Models of principally polarized abelian varieties and isogenies

Algorithmic Number Theory Symposium (ANTS XVII)

Sabrina Kunzweiler

Introduction

Principally polarized abelian varieties (p.p.a.v.) in this talk:

Isogenies in this talk:

Introduction

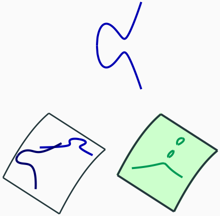
Principally polarized abelian varieties (p.p.a.v.) in this talk:

- dimension 1: Elliptic curves

Isogenies in this talk:

Introduction

Principally polarized abelian varieties (p.p.a.v.) in this talk:



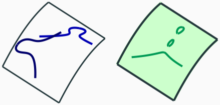
- dimension 1: Elliptic curves
- dimension 2: Products of elliptic curves, Jacobians of genus-2 curves

Isogenies in this talk:

Introduction

Principally polarized abelian varieties (p.p.a.v.) in this talk:

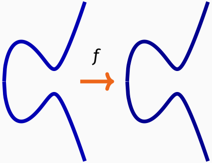
- dimension 1: Elliptic curves



- dimension 2: Products of elliptic curves, Jacobians of genus-2 curves

Isogenies in this talk:

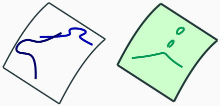
- dimension 1: 2-isogenies and 3-isogenies



Introduction

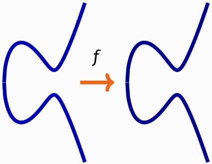
Principally polarized abelian varieties (p.p.a.v.) in this talk:

- dimension 1: Elliptic curves



- dimension 2: Products of elliptic curves, Jacobians of genus-2 curves

Isogenies in this talk:

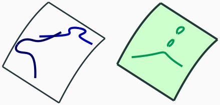


- dimension 1: 2-isogenies and 3-isogenies
- dimension 2: $(2,2)$-isogenies and $(3,3)$-isogenies

Introduction

Principally polarized abelian varieties (p.p.a.v.) in this talk:

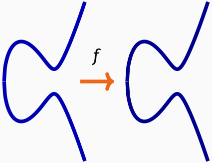
- dimension 1: Elliptic curves



- dimension 2: Products of elliptic curves, Jacobians of genus-2 curves

Isogenies in this talk:

- dimension 1: 2-isogenies and 3-isogenies
- dimension 2: $(2,2)$-isogenies and $(3,3)$-isogenies



Key idea: Work on models with symmetries to obtain easy formulas.

Main motivation: Isogeny-based cryptography

Isogeny-based cryptography

- Candidate for post-quantum cryptography
- Hardness assumption: Given two isogenous (superspecial) p.p.a.v. A, B over some finite field $\mathbb{F}_{p^k}$, it is hard to find an isogeny $f : A \to B$.

(startup: Alice & Bob)

Main motivation: Isogeny-based cryptography

Isogeny-based cryptography

- Candidate for post-quantum cryptography
- Hardness assumption: Given two isogenous (superspecial) p.p.a.v. A, B over some finite field $\mathbb{F}_{p^k}$, it is hard to find an isogeny $f : A \to B$.
- parameter sizes (exemplary): $p, \deg(f) \approx 2^{256}$

(startup: Alice & Bob)

Main motivation: Isogeny-based cryptography

Isogeny-based cryptography

- Candidate for post-quantum cryptography
- Hardness assumption: Given two isogenous (superspecial) p.p.a.v. A, B over some finite field $\mathbb{F}_{p^k}$, it is hard to find an isogeny $f : A \to B$.
- parameter sizes (exemplary): $p, \deg(f) \approx 2^{256}$

(startup: Alice & Bob)

Computing an isogeny of degree N

- General algorithms: Quasi-linear in N

Main motivation: Isogeny-based cryptography

Isogeny-based cryptography

- Candidate for post-quantum cryptography
- Hardness assumption: Given two isogenous (superspecial) p.p.a.v. A, B over some finite field $\mathbb{F}_{p^k}$, it is hard to find an isogeny $f : A \to B$.
- parameter sizes (exemplary): $p, \deg(f) \approx 2^{256}$

(startup: Alice & Bob)

Computing an isogeny of degree N

- General algorithms: Quasi-linear in N
- Composition of small degree isogenies: faster e.g. $O(\log N \log \log N)$ when $N = \ell^n$ for some small ℓ

this talk: building blocks for such isogeny chains

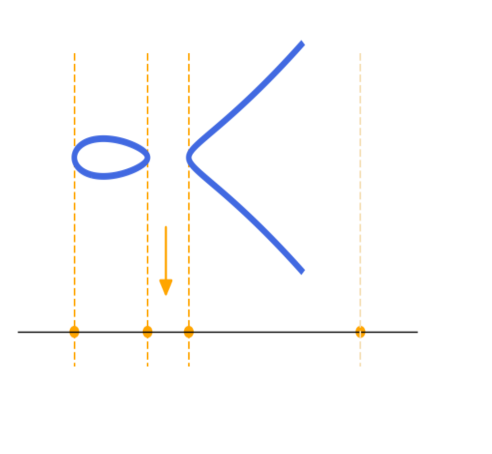
Kummer varieties and 2-isogenies ($\mathrm{char}(k) \neq 2$)

Elliptic curves

Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

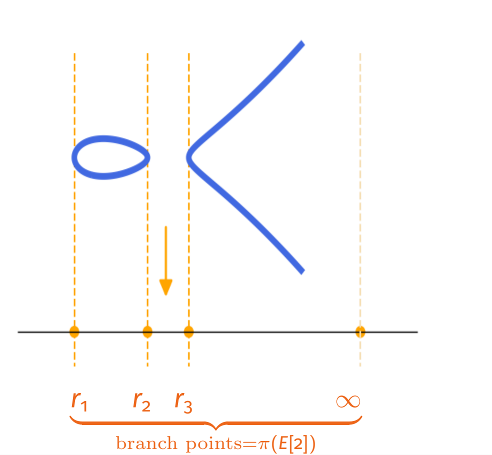
Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

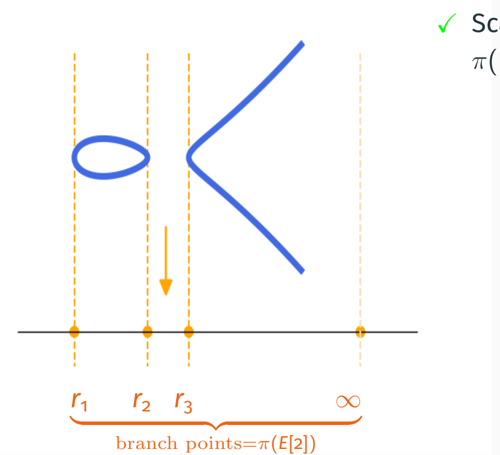
Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



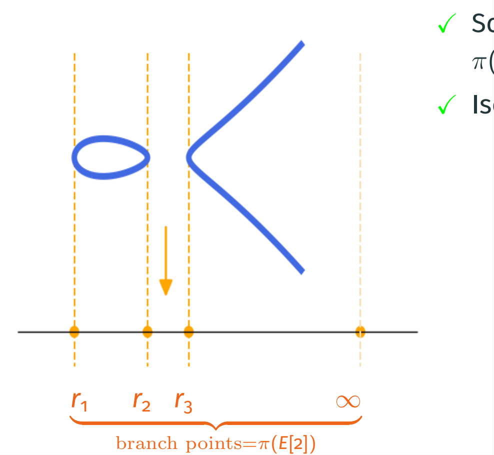
Reminiscents of the group structure

✓ Scalar multiplication:
$\pi([N](\pm P)) = \pi(\pm[N]P)$

Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



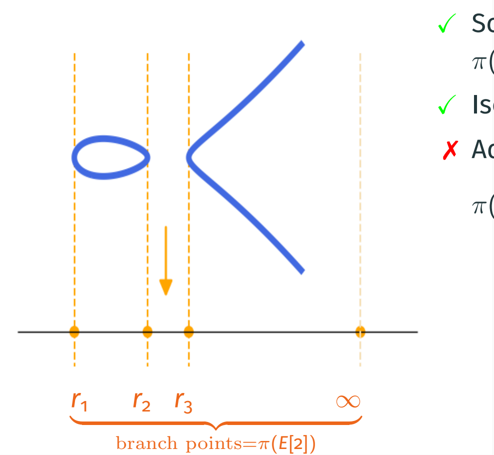
Reminiscents of the group structure

- ✓ Scalar multiplication: $\pi([N](\pm P)) = \pi(\pm [N]P)$
- ✓ Isogenies

Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



Reminiscents of the group structure

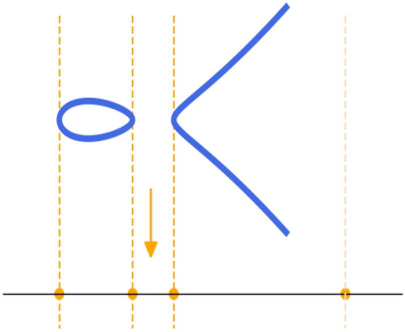
- ✓ Scalar multiplication:
  $\pi([N](\pm P)) = \pi(\pm [N]P)$
- ✓ Isogenies
- ✗ Addition

$$\pi(P) + \pi(Q) \stackrel{?}{=} \begin{cases} \pi(P + Q) \\ \pi(P - Q) \end{cases}$$

Kummer line

Elliptic curve: $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$.

Projection to the Kummer line: $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$



Reminiscents of the group structure

- ✓ Scalar multiplication:
  $\pi([N](\pm P)) = \pi(\pm[N]P)$
- ✓ Isogenies
- ✗ Addition
  $$\pi(P) + \pi(Q) \stackrel{?}{=} \begin{cases} \pi(P+Q) \\ \pi(P-Q) \end{cases}$$
- ✓ Addition by 2-torsion points: well defined since
  $\pi(P+Q) = \pi(P-Q)$ for $Q \in E[2]$

  given by linear transformations since Kummer coordinates x, z are a basis for $L(2\mathcal{O})$.

Normalizing the action of 2-torsion points

Setting: Legendre form $E : y^2 = x(x-1)(x-\lambda)$,
Kummer map $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$.

Normalizing the action of 2-torsion points

Setting: Legendre form $E : y^2 = x(x-1)(x-\lambda)$,
Kummer map $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$.

Translation by 2-torsion points

$E[2] = \langle P_1 = (0, 0), Q_1 = (1, 0) \rangle$
For $\pi(P) = (x : z) \in K$:

$\pi(P + P_1) = (\lambda z : x)$,
$\pi(P + Q_1) = (x - \lambda z : x - z)$

Normalizing the action of 2-torsion points

Setting: Legendre form $E : y^2 = x(x-1)(x-\lambda)$,
Kummer map $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x,y) \mapsto x$.

Translation by 2-torsion points

$E[2] = \langle P_1 = (0,0), Q_1 = (1,0) \rangle$

For $\pi(P) = (x : z) \in K$:

$\pi(P + P_1) = (\lambda z : x)$, $\quad \rightsquigarrow T_{P_1} = \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$

$\pi(P + Q_1) = (x - \lambda z : x - z)$ $\quad \rightsquigarrow T_{Q_1} = \begin{pmatrix} 1 & -\lambda \\ 1 & -1 \end{pmatrix}$

$\rightsquigarrow$ action of $\langle T_{P_1}, T_{Q_1} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on $K \cong \mathbb{P}^1$.

Normalizing the action of 2-torsion points

Setting: Legendre form $E : y^2 = x(x-1)(x-\lambda)$,
Kummer map $\pi : E \to K = E/\langle \pm 1 \rangle \cong \mathbb{P}^1,\ (x, y) \mapsto x$.

Translation by 2-torsion points

$E[2] = \langle P_1 = (0, 0), Q_1 = (1, 0) \rangle$

For $\pi(P) = (x : z) \in K$:

$\pi(P + P_1) = (\lambda z : x)$, $\quad \rightsquigarrow T_{P_1} = \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$

$\pi(P + Q_1) = (x - \lambda z : x - z)$ $\quad \rightsquigarrow T_{Q_1} = \begin{pmatrix} 1 & -\lambda \\ 1 & -1 \end{pmatrix}$

$\rightsquigarrow$ action of $\langle T_{P_1}, T_{Q_1} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on $K \cong \mathbb{P}^1$.

Normalizing the action:

Find change of coordinates $(\tilde{x} : \tilde{z}) = (\alpha x + \beta z : \gamma x + \delta z)$ so that

$$T_{\tilde{P}_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } T_{\tilde{Q}_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Then $(\tilde{x} : \tilde{z}) = (\theta_0 : \theta_1)$ are **level-2 theta coordinates** for E.

(see Mumford's "Equations Defining Abelian Varieties")

Properties of level-2 theta model (dimension 1)

Setting $(E, \mathcal{O})$ with $E[2] = \langle P_1, Q_1 \rangle$; and Kummer coordinates $(\theta_0 : \theta_1)$ with normalized action by P_1, Q_1.

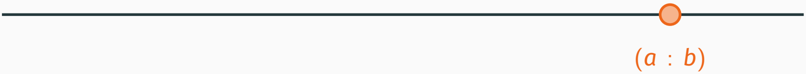
$$T_{P_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, T_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Properties of level-2 theta model (dimension 1)

Setting $(E, \mathcal{O})$ with $E[2] = \langle P_1, Q_1 \rangle$; and Kummer coordinates $(\theta_0 : \theta_1)$ with normalized action by P_1, Q_1.

$$T_{P_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, T_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- The point $(a : b) := (\theta_0(\mathcal{O}) : \theta_1(\mathcal{O}))$ is called the **theta null point**.

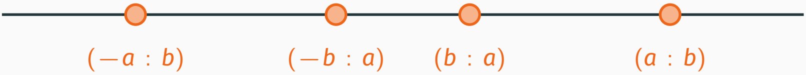


Properties of level-2 theta model (dimension 1)

Setting $(E, \mathcal{O})$ with $E[2] = \langle P_1, Q_1 \rangle$; and Kummer coordinates $(\theta_0 : \theta_1)$ with normalized action by P_1, Q_1.

$$T_{P_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, T_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- The point $(a : b) := (\theta_0(\mathcal{O}) : \theta_1(\mathcal{O}))$ is called the **theta null point**.
- Non-trivial 2-**torsion points**:
  - $(\theta_0(P_1) : \theta_1(P_1)) = T_{P_1} \circ (a : b) = (b : a)$
  - $(\theta_0(Q_1) : \theta_1(Q_1)) = T_{Q_1} \circ (a : b) = (-a : b)$
  - $(\theta_0(P_1 + Q_1) : \theta_1(P_1 + Q_1)) = (T_{P_1} \cdot T_{Q_1}) \circ (a : b) = (-b : a)$

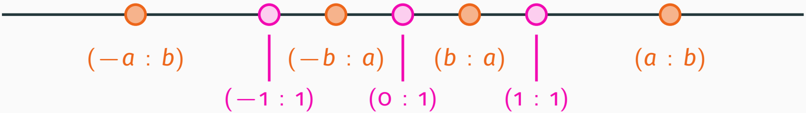


Properties of level-2 theta model (dimension 1)

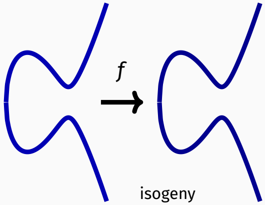
Setting $(E, \mathcal{O})$ with $E[2] = \langle P_1, Q_1 \rangle$;
and Kummer coordinates $(\theta_0 : \theta_1)$
with normalized action by P_1, Q_1.

$$T_{P_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, T_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- The point $(a : b) := (\theta_0(\mathcal{O}) : \theta_1(\mathcal{O}))$ is called the **theta null point**.
- Non-trivial **2-torsion points**:
  - $(\theta_0(P_1) : \theta_1(P_1)) = T_{P_1} \circ (a : b) = (b : a)$
  - $(\theta_0(Q_1) : \theta_1(Q_1)) = T_{Q_1} \circ (a : b) = (-a : b)$
  - $(\theta_0(P_1 + Q_1) : \theta_1(P_1 + Q_1)) = (T_{P_1} \cdot T_{Q_1}) \circ (a : b) = (-b : a)$
- Special **4-torsion points**: $E[4] = \langle P_1', Q_1' \rangle$
  - $[2] \cdot P_1' = P_1 \to (\theta_0(P_1') : \theta_1(P_1')) = (1 : 1)$ or $(-1 : 1)$
  - $[2] \cdot Q_1' = Q_1 \to (\theta_0(Q_1') : \theta_1(Q_1')) = (0 : 1)$ or $(1 : 0)$



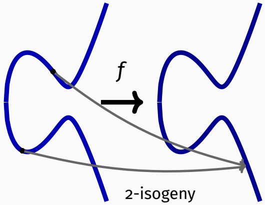
2-isogenies of Kummer lines



An **isogeny** is a nonzero morphism of elliptic curves $f : E \to E'$ with $f(\mathcal{O}) = \mathcal{O}'$.

*abuse of notation for points on the Kummer

2-isogenies of Kummer lines

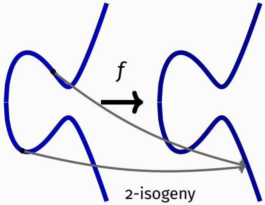


An **isogeny** is a nonzero morphism of elliptic curves $f : E \to E'$ with $f(\mathcal{O}) = \mathcal{O}'$.

A 2-**isogeny** is an isogeny of degree 2 with kernel $G \cong \mathbb{Z}/2\mathbb{Z}$.

*abuse of notation for points on the Kummer

2-isogenies of Kummer lines



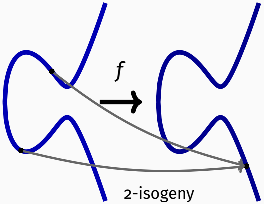
An **isogeny** is a nonzero morphism of elliptic curves $f : E \to E'$ with $f(\mathcal{O}) = \mathcal{O}'$.

A 2-**isogeny** is an isogeny of degree 2 with kernel $G \cong \mathbb{Z}/2\mathbb{Z}$.

$\Rightarrow$ induces a rational map of the Kummer lines $f : K \to K'$

*abuse of notation for points on the Kummer

2-isogenies of Kummer lines



An **isogeny** is a nonzero morphism of elliptic curves $f : E \to E'$ with $f(\mathcal{O}) = \mathcal{O}'$.

A 2**-isogeny** is an isogeny of degree 2 with kernel $G \cong \mathbb{Z}/2\mathbb{Z}$.

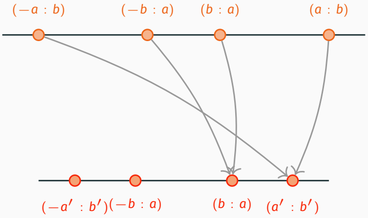
$\Rightarrow$ induces a rational map of the Kummer lines $f : K \to K'$

Illustration (level-2 theta-model)

$f : K \to K'$ with kernel

$G = \langle P_2 \rangle =^* \langle (-a : b) \rangle$

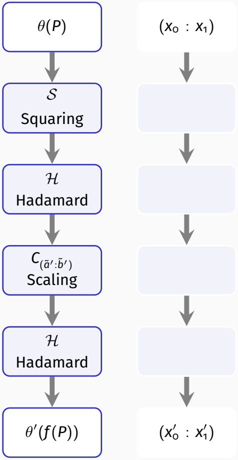
- $f((a : b)) = f((-a : b))$
  $=: (a' : b')$
- $f((b : a)) = f((-b : a))$
  $\in \{(-a' : b'), (b' : a'), (-b' : a')\}$.



*abuse of notation for points on the Kummer

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

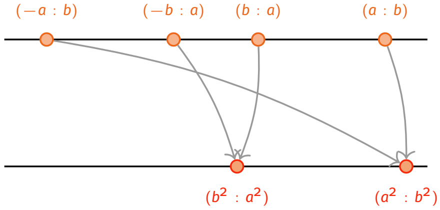


Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

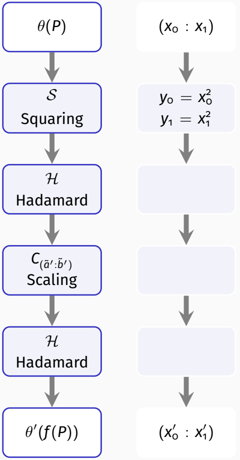
$\theta(P)$	$(x_0 : x_1)$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$ $y_1 = x_1^2$
$\mathcal{H}$ Hadamard	
$C_{(\tilde{a}' : \tilde{b}')}$ Scaling	
$\mathcal{H}$ Hadamard	
$\theta'(f(P))$	$(x_0' : x_1')$

Step 1: $\mathcal{S}$ (squaring)

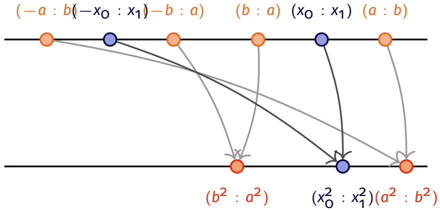


Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.



Step 1: $\mathcal{S}$ (squaring)



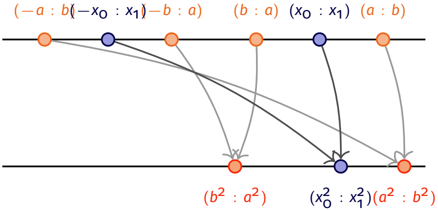
$\Rightarrow \mathcal{S}(X + Q_1) = \mathcal{S}(X)$ for all $X = (x_0 : x_1)$.
$\mathcal{S}$ is an “isogeny” with $\ker(\mathcal{S}) = \langle Q_1 \rangle$

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\downarrow$	$\downarrow$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$, $y_1 = x_1^2$
$\downarrow$	$\downarrow$
$\mathcal{H}$ Hadamard	
$\downarrow$	$\downarrow$
$C_{(\tilde{a}' : \tilde{b}')}$ Scaling	
$\downarrow$	$\downarrow$
$\mathcal{H}$ Hadamard	
$\downarrow$	$\downarrow$
$\theta'(f(P))$	$(x'_0 : x'_1)$

Step 1: $\mathcal{S}$ (squaring)



$\Rightarrow$ $\mathcal{S}(X + Q_1) = \mathcal{S}(X)$ for all $X = (x_0 : x_1)$.
$\mathcal{S}$ is an "isogeny" with $\ker(\mathcal{S}) = \langle Q_1 \rangle$

$\Rightarrow$ $\mathcal{S}(X + P_1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathcal{S}(X)$ for all X
Action of $\mathcal{S}(P_1)$ is normalized.

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\downarrow$	$\downarrow$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$ $y_1 = x_1^2$
$\downarrow$	$\downarrow$
$\mathcal{H}$ Hadamard	
$\downarrow$	$\downarrow$
$C_{(\tilde{a}' : \tilde{b}')}$ Scaling	
$\downarrow$	$\downarrow$
$\mathcal{H}$ Hadamard	
$\downarrow$	$\downarrow$
$\theta'(f(P))$	$(x_0' : x_1')$

Steps 2-4: Linear transformation M to normalize 2-torsion action:

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$ $y_1 = x_1^2$
$\mathcal{H}$ Hadamard	
$C_{(\tilde{a}' : \tilde{b}')}$ Scaling	
$\mathcal{H}$ Hadamard	
$\theta'(f(P))$	$(x_0' : x_1')$

Steps 2-4: Linear transformation M to normalize 2-torsion action:

- $\mathcal{S}(P_1)$ is in normal form, hence $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot M = \pm M \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$, $y_1 = x_1^2$
$\mathcal{H}$ Hadamard	$z_0 = y_0 + y_1$, $z_1 = y_0 - y_1$
$C_{(\tilde{a}':\tilde{b}')}$ Scaling	$w_0 = z_0/\tilde{a}'$, $w_1 = z_1/\tilde{b}'$
$\mathcal{H}$ Hadamard	$x'_0 = w_0 + w_1$, $x'_1 = w_0 - w_1$
$\theta'(f(P))$	$(x'_0 : x'_1)$

Steps 2-4: Linear transformation M to normalize 2-torsion action:

- $\mathcal{S}(P_1)$ is in normal form, hence $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot M = \pm M \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

$$\Rightarrow^{*} \; M = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \text{ for some } \alpha, \beta$$

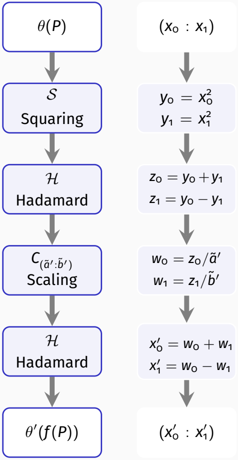
$$= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \alpha+\beta & 0 \\ 0 & \alpha-\beta \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

i.e. $M = \mathcal{H} \circ \mathcal{C}_{(\alpha+\beta:\alpha-\beta)} \circ \mathcal{H}$

[a] We avoid a sign ambiguity by setting $M(1:1) = (1:1)$.

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.



Steps 2-4: Linear transformation M to normalize 2-torsion action:

- $\mathcal{S}(P_1)$ is in normal form, hence $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot M = \pm M \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

$\Rightarrow^*$ $M = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$ for some α, β

$= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \alpha+\beta & 0 \\ 0 & \alpha-\beta \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

i.e. $M = \mathcal{H} \circ \mathcal{C}_{(\alpha+\beta:\alpha-\beta)} \circ \mathcal{H}$

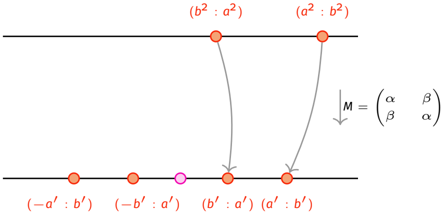
- How to find the scalars α, β?

Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$, $y_1 = x_1^2$
$\mathcal{H}$ Hadamard	$z_0 = y_0 + y_1$, $z_1 = y_0 - y_1$
$C_{(\tilde{a}' : \tilde{b}')}$ Scaling	$w_0 = z_0 / \tilde{a}'$, $w_1 = z_1 / \tilde{b}'$
$\mathcal{H}$ Hadamard	$x'_0 = w_0 + w_1$, $x'_1 = w_0 - w_1$
$\theta'(f(P))$	$(x'_0 : x'_1)$

Computing α, β:



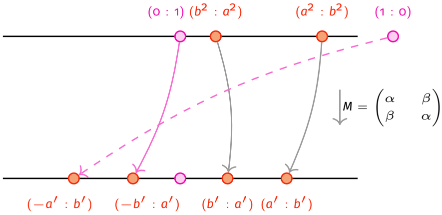
Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.

$\theta(P)$	$(x_0 : x_1)$
$\mathcal{S}$ Squaring	$y_0 = x_0^2$, $y_1 = x_1^2$
$\mathcal{H}$ Hadamard	$z_0 = y_0 + y_1$, $z_1 = y_0 - y_1$
$C_{(\tilde{a}':\tilde{b}')}$ Scaling	$w_0 = z_0/\tilde{a}'$, $w_1 = z_1/\tilde{b}'$
$\mathcal{H}$ Hadamard	$x_0' = w_0 + w_1$, $x_1' = w_0 - w_1$
$\theta'(f(P))$	$(x_0' : x_1')$

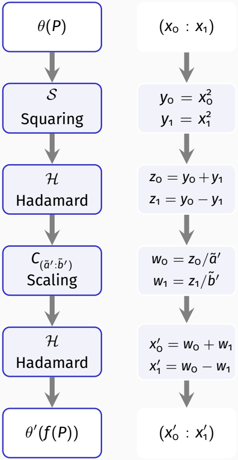
Computing α, β:

- Approach 1: Normalize image of 4-torsion $\to$ sqrt computation !



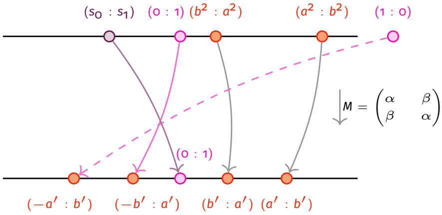
Explicit formulas for a 2-isogeny in the level-2 theta model

Setup: $\theta : E \to \mathbb{P}^1$ elliptic curve with level-2 theta structure.
$f : E \to E'$ a 2-isogeny with $\ker(f) = \langle Q_1 \rangle = \langle (-a : b) \rangle$.



Computing α, β:

- Approach 1: Normalize image of 4-torsion $\to$ sqrt computation !
- Approach 2: Use 8-torsion point $S = (s_1 : s_2)$ $\to$ no sqrts



Remarks on the 2-isogeny formula

Relation of the scalars $(\alpha : \beta)$ with the codomain theta null point $(a' : b')$ and the 8-torsion point $S = (s_0 : s_1)$

- $(\alpha : \beta) = (s_0^2 : -s_1^2) = (a' : -b')$
- Note: $(\alpha - \beta : \alpha + \beta) = (s_0^2 + s_1^2 : s_0^2 - s_1^2) = (\tilde{a}' : \tilde{b}')$ is the *dual theta null point* of the codomain.

Remarks on the 2-isogeny formula

Relation of the scalars $(\alpha : \beta)$ with the codomain theta null point $(a' : b')$ and the 8-torsion point $S = (s_0 : s_1)$

- $(\alpha : \beta) = (s_0^2 : -s_1^2) = (a' : -b')$
- Note: $(\alpha - \beta : \alpha + \beta) = (s_0^2 + s_1^2 : s_0^2 - s_1^2) = (\tilde{a}' : \tilde{b}')$ is the *dual theta null point* of the codomain.

Two kinds of formulas for the isogeny $f : E \to E' = E/\langle Q_1 \rangle$

- Isogeny evaluation in $2S + 2M$ (given S with $4 \cdot S = Q_1$)

$$\theta(P) \xrightarrow{} \underset{\text{Squaring}}{\mathcal{S}} \xrightarrow{} \underset{\text{Hadamard}}{\mathcal{H}} \xrightarrow{} \underset{\text{Scaling}}{C_{(\tilde{a}':\tilde{b}')}} \xrightarrow{} \underset{\text{Hadamard}}{\mathcal{H}} \xrightarrow{} \theta'(f(P))$$

$\Rightarrow$ Computation of 2^n-isogenies with given kernel

Remarks on the 2-isogeny formula

Relation of the scalars $(\alpha : \beta)$ **with the codomain theta null point** $(a' : b')$ **and the** 8**-torsion point** $S = (s_0 : s_1)$

- $(\alpha : \beta) = (s_0^2 : -s_1^2) = (a' : -b')$
- Note: $(\alpha - \beta : \alpha + \beta) = (s_0^2 + s_1^2 : s_0^2 - s_1^2) = (\tilde{a}' : \tilde{b}')$ is the *dual theta null point* of the codomain.

Two kinds of formulas for the isogeny $f : E \to E' = E/\langle Q_1 \rangle$

- Isogeny evaluation in $2S + 2M$ (given S with $4 \cdot S = Q_1$)

$$\theta(P) \to \underset{\text{Squaring}}{\mathcal{S}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \underset{\text{Scaling}}{C_{(\tilde{a}':\tilde{b}')}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \theta'(f(P))$$

  $\Rightarrow$ Computation of 2^n-isogenies with given kernel

- Radical isogeny formula $(a : b) \mapsto (a' : b')$ in $1\mathrm{Sqrt} + 1M + 2S$

$$(a : b) \to \underset{\text{Squaring}}{\mathcal{S}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \underset{\text{Square-Root}}{\mathcal{T}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to (a' : b')$$

  $\Rightarrow$ Exploration of isogeny graphs

Kummer varieties and 2-isogenies (char$(k) \neq 2$)

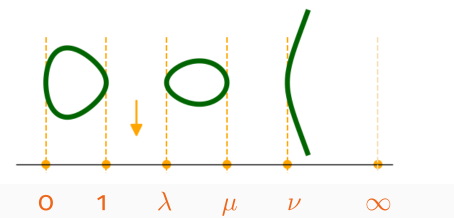
Generalizing to higher dimension

Jacobians of genus-2 curves and 2-torsion

Genus-2 curve in Rosenhain form $C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$

Jacobians of genus-2 curves and 2-torsion

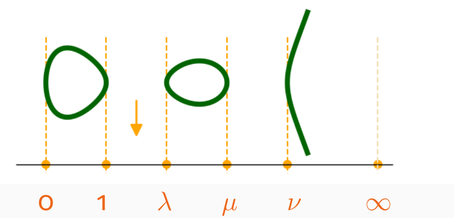
Genus-2 curve in Rosenhain form $C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$



Weierstrass points:
$(0,0), (1,0), (\lambda,0)$
$(\mu,0), (\nu,0), \infty$

Jacobians of genus-2 curves and 2-torsion

Genus-2 curve in Rosenhain form $C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$



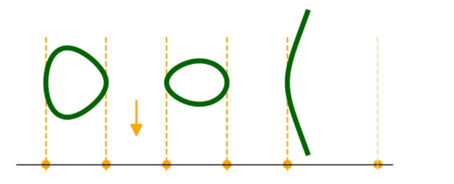
Weierstrass points:
$(0,0), (1,0), (\lambda,0)$
$(\mu,0), (\nu,0), \infty$

- The Jacobian of C, $Jac(C)$, is a principally polarized abelian variety of dimension 2.

$\rightarrow$ Elements $P \in Jac(C)$: $P = [T + S - 2\infty]$ with $T, S \in C$

Jacobians of genus-2 curves and 2-torsion

Genus-2 curve in Rosenhain form $C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$



$0 \quad 1 \quad \lambda \quad \mu \quad \nu \quad \infty$

Weierstrass points:
$(0,0), (1,0), (\lambda,0)$
$(\mu,0), (\nu,0), \infty$

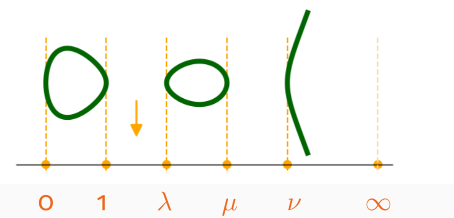
- The Jacobian of C, $Jac(C)$, is a principally polarized abelian variety of dimension 2.

$\rightarrow$ Elements $P \in Jac(C)$: $P = [T + S - 2\infty]$ with $T, S \in C$

2-Torsion points on $Jac(C) \leftrightarrow$ pairs of Weierstrass points
$Jac(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$,

Jacobians of genus-2 curves and 2-torsion

Genus-2 curve in Rosenhain form $C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$



Weierstrass points:
$(0,0), (1,0), (\lambda, 0)$
$(\mu, 0), (\nu, 0), \infty$

- The Jacobian of C, $Jac(C)$, is a principally polarized abelian variety of dimension 2.

$\rightarrow$ Elements $P \in Jac(C)$: $P = [T + S - 2\infty]$ with $T, S \in C$

2-Torsion points on $Jac(C) \leftrightarrow$ pairs of Weierstrass points
$Jac(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$, concretely: $Jac(C)[2] = \langle P_1, P_2, Q_1, Q_2 \rangle$:

- $P_1 = [(0,0) - \infty]$, $\quad P_2 = [(1,0) + (\lambda, 0) - 2\infty]$
- $Q_1 = [(\mu, 0) - \infty]$, $\quad Q_2 = [(1,0) + (\nu, 0) - 2\infty]$

$\Rightarrow$ **symplectic** w.r.t. the Weil pairing

2-torsion on the (Cassels–Flynn) Kummer surface

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

2-torsion on the (Cassels–Flynn) Kummer surface

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

- **Defining Equation** $K \subset \mathbb{P}^3$ (Cassels–Flynn '96): $(x_1^2 - 4x_0x_2)x_3^2 = 2F_1(x_0, x_1, x_2)x_3 - F_0(x_0, x_1, x_2)$

2-torsion on the (Cassels–Flynn) Kummer surface

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

- **Defining Equation** $K \subset \mathbb{P}^3$ (Cassels–Flynn '96): $(x_1^2 - 4x_0x_2)x_3^2 = 2F_1(x_0, x_1, x_2)x_3 - F_0(x_0, x_1, x_2)$
- **Quotient map**: $\pi : Jac(C) \to K$ $[(x_T, y_T) + (x_S, y_S) - 2\infty]$ $\mapsto (1 : x_T + x_S : x_T x_S : y)$, where $y = (f_0(x_T, x_S) - 2y_T y_S)/(x_T - s_S)^2$

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

- **Defining Equation** $K \subset \mathbb{P}^3$ (Cassels–Flynn '96): $(x_1^2 - 4x_0x_2)x_3^2 = 2F_1(x_0, x_1, x_2)x_3 - F_0(x_0, x_1, x_2)$
- **Quotient map**: $\pi : Jac(C) \to K$
  $[(x_T, y_T) + (x_S, y_S) - 2\infty]$
  $\mapsto (1 : x_T + x_S : x_T x_S : y)$, where
  $y = (f_0(x_T, x_S) - 2y_T y_S)/(x_T - s_S)^2$

Image of the 2-torsion points (branch points of $Jac(C) \to K$):

$\pi(P_1) = (0 : 1 : 0 : 0)$,
$\pi(P_2) = (1 : 1 + \lambda : \lambda : \mu\lambda + \nu\lambda)$,
$\pi(Q_1) = (0 : -1 : -\mu : -\mu^2)$,
$\pi(Q_2) = (1 : \nu + 1 : \nu : \mu\nu + \lambda\nu)$

2-torsion on the (Cassels–Flynn) Kummer surface

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

- **Defining Equation** $K \subset \mathbb{P}^3$ (Cassels–Flynn '96): $(x_1^2 - 4x_0x_2)x_3^2 = 2F_1(x_0, x_1, x_2)x_3 - F_0(x_0, x_1, x_2)$
- **Quotient map:** $\pi : Jac(C) \to K$ $[(x_T, y_T) + (x_S, y_S) - 2\infty] \mapsto (1 : x_T + x_S : x_Tx_S : y)$, where $y = (f_0(x_T, x_S) - 2y_Ty_S)/(x_T - s_S)^2$

Image of the 2-torsion points (branch points of $Jac(C) \to K$):

$\pi(P_1) = (0 : 1 : 0 : 0)$,
$\pi(P_2) = (1 : 1 + \lambda : \lambda : \mu\lambda + \nu\lambda)$,
$\pi(Q_1) = (0 : -1 : -\mu : -\mu^2)$,
$\pi(Q_2) = (1 : \nu + 1 : \nu : \mu\nu + \lambda\nu)$

Addition is given by linear transformations T_{P_i}, T_{Q_i}.

$$T_{P_1} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \mu\nu\lambda & 0 & 0 & 0 \\ 0 & \mu\nu\lambda & 0 & 0 \end{pmatrix}$$

2-torsion on the (Cassels–Flynn) Kummer surface

$K = Jac(C)/\langle \pm 1 \rangle$ is called the **Kummer surface**

- **Defining Equation** $K \subset \mathbb{P}^3$ (Cassels–Flynn '96): $(x_1^2 - 4x_0x_2)x_3^2 = 2F_1(x_0, x_1, x_2)x_3 - F_0(x_0, x_1, x_2)$
- **Quotient map**: $\pi : Jac(C) \to K$ $[(x_T, y_T) + (x_S, y_S) - 2\infty]$ $\mapsto (1 : x_T + x_S : x_T x_S : y)$, where $y = (f_0(x_T, x_S) - 2y_T y_S)/(x_T - s_S)^2$

Image of the 2-torsion points (branch points of $Jac(C) \to K$):

$\pi(P_1) = (0 : 1 : 0 : 0)$,
$\pi(P_2) = (1 : 1 + \lambda : \lambda : \mu\lambda + \nu\lambda)$,
$\pi(Q_1) = (0 : -1 : -\mu : -\mu^2)$,
$\pi(Q_2) = (1 : \nu + 1 : \nu : \mu\nu + \lambda\nu)$

$$T_{P_2} = \begin{pmatrix} -\lambda(\mu+\nu) & \lambda & \lambda(\lambda-1) & \lambda \\ \star & \lambda(\mu+\nu) & \star & \lambda+1 \\ \mu\nu(\lambda+1) & \mu\nu\lambda & -\lambda(\mu+\nu) & 1 \\ \star & \mu\nu\lambda(\lambda+1) & \star & \lambda(\mu+\nu) \end{pmatrix}$$

Addition is given by linear transformations T_{P_i}, T_{Q_i}.

($\star$ = longer expression)

Normalizing the action by 2-torsion points (as in Mumford '66)

Find $(\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2 : \tilde{x}_3) = M\,(x_0 : x_1 : x_2 : x_3)$ with $M \in \mathrm{PGL}(4)$ so that

$$T_{\tilde{P}_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T_{\tilde{P}_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_{\tilde{Q}_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \; T_{\tilde{Q}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Normalizing the action by 2-torsion points (as in Mumford '66)

Find $(\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2 : \tilde{x}_3) = M(x_0 : x_1 : x_2 : x_3)$ with $M \in \mathrm{PGL}(4)$ so that

$$T_{\tilde{P}_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T_{\tilde{P}_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_{\tilde{Q}_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad T_{\tilde{Q}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

With $\tilde{O} = (a : b : c : d)$:

- $\tilde{P}_1 = (b : a : d : c)$
- $\tilde{P}_2 = (c : d : a : b)$
- $\tilde{Q}_1 = (a : -b : c : -d)$
- $\tilde{Q}_2 = (a : b : -c : -d)$

The level-2 theta model (dimension 2)

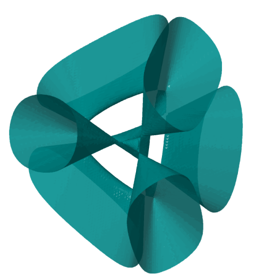
Normalizing the action by 2-torsion points (as in Mumford '66)
Find $(\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2 : \tilde{x}_3) = M\,(x_0 : x_1 : x_2 : x_3)$ with $M \in \mathrm{PGL}(4)$ so that

$$T_{\tilde{P}_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T_{\tilde{P}_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_{\tilde{Q}_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \; T_{\tilde{Q}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

With $\tilde{O} = (a : b : c : d)$:

- $\tilde{P}_1 = (b : a : d : c)$
- $\tilde{P}_2 = (c : d : a : b)$
- $\tilde{Q}_1 = (a : -b : c : -d)$
- $\tilde{Q}_2 = (a : b : -c : -d)$



Defining equation (Gaudry '05)
for some constants E, F, G, H:

$$\tilde{x}_0^4 + \tilde{x}_1^4 + \tilde{x}_2^4 + \tilde{x}_3^4 - E\tilde{x}_0\tilde{x}_1\tilde{x}_2\tilde{x}_3 - F(\tilde{x}_0^2\tilde{x}_3^2 + \tilde{x}_1^2\tilde{x}_2^2) - G(\tilde{x}_0^2\tilde{x}_2^2 + \tilde{x}_1^2\tilde{x}_3^2) - H(\tilde{x}_0^2\tilde{x}_1^2 + \tilde{x}_2^2\tilde{x}_3^2) = 0$$

$\tilde{x}_0, \tilde{x}_1, \tilde{x}_2, \tilde{x}_3$ are level-2 theta coordinates.
Notation: $\theta : K \hookrightarrow \mathbb{P}^3$.

$(2,2)$-isogenies of Kummer surfaces

An **isogeny** of principally polarized abelian varieties A, B is a surjective homomorphism $f : A \to B$ with finite kernel.

In dimension 2: A $(2,2)$**-isogeny** is an isogeny $f : A \to B$ with kernel $\ker(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel is isotropic w.r.t. the Weil pairing

$(2,2)$-isogenies of Kummer surfaces

An **isogeny** of principally polarized abelian varieties A, B is a surjective homomorphism $f : A \to B$ with finite kernel.

In dimension 2: A $(2,2)$**-isogeny** is an isogeny $f : A \to B$ with kernel $\ker(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel is isotropic w.r.t. the Weil pairing

- **Example**: Let (P_1, P_2, Q_1, Q_2) be a symplectic basis for $A[2]$, then $K_1 = \langle P_1, P_2 \rangle$ and $K_2 = \langle Q_1, Q_2 \rangle$ are isotropic $(2,2)$-groups.
  $\to$ in total: 15 isotropic $(2,2)$-groups

$(2,2)$-isogenies of Kummer surfaces

An **isogeny** of principally polarized abelian varieties A, B is a surjective homomorphism $f : A \to B$ with finite kernel.

In dimension 2: A $(2,2)$-**isogeny** is an isogeny $f : A \to B$ with kernel $\ker(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel is isotropic w.r.t. the Weil pairing

- **Example**: Let (P_1, P_2, Q_1, Q_2) be a symplectic basis for $A[2]$, then $K_1 = \langle P_1, P_2 \rangle$ and $K_2 = \langle Q_1, Q_2 \rangle$ are isotropic $(2,2)$-groups.
  $\to$ in total: 15 isotropic $(2,2)$-groups
- Induced rational map of Kummer surfaces: $f : K_A \to K_B$.

$(2,2)$-isogenies of Kummer surfaces

An **isogeny** of principally polarized abelian varieties A, B is a surjective homomorphism $f : A \to B$ with finite kernel.

In dimension 2: A $(2,2)$-**isogeny** is an isogeny $f : A \to B$ with kernel $\ker(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel is isotropic w.r.t. the Weil pairing

- **Example**: Let (P_1, P_2, Q_1, Q_2) be a symplectic basis for $A[2]$, then $K_1 = \langle P_1, P_2 \rangle$ and $K_2 = \langle Q_1, Q_2 \rangle$ are isotropic $(2,2)$-groups.
  $\to$ in total: 15 isotropic $(2,2)$-groups
- Induced rational map of Kummer surfaces: $f : \mathcal{K}_A \to \mathcal{K}_B$.

$(2,2)$**-isogeny formula**: $\ker(f) = \langle (a : -b : c : -d), (a : b : -c : -d) \rangle$

$(2,2)$-isogenies of Kummer surfaces

An **isogeny** of principally polarized abelian varieties A, B is a surjective homomorphism $f : A \to B$ with finite kernel.

In dimension 2: A $(2,2)$**-isogeny** is an isogeny $f : A \to B$ with kernel $\ker(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel is isotropic w.r.t. the Weil pairing

- **Example**: Let (P_1, P_2, Q_1, Q_2) be a symplectic basis for $A[2]$, then $K_1 = \langle P_1, P_2 \rangle$ and $K_2 = \langle Q_1, Q_2 \rangle$ are isotropic $(2,2)$-groups.
  $\to$ in total: 15 isotropic $(2,2)$-groups
- Induced rational map of Kummer surfaces: $f : K_A \to K_B$.

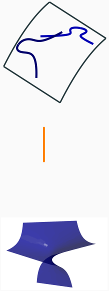
$(2,2)$-isogeny formula: $\ker(f) = \langle (a : -b : c : -d), (a : b : -c : -d) \rangle$

$$\theta(P) \to \begin{array}{c}\mathcal{S}\\ \text{Squaring}\end{array} \to \begin{array}{c}\mathcal{H}\\ \text{Hadamard}\end{array} \to \begin{array}{c}C_{(\tilde{a}':\tilde{b}':\tilde{c}':\tilde{d}')}\\ \text{Scaling}\end{array} \to \begin{array}{c}\mathcal{H}\\ \text{Hadamard}\end{array} \to \theta'(f(P))$$

Proof: very similar to the dimension-1 case.

Non-generic isogenies require special treatment

Product of elliptic curves $E \times E'$: The level-2 theta coordinates define an embedding $\theta : E/\langle\pm 1\rangle \times E'\langle\pm 1\rangle \hookrightarrow \mathbb{P}^3$.



Non-generic isogenies require special treatment

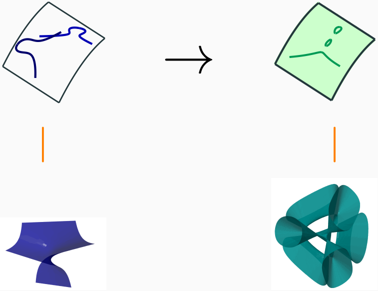
Product of elliptic curves $E \times E'$: The level-2 theta coordinates define an embedding $\theta : E/\langle \pm 1 \rangle \times E' \langle \pm 1 \rangle \hookrightarrow \mathbb{P}^3$.

- ! This is less information than $(E \times E')/\langle \pm 1 \rangle$.

Non-generic isogenies require special treatment

Product of elliptic curves $E \times E'$: The level-2 theta coordinates define an embedding $\theta : E/\langle \pm 1 \rangle \times E'\langle \pm 1 \rangle \hookrightarrow \mathbb{P}^3$.

- **!** This is less information than $(E \times E')/\langle \pm 1 \rangle$.
- $\rightarrow$ **Gluing isogeny** $f : E \times E' \rightarrow Jac(C)$ does not descend to a rational map $E/\langle \pm 1 \rangle \times E\langle \pm 1 \rangle \not\rightarrow Jac(C)/\langle \pm 1 \rangle$



General $(2, \ldots, 2)$-formulas

Consider A irreducible p.p.a.v. with $\dim(A) = g$, and the embedding

$$\theta : A/\langle \pm 1 \rangle \hookrightarrow \mathbb{P}^{2^g - 1}.$$

General $(2,\ldots,2)$-formulas

Consider A irreducible p.p.a.v. with $\dim(A) = g$, and the embedding

$$\theta : A/\langle \pm 1 \rangle \hookrightarrow \mathbb{P}^{2^g - 1}.$$

Let $\theta(0_A) = (a_0 : \cdots : a_{2^g-1})$ be the theta null point, then
$K_2 = \langle (a_0 : -a_1 : \ldots : -a_{2^g-1}), \ldots, (a_0 : \ldots : a_{2^{g-1}-1} : -a_{2^{g-1}} : \ldots : -a_{2^g-1}) \rangle$
is an isotropic $(2 : \ldots : 2)$-group $\cong (\mathbb{Z}/2\mathbb{Z})^g$.

General $(2, \ldots, 2)$-formulas

Consider A irreducible p.p.a.v. with $\dim(A) = g$, and the embedding

$$\theta : A/\langle \pm 1 \rangle \hookrightarrow \mathbb{P}^{2^g - 1}.$$

Let $\theta(0_A) = (a_0 : \cdots : a_{2^g-1})$ be the theta null point, then
$K_2 = \langle (a_0 : -a_1 : \ldots : -a_{2^g-1}), \ldots, (a_0 : \ldots : a_{2^{g-1}-1} : -a_{2^{g-1}} : \ldots : -a_{2^g-1}) \rangle$
is an isotropic $(2 : \ldots : 2)$-group $\cong (\mathbb{Z}/2\mathbb{Z})^g$.

Robert '23 (Renes–Smith '17 for $g = 2$):
The isogeny $f : A \to B$ with kernel K_2 is described by

$$\theta(P) \to \underset{\text{Squaring}}{\mathcal{S}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \underset{\text{Scaling}}{C_{\tilde{a}'}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \theta'(f(P))$$

General $(2,\dots,2)$-formulas

Consider A irreducible p.p.a.v. with $\dim(A) = g$, and the embedding

$$\theta : A/\langle \pm 1\rangle \hookrightarrow \mathbb{P}^{2^g-1}.$$

Let $\theta(0_A) = (a_0 : \cdots : a_{2^g-1})$ be the theta null point, then
$K_2 = \langle (a_0 : -a_1 : \ldots : -a_{2^g-1}), \ldots, (a_0 : \ldots : a_{2^{g-1}-1} : -a_{2^{g-1}} : \ldots : -a_{2^g-1})\rangle$
is an isotropic $(2 : \ldots : 2)$-group $\cong (\mathbb{Z}/2\mathbb{Z})^g$.

Robert '23 (Renes–Smith '17 for $g = 2$):
The isogeny $f : A \to B$ with kernel K_2 is described by

$$\theta(P) \to \underset{\text{Squaring}}{\mathcal{S}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \underset{\text{Scaling}}{C_{\tilde{a}'}} \to \underset{\text{Hadamard}}{\mathcal{H}} \to \theta'(f(P))$$

Analysis and implementation (including irreducible cases)

- $(2^n, \ldots, 2^n)$-isogenies: dimension 1 (Robert–Sarkis '24), dimension 2 (DMPR '24, Duparc '25), dimension 4 (Dartois '25)
- radical $(2, \ldots, 2)$-isogenies: dimensions 1-3 (**K**MMPPRST '24)

$(3, \ldots, 3)$-isogenies (char$(k) > 3$)

Elliptic curves in Hesse form

Action of 3-torsion points on elliptic curves

We now consider an embedding $(E, \mathcal{O}) \hookrightarrow \mathbb{P}^2 = \mathit{Proj}\, k[x, y, z]$

The coordinate functions x, y, z are a basis for $L(3\mathcal{O})$.
$\Rightarrow$ 3-torsion points act by linear transformations of $\mathbb{P}^2$

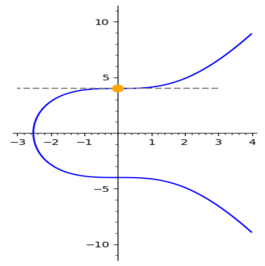
Action of 3-torsion points on elliptic curves

We now consider an embedding $(E, \mathcal{O}) \hookrightarrow \mathbb{P}^2 = \mathit{Proj}\, k[x, y, z]$

The coordinate functions x, y, z are a basis for $L(3\mathcal{O})$.
$\Rightarrow$ 3-torsion points act by linear transformations of $\mathbb{P}^2$

Example: $E : y^2 z = x^3 + 16z^3$

$\rightarrow$ $E[3] = \langle P, Q \rangle$ with $P = (0 : 4 : 1)$, $Q = (-4 : 4\alpha : 1)$, and $\alpha^2 = -3$



$P = (0, 4) \in E[3]$
tangent at P: $y = 4$

Action of 3-torsion points on elliptic curves

We now consider an embedding $(E, \mathcal{O}) \hookrightarrow \mathbb{P}^2 = \mathit{Proj}\, k[x, y, z]$

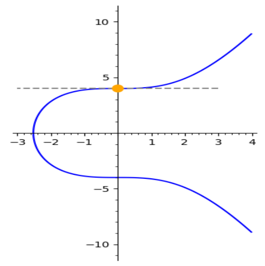
The coordinate functions x, y, z are a basis for $L(3\mathcal{O})$.
$\Rightarrow$ 3-torsion points act by linear transformations of $\mathbb{P}^2$

Example: $E : y^2z = x^3 + 16z^3$

$\rightarrow$ $E[3] = \langle P, Q \rangle$ with $P = (0 : 4 : 1)$, $Q = (-4 : 4\alpha : 1)$, and $\alpha^2 = -3$

$\rightarrow$ $P + (x : y : z) = T_P(x : y : z)$
$Q + (x : y : z) = T_Q(x : y : z)$
with

$$T_P = \begin{pmatrix} -8 & 0 & 0 \\ 0 & 4 & -48 \\ 0 & 1 & 4 \end{pmatrix}, T_Q = \begin{pmatrix} 0 & -4 & -16\alpha \\ -24 & 4\alpha & 48 \\ -2\alpha & 1 & -4\alpha \end{pmatrix}$$



$P = (0, 4) \in E[3]$
tangent at P: $y = 4$

Normalizing the action of 3-torsion points

There is a change of coordinates $(\tilde{x} : \tilde{y} : \tilde{z}) = M(x : y : z)$, so that

$$T_{\tilde{P}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad T_{\tilde{Q}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad \text{with } \omega^2 + \omega + 1 = 0.$$

Normalizing the action of 3-torsion points

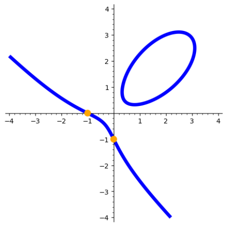
There is a change of coordinates $(\tilde{x} : \tilde{y} : \tilde{z}) = M(x : y : z)$, so that

$$T_{\tilde{P}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad T_{\tilde{Q}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad \text{with } \omega^2 + \omega + 1 = 0.$$

Then $(\tilde{x} : \tilde{y} : \tilde{z}) = (\theta_0 : \theta_1 : \theta_2)$ are **level-3 theta coordinates** for E and

$$E_d : \tilde{x}^3 + \tilde{y}^3 + \tilde{z}^3 = 3d\, \tilde{x}\tilde{y}\tilde{z}$$

is an equation in **Hesse form**.



$\tilde{x}^3 + \tilde{y}^3 + \tilde{z}^3 = 6\tilde{x}\tilde{y}\tilde{z}$

Normalizing the action of 3-torsion points

There is a change of coordinates $(\tilde{x} : \tilde{y} : \tilde{z}) = M(x : y : z)$, so that

$$T_{\tilde{P}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad T_{\tilde{Q}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad \text{with } \omega^2 + \omega + 1 = 0.$$

Then $(\tilde{x} : \tilde{y} : \tilde{z}) = (\theta_0 : \theta_1 : \theta_2)$ are **level-3 theta coordinates** for E and

$$E_d : \tilde{x}^3 + \tilde{y}^3 + \tilde{z}^3 = 3d\,\tilde{x}\tilde{y}\tilde{z}$$

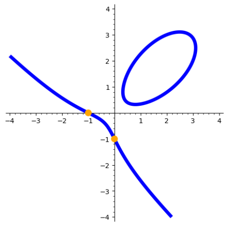
is an equation in **Hesse form**.

The 3-torsion

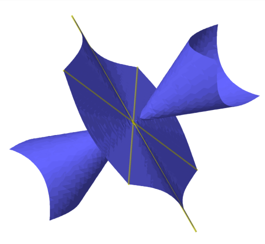
$\theta(O) = (0 : -1 : 1)$

$\theta(P) = (-1 : 0 : 1)$

$\theta(Q) = (0 : -\omega^2 : 1)$



$\tilde{x}^3 + \tilde{y}^3 + \tilde{z}^3 = 6\tilde{x}\tilde{y}\tilde{z}$



Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ ($d \neq 0$) with kernel $\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ ($d \neq 0$) with kernel
$\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

$\Rightarrow$ **Idea:** Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ ($d \neq 0$) with kernel $\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

⇒ **Idea**: Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

- $(x : y : z) + Q = (x : \omega y : \omega^2 z)$

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form
$f : E_d \to E_{d'}$ ($d \neq 0$) with kernel
$\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

$\Rightarrow$ **Idea:** Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

- $(x : y : z) + Q = (x : \omega y : \omega^2 z)$

$\to$ $\odot^3((x : y : z) + Q)$
$= \odot^3((x : y : z))$

$\to$ $\odot^3$ is an isogeny with kernel $\langle Q \rangle$

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ $(d \neq 0)$ with kernel
$\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

$\Rightarrow$ **Idea:** Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

- $(x : y : z) + Q = (x : \omega y : \omega^2 z)$

$\to$ $\odot^3((x : y : z) + Q)$
$= \odot^3((x : y : z))$

$\to$ $\odot^3$ is an isogeny with kernel $\langle Q \rangle$

- $T_P \circ \odot^3(x : y : z)$
$= \odot^3 \circ T_P(x : y : z))$

$\to$ $\odot^3(P)$ is in normal form.

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ ($d \neq 0$) with kernel $\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

$\Rightarrow$ **Idea**: Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

- $(x : y : z) + Q = (x : \omega y : \omega^2 z)$

$\to$ $\odot^3((x : y : z) + Q)$
$= \odot^3((x : y : z))$

$\to$ $\odot^3$ is an isogeny with kernel $\langle Q \rangle$

- $T_P \circ \odot^3(x : y : z)$
$= \odot^3 \circ T_P(x : y : z))$

$\to$ $\odot^3(P)$ is in normal form.

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

- Condition 1: $T_P \cdot M = \omega^i M \cdot T_P$ for some $i \in \{0, 1, 2\}$

$$\Rightarrow M = \begin{pmatrix} \alpha & \beta & \gamma \\ \omega^i \gamma & \omega^i \alpha & \omega^i \beta \\ \omega^{2i} \beta & \omega^{2i} \gamma & \omega^{2i} \alpha \end{pmatrix}$$

Finding a 3-isogeny formula

Goal: Compute the 3-isogeny of elliptic curves in Hesse form $f : E_d \to E_{d'}$ ($d \neq 0$) with kernel $\ker(f) = \langle Q \rangle = \{(0 : -1 : 1), (0 : -\omega^2 : 1), (0 : -\omega : 1)\}$.

$\Rightarrow$ **Idea**: Coordinate-wise cubing + a linear transformation.

Coordinate-wise cubing

$\odot^3 : (x : y : z) \mapsto (x^3 : y^3 : z^3)$

- $(x : y : z) + Q = (x : \omega y : \omega^2 z)$

$\to$ $\odot^3((x : y : z) + Q) = \odot^3((x : y : z))$

$\to$ $\odot^3$ is an isogeny with kernel $\langle Q \rangle$

- $T_P \circ \odot^3(x : y : z) = \odot^3 \circ T_P(x : y : z))$

$\to$ $\odot^3(P)$ is in normal form.

Linear transformation M

$M : (x : y : z) \mapsto M \cdot (x : y : z)$

- Condition 1: $T_P \cdot M = \omega^i M \cdot T_P$ for some $i \in \{0, 1, 2\}$

$$\Rightarrow \quad M = \begin{pmatrix} \alpha & \beta & \gamma \\ \omega^i \gamma & \omega^i \alpha & \omega^i \beta \\ \omega^{2i} \beta & \omega^{2i} \gamma & \omega^{2i} \alpha \end{pmatrix}$$

- Condition 2: $MX = X$ for $X \in \langle P \rangle$

$\Rightarrow$ $i = 0$ and $\beta = \gamma$

The 3-isogeny formula (with kernel $\langle Q \rangle$)

Result of previous slide:

$f : E_d \to E'_d$ is given by $M \circ \odot^3$ with $M = \begin{pmatrix} \alpha & \beta & \beta \\ \beta & \alpha & \beta \\ \beta & \beta & \alpha \end{pmatrix}$ for some α, β.

The 3-isogeny formula (with kernel $\langle Q \rangle$)

Result of previous slide:

$f : E_d \to E'_d$ is given by $M \circ \odot^3$ with $M = \begin{pmatrix} \alpha & \beta & \beta \\ \beta & \alpha & \beta \\ \beta & \beta & \alpha \end{pmatrix}$ for some α, β.

Decomposition:

$$M = \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}}_{\text{Fourier transform } \mathcal{F}} \cdot \begin{pmatrix} \alpha + 2\beta & 0 & 0 \\ 0 & \alpha - \beta & 0 \\ 0 & 0 & \alpha - \beta \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}}_{\mathcal{F}^{-1}}$$

The 3-isogeny formula (with kernel $\langle Q \rangle$)

Result of previous slide:

$f : E_d \to E'_d$ is given by $M \circ \odot^3$ with $M = \begin{pmatrix} \alpha & \beta & \beta \\ \beta & \alpha & \beta \\ \beta & \beta & \alpha \end{pmatrix}$ for some α, β.

Decomposition:

$$M = \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}}_{\text{Fourier transform } \mathcal{F}} \cdot \begin{pmatrix} \alpha + 2\beta & 0 & 0 \\ 0 & \alpha - \beta & 0 \\ 0 & 0 & \alpha - \beta \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}}_{\mathcal{F}^{-1}}$$

3-isogeny formula (Decru-K. '25)

$\theta(P)$ → $\odot^3$ Cubing → $\mathcal{F}$ Fourier → $C_{(\tilde{\alpha}:\tilde{\beta}:\tilde{\beta})}$ Scaling → $\mathcal{F}^{-1}$ Fourier → $\theta'(f(P))$

Computing α, β (using a 9-torsion point: $Q' = (x_0 : y_0 : z_0)$ with $3 \cdot Q' = Q$)

- $M \circ \odot^3(Q') = (0 : -\omega^2 : 1) \quad \Rightarrow \quad (\alpha : \beta) = (y_0^3 + z_0^3 : -x_0^3)$

$(3, \ldots, 3)$-isogenies (char$(k) > 3$)

Abelian surfaces in Hesse form

Level-3 model of a principally polarized abelian surface $(A, \mathcal{L}_0)$

$\mathcal{L}_0^3$ induces an embedding $A \hookrightarrow \mathbb{P}^8$.

Level-3 model of a principally polarized abelian surface $(A, \mathcal{L}_0)$

$\mathcal{L}_0^3$ induces an embedding $A \hookrightarrow \mathbb{P}^8$.

For $\theta : A \hookrightarrow \mathbb{P}^8$: **normalized action of 3-torsion basis** (P_1, P_2, Q_1, Q_2)

P_1, P_2: permutations σ_i:

$\sigma_1 = (0\,1\,2)(3\,4\,5)(6\,7\,8)$,

$\sigma_2 = (0\,3\,6)(1\,4\,7)(2\,5\,8)$

Q_1, Q_2: coordinate-wise scaling by s_{Q_i}:

$s_{Q_1} = (1 : \omega : \omega^2 : 1 : \omega : \omega^2 : 1 : \omega : \omega^2)$,

$s_{Q_2} = (1 : 1 : 1 : \omega : \omega : \omega : \omega^2 : \omega^2 : \omega^2)$

Level-3 model of a principally polarized abelian surface $(A, \mathcal{L}_0)$

$\mathcal{L}_0^3$ induces an embedding $A \hookrightarrow \mathbb{P}^8$.

For $\theta : A \hookrightarrow \mathbb{P}^8$: **normalized action of 3-torsion basis** (P_1, P_2, Q_1, Q_2)

P_1, P_2: permutations σ_i:

$\sigma_1 = (0\,1\,2)(3\,4\,5)(6\,7\,8)$,

$\sigma_2 = (0\,3\,6)(1\,4\,7)(2\,5\,8)$

Q_1, Q_2: coordinate-wise scaling by s_{Q_i}:

$s_{Q_1} = (1 : \omega : \omega^2 : 1 : \omega : \omega^2 : 1 : \omega : \omega^2)$,

$s_{Q_2} = (1 : 1 : 1 : \omega : \omega : \omega : \omega^2 : \omega^2 : \omega^2)$

Gunji '06 (+ Coble 1917, Barth'95, Birkenhake–Lange '90):

$A_{d,h} := \theta(A) = V(F_1, \ldots, F_4, G_0, \ldots, G_8) \subset \mathbb{P}^8$ with

$$\begin{aligned}
F_1 &= d_1 \textstyle\sum_{j=0}^8 X_j^3 - 3d_0(X_0X_1X_2 + X_3X_4X_5 + X_6X_7X_8),\\
F_2 &= d_2 \textstyle\sum_{j=0}^8 X_j^3 - 3d_0(X_0X_3X_6 + X_1X_4X_7 + X_2X_5X_8),\\
F_3 &= d_3 \textstyle\sum_{j=0}^8 X_j^3 - 3d_0(X_0X_4X_8 + X_1X_5X_6 + X_2X_3X_7),\\
F_4 &= d_4 \textstyle\sum_{j=0}^8 X_j^3 - 3d_0(X_0X_5X_7 + X_1X_3X_8 + X_2X_4X_6),
\end{aligned}$$

$$\begin{aligned}
G_0 &= h_0X_0^2 + h_1X_1X_2 + h_2X_3X_6 + h_3X_4X_8 + h_4X_5X_7,\\
&\vdots\\
G_8 &= h_0X_8^2 + h_1X_6X_7 + h_2X_2X_5 + h_3X_0X_4 + h_4X_1X_3.
\end{aligned}$$

for some $d = (d_0 : \cdots : d_4)$, $h = (h_0 : \cdots : h_4) \in \mathbb{P}^4$.

Excursion: the Burkhardt quartic

Burkhardt quartic $\mathcal{B} \subset \mathbb{P}^4$**:**
$F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0$

Excursion: the Burkhardt quartic

Burkhardt quartic $\mathcal{B} \subset \mathbb{P}^4$**:**
$F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0$

- $\mathcal{B}$ is birational to the moduli space of p.p.a.s. with level-3 structure (van der Geer '87)

Excursion: the Burkhardt quartic

Burkhardt quartic $\mathcal{B} \subset \mathbb{P}^4$:
$F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0$

- $\mathcal{B}$ is birational to the moduli space of p.p.a.s. with level-3 structure (van der Geer '87)
- $h \in \mathcal{B} \setminus H(\mathcal{B}) \rightsquigarrow (J(C), J(C)[3])$ (Bruin-Nasserden '18).

Excursion: the Burkhardt quartic

Burkhardt quartic $\mathcal{B} \subset \mathbb{P}^4$:
$F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0$

Hessian of the Burkhardt quartic $H(\mathcal{B}) \subset \mathbb{P}^4$:
$H(F) = \frac{1}{486} \det \left(\frac{\partial F}{\partial x_i \partial x_j} \right) = 0$

- $\mathcal{B}$ is birational to the moduli space of p.p.a.s. with level-3 structure (van der Geer '87)
- $h \in \mathcal{B} \setminus H(\mathcal{B}) \rightsquigarrow (J(C), J(C)[3])$ (Bruin-Nasserden '18).

Excursion: the Burkhardt quartic

Burkhardt quartic $\mathcal{B} \subset \mathbb{P}^4$:
$F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0$

Hessian of the Burkhardt quartic $H(\mathcal{B}) \subset \mathbb{P}^4$:
$H(F) = \frac{1}{486} \det\left(\frac{\partial F}{\partial x_i \partial x_j}\right) = 0$

Dual of the Burkhardt quartic $\tilde{B} \subset \mathbb{P}^4$: $\tilde{F} = 0$,
where $\tilde{F}(\nabla F) \equiv 0 \pmod{F}$.

- $\mathcal{B}$ is birational to the moduli space of p.p.a.s. with level-3 structure (van der Geer '87)
- $h \in \mathcal{B} \setminus H(\mathcal{B}) \rightsquigarrow (J(C), J(C)[3])$ (Bruin-Nasserden '18).
- Normalization of $\tilde{B}$ is the Satake compactification of the moduli space (Freitag–Manni '04)

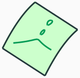
Relation of $A_{d,h}$ with the Burkhardt quartic

Coefficient vectors: $h \in \mathcal{B}$, $d \in \tilde{B}$ and $d_0 h_0 + \ldots d_4 h_4 = 0$

Relation of $A_{d,h}$ with the Burkhardt quartic

Coefficient vectors: $h \in \mathcal{B}$, $d \in \tilde{B}$ and $d_0 h_0 + \ldots d_4 h_4 = 0$

$\mathbf{A} = \mathbf{Jac}(\mathbf{C})$

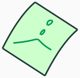


- $\theta(A) = V(G_0, \ldots G_8)$: A is defined by the quadrics

$\rightarrow$ $h \in \mathcal{B}$ uniquely defines A

Relation of $A_{d,h}$ with the Burkhardt quartic

Coefficient vectors: $h \in \mathcal{B}$, $d \in \tilde{B}$ and $d_0 h_0 + \dots d_4 h_4 = 0$



$\mathbf{A} = \mathbf{Jac}(\mathbf{C})$

- $\theta(A) = V(G_0, ...G_8)$: A is defined by the quadrics

$\rightarrow$ $h \in \mathcal{B}$ uniquely defines A

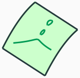
$\mathbf{A} = \mathbf{E} \times \mathbf{E}'$

- $\theta(A) \subsetneq V(G_0, \dots, G_8)$: the quadrics only define the Segre embedding $\iota : \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$

$\rightarrow$ $h \in \mathcal{B}$ is a singularity

Coefficient vectors: $h \in \mathcal{B}$, $d \in \tilde{B}$ and $d_0h_0 + \dots d_4h_4 = 0$

A = Jac(C)



- $\theta(A) = V(G_0, ...G_8)$: A is defined by the quadrics

$\rightarrow$ $h \in \mathcal{B}$ uniquely defines A

A = E × E′

- $\theta(A) \subsetneq V(G_0, \dots, G_8)$: the quadrics only define the Segre embedding $\iota : \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$

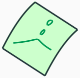
$\rightarrow$ $h \in \mathcal{B}$ is a singularity

The neutral element

- Even theta structure: $0_A = (t_0 : t_1 : t_1 : t_2 : t_3 : t_4 : t_2 : t_2 : t_3)$ for some $(t_0 : 2t_1 : 2t_2 : 2t_3 : 2t_4) \in H(\mathcal{B})$

Relation of $A_{d,h}$ with the Burkhardt quartic

Coefficient vectors: $h \in \mathcal{B}$, $d \in \tilde{B}$ and $d_0 h_0 + \ldots d_4 h_4 = 0$



A $=$ **Jac(C)**

- $\theta(A) = V(G_0, ...G_8)$: A is defined by the quadrics

$\rightarrow$ $h \in \mathcal{B}$ uniquely defines A

A $=$ **E** $\times$ **E**$'$

- $\theta(A) \subsetneq V(G_0, \ldots, G_8)$: the quadrics only define the Segre embedding $\iota : \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$

$\rightarrow$ $h \in \mathcal{B}$ is a singularity

The neutral element

- Even theta structure: $0_A = (t_0 : t_1 : t_1 : t_2 : t_3 : t_4 : t_2 : t_2 : t_3)$ for some $(t_0 : 2t_1 : 2t_2 : 2t_3 : 2t_4) \in H(\mathcal{B})$
- Odd theta structure: $0_A = (0 : s_1 : -s_1 : s_2 : s_3 : s_4 : -s_2 : -s_4 : -s_3)$, for some $(s_0 : s_1 : s_2 : s_3) \in \mathbb{P}^3$

$(3,3)$-Isogeny formula (Decru-K. '26)

Let $A_{d,h}$ be a p.p. abelian surface in Hesse form*, and (P_1, P_2, Q_1, Q_2) the canonical symplectic basis of $A_{d,h}[3]$. Then the $(3,3)$-isogeny $f : A_{d,h} \to A_{d',h'} = A_{d,h}/\langle Q_1, Q_2 \rangle$ is:

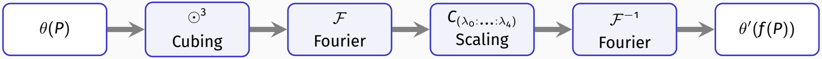
$\theta(P)$ → $\odot^3$ Cubing → $\mathcal{F}$ Fourier → $C_{(\lambda_0:\ldots:\lambda_4)}$ Scaling → $\mathcal{F}^{-1}$ Fourier → $\theta'(f(P))$

---

*We assume that $3 \nmid \mathrm{Aut}(A_{d,h})$.

$(3,3)$-Isogeny formula (Decru-K. '26)

Let $A_{d,h}$ be a p.p. abelian surface in Hesse form*, and (P_1, P_2, Q_1, Q_2) the canonical symplectic basis of $A_{d,h}[3]$. Then the $(3,3)$-isogeny $f : A_{d,h} \to A_{d',h'} = A_{d,h}/\langle Q_1, Q_2 \rangle$ is:



- Scaling vector $\lambda = (\lambda_0 : \cdots : \lambda_4)$ is computed using 9-torsion points Q_1', Q_2'.

We assume that $3 \nmid \mathrm{Aut}(A_{d,h})$.

$(3,3)$-Isogeny formula (Decru-K. '26)

Let $A_{d,h}$ be a p.p. abelian surface in Hesse form*, and (P_1, P_2, Q_1, Q_2) the canonical symplectic basis of $A_{d,h}[3]$. Then the $(3,3)$-isogeny $f : A_{d,h} \to A_{d',h'} = A_{d,h}/\langle Q_1, Q_2 \rangle$ is:

$\theta(P)$ → $\odot^3$ Cubing → $\mathcal{F}$ Fourier → $C_{(\lambda_0:\ldots:\lambda_4)}$ Scaling → $\mathcal{F}^{-1}$ Fourier → $\theta'(f(P))$

- Scaling vector $\lambda = (\lambda_0 : \cdots : \lambda_4)$ is computed using 9-torsion points Q_1', Q_2'.
- Description is also valid for non-generic isogenies: $f : E \times E' \to Jac(C)$ or $f : Jac(C) \to E \times E'$

*We assume that $3 \nmid \mathrm{Aut}(A_{d,h})$.

Computing arbitrary $(3,3)$-isogenies

Goal: Given $\langle S_1, S_2 \rangle \subset A_{d,h}[3]$, compute $A_{d,h} \to A_{d,h}/\langle S_1, S_2 \rangle$

Computing arbitrary $(3,3)$-isogenies

Goal: Given $\langle S_1, S_2 \rangle \subset A_{d,h}[3]$, compute $A_{d,h} \to A_{d,h}/\langle S_1, S_2 \rangle$

$\to$ Find a linear transformation $M : \mathbb{P}^8 \to \mathbb{P}^8$ with:

- $M(A_{d,h}) = A_{d',h'}$ for some d', h'
- $M(\langle S_1, S_2 \rangle) = \langle Q_1', Q_2' \rangle$ ("in canonical position")

Computing arbitrary $(3,3)$-isogenies

Goal: Given $\langle S_1, S_2 \rangle \subset A_{d,h}[3]$, compute $A_{d,h} \to A_{d,h}/\langle S_1, S_2 \rangle$

$\to$ Find a linear transformation $M : \mathbb{P}^8 \to \mathbb{P}^8$ with:

- $M(A_{d,h}) = A_{d',h'}$ for some d', h'
- $M(\langle S_1, S_2 \rangle) = \langle Q_1', Q_2' \rangle$ ("in canonical position")

$\to$ M is a symplectic transformation

- In correspondence with automorphisms of the Burkhardt quartic $\mathcal{B}$

Computing arbitrary $(3,3)$-isogenies

Goal: Given $\langle S_1, S_2\rangle \subset A_{d,h}[3]$, compute $A_{d,h} \to A_{d,h}/\langle S_1, S_2\rangle$

$\to$ Find a linear transformation $M : \mathbb{P}^8 \to \mathbb{P}^8$ with:

- $M(A_{d,h}) = A_{d',h'}$ for some d', h'
- $M(\langle S_1, S_2\rangle) = \langle Q_1', Q_2'\rangle$ ("in canonical position")

$\to$ M is a symplectic transformation

- In correspondence with automorphisms of the Burkhardt quartic $\mathcal{B}$
- $\mathrm{Aut}(\mathcal{B}) \cong \langle M_0, M_1, M_2, M_3\rangle$ with

$$M_0 = \begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & -1 & 2 & -1 & -1 \\ 1 & 2 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 2 \\ 1 & -1 & -1 & 2 & -1 \end{pmatrix},$$

$$\begin{aligned} M_1 &= \ diag(1, \omega, 1, \omega, \omega) \\ M_2 &= \ diag(1, 1, 1, \omega^2, \omega) \\ M_3 &= \ diag(1, 1, \omega, \omega, \omega). \end{aligned}$$

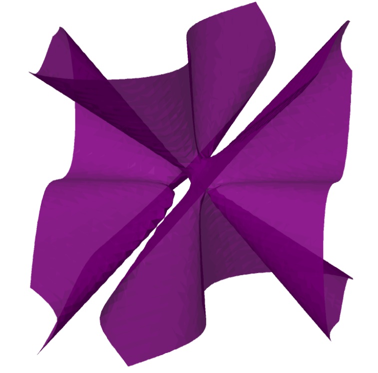
- Easy to compute the correct M

SageMath package: level-3-arithmetic

Implementation Sage

https://github.com/sabrinakunzweiler/level-3-arithmetic

- Elliptic curves and abelian surfaces in Hesse form
- Functionality to compute 3^n- and $(3^n, 3^n)$-isogenies
- Kummer surfaces



Implementation Sage

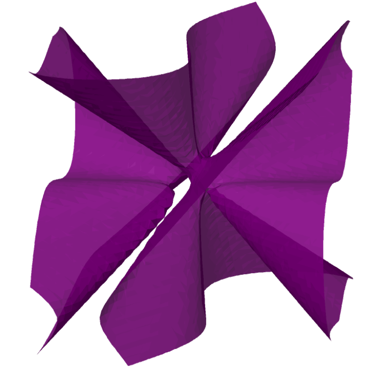
https://github.com/sabrinakunzweiler/level-3-arithmetic

- Elliptic curves and abelian surfaces in Hesse form
- Functionality to compute 3^n- and $(3^n, 3^n)$-isogenies
- Kummer surfaces

Work in progress

(with J. Eriksen, M. Houben, K. Rijnders)

- Addition formulas
- $(2, 2)$-isogenies
- pairings



Conclusion

Conclusion

Main takeaway

- Computing $(\ell, \ldots, \ell)$-isogenies in level-ℓ seems easy (shown for $g = 1, 2$ and $\ell = 2, 3$).
- General pattern

$\theta_\ell(P)$ → $\odot^\ell$ ℓ-th power → $\mathcal{F}_\ell$ Fourier → C_λ Scaling → $\mathcal{F}_\ell^{-1}$ Fourier → $\theta'(f(P))$

(Decomposition of $(\ell, \ldots, \ell)$-isogeny in the level-ℓ theta model)

Conclusion

Main takeaway

- Computing $(\ell, \ldots, \ell)$-isogenies in level-ℓ seems easy (shown for $g = 1, 2$ and $\ell = 2, 3$).
- General pattern

$\theta_\ell(P)$ → $\odot^\ell$ ℓ-th power → $\mathcal{F}_\ell$ Fourier → C_λ Scaling → $\mathcal{F}_\ell^{-1}$ Fourier → $\theta'(f(P))$

(Decomposition of $(\ell, \ldots, \ell)$-isogeny in the level-ℓ theta model)

$\to$ **some work in progress**

- $\ell = \mathbf{4}$ (with T. Decru, T. Lange, D. Lazzarini, L. Maino)
- $\ell = \mathbf{3}$ (radical isogeny formulas)
- $\ell = \mathbf{i} + \mathbf{1}$ where $i^2 = -1$ (with the MIKE team)

Conclusion

Main takeaway

- Computing $(\ell, \dots, \ell)$-isogenies in level-ℓ seems easy (shown for $g = 1, 2$ and $\ell = 2, 3$).
- General pattern

$$\theta_\ell(P) \to \underset{\ell\text{-th power}}{\odot^\ell} \to \underset{\text{Fourier}}{\mathcal{F}_\ell} \to \underset{\text{Scaling}}{C_\lambda} \to \underset{\text{Fourier}}{\mathcal{F}_\ell^{-1}} \to \theta'(f(P))$$

(Decomposition of $(\ell, \dots, \ell)$-isogeny in the level-ℓ theta model)

$\rightarrow$ **some work in progress**

- $\ell = \mathbf{4}$ (with T. Decru, T. Lange, D. Lazzarini, L. Maino)
- $\ell = \mathbf{3}$ (radical isogeny formulas)
- $\ell = \mathbf{i} + \mathbf{1}$ where $i^2 = -1$ (with the MIKE team)

Thank you!