

Progress on Mazur's Program B

David Zureick-Brown

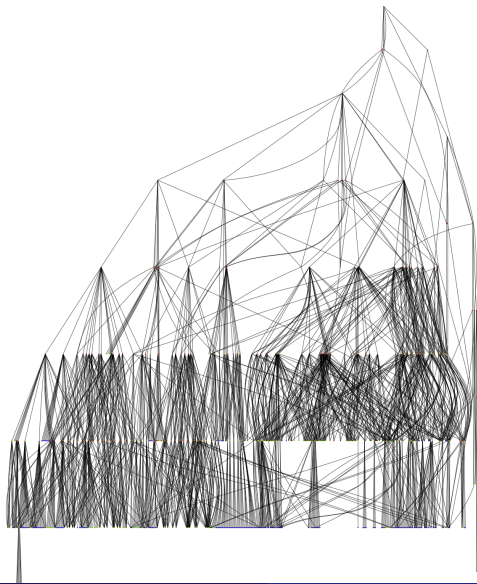
Emory University

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

University of Wisconsin, Madison

September 07, 2017

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



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

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

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

$$\rho_E: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim_n \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Background - Galois Representations

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

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

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** $\phi: E \rightarrow E'$ 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 $E(\overline{K})[n] \cong \langle P, Q \rangle$,

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

$$\sigma(Q) = b_\sigma P + c_\sigma Q$$

Example - other maximal subgroups

Normalizer of a split Cartan:

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

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

- there exists an unordered pair $\{\phi_1, \phi_2\}$ of cyclic isogenies,
- 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)

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

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

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

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

Sample subgroup (Dokchitser²)

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

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

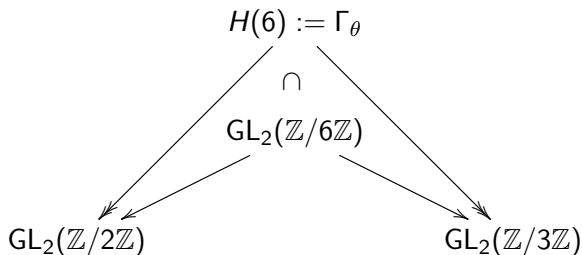
$$\begin{aligned} \mathrm{im} \rho_{E,4} \subset H(4) &\Leftrightarrow j(E) = -4t^3(t+8). \\ X_H &\cong \mathbb{P}^1 \xrightarrow{j} X(1). \end{aligned}$$

A typical subgroup

$\ker \phi_4$	\subset	$H(32)$	\subset	$GL_2(\mathbb{Z}/32\mathbb{Z})$	$\dim_{\mathbb{F}_2} \ker \phi_2 = 4$
		$\downarrow \phi_4$		\downarrow	
$\ker \phi_3$	\subset	$H(16)$	\subset	$GL_2(\mathbb{Z}/16\mathbb{Z})$	$\dim_{\mathbb{F}_2} \ker \phi_2 = 3$
		$\downarrow \phi_3$		\downarrow	
$\ker \phi_2$	\subset	$H(8)$	\subset	$GL_2(\mathbb{Z}/8\mathbb{Z})$	$\dim_{\mathbb{F}_2} \ker \phi_2 = 2$
		$\downarrow \phi_2$		\downarrow	
$\ker \phi_1$	\subset	$H(4)$	\subset	$GL_2(\mathbb{Z}/4\mathbb{Z})$	$\dim_{\mathbb{F}_2} \ker \phi_2 = 3$
		$\downarrow \phi_1$		\downarrow	
		$H(2)$	$=$	$GL_2(\mathbb{Z}/2\mathbb{Z})$	

Non-abelian entanglements

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



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

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

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

is open.

Note:

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

“Vertical” image conjecture

Conjecture

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

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

Remark

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

Problem

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

Main Theorems

Rouse, ZB (2-adic)

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

Zywina (mod ℓ)

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

Zywina (all possible indices)

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

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

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}_∞ 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

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

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.

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

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

- $X_H := X(N)/H$
- $X_H(K) \ni (E/K, \iota) \Leftrightarrow H(N) \subset H \pmod{N}$

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 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

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

Definition

- $H \subset H' \Leftrightarrow X_H \rightarrow X_{H'}$
- 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.

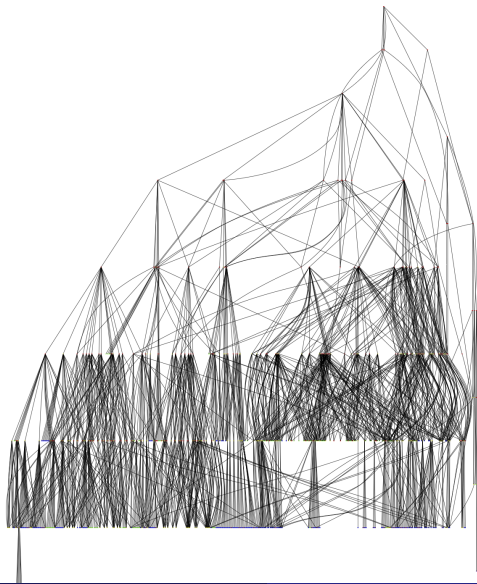
Definition

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

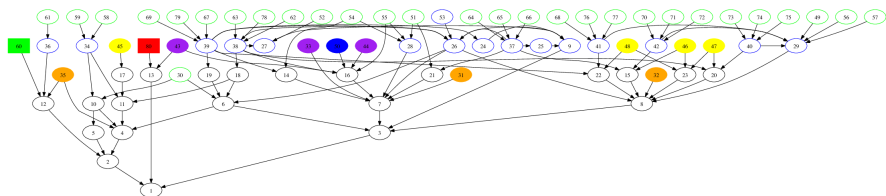
- ① $\det(H) = \widehat{\mathbb{Z}}^*$, and
- ② a few other conditions.

- 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 .

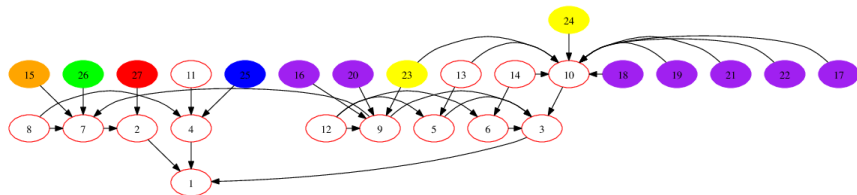
Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_2)$



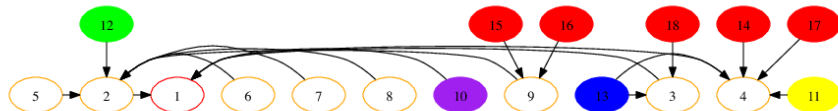
Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_3)$



Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_5)$



Gratuitous picture – subgroups of $GL_2(\mathbb{Z}_{11})$



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

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

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

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

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

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

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

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

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

Equations – general

- 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)

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

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

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 “Challenge. . .”

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

Solved by Balakrishnan, Müller

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 .

$$\begin{array}{ccc}
 D & \xrightarrow{\iota - \text{id} - (\iota(P) - P)} & \ker_0(J_D \rightarrow J_C) =: \text{Prym}(D \rightarrow C) \\
 \text{et} \downarrow \circlearrowleft \iota & & \\
 C & &
 \end{array}$$

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

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

$$D_\delta: Q_1(x, y, z) = \delta u^2$$

$$Q_2(x, y, z) = \delta uv$$

$$Q_3(x, y, z) = \delta v^2$$

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

Thank you!