Abelian surfaces of small conductor from genus 3 double covers

Raymond van Bommel

joint with Céline Maistret, Jia Shi, Andrew V. Sutherland

ANTS XVII

Motivation

Tables of elliptic curves of small conductor N have been made for a while and are a core part of the **LMFDB** (Cremona). Small N makes it feasible to match modular forms and compute L-functions.

Situation for genus 2:

- 66,158 curves with $|\Delta_{\min}| \leq 10^6$ listed in 2016 (Booker–Sijsling–Sutherland–Voight–Yasaki),
- $>$ 6 million L-functions of genus 2 and conductor $N \leq 10^6$ (Booker–Sutherland, in preparation),
- new phenomenon: there can be primes of almost good reduction (i.e., primes for which C has bad reduction, but $\mathrm{Jac}(C)$ has good reduction), so small *conductor* $\not\Rightarrow$ small *discriminant*,
- new phenomenon: not all abelian surfaces are Jacobians, and some are even not principally polarisable.

Goal

Find (non-Jacobian) abelian surfaces of small conductor, especially ones for which we already believe to have an L-function.

Prym varieties

After Jacobians and Weil restrictions, Prym varieties are the next place to look for abelian surfaces of small conductor.

Definition

Let $\varphi\colon C_1 \to C_2$ be a non-constant morphism of curves. Then the Prym variety associated to φ is $\ker \varphi_*$, where $\varphi_*\colon \mathrm{Jac}(C_1) \to \mathrm{Jac}(C_2)$ is the pushforward.

Prym varieties need not be principally polarisable. In fact, the natural polarisation that they are equipped with is of degree $\deg(\varphi)$.

This work

A heuristic algorithm to construct Pryms of small conductor, with $\mathrm{genus}(C_1) = 3$, $\mathrm{genus}(C_2) = 1$, and $\deg(\varphi) = 2$.

Motivating example: conductor-550 surface found while constructing a database of genus 3 curves (Sutherland), corresponding to one of nine Poor–Yuen paramodular forms of level < 1000 with *no* known Jacobian.

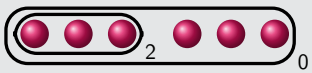
Warm-up: hyperelliptic curves

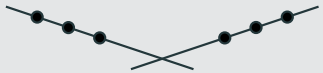
How do we determine the conductor of such Prym varieties? Let us first consider the case of degree 2 covers of $\mathbb{P}^1$. Let $H\colon y^2 = f(x)$.

The arithmetic and geometry of H can be studied by considering the p-adic distances between the roots of $f(x)$. Cluster pictures are used to visually display these distances.

Example

For the curve $H\colon y^2 = x(x-p^2)(x-2p^2)(x-1)(x-2)(x-3)$, we get





- The reduction of this curve modulo p consists of two genus 1 curves glued transversally to each other.
- The curve H has bad reduction at p, but its Jacobian has good reduction at p (product of the Jacobians of the genus 1 curves).
- The discriminant at p is p^{12} and the conductor is 1.

Constructing Pryms

Pryms can be constructed from a genus 1 curve $E/\mathbb{Q}$ by adjoining a square root of a rational function on E:

1. Pick a rational effective divisor D on E of degree 4 (each prime divisor with multiplicity 1), the branch locus.
2. Assume $D \sim 2D'$ for a rational divisor D', and take $f \in \mathscr{L}(D - 2D')$.
3. Adjoin $\sqrt{f}$ to the function field of E:

$$\phi\colon C \longrightarrow E, \qquad C \text{ has genus 3 (Riemann–Hurwitz).}$$

Two degrees of freedom

Quadratic twist: replace f by $d \cdot f$.

Different cover: replace D' by $D' + T$ for $T \in \mathrm{Pic}^0(E)[2]$.

Controlling the primes of bad reduction

Like in the case of hyperelliptic curves, we wish to study the stable reduction of C through the degeneration of the branch points on E.

Subtlety

The degeneration full divisor $D - 2D'$ matters, not just the branch locus D.

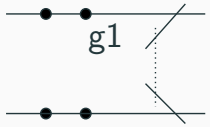
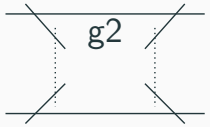
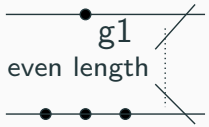
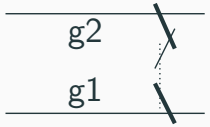
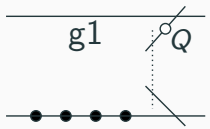
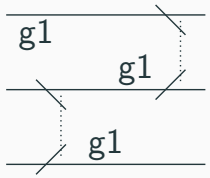
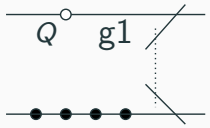
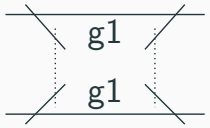
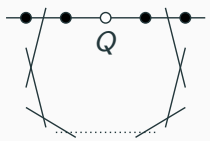
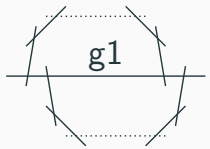
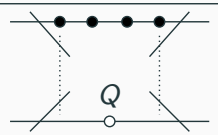
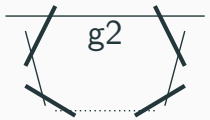
For simplicity, we will:

- only study the tame part of the conductor (there is no non-trivial wild part for $p > 3$),
- sometimes assume that $D = P_1 + P_2 + P_3 + P_4$ and $D' = P_4 + Q$ with P_1, P_2, P_3, P_4, Q defined over $\mathbb{Q}_p^{\mathrm{unr}}$,
- assume E has good or semi-stable (multiplicative) reduction.

In the next table:

- $\mathcal{E}$ is a regular model of E separating the points in D and D',
- $\mathcal{C}$ is a cover of $\mathcal{E}$; it is a regular model of C,
- all results apply after a suitable twist.

Example reductions with small conductor for the Prym

$\mathcal{E}_p$	N_E	$\mathcal{C}_p$	stable reduction of C	N_C	N_{Prym}
	0		good	0	0
	0		genus 2 with 1 self-intersection	1	1
	0		genus 2 and genus 1 intersecting in a node	0	0
	0		three genus 1s linked in a chain	0	0
	0		two genus 1s intersecting twice	1	1
	1		genus 1 with 2 self-intersections	2	1
	1		genus 2 with 1 self-intersection	1	0

Determining the conductor

Issue 1

Except in the case of good reduction of C, the (wild) conductor at 2 and 3 is not controlled by the method.

Issue 2

It is hard to find D and D' that reduce to one of the 7 cases modulo every prime $p > 2$. In the case of hyperelliptic curves, with D and D' on $\mathbb{P}^1$ that amounts to solving some unit equation.

Assuming modularity, we use the functional equation for the L-function to rule out some conductors. We only consider conductors up to a suitable chosen $N_{\max}$ (i.e., 2^{20}).

Average polynomial-time methods (Harvey–Sutherland and Costa–Harvey–Sutherland) are used to quickly determine almost all good Euler factors for all $p \leq B$. The current bottleneck is the combinatorics of the combinations of the remaining Euler factors.

The search

1. Iterate over pairs (E, K):
   - elliptic curves $E/\mathbb{Q}$ with $\mathrm{rad}(N_E) \leq 2^{10}$ (315,607 from the LMFDB),
   - number fields K, $[K : \mathbb{Q}] \leq 4$, $|\Delta_K| \leq 2^{20}$ (12,821 from the LMFDB), the field of definition for P_1, P_2, P_3, P_4.
2. Search for a subgroup $\langle x_1, \ldots, x_\ell \rangle$ of $E(K)$, as large as possible.
3. Iterate P_1, P_2, P_3, P_4 over linear combinations $\sum c_i x_i$ with c_i small. Only consider quadruples that are Galois-invariant, which satisfy $P_1 + P_2 + P_3 + P_4 \in 2E(K)$, and for which the product of the bad primes is at most 2^{10}.
4. Use Riemann-Roch to find f and hence C.
5. Deduplicate isogeny classes and twists with a trace hash (a linear combination of $a_p(A)$, $p \in [2^{12}, 2^{13}]$, over $\mathbb{F}_{2^{61}-1}$), and a twist-invariant twist hash.

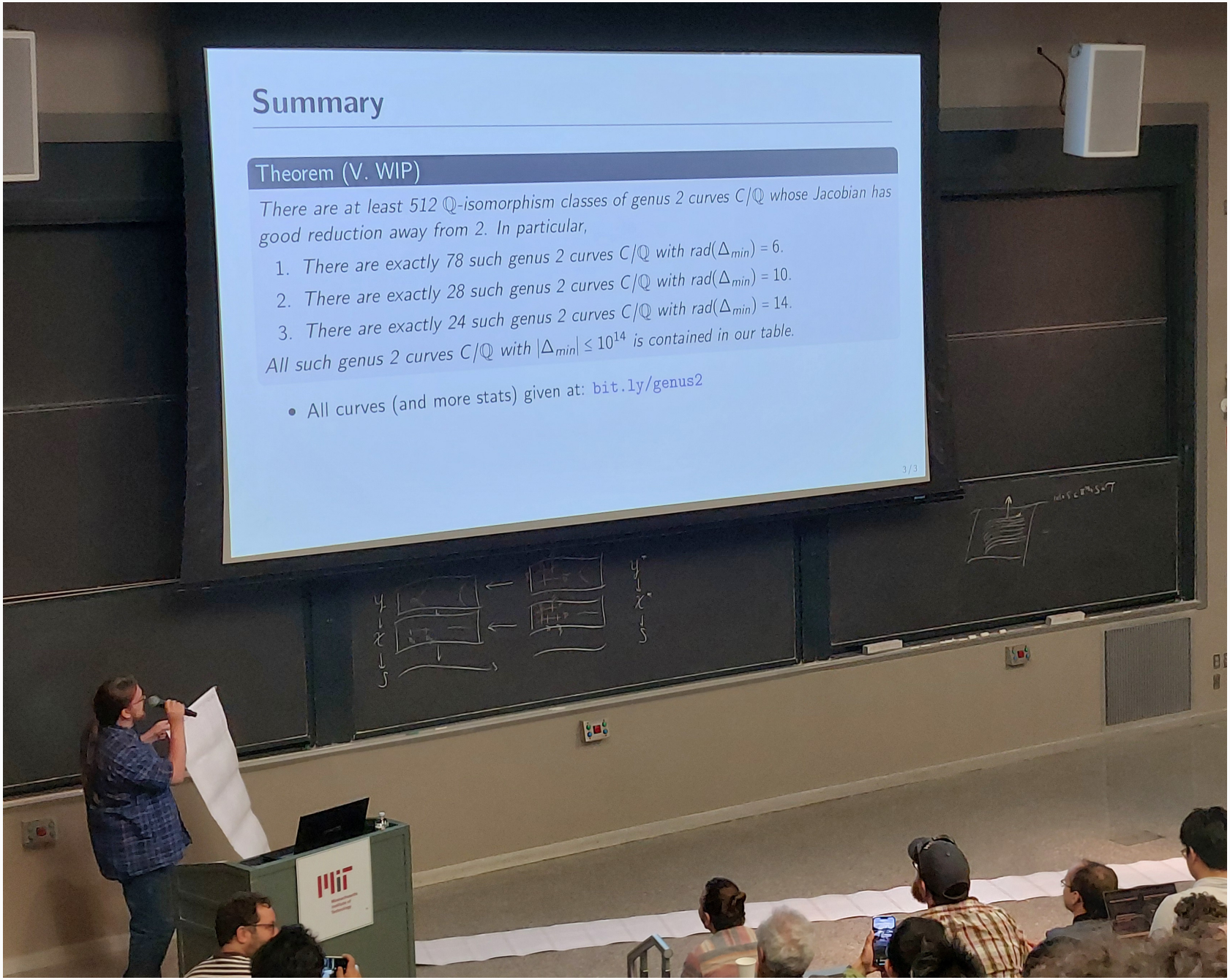
Remark

Note that $\Delta_{\min}(C)$ is not bounded in our search and can be very large!

Computation

A parallel computation on $\sim$250,000 cores, $\sim$100 CPU-years (half spent enumerating, half spent computing conductors).

	count
Genus 3 double covers $C \to E$ enumerated	117,615,804
Distinct Prym isogeny classes	80,904,678
Pryms of conductor $N \leq 2^{20}$:	
isogeny classes	454,153
not containing a previously known Jacobian	$\approx$ 80,000
new genus 2 Jacobians	$\approx$ 8,586


Summary
Theorem (V. WIP)
There are at least 512 $\mathbb{Q}$-isomorphism classes of genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2. In particular,
1. There are exactly 78 such genus 2 curves $C/\mathbb{Q}$ with $\mathrm{rad}(\Delta_{min}) = 6$.
2. There are exactly 28 such genus 2 curves $C/\mathbb{Q}$ with $\mathrm{rad}(\Delta_{min}) = 10$.
3. There are exactly 24 such genus 2 curves $C/\mathbb{Q}$ with $\mathrm{rad}(\Delta_{min}) = 14$.
All such genus 2 curves $C/\mathbb{Q}$ with $|\Delta_{min}| \leq 10^{14}$ is contained in our table.
All curves (and more stats) given at: bit.ly/genus2
3/3

Good reduction away from 2

Problem (Poonen, ANTS II, 1996)

Enumerate all genus 2 curves $/\mathbb{Q}$ whose *Jacobians* have good reduction away from 2.

Smart (1997): list of all genus 2 curves with good reduction away from 2.

Visser (2024): found 512 such Jacobians, wondered if these were all.

We add 10 new genus 2 curves, which we found because their Jacobians are isogenous to Pryms in our search.

N	$\lvert\Delta\rvert$	number of curves
2^{14}	$2^{54}3^{22}11^{22}$	2
2^{16}	$2^{49}3^{22}11^{22}$	2
2^{20}	$2^{54}13^{22}$ $(\times 3)$	6

All are isogenous to non-quadratic twists of Visser's curves, with isogenies hard to find directly.

The end.

Data and code: github.com/AndrewVSutherland/Genus3Covers

Article: arxiv.org/abs/2606.09512 or ANTS website

What about $p = 2$? Optional slide

Fact

The elliptic curve $y^2 = x^3 - n$ has good reduction at 2 if and only if

- $v_2(n) \equiv 4 \bmod 6$, and
- $\frac{n}{2^{v_2(n)}} \equiv 3 \bmod 4$,

where v_2 is the valuation at 2.

Rescaling n such that $v_2(n) = -2$, we note that the 2-adic distance between the four ramification points $\sqrt[3]{n}, \zeta_3\sqrt[3]{n}, \zeta_3^2\sqrt[3]{n}$, and ∞ is $2^{-\frac{2}{3}}$.

Criterion for $p = 2$

Assume E has good reduction, $P_4 = 0_E$, $D' = 2 \cdot 0_E$ and the 2-adic distances between any pair of P_1, P_2, P_3, and P_4 is $2^{-\frac{2}{3}}$. Then, after twisting if necessary, C has good reduction at 2.