Progress on Mazur’s program B

David Zureick-Brown

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

Explicit Methods in Number Theory
Oberwolfach

July 25, 2018
Background - Galois Representations

$G_Q := \text{Aut}(\overline{Q}/Q)$

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

$\rho_{E,n} : G_Q \to \text{Aut} E[n] \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$

$\rho_{E,\ell\infty} : G_Q \to \text{GL}_2(\mathbb{Z}_\ell) = \lim_{\leftarrow n} \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$

$\rho_E : G_Q \to \text{GL}_2(\hat{\mathbb{Z}}) = \lim_{\leftarrow n} \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$
Background - Image of Galois

\[ \rho_{E,n}: \mathbb{G}_\mathbb{Q} \to H(n) \hookrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \]

Problem (Mazur's "program B")

Classify all possibilities for \(H(n)\).
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 $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\sigma(P) = P$$

$$\sigma(Q) = a_\sigma P + b_\sigma Q$$
If $E$ has a $K$-rational, **cyclic isogeny** $\phi: E \to E'$ with $\ker \phi = \langle P \rangle$ then:

$$H(n) \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

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

$$\sigma(P) = a_\sigma P$$

$$\sigma(Q) = b_\sigma P + c_\sigma Q$$
Example - other maximal subgroups

Normalizer of a split Cartan:

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

\( H(n) \subset N_{sp} \) and \( H(n) \not\subset C_{sp} \) 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.
Problem (Mazur’s “program B”)

Classify all possibilities for $H(n)$. 

\[ \rho_{E,n}: \mathbb{G}_\mathbb{Q} \rightarrow H(n) \hookrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \] 

\[ \mathbb{G}_\mathbb{Q} \xrightarrow{\ker \rho_{E,n}} \mathbb{Q}(E[n]) \xrightarrow{H(n)} \]
**Modular curves**

**Definition**

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

**Definition**

- \( \Gamma(N) \subset H \subset \text{GL}_2(\hat{\mathbb{Z}}) \) (finite index)
- \( \mathbf{X}_H := \mathbf{X}(N)/\tilde{H} \)
- \( \mathbf{X}_H(K) \ni (E/K, \iota) \iff H(N) \subset H \pmod{N} \)

**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. \( -I \in H \).
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

$$g(X_H), \gamma(X_H) \to \infty \text{ as } \left[ \text{GL}_2(\widehat{\mathbb{Z}}) : H \right] \to \infty.$$
Theorem 1 also fits into a general program:

B. **Given a number field** $K$ **and a subgroup** $H$ **of** $\hat{\text{GL}}_2(\mathbb{Z}) = \prod_p \text{GL}_2(\mathbb{Z}_p)$ **classify all elliptic curves** $E/K$ **whose associated Galois representation on torsion points maps** $\text{Gal}(\overline{K}/K)$ **into** $H \subset \hat{\text{GL}}_2(\mathbb{Z})$.

Mazur - Rational points on modular curves (1977)
Sample subgroup (Serre)

\[
\begin{align*}
\ker \phi_2 & \subset H(8) \subset \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_2 = 3 \\
I + 2M_2(\mathbb{Z}/2\mathbb{Z}) & \subset H(4) = \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_1 = 4 \\
& \downarrow \phi_2 & \downarrow \\
& H(2) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})
\end{align*}
\]

\[\chi : \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{F}_2^3.\]

\[\chi = \text{sgn} \times \text{det}\]

\[H(8) := \chi^{-1}(G), \ G \subset \mathbb{F}_2^3.\]
Sample subgroup (Dokchitser$^2$)

\[ \langle I + 2E_{1,1}, I + 2E_{2,2} \rangle \subset H(4) \subset \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \quad \text{dim}_{\mathbb{F}_2} \ker \phi_1 = 2 \]

\[ \downarrow \quad \downarrow \]

\[ H(2) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \]

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

\[ \text{im} \rho_{E,4} \subset H(4) \iff j(E) = -4t^3(t + 8). \]

\[ X_H \cong \mathbb{P}^1 \xrightarrow{j} X(1). \]
A typical subgroup

\[
\begin{align*}
\ker \phi_4 & \subset H(32) \subset \GL_2(\mathbb{Z}/32\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_4 = 4 \\
\ker \phi_3 & \subset H(16) \subset \GL_2(\mathbb{Z}/16\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_3 = 3 \\
\ker \phi_2 & \subset H(8) \subset \GL_2(\mathbb{Z}/8\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_2 = 2 \\
\ker \phi_1 & \subset H(4) \subset \GL_2(\mathbb{Z}/4\mathbb{Z}) & \dim_{\mathbb{F}_2} \ker \phi_1 = 3 \\
H(2) & = \GL_2(\mathbb{Z}/2\mathbb{Z}) & 
\end{align*}
\]
There exists a surjection $\theta : \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

$$H(6) := \Gamma_\theta \cap \text{GL}_2(\mathbb{Z}/6\mathbb{Z})$$

$$\text{im } \rho_{E,6} \subset H(6) \Rightarrow K(E[2]) \subset K(E[3])$$
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 \( \ell \) image is not contained in a subgroup conjugate to

\[
\begin{pmatrix}
1 & * \\
0 & *
\end{pmatrix}.
\]
Theorem (Mazur)

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

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

Theorem (Bilu, Parent, Rebolledo)

Let $E$ be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 13$ the mod $\ell$ 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 (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 $\rho_E$

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

is open.

**Note:**

$$\text{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p \text{GL}_2(\mathbb{Z}_p)$$
**Conjecture**

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

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

**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 $\rho_{E,2^{\infty}}(G_Q)$ 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 $\text{GL}_2(\mathbb{Z}_2)$
<table>
<thead>
<tr>
<th>Index</th>
<th># of isogeny classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>727995</td>
</tr>
<tr>
<td>2</td>
<td>7281</td>
</tr>
<tr>
<td>3</td>
<td>175042</td>
</tr>
<tr>
<td>4</td>
<td>1769</td>
</tr>
<tr>
<td>6</td>
<td>57500</td>
</tr>
<tr>
<td>8</td>
<td>577</td>
</tr>
<tr>
<td>12</td>
<td>29900</td>
</tr>
<tr>
<td>16</td>
<td>235</td>
</tr>
<tr>
<td>24</td>
<td>5482</td>
</tr>
<tr>
<td>32</td>
<td>20</td>
</tr>
<tr>
<td>48</td>
<td>1544</td>
</tr>
<tr>
<td>64</td>
<td>0 (two examples)</td>
</tr>
<tr>
<td>96</td>
<td>241 (first example - $X_0(15)$)</td>
</tr>
<tr>
<td>CM</td>
<td>1613</td>
</tr>
</tbody>
</table>
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)
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 (Various authors)

Computation of \( S_\mathbb{Q}(d) \) for particular \( d \).

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

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

Theorem

Gonzalez–Jimenez, Lozano–Robledo Classify \( E/\mathbb{Q} \) with \( \rho_{E,N}(G_\mathbb{Q}) \) abelian.
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 $X_0(15)(\mathbb{Q}_\infty) = X_0(15)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$)
Recent theorems

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

Zywina (indices occurring infinitely often; modulo conjectures)
The index of $\rho_{E,N}(G_\mathbb{Q})$ divides 220, 336, 360, 504, 864, 1152, 1200, 1296 or 1536.

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

Brau–N. Jones, N. Jones–McMurdy (in progress)
Equations for $X_H$ for entanglement groups $H$. 
Morrow; Camacho–Li–Morrow–Petok–ZB (composite level)

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

Rouse–ZB for other prime powers (in progress)

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

1. Compute all arithmetically minimal $H \subset \text{GL}_2(\mathbb{Z}_2)$
2. Compute equations for each $X_H$
3. Find (with proof) all rational points on each $X_H$. 
Subgroups of $\text{GL}_2(\mathbb{Z}_2)$
The canonical map $C \hookrightarrow \mathbb{P}^{g-1}$ is given by $P \mapsto [\omega_1(P) : \cdots : \omega_g(P)]$. 

For a general curve, this is an embedding, and the relations are quadratic.

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

\[
q - 11q^5 + 10q^7 + O(q^8)
\]
\[
q^2 - 7q^5 + 6q^7 + O(q^8)
\]
\[
q^3 - 4q^5 + 2q^7 + O(q^8)
\]
\[
q^4 - 2q^5 + O(q^8)
\]
\[
q^6 - 3q^7 + O(q^8)
\]

\[
xu + 2xv - yz + yu - 3yv + z^2 - 4zu + 2u^2 + v^2 = 0
\]
\[
xu + xv - yz + yu - 2yv + z^2 - 3zu + 2uv = 0
\]
\[
2xz - 3xu + xv - 2y^2 + 3yz + 7yu - 4yv - 5z^2 - 3zu + 4zv = 0
\]
1. $H' \subset H$ of index 2, $X_{H'} \rightarrow X_H$ 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)

<table>
<thead>
<tr>
<th>Genus</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>175</td>
<td>52</td>
<td>56</td>
<td>18</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>Rank of Jacobian</td>
<td>0</td>
<td>25</td>
<td>46</td>
<td>–</td>
<td>–</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>27</td>
<td>3</td>
<td>9</td>
<td>10</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>7</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>9</td>
<td>–</td>
<td>–</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td>–</td>
<td>–</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>??</td>
</tr>
</tbody>
</table>
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

Many accidental isomorphisms of $X_H \cong X_{H'}$.

There is one $H$ such that $g(X_H) = 1$ and $X_H \in X_H(\mathbb{Q})$. 
Subgroups of $\text{GL}_2(\mathbb{Z}_2)$
Subgroups of $GL_2(\mathbb{Z}_{13})$
Subgroups of $\text{GL}_2(\mathbb{Z}_3)$
Subgroups of $\text{GL}_2(\mathbb{Z}_5)$
Subgroups of $GL_2(\mathbb{Z}_7)$
Subgroups of $GL_2(\mathbb{Z}_{11})$
### Rational Points rundown: $\ell = 3$

<table>
<thead>
<tr>
<th>$g$</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$g = 0$ Handled by Sutherland–Zywina</td>
</tr>
<tr>
<td></td>
<td>$g = 1$ all rank zero</td>
</tr>
<tr>
<td></td>
<td>$g = 4$ map to $g = 1$</td>
</tr>
<tr>
<td></td>
<td>$g = 2$ Chabauty works</td>
</tr>
<tr>
<td></td>
<td>$g = 4$ no 3-adic points</td>
</tr>
<tr>
<td></td>
<td>$g = 3$ Picard curves; map to rank 0 AV</td>
</tr>
<tr>
<td></td>
<td>$g = 4$ Admits étale triple cover</td>
</tr>
<tr>
<td></td>
<td>$g = 6$ Admits étale triple cover</td>
</tr>
<tr>
<td></td>
<td>$g = 12$ gonality $\leq 9$, plane model, degree 121</td>
</tr>
<tr>
<td></td>
<td>$g = 43$ New ideas needed</td>
</tr>
</tbody>
</table>
### Rational Points rundown: $\ell = 5$

<table>
<thead>
<tr>
<th>$g$</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5, 10 level 5, 3 level 25</td>
<td>All level 5 curves are genus 0</td>
</tr>
<tr>
<td>4</td>
<td>4 level 25</td>
<td>No 5-adic points</td>
</tr>
<tr>
<td>8, 22</td>
<td></td>
<td>known (e.g., $X_{ns}(25)$)</td>
</tr>
<tr>
<td>2</td>
<td>2 level 25</td>
<td>Rank 2, $A_5 \mod 2$ image</td>
</tr>
<tr>
<td>4</td>
<td>3 level 25</td>
<td>All isomorphic.</td>
</tr>
<tr>
<td></td>
<td>14, 36 (levels 25 and 125)</td>
<td>No models (or ideas, yet)</td>
</tr>
</tbody>
</table>
### Rational Points rundown: $\ell = 7$

<table>
<thead>
<tr>
<th>$g$</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7$</td>
<td>$g = 1, 3$</td>
</tr>
<tr>
<td></td>
<td>$[\mathbb{Z}, 4.4]$ handles these, $X_H(\mathbb{Q})$ is finite.</td>
</tr>
<tr>
<td></td>
<td>$g = 19, 26, \text{ level } 49$</td>
</tr>
<tr>
<td></td>
<td>Maps to one of the 6 above</td>
</tr>
<tr>
<td></td>
<td>$g = 1, \text{ level } 49$</td>
</tr>
<tr>
<td></td>
<td>$[SZ]$ handles this one (rank 0)</td>
</tr>
<tr>
<td></td>
<td>$g = 3, 19, 26, \text{ level } 49, 343$</td>
</tr>
<tr>
<td></td>
<td>Map to curve on previous line</td>
</tr>
<tr>
<td></td>
<td>$g = 12, \text{ level } 49$</td>
</tr>
<tr>
<td></td>
<td>Handled by</td>
</tr>
<tr>
<td></td>
<td>Greenberg– Rubin– Silverberg– Stoll</td>
</tr>
<tr>
<td>$94$</td>
<td>Known ($X_{ns}(49)$)</td>
</tr>
<tr>
<td>$9, 12, 69$</td>
<td>No models (or ideas, yet)</td>
</tr>
</tbody>
</table>
### Rational Points rundown: $\ell = 11$

<table>
<thead>
<tr>
<th>$\ell = 11$</th>
<th>all maximal are genus one</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only positive rank is $X_{ns}(11)$</td>
</tr>
<tr>
<td></td>
<td>All but one are ruled out by Zywina</td>
</tr>
<tr>
<td></td>
<td>some have sporadic points;</td>
</tr>
<tr>
<td></td>
<td>[Z, Theorem 1.6]</td>
</tr>
<tr>
<td>$g = 5$, level 11</td>
<td>[Z, Lemma 4.5]</td>
</tr>
<tr>
<td>$g = 5776$, level 121</td>
<td>“Challenge. . .”</td>
</tr>
</tbody>
</table>
Rational Points rundown: $\ell = 13$

Zywina handles all level 13 except for the cursed curve

<table>
<thead>
<tr>
<th>$g$</th>
<th>Level</th>
<th>Notable Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g = 2, 3$</td>
<td>13</td>
<td>Cursed, genus 3, rank 3, no torsion, some points</td>
</tr>
<tr>
<td>$g = 8$</td>
<td>169</td>
<td>$X_0(13^2)$ handled by Kenku</td>
</tr>
<tr>
<td>$X_{ns}(13)$</td>
<td></td>
<td>Cursed, genus 3, rank 3, no torsion, some points</td>
</tr>
<tr>
<td>$X_{S_4}(13)$</td>
<td></td>
<td>Also cursed</td>
</tr>
</tbody>
</table>
Rational Points: summary of remaining work.

<table>
<thead>
<tr>
<th>$g$</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$12, 43$</td>
</tr>
<tr>
<td>5</td>
<td>$2, 4, 14, 36$</td>
</tr>
<tr>
<td>7</td>
<td>$9, 12, 69$</td>
</tr>
<tr>
<td>11</td>
<td>a single genus 5776 curve remains</td>
</tr>
<tr>
<td>13</td>
<td>$X_{S_4}(13)$</td>
</tr>
</tbody>
</table>
Explicit methods: highlight reel

- Local methods
- Chabauty
- Elliptic Chabauty
- Mordell–Weil sieve
- étale descent
- Pryms
- Equationless descent via group theory.
- New techniques for computing $\text{Aut } C$. 
\[ D \xrightarrow{\nu - \text{id} - (\nu(P) - P)} \ker_0(J_D \to J_C) =: \text{Prym}(D \to C) \]

\[ C(\mathbb{Q}) = \bigcup_{\delta \in \{\pm 1, \pm 2\}} \text{im} \, D_\delta(\mathbb{Q}) \]
Pryms

\[ D \xrightarrow{\iota \text{id} - (\iota(P) - P)} \ker_0(J_D \to J_C) =: \text{Prym}(D \to C) \]

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

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

\[ D_\delta : \]

\[ Q_1(x, y, z) = \delta u^2 \]
\[ Q_2(x, y, z) = \delta uv \]
\[ Q_3(x, y, z) = \delta v^2 \]

- \( \text{Prym}(D_\delta \to C) \cong \text{Jac}_{H_\delta} \),
- \( H_\delta : y^2 = -\delta \det(M_1 + 2xM_2 + x^2M_3). \)
Thank you!