Superspecial Cryptography

Computing Isogenies Between Elliptic Products

Giacomo Pope
SIAM (AG23) — TU/e Eindhoven

NCC Group
University of Bristol

I have brilliant friends

Isogeny Friends

- Rémy Oudompheng
- Chloe Martindale
- Luciano Maino
- Lorenz Panny
- Damien Robert
- Sabrina Kunzweiler
- Pierrick Dartois
- Many other people!

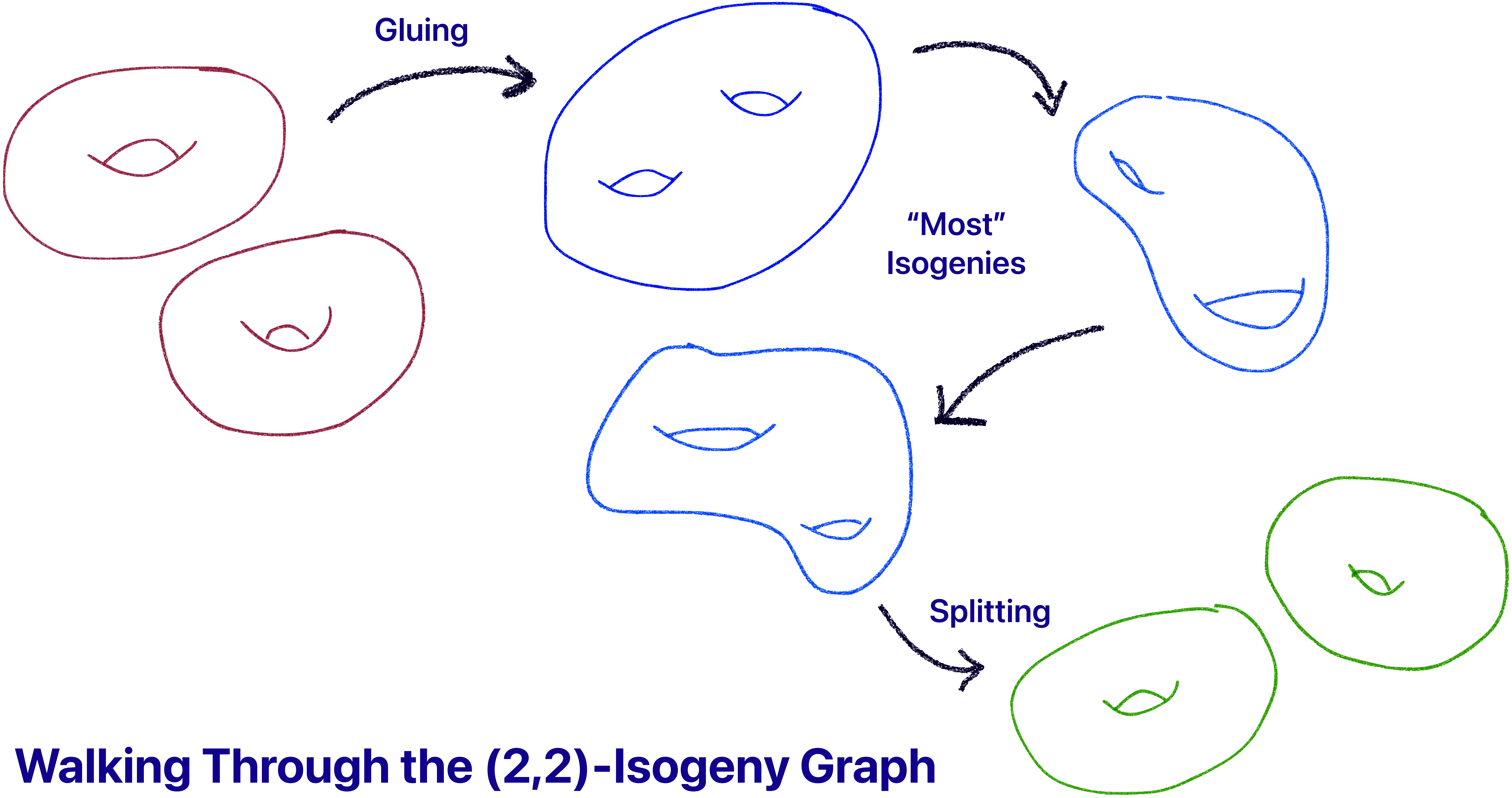
What's the Plan?

- What is an isogeny between elliptic products?
- How are we asking computers to calculate these maps?
- An open puzzle: a magical square root.

What is an isogeny between elliptic products?

Superspecial Abelian Varieties

- A generalisation of supersingular curves
- In dimension two, we have **two distinct** nodes on our graph
- In characteristic p we have approximately
  - Jacobians of hyperelliptic curves (~p^3 nodes)
  - Products of elliptic curves (~p^2 nodes)



Walking Through the (2,2)-Isogeny Graph

Jacobians of Hyperelliptic Curves

- A **hyperelliptic curve** is a generalisation of an **elliptic curve**
- The **Jacobian** of the hyperelliptic curve is where we find our group
- The **Divisor** of a Jacobian is our group element
- The **Mumford representation** of a divisor is a pair of polynomials

- $C : y^2 = f(x)$ $\qquad$ $\deg(f) = 2g + 2$
- $D = (u(x), v(x)) \in \textbf{Jac}(C)$ $\qquad$ $\deg(v) < \deg(u) \leq g$

Jacobians of Hyperelliptic Curves

- A **hyperelliptic curve** is a generalisation of an **elliptic curve**
- The **Jacobian** of the hyperelliptic curve is where we find our group
- The **Divisor** of a Jacobian is our group element
- The **Mumford representation** of a divisor is a pair of polynomials

- $C : y^2 = x^6 + 73x^5 + 144x^4 + 18x^3 + 151x^2 + 20x + 80 \mod 163$
- $(u, v) = \left(x^2 + 14x + 113,\ 0\right)$

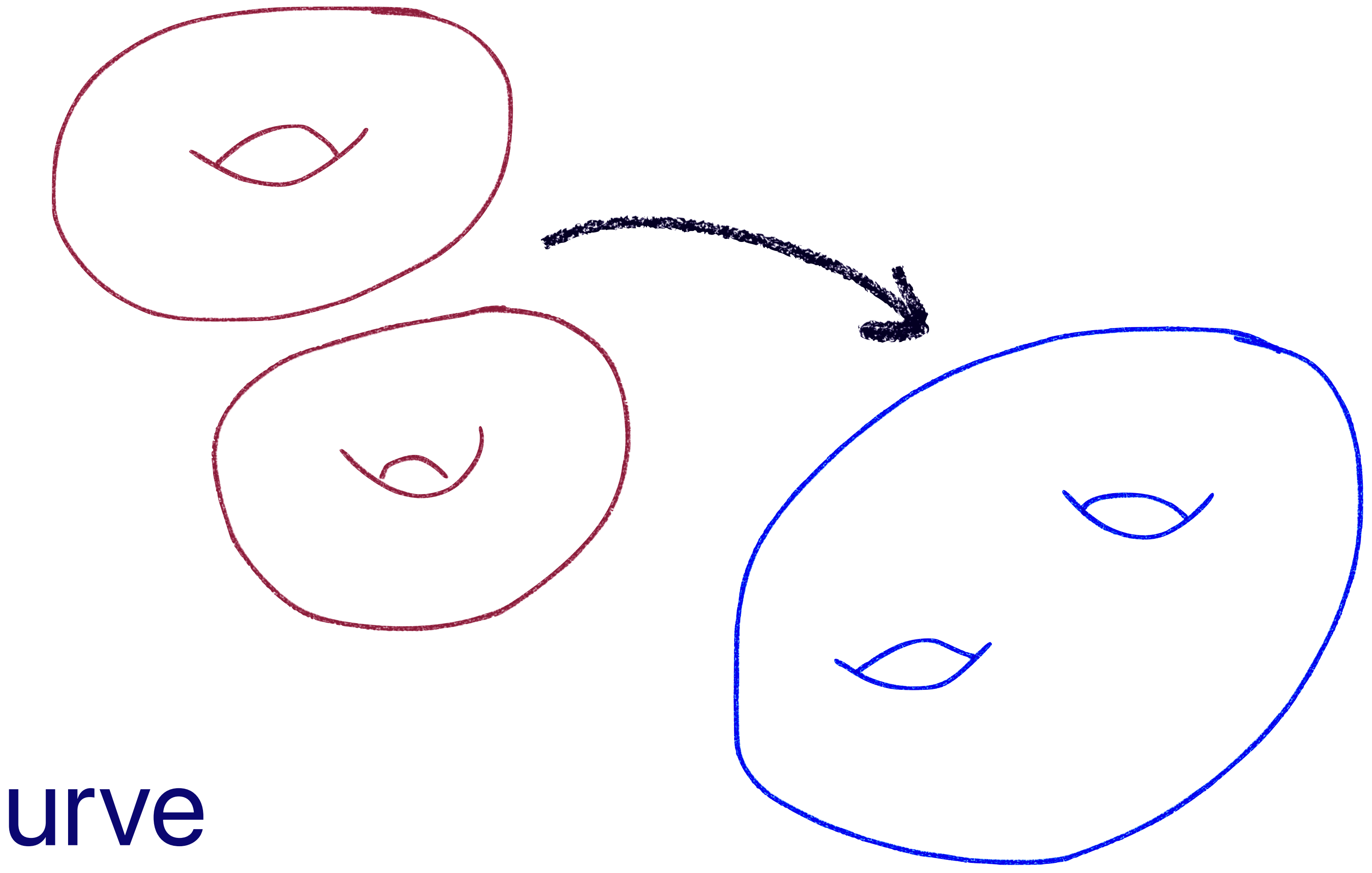
Jacobians of Hyperelliptic Curves

- A **hyperelliptic curve** is a generalisation of an **elliptic curve**
- The **Jacobian** of the hyperelliptic curve is where we find our group
- The **Divisor** of a Jacobian is our group element
- The **Mumford representation** of a divisor is a pair of polynomials

- $C : y^2 = (x^2 + 14x + 113)(x^2 + 84x + 12)(x^2 + 138x + 152) \mod 163$
- $(u, v) = \left(x^2 + 14x + 113,\ 0\right)$

How can we compute these isogenies?

Gluing Elliptic Products



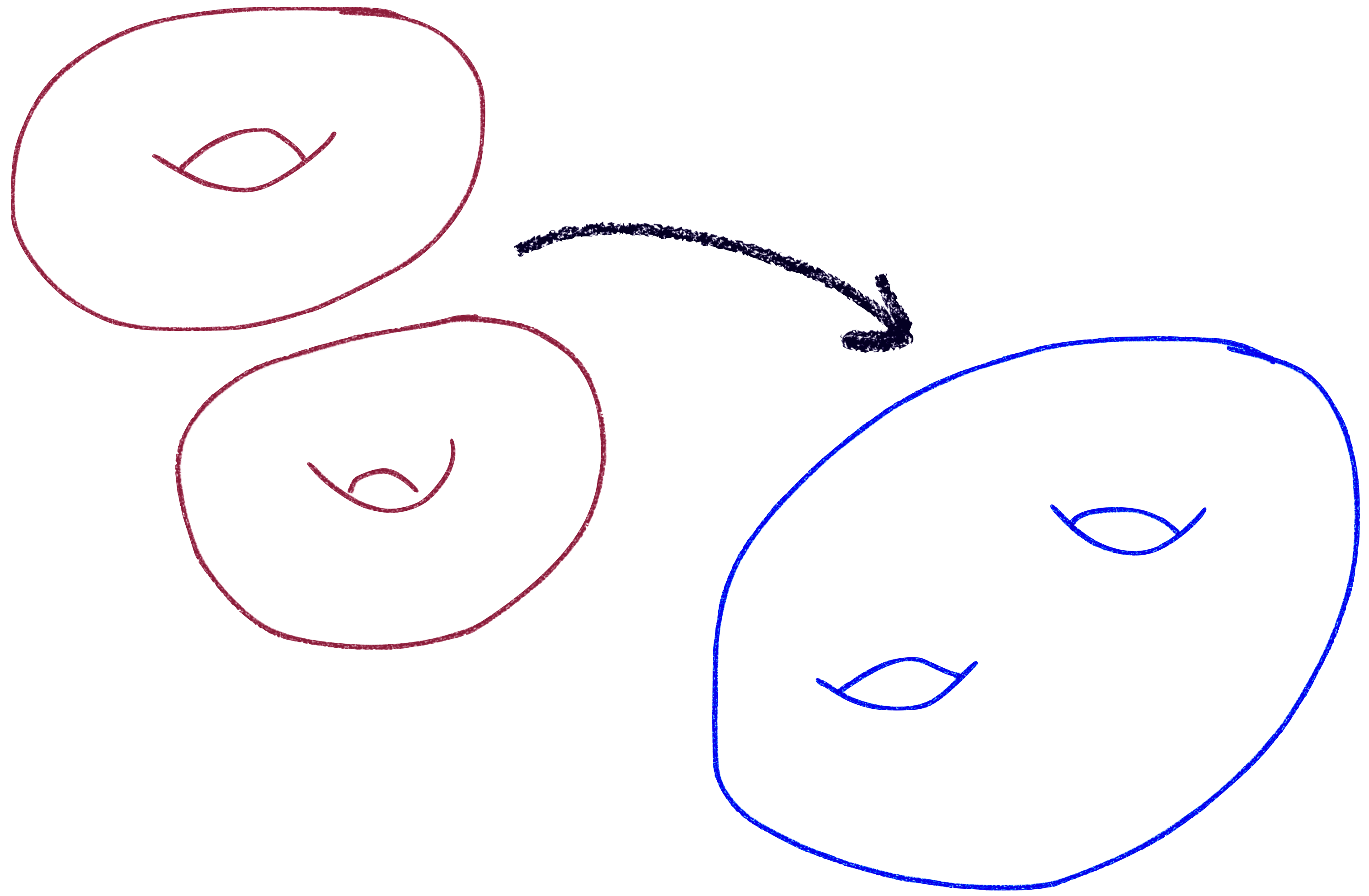
- Given two elliptic curves, find the isogenous hyperelliptic curve
- The gluing isogeny can also be understood as a bijection of roots

$$E_1 : y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad \ker(\gamma) = \langle (P_1, P_2), (Q_1, Q_2) \rangle \subset E_1 \times E_2$$

$$E_2 : y^2 = (x - b_1)(x - b_2)(x - b_3) \qquad \{a_1, a_2, a_3\} \to \{b_1, b_2, b_3\}$$

$$H : y^2 = s_1(x^2 - \alpha_1)(x^2 - \alpha_2)(x^2 - \alpha_3) \qquad \alpha_i = \frac{b_j - b_k}{a_j - a_k}$$

Gluing Montgomery Curves



- Gluing Montgomery curves is particularly beautiful
- Codomain can be computed in only 7 multiplications and 1 inversion

$$E_1 : y^2 = x(x-a)(x-a^{-1})$$
$$E_2 : y^2 = x(x-b)(x-b^{-1})$$

$$H : y^2 = s_1(x^2-\alpha_1)(x^2-\alpha_2)(x^2-\alpha_3)$$

$$\alpha_1 = \frac{b-b^{-1}}{a-a^{-1}} \quad \alpha_2 = \frac{a}{b} \quad \alpha_3 = \frac{b}{a} \qquad s_1 = \frac{a-1/a}{a/b-b/a}$$

Pushing through points

Jacobian Arithmetic

Doubling: 32M + 6S + 1I
Addition: 25M + 4S + 1I

- Given a pair of points, compute the isogenous divisor

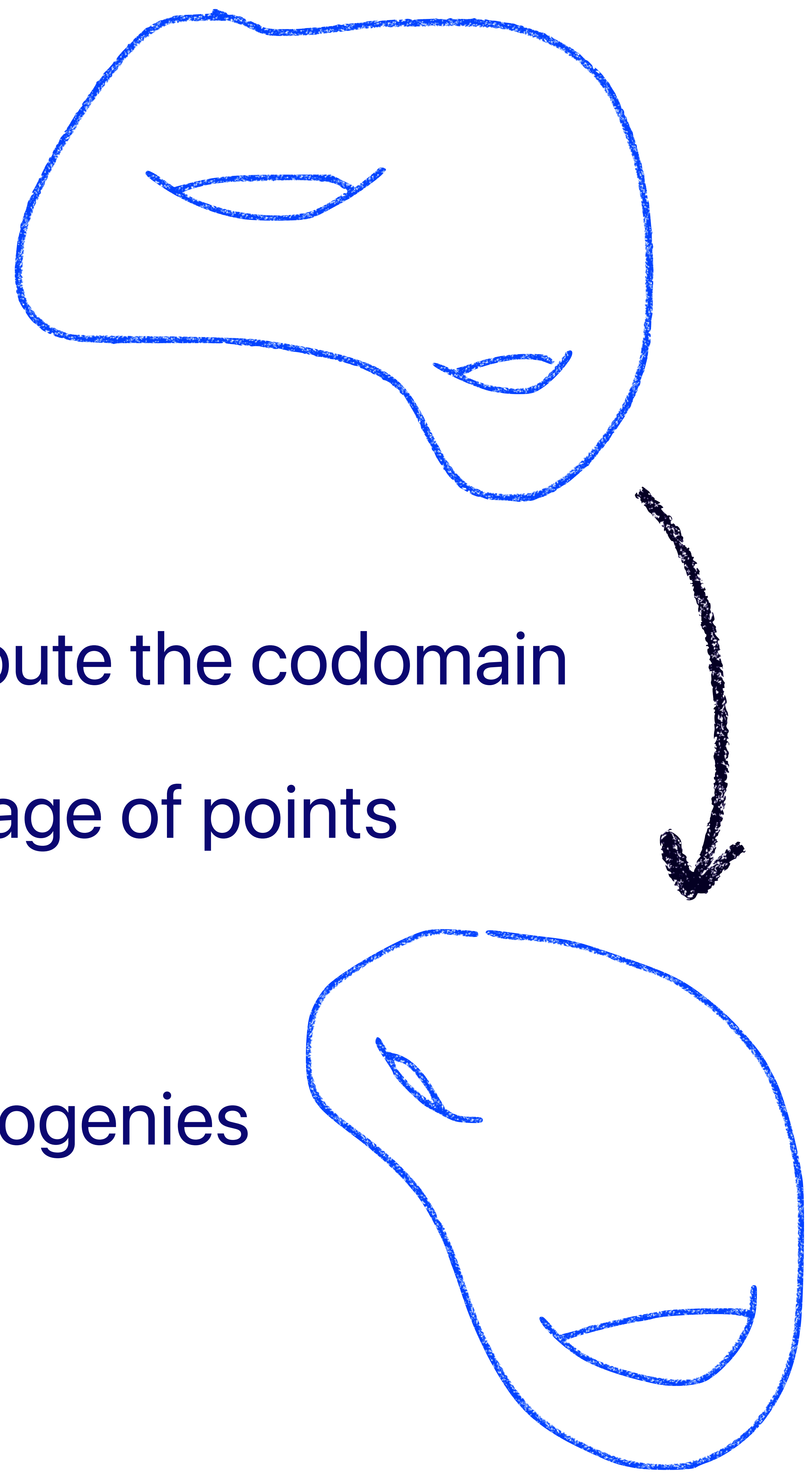
$$(P, Q) \in E_1 \times E_2$$
$$\gamma(P, Q) = \gamma(P, \mathcal{O}_{E_2}) + \gamma(\mathcal{O}_{E_1}, Q)$$

$$H \to E_1 : (x, y) \mapsto (s_1 x + s_2, s_1 y)$$
$$H \to E_2 : (x, y) \mapsto (s_2/x^2 + s_1, s_2 y/x^3)$$

$$u_P = x^2 + (s_2 - P_x)/s_1,$$
$$v_P = P_y/s_1,$$

$$u_Q = x^2 - s_2/(Q_x - s_1),$$
$$v_Q = xQ_y/(Q_x - s_1)\,.$$

Mapping between Jacobians



- A (2,2)-isogeny is a very **special** map!
- In **1842**, Richelot showed there are compact formula to compute the codomain
- The **Richelot correspondence** allows us to compute the image of points
- Some recent progress by Sabrina Kunzweiler (2022/990)
- I believe there's interesting work in further optimising these isogenies

Richelot's Codomain

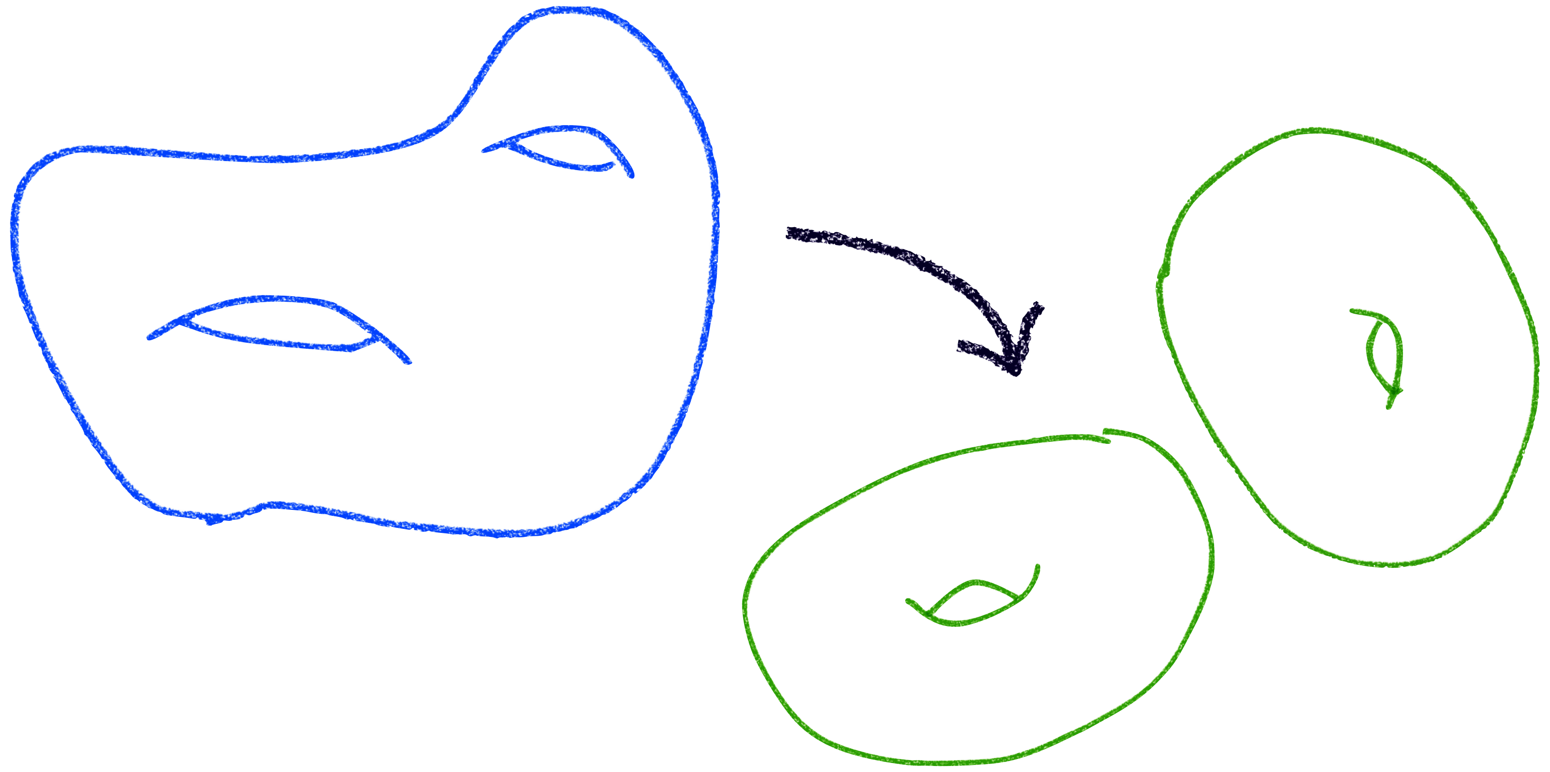
- Our kernel is determined by two quadratic polynomials

$$C_1 : y^2 = f(x) = G_1 G_2 G_3, \quad \ker(\varphi) = \langle (G_1, 0), (G_2, 0) \rangle, \qquad G_i = g_{i,2} x^2 + g_{i,1} x + g_{i,0}$$

- Codomain computation cost: 20M 1I

$$D = \begin{vmatrix} g_{1,0} & g_{1,1} & g_{1,2} \\ g_{2,0} & g_{2,1} & g_{2,2} \\ g_{3,2} & g_{3,1} & g_{3,2} \end{vmatrix} \qquad H_i = D^{-1} \left(G_j' G_k - G_k' G_j \right) \qquad \varphi : C_1 \to C_2 : y^2 = H_1 H_2 H_3$$

Splitting to Elliptic Products



- Given a hyperelliptic curve, recover the isogenous product of elliptic curves
- **Method:** find a coordinate transformation to make this "easy"

$$\theta : x \mapsto \frac{\alpha_1 x + \alpha_0}{\beta_1 x + \beta_0} \qquad \tilde{C} : y^2 = c_3 x^6 + c_2 x^4 + c_1 x^2 + c_0$$

$$(x^2, y) \mapsto (X, Y) \qquad E_1 : Y^2 = c_3 X^3 + c_2 X^2 + c_1 X + c_0$$

$$(x^{-2}, yx^{-3}) \mapsto (U, V) \qquad E_2 : V^2 = c_0 U^3 + c_1 U^2 + c_2 U + c_3$$

Computing the Isomorphism

$$\theta : x \mapsto \frac{\alpha_1 x + \alpha_0}{\beta_1 x + \beta_0}$$

- Once we have our isomorphism, splitting is very natural
- Uncovering the isomorphism is where the work is
- A splitting to an elliptic product is revealed when the determinant vanishes

$$G_3 = \kappa_1 G_1 + \kappa_2 G_2$$

$$D = \begin{vmatrix} g_{1,0} & g_{1,1} & g_{1,2} \\ g_{2,0} & g_{2,1} & g_{2,2} \\ g_{3,2} & g_{3,1} & g_{3,2} \end{vmatrix} = 0$$

$$\ker(\sigma) = \langle (G_1, 0), (G_2, 0) \rangle$$

- The isomorphism can be set by removing linear terms from G_1 and G_2

A Magical Formula

$$\sqrt{\mathrm{Res}(G_1, G_2)} = \left(\frac{N_1 + N_2}{N_1 - N_2}\right)(b_1 - b_2)$$

A Magical Formula

$$\Phi \;:\; E_1 \times E_2 \to E_0 \times F$$

$$\phi_i \;:\; E_0 \to E_i$$

$$N_i = \deg(\phi_i)$$

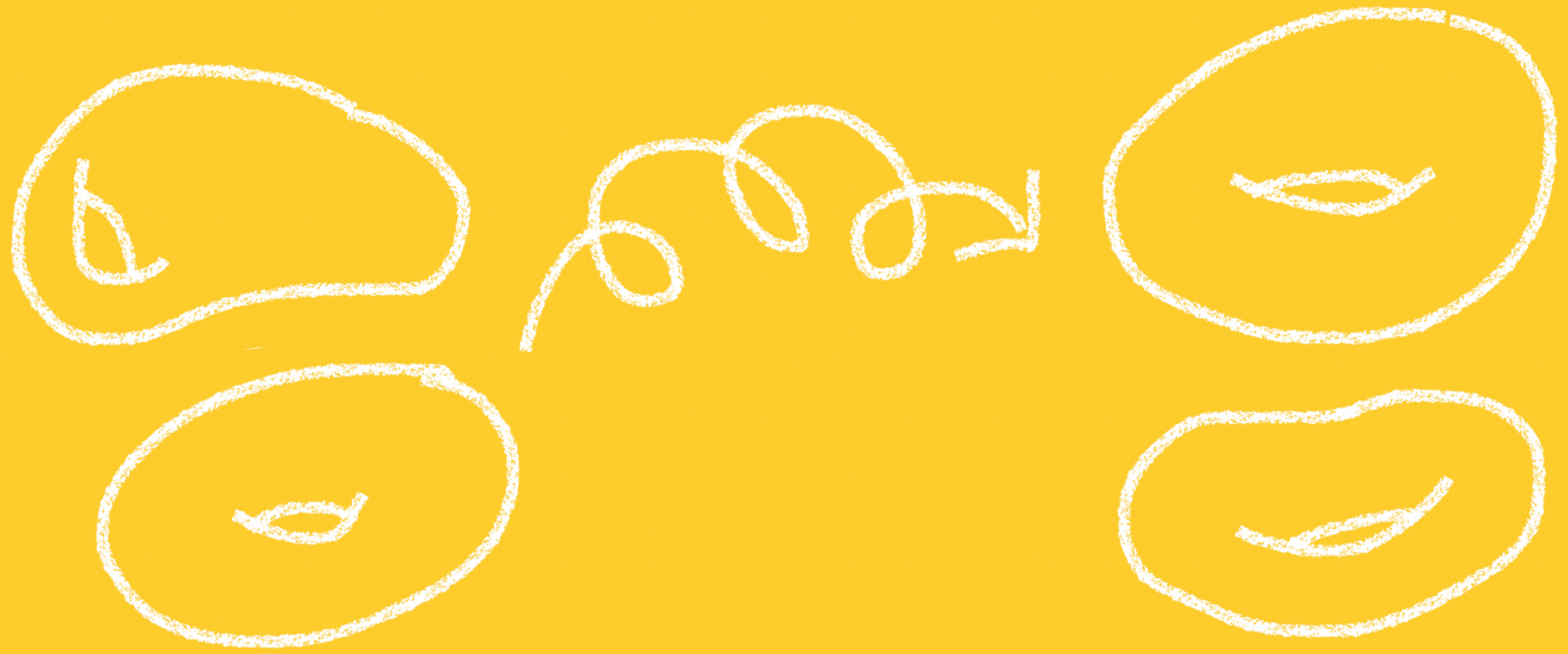
Isogeny Diamond

$$\ker(\sigma) = \langle (G_1, 0), (G_2, 0) \rangle$$

$$G_i = x^2 + a_i x + b_i$$

Splitting Isogeny

$$\sqrt{\mathrm{Res}(G_1, G_2)} = \left(\frac{N_1 + N_2}{N_1 - N_2}\right)(b_1 - b_2)$$



Thank You