Introduction on Isogenies between Elliptic Curves

Hiroshi Onuki

The University of Tokyo

2024/10/28

Text books

The mathematical details of this presentation can be found in

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*

[Was08] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*

Notation

- p is a **prime number** not equal to 2 or 3.
- q is a **power** of p.
- We only consider elliptic curves defined by

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \overline{\mathbb{F}}_p.$$

  If not specified, an elliptic curve is defined over $\mathbb{F}_q$.
- Elliptic curves are denoted by $E, E', E_1, E_2, \dots$
- The **neutral element** of an elliptic curve E is denoted by 0_E.
- For $P \in E$, the x-coordinate of P is denoted by $x(P)$ (similarly for $y(P)$).
- The **multiplication-by-n map** is denoted by $[n]$.

Isogeny (Definition)

Definition 1

Let E_1 and E_2 be elliptic curves.
An *isogeny* is a non-constant rational map

$$\varphi : E_1 \to E_2$$

such that $\varphi(0_{E_1}) = 0_{E_2}$.

Theorem 2 (Theorem III.4.8 in [Sil09])

Let $\varphi : E_1 \to E_2$ be an isogeny. Then φ is a **group homomorphism**, *i.e.,*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

for all $P, Q \in E_1$.

Isogeny (Explicit form)

Since we consider elliptic curves defined by $y^2 = x^3 + ax^2 + bx + c$, we can write an **isogeny** φ in the form

$$\varphi(x, y) = \left(\frac{g_1(x)}{h_1(x)},\ y\frac{g_2(x)}{h_2(x)} \right),$$

where

- g_1, h_1, g_2, h_2 are polynomials over $\overline{\mathbb{F}}_p$,
- g_1 (resp. g_2) and h_1 (resp. h_2) have no common factors,
- h_1 and h_2 have the same roots.

Isogeny (Explicit form)

Since we consider elliptic curves defined by $y^2 = x^3 + ax^2 + bx + c$, we can write an **isogeny** φ in the form

$$\varphi(x, y) = \left(\frac{g_1(x)}{h_1(x)},\ y\frac{g_2(x)}{h_2(x)} \right),$$

where

- g_1, h_1, g_2, h_2 are polynomials over $\overline{\mathbb{F}}_p$,
- g_1 (resp. g_2) and h_1 (resp. h_2) have no common factors,
- h_1 and h_2 have the same roots.

For $P \in E_1$,

$$\varphi(P) = 0_{E_2} \iff P = 0_{E_1} \text{ or } h_1(x(P)) = 0.$$

If g_1, h_1, g_2, h_2 are polynomials over $\mathbb{F}_{q^k}$, then we say φ is *defined over* $\mathbb{F}_{q^k}$.

Example (Scalar multiplication)

Let m be a nonzero integer. Then the **multiplication-by-m map**

$$[m] : E \to E$$

is an isogeny.

Example

Consider two elliptic curves E_1 and E_2:

$$\begin{aligned} E_1 : & y^2 = x^3 + ax^2 + bx, \\ E_2 : & y^2 = x^3 - 2ax^2 + (a^2 - 4b)x, \end{aligned}$$

where $a, b \in \mathbb{F}_q$ and $b(a^2 - 4b) \neq 0$.

The map $\varphi : E_1 \to E_2$ defined by

$$\varphi(x, y) = \left(\frac{x^2 + ax + b}{x},\ y\frac{b - x^2}{x^2} \right)$$

is an isogeny defined over $\mathbb{F}_q$.

Example (Frobenius map)

Let E be an elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c$.

For an integer $k \geq 0$, we define an elliptic curve $E^{(p^k)}$ by

$$E^{(p^k)} : y^2 = x^3 + a^{p^k} x^2 + b^{p^k} x + c^{p^k}.$$

Example (Frobenius map)

Let E be an elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c$.

For an integer $k \geq 0$, we define an elliptic curve $E^{(p^k)}$ by

$$E^{(p^k)} : y^2 = x^3 + a^{p^k} x^2 + b^{p^k} x + c^{p^k}.$$

Then the *p^k-th power Frobenius map* $\pi_{p^k} : E \to E^{(p^k)}$ defined by

$$\pi_{p^k}(x, y) = (x^{p^k}, y^{p^k})$$

is an isogeny.

Example (Frobenius map)

Let E be an elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c$.

For an integer $k \geq 0$, we define an elliptic curve $E^{(p^k)}$ by

$$E^{(p^k)} : y^2 = x^3 + a^{p^k} x^2 + b^{p^k} x + c^{p^k}.$$

Then the *p^k-th power Frobenius map* $\pi_{p^k} : E \to E^{(p^k)}$ defined by

$$\pi_{p^k}(x, y) = (x^{p^k}, y^{p^k})$$

is an isogeny.

Note:

$$y^{p^k} = y(x^3 + ax^2 + bx + c)^{(p^k - 1)/2}.$$

Isogeny theorem

Theorem 3 (Exercise 5.4 in [Sil09])

Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.
Then the following are equivalent:

- *There exists an isogeny $\varphi : E_1 \to E_2$ defined over $\mathbb{F}_{q^k}$.*
- $\#E_1(\mathbb{F}_{q^k}) = \#E_2(\mathbb{F}_{q^k})$.

Isogeny theorem

Theorem 3 (Exercise 5.4 in [Sil09])

Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.
Then the following are equivalent:

- *There exists an isogeny $\varphi : E_1 \to E_2$ defined over $\mathbb{F}_{q^k}$.*
- $\#E_1(\mathbb{F}_{q^k}) = \#E_2(\mathbb{F}_{q^k})$.

Remark

The latter statement does NOT mean $E_1(\mathbb{F}_{q^k}) \cong E_2(\mathbb{F}_{q^k})$ **as groups**.

E.g., There is an isogeny defined over $\mathbb{F}_7$ between

$$E_1 : y^2 = x^3 - x \quad \text{and} \quad E_2 : y^2 = x^3 + 4x.$$

Easy calculation shows that

$$E_1(\mathbb{F}_7) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{and} \quad E_2(\mathbb{F}_7) \cong \mathbb{Z}/8\mathbb{Z}.$$

Degree of isogeny

Definition 4

Let $\varphi : E_1 \to E_2$ be an isogeny given by

$$\varphi(x,y) = \left(\frac{g_1(x)}{h_1(x)},\ y\frac{g_2(x)}{h_2(x)} \right).$$

The *degree* of φ is $\max\{\deg g_1, \deg h_1\}$ and is denoted by $\deg \varphi$.

Proposition 5

Let $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ be isogenies. Then

$$\deg(\psi \circ \varphi) = \deg \psi \cdot \deg \varphi.$$

Degree of isogeny (Examples)

- $\deg \pi_{p^k} = p^k$.
- The isogeny defined by

$$\varphi(x, y) = \left(\frac{x^2 + ax + b}{x},\ y \frac{b - x^2}{x^2} \right)$$

is of degree 2.

Endomorphism

Definition 6

Let E be an elliptic curve. An *endomorphism* of E is

- an isogeny $\varphi : E \to E$
- or the zero map ($P \mapsto 0_E$ for all $P \in E$).

- $[n]$ is an endomorphism for all $n \in \mathbb{Z}$.
- $\pi_q : (x, y) \mapsto (x^q, y^q)$ is an endomorphism.
  ($\because$ E is defined over $\mathbb{F}_q \Rightarrow E = E^{(q)}$)

Endomorphism ring

Definition 7

The set of all **endomorphisms** of an elliptic curve E forms a **ring** under the point-wise addition and composition.

I.e., for endomorphisms α, β of E,

- $(\alpha + \beta)(P) := \alpha(P) + \beta(P)$ for all $P \in E$,
- $\alpha \cdot \beta := \alpha \circ \beta$.

We call this ring the *endomorphism ring* of E and denote it by $\mathrm{End}(E)$.

Endomorphism ring

Definition 7

The set of all **endomorphisms** of an elliptic curve E forms a **ring** under the point-wise addition and composition.

I.e., for endomorphisms α, β of E,

- $(\alpha + \beta)(P) := \alpha(P) + \beta(P)$ for all $P \in E$,
- $\alpha \cdot \beta := \alpha \circ \beta$.

We call this ring the *endomorphism ring* of E and denote it by $\mathrm{End}(E)$.

Theorem 8 (Theorem III.9.3 and Theorem V.3.1 in [Sil09])

- E *is* **ordinary**

  $\Leftrightarrow \mathrm{End}(E) \cong$ *an order in an* **imaginary quadratic field***.*

- E *is* **supersingular**

  $\Leftrightarrow \mathrm{End}(E) \cong$ *a* **maximal** *order in a* **quaternion algebra***.*

Isomorphism

Definition 9

An *isomorphism* is an isogeny of degree 1.

Two elliptic curves E_1 and E_2 are *isomorphic*
if there is an isomorphism $\varphi : E_1 \to E_2$. We denote this by $E_1 \cong E_2$.

If φ is defined over $\mathbb{F}_{q^k}$, then we say E_1 and E_2 are *isomorphic over* $\mathbb{F}_{q^k}$.
We denote this by $E_1 \cong_{\mathbb{F}_{q^k}} E_2$.

Isomorphism

Definition 9

An *isomorphism* is an isogeny of degree 1.

Two elliptic curves E_1 and E_2 are *isomorphic*
if there is an isomorphism $\varphi : E_1 \to E_2$. We denote this by $E_1 \cong E_2$.

If φ is defined over $\mathbb{F}_{q^k}$, then we say E_1 and E_2 are *isomorphic over $\mathbb{F}_{q^k}$*.
We denote this by $E_1 \cong_{\mathbb{F}_{q^k}} E_2$.

Remark

If φ is an isomorphism, then φ is bijective.
However, the converse is NOT true in general.

E.g., the p-th power Frobenius map π_p is bijective but not an isomorphism.

Automorphism

Definition 10

An *automorphism* is an isomorphism from an elliptic curve to itself.

Definition 11

The set of all **automorphisms** of an elliptic curve E forms a **group** under the composition.

We call this group the *automorphism group* of E and denote it by $\mathrm{Aut}(E)$.

Note: $\mathrm{Aut}(E)$ is the unit group of $\mathrm{End}(E)$.

Automorphism group

Proposition 12 (Theorem III.10.1 and Corollary III.10.2 in [Sil09])

Let E be an elliptic curve.

1. $\mathrm{Aut}(E) = \{[\pm 1]\}$ *if* $j(E) \neq 0, 1728$.
2. $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$ *if* $j(E) = 1728$.
3. $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$ *if* $j(E) = 0$.

Automorphism group

Proposition 12 (Theorem III.10.1 and Corollary III.10.2 in [Sil09])

Let E be an elliptic curve.

1. $\mathrm{Aut}(E) = \{[\pm 1]\}$ *if* $j(E) \neq 0, 1728$.
2. $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$ *if* $j(E) = 1728$.
3. $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$ *if* $j(E) = 0$.

- For $E : y^2 = x^3 + x$ with $j(E) = 1728$,
$$(x, y) \mapsto (-x, \sqrt{-1}y)$$
generates $\mathrm{Aut}(E)$.

- For $E : y^2 = x^3 + 1$ with $j(E) = 0$,
$$(x, y) \mapsto (\zeta_3 x, -y)$$
generates $\mathrm{Aut}(E)$. (ζ_3 is a primitive 3rd root of unity in $\overline{\mathbb{F}}_p$.)

Separable isogeny (Definition)

Definition 13

Let $\varphi : E_1 \to E_2$ be an isogeny given by

$$\varphi(x,y) = \left(\frac{g_1(x)}{h_1(x)},\ y\frac{g_2(x)}{h_2(x)} \right).$$

We say φ is *separable* if $\frac{d}{dx}\frac{g_1(x)}{h_1(x)} \neq 0$ as a rational function, otherwise φ is *inseparable*.

Separable isogeny (Definition)

Definition 13

Let $\varphi : E_1 \to E_2$ be an isogeny given by

$$\varphi(x, y) = \left(\frac{g_1(x)}{h_1(x)},\ y\frac{g_2(x)}{h_2(x)} \right).$$

We say φ is *separable* if $\frac{d}{dx}\frac{g_1(x)}{h_1(x)} \neq 0$ as a rational function, otherwise φ is *inseparable*.

- The p^k-th power Frobenius map π_{p^k} is **inseparable**.
- The isogeny defined by

$$\varphi(x, y) = \left(\frac{x^2 + ax + b}{x},\ y\frac{b - x^2}{x^2} \right)$$

is **separable**.

Separable isogeny (Properties)

Proposition 14 (Corollary II.2.12 in [Sil09])

An isogeny $\varphi : E_1 \to E_2$ decomposes into a composition

$$E_1 \xrightarrow{\pi_{p^k}} E_1^{(p^k)} \xrightarrow{\psi} E_2,$$

where ψ is **separable**.

Separable isogeny (Properties)

Proposition 14 (Corollary II.2.12 in [Sil09])

An isogeny $\varphi : E_1 \to E_2$ decomposes into a composition

$$E_1 \xrightarrow{\pi_{p^k}} E_1^{(p^k)} \xrightarrow{\psi} E_2,$$

where ψ is **separable**.

Corollary 15

- *φ is* **inseparable** $\Leftrightarrow \dfrac{g_1(x)}{h_1(x)} = \dfrac{r(x^p)}{s(x^p)}$ *for some polynomials r, s.*
- *φ is* **inseparable** $\Rightarrow \deg \varphi \equiv 0 \pmod{p}$.

Kernel of isogeny (Definition)

Definition 16

Let $\varphi : E_1 \to E_2$ be an isogeny. The *kernel* of φ is

$$\ker \varphi = \{P \in E_1 \mid \varphi(P) = 0_{E_2}\}.$$

- $\ker[n] = E_1[n]$.
- $\ker \pi_{p^k} = \{0_{E_1}\}$.
- The kernel of the isogeny defined by

$$\varphi(x, y) = \left(\frac{x^2 + ax + b}{x},\ y\frac{b - x^2}{x^2}\right)$$

is $\{0_{E_1}, (0, 0)\}$.

Kernel of isogeny (Properties)

Proposition 17 (Theorem III.4.10 in [Sil09])

Let φ be an isogeny. Then

$$\#\ker\varphi \leq \deg\varphi.$$

If φ is **separable** *then $\#\ker\varphi = \deg\varphi$.*

Kernel of isogeny (Properties)

Proposition 17 (Theorem III.4.10 in [Sil09])

Let φ be an isogeny. Then

$$\# \ker \varphi \leq \deg \varphi.$$

If φ is **separable** *then $\# \ker \varphi = \deg \varphi$.*

Let φ be the isogeny defined by

$$\varphi(x, y) = \left(\frac{x^2 + ax + b}{x}, \ y \frac{b - x^2}{x^2} \right).$$

φ is separable, $\deg \varphi = 2$, and $\# \ker \varphi = \# \{0_{E_1}, (0, 0)\} = 2$.

Kernel of isogeny (Properties)

Proposition 18 (Proposition III.4.12 in [Sil09])

Let E be an elliptic curve and G be a finite subgroup of E.
Then there exist a unique (up to isomorphism) E' and a **separable** *isogeny*

$$\varphi : E \to E'$$

such that $\ker \varphi = G$. (E' and φ are not necessarily defined over $\mathbb{F}_q$.)

Kernel of isogeny (Properties)

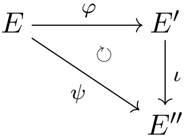
Proposition 18 (Proposition III.4.12 in [Sil09])

Let E be an elliptic curve and G be a finite subgroup of E.
Then there exist a unique (up to isomorphism) E' and a **separable** *isogeny*

$$\varphi : E \to E'$$

such that $\ker \varphi = G$. (E' and φ are not necessarily defined over $\mathbb{F}_q$.)

"up to isomorphism" means:
E'' and ψ satisfy the same conditions $\Rightarrow$ there is an **isomorphism** ι s.t.



We denote E' by E/G.

Proposition 19 (Remark III.4.13.2 in [Sil09])

In the previous proposition, suppose that G is invariant under **the q^k-th power Frobenius map** π_{q^k}*, i.e.,*

$$\pi_{q^k}(P) \in G \quad \text{for all } P \in G.$$

Then there exist a unique (up to isomorphism over $\mathbb{F}_{q^k}$) E' defined over $\mathbb{F}_{q^k}$ and a separable isogeny

$$\varphi : E \to E'$$

defined over $\mathbb{F}_{q^k}$ such that $\ker \varphi = G$.

Equivalence of isogenies

Definition 20

Two separable isogenies φ_1 and φ_2 are *equivalent* if $\ker \varphi_1 = \ker \varphi_2$.

Equivalence of isogenies

Definition 20

Two separable isogenies φ_1 and φ_2 are *equivalent* if $\ker \varphi_1 = \ker \varphi_2$.

Let φ_1 and φ_2 be equivalent isogenies with the same codomain.

$$E_1 \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} E_2$$

By Proposition 18, $\exists \iota \in \mathrm{Aut}(E_2)$ such that $\varphi_1 = \iota \circ \varphi_2$.

Equivalence of isogenies

Definition 20

Two separable isogenies φ_1 and φ_2 are *equivalent* if $\ker\varphi_1 = \ker\varphi_2$.

Let φ_1 and φ_2 be equivalent isogenies with the same codomain.

$$E_1 \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} E_2$$

By Proposition 18, $\exists\iota \in \mathrm{Aut}(E_2)$ such that $\varphi_1 = \iota \circ \varphi_2$.

More explicitly, one of the following holds:

- $\varphi_1 = \varphi_2$ or $\varphi_1 = -\varphi_2$.
- $j(E_2) = 1728$ and $\varphi_1 = \iota \circ \varphi_2$ for $\iota \in \mathrm{Aut}(E_2)$ of order 4.
- $j(E_2) = 0$ and $\varphi_1 = \iota \circ \varphi_2$ for $\iota \in \mathrm{Aut}(E_2)$ of order 3 or 6.

Dual isogeny

Theorem 21 (Theorem III.6.1 in [Sil09])

Let $\varphi : E_1 \to E_2$ *be an isogeny of degree* m.
Then there is a unique isogeny

$$\hat{\varphi} : E_2 \to E_1 \ \ \textit{such that} \ \ \hat{\varphi} \circ \varphi = [m].$$

We call $\hat{\varphi}$ the *dual isogeny* of φ and always use the notation $\hat{\varphi}$ for it.

"Unique" means that $\hat{\varphi}$ is literally unique.

Dual isogeny

Proposition 22 (Theorem III.6.2 in [Sil09])

Let $\varphi : E_1 \to E_2$ *be an isogeny.*

1. *For another isogeny* $\psi : E_2 \to E_3$*,*
$$\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}.$$
2. *For another isogeny* $\lambda : E_1 \to E_2$*,*
$$\widehat{\varphi + \lambda} = \hat{\varphi} + \hat{\lambda}.$$
3. *For all* $m \in \mathbb{Z} \setminus \{0\}$*,*
$$\widehat{[m]} = [m] \text{ and } \deg[m] = m^2.$$
4. $\deg \hat{\varphi} = \deg \varphi.$
5. $\hat{\hat{\varphi}} = \varphi.$

Dual isogeny

Remark

Let φ_1 and φ_2 be **equivalent** isogenies with the same codomain.

$$E_1 \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} E_2$$

If $j(E_2) = 0$ or 1728 and $E_1 \not\cong E_2$, then $\hat{\varphi}_1$ and $\hat{\varphi}_2$ could be **NOT equivalent**.

Dual isogeny

Remark

Let φ_1 and φ_2 be **equivalent** isogenies with the same codomain.

$$E_1 \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} E_2$$

If $j(E_2) = 0$ or 1728 and $E_1 \not\cong E_2$, then $\hat{\varphi}_1$ and $\hat{\varphi}_2$ could be **NOT equivalent**.

Example:
Suppose $j(E_2) = 1728$ and let $\iota \in \mathrm{Aut}(E_2)$ of order 4.
An separable isogeny $\varphi : E_1 \to E_2$ and $\iota \circ \varphi$ are **equivalent**.

$$\ker \widehat{\iota \circ \varphi} = \ker(\hat{\varphi} \circ \hat{\iota}) = \hat{\iota}^{-1}(\ker \hat{\varphi}) \neq \ker \hat{\varphi} \text{ in general.}$$

So $\hat{\varphi}$ and $\widehat{\iota \circ \varphi}$ are **NOT equivalent** in general.

Decomposition of isogeny

Proposition 23

Let $\varphi : E_1 \to E_2$ *be a separable isogeny of degree* $m_1 m_2$*.*
Then φ *can be decomposed into*

$$E_2 \xrightarrow{\varphi_1} E_3 \xrightarrow{\varphi_2} E_2,$$

where $\deg \varphi_1 = m_1$ *and* $\deg \varphi_2 = m_2$*.*

Decomposition of isogeny

Proposition 23

Let $\varphi : E_1 \to E_2$ *be a separable isogeny of degree* $m_1 m_2$*.*
Then φ *can be decomposed into*

$$E_2 \xrightarrow{\varphi_1} E_3 \xrightarrow{\varphi_2} E_2,$$

where $\deg \varphi_1 = m_1$ *and* $\deg \varphi_2 = m_2$*.*

(**Sketch of proof**)
$G := \ker \varphi$ contains a subgroup G_1 of order m_1.
$\exists \varphi_1 : E_1 \to E_3$ such that $\ker \varphi_1 = G_1$ (Proposition 18).
$\exists \varphi_2 : E_3 \to E_4$ such that $\ker \varphi_2 = \varphi_1(G)$ (Proposition 18).
Then $\ker(\varphi_2 \circ \varphi_1) = \varphi_1^{-1}(G) = G_1 + G = G$.
Thus, there is an isomorphism $\iota : E_4 \to E_2$ such that $\varphi = \iota \circ \varphi_2 \circ \varphi_1$. □

Isogeny of degree p

Proposition 24 (Corollary III.6.4 and Theorem V.3.1 in [Sil09])

- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ *for* $m \not\equiv 0 \pmod p$.
- $E[p] \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } E \text{ is ordinary,} \\ \{0_E\} & \text{if } E \text{ is supersingular.} \end{cases}$

Isogeny of degree p

Proposition 24 (Corollary III.6.4 and Theorem V.3.1 in [Sil09])

- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ *for* $m \not\equiv 0 \pmod{p}$.
- $E[p] \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } E \text{ is ordinary,} \\ \{0_E\} & \text{if } E \text{ is supersingular.} \end{cases}$

Corollary 25

- *If* E *is* **ordinary**, *there are exactly two isogenies of degree* p *from* E,
  1. π_p
  2. *the separable isogeny of kernel* $E[p]$.
- *If* E *is* **supersingular**, *only* π_p *is the isogeny of degree* p *from* E.

Cyclic isogeny

Proposition 26

Let $\varphi : E_1 \to E_2$ *be a separable isogeny.*
Then there exists an integer m *such that* φ *can be decomposed into*

$$E_1 \xrightarrow{[m]} E_1 \xrightarrow{\varphi_1} E_2,$$

where $\ker \varphi_1$ *is cyclic.*

Cyclic isogeny

Proposition 26

Let $\varphi : E_1 \to E_2$ *be a separable isogeny.*
Then there exists an integer m *such that* φ *can be decomposed into*

$$E_1 \xrightarrow{[m]} E_1 \xrightarrow{\varphi_1} E_2,$$

where $\ker \varphi_1$ *is cyclic.*

Sketch of proof

From the structure theorem of finite abelian groups,

$$\ker \varphi \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \quad (m \mid n).$$

Therefore, φ can be decomposed into

$$E \xrightarrow{[m]} E \xrightarrow{\varphi_1} E_1,$$

where $\ker \varphi_1 = [m] \ker \varphi \cong \mathbb{Z}/(n/m)\mathbb{Z}$. □

Cyclic isogeny

Definition 27

Let m be a positive integer.
An *m-isogeny* is a **separable** isogeny with **cyclic** kernel of order m.

Cyclic isogeny

Definition 27

Let m be a positive integer.
An *m-isogeny* is a **separable** isogeny with **cyclic** kernel of order m.

Theorem 28

Let m be a positive integer coprime with p.
*Then the number of m-**isogenies** from E is*

$$m \prod_{\ell} \left(1 + \frac{1}{\ell}\right),$$

where the product is taken over all prime divisors ℓ of m.

Cyclic isogeny

Definition 27

Let m be a positive integer.
An *m-isogeny* is a **separable** isogeny with **cyclic** kernel of order m.

Theorem 28

Let m be a positive integer coprime with p.
*Then the number of m-**isogenies** from E is*

$$m \prod_{\ell} \left(1 + \frac{1}{\ell}\right),$$

where the product is taken over all prime divisors ℓ of m.

Sketch of proof

Consider the number of cyclic subgroups of order m in $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Algorithm

Computing isogenies

Our task

Given an **elliptic curve** E and a **finite subgroup** G of E,
compute the **codomain** E' of a **separable isogeny** φ with kernel G.

In addition, given a point P on E, compute $\varphi(P)$.

Computing isogenies

Our task

Given an **elliptic curve** E and a **finite subgroup** G of E,
compute the **codomain** E' of a **separable isogeny** φ with kernel G.

In addition, given a point P on E, compute $\varphi(P)$.

Note:

- It is enough to consider separable isogenies.
  $\because$ An inseparable is decomposed into a separable isogeny
  and a Frobenius isogeny. (Frobenius isogenies are easy to compute.)

- We can assume that G is cyclic.
  $\because$ Otherwise, φ is decomposed into a scalar multiplication
  and an isogeny with a cyclic kernel.

Theorem 29 (Vélu's Formula, Theorem 12.16 in [Was08])

Let E be an elliptic curve defined by

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 =: f(x),$$

and G be a finite subgroup of E.
The following E' and φ give an isogeny $\varphi : E \to E'$ with kernel G.

$$E' : y^2 = x^3 + a_2x^2 + (a_4 - 5v)x + a_6 - 4a_2v - 7w,$$
$$\varphi(x, y) = \left(F(x),\ y \cdot F'(x)\right),$$

where $v = \sum_{P \in G \setminus \{0_E\}} f'(x(P)),\ w = \sum_{P \in G \setminus \{0_E\}} \left(2f(x(P)) + xf'(x(P))\right),$

$$F(x) = x + \sum_{P \in G \setminus \{0_E\}} \left(\frac{f'(x(P))}{x - x(P)} + \frac{2f(x(P))}{(x - x(P))^2} \right).$$

For a rational function $r(x)$, $r'(x)$ denotes the derivative of $r(x)$.

Remarks on Vélu's Formula

- Vélu's formula requires $O(\#G)$ operations.
- We do NOT need the y-coordinate of the points in G.
  $\because G = -G$.
- The operations in the computation are on a field containing the x-coordinates of the points in G.

  I.e., the operations are on $\mathbb{F}_{q^k}$ such that

  $$\pi_{q^k}(P) = P \text{ or } -P \text{ for all } P \in G.$$

  Note: φ could be defined over a smaller field than $\mathbb{F}_{q^k}$.
- In practice, we often use Montgomery curves, which have more efficient formulas for isogenies (see Appendix).

Chain of isogenies

Let G be a **cyclic** subgroup of E of order n and φ be the separable isogeny with kernel G.

Chain of isogenies

Let G be a **cyclic** subgroup of E of order n and φ be the separable isogeny with kernel G.

Assume that $n = \prod_{i=1}^{k} \ell_i$ for primes ℓ_i (not necessarily distinct). From Proposition 23, we can decompose φ into a chain of isogenies

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

where $\deg \varphi_i = \ell_i$.

Chain of isogenies

Let G be a **cyclic** subgroup of E of order n and φ be the separable isogeny with kernel G.

Assume that $n = \prod_{i=1}^{k} \ell_i$ for primes ℓ_i (not necessarily distinct).
From Proposition 23, we can decompose φ into a chain of isogenies

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

where $\deg \varphi_i = \ell_i$.

In many cases,
computing φ_i's sequentially is **more efficient** than computing φ directly.

Chain of isogenies

Let G be a **cyclic** subgroup of E of order n and φ be the separable isogeny with kernel G.

Assume that $n = \prod_{i=1}^{k} \ell_i$ for primes ℓ_i (not necessarily distinct). From Proposition 23, we can decompose φ into a chain of isogenies

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

where $\deg \varphi_i = \ell_i$.

In many cases,
computing φ_i's sequentially is **more efficient** than computing φ directly.

$\because$ The cost of computing φ is linear in $n = \prod_{i=1}^{k} \ell_i$,
while the cost of computing all φ_i's is linear in $\sum_{i=1}^{k} \ell_i$.

Computing a chain of isogenies

We consider computing a chain of isogenies

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

where $\deg \varphi_i = \ell_i$.

Computing a chain of isogenies

We consider computing a chain of isogenies

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

where $\deg \varphi_i = \ell_i$.

Since the kernel G of the composite isogeny is cyclic, we have

$$\begin{aligned}
\ker \varphi_1 &= [n/\ell_1]G, \\
\ker \varphi_2 &= [n/(\ell_1\ell_2)]\varphi_1(G), \quad (\because \#\varphi_1(G) = n/\ell_1), \\
&\vdots \\
\ker \varphi_i &= [n/(\ell_1 \cdots \ell_i)]\varphi_{i-1} \circ \cdots \circ \varphi_1(G), \\
&\vdots \\
\ker \varphi_k &= \varphi_{k-1} \circ \cdots \circ \varphi_1(G).
\end{aligned}$$

Computing a chain of isogenies

Given E and $x(P)$ for a generator P of G, compute φ_i's:

E

$x(P)$

Computing a chain of isogenies

Given E and $x(P)$ for a generator P of G, compute φ_i's:

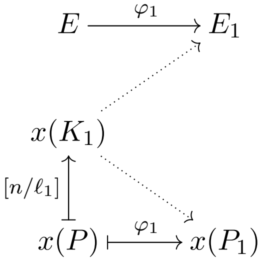
$$E$$

$$x(K_1)$$

$$\uparrow [n/\ell_1]$$

$$x(P)$$

Given E and $x(P)$ for a generator P of G, compute φ_i's:



Computing a chain of isogenies

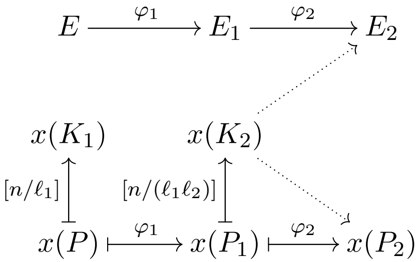
Given E and $x(P)$ for a generator P of G, compute φ_i's:

$$E \xrightarrow{\varphi_1} E_1$$

$$\begin{array}{ccc} x(K_1) & & x(K_2) \\ \uparrow{\scriptstyle [n/\ell_1]} & & \uparrow{\scriptstyle [n/(\ell_1\ell_2)]} \\ x(P) & \xmapsto{\varphi_1} & x(P_1) \end{array}$$

Computing a chain of isogenies

Given E and $x(P)$ for a generator P of G, compute φ_i's:



Computing a chain of isogenies

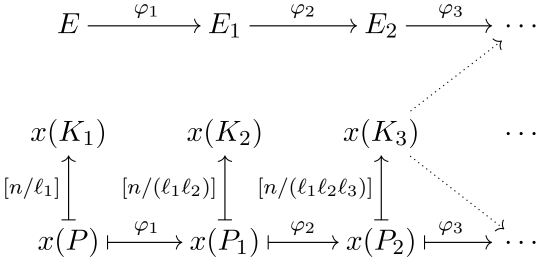
Given E and $x(P)$ for a generator P of G, compute φ_i's:

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2$$

$$\begin{array}{ccccc} x(K_1) & & x(K_2) & & x(K_3) \\ \uparrow{\scriptstyle [n/\ell_1]} & & \uparrow{\scriptstyle [n/(\ell_1\ell_2)]} & & \uparrow{\scriptstyle [n/(\ell_1\ell_2\ell_3)]} \\ x(P) & \xmapsto{\varphi_1} & x(P_1) & \xmapsto{\varphi_2} & x(P_2) \end{array}$$

Computing a chain of isogenies

Given E and $x(P)$ for a generator P of G, compute φ_i's:



Computing a chain of isogenies

Given E and $x(P)$ for a generator P of G, compute φ_i's:

$$E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_{k-1}} E_{k-1} \xrightarrow{\varphi_k}$$

$$\begin{array}{ccccccccc}
x(K_1) & & x(K_2) & & x(K_3) & & \cdots & & \\
\uparrow [n/\ell_1] & & \uparrow [n/(\ell_1\ell_2)] & & \uparrow [n/(\ell_1\ell_2\ell_3)] & & & & \\
x(P) & \xmapsto{\varphi_1} & x(P_1) & \xmapsto{\varphi_2} & x(P_2) & \xmapsto{\varphi_3} & \cdots & \xmapsto{\varphi_{k-1}} & x(P_k)
\end{array}$$

Given E and $x(P)$ for a generator P of G, compute φ_i's:

$$
\begin{array}{ccccccccccc}
E & \xrightarrow{\varphi_1} & E_1 & \xrightarrow{\varphi_2} & E_2 & \xrightarrow{\varphi_3} & \cdots & \xrightarrow{\varphi_{k-1}} & E_{k-1} & \xrightarrow{\varphi_k} & E_k \\
 & & & & & & & & & \nearrow & \\
x(K_1) & & x(K_2) & & x(K_3) & & \cdots & & x(K_k) & & \\
{\scriptstyle [n/\ell_1]}\uparrow & & {\scriptstyle [n/(\ell_1\ell_2)]}\uparrow & & {\scriptstyle [n/(\ell_1\ell_2\ell_3)]}\uparrow & & & & \| & & \\
x(P) & \xmapsto{\varphi_1} & x(P_1) & \xmapsto{\varphi_2} & x(P_2) & \xmapsto{\varphi_3} & \cdots & \xmapsto{\varphi_{k-1}} & x(P_k) & &
\end{array}
$$

Cost of computing a chain of isogenies

We need to compute the following in each step:

- E_i : $O(\ell_i)$ operations by Vélu's formula.
- $x(P_i)$: $O(\ell_i)$ operations by Vélu's formula.
- $x(K_i)$: $O(\log(n/(\ell_1 \cdots \ell_i)))$ operations by binary multiplication.

Cost of computing a chain of isogenies

We need to compute the following in each step:

- E_i : $O(\ell_i)$ operations by Vélu's formula.
- $x(P_i)$: $O(\ell_i)$ operations by Vélu's formula.
- $x(K_i)$: $O(\log(n/(\ell_1 \cdots \ell_i)))$ operations by binary multiplication.

The total cost is

$$O\left(\sum_{i=1}^{k} \ell_i\right) + O\left(k \log(n) - \sum_{i=1}^{k} (k+1-i) \log(\ell_i)\right).$$

Cost of computing a chain of isogenies

We need to compute the following in each step:

- E_i : $O(\ell_i)$ operations by Vélu's formula.
- $x(P_i)$: $O(\ell_i)$ operations by Vélu's formula.
- $x(K_i)$: $O(\log(n/(\ell_1 \cdots \ell_i)))$ operations by binary multiplication.

The total cost is

$$O\left(\sum_{i=1}^{k} \ell_i\right) + O\left(k\log(n) - \sum_{i=1}^{k}(k+1-i)\log(\ell_i)\right).$$

Assume that $\max_i\{\ell_i\}$ in $O(1)$.

Cost of computing a chain of isogenies

We need to compute the following in each step:

- E_i : $O(\ell_i)$ operations by Vélu's formula.
- $x(P_i)$: $O(\ell_i)$ operations by Vélu's formula.
- $x(K_i)$: $O(\log(n/(\ell_1 \cdots \ell_i)))$ operations by binary multiplication.

The total cost is

$$O\left(\sum_{i=1}^{k} \ell_i\right) + O\left(k \log(n) - \sum_{i=1}^{k}(k+1-i)\log(\ell_i)\right).$$

Assume that $\max_i\{\ell_i\}$ in $O(1)$.

Then $k \in O(\log n)$, so the total cost is

$$O\left((\log n)^2\right).$$

Strategy

We can reduce the cost from

$$O((\log n)^2) \quad \text{to} \quad O(\log n \log\log n).$$

(so called *stragegy technique* proposed by [DFJP14])

Strategy

We can reduce the cost from

$$O((\log n)^2) \quad \text{to} \quad O(\log n \log\log n).$$

(so called *stragegy technique* proposed by [DFJP14])

For simplicity, we assume that $n = \ell^k$.

We denote the cost of computing the following by

C_{cod} : the **codomain** of an ℓ-isogeny

C_{evl} : the **image of a point** under an ℓ-isogeny

C_{mul} : the **multiplication** by ℓ

Example of strategies

Let $P \in E$ be a point of order ℓ^3.
Decompose the separable isogeny with kernel $\langle P \rangle$ into

$$E \xrightarrow[\langle K_1 \rangle]{\varphi_1} E_1 \xrightarrow[\langle K_2 \rangle]{\varphi_2} E_2 \xrightarrow[\langle K_3 \rangle]{\varphi_3} E_3$$

Step	Objects	Cost
0	E, $x(P)$	
1	$x([\ell^2]P) = x(K_1)$	$(2\ C_{\mathsf{mul}})$
2	E_1, $x(\varphi_1(P))$	$(C_{\mathsf{cod}} + C_{\mathsf{evl}})$
3	$x([\ell]\varphi_1(P)) = x(K_2)$	(C_{mul})
4	E_2, $x(\varphi_1 \circ \varphi_2(P)) = x(K_3)$	$(C_{\mathsf{cod}} + C_{\mathsf{evl}})$
5	E_3	(C_{cod})

The total cost is $3C_{\mathsf{cod}} + 2C_{\mathsf{evl}} + 3C_{\mathsf{mul}}$.

Example of strategies

Let $P \in E$ be a point of order ℓ^3.
Decompose the separable isogeny with kernel $\langle P \rangle$ into

$$E \xrightarrow[\langle K_1 \rangle]{\varphi_1} E_1 \xrightarrow[\langle K_2 \rangle]{\varphi_2} E_2 \xrightarrow[\langle K_3 \rangle]{\varphi_3} E_3$$

Step	Objects	Cost
0	E, $x(P)$	
1	$x([\ell]P), x([\ell^2]P) = x(K_1)$	$(2\ C_{\mathsf{mul}})$
2	E_1, $x(\varphi_1(P)), x(\varphi([\ell]P))$	$(C_{\mathsf{cod}} + 2C_{\mathsf{evl}})$
3	$x(\varphi_1([\ell]P)) = x([\ell]\varphi_1(P)) = x(K_2)$	(0)
4	E_2, $x(\varphi_1 \circ \varphi_2(P)) = x(K_3)$	$(C_{\mathsf{cod}} + C_{\mathsf{evl}})$
5	E_3	(C_{cod})

The total cost is $3C_{\mathsf{cod}} + 3C_{\mathsf{evl}} + 2C_{\mathsf{mul}}$.

Example of strategies

Let $P \in E$ be a point of order ℓ^3.
Decompose the separable isogeny with kernel $\langle P \rangle$ into

$$E \xrightarrow[\langle K_1 \rangle]{\varphi_1} E_1 \xrightarrow[\langle K_2 \rangle]{\varphi_2} E_2 \xrightarrow[\langle K_3 \rangle]{\varphi_3} E_3$$

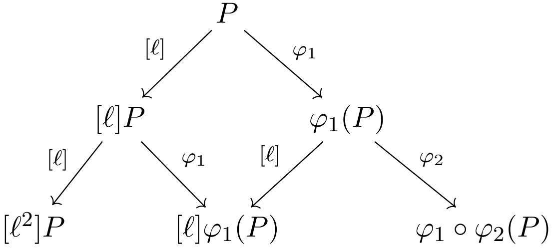
Step	Objects	Cost
0	E, $x(P)$	
1	$x([\ell]P), x([\ell^2]P) = x(K_1)$	$(2\ C_{\mathsf{mul}})$
2	E_1, $x(\varphi_1(P)), x(\varphi([\ell]P))$	$(C_{\mathsf{cod}} + 2C_{\mathsf{evl}})$
3	$x(\varphi_1([\ell]P)) = x([\ell]\varphi_1(P)) = x(K_2)$	(0)
4	E_2, $x(\varphi_1 \circ \varphi_2(P)) = x(K_3)$	$(C_{\mathsf{cod}} + C_{\mathsf{evl}})$
5	E_3	(C_{cod})

The total cost is $3C_{\mathsf{cod}} + 3C_{\mathsf{evl}} + 2C_{\mathsf{mul}}$.

$\Rightarrow$ We can replace C_{mul} by C_{evl}.

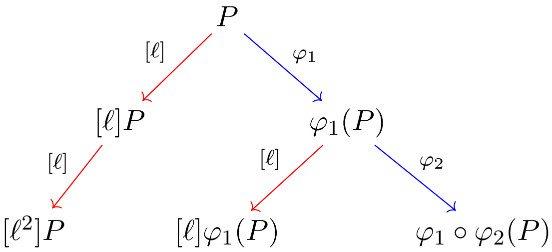
Visualization of strategies

The relationship among the points in the previous example:



Visualization of strategies

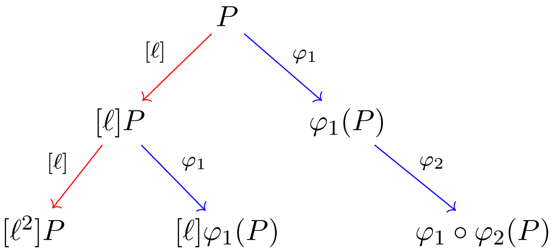
The first strategy:



The cost is $3C_{\mathsf{cod}} + 2C_{\mathsf{evl}} + 3C_{\mathsf{mul}}$.

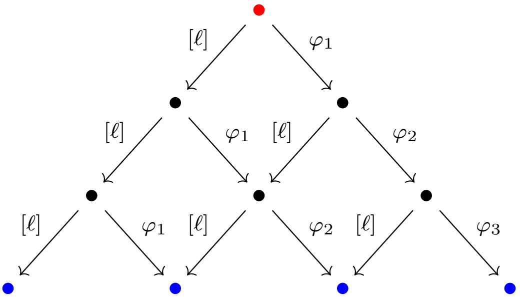
Visualization of strategies

The second strategy:



The cost is $3C_{\mathsf{cod}} + 3C_{\mathsf{evl}} + 2C_{\mathsf{mul}}$.

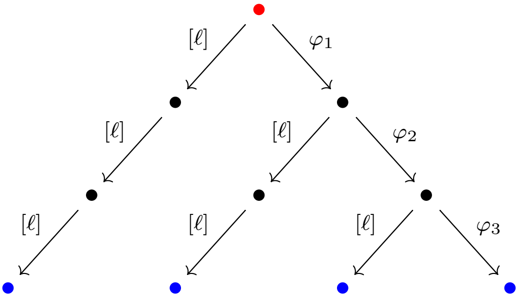
$k = 4$



Problem:

Choose edges connecting the top and bottom vertices to **minimize the cost**.

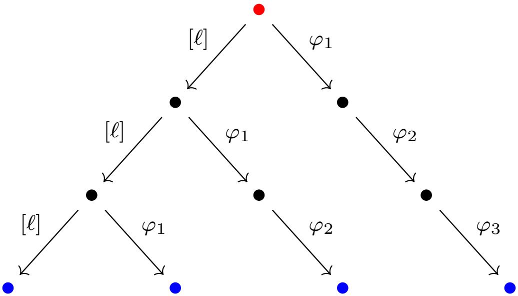
$k = 4$



Cost: $4C_{\text{cod}} + 3C_{\text{evl}} + 6C_{\text{mul}}$

We call this *multiplication-based strategy*.

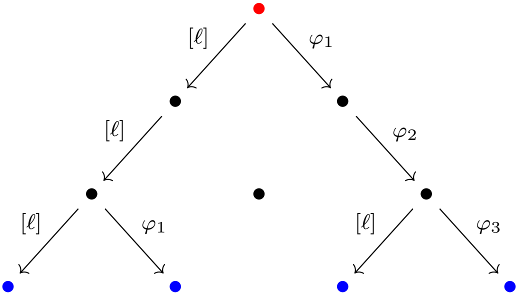
$k = 4$



Cost: $4C_{\mathsf{cod}} + 6C_{\mathsf{evl}} + 3C_{\mathsf{mul}}$

We call this *isogeny-based strategy*.

$k = 4$



Cost: $4C_{\mathsf{cod}} + 4C_{\mathsf{evl}} + 4C_{\mathsf{mul}}$

This strategy minimizes the cost if

$$\frac{1}{2}C_{\mathsf{mul}} \leq C_{\mathsf{evl}} \leq 2C_{\mathsf{mul}}.$$

Cost of strategy

Consider a chain of isogenies of length k.

The cost of the **multiplication-based strategy** is

$$kC_{\mathsf{cod}} + (k-1)C_{\mathsf{evl}} + \frac{k(k-1)}{2}C_{\mathsf{mul}}.$$

The cost of the **isogeny-based strategy** is

$$kC_{\mathsf{cod}} + \frac{k(k-1)}{2}C_{\mathsf{evl}} + (k-1)C_{\mathsf{mul}}.$$

These are $O(k^2)$.

Cost of optimized strategy

A strategy is *optimized* if its cost is **minimum** among all strategies of the same length.

We denote the cost of an **optimized strategy** by $C_{\mathsf{opt}}(k)$.

Cost of optimized strategy

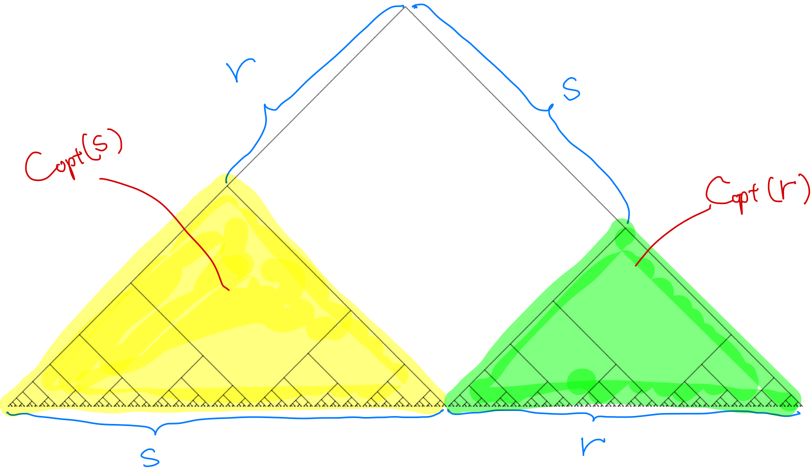
A strategy is *optimized* if its cost is **minimum** among all strategies of the same length.

We denote the cost of an **optimized strategy** by $C_{\mathsf{opt}}(k)$.

Theorem 30 (Lemma 4.5 in [DFJP14])

$$C_{\mathsf{opt}}(k) = \min_{r+s=k} \left\{ r \cdot C_{\mathsf{mul}} + s \cdot C_{\mathsf{evl}} + C_{\mathsf{opt}}(r) + C_{\mathsf{opt}}(s) \right\}.$$

Sketch of proof



* The figure is from [DFJP14].

Bound of cost

Theorem 31

Let $C = \max\{C_{\mathsf{evl}}, C_{\mathsf{mul}}\}$. *Then*

$$C_{\mathsf{opt}}(k) \leq k \cdot C_{\mathsf{cod}} + (k\lceil \log_2 k \rceil)C.$$

Sketch of proof

$$C_{\mathsf{opt}}(k) \leq \lfloor k/2 \rfloor C + \lceil k/2 \rceil C + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil)$$
$$= kC + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil)$$

Sketch of proof

$$
\begin{aligned}
C_{\mathsf{opt}}(k) &\le \lfloor k/2 \rfloor C + \lceil k/2 \rceil C + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil) \\
&= kC + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil) \\
&\le kC + kC + C_{\mathsf{opt}}(\lfloor \lfloor k/2 \rfloor /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lfloor k/2 \rfloor /2 \rceil) \\
&\quad + C_{\mathsf{opt}}(\lfloor \lceil k/2 \rceil /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lceil k/2 \rceil /2 \rceil) \\
&= 2kC + C_{\mathsf{opt}}(\lfloor \lfloor k/2 \rfloor /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lfloor k/2 \rfloor /2 \rceil) \\
&\quad + C_{\mathsf{opt}}(\lfloor \lceil k/2 \rceil /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lceil k/2 \rceil /2 \rceil)
\end{aligned}
$$

Sketch of proof

$$
\begin{aligned}
C_{\mathsf{opt}}(k) &\leq \lfloor k/2 \rfloor C + \lceil k/2 \rceil C + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil) \\
&= kC + C_{\mathsf{opt}}(\lfloor k/2 \rfloor) + C_{\mathsf{opt}}(\lceil k/2 \rceil) \\
&\leq kC + kC + C_{\mathsf{opt}}(\lfloor \lfloor k/2 \rfloor /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lfloor k/2 \rfloor /2 \rceil) \\
&\quad + C_{\mathsf{opt}}(\lfloor \lceil k/2 \rceil /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lceil k/2 \rceil /2 \rceil) \\
&= 2kC + C_{\mathsf{opt}}(\lfloor \lfloor k/2 \rfloor /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lfloor k/2 \rfloor /2 \rceil) \\
&\quad + C_{\mathsf{opt}}(\lfloor \lceil k/2 \rceil /2 \rfloor) + C_{\mathsf{opt}}(\lceil \lceil k/2 \rceil /2 \rceil) \\
&\;\vdots \\
&\leq k \lceil \log_2 k \rceil C + kC_{\mathsf{opt}}(1) \\
&= k \lceil \log_2 k \rceil C + kC_{\mathsf{cod}}.
\end{aligned}
$$

Example

Assume $k = 100$ and $C_{\mathsf{cod}} = C_{\mathsf{evl}} = C_{\mathsf{mul}} = C$.

The cost the mulitplication-based (isogeny-based) strategy is

$$100C + 99C + 4950C = 5149C.$$

The cost of the optimized strategy is

$$100C + 672C = 772C.$$

This is about 15% of the cost of the multiplication-based strategy.

How to compute the optimized strategy?

There exists an algorithm to compute an optimized strategy.
(see Algorithm 60 in [JAC+22])

- Use Theorem 30.
- The computation is **recursive**.
- The cost is $O(k^2)$.
- In applications, an optimized strategy is computed in **advance**.
  $\because k$ is fixed (in most cases).

Further topics

Modular polynomials

Let $n > 1$ be an integer.

The *modular polynomial of order n* is a polynomial $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$ such that

$$\Phi_n(j_1, j_2) = 0 \Leftrightarrow \exists n\text{-isogeny } \varphi : E_{j_1} \to E_{j_2},$$

where E_{j_i} is the elliptic curve with j-invariant j_i.

Example:

$$\begin{aligned}\Phi_2(X,Y) = &X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + XY^2) - 162000(X^2 + Y^2) \\ &+ 40773375XY + 8748000000(X + Y) - 157464000000000.\end{aligned}$$

See Chapter 10.3 in [Was08] or Chapter 5 in [Lan87] for more details.

$\sqrt{}$élu's formulas

A *$\sqrt{}$élu's formula* is an algorithm to compute an ℓ-isogeny.

- by [BDFLS20].
- based on Vélu's formula.
- The cost is $\tilde{O}(\sqrt{\ell})$ operations, not $O(\ell)$.
- uses the resultant of two polynomials.

In practice, $\sqrt{}$élu's formulas are faster than Vélu's formulas for $\ell > 100$.

Radical isogenies

Radical isogenies are formulas to compute an ℓ-isogeny.

- by [CDV20],
- uses an ℓ-th root (radical) of an element.

Which of Vélu's formulas or radical isogenies is faster depends on applications.

Appendix

Montgomery curves

Definition 32

A *Montgomery curve* is an elliptic curve defined by

$$E_A : y^2 = x^3 + Ax^2 + x, \quad A^2 \neq 4.$$

We call A the *Montgomery coefficient* of E_A.

We denote the Montgomery curve with coefficient A by E_A.

Addition on Montgomery curves

Proposition 33 (§10.3 in [Mon87])

Let E_A be a Montgomery curve with the Montgomery coefficient A, and $P, Q \in E_A \setminus \{0_{E_A}\}$. Then, the following hold:

$$x(P+Q)x(P-Q) = \left(\frac{x(P)x(Q)-1}{x(P)-x(Q)}\right)^2,$$

$$x(2P) = \frac{(x(P)^2-1)^2}{4(x(P)^3 + A \cdot x(P)^2 + x(P))}.$$

Note:

- $x(P) - x(Q) = 0 \Leftrightarrow P + Q = 0_{E_A}$ or $P - Q = 0_{E_A}$.
- $x(P)^3 + A \cdot x(P)^2 + x(P) = 0 \Leftrightarrow [2]P = 0_{E_A}$.

xADD and xDBL on Montgomery curves

Let E_A be a Montgomery curve and $P, Q \in E_A$.

From Proposition 33, we define the following two algorithms.

xADD:

Input: $A, x(P), x(Q), x(P - Q)$
Output: $x(P + Q)$

xDBL:

Input: $A, x(P)$
Output: $x([2]P)$

Scalar multiplication on Montgomery curves

Algorithm 1: Montgomery ladder

Input: A Montgomery coefficient A, the x-coordinate of a point $P \in E_A$, and an integer $n > 0$.

Output: The x-coordinate of $[n]P$.

Let $(n_0, n_1, \dots, n_k)$ be the binary expansion of n. // $n = \sum_{i=0}^{k} n_i 2^i$.
Let $(x_0, x_1) := (x(P), x([2]P))$
for $i = k - 1$ **to** 0 **do**
  if $n_i = 1$ **then**
    $(x_0, x_1) := (\mathsf{xADD}(A, x_0, x_1, x(P)), \mathsf{xDBL}(A, x_0))$
  else
    $(x_0, x_1) := (\mathsf{xDBL}(A, x_0)), \mathsf{xADD}(A, x_0, x_1, x(P))$
  // $x_0 = x([n_k 2^{k-i} + \cdots + n_i 2^i]P)$
  // $x_1 = x([n_k 2^{k-i} + \cdots + n_i 2^i + 1]P)$
return x_0

Remarks on Montgomery ladder

- We can give a constant-time implementation of the Montgomery ladder.

  I.e., the computational time only depends on the bit-length of the scalar n, not on the value of n.

- If we do not need a constant-time implementation, we can construct a more efficient *differential addition chain* (see [CS17] for more details).

Theorem 34 (2-isogeny formula, Section 4.3 in [JD11])

An isogeny $\varphi : E_A \to E_{A'}$ *with kernel* $\langle (0,0) \rangle$ *is given by*

$$A' = \frac{A+6}{2\sqrt{A+2}},$$

$$x(\varphi(P)) = \frac{(x(P)-1)^2}{(2\sqrt{A+2})x(P)} \text{ for } P \in E_A.$$

Isogeny formulas on Montgomery curves

Theorem 35 (2-isogeny formula, Section 1.1.9 in [JAC+22])

Let $(x_2, 0)$ *be a point on* E_A *of order 2.*
Then an isogeny $\varphi : E_A \to E_{A'}$ *with kernel* $\langle (x_2, 0) \rangle$ *is given by*

$$A' = 2(2 - x_2),$$

$$x(\varphi(P)) = \frac{x(P)(x_2 - x(P))}{x(P) - x_2} \text{ for } P \in E_A.$$

Isogeny formulas on Montgomery curves

Theorem 36 (4-isogeny formula, Section 4.3.2 in [DFJP14])

An isogeny $\varphi : E_A \to E_{A'}$ *with kernel* $\langle(1, \sqrt{A+2})\rangle$ *is given by*

$$A' = 2\frac{A+6}{A-2},$$

$$x(\varphi(P)) = \frac{(x(P)+1)^2(x(P)^2 + Ax(P) + 1)}{(2-A)x(P)(x(P)-1)^2} \text{ for } P \in E_A.$$

Theorem 37 (4-isogeny formula, Section 4.3.2 in [DFJP14])

An isogeny $\varphi : E_A \to E_{A'}$ *with kernel* $\langle(-1, \sqrt{A-2})\rangle$ *is given by*

$$A' = -2\frac{A-6}{A+2},$$

$$x(\varphi(P)) = -\frac{(x(P)-1)^2(x(P)^2 + Ax(P) + 1)}{(2+A)x(P)(x(P)+1)^2} \text{ for } P \in E_A.$$

Isogeny formulas on Montgomery curves

Theorem 38 (4-isogeny formula, Section 1.1.9 in [JAC+22])

Let (x_4, y_4) *be a point on* E_A *of order 4.*
Then an isogeny $\varphi : E_A \to E_{A'}$ *with kernel* $\langle (x_4, y_4) \rangle$ *is given by*

$$A' = 4x_4^4 - 2,$$

$$x(\varphi(P)) = -\frac{x(P)((x_4^2+1)x(P) - 2x_4)(x_4 x(P) - 1)^2}{(x(P) - x_4)^2(2x_4 x(P) - x_4^2 - 1)} \text{ for } P \in E_A.$$

Theorem 39 (Odd-degree isogeny formula, Theorem 1 in [CH17])

Let K be a point on E_A of odd order ℓ. We denote the x-coordinate of $[i]K$ by x_i for $i = 1, 2, \ldots, (\ell-1)/2$.
Then an isogeny $\varphi : E_A \to E_{A'}$ with kernel $\langle K \rangle$ is given by

$$A' = \left(6 \sum_{i=1}^{\frac{\ell-1}{2}} \left(\frac{1}{x_i} - x_i \right) + A \right) \left(\prod_{i=1}^{\frac{\ell-1}{2}} x_i \right)^2,$$

$$x(\varphi(P)) = x(P) \left(\prod_{i=1}^{\frac{\ell-1}{2}} \frac{x_i x(P) - 1}{x(P) - x_i} \right)^2.$$

Isogeny formulas on Montgomery curves

Theorem 40 (Odd-degree isogeny formula, Section 4.2 in [MR18])

We use the same notation as in the previous theorem. Then we have

$$A' = 2\frac{a+d}{a-d},$$

where a and d are defined by

$$a = (A+2)^{\ell}\left(\prod_{i=1}^{\frac{\ell-1}{2}}(x_i+1)\right)^8,$$

$$d = (A-2)^{\ell}\left(\prod_{i=1}^{\frac{\ell-1}{2}}(x_i-1)\right)^8.$$

Note: This formula is more efficient than the previous one if $\ell \geq 7$.

References I

[BDFLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith.
Faster computation of isogenies of large prime degree.
In Steven Galbraith, editor, *ANTS-XIV - 14th Algorithmic Number Theory Symposium*, volume 4 of *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, pages 39–55, Auckland, New Zealand, 2020. Mathematical Sciences Publishers.

[CDV20] Wouter Castryck, Thomas Decru, and Frederik Vercauteren.
Radical isogenies.
In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 493–519. Springer, Cham, December 2020.

[CH17] Craig Costello and Hüseyin Hisil.
A simple and compact algorithm for SIDH with arbitrary degree isogenies.
In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 303–329. Springer, Cham, December 2017.

[CS17] Craig Costello and Benjamin Smith.
Montgomery curves and their arithmetic: The case of large characteristic fields.
Cryptology ePrint Archive, Report 2017/212, 2017.

References II

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût.
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
Journal of Mathematical Cryptology, 8(3):209–247, 2014.

[JAC+22] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson.
SIKE.
Technical report, National Institute of Standards and Technology, 2022.
available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions`.

[JD11] David Jao and Luca De Feo.
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34. Springer, Berlin, Heidelberg, November / December 2011.

References III

[Lan87] Serge Lang.
Elliptic Functions.
Graduate texts in mathematics. Springer, 2nd edition, 1987.

[Mon87] P. L. Montgomery.
Speeding the Pollard and elliptic curve methods of factorization.
Mathematics of Computation, 48(177):243–264, 1987.

[MR18] Michael Meyer and Steffen Reith.
A faster way to the CSIDH.
In Debrup Chakraborty and Tetsu Iwata, editors, *INDOCRYPT 2018*, volume 11356 of *LNCS*, pages 137–152. Springer, Cham, December 2018.

[Sil09] Joseph H. Silverman.
The Arithmetic of Elliptic Curves.
Graduate Texts in Mathematics. Springer New York, 2nd edition, 2009.

[Was08] Lawrence C. Washington.
Elliptic Curves: Number Theory and Cryptography, Second Edition.
Chapman & Hall/CRC, 2 edition, 2008.