13^3 \cdot 23^3 \cdot 41^3 / (2^{16} \cdot 31^4)$
25.50.2.1	5 <sup>2</sup>	$H(5) = N_{\text{ns}}(5)$	$2^4 \cdot 3^2 \cdot 5^7 \cdot 23^3$
25.75.2.1	5 <sup>2</sup>	$H(5) = N_{\text{sp}}(5)$	$2^{12} \cdot 3^3 \cdot 5^7 \cdot 29^3 / 7^5$
7.56.1.2	7	$\subsetneq N_{\text{ns}}(7)$	$3^3 \cdot 5 \cdot 7^5 / 2^7$
7.112.1.2	7	$-I \notin H$	$y^2 + xy + y = x^3 - x^2 - 2680x - 50053$ $y^2 + xy + y = x^3 - x^2 - 131305x + 17430697$
11.60.1.3	11	$\subsetneq B(11)$	$-11 \cdot 131^3$
11.120.1.8	11	$-I \notin H$	$y^2 + xy + y = x^3 + x^2 - 30x - 76$
11.120.1.9	11	$-I \notin H$	$y^2 + xy = x^3 + x^2 - 2x - 7$
11.60.1.4	11	$\subsetneq B(11)$	$-11^2$
11.120.1.3	11	$-I \notin H$	$y^2 + xy = x^3 + x^2 - 3632x + 82757$
11.120.1.4	11	$-I \notin H$	$y^2 + xy + y = x^3 + x^2 - 305x + 7888$
13.91.3.2	13	$S_4(13)$	$2^4 \cdot 5 \cdot 13^4 \cdot 17^3 / 3^{13}, -2^{12} \cdot 5^3 \cdot 11 \cdot 13^4 / 3^{13}$ $2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929 / (5^{13} \cdot 61^{13})$
17.72.1.2	17	$\subsetneq B(17)$	$-17 \cdot 373^3 / 2^{17}$
17.72.1.4	17	$\subsetneq B(17)$	$-17^2 \cdot 101^3 / 2$
37.114.4.1	37	$\subsetneq B(37)$	$-7 \cdot 11^3$
37.114.4.2	37	$\subsetneq B(37)$	$-7 \cdot 137^3 \cdot 2083^3$

Table 1. All known exceptional groups,  $j$ -invariants, and points of prime power level.

U N S O L V E D  
*mysteries*

Arithmetically maximal level  $\ell^n$  groups with  $\ell \leq 13$  with  $X_H(\mathbb{Q})$  **unknown**.

label	level	group	genus
27.243.12.1	$3^3$	$N_{\text{ns}}(3^3)$	12
25.250.14.1	$5^2$	$N_{\text{ns}}(5^2)$	14
49.1029.69.1	$7^2$	$N_{\text{ns}}(7^2)$	69
49.147.9.1	$7^2$	$\langle \left( \begin{smallmatrix} 16 & 6 \\ 20 & 45 \end{smallmatrix} \right), \left( \begin{smallmatrix} 20 & 17 \\ 40 & 36 \end{smallmatrix} \right) \rangle$	9
49.196.9.1	$7^2$	$\langle \left( \begin{smallmatrix} 42 & 3 \\ 16 & 31 \end{smallmatrix} \right), \left( \begin{smallmatrix} 16 & 23 \\ 8 & 47 \end{smallmatrix} \right) \rangle$	9
121.6655.511.1	$11^2$	$N_{\text{ns}}(11^2)$	511

Each has **rank = genus**, **rational CM points**, **no rational cusps**, and **no known exceptional points**.

U N S O L V E D  
*mysteries*

Arithmetically maximal level  $\ell^n$  groups with  $\ell \leq 13$  with  $X_H(\mathbb{Q})$  **unknown**.

label	level	group	genus
<del>27.243.12.1</del> <sup>1</sup>	$3^3$	$N_{\text{ns}}(3^3)$	12
25.250.14.1	$5^2$	$N_{\text{ns}}(5^2)$	14
<del>49.1029.69.1</del> <sup>2</sup>	$7^2$	$N_{\text{ns}}(7^2)$	69
49.147.9.1	$7^2$	$\langle \left( \begin{smallmatrix} 16 & 6 \\ 20 & 45 \end{smallmatrix} \right), \left( \begin{smallmatrix} 20 & 17 \\ 40 & 36 \end{smallmatrix} \right) \rangle$	9
49.196.9.1	$7^2$	$\langle \left( \begin{smallmatrix} 42 & 3 \\ 16 & 31 \end{smallmatrix} \right), \left( \begin{smallmatrix} 16 & 23 \\ 8 & 47 \end{smallmatrix} \right) \rangle$	9
121.6655.511.1	$11^2$	$N_{\text{ns}}(11^2)$	511

Each has **rank = genus**, **rational CM points**, **no rational cusps**, and **no known exceptional points**.

<sup>1</sup><https://arxiv.org/abs/2501.07833>

<sup>2</sup><https://arxiv.org/abs/2507.17967>

## Summary of $\ell$ -adic images of Galois for non-CM $E/\mathbb{Q}$ .

$\ell$	2	3	5*	7*	11*	13	17	37*	other*
subgroups	1208	47	25	17	8	12	3	3	1
exceptional	7	0	2	2	6	1	2	2	0
unexceptional	1201	47	23	15	2	11	1	1	1
max level	32	27	25	7	11	13	17	37	1
max index	96	72	120	112	120	91	72	114	1
max genus	3	0	2	1	1	3	1	4	0

Summary of  $H \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$  which occur as  $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$  for some non-CM  $E/\mathbb{Q}$ .

Starred primes are conjectural.

In particular, we conjecture that there are 1207, 46, 24, 16, 7, 11, 2, 2 proper subgroups of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  that arise as  $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$  for non-CM  $E/\mathbb{Q}$  for  $\ell = 2, 3, 5, 7, 11, 13, 17, 37$  and none for any other  $\ell$ .

# Applications

## Theorem (R. Jones, Rouse, ZB)

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

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

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

## Theorem (Gonzalez-Jimenez, Lozano-Robledo)

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

## Theorem (Rouse–Sutherland–ZB)

Improved algorithms for computing  $\rho_{E,n}(G_{\mathbb{Q}})$ .

# Arithmetically maximal groups

## Definition

We say that an open subgroup  $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$  is **arithmetically maximal** if

- 1  $\det(H) = \widehat{\mathbb{Z}}^\times$  (necessary for  $\mathbb{Q}$ -points),
- 2 a conjugate of  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$  lies in  $H$  (necessary for  $\mathbb{R}$ -points),
- 3  $j(X_H(\mathbb{Q}))$  is finite but  $j(X_{H'}(\mathbb{Q}))$  is infinite for  $H \subsetneq H' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ .

Arithmetically maximal groups  $H$  arise as maximal subgroups of an  $H'$  with  $X_{H'}(\mathbb{Q})$  infinite.

# Arithmetically maximal groups

## Definition

We say that an open subgroup  $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$  is **arithmetically maximal** if

- 1  $\det(H) = \widehat{\mathbb{Z}}^\times$  (necessary for  $\mathbb{Q}$ -points),
- 2 a conjugate of  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$  lies in  $H$  (necessary for  $\mathbb{R}$ -points),
- 3  $j(X_H(\mathbb{Q}))$  is finite but  $j(X_{H'}(\mathbb{Q}))$  is infinite for  $H \subsetneq H' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ .

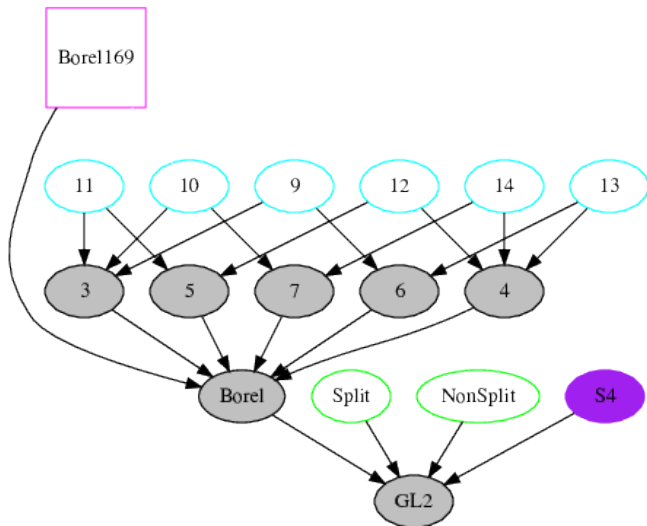
Arithmetically maximal groups  $H$  arise as maximal subgroups of an  $H'$  with  $X_{H'}(\mathbb{Q})$  infinite.

## Theorem (Sutherland–Zywina 2017)

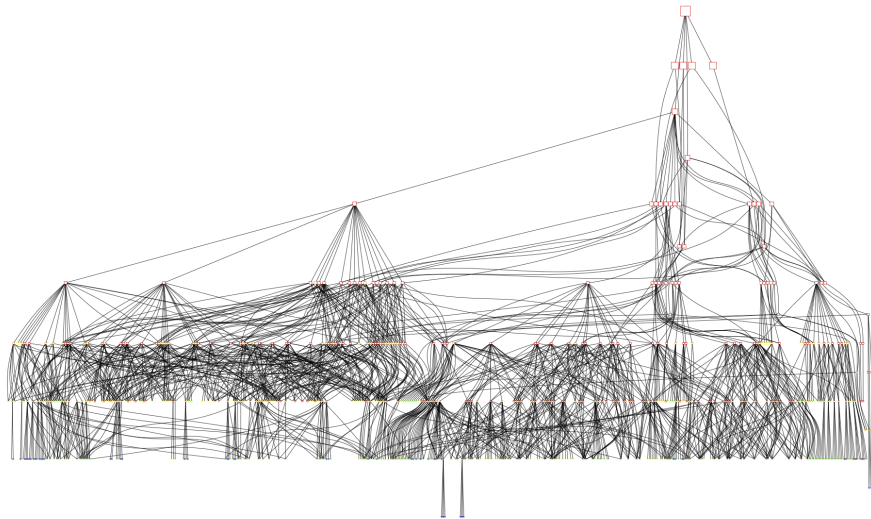
*For  $\ell = 2, 3, 5, 7, 11, 13$  there are 1208, 47, 23, 15, 2, 11 subgroups  $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$  of  $\ell$ -power level with  $X_H(\mathbb{Q})$  infinite, and only  $H = \mathrm{GL}_2(\widehat{\mathbb{Z}})$  for  $\ell > 13$ .*

This allows us to compute explicit upper bounds on the level and index of arithmetically maximal subgroup of prime power level  $\ell$  and we can then exhaustively enumerate them.

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



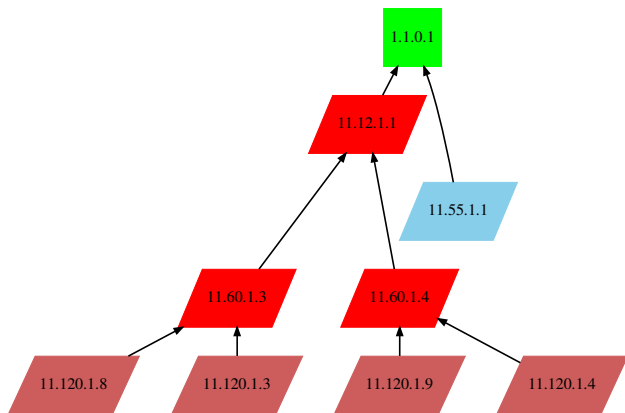
# Subgroups of $GL_2(\mathbb{Z}_2)$



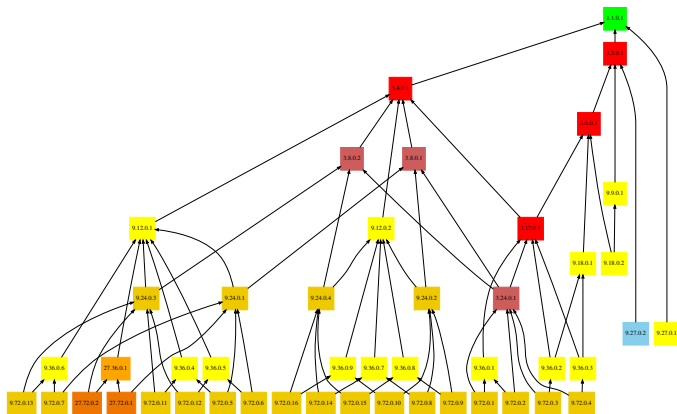
# Steps of the proof

- 1 Compute the set  $\mathcal{S}$  of **arithmetically maximal** subgroups of  $\ell$ -power level for  $\ell \leq 37$  (for all  $\ell > 37$  we already know  $N_{\text{ns}}(\ell)$  is the only possible exceptional group).
- 2 For  $H \in \mathcal{S}$  check for **local obstructions** and compute the **isogeny decomposition** of the Jacobian of  $X_H$  and the analytic ranks of all its simple factors.
- 3 For  $H \in \mathcal{S}$  **compute equations** for  $X_H$  and  $j_H: X_H \rightarrow X(1)$  (if needed). In several cases we can prove  $X_H(\mathbb{Q})$  is empty without a model for  $X_H$ .
- 4 For  $H \in \mathcal{S}$  with  $-I \in H$  **determine the rational points** in  $X_H(\mathbb{Q})$  (if possible). In several cases we are able to exploit recent progress by others ( $\ell = 13$  for example).
- 5 For  $H \in \mathcal{S}$  with  $-I \notin H$  **compute equations** for the universal curve  $\mathcal{E} \rightarrow U$ , where  $U \subseteq X_H$  is the locus with  $j(P) \neq 0, 1728, \infty$ .

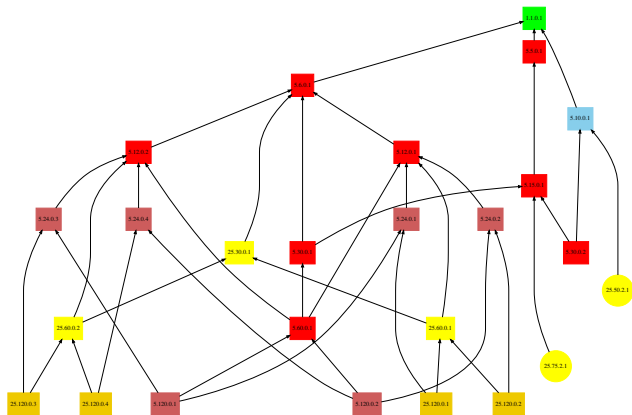
# Subgroups of $GL_2(\mathbb{Z}_{11})$



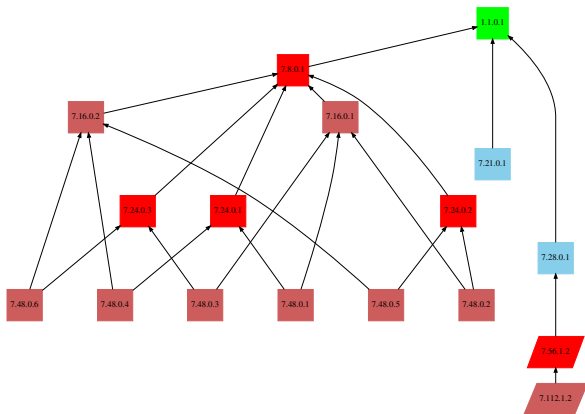
# Subgroups of $GL_2(\mathbb{Z}_3)$



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



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



## Finding Equations for $X_H$ – Basic idea

- 1 The canonical 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: $X_1(17) \subset \mathbb{P}^4$

### Cusp forms

$$q - 11q^5 + 10q^7 + O(q^8)$$

$$q^2 - 7q^5 + 6q^7 + O(q^8)$$

$$q^3 - 4q^5 + 2q^7 + O(q^8)$$

$$q^4 - 2q^5 + O(q^8)$$

$$q^6 - 3q^7 + O(q^8)$$

$$xu + 2xv - yz + yu - 3yv + z^2 - 4zu + 2u^2 + v^2 = 0$$

$$xu + xv - yz + yu - 2yv + z^2 - 3zu + 2uv = 0$$

$$2xz - 3xu + xv - 2y^2 + 3yz + 7yu - 4yv - 5z^2 - 3zu + 4zv = 0$$

# Computing models of modular curves

- We introduce a variety of improvements and tricks to compute models of various  $X_H$ .
- The **LMFDB** often has equations for  $X_H$  and its  $j$ -map.
- See Rouse's [VaNTAGe talk](#) for details and examples.
- We used this method to compute canonical models for many curves of large genus.
- See Assaf's [recent paper](#) and Zywina's [BIRS talk](#) for other efficient approaches.
- A current student of Zywina has recently massively improved all of these algorithms.

## Explicit methods: highlight reel

- Local methods
  - Chabauty and Elliptic Chabauty
  - Mordell–Weil sieve
  - étale descent
  - Pryms
  - *Equationless étale descent via group theory*
  - *New techniques for computing  $\text{Aut } C$*
- 
- *Nonabelian Chabauty*
  - **“Equationless” local methods** and **Mordell–Weil sieve**
  - **Greenberg Transforms** (and big computations)
  - **Novel variants of existing techniques**
  - **Modularity of isogeny factors of  $J_H$**  (w/ Voight)

## Computing $X_H(\mathbb{F}_p)$ “via moduli”

### Enumeration

One can compute  $\#X_1(N)(\mathbb{F}_{p^n})$  by enumerating elliptic curves over  $\mathbb{F}_{p^n}$ , then computing their  $N$  torsion subgroups.

# Computing $X_H(\mathbb{F}_p)$ “via moduli”

## Enumeration

One can compute  $\#X_1(N)(\mathbb{F}_{p^n})$  by enumerating elliptic curves over  $\mathbb{F}_{p^n}$ , then computing their  $N$  torsion subgroups.

## Deligne–Rapoport 1973

The **modular curves**  $X_H$  and  $Y_H$  are coarse spaces for the stacks  $\mathcal{M}_H$  and  $\mathcal{M}_H^0$  that parameterize elliptic curves  $E$  with  **$H$ -level structure**, by which we mean an equivalence class  $[\iota]_H$  of isomorphisms  $\iota: E[N] \rightarrow \mathbb{Z}(N)^2$ , where  $\iota \sim \iota'$  if  $\iota = h \circ \iota'$  for some  $h \in H$ .

See Drew’s [Slides](#) for a nice summary of the implementation.

Arithmetically maximal  $H$  of  $\ell$ -power level for which  
 $X_H(\mathbb{F}_p) = \emptyset$  for some  $p \neq \ell \leq 37$

label	level	generators	$p$	rank	genus
16.48.2.17	$2^4$	$\begin{pmatrix} 11 & 9 \\ 4 & 13 \end{pmatrix}, \begin{pmatrix} 13 & 5 \\ 4 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 12 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 0 & 5 \end{pmatrix}$	3, 11	0	2
27.108.4.5	$3^3$	$\begin{pmatrix} 4 & 25 \\ 6 & 14 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 3 & 1 \end{pmatrix}$	7, 31	0	4
25.150.4.2	$5^2$	$\begin{pmatrix} 7 & 20 \\ 20 & 7 \end{pmatrix}, \begin{pmatrix} 22 & 2 \\ 13 & 22 \end{pmatrix}$	2	0	4
25.150.4.7	$5^2$	$\begin{pmatrix} 24 & 24 \\ 0 & 18 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 0 & 23 \end{pmatrix}$	3, 23	4	4
25.150.4.8	$5^2$	$\begin{pmatrix} 8 & 4 \\ 0 & 23 \end{pmatrix}, \begin{pmatrix} 16 & 7 \\ 0 & 8 \end{pmatrix}$	2	0	4
25.150.4.9	$5^2$	$\begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 3 & 18 \\ 0 & 14 \end{pmatrix}$	2	0	4
49.168.12.1	$7^2$	$\begin{pmatrix} 39 & 6 \\ 36 & 24 \end{pmatrix}, \begin{pmatrix} 11 & 9 \\ 24 & 2 \end{pmatrix}$	2	3	12
13.84.2.2	13	$\begin{pmatrix} 3 & 7 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 12 & 4 \\ 0 & 12 \end{pmatrix}$	2	0	2
13.84.2.3	13	$\begin{pmatrix} 9 & 2 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 0 & 7 \end{pmatrix}$	3	0	2
13.84.2.4	13	$\begin{pmatrix} 8 & 12 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 8 & 3 \\ 0 & 9 \end{pmatrix}$	2	0	2
13.84.2.6	13	$\begin{pmatrix} 9 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 11 & 3 \\ 0 & 10 \end{pmatrix}$	3	0	2

## Decomposing the Jacobian of $X_H$

Let  $H$  be an open subgroup of  $GL_2(\widehat{\mathbb{Z}})$  of level  $N$ .

Let  $J_H$  denote the Jacobian of  $X_H$ .

### Theorem (Rouse–Sutherland–Voight–ZB 2021)

Each **simple factor**  $A$  of  $J_H$  is **isogenous** to  $A_f$  for a weight-2 eigenform  $f$  on  $\Gamma_0(N^2) \cap \Gamma_1(N)$ .

### Corollary (Kolyvagin's theorem)

If  $A$  is an **isogeny factor** of  $X_H$ , and if the **analytic rank** of  $A$  is **zero**, then  $A(\mathbb{Q})$  is finite.

### Corollary (Decomposition)

We can **decompose**  $J_H$  up to isogeny using linear algebra and point-counting.

# Mordell–Weil sieve

- Let  $X$  be a **curve** and  $A$  be an **abelian variety**.

$$\begin{array}{c} X(\mathbb{Q}) \\ \downarrow \\ X(\mathbb{F}_p) \end{array}$$

- If  $X(\mathbb{F}_p)$  is **empty** for some  $p$  then  $X(\mathbb{Q})$  is **empty**.

# Mordell–Weil sieve

- Let  $X$  be a **curve** and  $A$  be an **abelian variety**.

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \beta \\ X(\mathbb{F}_p) & \xrightarrow{\pi} & A(\mathbb{F}_p). \end{array}$$

- If  $X(\mathbb{F}_p)$  is **empty** for some  $p$  then  $X(\mathbb{Q})$  is **empty**.
- If  $\text{im } \pi \cap \text{im } \beta$  is **empty** then  $X(\mathbb{Q})$  is **empty**.

# Mordell–Weil sieve

- Let  $X$  be a **curve** and  $A$  be an **abelian variety**.

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \beta \\ \prod_{p \in S} X(\mathbb{F}_p) & \xrightarrow{\pi_S} & \prod_{p \in S} A(\mathbb{F}_p). \end{array}$$

- If  $X(\mathbb{F}_p)$  is **empty** for some  $p$  then  $X(\mathbb{Q})$  is **empty**.
- If  $\text{im } \pi \cap \text{im } \beta$  is **empty** then  $X(\mathbb{Q})$  is **empty**.
- This is explicit and is implemented in Magma.

# An equationless sieve for the group $121 \cdot 605 \cdot 41 \cdot 1$

The curve  $X_H$  has **local points everywhere**, and analytic **rank = genus = 41**.

$H(11) \subset N_{\text{ns}}(11)$ , so  $X_H$  maps to  $X_{\text{ns}}^+(11)$ , which is an elliptic curve of rank 1.

$$\begin{array}{ccc} X_H(\mathbb{Q}) & \longrightarrow & X_{\text{ns}}^+(11)(\mathbb{Q}) \quad \text{=====} \quad \langle R \rangle \cong \mathbb{Z} \\ \downarrow & & \downarrow \beta \\ \prod_{p \in S} X_H(\mathbb{F}_p) & \xrightarrow{\pi_S} & \prod_{p \in S} X_{\text{ns}}^+(11)(\mathbb{F}_p) \end{array}$$

We can compute  $\text{im } \pi_S$  without *equations* for  $X_H$  or  $\pi_S$

- A point of  $X_{\text{ns}}^+(11)(\mathbb{F}_p)$  corresponds to  $E$  with  $\rho_{E,11}(G_{\mathbb{F}_p}) \subset N_{\text{ns}}(11)$  and lifts to a point of  $X_H(\mathbb{F}_p)$  if and only if  $\rho_{E,121}(G_{\mathbb{F}_p}) \subset H(121)$ .
- For  $p = 13$  the image of any point in  $Y_H(\mathbb{Q})$  maps to  $nR$  with  $n \equiv 1, 5 \pmod{7}$ .
- For  $p = 307$  any point in  $Y_H(\mathbb{Q})$  maps to  $nR$  with  $n \equiv 2, 3, 4, 7, 10, 13 \pmod{14}$ .
- Therefore  $Y_H(\mathbb{Q}) = \emptyset$  (and in fact  $X_H(\mathbb{Q}) = \emptyset$ ; there are no rational cusps).

## Gargantuan models of modular curves<sup>3</sup>

- We computed canonical models (over  $\mathbb{Q}$ ) for 27.729.43.1 (resp. 25.625.36.1).
- We use these models to prove that  $X_H$  has no  $\mathbb{Q}_3$  (resp.  $\mathbb{Q}_5$ ) as follows.
- These models have very bad reduction at  $p = 3$  (resp. 5). (They're not even flat.)
- $X_H(\mathbb{F}_p) \neq \emptyset$  for all  $p$ , but  $X_H(\mathbb{Z}/p^2\mathbb{Z}) = \emptyset$  for  $p = 3$  (resp. 5).
- The “Greenberg transform” (i.e., the “Wittferential tangent space” of Buium) is adjoint to Witt vectors:  $X_H^{(1)}(\mathbb{F}_p) = X_H(\mathbb{Z}/p^2\mathbb{Z})$ .
- The fibers of the map  $X_H^{(1)} \rightarrow X_H$  have no  $\mathbb{F}_p$  points.

---

<sup>3</sup>We give thanks to Poonen and Zywna

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

