

Gluing Genus 1 and Genus 2 Curves along ℓ -torsion

Pitchayut (Mark) Saengrungkongka

MIT

LuCaNT

July 10, 2025

(based on joint work with Noah Walsh)

Let X and Y be curves over \mathbb{Q} .

A **gluing** of X and Y consists of a curve Z and a surjective map

$$\mathrm{Jac} X \times \mathrm{Jac} Y \twoheadrightarrow \mathrm{Jac} Z$$

with finite kernel G .

(Here, $\mathrm{Jac} C$ is a Jacobian of a curve C , which is a g -dimensional group variety parametrizing unordered g -tuple of points, where g is the genus of C .)

Let X and Y be curves over \mathbb{Q} .

A **gluing** of X and Y consists of a curve Z and a surjective map

$$\mathrm{Jac} X \times \mathrm{Jac} Y \twoheadrightarrow \mathrm{Jac} Z$$

with finite kernel G .

(Here, $\mathrm{Jac} C$ is a Jacobian of a curve C , which is a g -dimensional group variety parametrizing unordered g -tuple of points, where g is the genus of C .)

If $G \subseteq \mathrm{Jac}(X)[\ell] \times \mathrm{Jac}(Y)[\ell]$, then we say that the gluing is **along ℓ -torsion**.

We are interested in the case where

- X is an elliptic curve,
- Y has genus 2, and
- ℓ is prime,

in which case the resulting gluing will have genus 3 (i.e., $1 + 2 = 3$).

We will discuss two results.

- 1 Given a genus 2 curve Y , we describe a framework to search for ℓ and X for which we can produce a gluing over \mathbb{Q} .
- 2 We describe a improved algorithm to compute gluing Z .

These allow us to find X and Y and glue them along 13-torsion. 😎

👉 **Recall.** $\text{Jac}(X)[\ell] \simeq \mathbb{F}_\ell^2$ and $\text{Jac}(Y)[\ell] \simeq \mathbb{F}_\ell^4$. Both are equipped with the bilinear alternating **Weil pairing**.

Not all subgroups $G \subset \text{Jac}(X)[\ell] \times \text{Jac}(Y)[\ell]$ lead to a gluing because the quotient must respect the Weil pairing.

👉 **Recall.** $\text{Jac}(X)[\ell] \simeq \mathbb{F}_\ell^2$ and $\text{Jac}(Y)[\ell] \simeq \mathbb{F}_\ell^4$. Both are equipped with the bilinear alternating **Weil pairing**.

Not all subgroups $G \subset \text{Jac}(X)[\ell] \times \text{Jac}(Y)[\ell]$ lead to a gluing because the quotient must respect the Weil pairing.

Hanselman-Schiavone-Sijsling: this means that G must be a **maximal isotropic subgroup**, which is parametrized by

- a one-dimensional subgroup $H \subset \text{Jac}(Y)[\ell]$
- a antisymplectic isomorphism $\text{Jac}(X)[\ell] \rightarrow H^\perp/H$.

There are $\approx \ell^6$ such subgroups, each of them produce a gluing over $\overline{\mathbb{Q}}$.

Gluability Criteria 🤔

It's very rare to get a gluing over \mathbb{Q} .

Hanselman-Schiavone-Sijsling: we need

- a **$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable** one-dimensional subgroup $H \subset \mathrm{Jac}(Y)[\ell]$
- a **$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -equivariant** antisymplectic isomorphism $\mathrm{Jac}(X)[\ell] \rightarrow H^\perp/H$.

Gluability Criteria 🤔

It's very rare to get a gluing over \mathbb{Q} .

Hanselman-Schiavone-Sijsling: we need

- a **$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable** one-dimensional subgroup $H \subset \text{Jac}(Y)[\ell]$
- a **$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -equivariant** antisymplectic isomorphism $\text{Jac}(X)[\ell] \rightarrow H^\perp/H$.

Our 3-step workflow.

- 1 Find ℓ for which there exists a one-dimensional $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable subgroup $H \subset \text{Jac}(Y)[\ell]$.
- 2 Find X such that $\text{Jac}(X)[\ell] \simeq H^\perp/H$ (as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module).
- 3 Check that the isomorphism in (2) is antisymplectic.

Running Example

We will demonstrate our workflow with Y being the curve 277.a.277.1 in the LMFDB:

$$y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x,$$


which has conductor $N_Y = 277$.

Running Example

We will demonstrate our workflow with Y being the curve 277.a.277.1 in the LMFDB:

$$y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x,$$

which has conductor $N_Y = 277$.

 **Recall.** For any prime p at which Y has a good reduction, there exists Frobenius element $\text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that

- acts like $(x : y : z) \mapsto (x^p : y^p : z^p) \pmod{p}$;
- acts on $\text{Jac}(Y)[\ell] \simeq \mathbb{F}_\ell^4$ with a degree 4 characteristic polynomial congruent mod ℓ to the **Frobenius Polynomial** $F_{Y,p}(T) \in \mathbb{Z}[T]$, independent of ℓ .

Frobenius polynomials are easy to compute.

Step 1. Finding Primes ℓ 🐼

Condition 1

There exists one-dimensional $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable subgroup $H \subset \text{Jac}(Y)[\ell]$.

Let p be a prime at which Y has a good reduction.

- If H exists, then Frob_p acts on H by multiplying by some number $\chi(p) \in \mathbb{F}_\ell^\times$, which must be a root of $F_{Y,p}(T)$ modulo ℓ .
- χ must be a Dirichlet character with conductor dividing 277.
- Thus, $\chi(p)^{276} = 1$, so $F_{Y,p}(T)$ and $T^{276} - 1$ must have common root modulo ℓ .
- This already restricts possible ℓ 's to a finite set 🐼. Repeating this test for several p gives $\boxed{\ell \in \{3, 5\}}$.

Let's assume that we are looking for **gluing along 5-torsion** for now ➡.

Step 2. Finding Elliptic Curves X

Condition 2

$\text{Jac}(X)[\ell] \simeq H^\perp/H$ (as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module).

We first understand H better.

From last slide:

- Frob_p acts on H by multiplying by some number $\chi(p) \in \mathbb{F}_\ell^\times$, which must be a root of $F_{Y,p}(T)$ modulo ℓ .
- χ must be a Dirichlet character with conductor dividing 277.

Out of all characters with conductor dividing 277, we eliminate ones which $\chi(p)$ is not a root of $F_{Y,p}(T)$ (modulo ℓ). Repeat this for several p 's.

Eventually, we are left with $\chi = \chi_{\text{triv}}$. In particular, Frob_p fixes H for any prime p .

(In general, χ may be nontrivial, but this process will very likely result in only one candidate χ corresponding to each H .)

Step 2. Finding Elliptic Curves X

Condition 2

$\text{Jac}(X)[\ell] \simeq H^\perp/H$ (as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module).

Note that Frob_p acts on

- H by multiplication by $\chi(p)$;
- $\text{Jac}(Y)[\ell]/H^\perp$ by multiplication by $p/\chi(p)$.

The remaining two eigenvalues must come from H^\perp/H .

Step 2. Finding Elliptic Curves X

Condition 2

$\text{Jac}(X)[\ell] \simeq H^\perp/H$ (as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module).

Note that Frob_p acts on

- H by multiplication by $\chi(p)$;
- $\text{Jac}(Y)[\ell]/H^\perp$ by multiplication by $p/\chi(p)$.

The remaining two eigenvalues must come from H^\perp/H .

Example

In our curve and $p = 19$:

$$\begin{aligned} F_{Y,19}(T) &= x^4 + x^3 - 22x^2 + 19x + 361 \\ &\equiv (x-1)(x-4)(x^2 - x + 4) \pmod{5}. \end{aligned}$$

Thus, we know that **the trace of Frob_{19} in $\text{Jac}(X)[\ell]$ is $1 \pmod{5}$.**

Step 2. Finding Elliptic Curves X

Condition 2

$\text{Jac}(X)[\ell] \simeq H^\perp/H$ (as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module).

For all p , we know what the trace of Frob_p in X must be (modulo ℓ).

Out of all elliptic curves in the LMFDB, there are 4 curves that satisfy our trace constraints for all $p \leq 100$:

1939.b1 18559.a1 21883.b1 32963.c1

By modularity, there is an (impractical 🤖) algorithm to verify the isomorphism.

Step 3. Symplectic Test

Condition 3

The isomorphism in condition 2 is anti-symplectic.

Freitas and Kraus: if Frob_p acts on $X[\ell]$ by a matrix conjugate to

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix},$$

then we can use this Frob_p to check whether the isomorphism is anti-symplectic.

We adapt this test and run it on our four candidates.

1939.b1 18559.a1 21883.b1 32963.c1

Step 3. Symplectic Test

Condition 3

The isomorphism in condition 2 is anti-symplectic.

Freitas and Kraus: if Frob_p acts on $X[\ell]$ by a matrix conjugate to

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix},$$

then we can use this Frob_p to check whether the isomorphism is anti-symplectic.

We adapt this test and run it on our four candidates.


1939.b1 ~~18559.a1~~  21883.b1 32963.c1

Right now we have 3 candidates that can be glued along 5-torsion to $277.a.277.1$.

1939.b1 21883.b1 32963.c1

Right now we have 3 candidates that can be glued along 5-torsion to $277.a.277.1$.

1939.b1 21883.b1 32963.c1

All of them produce a gluing .

Elliptic Curve	Resulting Gluing
1939.b1	$88189x^4 - 398531x^3y + 7700x^3z - 678120x^2y^2 + 1444780x^2yz$ $+ 231034x^2z^2 + 238603xy^3 - 1620885xy^2z = 0$
21883.b1	$y^2 = 448x^8 + 3584x^7 + 2016x^6 - 476x^5 - 13020x^4$ $- 16408x^3 - 18340x^2 - 8988x - 4025$
32963.c1	$19351616x^4 + 136748535x^3y + 106394158x^3z$ $- 235515177x^2y^2 - 46043175x^2yz + 67674485x^2z^2$ $- 549641282xy^3 + 36999650xy^2z - 160500711xyz^2$ $- 36439076xz^3 + 272167382y^4 + 488584945y^3z$ $- 488728851y^2z^2 + 152950443yz^3 - 115190535z^4 = 0$

Original algorithm (by Hanselman, Schiavone, Sijsling):

- Enumerate all $\approx \ell^6$ subgroups G .
- For each subgroup, compute the quotient $(\text{Jac}(X) \times \text{Jac}(Y))/G$ as a lattice in \mathbb{C}^6 .
- Reconstruct the curve and check if it is defined over \mathbb{Q} .

Problem. ℓ^6 is too slow. 🤔

Original algorithm (by Hanselman, Schiavone, Sijsling):

- Enumerate all $\approx \ell^6$ subgroups G .
- For each subgroup, compute the quotient $(\text{Jac}(X) \times \text{Jac}(Y))/G$ as a lattice in \mathbb{C}^6 .
- Reconstruct the curve and check if it is defined over \mathbb{Q} .

Problem. ℓ^6 is too slow. 🐢

But we can improve! 😊

- For each one-dimensional subgroup $H \subseteq \text{Jac}(Y)[\ell]$, check if it is $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable
 - by computing coordinates in \mathbb{C} and rational-recognize its minimal polynomial.
- Enumerate all antisymplectic isomorphisms $\phi : \text{Jac}(X)[\ell] \xrightarrow{\sim} H^\perp/H$. Then, use it to construct G .

$\approx \ell^3$ check in each step, so profit! 🎉

(Not including curve reconstruction)

	$\ell = 3$	$\ell = 5$	$\ell = 7$
Original	144.5 s	5760 s	(not attempted)
Fast	11.8 s	71.9 s	241 s

13-Gluing 🤖

The current list of genus 2 curves in the LMFDB is not enough to produce (interesting) gluing along 13-torsion.

We use Sutherland's database and found the following 🔥:

$$X : \quad y^2 + y = x^3 + x^2 - 208x - 1256 \quad 75.a1$$

$$Y : \quad y^2 + x^3y = -5x^4 + 45x^2 + 9x.$$

(Y has conductor 151 875.)

A gluing along 13-torsion of X and Y is

$$\begin{aligned} Z : y^2 = & 1008x^8 - 4032x^7 + 336x^6 + 8064x^5 + 9660x^4 \\ & - 4914x^3 - 7434x^2 - 2478x + 2058. \end{aligned}$$

13-Gluing 🤖

The current list of genus 2 curves in the LMFDB is not enough to produce (interesting) gluing along 13-torsion.

We use Sutherland's database and found the following 🔥:

$$X : \quad y^2 + y = x^3 + x^2 - 208x - 1256 \quad 75.a1$$

$$Y : \quad y^2 + x^3y = -5x^4 + 45x^2 + 9x.$$

(Y has conductor 151 875.)

A gluing along 13-torsion of X and Y is

$$\begin{aligned} Z : y^2 = & 1008x^8 - 4032x^7 + 336x^6 + 8064x^5 + 9660x^4 \\ & - 4914x^3 - 7434x^2 - 2478x + 2058. \end{aligned}$$

Questions ?