Progress on Mazur’s Program B

David Zureick-Brown

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

Southern California Number Theory Day

October 21, 2017
\[ G_\mathbb{Q} := \text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) \]
\[ E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2 \]

\[ \rho_{E,n} : G_\mathbb{Q} \rightarrow \text{Aut } E[n] \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \]

\[ \rho_{E,\ell^\infty} : G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \]

\[ \rho_E : G_\mathbb{Q} \rightarrow \text{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim_n \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \]
Background - Galois Representations

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

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

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

$$\sigma(P) = P$$

$$\sigma(Q) = a_\sigma P + b_\sigma Q$$
Example - Isogenies

If $E$ has a $K$-rational, **cyclic isogeny** $\phi: E \to E'$ with $\ker \phi = \langle P \rangle$ then:

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

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:

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

\[ H(n) \subset N_{sp} \text{ and } H(n) \not\subset C_{sp} \text{ iff} \]

- 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.
Background - Galois Representations

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

\[
\begin{align*}
\{ & \quad \overline{Q} \\
\{ & \quad \ker \rho_{E,n} = \mathbb{Q}(E[n]) \\
\{ & \quad \mathbb{Q} \hookrightarrow H(n) \}
\end{align*}
\]

Problem (Mazur’s “program B”)

Classify all possibilities for \( H(n) \).
Modular curves

Definition

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

Definition

- $\Gamma(N) \subset H \subset \text{GL}_2(\widehat{\mathbb{Z}})$ (finite index)
- $X_H := X(N)/H$
- $X_H(K) \ni (E/K, \iota) \iff H(N) \subset H \mod N$

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. $-I \in H$. 
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

$g(X_H), \gamma(X_H) \to \infty$ as $\left[ \text{GL}_2(\hat{\mathbb{Z}}) : H \right] \to \infty$. 
Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_2)$
Sample subgroup (Serre)

\[
\ker \phi_2 \subset H(8) \subset \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \quad \text{dim}_{\mathbb{F}_2} \ker \phi_2 = 3
\]

\[
I + 2M_2(\mathbb{Z}/2\mathbb{Z}) \subset H(4) = \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \quad \text{dim}_{\mathbb{F}_2} \ker \phi_1 = 4
\]

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

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

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

\[H(8) := \chi^{-1}(G), \ G \subset \mathbb{F}_2^3.\]
\[ \langle I + 2E_{1,1}, I + 2E_{2,2} \rangle \subset H(4) \subset \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \quad \text{dim}_{\mathbb{F}_2} \ker \phi_1 = 2 \]

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

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

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

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

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

\[
H(6) := \Gamma_{\theta} \subset \text{GL}_2(\mathbb{Z}/6\mathbb{Z}) \cap \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cap \text{GL}_2(\mathbb{Z}/3\mathbb{Z})
\]

\[
\text{im} \rho_{E,6} \subset H(6) \iff K(E[2]) \subset K(E[3])
\]
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)

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
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:

$$\text{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p \text{GL}_2(\mathbb{Z}_p)$$
“Vertical” image conjecture

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

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

Remark
This follows from the “$\ell > 37$” conjecture.

Problem
Assume the “$\ell > 37$” conjecture and compute $N$. 
### Main Theorems

<table>
<thead>
<tr>
<th>Theorem</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rouse, ZB (2-adic)</strong></td>
<td>The index of $\rho_{E,2^{\infty}}(G_\mathbb{Q})$ divides 64 or 96; all such indices occur.</td>
</tr>
<tr>
<td><strong>Zywina (mod $\ell$)</strong></td>
<td>Classifies $\rho_{E,\ell}(G_\mathbb{Q})$ (modulo some conjectures).</td>
</tr>
<tr>
<td><strong>Zywina (all possible indices)</strong></td>
<td>The index of $\rho_{E,N}(G_\mathbb{Q})$ divides 220, 336, 360, 504, 864, 1152, 1200, 1296 or 1536.</td>
</tr>
<tr>
<td><strong>Morrow (composite level)</strong></td>
<td>Classifies $\rho_{E,2\cdot\ell}(G_\mathbb{Q})$.</td>
</tr>
<tr>
<td><strong>Camacho–Li–Morrow–Petok–ZB (composite level)</strong></td>
<td>Classifies $\rho_{E,\ell_1\cdot\ell_2}(G_\mathbb{Q})$ (partially).</td>
</tr>
</tbody>
</table>
**Main Theorems continued**

**Zywina–Sutherland**
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 (in progress)**
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 $\tilde{P} \in E(\mathbb{F}_p)$ 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 $S_{\mathbb{Q}}(d)$ and $S(d)$ for particular $d$.

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

Classification of $E(\mathbb{Q}(3^\infty))_{\text{tors}}$
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.
### Index, # of isogeny classes

<table>
<thead>
<tr>
<th>Index</th>
<th>Number of 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)
Fun 2-adic facts

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.
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).
Minimality

**Definition**

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

**Definition**

We say that \( H \) is **arithmetically minimal** if

1. \( \det(H) = \hat{\mathbb{Z}}^* \), and
2. a few other conditions.
1. Compute all arithmetically minimal $H \subseteq \text{GL}_2(\mathbb{Z}_2)$
2. Compute equations for each $X_H$
3. Find (with proof) all rational points on each $X_H$. 
Gratuitous picture – subgroups of $\text{GL}_2(\mathbb{Z}_2)$
Gratuitous picture – subgroups of \( \text{GL}_2(\mathbb{Z}_3) \)
Gratuitous picture – subgroups of $\text{GL}_2(\mathbb{Z}_5)$
Gratuitous picture – subgroups of $\text{GL}_2(\mathbb{Z}_{11})$
318 curves $X_H$ with $-I \in H$ (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>57</td>
<td>18</td>
<td>20</td>
<td>4</td>
</tr>
</tbody>
</table>
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>Number</th>
<th>Rank of Jacobian</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>175</td>
<td>25 46</td>
</tr>
<tr>
<td>1</td>
<td>52</td>
<td>27 3 9 10 ??</td>
</tr>
<tr>
<td>2</td>
<td>56</td>
<td>7 – – ??</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>9 – ??</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>10 ??</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

- Lots of isomorphisms.
- ??? require real work
- Biggest level of an index.
- Put "achievements" all of the genus $\geq 3$ curves that we have to deal with map to a rank 1 elliptic curve with a rational 2-torsion point.
- Each $X_H$ has good reduction outside of 2, so the mod 2 image of the Galois of $\text{Jac}(X_H)$ is small.
- Difficult to find extensions of $\mathbb{Q}$ ramified only at 2; all of degree up to 8 are cyclic.
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: $\ell = 3$

$g = 0$  
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; map to rank 0 AV

$g = 4$  
Admits étale triple cover

$g = 6$  
Admits étale triple cover

$g = 12$  
gonality $\leq 9$, plane model, degree 121

$g = 43$  
New ideas needed
$\ell = 3$ example

$X_H: -x^3y + x^2y^2 - xy^3 + 3xz^3 + 3yz^3 = 0$
### Rational Points rundown: $\ell = 5$

<table>
<thead>
<tr>
<th>$g$</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$g = 0$ (10 level 5, 3 level 25) All level 5 curves are genus 0</td>
</tr>
<tr>
<td>$g = 4$</td>
<td>(4 level 25) No 5-adic points</td>
</tr>
<tr>
<td>$g = 2$</td>
<td>(2 level 25) Rank 2, $A_5$ mod 2 image</td>
</tr>
<tr>
<td>$g = 4$</td>
<td>(3 level 25) All isomorphic.</td>
</tr>
<tr>
<td>$g = 8, 14, 22, 36$</td>
<td>(levels 25 and 125) Each has 5 rational points</td>
</tr>
<tr>
<td></td>
<td>Each admits an order 5 aut Simple Jacobian</td>
</tr>
<tr>
<td></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>1, 3</td>
<td>$[Z, 4.4]$ handles these, $X_H(\mathbb{Q})$ is finite.</td>
</tr>
<tr>
<td>19, 26, level 49</td>
<td>Maps to one of the 6 above</td>
</tr>
<tr>
<td>1, level 49</td>
<td>$[SZ]$ handles this one (rank 0)</td>
</tr>
<tr>
<td>3, 19, 26, level 49, 343</td>
<td>Map to curve on previous line</td>
</tr>
<tr>
<td>12, level 49</td>
<td>Handled by Greenberg–Rubin–Silverberg–Stoll</td>
</tr>
<tr>
<td>9, 12, 69, 94</td>
<td>No models (or ideas, yet)</td>
</tr>
</tbody>
</table>
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;

$g = 5$, level 11

[Z, Theorem 1.6]

$g = 5776$, level 121

[Z, Lemma 4.5]

“Challenge...”
Rational Points rundown: $\ell = 13$

Zywina handles all level 13 except for the cursed curve

<table>
<thead>
<tr>
<th>Level</th>
<th>Genus</th>
<th>Curves</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>$g = 2, 3$</td>
<td>level 13 (8 total)</td>
</tr>
<tr>
<td></td>
<td>$g = 8$</td>
<td>level 169</td>
</tr>
<tr>
<td></td>
<td>$X_{ns}(13)$</td>
<td>Cursed. Genus 3, rank 3. No torsion. Some points</td>
</tr>
<tr>
<td></td>
<td>$X_0(13^2)$, handled by Kenku</td>
<td>Probably has maximal mod 2 image</td>
</tr>
<tr>
<td></td>
<td>Solved by Balakrishnan, Müller</td>
<td></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** \( \text{Aut } C \).
Example (Genus $C = 3 \Rightarrow$ Genus $D = 5$)

- $C : Q(x, y, z) = 0$
- $Q = Q_1Q_3 - Q_2^2$

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

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

Thank you!