2-adic images of Galois representations

David Zureick-Brown (Emory University)
Jeremy Rouse (Wake Forest University)

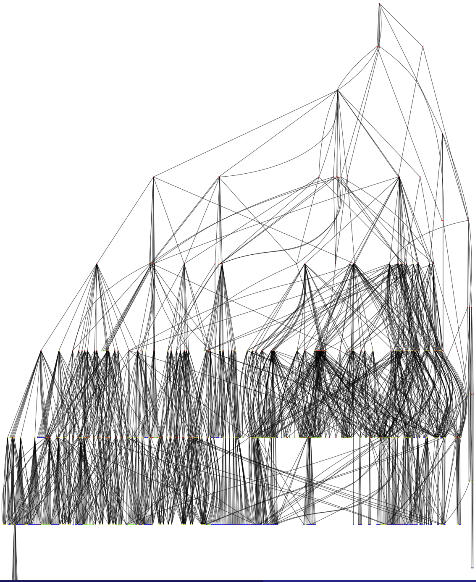
Emory University

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

PANTS XX,
Davidson College

September 7-8, 2013

Gratuitous picture – subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ containing $-I$



Background - Image of Galois

$$G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$$

$$E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$$

$$\begin{aligned}
\rho_{E,n}\colon \quad G_{\mathbb{Q}} \to \mathrm{Aut}\, E[n] \quad &\cong \quad \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\
\rho_{E,\ell^\infty}\colon \quad G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell) \quad &= \quad \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \\
\rho_{E}\colon \quad G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \quad &= \quad \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)
\end{aligned}$$

Background - Galois Representations

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

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

Example - torsion on an ellitpic curve

If E has a K-rational torsion point $P \in E(K)[n]$ (of exact order n), then the image is constrained:

$$G_n \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

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

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

Example - Isogenies

If E has a K-rational, cyclic isogeny $\phi\colon E \to E'$ with $\ker\phi = \langle P \rangle$, then the image is constrained

$$G_n \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

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:

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

$G_n \subset N_{\mathrm{sp}}$ iff

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

Classification of Images - Mazur's Theorem

Theorem

Let E be an elliptic curve over $\mathbb{Q}$. Then for $\ell > 11$, $E(\mathbb{Q})[\ell] = \{cusps\}$.

In other words, for $\ell > 11$ the mod ℓ image is not contained in a subgroup conjugate to

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

Classification of Images - Mazur; Bilu, Parent

Theorem (Mazur)

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 37$ the mod ℓ image is not contained in a subgroup conjugate to

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Theorem (Bilu, Parent)

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 13$ the mod ℓ image is not contained in a subgroup conjugate to

$$\left\langle \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Main conjecture

Conjecture

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

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

is open.

Note:

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

Sample Consequences of Serre's Theorem

Surjectivity

For large ℓ, $\rho_{E,\ell}$ is surjective.

Lang-Trotter

Density of supersingular primes is 0.

"Vertical" image conjecture

Conjecture

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

$$[\rho_E(G_K) : \mathrm{GL}_2(\hat{\mathbb{Z}})] \leq N.$$

Remark

This follows from the "$\ell > 37$" conjecture.

Problem

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

Main Theorem

Theorem (Rouse, ZB)

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

Cremona Database

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 (one example)

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

CM , 1613

Cremona Database

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

64 , 0

$j = -3 \cdot 2^{18} \cdot 5 \cdot 13^3 \cdot 41^3 \cdot 107^3 \cdot 17^{-16}$ on $X_{ns}^{+}(16)$ (Heegner, Baran)

Modular curves

Definition

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

Definition

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

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

Rational Points on modular curves

Goal

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

Remark

- Sometimes $X_H \cong \mathbb{P}^1$ or elliptic.
- Can compute $g(X_H)$ group theoretically (via Riemann-Hurwitz).

Fact

$g(X_H) \to \infty$.

Arithmetically maximality

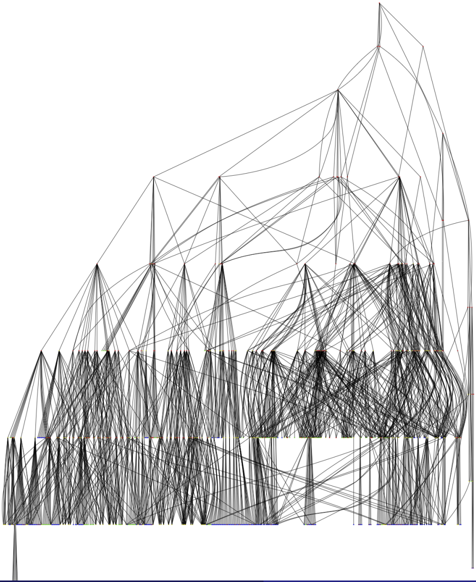
Definition

- $H \subset H' \Leftrightarrow X_H \to X_{H'}$
- Say that H is **arithmetically maximal** if
  1. $g(X_H) > 1$ and
  2. $H \subset H' \Leftrightarrow g(X_{H'}) \leq 1$
- Every modular curve maps to an arithmetically maximal or genus ≤ 1 curve.

Template

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

Gratuitous picture – subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ containing $-I$



Sample subgroup (Serre): $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$, $H(n) \subset \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$.

$$\begin{array}{ccccc}
\ker \phi_2 & \subset & H(3) & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \\
 & & \downarrow \phi_2 & & \downarrow \\
I + 2M_2(\mathbb{F}_2) & = & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \\
 & & \downarrow \phi_1 & & \downarrow \\
 & & H(1) & = & \mathrm{GL}_2(\mathbb{F}_2)
\end{array}$$

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

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

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

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

Sample subgroup (Dokchitser, Dokchitser): $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$, $H(n) \subset \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$.

$$\begin{array}{ccccc} \langle I + 2E_{1,1}, I + 2E_{2,2} \rangle & \subset & H(2) & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \\ & & \downarrow & & \downarrow \\ & & H(1) & = & \mathrm{GL}_2(\mathbb{F}_2) \end{array} \qquad \dim_{\mathbb{F}_2} \ker \phi_1 = 2$$

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

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

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

Sample subgroup: $H \subset \mathrm{GL}_2(\mathbb{Z}_2)$, $H(n) \subset \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$.

$$\begin{array}{ccccccc}
\ker\phi_4 & \subset & H(5) & \subset & \mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z}) & & \color{red}{\dim_{\mathbb{F}_2}\ker\phi_2 = 4} \\
 & & \downarrow{\scriptstyle \phi_4} & & \downarrow & & \\
\ker\phi_3 & \subset & H(4) & \subset & \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}) & & \color{red}{\dim_{\mathbb{F}_2}\ker\phi_2 = 3} \\
 & & \downarrow{\scriptstyle \phi_3} & & \downarrow & & \\
\ker\phi_2 & \subset & H(3) & \subset & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) & & \color{red}{\dim_{\mathbb{F}_2}\ker\phi_2 = 2} \\
 & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\
\ker\phi_1 & \subset & H(2) & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) & & \color{red}{\dim_{\mathbb{F}_2}\ker\phi_2 = 3} \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow & & \\
 & & H(1) & = & \mathrm{GL}_2(\mathbb{F}_2) & &
\end{array}$$

Fun facts

318 curves (excluding pointless conics)

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

Equations – Basic idea

1. The canoncial map $C \hookrightarrow \mathbb{P}^{g-1}$ is given by $P \mapsto [\omega_1(P) : \ldots : \omega_g(P)]$.
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 with different values at "new cusps".

Rational points rundown

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	??

Techniques

- Local methods
- Chabauty
- Elliptic Chabauty
- Mordell-Weil sieve
- étale descent
- Pryms
- ~~Dem'janenko-Manin~~
- A novel, indirect argument (étale descent + group theory) for genus 7 curves

Pryms

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

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

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 $D = 5$)

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

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

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

Thanks

Thank you!