Gluing curves along their torsion

Jeroen Sijsling
Universität Ulm

joint work with
Jeroen Hanselman (Ulm) and Sam Schiavone (MIT)

Arithmetic, Geometry, Cryptography and Coding Theory
Centre International de Rencontres Mathématiques
31 May 2021

Motivation

This Monday morning talk is really about

$$1 + 2 = 3.$$

Motivation

This Monday morning talk is really about

$$1 + 2 = 3.$$

As a warm-up, we will first consider the simpler equality

$$1 + 1 = 2.$$

Motivation

This Monday morning talk is really about

$$1 + 2 = 3.$$

As a warm-up, we will first consider the simpler equality

$$1 + 1 = 2.$$

But in what context?

Motivation

Theorem (Poincaré Reducibility)

Let A be an abelian variety over a field k. Then A is isogenous to a product

$$A \sim B_1^{d_1} \times \cdots \times B_n^{d_n}$$

with $B_1, \ldots, B_n$ simple and pairwise non-isogenous over k.

Motivation

Theorem (Poincaré Reducibility)

Let A be an abelian variety over a field k. Then A is isogenous to a product

$$A \sim B_1^{d_1} \times \cdots \times B_n^{d_n}$$

with $B_1, \ldots, B_n$ simple and pairwise non-isogenous over k.

We are interested in the case where $A = \mathrm{Jac}(Z)$ (resp. $B_i = \mathrm{Jac}(Y_i)$) is the Jacobian of a curve Z (resp. Y_i) over k; this yields arithmetic information on Z in terms of curves Y_i of curves of smaller genus.

General decomposition (by cheating)

$$\mathrm{Jac}(Z) = A \rightsquigarrow B_1^{d_1} \times \cdots \times B_n^{d_n}$$

General decomposition (by cheating)

$$\mathrm{Jac}(Z) = A \rightsquigarrow B_1^{d_1} \times \cdots \times B_n^{d_n}$$

If k is a number field, then results by Costa–Mascot–S–Voight (2017) make it possible to determine this decomposition if its factors B_i are of small dimension.

General decomposition (by cheating)

$$\mathrm{Jac}(Z) = A \rightsquigarrow B_1^{d_1} \times \cdots \times B_n^{d_n}$$

If k is a number field, then results by Costa–Mascot–S–Voight (2017) make it possible to determine this decomposition if its factors B_i are of small dimension.

- Determine $\mathrm{End}(A)$ heuristically by calculating the period matrix of Z;

General decomposition (by cheating)

$$\mathrm{Jac}(Z) = A \rightsquigarrow B_1^{d_1} \times \cdots \times B_n^{d_n}$$

If k is a number field, then results by Costa–Mascot–S–Voight (2017) make it possible to determine this decomposition if its factors B_i are of small dimension.

- Determine $\mathrm{End}(A)$ heuristically by calculating the period matrix of Z;
- Find idempotents $e_i \in \mathrm{End}(A) \otimes \mathbb{Q}$;
- Determine the period matrix of $B_i = e_i A$ and reconstruct Y_i with $\mathrm{Jac}(Y_i) = B_i$ (perhaps over an extension of k);
- Verify the existence of a correspondence between Z and Y_i.

$1 + 1 = 2$: Gluing

$$\mathrm{Jac}(Z) = A \rightsquigarrow B_1^{d_1} \times \cdots \times B_n^{d_n}$$

$1 + 1 = 2$: Gluing

$$\mathrm{Jac}(Z) \rightsquigarrow E_1 \times E_2$$

$1 + 1 = 2$: Gluing

$$\mathrm{Jac}(Z) \rightsquigarrow E_1 \times E_2$$

Theorem (Frey–Kani, 1991)

Let E_1, E_2 be elliptic curves over k, and let $N > 1$ be an integer. If there is a Galois-equivariant anti-symplectic isomorphism

$$\varphi : E_1[N] \xrightarrow{\sim} E_2[N]$$

then let $G \subset (E_1 \times E_2)[N]$ be the graph of φ. Generically, there is a curve Z of genus 2 over k such that

$$E_1 \times E_2 \sim (E_1 \times E_2)/G \cong \mathrm{Jac}(Z).$$

$1 + 1 + 1 = 3$: Gluing

$$\mathrm{Jac}(Z) \rightsquigarrow E_1 \times E_2 \times E_3$$

- Similarly, Howe–Leprévost–Poonen (2000) find Z of genus 3 over k from E_1, E_2, E_3 and a k-rational maximal isotropic subgroup
$$G \subset (E_1 \times E_2 \times E_3)[2].$$
We again have
$$E_1 \times E_2 \times E_3 \sim (E_1 \times E_2 \times E_3)/G \cong \mathrm{Jac}(Z),$$
this time over $\overline{k}$.
- In this case $Z : F(x^2, y^2, z^2) = 0$ is a Ciani quartic.
- This leads to genus 3 Jacobians with rational torsion of order up to 864.

$3 = 1 + 2$: Decomposition

$$\mathrm{Jac}(Z) \rightsquigarrow \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

Now consider a degree 2 map

$$Z \to X$$

with Z non-hyperelliptic of genus 3 and X of genus 1.

$3 = 1 + 2$: Decomposition

$$\mathrm{Jac}(Z) \rightsquigarrow \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

Now consider a degree 2 map

$$Z \to X$$

with Z non-hyperelliptic of genus 3 and X of genus 1.

- Work by Ritzenthaler–Romagny (2018) furnishes (generically)

  $$\mathrm{Jac}(Z) \sim \mathrm{Jac}(X) \times B$$

  where $B = \mathrm{Jac}(Y)$ is the Jacobian of a curve of genus 2.
- Y can be defined over k if Z admits an equation

  $$Z : x^4 + x^2 g(y, z) + f(y, z)h(y, z) = 0.$$

$1 + 2 = 3$: Gluing

$$\mathrm{Jac}(Z) \rightsquigarrow \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

Theorem (Hanselman–Schiavone–S, 2020)

If $\mathrm{char}(k) \neq 2$, with X (resp. Y) of genus 1 (resp. 2) over k.

$1 + 2 = 3$: Gluing

$$\mathrm{Jac}(Z) \rightsquigarrow \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

Theorem (Hanselman–Schiavone–S, 2020)

If $\mathrm{char}(k) \neq 2$, with X (resp. Y) of genus 1 (resp. 2) over k. One can determine the k-rational indecomposable maximal isotropic subgroups

$$G \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2].$$

$1 + 2 = 3$: Gluing

$$\mathrm{Jac}(Z) \leftsquigarrow \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

Theorem (Hanselman–Schiavone–S, 2020)

If $\mathrm{char}(k) \neq 2$, with X (resp. Y) of genus 1 (resp. 2) over k. One can determine the k-rational indecomposable maximal isotropic subgroups

$$G \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2].$$

Given such a G, one can generically determine (Z, μ) with Z a smooth plane quartic over k and $\mu \in k^*/(k^*)^2$ such that

$$\mathrm{Jac}(X) \times \mathrm{Jac}(Y) \sim (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G \cong \mu * \mathrm{Jac}(Z).$$

Here $*$ denotes the quadratic twist of $\mathrm{Jac}(Z)$ with respect to -1.

Finding G

We first determine the k-rational maximal isotropic subgroups

$$G \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2]$$

that are not a product; given such a group, the quotient

$$(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G$$

is defined over k and principally polarized.

We need to describe $\mathrm{Jac}(X)[2]$ and $\mathrm{Jac}(Y)[2]$.

The group $\mathcal{G}(\mathcal{P})$

To describe $\mathrm{Jac}(X)[2]$, choose a defining equation

$$X : y^2 = p_X,$$

let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \overline{k}$ be the roots of p_X, and let

$$\mathcal{P} = \left\{ P_i = (\alpha_i, 0) \in X(\overline{k}) : i \in \{1, \ldots, 4\} \right\}.$$

The group $\mathcal{G}(\mathcal{P})$

To describe $\mathrm{Jac}(X)[2]$, choose a defining equation

$$X : y^2 = p_X,$$

let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \overline{k}$ be the roots of p_X, and let

$$\mathcal{P} = \left\{ P_i = (\alpha_i, 0) \in X(\overline{k}) : i \in \{1, \ldots, 4\} \right\}.$$

Let $\mathcal{G}(\mathcal{P})$ be the set of subsets $S \subset \mathcal{P}$ of even cardinality up to the equivalence $S \sim S^c$. This is an $\mathbb{F}_2$-vector space under

$$(S_1, S_2) \mapsto S_1 \oplus S_2 = (S_1 \cup S_2) \setminus (S_1 \cap S_2).$$

and admits the symplectic pairing

$$\begin{aligned} \mathcal{G}(\mathcal{P}) \times \mathcal{G}(\mathcal{P}) &\to \mathbb{F}_2 \\ (S_1, S_2) &\mapsto \#(S_1 \cap S_2) \bmod 2. \end{aligned}$$

The group $\mathcal{G}(\mathcal{Q})$

To describe $\mathrm{Jac}(Y)[2]$, choose a defining equation

$$Y : y^2 = p_Y,$$

let $\beta_1, \ldots, \beta_6 \in \overline{k}$ be the roots of p_Y, and let

$$\mathcal{Q} = \left\{ Q_j = (\beta, 0) \in Y(\overline{k}) : j \in \{1, \ldots, 6\} \right\}.$$

Let $\mathcal{G}(\mathcal{Q})$ be the set of subsets $S \subset \mathcal{Q}$ of even cardinality up to the equivalence $S \sim S^c$. This is an $\mathbb{F}_2$-vector space under

$$(S_1, S_2) \mapsto S_1 \oplus S_2 = (S_1 \cup S_2) \setminus (S_1 \cap S_2).$$

and admits the symplectic pairing

$$\begin{aligned} \mathcal{G}(\mathcal{Q}) \times \mathcal{G}(\mathcal{Q}) &\to \mathbb{F}_2 \\ (S_1, S_2) &\mapsto \#(S_1 \cap S_2) \bmod 2. \end{aligned}$$

Interpreting 2-torsion

Proposition

There are symplectic isomorphisms of $\mathbb{F}_2$-vector spaces

$$\mathcal{G}(\mathcal{P}) \xrightarrow{\sim} \mathrm{Jac}(X)[2]$$

and

$$\mathcal{G}(\mathcal{Q}) \xrightarrow{\sim} \mathrm{Jac}(Y)[2].$$

To the equivalence class $\overline{S}$ of a subgroup $S = \{P_1, P_2\}$ with $\#S = 2$ there corresponds the 2-torsion point $[P_1] - [P_2]$.

Interpreting 2-torsion

Proposition

There are symplectic isomorphisms of $\mathbb{F}_2$-vector spaces

$$\mathcal{G}(\mathcal{P}) \xrightarrow{\sim} \mathrm{Jac}(X)[2]$$

and

$$\mathcal{G}(\mathcal{Q}) \xrightarrow{\sim} \mathrm{Jac}(Y)[2].$$

To the equivalence class $\overline{S}$ of a subgroup $S = \{P_1, P_2\}$ with $\#S = 2$ there corresponds the 2-torsion point $[P_1] - [P_2]$.

Proposition

Let $\mathcal{T} \subset \mathcal{Q}$ with $\#\mathcal{T} = 2$ correspond to $H \subset \mathrm{Jac}(Y)[2]$, and let $\mathcal{R} = \mathcal{Q} \setminus \mathcal{T}$. Then there is a canonical symplectic isomorphism

$$\mathcal{G}(\mathcal{R}) \xrightarrow{\sim} H^{\perp}/H.$$

Description of subgroups

Proposition

Giving an indecomposable maximal isotropic subgroup

$$G \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2]$$

is the same as giving a subset $\mathcal{T}$ of $\mathcal{Q}$ of cardinality 2 along with a symplectic isomorphism

$$\ell : \mathcal{G}(\mathcal{P}) \to \mathcal{G}(\mathcal{R}),$$

where $\mathcal{R} = \mathcal{Q} \setminus \mathcal{T}$.

Some Galois theory

Let

$$p = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in k[x]$$

be a monic quartic polynomial with zeros

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4.$$

Then the Galois action on the pairs of roots of p up to complements is described by the cubic resolvent

$$\rho(p) = x^3 - a_2x^2 + (a_1a_3 + 4a_0)x + (4a_0a_2 - a_1^2 - a_0a_3^2),$$

which has zeros

$$\gamma_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4,$$
$$\gamma_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4,$$
$$\gamma_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Galois stability

Theorem

Let $X : y^2 = p_X$ and $Y : y^2 = p_Y$. There exists a k-rational indecomposable maximal isotropic subgroup

$$G \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2]$$

if and only if

1. p_Y admits a quadratic factor q_Y over k;
2. For $r_Y = p_Y/q_Y$ we have that the cubic resolvents $\rho(p_X)$ and $\rho(r_Y)$ have isomorphic splitting fields over k.

Is that it? Not quite...

If our theorem furnishes a group G, then we can form the corresponding quotient

$$Q = (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G.$$

Over $\overline{k}$, this is generically a Jacobian... but not over k.

Is that it? Not quite...

If our theorem furnishes a group G, then we can form the corresponding quotient

$$Q = (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G.$$

Over $\overline{k}$, this is generically a Jacobian... but not over k.

Theorem (Beauville–Ritzenthaler, 2011)

Let Q be a principally polarized abelian threefold over k that is not a product over $\overline{k}$. Then there exists a curve Z over k and a class $\mu \in k^*/(k^*)^2$ such that we have

$$Q \cong \mu * \mathrm{Jac}(Z)$$

where $\mu * \mathrm{Jac}(Z)$ is the quadratic twist of $\mathrm{Jac}(Z)$ with respect to the automorphism -1.

Interpolation

Given X, Y, and G, we want to find (Z, μ) such that

$$Q = (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G \cong \mu * \mathrm{Jac}(Z).$$

We cheat and do this over $\mathbb{C}$ first, by using period lattices.

Interpolation

Given X, Y, and G, we want to find (Z, μ) such that

$$Q = (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G \cong \mu * \mathrm{Jac}(Z).$$

We cheat and do this over $\mathbb{C}$ first, by using period lattices.

If $g = 2$, then given a hyperelliptic defining equation

$$Y : y^2 = p_Y(x)$$

we obtain a distinguished basis of global differentials

$$\mathcal{B} = \{x dx/y, dx/y\}.$$

and hence a distinguished period lattice $\Lambda_{\mathcal{B}} \subset \mathbb{C}^2$.

Interpolation

Given X, Y, and G, we want to find (Z, μ) such that

$$Q = (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G \cong \mu * \mathrm{Jac}(Z).$$

We cheat and do this over $\mathbb{C}$ first, by using period lattices.

If $g = 2$, then given a hyperelliptic defining equation

$$Y : y^2 = p_Y(x)$$

we obtain a distinguished basis of global differentials

$$\mathcal{B} = \{x dx/y, dx/y\}.$$

and hence a distinguished period lattice $\Lambda_{\mathcal{B}} \subset \mathbb{C}^2$.

Proposition

Giving a defining polynomial p_Y for Y is the same as giving a period lattice with symplectic pairing $\Lambda_{\mathcal{B}} \subset \mathbb{C}^2$ such that

$$\mathrm{Jac}(Y) \cong \mathbb{C}^2/\Lambda_{\mathcal{B}}.$$

From lattices to equations

If $g = 3$, then given a ternary defining equation

$$Z : F_Z(x, y, z) = 0 \subset \mathbb{P}^2$$

we obtain the distinguished basis of global differentials

$$\mathcal{B} = \{x dx/(\partial f_Z/\partial y), y dx/(\partial f_Z/\partial y), dx/(\partial f_Z/\partial y)\},$$

where $f_Z(x, y) = F_Z(x, y, 1)$, and hence a distinguished period lattice $\Lambda_{\mathcal{B}} \subset \mathbb{C}^3$.

Proposition

Giving a defining polynomial F_Z for Z up to sign is the same as giving a period matrix with symplectic pairing $\Lambda_{\mathcal{B}} \subset \mathbb{C}^3$ such that

$$\mathrm{Jac}(Z) \cong \mathbb{C}^3/\Lambda_{\mathcal{B}}.$$

Using canonicity 1

Since everything in sight is canonical, we are in business:

1. Take defining equations
$$X : y^2 = x(x-1)(x-\alpha)$$
and
$$Y : y^2 = x(x-1)(x-\beta)(x^2+ax+b)$$
for random values of $\alpha, \beta, a, b \in \mathbb{Z}$. Note that the ordering of the roots also picks out a distinguished G.
2. Determine the lattices Λ_X and Λ_Y (Molin–Neurohr, 2017);
3. Form the overlattice Λ_Z corresponding to G;
4. Construct a Weber model corresponding to Λ_Z;
5. Transform to get the distinguished defining polynomial F_Z corresponding to Λ_Z.

An equation

Doing this for many α, β, a, b gives the following interpolated equation for Z:

$$
\begin{aligned}
&(\alpha^2\beta^2 - \alpha^2\beta - \alpha\beta^2 + \alpha\beta)x^4 \\
&+ (a\alpha^2\beta - a\alpha\beta^2 - a\alpha\beta + a\beta^2 + b\alpha^2 - 2b\alpha\beta + b\beta^2 + \alpha^2\beta - 2\alpha\beta^3 + 2\alpha\beta^2 - 2\alpha\beta + \beta^3)x^2y^2 \\
&+ (-2a\alpha^2\beta^2 + 4a\alpha\beta^2 - 2a\beta^2 - 2b\alpha^2\beta + 2b\alpha\beta^2 + 2b\alpha\beta - 2b\beta^2 - 2\alpha^2\beta^2 + 2\alpha\beta^3 + 2\alpha\beta^2 - 2\beta^3)x^2yz \\
&+ (a\alpha^2\beta^2 - a\alpha\beta^3 - a\alpha\beta^2 + a\beta^3 + b\alpha^2\beta - 2b\alpha\beta^3 + 2b\alpha\beta^2 - 2b\alpha\beta + b\beta^3 + \alpha^2\beta^2 - 2\alpha\beta^3 + \beta^4)x^2z^2 \\
&+ (-a\alpha\beta^2 + a\alpha\beta + a\beta^3 - a\beta^2 - \alpha\beta^2 + \alpha\beta + \beta^4 - \beta^3)y^4 \\
&+ (2a\alpha\beta^3 - 2a\alpha\beta^2 - 2a\beta^3 + 2a\beta^2 - 2b\alpha\beta^2 + 2b\alpha\beta + 2b\beta^3 - 2b\beta^2 + 2\alpha\beta^3 - 2\alpha\beta^2 - 2\beta^4 + 2\beta^3)y^3z \\
&+ (a^2\alpha\beta^3 - a^2\alpha\beta^2 - a^2\beta^3 + a^2\beta^2 + ab\alpha\beta^2 - ab\alpha\beta - ab\beta^3 + ab\beta^2 + a\alpha\beta^3 - a\alpha\beta^2 \\
&\quad - a\beta^4 + a\beta^3 + 4b\alpha\beta^3 - 2b\alpha\beta^2 - 2b\alpha\beta - 2b\beta^4 - 2b\beta^3 + 4b\beta^2)y^2z^2 \\
&+ (2ab\alpha\beta^3 - 2ab\alpha\beta^2 - 2ab\beta^3 + 2ab\beta^2 + 2b^2\alpha\beta^2 - 2b^2\alpha\beta - 2b^2\beta^3 \\
&\quad + 2b^2\beta^2 - 2b\alpha\beta^3 + 2b\alpha\beta^2 + 2b\beta^4 - 2b\beta^3)yz^3 \\
&+ (-ab\alpha\beta^3 + ab\alpha\beta^2 + ab\beta^4 - ab\beta^3 - b^2\alpha\beta^2 + b^2\alpha\beta + b^2\beta^4 - b^2\beta^3)z^4.
\end{aligned}
$$

Now let us go all out!

Using canonicity 2

Since everything in sight is canonical, we are in business!

1. Take defining equations
$$X : y^2 = (x - \alpha_1) \cdots (x - \alpha_4) = p_X$$
and
$$Y : y^2 = (x - \beta_1) \cdots (x - \beta_4)(x^2 + ax + b) = p_Y$$
for random values of $\alpha_i, \beta_j, a, b \in \mathbb{Z}$. Note that the ordering of the roots also picks out a distinguished G.
2. Then perform the same steps as before, sped up with the previous results and some other tricks.

We obtain an algebraic expression for an interpolated curve Z. Its coefficients involve:

- The coefficients of p_X and p_Y;
- Roots of their cubic resolvent.

Verification

We get a closed formula for Z. How to show that it is correct?

Verification

We get a closed formula for Z. How to show that it is correct?

1. The involution on the curve Z is nothing but

$$(x : y : z) \mapsto (-x : y : z)$$

   and we can recover the genus 1 factor X as the corresponding quotient.
2. The genus 2 factor Y can be recovered using the result of Ritzenthaler–Romagny.

This indeed recovers the input factors X and Y . . . up to twist.

Effect of twists

Let $\mu, \nu \in k^*/(k^*)^2$. For curves X and Y of genus 1 and 2, we denote the usual quadratic twists by X_μ and Y_μ. Moreover, for a genus 3 curve $Z : F(x^2, y, z) = 0$ we let

$$Z_\nu : F(\nu x^2, y, z) = 0.$$

Effect of twists

Let $\mu, \nu \in k^*/(k^*)^2$. For curves X and Y of genus 1 and 2, we denote the usual quadratic twists by X_μ and Y_μ. Moreover, for a genus 3 curve $Z : F(x^2, y, z) = 0$ we let

$$Z_\nu : F(\nu x^2, y, z) = 0.$$

Then if

$$\mathrm{Jac}(Z) \sim \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

we have

$$\mu * \mathrm{Jac}(Z) \sim \mathrm{Jac}(X_\mu) \times \mathrm{Jac}(Y_\mu)$$

and

$$\mathrm{Jac}(Z_\nu) \sim \mathrm{Jac}(X) \times \mathrm{Jac}(Y_\nu).$$

Effect of twists

Let $\mu, \nu \in k^*/(k^*)^2$. For curves X and Y of genus 1 and 2, we denote the usual quadratic twists by X_μ and Y_μ. Moreover, for a genus 3 curve $Z : F(x^2, y, z) = 0$ we let

$$Z_\nu : F(\nu x^2, y, z) = 0.$$

Then if

$$\mathrm{Jac}(Z) \sim \mathrm{Jac}(X) \times \mathrm{Jac}(Y)$$

we have

$$\mu * \mathrm{Jac}(Z) \sim \mathrm{Jac}(X_\mu) \times \mathrm{Jac}(Y_\mu)$$

and

$$\mathrm{Jac}(Z_\nu) \sim \mathrm{Jac}(X) \times \mathrm{Jac}(Y_\nu).$$

Combining these statements allows us to algebraically recover twisting scalars μ, ν such that

$$(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G = Q \cong \mu * \mathrm{Jac}(Z_\nu).$$

Summary

What we did:

- Find a group G algebraically;
- Via period matrices and interpolation, construct a curve Z such that

$$(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G = Q \cong \mathrm{Jac}(Z)$$

  up to twist;
- Find μ, ν such that

$$(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))/G = Q \cong \mu * \mathrm{Jac}(Z_\nu)$$

  for real.
- The result is a closed formula valid over any base field k with $\mathrm{char}(k) \neq 2$.

An example

Consider the genus 1 curve defined by the equation

$$X : y^2 = 4x^3 + 5x^2 - 98x + 157 = p_X$$

It has a rational 5-torsion point. Similarly, let

$$Y : y^2 = x^6 + 2x^3 - 4x^2 + 1 = (x^2 + x - 1)(x - 1)(x^3 + 2x + 1).$$

It has a rational 14-torsion point.

If $q_Y = x^2 + x - 1$, then the polynomials p_X and $r_Y = p_Y/q_Y = (x - 1)(x^3 + 2x + 1)$ have the same cubic resolvent, which yields a group G.

An example

Given G, our algorithms directly furnish

$$Z : 32x^4+3x^2y^2-132x^2yz+37x^2z^2+3y^4-14y^3z+7y^2z^2-6yz^3-2z^4 = 0$$

and $\mu = 5^3$.

Because there is a degree-8 isogeny

$$\mathrm{Jac}(X) \times \mathrm{Jac}(Y) \to Q = \mu * \mathrm{Jac}(Z)$$

we see that Q has a rational 35-torsion point. Closer analysis shows that it has a rational 70-torsion point as well, since

$$(\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[2]/G$$

contains a rational point.

Geometry

Over $\overline{k}$ there is an alternative procedure to recover Z:

Theorem (Hanselman–Schiavone–S, 2020)

Let $\mathrm{Kum}(Y)^{\mathrm{t}} = \mathrm{Jac}(Y)^{\mathrm{t}}/\langle -1 \rangle \subset \mathbb{P}^3_k$ be the Kummer of $\mathrm{Jac}(Y)^{\mathrm{t}}$. Then over $\overline{k}$ there is a cartesian diagram

$$\begin{array}{ccc} Z & \xrightarrow{i_Z} & \mathrm{Jac}(Y)^{\mathrm{t}} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \pi} \\ X & \xrightarrow[i_X]{} & \mathrm{Kum}(Y)^{\mathrm{t}}. \end{array}$$

where i_X is a rational map of degree 1 such that

$$i_X(X) = H \cap \mathrm{Kum}(Y)^{\mathrm{t}}$$

for a plane $H \subset \mathbb{P}^3_k$ through two singular points of $\mathrm{Kum}(Y)^{\mathrm{t}}$.