# Ideal-to-isogeny algorithms: An overview

Lorenz Panny

Technische Universität München

KULB Seminar, 15 December 2023

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

(The $\Longleftarrow$ direction is exponential-time as far as we know.)

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

(The $\Longleftarrow$ direction is exponential-time as far as we know.)

*...but also:*

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.
(The $\Longleftarrow$ direction is exponential-time as far as we know.)

*...but also:*

**The CM action**:

Action of the ideal-class group of an imaginary-quadratic order on the set of curves oriented by that order.

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

(The $\Longleftarrow$ direction is exponential-time as far as we know.)

*...but also:*

**The CM action**:

Action of the ideal-class group of an imaginary-quadratic order on the set of curves oriented by that order.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

# What?

**The Deuring correspondence**:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.
(The $\Longleftarrow$ direction is exponential-time as far as we know.)

*...but also:*

**The CM action**:

Action of the ideal-class group of an imaginary-quadratic order on the set of curves oriented by that order.

The correspondence is polynomial-time in the $\Longrightarrow$ direction. NEW
(The $\Longleftarrow$ direction is quantumly subexponential-time as far as we know.)

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

(Wesolowski ’21: “Orientations and the supersingular endomorphism ring problem”).

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.
- Essential tool for both constructions and attacks.

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.
- Essential tool for both constructions and attacks.

Constructively, *partially* known endomorphism rings are useful.
$\rightsquigarrow$ **Oriented curves** and **the isogeny class-group action**.

# Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

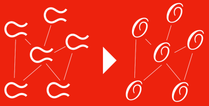
(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.
- Essential tool for both constructions and attacks.

Constructively, *partially* known endomorphism rings are useful.
$\rightsquigarrow$ **Oriented curves** and **the isogeny class-group action**.

- C/R–S/DF–K–S/CSIDH/SCALLOP(-HD)/Clapoti(s)

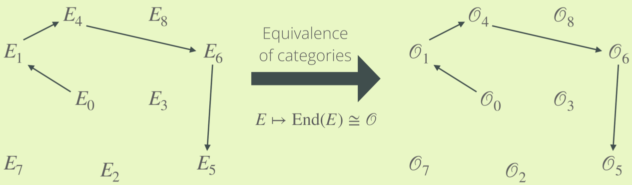
# Part 1: Deuring



# The Deuring Correspondence

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




## curve-order dictionary

| **supersingular curves** | **quaternion orders** |
|---|---|
| curve $E$ (up to Galois conjugacy) | maximal order $\mathcal{O}$ (up to isomorphism) |
| isogeny $\varphi : E_1 \to E_2$ | integral ideal $I_\varphi$ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal |
| endomorphism $\psi : E \to E$ | principal ideal $(\beta) \subset \mathcal{O}$ |
| and this continues for the *degree*, the *dual*, *equivalence*, *composition*... | and this continues for the *norm*, the *dual*, *equivalence*, *multiplication*... |

Radboud University

# History (Deuring)

- **1941**: Deuring proves the correspondence.

# History (Deuring)

- **1941**: Deuring proves the correspondence.

Wenn aber **R** eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von $p$ Hauptideal ist, so gibt es genau eine Invariante $j$, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von $p$ kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der $j$, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

# History (Deuring)

- **1941**: Deuring proves the correspondence.

  Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von $p$ Hauptideal ist, so gibt es genau eine Invariante $j$, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von $p$ kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der $j$, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given $p$.

# History (Deuring)

- **1941**: Deuring proves the correspondence.

  > Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von $p$ Hauptideal ist, so gibt es genau eine Invariante $j$, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von $p$ kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der $j$, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given $p$.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.

# History (Deuring)

- **1941**: Deuring proves the correspondence.

  > Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von $p$ Hauptideal ist, so gibt es genau eine Invariante $j$, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von $p$ kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der $j$, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given $p$.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014)) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.

# History (Deuring)

- **1941**: Deuring proves the correspondence.

  > Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von $p$ Hauptideal ist, so gibt es genau eine Invariante $j$, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von $p$ kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der $j$, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given $p$.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014)) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.
- **2021**: Wesolowski assumes GRH and gives a provably polynomial-time variant.

# Curve world

- Universe: Characteristic $p$. Assume $p \geq 5$.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.

# Curve world

- Universe: Characteristic $p$. Assume $p \geq 5$.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.
- Isogenies, endomorphisms, and so on and so forth.

# Curve world

- Universe: Characteristic $p$. Assume $p \geq 5$.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.
- Isogenies, endomorphisms, and so on and so forth.
- Famous examples:
  - $p \equiv 3 \pmod 4$ and $E\colon y^2 = x^3 + x$ with $j$-invariant 1728.
  - $p \equiv 2 \pmod 3$ and $E\colon y^2 = x^3 + 1$ with $j$-invariant 0.

# Computationally...

- We work with curves defined over $\mathbb{F}_{p^2}$ such that $\pi = [-p]$.
  (This choice is natural: It includes the base-changes of curves defined over $\mathbb{F}_p$.)

# Computationally...

- We work with curves defined over $\mathbb{F}_{p^2}$ such that $\pi = [-p]$.
  (This choice is natural: It includes the base-changes of curves defined over $\mathbb{F}_p$.)
- The group structure is known over all extensions:
  $E(\mathbb{F}_{p^{2k}}) \cong \mathbb{Z}/n \times \mathbb{Z}/n$ where $n = p^k - (-1)^k$.

# Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.

# Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.

# Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.
- Multiplication defined by relations $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$, $\mathbf{ji} = -\mathbf{ij}$.
  Here $q$ is a positive integer satisfying some conditions with respect to $p$.
  ⚠ All valid $q$ define isomorphic algebras $B_{p,\infty}$.

# Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.
- Multiplication defined by relations $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$, $\mathbf{ji} = -\mathbf{ij}$.
  Here $q$ is a positive integer satisfying some conditions with respect to $p$.
  ⚠ All valid $q$ define isomorphic algebras $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ has a conjugation $\overline{\phantom{x}}$ which negates $\mathbf{i}, \mathbf{j}, \mathbf{ij}$.
  The norm and trace of an element $\alpha$ are $\alpha\overline{\alpha} \in \mathbb{Z}_{\geq 0}$ and $\alpha + \overline{\alpha} \in \mathbb{Z}$.

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.
- A fractional ideal $I$ is a left $\mathcal{O}$-ideal if $\mathcal{O}I \subseteq I$. (Similarly on the right.)

# Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.
- A fractional ideal $I$ is a left $\mathcal{O}$-ideal if $\mathcal{O}I \subseteq I$. (Similarly on the right.)
  We say $I$ connects $\mathcal{O}$ and $\mathcal{O}'$ if $\mathcal{O}I \subseteq I$ and $I\mathcal{O}' \subseteq I$.

# Computationally, ...

- We typically work with one fixed choice of $q$ for each $p$.

# Computationally, ...

- We typically work with one fixed choice of $q$ for each $p$.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.

# Computationally, ...

- We typically work with one fixed choice of $q$ for each $p$.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.
- Quaternion lattices are represented by **a** $\mathbb{Z}$-basis.

# Computationally, ...

- We typically work with one fixed choice of $q$ for each $p$.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.
- Quaternion lattices are represented by **a** $\mathbb{Z}$-basis.
- All the basic algorithms are essentially linear algebra.

# Computationally, ...

- We typically work with one fixed choice of $q$ for each $p$.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.
- Quaternion lattices are represented by **a** $\mathbb{Z}$-basis.
- All the basic algorithms are essentially linear algebra.

General theme: Things are easy in quaternion land.

# From curves to quaternions

$$E \mapsto \mathcal{O}$$

# Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon \ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon \ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

# Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$\iota^2 = [-1]$, $\pi\iota = -\iota\pi$, and $\pi^2 = [-p]$.

# Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$$\iota^2 = [-1],\ \pi\iota = -\iota\pi,\ \text{and } \pi^2 = [-p].$$

Hence, in the quaternion algebra where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$, the pair $(\iota, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

# Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon \ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon \ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\iota^2 = [-1]$, $\pi\iota = -\iota\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$, the pair $(\iota, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

In fact, the image in $B_{p,\infty}$ of a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ is given by

$$\{1, \quad \mathbf{i}, \quad (\mathbf{i}+\mathbf{j})/2, \quad (1+\mathbf{ij})/2\}\,.$$

# Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon\; (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon\; (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

# Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon \ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon \ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\omega^3 = [1]$, $\omega\pi + \pi\omega = -\pi$, and $\pi^2 = [-p]$.

# Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E \colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega \colon\ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi \colon\ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\omega^3 = [1]$, $\omega\pi + \pi\omega = -\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -3$ and $\mathbf{j}^2 = -p$, the pair $(2\omega + 1, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

# Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon\ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon\ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\omega^3 = [1]$, $\omega\pi + \pi\omega = -\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -3$ and $\mathbf{j}^2 = -p$, the pair $(2\omega + 1, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

In fact, the image in $B_{p,\infty}$ of a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ is given by

$$\{1, \quad (1 + \mathbf{i})/2, \quad (\mathbf{j} + \mathbf{ij})/2, \quad (\mathbf{i} + \mathbf{ij})/3\}\,.$$

# From curves to quaternions

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.

# From curves to quaternions

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is polynomial-time.

# From curves to quaternions

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \; (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is polynomial-time.
  - Multiple $q$ define the *same* $B_{p,\infty}$.
    Need to convert from $\mathbf{i}^2 = -q$ basis to $\mathbf{i}'^2 = -q'$ basis.

# From curves to quaternions

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is polynomial-time.
  - Multiple $q$ define the *same* $B_{p,\infty}$.
    Need to convert from $\mathbf{i}^2 = -q$ basis to $\mathbf{i}'^2 = -q'$ basis.

**Lemma 10.** *Let $p$ be a prime number and $q, q' \in \mathbb{Z}_{>0}$ such that $B = (-q, -p \mid \mathbb{Q})$ and $B' = (-q', -p \mid \mathbb{Q})$ are quaternion algebras ramified at $p$ and $\infty$.*

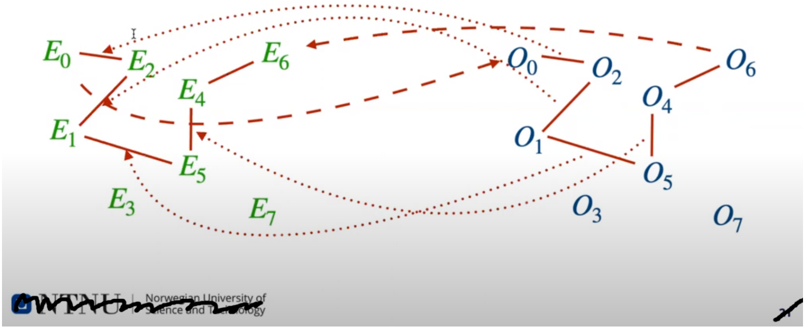
*Then there exist $x, y \in \mathbb{Q}$ such that $x^2 + py^2 = q'/q$. Writing $1, \mathbf{i}', \mathbf{j}', \mathbf{k}'$ for the generators of $B'$ and $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ for the generators of $B$, and setting $\gamma := x + y\mathbf{j}$, the mapping*

$$\mathbf{i}' \mapsto \mathbf{i}\gamma, \qquad \mathbf{j}' \mapsto \mathbf{j}, \qquad \mathbf{k}' \mapsto \mathbf{k}\gamma$$

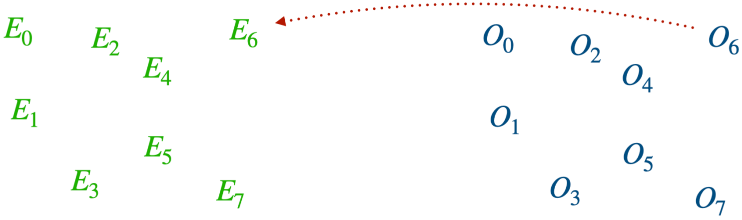
*defines a $\mathbb{Q}$-algebra isomorphism $B' \xrightarrow{\sim} B$.*

# From quaternions to curves

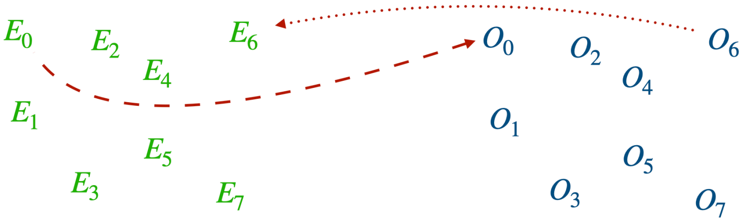
# From quaternions to curves



# From quaternions to curves

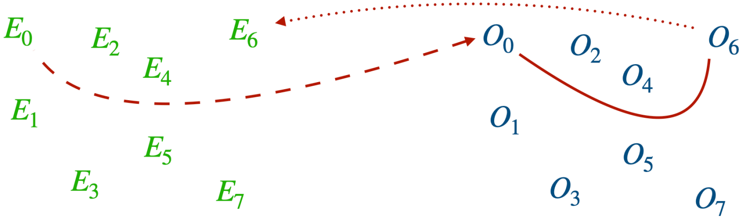


# From quaternions to curves



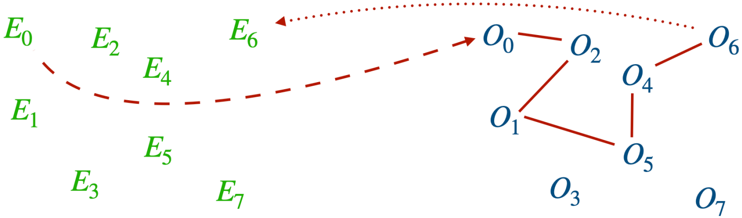

- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.

# From quaternions to curves



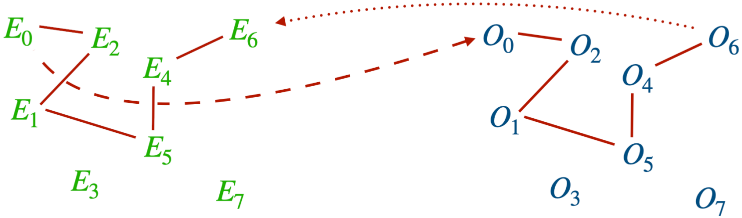

- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal.
  Solve the "isogeny problem" in quaternion land.

# From quaternions to curves



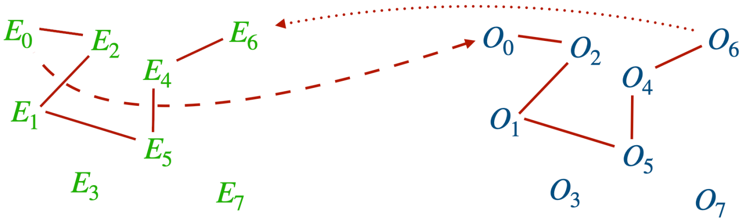

- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT.
  Solve the "isogeny problem" in quaternion land.

# From quaternions to curves




- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT.
  Solve the "isogeny problem" in quaternion land.
- Step 2: Ideal-to-isogeny.
  Map the solution "down" to curve land.

# From quaternions to curves




- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT.
  Solve the "isogeny problem" in quaternion land.
- Step 2: Ideal-to-isogeny.
  Map the solution "down" to curve land.

I will talk about these *in reverse order*.

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

Algorithms:

- Write $I = (N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

Algorithms:

- Write $I = (N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, ..., H'_r \rangle$.

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

Algorithms:

- Write $I = (N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, \ldots, H'_r \rangle$.
- If $\varphi_I$ is cyclic, we have $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

<u>Algorithms:</u>

- Write $I = (N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, ..., H'_r \rangle$.
- If $\varphi_I$ is cyclic, we have $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

Crucial observation: Complexity depends on factorization of $N$.

# Step 2: Ideal-to-isogeny

The isogeny $\varphi_I$ defined by an ideal $I$ has kernel $H_I = \bigcap_{\omega \in I} \ker \omega$.

<u>Algorithms:</u>

- Write $I = (N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, \ldots, H'_r \rangle$.
- If $\varphi_I$ is cyclic, we have $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

Crucial observation: Complexity depends on factorization of $N$.
$\therefore$ No choice in $N$: It's the norm of $I$.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1}\cdots\ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* $\varphi_J$ will be different from $\varphi_I$.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* $\varphi_J$ will be different from $\varphi_I$.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^{\bullet}$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* $\varphi_J$ will be different from $\varphi_I$.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by $\gamma$! (Proof: $I\gamma^{-1}\bar{J}\gamma$)

    $\rightsquigarrow$ We can evaluate $\omega$ without computing $\varphi_I$ first.

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* $\varphi_J$ will be different from $\varphi_I$.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by $\gamma$! (Proof: $I\gamma^{-1}\bar{J}\gamma$)
    $\rightsquigarrow$ We can evaluate $\omega$ without computing $\varphi_I$ first.
  - Hence, for $T$ coprime to $N'$, with $S := N'^{-1} \bmod T$,
    $$\varphi_I|_{E[T]} = S\varphi_J\omega|_{E[T]}\,.$$

# Step 1: Convenient connecting ideals

**KLPT**

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm $N'$.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* $\varphi_J$ will be different from $\varphi_I$.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by $\gamma$! (Proof: $I\gamma^{-1}\bar{J}\gamma$)

    $\rightsquigarrow$ We can evaluate $\omega$ without computing $\varphi_I$ first.
  - Hence, for $T$ coprime to $N'$, with $S := N'^{-1} \bmod T$,

$$\varphi_I|_{E[T]} = S\varphi_J\omega|_{E[T]}\,.$$

$\rightsquigarrow$ Do it twice with coprime degrees to evaluate on any point.

# Advertisement: *Deuring for the People!*

So we now know a way to do it, but how do we *actually* do it?

# Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ We have to work in field extensions.

# Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ We have to work in field extensions.

!! Lots of choice for prime powers $\ell^e$.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with $k$ small.

# Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ We have to work in field extensions.

!! Lots of choice for prime powers $\ell^e$.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with $k$ small.

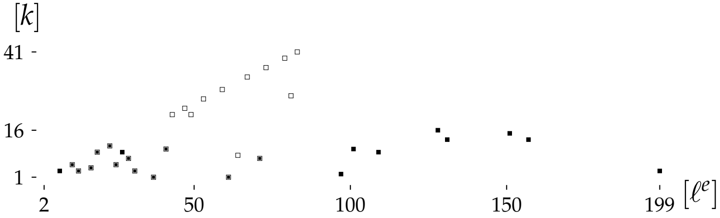
$\rightsquigarrow$ Tradeoff: *number* of operations $\longleftrightarrow$ *cost* of arithmetic.

# Cool trick #1: Convenient torsion is convenient

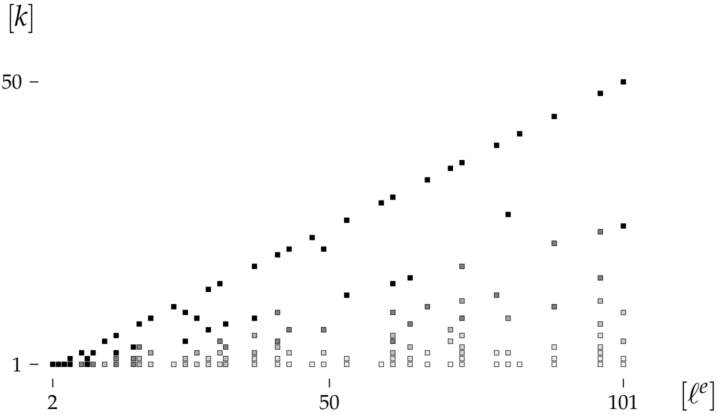
- Norm is big $\rightsquigarrow$ We have to work in field extensions.

!! Lots of choice for prime powers $\ell^e$.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with $k$ small.

$\rightsquigarrow$ <u>Tradeoff:</u> *number* of operations $\longleftrightarrow$ *cost* of arithmetic.



# Heatmap




Average extension $k$ required to access $\ell^e$-torsion.

# Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by smaller minimal polynomials of isogenies.

  They are irreducible divisors of the kernel polynomial.

# Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.
- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

# Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.
- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

**Algorithm 5:** `PushSubgroup`$(E, f, \varphi)$

**Input:** Elliptic curve $E/\mathbb{F}_q$, minimal polynomial $f \in \mathbb{F}_q[X]$ of a subgroup $G \leq E$, isogeny $\varphi \colon E \to E'$ defined over $\mathbb{F}_q$.

**Output:** Minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of the subgroup $\varphi(G) \leq E'$.

1 Write the x-coordinate map of $\varphi$ as a fraction $g_1/g_2$ of polynomials $g_1, g_2 \in \mathbb{F}_q[X]$.
2 Let $g_{\ker} \leftarrow \gcd(g_2, f)$ and $f_1 \leftarrow f/g_{\ker}$.
3 Compute $g_1 \cdot g_2^{-1} \bmod f_1 \in \mathbb{F}_q[X]$ and reinterpret it as a quotient-ring element $\alpha \in \mathbb{F}_q[X]/f_1$.
4 Find the minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of $\alpha$ over $\mathbb{F}_q$ using Shoup's algorithm.
5 Return $f^\varphi$.

# Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.
- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

**Algorithm 5:** `PushSubgroup`$(E, f, \varphi)$

**Input:** Elliptic curve $E/\mathbb{F}_q$, minimal polynomial $f \in \mathbb{F}_q[X]$ of a subgroup $G \leq E$, isogeny $\varphi\colon E \to E'$ defined over $\mathbb{F}_q$.

**Output:** Minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of the subgroup $\varphi(G) \leq E'$.

1. Write the x-coordinate map of $\varphi$ as a fraction $g_1/g_2$ of polynomials $g_1, g_2 \in \mathbb{F}_q[X]$.
2. Let $g_{\ker} \leftarrow \gcd(g_2, f)$ and $f_1 \leftarrow f/g_{\ker}$.
3. Compute $g_1 \cdot g_2^{-1} \bmod f_1 \in \mathbb{F}_q[X]$ and reinterpret it as a quotient-ring element $\alpha \in \mathbb{F}_q[X]/f_1$.
4. Find the minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of $\alpha$ over $\mathbb{F}_q$ using Shoup's algorithm.
5. Return $f^\varphi$.

Complexity: $O(k^2) + \widetilde{O}(n)$. Naïvely $O(nk(\log k)^{O(1)})$.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- Ingredient #1: Bröker's algorithm.
  Find $q$ such that $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial $H_{-q}$, construct a curve with this $j$-invariant.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- Ingredient #1: Bröker's algorithm.
  Find $q$ such that $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial $H_{-q}$, construct a curve with this $j$-invariant.

- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  Algorithm to compute a *normalized* degree-$q$ isogeny in time $\widetilde{O}(q)$.
  Composing the desired endomorphism $\vartheta \colon E \to E$ with the isomorphism $\tau \colon (x, y) \mapsto (-qx, \sqrt{-q}^3 y)$ makes it normalized.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- Ingredient #1: Bröker's algorithm.
  Find $q$ such that $\mathbf{i}^2{=}-q$, $\mathbf{j}^2{=}-p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial $H_{-q}$, construct a curve with this $j$-invariant.

- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  Algorithm to compute a *normalized* degree-$q$ isogeny in time $\widetilde{O}(q)$.
  Composing the desired endomorphism $\vartheta\colon E \to E$ with the isomorphism $\tau\colon (x,y) \mapsto (-qx, \sqrt{-q}^3 y)$ makes it normalized.

- Ingredient #3: Ibukiyama's theorem.
  Explicit basis for a maximal order of $B_{p,\infty}$ with an endomorphism $\sqrt{-q}$.
  In fact, such a maximal order is almost unique.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- Ingredient #1: Bröker's algorithm.
  !! Part of SageMath $\geq 10.3$.

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.
- Ingredient #1: Bröker's algorithm.
  !! Part of SageMath $\geq$ 10.3.
- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  !! Part of SageMath $\geq$ 10.2 (thanks to Rémy Oudompheng).

# Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- Ingredient #1: Bröker's algorithm.
  !! Part of SageMath $\geq 10.3$.

- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  !! Part of SageMath $\geq 10.2$ (thanks to Rémy Oudompheng).

- Ingredient #3: Ibukiyama's theorem.
  ?? Are we waiting for proper endomorphism-ring code?

# Connecting ideals

Finding **a** connecting $(\mathcal{O}, \mathcal{O}')$-ideal is straightforward:

1. Compute $\mathcal{O}\mathcal{O}' = \mathrm{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.

# Connecting ideals

Finding **a** connecting $(\mathcal{O}, \mathcal{O}')$-ideal is straightforward:

1. Compute $\mathcal{O}\mathcal{O}' = \operatorname{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.
   (Also, it's integral only in trivial cases $\rightsquigarrow$ scale by denominator in $\mathbb{Z}$.)

# Open-source code

`https://github.com/friends-of-quaternions/deuring`

# Open-source code

https://github.com/friends-of-quaternions/deuring

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
```

# Open-source code

https://github.com/friends-of-quaternions/deuring

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
```

# Open-source code

https://github.com/friends-of-quaternions/deuring

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
```

# Open-source code

https://github.com/friends-of-quaternions/deuring

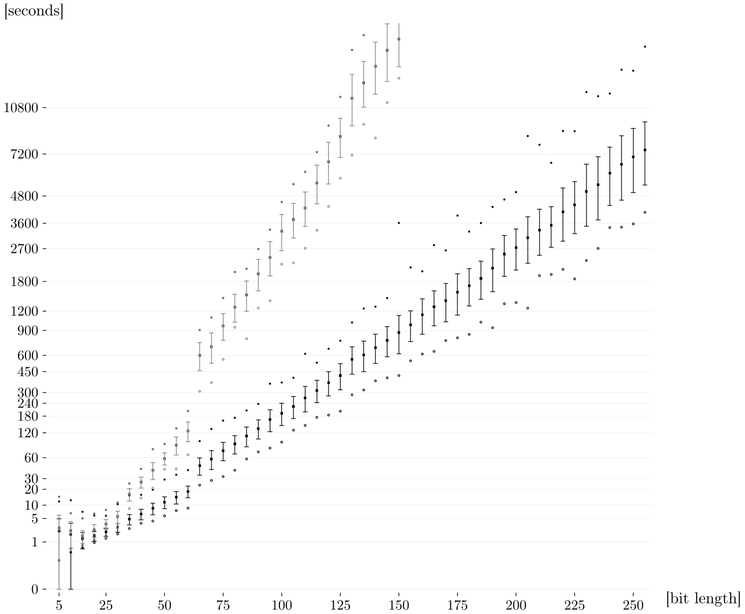
```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
sage: I = random_ideal(O0)
sage: I
Fractional ideal (-2227737332 - 2733458099/2*i - 36405/2*j
    + 7076*k, -1722016565/2 + 1401001825/2*i + 551/2*j
    + 16579/2*k, -2147483647 - 9708*j + 12777*k, -2147483647
    - 2147483647*i - 22485*j + 3069*k)
```

# Open-source code

https://github.com/friends-of-quaternions/deuring

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
sage: I = random_ideal(O0)
sage: I
Fractional ideal (-2227737332 - 2733458099/2*i - 36405/2*j
    + 7076*k, -1722016565/2 + 1401001825/2*i + 551/2*j
    + 16579/2*k, -2147483647 - 9708*j + 12777*k, -2147483647
    - 2147483647*i - 22485*j + 3069*k)
sage: E1, phi, _ = constructive_deuring(I, E0, iota)
sage: phi
Composite morphism of degree 14763897348161206530374369280
          = 2^29*3^3*5*7^2*11*13*17*31*41*43^2*61*79*151:
  From: Elliptic Curve defined by y^2 = x^3 + x over
          Finite Field in i of size 2147483647^2
  To:   Elliptic Curve defined by y^2 = x^3 + (1474953432*i
              +1816867654)*x + (581679615*i+260136654)
          over Finite Field in i of size 2147483647^2
```

# Timings (SageMath, single core)



# Timings (SageMath, single core)

We've been informed of one run for a 521-bit characteristic that took only about 7 hours.

$\rightsquigarrow$ Definitely practical for parameter setup etc.!

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.
- General starting curves: Easy to compute $E \to E_0 \to E'$.

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.
- General starting curves: Easy to compute $E \to E_0 \to E'$.
- Doing this would break SQIsign.

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.
- General starting curves: Easy to compute $E \to E_0 \to E'$.
- Doing this would break SQIsign.

Solution:

$$E_1 \xrightarrow{I_1} E_2 \xrightarrow{I_2} E_3 \xrightarrow{I_3} \cdots \xrightarrow{I_{n-1}} E_{n-1} \xrightarrow{I_n} E_n$$

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.
- General starting curves: Easy to compute $E \to E_0 \to E'$.
- Doing this would break SQIsign.

<u>Solution:</u>

$$\begin{tikzcd}
E_1 \arrow[r, "I_1"] & E_2 \arrow[r, "I_2"] & E_3 \arrow[r, "I_3"] & \cdots \arrow[r, "I_{n-1}"] & E_{n-1} \arrow[r, "I_n"] & E_n \\
& & E_0 \arrow[ull, bend left, "J_1"] \arrow[ul, bend left, "J_2"] \arrow[u, "J_3"] \arrow[urr, bend right, "J_{n-1}"'] \arrow[urrr, bend right, "J_n"'] & & &
\end{tikzcd}$$

# Non-special starting curves (e.g., SQIsign)

- Previous discussion: Special starting curve $E_0$.
- General starting curves: Easy to compute $E \to E_0 \to E'$.
- Doing this would break SQIsign.

Solution:

$$\begin{tikzcd}
E_1 \arrow[r, "I_1"] & E_2 \arrow[r, "I_2"] & E_3 \arrow[r, "I_3"] & \cdots \arrow[r, "I_{n-1}"] & E_{n-1} \arrow[r, "I_n"] & E_n \\
 & & E_0 \arrow[ull, bend left, "J_1"] \arrow[ul, "J_2"] \arrow[u, "J_3"] \arrow[urr, bend right, "J_{n-1}"'] \arrow[urrr, bend right, "J_n"'] & & &
\end{tikzcd}$$

∴ Algorithms for one "step" are quite technical.
See [ePrint 2022/234] and the more recent [ePrint 2023/1251].

# Part 2: The CM action

# The CM action on oriented curves

Now let $\mathcal{O}$ be an imaginary-quadratic order, say $\mathcal{O} = \mathbb{Z}[\vartheta]$.

- We consider $\mathcal{O}$-oriented elliptic curves: pairs $(E, \iota)$ with an explicit embedding $\iota\colon \mathcal{O} \to \mathrm{End}(E)$.

# The CM action on oriented curves

Now let $\mathcal{O}$ be an imaginary-quadratic order, say $\mathcal{O} = \mathbb{Z}[\vartheta]$.

- We consider $\mathcal{O}$-oriented elliptic curves: pairs $(E, \iota)$ with an explicit embedding $\iota\colon \mathcal{O} \to \mathrm{End}(E)$.
- Basic example: If $E/\mathbb{F}_q$ and $\pi \notin \mathbb{Z}$, then $\mathcal{O} = \mathbb{Z}[\pi]$ works.

# The CM action on oriented curves

Now let $\mathcal{O}$ be an imaginary-quadratic order, say $\mathcal{O} = \mathbb{Z}[\vartheta]$.

- We consider $\mathcal{O}$-oriented elliptic curves: pairs $(E, \iota)$ with an explicit embedding $\iota \colon \mathcal{O} \to \mathrm{End}(E)$.
- Basic example: If $E/\mathbb{F}_q$ and $\pi \notin \mathbb{Z}$, then $\mathcal{O} = \mathbb{Z}[\pi]$ works.
- Other examples: $E/\mathbb{F}_{p^2}$ supersingular; many possible $\mathcal{O}$.

# The CM action on oriented curves

Now let $\mathcal{O}$ be an imaginary-quadratic order, say $\mathcal{O} = \mathbb{Z}[\vartheta]$.

- We consider $\mathcal{O}$-oriented elliptic curves: pairs $(E, \iota)$ with an explicit embedding $\iota \colon \mathcal{O} \to \mathrm{End}(E)$.
- Basic example: If $E/\mathbb{F}_q$ and $\pi \notin \mathbb{Z}$, then $\mathcal{O} = \mathbb{Z}[\pi]$ works.
- Other examples: $E/\mathbb{F}_{p^2}$ supersingular; many possible $\mathcal{O}$.

Ideals of $\mathcal{O}$ again define isogenies

$$\varphi \colon (E, \iota) \longrightarrow (E', \iota')$$

satisfying $\varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi$ for all $\alpha \in \mathcal{O}$.

# The CM action on oriented curves

Now let $\mathcal{O}$ be an imaginary-quadratic order, say $\mathcal{O} = \mathbb{Z}[\vartheta]$.

- We consider $\mathcal{O}$-oriented elliptic curves: pairs $(E, \iota)$ with an explicit embedding $\iota\colon \mathcal{O} \to \mathrm{End}(E)$.
- Basic example: If $E/\mathbb{F}_q$ and $\pi \notin \mathbb{Z}$, then $\mathcal{O} = \mathbb{Z}[\pi]$ works.
- Other examples: $E/\mathbb{F}_{p^2}$ supersingular; many possible $\mathcal{O}$.

Ideals of $\mathcal{O}$ again define isogenies

$$\varphi\colon (E, \iota) \longrightarrow (E', \iota')$$

satisfying $\varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi$ for all $\alpha \in \mathcal{O}$.

$\Longrightarrow$ Compatibility for repeated applications of ideals of $\mathcal{O}$.
$\Longrightarrow$ Group action of $\mathrm{cl}(\mathcal{O})$ on such pairs!

# The basic strategy à la C/R–S

- Let $\mathfrak{l}_1, ..., \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.

# The basic strategy à la C/R–S

- Let $\mathfrak{l}_1, ..., \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.
- Evaluating a single $\mathfrak{l}_i$: Write $\mathfrak{l}_i = (\ell_i, \vartheta - \lambda_i)$.
  Then the kernel is an order-$\ell_i$ point $P$ with $\vartheta(P) = [\lambda_i]P$.

# The basic strategy à la C/R–S

- Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and <u>suppose</u> $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.

- Evaluating a single $\mathfrak{l}_i$: Write $\mathfrak{l}_i = (\ell_i, \vartheta - \lambda_i)$.
  Then the kernel is an order-$\ell_i$ point $P$ with $\vartheta(P) = [\lambda_i]P$.
- Optimizations: Batch multiple $\mathfrak{l}_i$ together $\rightsquigarrow$ "strategies".

# The basic problem with the basic strategy

- Couveignes: This gives a “hard homogeneous space” (weirder name for a one-way group action).
- The CSIDH paper repeats this.

# The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way group action).
- The CSIDH paper repeats this.

<u>Issue:</u>

- Representing $\mathrm{cl}(\mathcal{O})$ by the group $(\mathbb{Z}^n, +)$ of exponents makes the exponents grow larger with each operation.
  - $\rightsquigarrow$ Cost of evaluating after $k$ operations is $O(\exp(k))$.

# The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way group action).
- The CSIDH paper repeats this.

Issue:

- Representing $\mathrm{cl}(\mathcal{O})$ by the group $(\mathbb{Z}^n, +)$ of exponents makes the exponents grow larger with each operation.
  - $\rightsquigarrow$ Cost of evaluating after $k$ operations is $O(\exp(k))$.
- Representing $\mathrm{cl}(\mathcal{O})$ as reduced ideals allows computing in $\mathrm{cl}(\mathcal{O})$ efficiently, but evaluation becomes superpolynomial.

# Effective group actions à la CSI-FiSh/SCALLOP(-HD)

Partial solution:

- Compute the relation lattice $\Lambda := \{v \in \mathbb{Z}^n \mid v * E_0 = E_0\}$.

# Effective group actions à la CSI-FiSh/SCALLOP(-HD)

<u>Partial solution:</u>

- Compute the relation lattice $\Lambda := \{v \in \mathbb{Z}^n \mid v * E_0 = E_0\}$.
- Work with exponent vectors anyway, but now in $\mathbb{Z}^n/\Lambda$.

# Effective group actions à la CSI-FiSh/SCALLOP(-HD)

Partial solution:

- Compute the relation lattice $\Lambda := \{v \in \mathbb{Z}^n \mid v * E_0 = E_0\}$.
- Work with exponent vectors anyway, but now in $\mathbb{Z}^n/\Lambda$.
- To evaluate the action, solve a close(st)-vector problem.
  $\rightsquigarrow$ short equivalent exponent vector!

# "Effective" group actions à la CSI-FiSh/SCALLOP(-HD)

- To evaluate the action, solve a close(st)-vector problem.

# “Effective” group actions à la CSI-FiSh/SCALLOP(-HD)

- To evaluate the action, solve a close(st)-vector problem.
- CSI-FiSh: This is practically fast for CSIDH-512.

# “Effective” group actions à la CSI-FiSh/SCALLOP(-HD)

- To evaluate the action, solve a close(st)-vector problem.
- CSI-FiSh: This is practically fast for CSIDH-512.
- Still, it’s asymptotically the bottleneck!

  https://yx7.cc/blah/2023-04-14.html

# SCALLO, PhD

# Even more maritime isogenies??

## Noun [ edit ]

**clapotis** *m* (*plural* **clapotis**)

1. lapping of water against a surface [synonyms ▲]

# Polynomial-time group action: Clapoti(s)

- Recently, Page–Robert announced a polynomial-time algorithm for evaluating the action on arbitrary ideals.

# Polynomial-time group action: Clapoti(s)

- Recently, Page–Robert announced a polynomial-time algorithm for evaluating the action on arbitrary ideals.

Idea:

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$.
  Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

# Polynomial-time group action: Clapoti(s)

- Recently, Page–Robert announced a polynomial-time algorithm for evaluating the action on arbitrary ideals.

<u>Idea:</u>

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$. Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

$$\begin{tikzcd} E \arrow[r, "\phi_{\mathfrak{b}}"] \arrow[d, "\phi_{\overline{\mathfrak{c}}}"'] & E_{\mathfrak{a}} \arrow[d, "\psi_{\overline{\mathfrak{c}}}"] \\ E_{\overline{\mathfrak{a}}} \arrow[r, "\psi_{\mathfrak{b}}"'] & E \end{tikzcd}$$

# Polynomial-time group action: Clapoti(s)

- Recently, Page–Robert announced a polynomial-time algorithm for evaluating the action on arbitrary ideals.

<u>Idea:</u>

- Find two ideals $\mathfrak{b}$, $\mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$. Let $N := \operatorname{norm}(\mathfrak{b}) + \operatorname{norm}(\mathfrak{c})$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ {\scriptstyle \phi_{\overline{\mathfrak{c}}}}\big\downarrow & & \big\downarrow{\scriptstyle \psi_{\overline{\mathfrak{c}}}} \\ E_{\overline{\mathfrak{a}}} & \xrightarrow[\psi_{\mathfrak{b}}]{} & E \end{array}$$

- Kani: This gives an $N$-isogeny $F\colon\ E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$,

$$(P, Q) \mapsto (\phi_{\mathfrak{b}}(P) + \widehat{\psi_{\overline{\mathfrak{c}}}}(Q),\ -\phi_{\overline{\mathfrak{c}}}(P) + \widehat{\psi_{\mathfrak{b}}}(Q)).$$

# Polynomial-time group action: Clapoti(s)

- Recently, Page–Robert announced a polynomial-time algorithm for evaluating the action on arbitrary ideals.

<u>Idea:</u>

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$. Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ {\scriptstyle \phi_{\overline{\mathfrak{c}}}}\downarrow & & \downarrow{\scriptstyle \psi_{\overline{\mathfrak{c}}}} \\ E_{\overline{\mathfrak{a}}} & \xrightarrow[\psi_{\mathfrak{b}}]{} & E \end{array}$$

- Kani: This gives an $N$-isogeny $F\colon\ E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$,
$$(P, Q) \mapsto (\phi_{\mathfrak{b}}(P) + \widehat{\psi_{\overline{\mathfrak{c}}}}(Q),\ -\phi_{\overline{\mathfrak{c}}}(P) + \widehat{\psi_{\mathfrak{b}}}(Q)).$$

- The kernel is $\ker(F) = \{(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\overline{\mathfrak{c}}}(R)) : R \in E_{\mathfrak{a}}[N]\}$.

# Polynomial-time group action: Clapoti(s)

- The kernel is $\ker(F) = \{(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\bar{\mathfrak{c}}}(R)) : R \in E_{\mathfrak{a}}[N]\}$.

# Polynomial-time group action: Clapoti(s)

- The kernel is $\ker(F) = \{(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\bar{\mathfrak{c}}}(R)) : R \in E_{\mathfrak{a}}[N]\}$.

*For some reason* this is supposedly the same thing as

$$\ker(F) = \left\{([\mathrm{norm}(\mathfrak{b})]R, \gamma(R)) \mid R \in E[N]\right\}$$

where $\gamma \in \mathrm{End}(E)$ is a generator of the principal ideal $\mathfrak{b}\bar{\mathfrak{c}}$.

# Polynomial-time group action: Clapoti(s)

- The kernel is $\ker(F) = \{(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\overline{\mathfrak{c}}}(R)) : R \in E_{\mathfrak{a}}[N]\}$.

*For some reason* this is supposedly the same thing as

$$\ker(F) = \left\{([\mathrm{norm}(\mathfrak{b})]R, \gamma(R)) \mid R \in E[N]\right\}$$

where $\gamma \in \mathrm{End}(E)$ is a generator of the principal ideal $\mathfrak{b}\overline{\mathfrak{c}}$.

Let us explain the case of the specific isogeny $F$ to illustrate the usefulness of the module representation. We have $\mathfrak{b} = \frac{\overline{\gamma_b}}{\mathcal{N}(\mathfrak{a})}\mathfrak{a}$, so the multiplication map $\overline{\gamma_b}/\mathcal{N}(\mathfrak{a})\colon (\mathfrak{a}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \to (\mathfrak{b}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{b}))$ is an isomorphism $\alpha_b$ of unimodular Hermitian modules. The isogeny $\phi_{\mathfrak{b}} : E \to E_{\mathfrak{a}}$ corresponds from the module point of view to the post-composition of $\alpha_b$ with the natural $\mathcal{N}(\mathfrak{b})$-similitude given by the inclusion $(\mathfrak{b}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{b})) \to (R, \mathcal{N}(\cdot))$.

Likewise, the isogeny $F$ from Proposition 2.1 corresponds to a $N$-similitude $\psi\colon (\mathfrak{a}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \oplus (\overline{\mathfrak{a}}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \to (R, \mathcal{N}(\cdot)) \oplus (R, \mathcal{N}(\cdot))$.

The anti-equivalence of categories is exact, so the kernel of $F$ corresponds to the cokernel of $\psi$. Fix two generators of $\mathfrak{a}$, these generators induce surjective maps $R^2 \twoheadrightarrow \mathfrak{a}$, $R^2 \twoheadrightarrow \overline{\mathfrak{a}}$. Pre-composing $\psi$ with these epimorphisms, we get a module map $\tilde{\psi}\colon R^4 \to R^2$, whose cokernel is exactly the cokernel of $\psi$. The map $\tilde{\psi}$ is given by a $4 \times 2$ matrix of elements of $R$, hence of endomorphisms on $E$, and corresponds on the abelian variety side to a morphism $\tilde{\Phi}\colon E^2 \to E^4$. By exactness, the cokernel $\operatorname{coker}\tilde{\psi} = \operatorname{coker}\psi$, which as we have seen corresponds to $\operatorname{Ker} F$, is given by $\operatorname{Ker}\tilde{\Phi}$ which we can explicitly compute since the orientation by $R$ is effective on $E$.

# Polynomial-time group action: Clapoti(s)

- Minor detail: $N$ has no reason at all to be "nice".

$\rightsquigarrow$ $\{4, 8\}$-dimensional isogenies, per the usual...

# Interlude

# We could've had it all (5 years ago) [ePrint 2018/665]

$$(\mathfrak{a}_1 * E) \times \cdots \times (\mathfrak{a}_n * E) \cong (\mathfrak{a}_1 \cdots \mathfrak{a}_n) * E \times E^{n-1}. \tag{4}$$

and more generally, we have

$$\begin{aligned} (\mathfrak{a}_1 * E) \times \cdots \times (\mathfrak{a}_n * E) \cong (\mathfrak{a}'_1 * E) \times \cdots \times (\mathfrak{a}'_n * E) \quad & \text{if and only if} \\ \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}'_1 \cdots \mathfrak{a}'_n \quad & \text{as ideal classes in } \mathrm{Cl}(\mathscr{O}). \end{aligned} \tag{5}$$

As a side note, we now mention that those properties can *in part* be established using elementary techniques. More precisely, (4) is a consequence of the following elementary result.

**Theorem A.1.** *Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$, and $K$ a finite étale subgroup of $E$ (i.e., the map $E \to E/K$ is separable) defined over $\mathbb{F}_q$. Suppose that $K$ contains subgroups $K_i$ defined over $\mathbb{F}_q$, for $1 \leq i \leq n$, whose orders are pairwise coprime, and suppose $K = K_1 + \cdots + K_n$. Then:*

$$(E/K_1) \times \cdots \times (E/K_n) \cong (E/K) \times E^{n-1}.$$

# We could've had it all (5 years ago) [ePrint 2018/665]

**Theorem A.1.** *Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$, and $K$ a finite étale subgroup of $E$ (i.e., the map $E \to E/K$ is separable) defined over $\mathbb{F}_q$. Suppose that $K$ contains subgroups $K_i$ defined over $\mathbb{F}_q$, for $1 \le i \le n$, whose orders are pairwise coprime, and suppose $K = K_1 + \cdots + K_n$. Then:*

$$(E/K_1) \times \cdots \times (E/K_n) \cong (E/K) \times E^{n-1}.$$

*Proof.* The result is immediate for $n = 1$. We next prove the result for $n = 2$ by constructing an explicit isomorphism. Consider the commutative diagram:

$$\begin{tikzcd} E \arrow[r, "\varphi_1"] \arrow[d, "\varphi_2"'] \arrow[dr, "\theta"] & E/K_1 \arrow[d, "\psi_1"] \\ E/K_2 \arrow[r, "\psi_2"'] & E/K \end{tikzcd}$$

where all maps are the natural quotient isogenies. If we denote by $m_1$ and $m_2$ the orders of $K_1$ and $K_2$, we have $\deg \varphi_1 = \deg \psi_2 = m_1$ and $\deg \varphi_2 = \deg \psi_1 = m_2$. Now choose integers $a, b \in \mathbb{Z}$ such that $am_1 + bm_2 = 1$. We define morphisms

$$f\colon E \times (E/K) \to (E/K_1) \times (E/K_2) \qquad \text{and} \qquad g\colon (E/K_1) \times (E/K_2) \to E \times (E/K)$$

by the following matrices:

$$\mathrm{Mat}(f) = \begin{pmatrix} \varphi_1 & \widehat{\psi_1} \\ -b\varphi_2 & a\widehat{\psi_2} \end{pmatrix} \qquad \text{and} \qquad \mathrm{Mat}(g) = \begin{pmatrix} a\widehat{\varphi_1} & -\widehat{\varphi_2} \\ b\psi_1 & \psi_2 \end{pmatrix}.$$

Questions?