Rational isogenies from irrational endomorphisms

Wouter Castryck[1] Lorenz Panny[2] Frederik Vercauteren[1]

[1]imec-COSIC, ESAT, KU Leuven [2]Academia Sinica, Taipei, Taiwan

SIAM-AG, online, 20 August 2021

The upshot

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$* : G \times X \longrightarrow X$$

on a certain set X of supersingular elliptic curves.
(cf. how integer exponents can be applied to Diffie–Hellman public keys)

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action
$$*\colon G \times X \longrightarrow X$$
on a certain set X of supersingular elliptic curves.
(cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

  on a certain set X of supersingular elliptic curves.
  (cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.
  (Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

  on a certain set X of supersingular elliptic curves.
  (cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.
  (Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

- Known methods to produce elements of X:

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

  on a certain set X of supersingular elliptic curves.
  (cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.
  (Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

- Known methods to produce elements of X:
  - Take known $x \in X$; pick random $g \in G$; compute $y := g * x$.
    $\rightsquigarrow$ obviously leaks a connection from x to y: it's g.

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

on a certain set X of supersingular elliptic curves.

(cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.

(Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

- Known methods to produce elements of X:
  - Take known $x \in X$; pick random $g \in G$; compute $y := g * x$.
  $\rightsquigarrow$ obviously leaks a connection from x to y: it's g.
  - Reduce a suitable CM curve $\mathcal{E}/\bar{\mathbb{Q}}$ modulo q.
  $\rightsquigarrow$ **???????**

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

  on a certain set X of supersingular elliptic curves.
  (cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.
  (Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

- Known methods to produce elements of X:
  - Take known $x \in X$; pick random $g \in G$; compute $y := g * x$.
    $\rightsquigarrow$ obviously leaks a connection from x to y: it's g.
  - Reduce a suitable CM curve $\mathcal{E}/\bar{\mathbb{Q}}$ modulo q.
    $\rightsquigarrow$ **Our work** can find a connection to a certain $x \in X$.

The upshot

- CSIDH [ˈsiːˌsaɪd] is a cryptographic (abelian) group action

$$*\colon G \times X \longrightarrow X$$

  on a certain set X of supersingular elliptic curves.
  (cf. how integer exponents can be applied to Diffie–Hellman public keys)

- Open problem: 'Hash into X': compute elements of X with no known connection (element of G) between them.
  (Situation with DLP: We can easily sample from $(\mathbb{Z}/p)^*$, $E(\mathbb{F}_q)$, ...)

- Known methods to produce elements of X:
  - Take known $x \in X$; pick random $g \in G$; compute $y := g * x$.
    $\rightsquigarrow$ obviously leaks a connection from x to y: it's g.
  - Reduce a suitable CM curve $\mathcal{E}/\bar{\mathbb{Q}}$ modulo q.
    $\rightsquigarrow$ **Our work** can find a connection to a certain $x \in X$.

See also very much related parallel work by Boneh and Love [arXiv:1910.03180].

Overview of CSIDH

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of elliptic curves $E/\mathbb{F}_p$ with $\text{End}_p(E) = \mathcal{O}$.
  ($\mathbb{F}_p$-isomorphism classes of)

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of $\underset{(\mathbb{F}_p\text{-isomorphism classes of})}{\curlywedge}$ elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) = \mathcal{O}$.
- This means: An invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on $E \in X$ by quotienting out the kernel subgroup $E[\mathfrak{a}]$.

  $\rightsquigarrow$ free and transitive action of $\mathrm{cl}(\mathcal{O})$ on X.

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of (${\mathbb{F}_p}$-isomorphism classes of) elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) = \mathcal{O}$.
- This means: An invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on $E \in X$ by quotienting out the kernel subgroup $E[\mathfrak{a}]$.
  $\rightsquigarrow$ free and transitive action of $\mathrm{cl}(\mathcal{O})$ on X.
- Computing the action of $\mathfrak{a} \subseteq \mathcal{O}$ is generally hard. ☹

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of ($\mathbb{F}_p$-isomorphism classes of) elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) = \mathcal{O}$.
- This means: An invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on $E \in X$ by quotienting out the kernel subgroup $E[\mathfrak{a}]$.
  $\rightsquigarrow$ free and transitive action of $\mathrm{cl}(\mathcal{O})$ on X.
- Computing the action of $\mathfrak{a} \subseteq \mathcal{O}$ is generally hard. :-(
  $\rightsquigarrow$ Use $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ with small $\mathrm{N}(\mathfrak{l}_i)$ and $|e_i|$ $\rightsquigarrow$ efficient!

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of ($\mathbb{F}_p$-isomorphism classes of) elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) = \mathcal{O}$.
- This means: An invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on $E \in X$ by quotienting out the kernel subgroup $E[\mathfrak{a}]$.
  $\rightsquigarrow$ free and transitive action of $\mathrm{cl}(\mathcal{O})$ on X.
- Computing the action of $\mathfrak{a} \subseteq \mathcal{O}$ is generally hard. :(
  $\rightsquigarrow$ Use $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ with small $\mathrm{N}(\mathfrak{l}_i)$ and $|e_i|$ $\rightsquigarrow$ efficient!
  (Advantage of CSIDH: applying $\mathfrak{l}_i$ is particularly cheap.)

Overview of CSIDH

- CSIDH is the CM action of an order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-p})$ on the set X of elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) = \mathcal{O}$.
  ($\mathbb{F}_p$-isomorphism classes of)

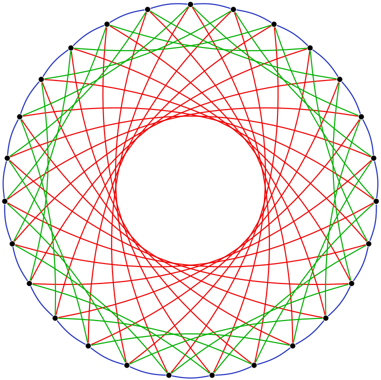
- This means: An invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on $E \in X$ by quotienting out the kernel subgroup $E[\mathfrak{a}]$.
  $\rightsquigarrow$ free and transitive action of $\mathrm{cl}(\mathcal{O})$ on X.

- Computing the action of $\mathfrak{a} \subseteq \mathcal{O}$ is generally hard. ☹
  $\rightsquigarrow$ Use $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ with small $\mathrm{N}(\mathfrak{l}_i)$ and $|e_i|$ $\rightsquigarrow$ efficient!
  (Advantage of CSIDH: applying $\mathfrak{l}_i$ is particularly cheap.)

$\Longrightarrow$ Bottom line: Relatively fast non-interactive key exchange.
Think Diffie–Hellman, but post-quantum! (and slower...)

Isogeny graphs

Visualizing the action of $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$:



Each node is an elliptic curve over $\mathbb{F}_p$, up to $\cong_{\mathbb{F}_p}$.

Each edge is the action of $\mathfrak{l}_1$, $\mathfrak{l}_2$, or $\mathfrak{l}_3$, or their inverses.

Notation for this talk

- The prime p is 'large', certainly > 3.
- Curves are elliptic, supersingular, and defined over $\mathbb{F}_{p^2}$.
- E^t: the *quadratic twist* of E.
- $\mathrm{End}(E)$: *full* endomorphism ring (over $\bar{\mathbb{F}}_p$).
- $\mathrm{End}_p(E)$: *rational* endomorphism ring (over $\mathbb{F}_p$).
- E_0: a starting curve with known endomorphism ring.
  For instance: $p \equiv 3 \bmod 4$ and $E_0 : y^2 = x^3 + x$.
  Endomorphism ring: $\mathrm{End}(E_0) = \left\langle 1, \iota, \frac{\iota+\pi}{2}, \frac{1+\iota\pi}{2} \right\rangle$
  where $\iota : (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ and $\pi : (x, y) \mapsto (x^p, y^p)$.
- $\mathcal{O}$: the order $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[(1+\sqrt{-p})/2]$ in $\mathbb{Q}(\sqrt{-p})$.
- $\mathfrak{l}$: a fixed prime ideal of $\mathcal{O}$ lying above ℓ.

A starting point...

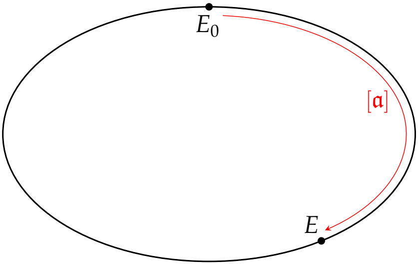
Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$, say of prime degree ℓ.

Q: Where in the isogeny graph is it?

A starting point...

Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$, say of prime degree ℓ.

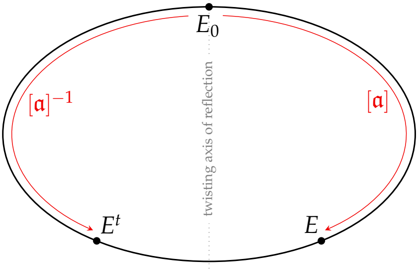
Q: Where in the isogeny graph is it?



A starting point...

Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$, say of prime degree ℓ.

Q: Where in the isogeny graph is it?

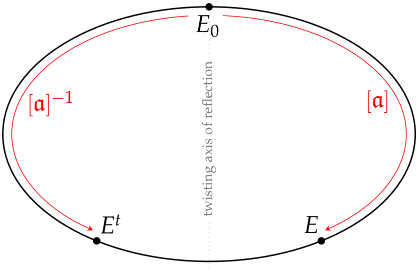


Fact: *If* $p \equiv 3 \bmod 4$ and $E_0 : y^2 = x^3 + x$, then "given $[\mathfrak{a}]E_0$ we can compute $[\mathfrak{a}]^{-1}E_0$ by mere quadratic twisting". [CSIDH paper]

A starting point...

Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$, say of prime degree ℓ.

Q: Where in the isogeny graph is it?



Fact: *If* $p \equiv 3 \bmod 4$ and $E_0 : y^2 = x^3 + x$, then "given $[\mathfrak{a}]E_0$ we can compute $[\mathfrak{a}]^{-1}E_0$ by mere quadratic twisting". [CSIDH paper]

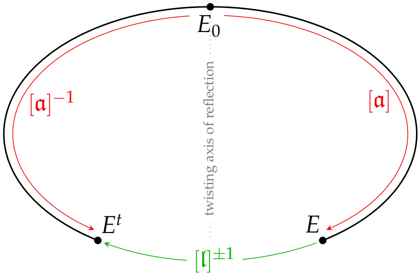
Fact: *If* $\tau\pi = -\pi\tau$, then $(E \xrightarrow{\sim} E^t) \circ \tau$ is an $\mathbb{F}_p$-rational isogeny.

Therefore τ implies an edge $E \to E^t$ in the ℓ-isogeny graph.

A starting point...

Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \setminus \mathrm{End}_p(E)$, say of prime degree ℓ.

Q: Where in the isogeny graph is it?



Fact: *If* $p \equiv 3 \bmod 4$ and $E_0 : y^2 = x^3 + x$, then "given $[\mathfrak{a}]E_0$ we can compute $[\mathfrak{a}]^{-1}E_0$ by mere quadratic twisting". [CSIDH paper]

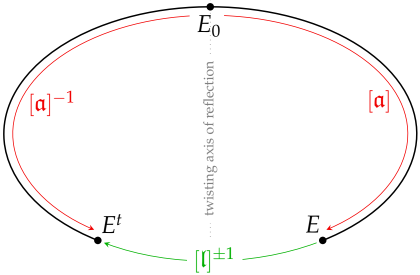
Fact: *If* $\tau\pi = -\pi\tau$, then $(E \xrightarrow{\sim} E^t) \circ \tau$ is an $\mathbb{F}_p$-rational isogeny.

Therefore τ implies an edge $E \to E^t$ in the ℓ-isogeny graph.

A starting point...

Suppose a curve $E = [\mathfrak{a}]E_0$ has an irrational endomorphism $\tau \in \mathrm{End}(E) \setminus \mathrm{End}_p(E)$, say of prime degree ℓ.

Q: Where in the isogeny graph is it?



$\implies [\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$!

Fact: *If* $p \equiv 3 \bmod 4$ and $E_0 : y^2 = x^3 + x$, then "given $[\mathfrak{a}]E_0$ we can compute $[\mathfrak{a}]^{-1}E_0$ by mere quadratic twisting". [CSIDH paper]

Fact: *If* $\tau\pi = -\pi\tau$, then $(E \xrightarrow{\sim} E^t) \circ \tau$ is an $\mathbb{F}_p$-rational isogeny.

Therefore τ implies an edge $E \to E^t$ in the ℓ-isogeny graph.

Coincidence?

Previous slide:

Knowing that $E = [\mathfrak{a}]E_0$ has a 'special' endomorphism τ allows us to recover $[\mathfrak{a}]$ up to 2-torsion.

Q: Is this just a weird special case?

Coincidence?

Previous slide:

Knowing that $E = [\mathfrak{a}]E_0$ has a 'special' endomorphism τ allows us to recover $[\mathfrak{a}]$ up to 2-torsion.

Q: Is this just a weird special case? (**A**: No.)

Coincidence?

<u>Previous slide</u>:

Knowing that $E = [\mathfrak{a}]E_0$ has a 'special' endomorphism τ allows us to recover $[\mathfrak{a}]$ up to 2-torsion.

Q: Is this just a weird special case? (**A**: No.)

Definition. Let E be defined over $\mathbb{F}_p$.
Then $\alpha \in \mathrm{End}(E)$ is a *twisting endomorphism* of E if $\alpha\pi = -\pi\alpha$.

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0\colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0 \colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \setminus \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$?

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0 \colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \setminus \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$?
- How much ambiguity is in the 2-torsion?

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0 \colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$?
- How much ambiguity is in the 2-torsion?
- When are endomorphisms *twisting*?

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0\colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \setminus \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$?
- How much ambiguity is in the 2-torsion?
- When are endomorphisms *twisting*?
- Can we deal with starting curves $E_0 \neq E_0^t$?

To-do list

Let $E = [\mathfrak{a}]E_0$. We've seen:

If $p \equiv 3 \bmod 4$ **and** $E_0 \colon y^2 = x^3 + x$ **and** $\tau \in \mathrm{End}(E) \backslash \mathrm{End}_p(E)$ with $\deg \tau = \ell$ prime **and** $\tau\pi = -\pi\tau$, **then** $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$.

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$?
- How much ambiguity is in the 2-torsion?
- When are endomorphisms *twisting*?
- Can we deal with starting curves $E_0 \neq E_0^t$?
- Can we generalize to primes $p \not\equiv 3 \bmod 4$?

Square roots in $\mathrm{cl}(\mathcal{O})$

From ℓ we learn that $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$. But how to recover (an) $[\mathfrak{a}]$?

Square roots in $\mathrm{cl}(\mathcal{O})$

From ℓ we learn that $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$. But how to recover (an) $[\mathfrak{a}]$?

Perhaps unsurprisingly, Gauß knew how to do this. [DA § 286]

His method is polynomial-time.

Square roots in $\mathrm{cl}(\mathcal{O})$

From ℓ we learn that $[\mathfrak{a}]^2 = [\mathfrak{l}]^{\pm 1}$. But how to recover (an) $[\mathfrak{a}]$?

Perhaps unsurprisingly, Gauß knew how to do this. [DA § 286]

His method is polynomial-time.

Note: *If* the class number $h(\mathcal{O}) = |\mathrm{cl}(\mathcal{O})|$ is known and odd, then

$$\sqrt{[\mathfrak{s}]} = [\mathfrak{s}]^{(h(\mathcal{O})+1)/2}.$$

Gauß' algorithm does not require computing $h(\mathcal{O})$.

Square roots in $\mathrm{cl}(\mathcal{O})$

How many square roots exist?

Square roots in $\mathrm{cl}(\mathcal{O})$

How many square roots exist?

Fact: If $\mathfrak{r} \subseteq \mathcal{O}$ is a non-principal prime ideal such that $\mathfrak{r}^2$ is principal, then $\mathrm{N}(\mathfrak{r})$ divides $\Delta := \mathrm{disc}(\mathbb{Q}(\sqrt{-p})) \in \{-p, -4p\}$.

Square roots in $\mathrm{cl}(\mathcal{O})$

How many square roots exist?

Fact: If $\mathfrak{r} \subseteq \mathcal{O}$ is a non-principal prime ideal such that $\mathfrak{r}^2$ is principal, then $\mathrm{N}(\mathfrak{r})$ divides $\Delta := \mathrm{disc}(\mathbb{Q}(\sqrt{-p})) \in \{-p, -4p\}$.

For the potential divisors of Δ, we get:

- $p \mid \Delta$: yields $(\pi) \subseteq \mathcal{O}$ (principal).
- $2 \mid \Delta$: yields $(2, \pi+1) \subseteq \mathcal{O}$ (non-principal).

Square roots in $\mathrm{cl}(\mathcal{O})$

How many square roots exist?

Fact: If $\mathfrak{r} \subseteq \mathcal{O}$ is a non-principal prime ideal such that $\mathfrak{r}^2$ is principal, then $\mathrm{N}(\mathfrak{r})$ divides $\Delta := \mathrm{disc}(\mathbb{Q}(\sqrt{-p})) \in \{-p, -4p\}$.

For the potential divisors of Δ, we get:

- $p \mid \Delta$: yields $(\pi) \subseteq \mathcal{O}$ (principal).
- $2 \mid \Delta$: yields $(2, \pi+1) \subseteq \mathcal{O}$ (non-principal).

$$\implies \mathrm{cl}(\mathcal{O})[2] \cong \begin{cases} \{\mathrm{id}\} & \text{when } p \equiv 3 \pmod 4; \\ \mathbb{Z}/2 & \text{when } p \equiv 1 \pmod 4. \end{cases}$$

Bottom line: Elements $[\mathfrak{s}] \in \mathrm{cl}(\mathcal{O})^2$ have either one or two square roots, depending on $p \bmod 4$.

To-do list

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$? ✓
  Gauß found a polynomial-time algorithm.
- How much ambiguity is in the 2-torsion? ✓
  At most two square roots; $\mathrm{cl}(\mathcal{O})[2] \leq \mathbb{Z}/2$.
- When are endomorphisms *twisting*?
- Can we deal with starting curves $E_0 \neq E_0^t$?
- Can we generalize to primes $p \not\equiv 3 \bmod 4$?

Twisting endomorphisms

We wanted to locate reduced CM curves in the isogeny graph.

Q: How common is it for an endomorphism to be twisting?

Twisting endomorphisms

We wanted to locate reduced CM curves in the isogeny graph.

Q: How common is it for an endomorphism to be twisting?

Suppose $E/\mathbb{F}_p$ is the supersingular reduction of a curve $\mathcal{E}/\bar{\mathbb{Q}}$ with CM by $\mathbb{Z}[\Psi]$ where Ψ has prime degree $\ell \leq (p+1)/4$.

Then the reduction ψ of Ψ is a twisting endomorphism.

Twisting endomorphisms

We wanted to locate reduced CM curves in the isogeny graph.

Q: How common is it for an endomorphism to be twisting?

Suppose $E/\mathbb{F}_p$ is the supersingular reduction of a curve $\mathcal{E}/\bar{\mathbb{Q}}$ with CM by $\mathbb{Z}[\Psi]$ where Ψ has prime degree $\ell \leq (p+1)/4$.

Then the reduction ψ of Ψ is a twisting endomorphism.

$\Longrightarrow$ For large p, reduced CM endomorphisms are practically always twisting.

Twisting endomorphisms

We wanted to locate reduced CM curves in the isogeny graph.

Q: How common is it for an endomorphism to be twisting?

Suppose $E/\mathbb{F}_p$ is the supersingular reduction of a curve $\mathcal{E}/\bar{\mathbb{Q}}$ with CM by $\mathbb{Z}[\Psi]$ where Ψ has prime degree $\ell \leq (p+1)/4$.

Then the reduction ψ of Ψ is a twisting endomorphism.

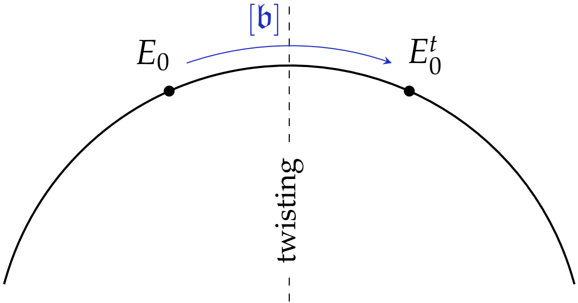
$\Longrightarrow$ For large p, reduced CM endomorphisms are practically always twisting.

Moreover, given any irrational endomorphism, it is typically easy to find a twisting endomorphism.

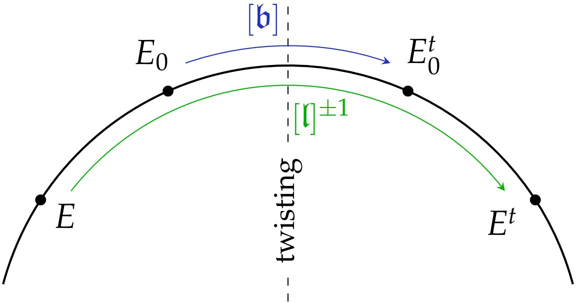
To-do list

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$? ✓
  Gauß found a polynomial-time algorithm.
- How much ambiguity is in the 2-torsion? ✓
  At most two square roots; $\mathrm{cl}(\mathcal{O})[2] \leq \mathbb{Z}/2$.
- When are endomorphisms *twisting*? ✓
  Sufficient: reduced CM endomorphisms with $\deg \leq (p+1)/4$.
- Can we deal with starting curves $E_0 \neq E_0^t$?
- Can we generalize to primes $p \not\equiv 3 \bmod 4$?

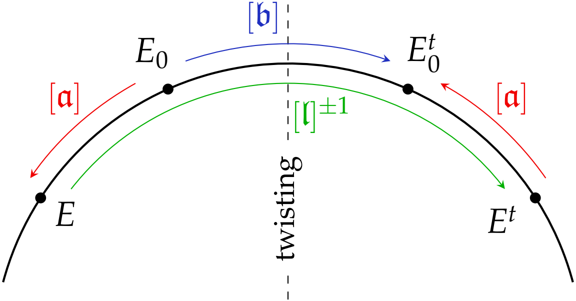
Starting curves which are not their own twist



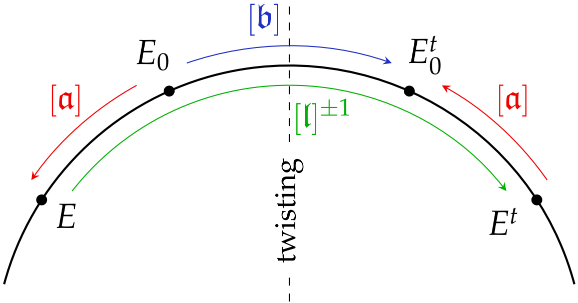
Starting curves which are not their own twist



Starting curves which are not their own twist



Starting curves which are not their own twist

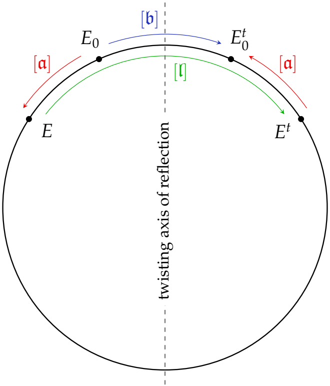


$$[\mathfrak{l}]^{\pm 1} = [\mathfrak{b}][\mathfrak{a}]^{-2} \implies [\mathfrak{a}]^2 = [\mathfrak{b}][\mathfrak{l}]^{\mp 1}$$

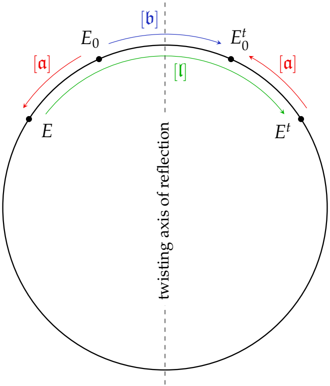
To-do list

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$? ✓
  Gauß found a polynomial-time algorithm.
- How much ambiguity is in the 2-torsion? ✓
  At most two square roots; $\mathrm{cl}(\mathcal{O})[2] \leq \mathbb{Z}/2$.
- When are endomorphisms *twisting*? ✓
  Sufficient: reduced CM endomorphisms with $\deg \leq (p+1)/4$.
- Can we deal with starting curves $E_0 \neq E_0^t$? ✓
  Yes; the same idea works modulo technicalities.
- Can we generalize to primes $p \not\equiv 3 \bmod 4$?

The case $p \equiv 1 \bmod 4$

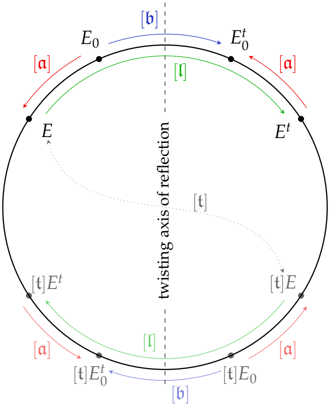


The case $p \equiv 1 \bmod 4$



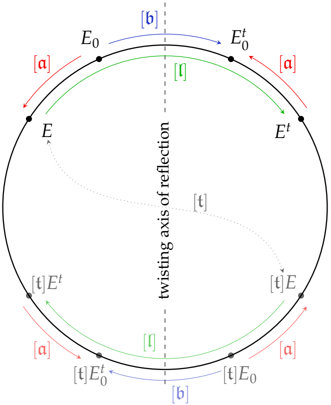
<u>Long story short</u>: Everything works the same, but the element $\mathfrak{t} := [(2, \pi+1)]$ of order 2 introduces an additional symmetry.

The case $p \equiv 1 \bmod 4$



Long story short: Everything works the same, but the element $\mathfrak{t} := [(2, \pi + 1)]$ of order 2 introduces an additional symmetry.

The case $p \equiv 1 \bmod 4$



Long story short: Everything works the same, but the element $\mathfrak{t} := [(2, \pi+1)]$ of order 2 introduces an additional symmetry.

$\rightsquigarrow$ Two candidates for $[\mathfrak{a}]$. Find $[\mathfrak{a}]$ by brute-force testing or use ePrint 2020/151, which breaks DDH for the case $p \equiv 1 \bmod 4$.

To-do list

- How to compute square roots in $\mathrm{cl}(\mathcal{O})$? ✓
  Gauß found a polynomial-time algorithm.
- How much ambiguity is in the 2-torsion? ✓
  At most two square roots; $\mathrm{cl}(\mathcal{O})[2] \leq \mathbb{Z}/2$.
- When are endomorphisms *twisting*? ✓
  Sufficient: reduced CM endomorphisms with $\deg \leq (p+1)/4$.
- Can we deal with starting curves $E_0 \neq E_0^t$? ✓
  Yes; the same idea works modulo technicalities.
- Can we generalize to primes $p \not\equiv 3 \bmod 4$? ✓
  Yes.

Our ‘locating CM curves’ theorem

Let $p \equiv 3 \bmod 4$ and $\ell < (p+1)/4$ be primes with $\left(\frac{-p}{\ell}\right) = 1$.

We show:

- How many curves $/\mathbb{F}_p$ are reductions of curves $/\bar{\mathbb{Q}}$ with CM by orders $\mathcal{R} \subseteq \mathbb{Q}(\sqrt{-\ell})$ containing $\mathbb{Z}[\sqrt{-\ell}]$.
- Which combinations of $(\mathrm{End}_p, \mathcal{R})$ are possible.
- Where in the isogeny graph all these curves are located: We give connecting ideals to the curve $E_0 \colon y^2 = x^3 \pm x$.

Our ‘locating CM curves’ theorem

Let $p \equiv 3 \bmod 4$ and $\ell < (p+1)/4$ be primes with $\left(\frac{-p}{\ell}\right) = 1$.

We show:

- How many curves $/\mathbb{F}_p$ are reductions of curves $/\bar{\mathbb{Q}}$ with CM by orders $\mathcal{R} \subseteq \mathbb{Q}(\sqrt{-\ell})$ containing $\mathbb{Z}[\sqrt{-\ell}]$.
- Which combinations of $(\mathrm{End}_p, \mathcal{R})$ are possible.
- Where in the isogeny graph all these curves are located: We give connecting ideals to the curve $E_0 \colon y^2 = x^3 \pm x$.

Remark: Similar results are possible for $p \equiv 1 \bmod 4$.

An example

In the CSIDH-512 parameter set, $p \equiv 11 \bmod 12$.
Q: Where is $E\colon y^2 = x^3 + 1$?

An example

In the CSIDH-512 parameter set, $p \equiv 11 \bmod 12$.
Q: Where is $E\colon y^2 = x^3 + 1$?

Our very explicit **a**nswer:

$$E = \left[(3, \pi - 1)^{127326221114742137588515093005319601080810257152743211796285430487798805863095}\right] E_0$$

An example

In the CSIDH-512 parameter set, $p \equiv 11 \bmod 12$.
Q: Where is $E\colon y^2 = x^3 + 1$?

Our very explicit **a**nswer:

$$E = \left[(3, \pi - 1)^{1273262221114742137588515093005319601080810257152743211796285430487798805863095}\right] E_0$$

This ideal class corresponds to (e.g.) the private key:

$$\begin{array}{l}(5, -7, -1, 1, -4, -5, -8, 4, -1, 5, 1, 0, -2, -4, -2, 2, -9, 4, 2, \\ 5, 1, 1, 1, 5, -4, 2, 6, 5, -1, 0, 0, -4, -1, -3, -1, -4, 1, 7, \\ 1, 4, 1, 4, -7, 0, -3, -1, 0, 1, 2, 3, 1, 2, -4, -5, 9, -1, 4, \\ 0, 5, 1, 0, 1, 1, 3, 0, 2, 2, 2, -1, 2, 1, -1, 11, 3).\end{array}$$

[relies on data from ePrint 2019/498]

One last thing: $\mathbb{F}_p$-ifying the KLPT algorithm

Let E be a supersingular elliptic curve.

- Known [KLPT'14]: When $E/\mathbb{F}_{p^2}$ and given $\mathrm{End}(E)$, one can compute an isogeny $E_0 \longrightarrow E$ in polynomial time.

One last thing: $\mathbb{F}_p$-ifying the KLPT algorithm

Let E be a supersingular elliptic curve.

- Known [KLPT'14]: When $E/\mathbb{F}_{p^2}$ and given $\mathrm{End}(E)$, one can compute an isogeny $E_0 \longrightarrow E$ in polynomial time.

  This isogeny is usually not defined over $\mathbb{F}_p$!
  $\rightsquigarrow$ **Q**: Can we safely reveal endomorphisms in CSIDH?

One last thing: $\mathbb{F}_p$-ifying the KLPT algorithm

Let E be a supersingular elliptic curve.

- Known [KLPT'14]: When $E/\mathbb{F}_{p^2}$ and given $\mathrm{End}(E)$, one can compute an isogeny $E_0 \longrightarrow E$ in polynomial time.

  This isogeny is usually not defined over $\mathbb{F}_p$!
  $\rightsquigarrow$ **Q**: Can we safely reveal endomorphisms in CSIDH?

- We show: When $E/\mathbb{F}_{\boldsymbol{p}}$ and given $\mathrm{End}(E)$, one can compute an ideal $\mathfrak{a} \subseteq \mathrm{End}_p(E_0)$ with $E_0/\mathfrak{a} \cong E$ in polynomial time.

One last thing: $\mathbb{F}_p$-ifying the KLPT algorithm

Let E be a supersingular elliptic curve.

- Known [KLPT'14]: When $E/\mathbb{F}_{p^2}$ and given $\mathrm{End}(E)$, one can compute an isogeny $E_0 \longrightarrow E$ in polynomial time.

  This isogeny is usually not defined over $\mathbb{F}_p$!
  $\rightsquigarrow$ **Q**: Can we safely reveal endomorphisms in CSIDH?

- We show: When $E/\mathbb{F}_p$ and given $\mathrm{End}(E)$, one can compute an ideal $\mathfrak{a} \subseteq \mathrm{End}_p(E_0)$ with $E_0/\mathfrak{a} \cong E$ in polynomial time.
  - Caveat: Turning $\mathfrak{a}$ into an isogeny $E_0 \longrightarrow E$ takes superpolynomial time $L_p[1/2, \sqrt{2}]$.

One last thing: $\mathbb{F}_p$-ifying the KLPT algorithm

Let E be a supersingular elliptic curve.

- Known [KLPT'14]: When $E/\mathbb{F}_{p^2}$ and given $\mathrm{End}(E)$, one can compute an isogeny $E_0 \longrightarrow E$ in polynomial time.

  This isogeny is usually not defined over $\mathbb{F}_p$!
  $\rightsquigarrow$ **Q**: Can we safely reveal endomorphisms in CSIDH?

- We show: When $E/\mathbb{F}_p$ and given $\mathrm{End}(E)$, one can compute an ideal $\mathfrak{a} \subseteq \mathrm{End}_p(E_0)$ with $E_0/\mathfrak{a} \cong E$ in polynomial time.
  - Caveat: Turning $\mathfrak{a}$ into an isogeny $E_0 \longrightarrow E$ takes superpolynomial time $L_p[1/2, \sqrt{2}]$.
  - But this might be optimal: we show that doing better implies faster discrete logarithms in $\mathrm{cl}(\mathbb{Q}(\sqrt{-p}))$.

Thanks!

Further reading for any newcomers who may have now acquired an interest in the actual isogeny session (later today):

- `https://arxiv.org/abs/1711.04062`
- `https://yx7.cc/docs/phd/thesis.pdf` (§2)