Progress on Mazur's Program B

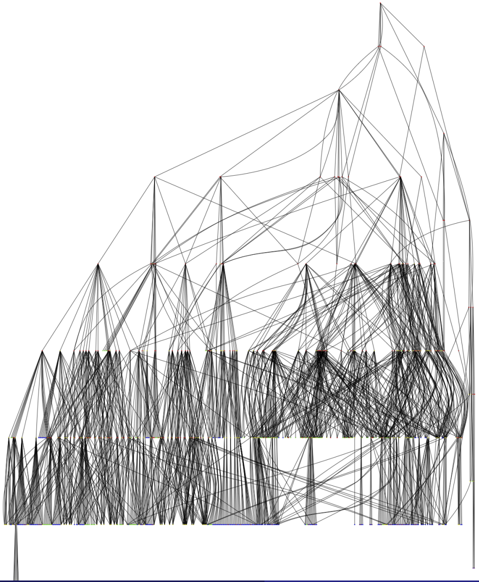
David Zureick-Brown

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

Stanford Universitiy

September 25, 2017

Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_2)$



Background - Image of Galois

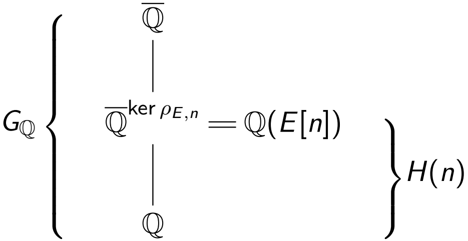
$$G_{\mathbb{Q}} := \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$$

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

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

Background - Galois Representations

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


$G_{\mathbb{Q}}$
$\overline{\mathbb{Q}}$
$\overline{\mathbb{Q}}^{\ker \rho_{E,n}} = \mathbb{Q}(E[n])$
$\mathbb{Q}$
$H(n)$

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

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

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,
- neither of which is defined over K
- but which are both defined over some quadratic extension of K
- and which are Galois conjugate.

Sample subgroup (Serre)

$$\begin{tikzcd}
\ker \phi_2 \arrow[r, phantom, "\subset"] & H(8) \arrow[r, phantom, "\subset"] \arrow[d, "\phi_2"] & \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \arrow[d] & \dim_{\mathbb{F}_2} \ker \phi_2 = 3 \\
I + 2M_2(\mathbb{Z}/2\mathbb{Z}) \arrow[r, phantom, "\subset"] & H(4) \arrow[r, phantom, "="] \arrow[d, "\phi_1"] & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \arrow[d] & \dim_{\mathbb{F}_2} \ker \phi_1 = 4 \\
 & H(2) \arrow[r, phantom, "="] & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) &
\end{tikzcd}$$

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

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

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

Sample subgroup (Dokchitser^2)

$$\begin{tikzcd}
\langle I + 2E_{1,1}, I + 2E_{2,2} \rangle & \subset & H(4) \arrow[d] & \subset & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \arrow[d] \\
 & & H(2) & = & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})
\end{tikzcd}$$

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

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

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

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

A typical subgroup

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

Non-abelian entanglements

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

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

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

Classification of Images - Mazur's Theorem

Theorem

Let E be an elliptic curve over $\mathbb{Q}$. Then for $\ell > 11$, $E(\mathbb{Q})[\ell] = \{0\}$.

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

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

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

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

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 indicies occur.

Zywina (mod ℓ)

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

Zywina (all possible indicies)

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

Morrow (composite level)

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

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

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

Main Theorems continued

Zywina–Sutherland (stay tuned!)

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

Gonzalez–Jimenez, Lozano–Robledo

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

Brau–Jones, Jones–McMurdy (in progress)

Equations for X_H for entanglement groups H.

Rouse–ZB for other primes (tonite's problem session)

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

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 indicies 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).

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

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

Minimality

Definition

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

Definition

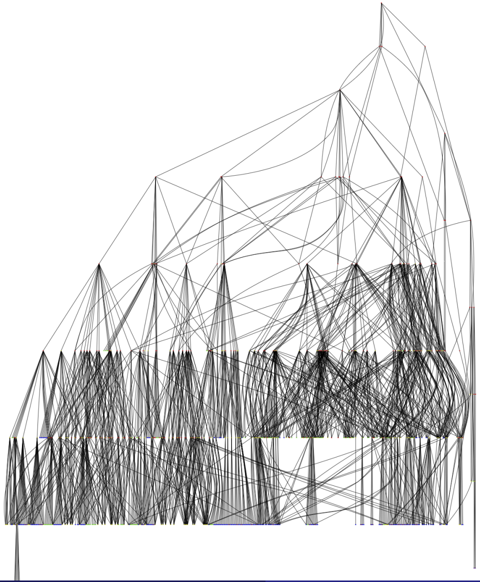
We say that H is **arithmetically minimal** if

1. $\det(H) = \widehat{\mathbb{Z}}^*$, and
2. a few other conditions.

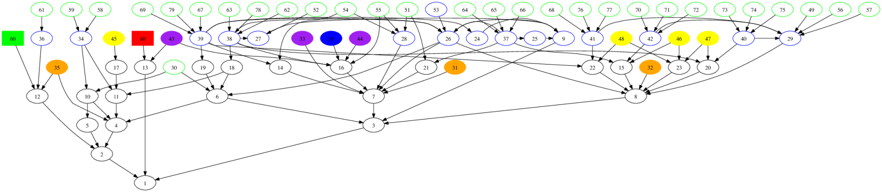
Template

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.

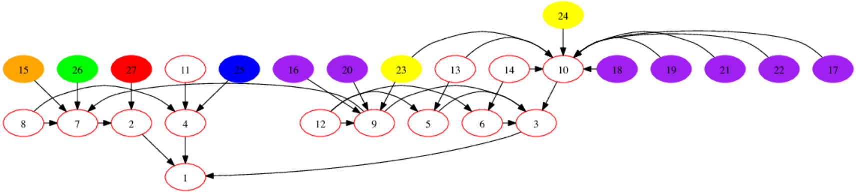
Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_2)$



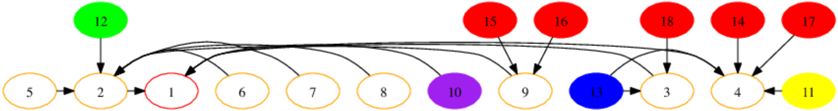
Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_3)$



Gratuitous picture – subgroups of $\mathrm{GL}_2(\mathbb{Z}_5)$



Gratuitous picture – subgroups of $\mathrm{GL}_2(\mathbb{Z}_{11})$



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

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".

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; descent works, try Chabauty
	$g = 4$	3 left; have models, ≥ 3 rational points
	$g = 6$	trigonal, with model, ≥ 3 rat pts
	$g = 12$	gonality ≤ 9, plane model, degree 121
	$g = 43$	New ideas needed

$\ell = 3$ example

$$X_H \colon -x^3y + x^2y^2 - xy^3 + 3xz^3 + 3yz^3 = 0$$

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
	$g = 2$ (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
	$g = 8, 14, 22, 36$ (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
	$g = 9, 12, 69, 94$	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	Problem session

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

Explicit methods: highlight reel

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

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!