Computing Isomorphisms between Products of Supersingular Elliptic Curves

Joint work with P.-J. Spaenlehauer and P. Gaudry

Julien Soumier

ANTS, July 6, 2026

Contributions

Theorem: Deligne-Ogus-Shioda *[Shioda; 1979]*

Let $E_1, \ldots, E_g$ and $E'_1, \ldots, E'_g$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E'_1 \times \cdots \times E'_g.$$

Contributions

Theorem: Deligne-Ogus-Shioda *[Shioda; 1979]*

Let $E_1, \ldots, E_g$ and $E'_1, \ldots, E'_g$ be supersingular elliptic curves $(g \geq 2)$.
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E'_1 \times \cdots \times E'_g.$$

We provide:

Algorithm to compute a Φ in polynomial time under GRH, given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$.

Contributions

Theorem: Deligne-Ogus-Shioda *[Shioda; 1979]*

Let $E_1, \dots, E_g$ and $E'_1, \dots, E'_g$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E'_1 \times \cdots \times E'_g.$$

We provide:

Algorithm to compute a Φ in polynomial time under GRH, given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$.

Proof-of-concept implementation in Magma.

Contributions

Theorem: Deligne-Ogus-Shioda *[Shioda; 1979]*

Let $E_1, \ldots, E_g$ and $E'_1, \ldots, E'_g$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E'_1 \times \cdots \times E'_g.$$

We provide:

Algorithm to compute a Φ in polynomial time under GRH, given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$.

Proof-of-concept implementation in Magma.

- Isomorphism of **unpolarized** abelian varieties.

Contributions

Theorem: Deligne-Ogus-Shioda *[Shioda; 1979]*

Let $E_1, \ldots, E_g$ and $E'_1, \ldots, E'_g$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E'_1 \times \cdots \times E'_g.$$

We provide:

Algorithm to compute a Φ in polynomial time under GRH, given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$.

Proof-of-concept implementation in Magma.

- Isomorphism of **unpolarized** abelian varieties.
- False for $g = 1$.

Motivation:

Post-quantum cryptography:

Designing and attacking security protocols, resilient against a quantum adversary.

Motivation:

Post-quantum cryptography:

Designing and attacking security protocols, resilient against a quantum adversary.

- Code-based cryptography,
- Lattice-based cryptography,
- Isogeny-based cryptography.
  SQIsignHD: *[Dartois, Leroux, Robert, Wesolowski; 2023]*
  KLPT^2: *[Castryck, Decru, Kutas, Laval, Petit, Ti; 2025]*

Motivation:

Post-quantum cryptography:

Designing and attacking security protocols, resilient against a quantum adversary.

- Code-based cryptography,
- Lattice-based cryptography,
- Isogeny-based cryptography.
  SQIsignHD: *[Dartois, Leroux, Robert, Wesolowski; 2023]*
  KLPT^2: *[Castryck, Decru, Kutas, Laval, Petit, Ti; 2025]*

Recent breakthrough in isogeny based cryptography.

$\Downarrow$

Toolbox needed to work with products of elliptic curves.

Contents

1. Elliptic curves and Deuring correspondence

2. The Deligne-Ogus-Shioda theorem

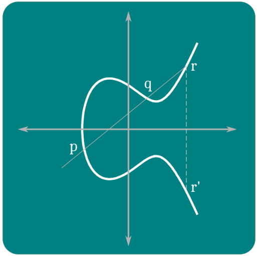
3. The strategy to compute an isomorphism

Elliptic curves and their morphisms

Elliptic curves:

Projective (abelian) algebraic group of dimension 1.

Figure: Example over $\mathbb{R}$.

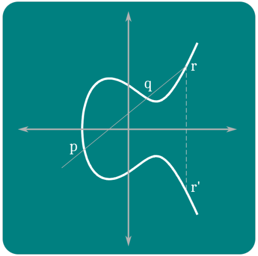


Elliptic curves and their morphisms

Elliptic curves:

Projective (abelian) algebraic group of dimension 1.

Figure: Example over $\mathbb{R}$.



Morphisms of Elliptic Curves

A morphism $\varphi : E \to E'$ is:

- A morphism of varieties,
- A group homomorphism: $\varphi(P +_E Q) = \varphi(P) +_{E'} \varphi(Q)$.

Supersingular elliptic curves

Elliptic curve E over a field k

$\mathbb{Z} \subset \mathrm{End}(E)$

Supersingular elliptic curves

Elliptic curve E over a field k

$\mathbb{Z} \subset \mathrm{End}(E)$

Elliptic curve E over $\mathbb{F}_{p^n}$

$\mathbb{Z}[\pi] \subset \mathrm{End}(E)$,
where $\pi : (x, y) \mapsto (x^{p^n}, y^{p^n})$

Supersingular elliptic curves

Elliptic curve E over a field k

$\mathbb{Z} \subset \mathrm{End}(E)$

Elliptic curve E over $\mathbb{F}_{p^n}$

$\mathbb{Z}[\pi] \subset \mathrm{End}(E)$,
where $\pi : (x, y) \mapsto (x^{p^n}, y^{p^n})$

Supersingular elliptic curve E over $\mathbb{F}_{p^n}$

$\mathrm{End}(E)$ is noncommutative,
of rank 4

Deuring correspondence

Theorem: Structure of Endomorphism Rings

Let E be a supersingular elliptic curve.

$$\mathrm{End}(E) \text{ is a maximal order in the quaternion algebra } \mathbb{Q}_{p,\infty}.$$

Deuring correspondence

Theorem: Structure of Endomorphism Rings

Let E be a supersingular elliptic curve.

$$\mathrm{End}(E) \text{ is a maximal order in the quaternion algebra } \mathbb{Q}_{p,\infty}.$$

Fix E_0 supersingular such that $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ contains a **low-discriminant** quadratic imaginary order (polynomial under GRH).

Deuring correspondence

Theorem: Structure of Endomorphism Rings

Let E be a supersingular elliptic curve.

$$\mathrm{End}(E) \text{ is a maximal order in the quaternion algebra } \mathbb{Q}_{p,\infty}.$$

Fix E_0 supersingular such that $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ contains a **low-discriminant** quadratic imaginary order (polynomial under GRH).

Example when $p \equiv 3 \bmod 4$:

$E_0 : y^2 = x^3 + x, \quad (j(E_0) = 1728).$

$$\mathcal{O}_0 = \mathbb{Z} + i\,\mathbb{Z} + \tfrac{1+i\pi}{2}\,\mathbb{Z} + \tfrac{i+\pi}{2}\,\mathbb{Z},$$

with $i^2 = -1$.

Algorithmic consequences

Hard geometric problems	**Easy algebraic problems**
Compute morphisms $\varphi : E_1 \to E_2$.	$\mathbb{Z}$-linear algebra over quaternions

Algorithmic consequences

Hard geometric problems	**Easy algebraic problems**
Compute morphisms $\varphi : E_1 \to E_2$.	$\mathbb{Z}$-linear algebra over quaternions

(GRH) Proposition: *[Kohel/Lauter/Petit/Tignol; 2014], [Wesolowski; 2021]*

Given $\mathrm{End}(E_i) \simeq \mathcal{O}_i \subset \mathbb{Q}_{p,\infty}$, we can compute morphisms $E_1 \to E_2$.

Algorithmic consequences

Hard geometric problems	Easy algebraic problems
Compute morphisms $\varphi : E_1 \to E_2$.	$\mathbb{Z}$-linear algebra over quaternions

(GRH) Proposition: *[Kohel/Lauter/Petit/Tignol; 2014], [Wesolowski; 2021]*

Given $\mathrm{End}(E_i) \simeq \mathcal{O}_i \subset \mathbb{Q}_{p,\infty}$, we can compute morphisms $E_1 \to E_2$.

$$\text{Compute } \alpha \in \mathrm{End}(E) \text{ such that } \deg(\alpha) = n$$
$$\iff$$
$$\text{Compute } a \in \mathcal{O} \text{ such that } \mathrm{Nrd}(a) = n$$

Our approach: toy example

Compute $\alpha\colon E \to E\,,\ \deg(\alpha) = n$

Our approach: toy example

$$\begin{tikzcd} & \text{Compute } \alpha\colon E \to E\,,\ \deg(\alpha) = n \arrow[dl, "\text{Given End}(E)"'] \\ \begin{array}{c}\text{Compute } a \in \mathcal{O}, \\ \mathrm{Nrd}(a) = n\end{array} & \end{tikzcd}$$

Our approach: toy example

$$\begin{tikzcd} & \text{Compute } \alpha\colon E \to E,\ \deg(\alpha) = n \arrow[dl, "\text{Given } \mathrm{End}(E)"'] \arrow[dr, "\text{Reduce to } E_0"] & \\ \begin{array}{c}\text{Compute } a \in \mathcal{O},\\ \mathrm{Nrd}(a) = n\end{array} & & \begin{array}{c}\text{Compute } \alpha_0\colon E_0 \to E_0,\\ \deg(\alpha) = n\end{array} \end{tikzcd}$$

Our approach: toy example

$$
\begin{tikzcd}
 & \text{Compute } \alpha\colon E \to E\,,\ \deg(\alpha) = n \arrow[dl, "\text{Given } \mathrm{End}(E)"'] \arrow[dr, "\text{Reduce to } E_0"] & \\
\begin{array}{c}\text{Compute } a \in \mathcal{O},\\ \mathrm{Nrd}(a) = n\end{array} \arrow[r, dashed, no head] & \bigoplus \arrow[d] & \begin{array}{c}\text{Compute } \alpha_0\colon E_0 \to E_0,\\ \deg(\alpha) = n\end{array} \arrow[l, dashed, no head] \\
 & \text{Compute } a_0 \in \mathcal{O}_0,\ \mathrm{Nrd}(a_0) = n &
\end{tikzcd}
$$

Our approach: toy example

$$\begin{tikzcd}
& \text{Compute } \alpha\colon E \to E\,,\ \deg(\alpha) = n \arrow[dl, "\text{Given End}(E)"'] \arrow[dr, "\text{Reduce to } E_0"] & \\
\begin{array}{c}\text{Compute } a \in \mathcal{O}, \\ \mathrm{Nrd}(a) = n\end{array} \arrow[r, dash, dashed] & \bigoplus \arrow[d] & \begin{array}{c}\text{Compute } \alpha_0\colon E_0 \to E_0, \\ \deg(\alpha) = n\end{array} \arrow[l, dash, dashed] \\
& \text{Compute } a_0 \in \mathcal{O}_0,\ \mathrm{Nrd}(a_0) = n &
\end{tikzcd}$$

Cornacchia's algorithm is efficient in $\mathcal{O}_0$
thanks to low-discriminant subring.

Contents

1. Elliptic curves and Deuring correspondence

2. **The Deligne-Ogus-Shioda theorem**

3. The strategy to compute an isomorphism

Superspecial Abelian Varieties

Definition-Proposition: Product of Elliptic Curves

Let $E_1, \dots, E_g$ be elliptic curves.

- The product $E_1 \times \cdots \times E_g$ is still a variety and a group.
- A morphism $E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'$ is a morphism of variety and group.

Superspecial Abelian Varieties

Definition-Proposition: Product of Elliptic Curves

Let $E_1, \ldots, E_g$ be elliptic curves.

- The product $E_1 \times \cdots \times E_g$ is still a variety and a group.
- A morphism $E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'$ is a morphism of variety and group.

Theorem: Deligne-Ogus-Shioda *[Shioda 1979]*

Let $E_1, \ldots, E_g$ and $E_1', \ldots, E_g'$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E_1' \times \cdots \times E_g'.$$

Superspecial Abelian Varieties

Definition-Proposition: Product of Elliptic Curves

Let $E_1, \ldots, E_g$ be elliptic curves.

- The product $E_1 \times \cdots \times E_g$ is still a variety and a group.
- A morphism $E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'$ is a morphism of variety and group.

Theorem: Deligne-Ogus-Shioda *[Shioda 1979]*

Let $E_1, \ldots, E_g$ and $E_1', \ldots, E_g'$ be supersingular elliptic curves ($g \geq 2$).
There exists an isomorphism:

$$\Phi : E_1 \times \cdots \times E_g \simeq E_1' \times \cdots \times E_g'.$$

Purpose of our work: Compute Φ such that $\deg(\Phi) = 1$.

Reducing to dimension 2

Representation

g-dimensional morphism
$\Phi : E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_g$

$$\Longleftrightarrow \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1g} \\ \vdots & \ddots & \vdots \\ \varphi_{g1} & \cdots & \varphi_{gg} \end{pmatrix}$$

Reducing to dimension 2

Representation

$$\begin{array}{c} g\text{-dimensional morphism} \\ \Phi : E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_g \end{array} \iff \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1g} \\ \vdots & \ddots & \vdots \\ \varphi_{g1} & \cdots & \varphi_{gg} \end{pmatrix}$$

The 2-dimensional case implies the g-dimensional case.

Reducing to dimension 2

Representation

$$\begin{array}{c} g\text{-dimensional morphism} \\ \Phi : E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_g \end{array} \iff \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1g} \\ \vdots & \ddots & \vdots \\ \varphi_{g1} & \cdots & \varphi_{gg} \end{pmatrix}$$

The 2-dimensional case implies the g-dimensional case.

If $g = 2k$:

- Compute $\Phi_i : E_{2i-1} \times E_{2i} \to E'_{2i-1} \times E'_{2i}$.
- Glue them $\mathrm{diag}(\Phi_1, \ldots, \Phi_k)$.

Reducing to dimension 2

Representation

g-dimensional morphism
$\Phi : E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_g$ $\iff$ $\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1g} \\ \vdots & \ddots & \vdots \\ \varphi_{g1} & \cdots & \varphi_{gg} \end{pmatrix}$

The 2-dimensional case implies the g-dimensional case.

If $g = 2k$:

- Compute $\Phi_i : E_{2i-1} \times E_{2i} \to E'_{2i-1} \times E'_{2i}$.
- Glue them $\mathrm{diag}(\Phi_1, \dots, \Phi_k)$.

If $g = 2k+1$, need the 3×3 case:

Compose:

$$E_1 \times E_2 \times E_3 \xrightarrow{(\Phi_1, \mathrm{Id}_{E_3})} E'_1 \times E'_2 \times E_3$$
$$E'_1 \times E'_2 \times E_3 \xrightarrow{(\mathrm{Id}_{E'_1}, \Phi_2)} E'_1 \times E'_2 \times E'_3$$

Morphisms in dimension 2

Compute $\Phi : E_1 \times E_2 \to E_1' \times E_2'$ **such that** $\deg(\Phi) = 1$**.**

Morphisms in dimension 2

Compute $\Phi : E_1 \times E_2 \to E_1' \times E_2'$ **such that** $\deg(\Phi) = 1$**.**

Proposition: Slight improvement of *[Kani; 2014]* formula

Denote $d_{ij} := \deg(\varphi_{ij})$.

$$(\mathrm{Eq}_{\deg}) \quad \deg(\Phi) = (d_{11} + d_{21})(d_{12} + d_{22}) - \deg(\widehat{\varphi}_{12}\varphi_{11} + \widehat{\varphi}_{22}\varphi_{21}).$$

The underlying algorithmic problems

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.

The underlying algorithmic problems

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.

$\Downarrow$ By Kani's formula.

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute $(\varphi_{ij} : E_j \to E_i')$ satisfying $(\mathrm{Eq}_{\mathrm{deg}})$

The underlying algorithmic problems

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.

$\Downarrow$ By Kani's formula.

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute $(\varphi_{ij} : E_j \to E_i')$ satisfying $(\mathrm{Eq}_{\mathrm{deg}})$

Lemma

Given an isomorphism $(\varphi_{ij})\colon E_1 \times E_2 \to E_1' \times E_2'$, we have an isomorphism:

$$(\widehat{\varphi_{ji}})\colon E_1' \times E_2' \to E_1 \times E_2$$

The underlying algorithmic problems

Given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$ compute an isomorphism $E_1 \times E_2 \to E'_1 \times E'_2$.

$\Downarrow$ By Kani's formula.

Given $\mathrm{End}(E_i), \mathrm{End}(E'_i)$ compute $(\varphi_{ij} : E_j \to E'_i)$ satisfying $(\mathrm{Eq}_{\deg})$

Lemma

Given an isomorphism $(\varphi_{ij})\colon E_1 \times E_2 \to E'_1 \times E'_2$, we have an isomorphism:

$$(\widehat{\varphi_{ji}})\colon E'_1 \times E'_2 \to E_1 \times E_2$$

$$E_1 \times E_2 \longrightarrow E_0 \times E_0 \longleftarrow E'_1 \times E'_2$$

The underlying algorithmic problems

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.

$\Downarrow$ By Kani's formula.

Given $\mathrm{End}(E_i), \mathrm{End}(E_i')$ compute $(\varphi_{ij} : E_j \to E_i')$ satisfying $(\mathrm{Eq}_{\mathrm{deg}})$

Lemma

Given an isomorphism $(\varphi_{ij})\colon E_1 \times E_2 \to E_1' \times E_2'$, we have an isomorphism:

$$(\widehat{\varphi_{ji}})\colon E_1' \times E_2' \to E_1 \times E_2$$

$$E_1 \times E_2 \longrightarrow E_0 \times E_0 \longleftarrow E_1' \times E_2'$$

$\Longrightarrow$

Given $\mathrm{End}(E_i)$, compute $(\varphi_{ij} : E_j \to E_0)$ satisfying $(\mathrm{Eq}_{\mathrm{deg}})$

Contents

1. Elliptic curves and Deuring correspondence

2. The Deligne-Ogus-Shioda theorem

3. The strategy to compute an isomorphism

Completing matrices

Question: Given $\varphi_{11} : E_1 \to E_1'$ and $\varphi_{12} : E_2 \to E_1'$ compute $\varphi_{12}, \varphi_{22}$ such that $\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} : E_1 \times E_2 \to E_1' \times E_2'$ is an isomorphism.

Completing matrices

Question: Given $\varphi_{11} : E_1 \to E_1'$ and $\varphi_{12} : E_2 \to E_1'$ compute $\varphi_{12}, \varphi_{22}$ such that $\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} : E_1 \times E_2 \to E_1' \times E_2'$ is an isomorphism.

We provide

- Algebraic conditions on $\varphi_{11}, \varphi_{12}$ so that $\varphi_{12}, \varphi_{22}$ exist.

Completing matrices

Question: Given $\varphi_{11} : E_1 \to E_1'$ and $\varphi_{12} : E_2 \to E_1'$ compute $\varphi_{12}, \varphi_{22}$ such that $\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} : E_1 \times E_2 \to E_1' \times E_2'$ is an isomorphism.

We provide

- Algebraic conditions on $\varphi_{11}, \varphi_{12}$ so that $\varphi_{12}, \varphi_{22}$ exist.
- An algorithm that given $\mathrm{End}(E_1), \mathrm{End}(E_1'), \mathrm{End}(E_2)$ and $\varphi_{11}, \varphi_{12}$ compute $\varphi_{12}, \varphi_{22}$ at the cost of fixing E_2'.

Computing $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

Computing $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

$$E_1 \times E_2 \xrightarrow[\textbf{Step 1}]{} E_0 \times E \xrightarrow[\text{Step 2}]{} E_0 \times E_0$$

Computing $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

$$E_1 \times E_2 \xrightarrow[\textbf{Step 1}]{} E_0 \times E \xrightarrow[\text{Step 2}]{} E_0 \times E_0$$

(GRH) Step 1

Compute an isomorphism $E_1 \times E_2 \to E_0 \times E$,
for some curve E over which we have no control.

Computing $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

$$E_1 \times E_2 \xrightarrow[\textbf{Step 1}]{} E_0 \times E \xrightarrow[\text{Step 2}]{} E_0 \times E_0$$

(GRH) Step 1

Compute an isomorphism $E_1 \times E_2 \to E_0 \times E$,
for some curve E over which we have no control.

Ingredients:

- Use the Deuring correspondence to compute $\varphi_{11}, \varphi_{12}$.
- Apply previous algorithm to recover $\varphi_{21}, \varphi_{22}$ fixing E.

Computing : $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

$$E_1 \times E_2 \xrightarrow[\text{Step 1}]{} E_0 \times E \xrightarrow[\textbf{Step 2}]{} E_0 \times E_0$$

(GRH) Step 2

Compute an isomorphism $E_0 \times E \to E_0 \times E_0$,
for the curve E given by Step 1.

Computing : $E_1 \times E_2 \to E_0 \times E_0$

Input: E_1, E_2 and their endomorphism rings.

$$E_1 \times E_2 \xrightarrow[\text{Step 1}]{} E_0 \times E \xrightarrow[\textbf{Step 2}]{} E_0 \times E_0$$

(GRH) Step 2

Compute an isomorphism $E_0 \times E \to E_0 \times E_0$,
for the curve E given by Step 1.

Ingredients:

- Rewrite (Eq_{deg}) as $\mathrm{Nrd}(d_{21}\mu - d_{11}\nu) = d_{11}d_{21}$, $\mu, \nu \in \mathcal{O}_0$, Cornacchia's algorithm.
- ℓ-adic algorithms for $\mathcal{M}_2(\mathbb{Z}_\ell) \simeq \mathrm{End}(E_0) \otimes \mathbb{Z}_\ell$ at a prime $\ell \neq p$.

Conclusion

Isomorphisms
$E_1 \times E_2 \to E_0 \times E_0$

Conclusion

$\boxed{\text{Isomorphisms } E_1 \times E_2 \to E_0 \times E_0} \xRightarrow{\textit{duality}} \boxed{\text{Isomorphisms } E_1 \times E_2 \to E_1' \times E_2'}$

Conclusion

$$\boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_0 \times E_0\end{array}} \xRightarrow{\textit{duality}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_1' \times E_2'\end{array}} \xRightarrow{\textit{gluing}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ \prod_{i=1}^{g \geq 2} E_i \to \prod_{i=1}^{g \geq 2} E_i'\end{array}}$$

Conclusion

$$\boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_0 \times E_0\end{array}} \xrightarrow{\textit{duality}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_1' \times E_2'\end{array}} \xrightarrow{\textit{gluing}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ \prod_{i=1}^{g\geq 2} E_i \to \prod_{i=1}^{g\geq 2} E_i'\end{array}}$$

(GRH) Effective Deligne-Ogus-Shioda Theorem:

Let $g \geq 2$. Given supersingular elliptic curves, $E_1, \ldots, E_g$ and $E_1', \ldots, E_g'$ along with their endomorphism rings, we can compute in polynomial time an isomorphism:

$$E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'.$$

Conclusion

$$\boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_0 \times E_0\end{array}} \xRightarrow{\textit{duality}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ E_1 \times E_2 \to E_1' \times E_2'\end{array}} \xRightarrow{\textit{gluing}} \boxed{\begin{array}{c}\text{Isomorphisms}\\ \prod_{i=1}^{g\geq 2} E_i \to \prod_{i=1}^{g\geq 2} E_i'\end{array}}$$

(GRH) Effective Deligne-Ogus-Shioda Theorem:

Let $g \geq 2$. Given supersingular elliptic curves, $E_1, \ldots, E_g$ and $E_1', \ldots, E_g'$ along with their endomorphism rings, we can compute in polynomial time an isomorphism:

$$E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'.$$

Can we compute isomorphisms between more general abelian varieties ?

Generalizations

Let $A/\mathbb{F}_{p^2}$ such that $A \simeq E^g$, for E a supersingular elliptic curve and $g \geq 2$.

How can we compute $\varphi\colon A \simeq E^g$?

Generalizations

Let $A/\mathbb{F}_{p^2}$ such that $A \simeq E^g$, for E a supersingular elliptic curve and $g \geq 2$.

How can we compute $\varphi \colon A \simeq E^g$?

- *This work* solves the case $A = E_1 \times \cdots \times E_g$,
  $\Rightarrow$ with known $\mathrm{End}(E_i)$.

Generalizations

Let $A/\mathbb{F}_{p^2}$ such that $A \simeq E^g$, for E a supersingular elliptic curve and $g \geq 2$.

How can we compute $\varphi \colon A \simeq E^g$?

- *This work* solves the case $A = E_1 \times \cdots \times E_g$,
  $\Rightarrow$ with known $\mathrm{End}(E_i)$.
- *[Montessinos; 2026]* solves the case for any principally polarized abelian surface,
  $\Rightarrow$ with known IKO matrix.

Generalizations

Let $A/\mathbb{F}_{p^2}$ such that $A \simeq E^g$, for E a supersingular elliptic curve and $g \geq 2$.

How can we compute $\varphi \colon A \simeq E^g$?

- *This work* solves the case $A = E_1 \times \cdots \times E_g$,
  $\Rightarrow$ with known $\mathrm{End}(E_i)$.
- *[Montessinos; 2026]* solves the case for any principally polarized abelian surface,
  $\Rightarrow$ with known IKO matrix.
- *[Page, Robert, S.; 2026]* solves the general case,
  $\Rightarrow$ given the module represention of A.

Generalizations

Let $A/\mathbb{F}_{p^2}$ such that $A \simeq E^g$, for E a supersingular elliptic curve and $g \geq 2$.

How can we compute $\varphi\colon A \simeq E^g$?

- *This work* solves the case $A = E_1 \times \cdots \times E_g$,
  $\Rightarrow$ with known $\mathrm{End}(E_i)$.
- *[Montessinos; 2026]* solves the case for any principally polarized abelian surface,
  $\Rightarrow$ with known IKO matrix.
- *[Page, Robert, S.; 2026]* solves the general case,
  $\Rightarrow$ given the module represention of A.

Thank you for your attention!