Talk 1

Elliptic curves and endomorphism rings

Talk 2

Computing the endomorphism ring of low-dimensional abelian varieties over finite fields

Annamaria Iezzi

Université Grenoble Alpes

CAIPI : *Endomorphisms and invariants of some abelian varieties*

Nancy - April 7, 2025

Abelian varieties

An **abelian variety** over a field K is a projective algebraic variety $\mathcal{A}$ defined over K which is also an algebraic group. This means that $\mathcal{A}$ is endowed with a group structure and that the group operations

$$\begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \to & \mathcal{A} \\ (P, Q) & \mapsto & P + Q \end{array} \qquad \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ P & \mapsto & -P \end{array}$$

are given by regular maps.

Abelian varieties

An **abelian variety** over a field K is a projective algebraic variety $\mathcal{A}$ defined over K which is also an algebraic group. This means that $\mathcal{A}$ is endowed with a group structure and that the group operations

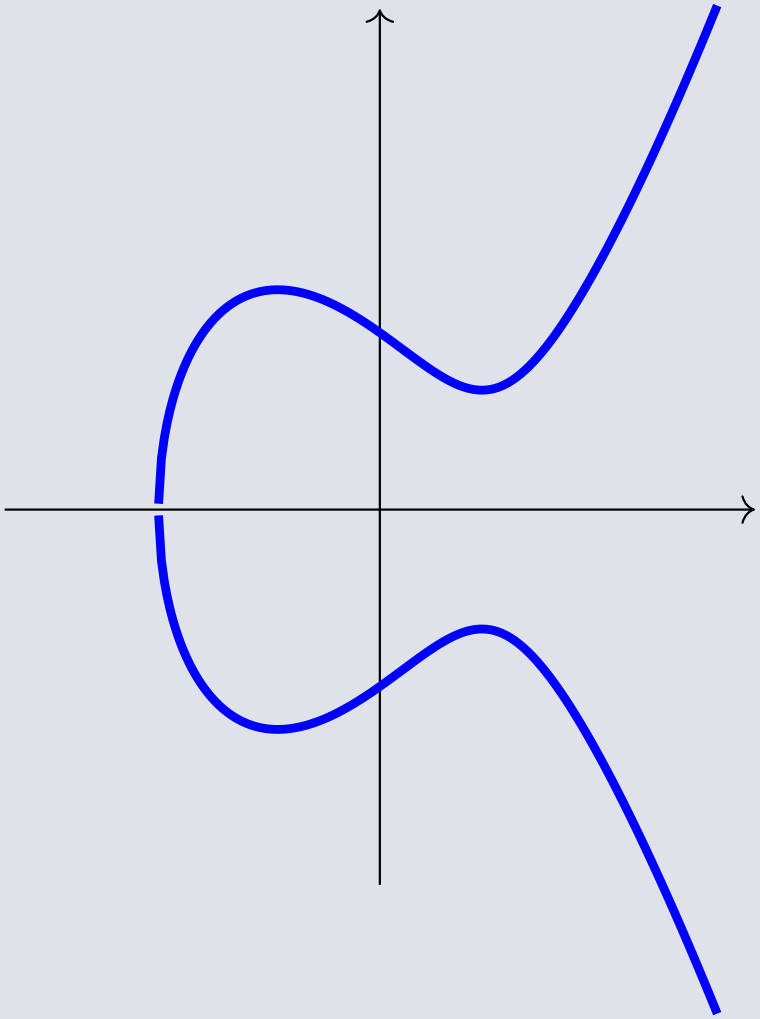
$$\begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \to & \mathcal{A} \\ (P, Q) & \mapsto & P + Q \end{array} \qquad \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ P & \mapsto & -P \end{array}$$

are given by regular maps.

The group law of an abelian variety is necessarily commutative and the variety is non-singular. We denote by $0_{\mathcal{A}}$ the identity element of $\mathcal{A}$.

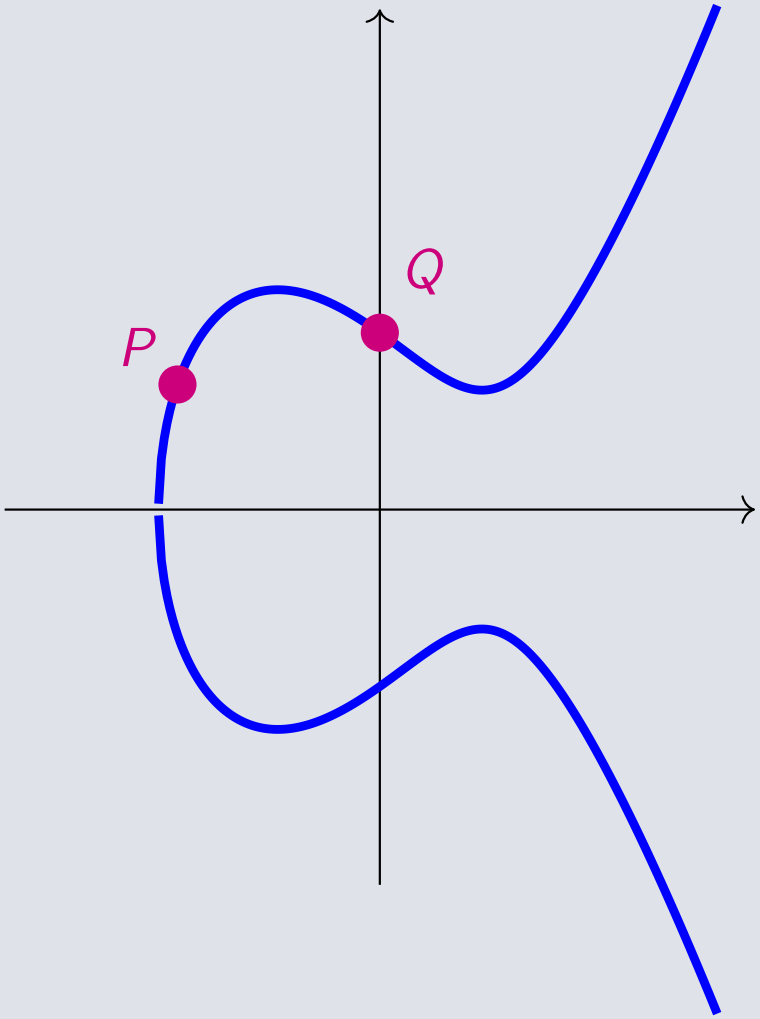
An abelian variety of dimension 1

$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$



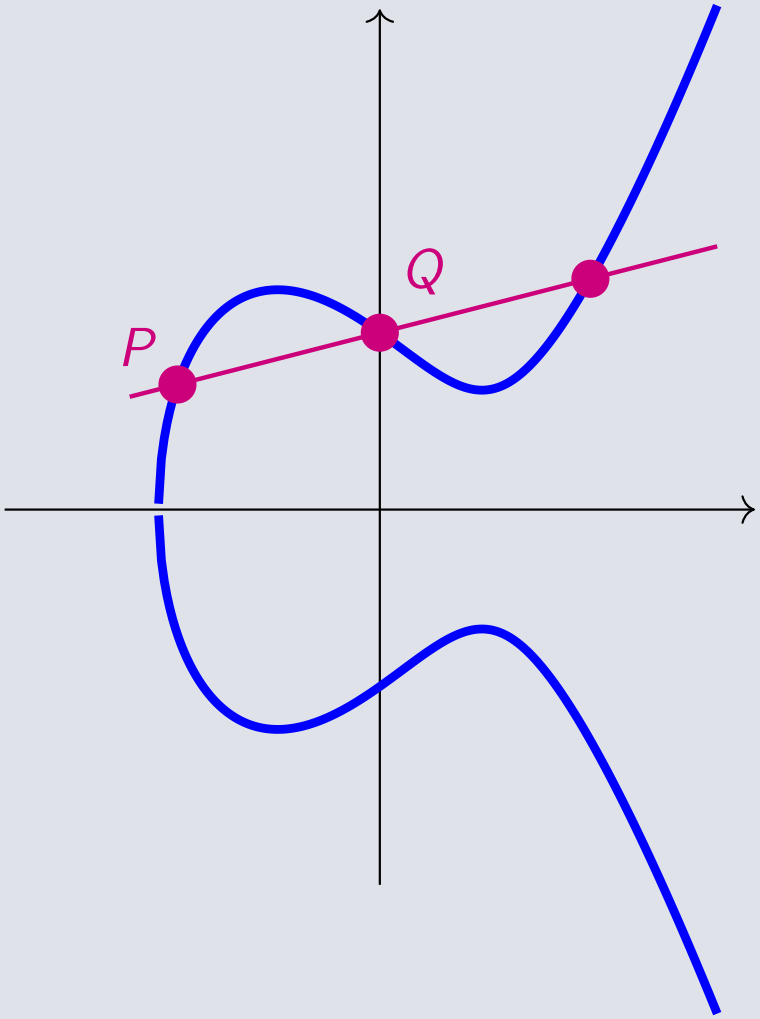
An abelian variety of dimension 1

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



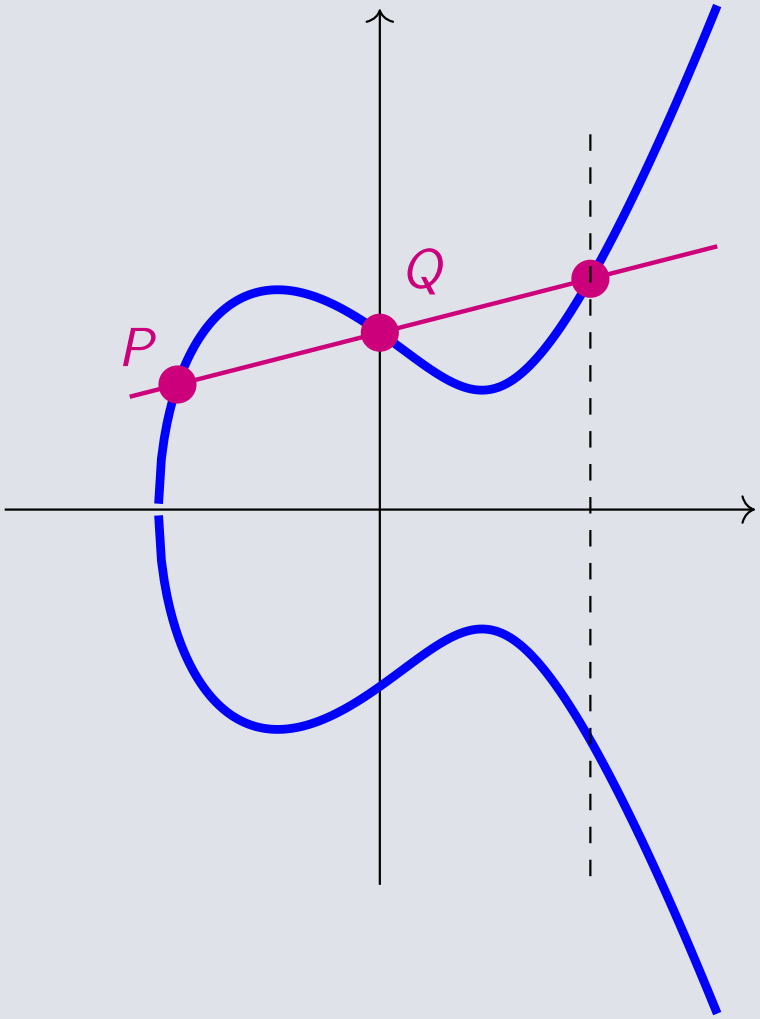
An abelian variety of dimension 1

$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$



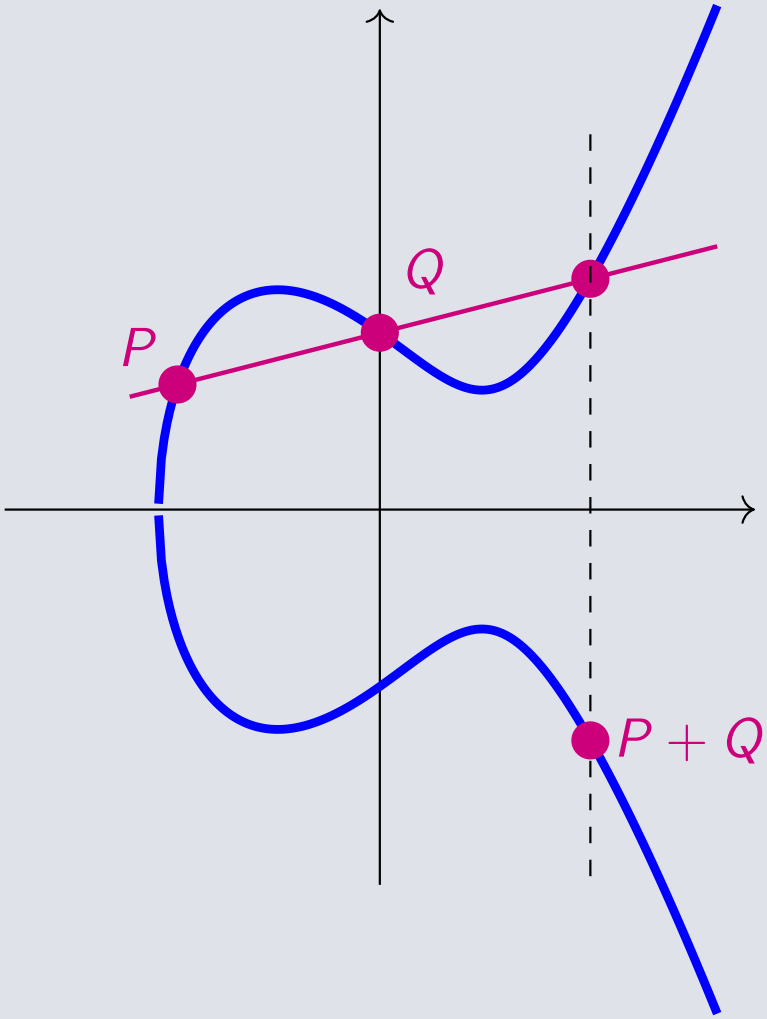
An abelian variety of dimension 1

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



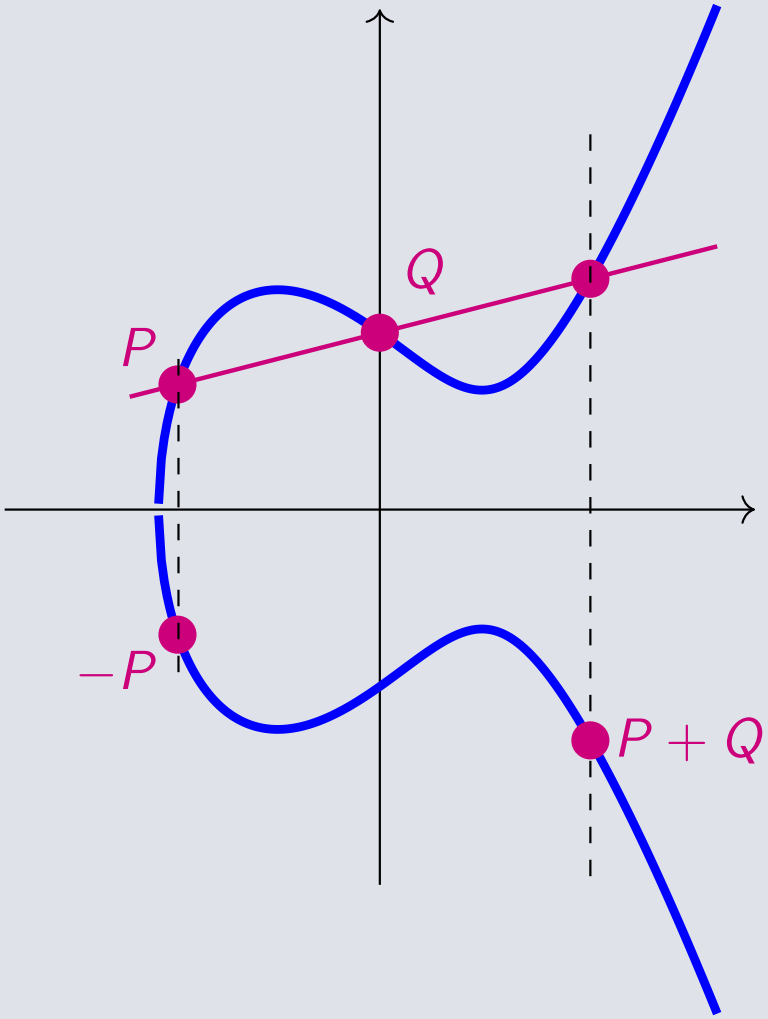
An abelian variety of dimension 1

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



An abelian variety of dimension 1

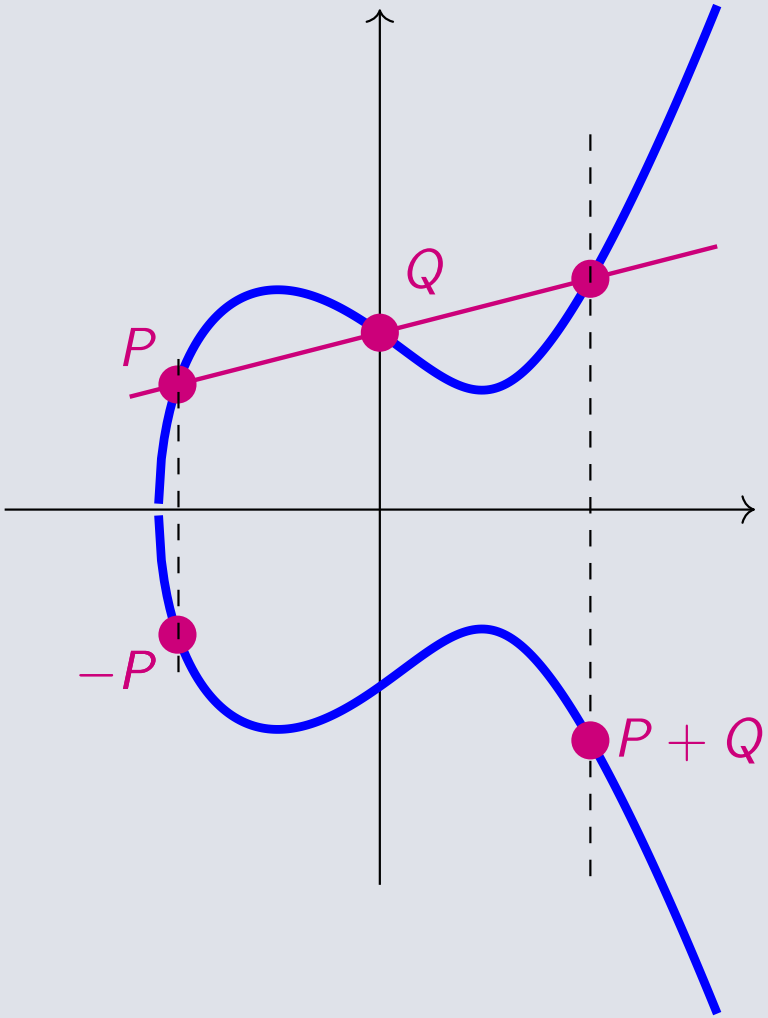
$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



An abelian variety of dimension 1

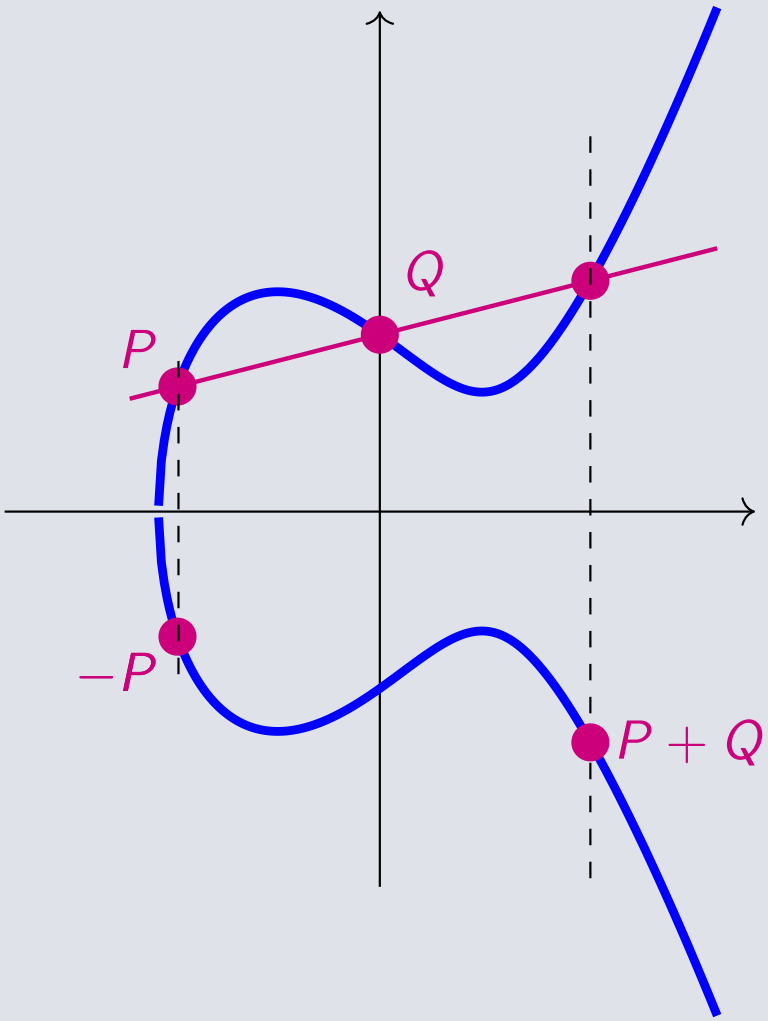
If $P = (x_P, y_P), Q = (x_Q, y_Q)$ with $x_P \neq x_Q$, then

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



An abelian variety of dimension 1

$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$

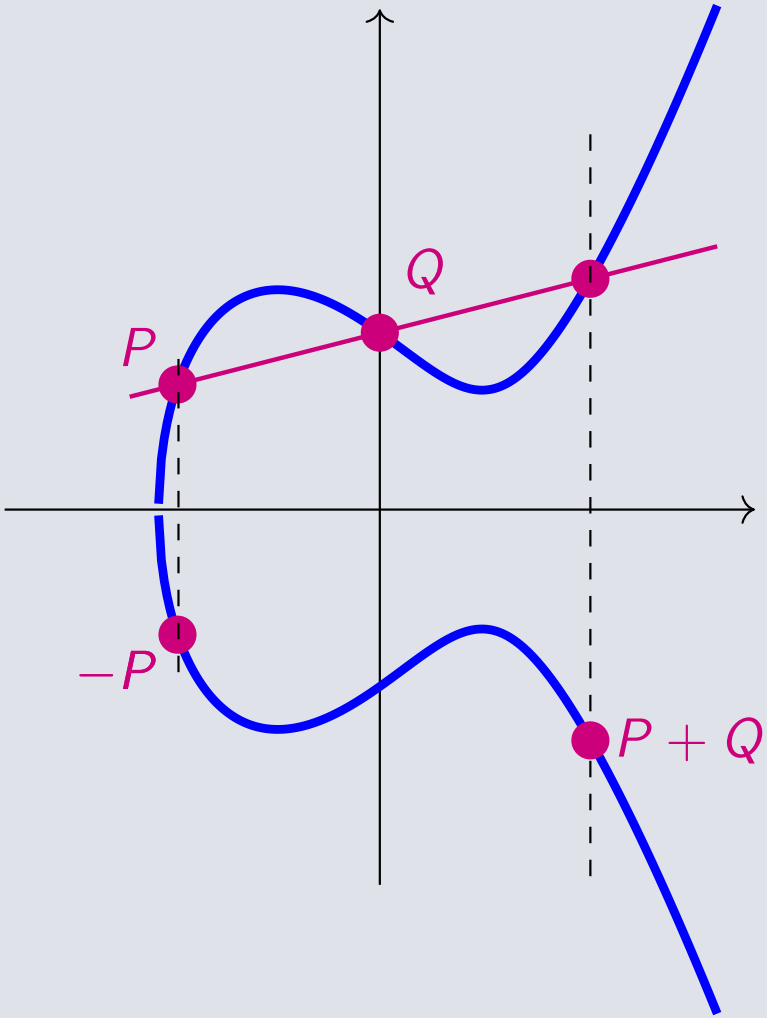


If $P = (x_P, y_P), Q = (x_Q, y_Q)$ with $x_P \neq x_Q$, then

$$-P = (x_P, -y_P)$$

An abelian variety of dimension 1

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



If $P = (x_P, y_P), Q = (x_Q, y_Q)$ with $x_P \neq x_Q$, then

$$-P = (x_P, -y_P)$$

and

$$P + Q = (x_{P+Q}, y_{P+Q})$$

where

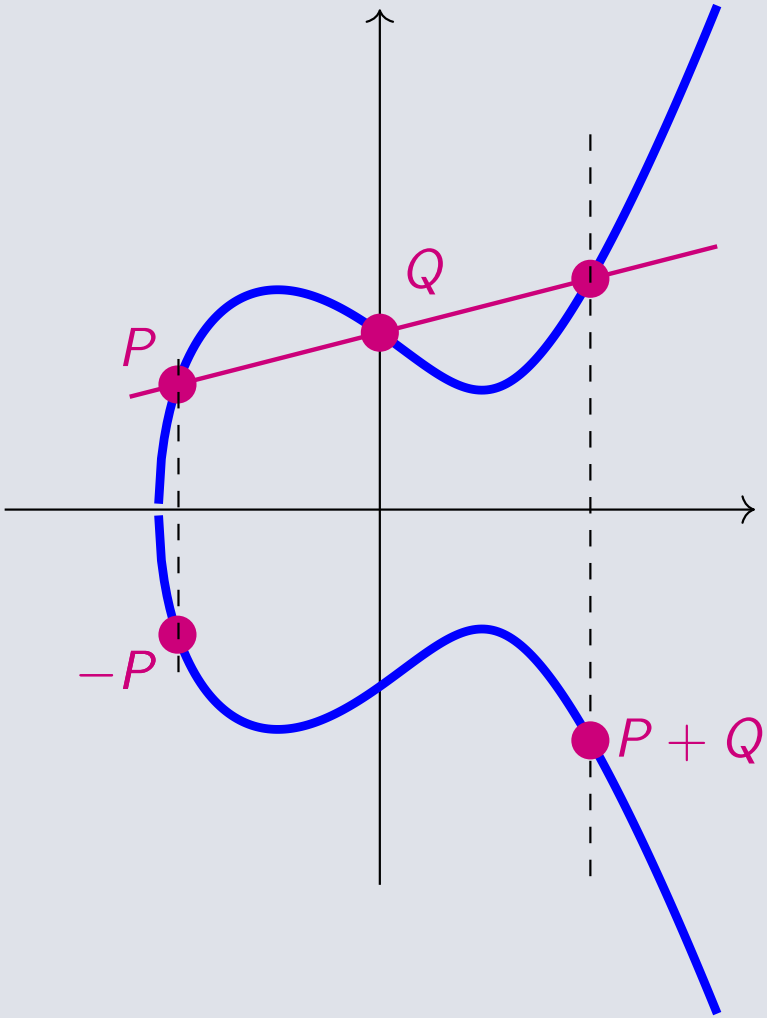
$$\begin{cases} x_{P+Q} = m^2 - x_P - x_Q, \\ y_{P+Q} = m(x_P - x_{P+Q}) - y_P \end{cases}$$

with

$$m = \frac{y_Q - y_P}{x_Q - x_P}.$$

An abelian variety of dimension 1

$$\mathcal{A} : y^2 = x^3 + Ax + B, \quad A, B \in K$$



If $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ with $x_P \neq x_Q$, then

$$-P = (x_P, -y_P)$$

and

$$P + Q = (x_{P+Q}, y_{P+Q})$$

where

$$\begin{cases} x_{P+Q} = m^2 - x_P - x_Q, \\ y_{P+Q} = m(x_P - x_{P+Q}) - y_P \end{cases}$$

with

$$m = \frac{y_Q - y_P}{x_Q - x_P}.$$

Similarly, one can find equations when $x_P = x_Q$.

Elliptic curves, the easiest examples of abelian varieties

$\mathcal{A} : y^2 = x^3 + Ax + B$ is an example of elliptic curve.

Elliptic curves, the easiest examples of abelian varieties

$\mathcal{A} : y^2 = x^3 + Ax + B$ is an example of elliptic curve.

Elliptic curves are abelian varieties of dimension one and all one-dimensional abelian varieties are elliptic curves.

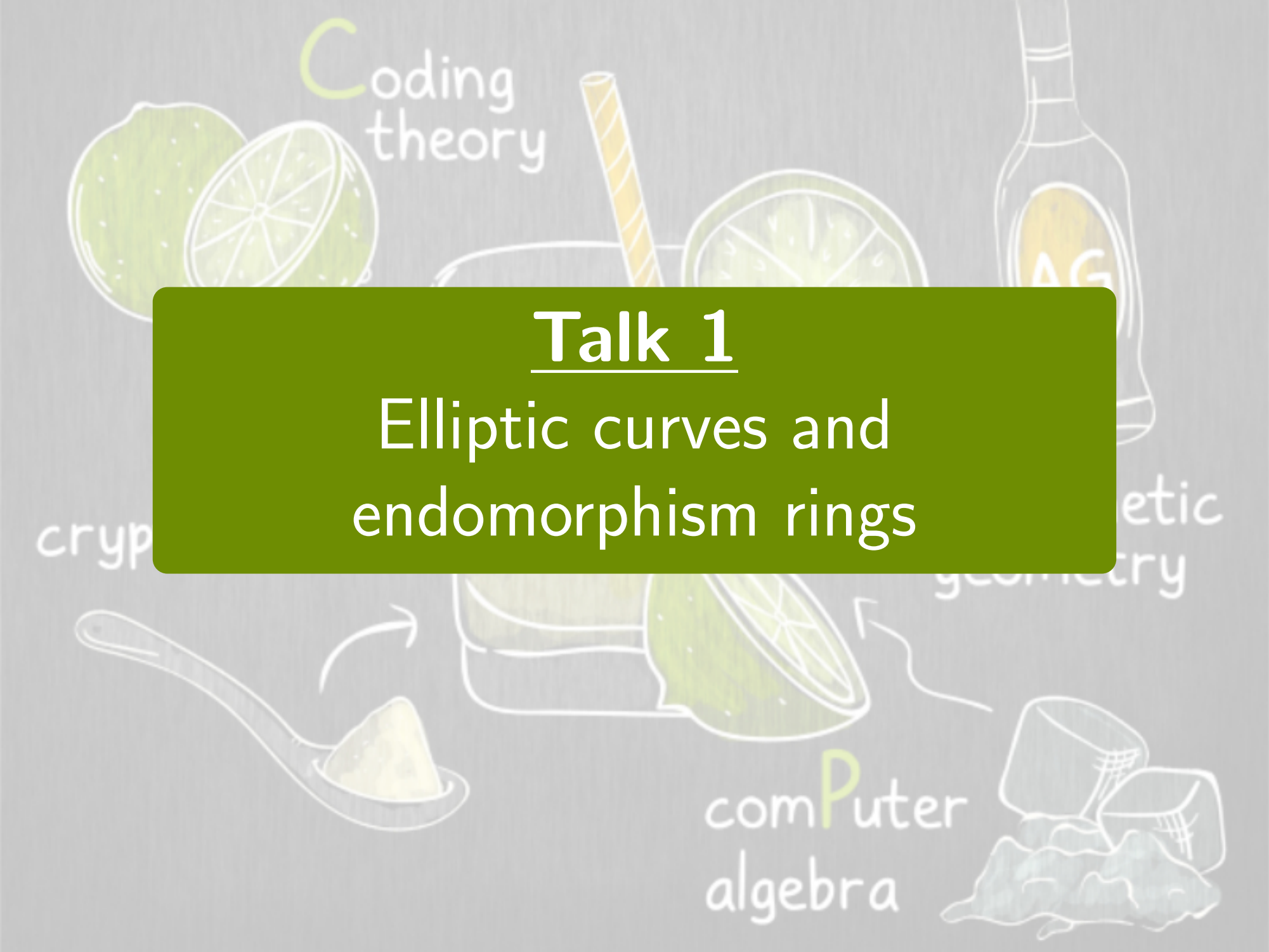
Plan of the day

- **Talk 1: Elliptic curves and endomorphism rings**
  - We will define the endomorphism ring of an elliptic curve defined over an arbitrary field K.
  - We will review the structure of such endomorphism ring when K is a number field or a finite field.
  - For K a finite field, we will go through the references and the historical development of the problem of computing the endomorphism ring and we will explore its connections with cryptography.

- **Elisa's and Stefano's introductory talks.**

- **Talk 2: Computing the endomorphism ring of low-dimensional abelian varieties over finite fields**

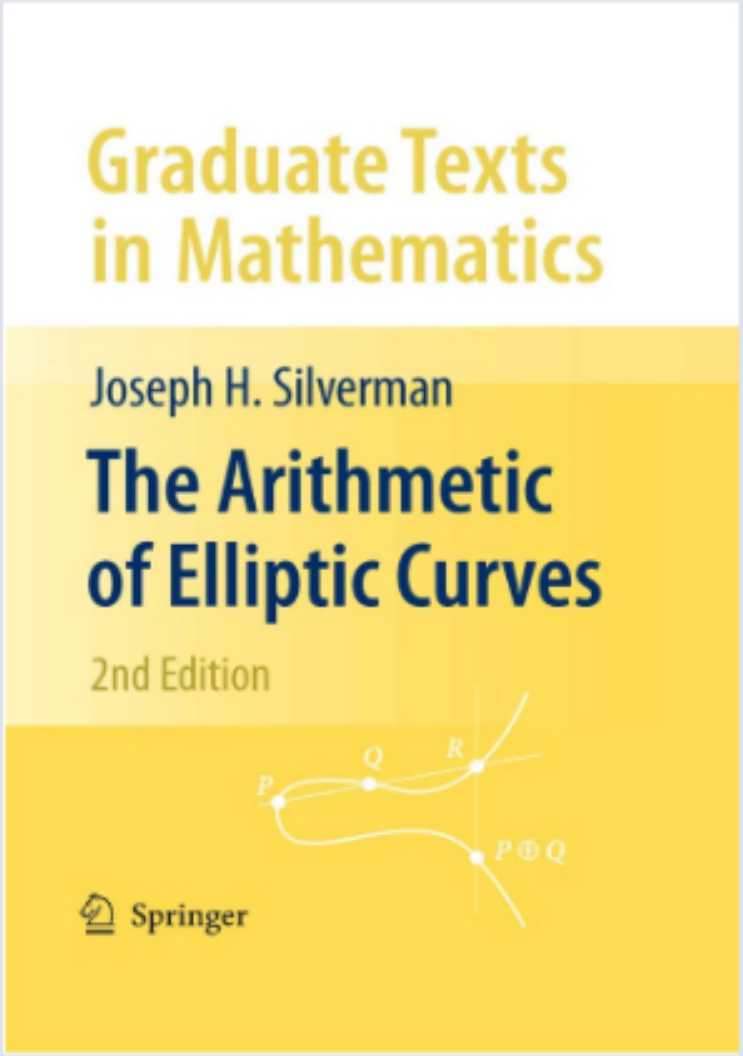
  Now K is a finite field. We will discuss some algorithms for computing the endomorphism ring of elliptic curves and two-dimensional abelian varieties (abelian surfaces).



Talk 1

Elliptic curves and endomorphism rings

SILVERMAN


Graduate Texts
in Mathematics
Joseph H. Silverman
The Arithmetic
of Elliptic Curves
2nd Edition
P
Q
R
P⊕Q
Springer

Andrew Sutherland's course

https://math.mit.edu/classes/18.783/2017/lectures.html

MIT MATHEMATICS **18.783 - Elliptic Curves**

Home | Syllabus | Lectures | Problem Sets | Links

SCHEDULE

#	Date	Topic (references)	Materials
1	2/8	Introduction	slides
2	2/15	The group law, Weierstrass and Edwards equations (Washington 2.1-3, 2.6.3, Bernstein-Lange)	notes, worksheet 1, worksheet 2
3	2/15	Finite fields and integer arithmetic (Modern Computer Algebra Ch. 8)	notes
4	2/21	Finite field arithmetic (Modern Computer Algebra: Sec. 3.2, 9.1, 11.1, HEHCC Ch. 9, Rabin)	notes
5	2/22	Isogenies (Washington 2.9, Silverman III.4)	notes
6	2/27	Isogeny kernels and division polynomials (Washington 3.2, 12.3, Silverman III.4))	notes, worksheet
7	3/1	Endomorphism rings (Washington 4.2, , Silverman III.6)	notes
8	3/6	Hasse's Theorem, point counting (Washington 4.3)	notes
9	3/8	Schoof's algorithm (Washington 4.2, 4.5, Schoof)	notes, worksheet
10	3/13	Generic algorithms for discrete logarithms (Washington 5.2, Pohlig-Hellman, Pollard, Shoup)	notes
11	3/15	Index calculus, smooth numbers, factoring integers (Washington 5.1, 7.1, Granville, Lenstra)	notes, worksheet 1, worksheet 2
12	3/20	Elliptic curve primality proving (ECPP) (Washington 7.2, Goldwasser-Kilian, Pomerance)	notes
13	3/22	Endomorphism algebras (Silverman III.9)	notes
14	4/3	Ordinary and supersingular curves (Silverman III.1,V, Washington 2.7, 4.6)	notes

Elliptic curves

An **elliptic curve** over a field K is a smooth, projective, algebraic curve of genus one defined over K with a distinguished K-rational point O_E.

Elliptic curves

An **elliptic curve** over a field K is a smooth, projective, algebraic curve of genus one defined over K with a distinguished K-rational point O_E.

If $\mathrm{char}(K) \neq 2, 3$, any **elliptic curve** defined over K is isomorphic to an elliptic curve E in short Weierstrass affine form:

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

We take the point at infinity as our distinguished point O_E.

Elliptic curves

An **elliptic curve** over a field K is a smooth, projective, algebraic curve of genus one defined over K with a distinguished K-rational point O_E.

If $\mathrm{char}(K) \neq 2, 3$, any **elliptic curve** defined over K is isomorphic to an elliptic curve E in short Weierstrass affine form:

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

We take the point at infinity as our distinguished point O_E.

The set of points of an elliptic curve has the structure of an abelian group with identity O_E:

$$E(\overline{K}) = \{(x, y) \in \overline{K}^2 : y^2 = x^3 + Ax + B\} \cup \{O_E\}.$$

Elliptic curves

An **elliptic curve** over a field K is a smooth, projective, algebraic curve of genus one defined over K with a distinguished K-rational point O_E.

If $\mathrm{char}(K) \neq 2, 3$, any **elliptic curve** defined over K is isomorphic to an elliptic curve E in short Weierstrass affine form:

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

We take the point at infinity as our distinguished point O_E.

The set of points of an elliptic curve has the structure of an abelian group with identity O_E:

$$E(\overline{K}) = \{(x, y) \in \overline{K}^2 : y^2 = x^3 + Ax + B\} \cup \{O_E\}.$$

The same is true for the set of K-rational points:

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{O_E\}.$$

The j-invariant

For an elliptic curve E given in short Weierstrass form

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

we define the j-invariant as

$$j_E := 1728 \cdot \frac{4A^3}{4A^3 + 27B^2} \in K.$$

The j-invariant

For an elliptic curve E given in short Weierstrass form

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

we define the j-invariant as

$$j_E := 1728 \cdot \frac{4A^3}{4A^3 + 27B^2} \in K.$$

Let E_1, E_2 two elliptic curves defined over K, then

E_1 and E_2 are $\overline{K}$-isomorphic $\Leftrightarrow j_{E_1} = j_{E_2}$

The j-invariant

Every element j_0 in $\overline{K}$ corresponds to the j-invariant of an elliptic curve over $K(j_0)$.

The j-invariant

Every element j_0 in $\overline{K}$ corresponds to the j-invariant of an elliptic curve over $K(j_0)$.

Let $j_0 \in \overline{K}$ then:

- If $j_0 = 0$, then
$$E_0 : y^2 = x^3 + 1;$$
- $j_0 = 1728$, then
$$E_{1728} : y^2 = x^3 + x;$$
- $j_0 \neq 0, 1728$, then
$$E_{j_0} : y^2 = x^3 + 3j_0(1728 - j_0)x + 2j_0(1728 - j_0)^2.$$

An example over finite fields

$E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{101}$

An example over finite fields

$E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{101} \Rightarrow j_E = 5 \in \mathbb{F}_{101}$

An example over finite fields

$E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{101} \Rightarrow j_E = 5 \in \mathbb{F}_{101}$

$E_5 : y^2 = x^3 + 90x + 57$ over $\mathbb{F}_{101}$ has also j-invariant equal to 5.

An example over finite fields

$E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{101} \Rightarrow j_E = 5 \in \mathbb{F}_{101}$

$E_5 : y^2 = x^3 + 90x + 57$ over $\mathbb{F}_{101}$ has also j-invariant equal to 5.

The elliptic curves E and E_5 are **not** isomorphic over $\mathbb{F}_{101}$, but they are isomorphic over $\mathbb{F}_{101^2}$

An example over finite fields

$E : y^2 = x^3 + 3x + 5$ over $\mathbb{F}_{101} \Rightarrow j_E = 5 \in \mathbb{F}_{101}$

$E_5 : y^2 = x^3 + 90x + 57$ over $\mathbb{F}_{101}$ has also j-invariant equal to 5.

The elliptic curves E and E_5 are **not** isomorphic over $\mathbb{F}_{101}$, but they are isomorphic over $\mathbb{F}_{101^2}$ and an isomorphism over $\mathbb{F}_{101^2}$ is given by:

$$\begin{array}{ccc} E & \to & E_5 \\ (x, y) & \mapsto & (-38x, (6\alpha - 12)y), \end{array}$$

where $\mathbb{F}_{101^2} = \mathbb{F}_{101}(\alpha)$.

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ over K (resp. $\overline{K}$) is a non-constant rational map over K (resp. $\overline{K}$) which is also a group homomorphism:

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

$$\varphi(O_{E_1}) = O_{E_2}$$

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ over K (resp. $\overline{K}$) is a non-constant rational map over K (resp. $\overline{K}$) which is also a group homomorphism:

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

$$\varphi(O_{E_1}) = O_{E_2}$$

An isogeny is surjective and has finite kernel.

If E_1 and E_2 are in short Weierstrass form, then φ can be written in standard affine form:

$$\begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x,y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right) \end{array}$$

where $f_1, g_1, f_2, g_2 \in K[x]$ (resp. $\overline{K}[x]$) and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ over K (resp. $\overline{K}$) is a non-constant rational map over K (resp. $\overline{K}$) which is also a group homomorphism:

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

$$\varphi(O_{E_1}) = O_{E_2}$$

An isogeny is surjective and has finite kernel.

If E_1 and E_2 are in short Weierstrass form, then φ can be written in standard affine form:

$$\begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x,y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right) \end{array}$$

where $f_1, g_1, f_2, g_2 \in K[x]$ (resp. $\overline{K}[x]$) and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

The **degree** of φ is $\deg(\varphi) = \max\{\deg(f_1), \deg(g_1)\}$.

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ over K (resp. $\overline{K}$) is a non-constant rational map over K (resp. $\overline{K}$) which is also a group homomorphism:

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

$$\varphi(O_{E_1}) = O_{E_2}$$

An isogeny is surjective and has finite kernel.

If E_1 and E_2 are in short Weierstrass form, then φ can be written in standard affine form:

$$\begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x,y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right) \end{array}$$

where $f_1, g_1, f_2, g_2 \in K[x]$ (resp. $\overline{K}[x]$) and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

The **degree** of φ is $\deg(\varphi) = \max\{\deg(f_1), \deg(g_1)\}$.

The isogeny φ is said to be **separable** if $\left[\frac{f_1(x)}{g_1(x)}\right]' \neq 0$.

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ over K (resp. $\overline{K}$) is a non-constant rational map over K (resp. $\overline{K}$) which is also a group homomorphism:

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

$$\varphi(O_{E_1}) = O_{E_2}$$

An isogeny is surjective and has finite kernel.

If E_1 and E_2 are in short Weierstrass form, then φ can be written in standard affine form:

$$\begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x,y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right) \end{array}$$

where $f_1, g_1, f_2, g_2 \in K[x]$ (resp. $\overline{K}[x]$) and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

The **degree** of φ is $\deg(\varphi) = \max\{\deg(f_1), \deg(g_1)\}$.

The isogeny φ is said to be **separable** if $\left[\frac{f_1(x)}{g_1(x)}\right]' \neq 0$.

If φ is separable, then $\sharp \ker(\varphi) = \deg(\varphi)$.

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

$$\begin{array}{rccc} [2] : & E & \to & E \\ & P & \mapsto & 2P \end{array}$$

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

$$\begin{array}{rccc} [2] : & E & \to & E \\ & P & \mapsto & 2P \\ & (x, y) & \mapsto & \left(\frac{x^4 - 2x^2 + 1}{-3x^3 - 3x}, y \frac{x^6 - 2x^4 + 2x^2 - 1}{x^6 + 2x^4 + x^2} \right) \end{array}$$

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

$$\begin{array}{rccc} [2]: & E & \to & E \\ & P & \mapsto & 2P \\ & (x,y) & \mapsto & \left(\frac{x^4-2x^2+1}{-3x^3-3x}, y\frac{x^6-2x^4+2x^2-1}{x^6+2x^4+x^2}\right) \end{array}$$

We see that:

- $\deg([2]) = 4$.

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

$$\begin{array}{rccc} [2]: & E & \to & E \\ & P & \mapsto & 2P \\ & (x,y) & \mapsto & \left(\frac{x^4-2x^2+1}{-3x^3-3x}, y\frac{x^6-2x^4+2x^2-1}{x^6+2x^4+x^2}\right) \end{array}$$

We see that:

- $\deg([2]) = 4$.
- $[2]$ is separable.

An example

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_7$$

$$\begin{array}{rccc} [2]: & E & \to & E \\ & P & \mapsto & 2P \\ & (x,y) & \mapsto & \left(\frac{x^4-2x^2+1}{-3x^3-3x}, y\frac{x^6-2x^4+2x^2-1}{x^6+2x^4+x^2}\right) \end{array}$$

We see that:

- $\deg([2]) = 4$.
- $[2]$ is separable.
- $\sharp \ker([2]) = \deg([2]) = 4$ and $\ker([2]) = E[2] = \{(0,0), (a,0), (6a,0), O_E\}$, where $a^2 = -1$.

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

$$\begin{array}{rccc} \alpha+\beta: & E & \to & E \\ & P & \mapsto & \alpha(P)+\beta(P) \end{array}$$

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

$$\begin{array}{rccc} \alpha+\beta: & E & \to & E \\ & P & \mapsto & \alpha(P)+\beta(P) \end{array} \qquad \begin{array}{rccc} \alpha\circ\beta: & E & \to & E \\ & P & \mapsto & \alpha(\beta(P)) \end{array}$$

The endomorphism ring

An endomorphism of an elliptic curve E is an isogeny

$$\alpha : E \to E$$

or the zero morphism

$$\begin{array}{rccc} [0]: & E & \to & E \\ & P & \mapsto & O_E. \end{array}$$

We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

$$\begin{array}{rccc} \alpha+\beta: & E & \to & E \\ & P & \mapsto & \alpha(P)+\beta(P) \end{array} \qquad \begin{array}{rccc} \alpha\circ\beta: & E & \to & E \\ & P & \mapsto & \alpha(\beta(P)) \end{array}$$

$(\mathrm{End}(E), +, \circ)$ is a ring, called the (geometric) endomorphism ring.

The multiplication-by-n map

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \to & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

The multiplication-by-n map

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \to & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

Therefore there is an embedding:

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E) \\ n & \mapsto & [n]. \end{array}$$

The multiplication-by-n map

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \to & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

Therefore there is an embedding:

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E) \\ n & \mapsto & [n]. \end{array}$$

and $\mathrm{End}(E)$ has also the structure of a free $\mathbb{Z}$-module.

The dual isogeny

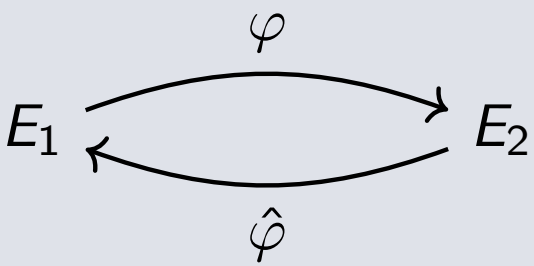
Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves of degree n. The **dual isogeny** is the unique isogeny $\hat{\varphi} : E_2 \to E_1$ for which

$$\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [n].$$

The dual isogeny

Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves of degree n. The **dual isogeny** is the unique isogeny $\hat{\varphi} : E_2 \to E_1$ for which

$$\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [n].$$

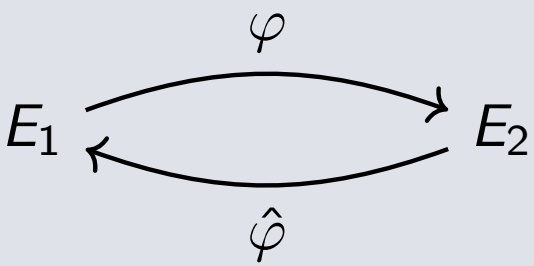


$\hat{\varphi} \circ \varphi = [n]_{E_1}$ and $\varphi \circ \hat{\varphi} = [n]_{E_2}$

The dual isogeny

Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves of degree n. The **dual isogeny** is the unique isogeny $\hat{\varphi} : E_2 \to E_1$ for which

$$\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [n].$$



$$\hat{\varphi} \circ \varphi = [n]_{E_1} \text{ and } \varphi \circ \hat{\varphi} = [n]_{E_2}$$

Clearly:

- $\deg(\hat{\varphi}) = \deg(\varphi)$;
- $\hat{\hat{\varphi}} = \varphi$.

Endomorphisms as algebraic integers

Let us consider the involution

$$\begin{array}{ccc} \mathrm{End(E)} & \to & \mathrm{End(E)} \\ \alpha & \mapsto & \hat{\alpha}. \end{array}$$

Endomorphisms as algebraic integers

Let us consider the involution

$$\begin{array}{ccc} \mathrm{End}(E) & \to & \mathrm{End}(E) \\ \alpha & \mapsto & \hat{\alpha}. \end{array}$$

We define

- the **reduced norm** of α:

$$\mathrm{Nrd}(\alpha) = \alpha \circ \hat{\alpha} = [\deg(\alpha)] \in \mathbb{Z};$$

Endomorphisms as algebraic integers

Let us consider the involution

$$\begin{array}{ccc} \mathrm{End}(E) & \to & \mathrm{End}(E) \\ \alpha & \mapsto & \hat{\alpha}. \end{array}$$

We define

- the **reduced norm** of α:

$$\mathrm{Nrd}(\alpha) = \alpha \circ \hat{\alpha} = [\deg(\alpha)] \in \mathbb{Z};$$

- the **reduced trace** of α:

$$\mathrm{Trd}(\alpha) = \alpha + \hat{\alpha} \in \mathbb{Z}.$$

Endomorphisms as algebraic integers

Let us consider the involution

$$\begin{array}{ccc} \mathrm{End}(E) & \to & \mathrm{End}(E) \\ \alpha & \mapsto & \hat{\alpha}. \end{array}$$

We define

- the **reduced norm** of α:

$$\mathrm{Nrd}(\alpha) = \alpha \circ \hat{\alpha} = [\deg(\alpha)] \in \mathbb{Z};$$

- the **reduced trace** of α:

$$\mathrm{Trd}(\alpha) = \alpha + \hat{\alpha} \in \mathbb{Z}.$$

Therefore $\alpha, \hat{\alpha}$ can be interpreted as algebraic integers, since they are roots of the unitary polynomial

$$(x - \alpha)(x - \hat{\alpha}) = x^2 - \mathrm{Trd}(\alpha)\, x + \mathrm{Nrd}(\alpha) \in \mathbb{Z}[x].$$

The endomoprhism algebra

The **endomorphism algebra** of an elliptic curve E is the algebra over $\mathbb{Q}$ defined by

$$\mathsf{End}^0(E) := \mathsf{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Therefore $\mathsf{End}^0(E) := \{r\alpha : r \in \mathbb{Q} \text{ and } \alpha \in \mathsf{End}(E)\}$.

The endomoprhism algebra

The **endomorphism algebra** of an elliptic curve E is the algebra over $\mathbb{Q}$ defined by

$$\mathsf{End}^0(E) := \mathsf{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Therefore $\mathsf{End}^0(E) := \{r\alpha : r \in \mathbb{Q} \text{ and } \alpha \in \mathsf{End}(E)\}$.

Setting $\widehat{r\alpha} = r\hat{\alpha}$, we can extend the notions of reduced norm and trace to $\mathsf{End}^0(E)$. So for every $\gamma \in \mathsf{End}^0(E)$ we have:

- reduced norm: $\mathsf{Nrd}(\gamma) = \gamma \circ \hat{\gamma} \in \mathbb{Q}$;
- reduced trace $\mathsf{Trd}(\gamma) = \gamma + \hat{\gamma} \in \mathbb{Q}$.

The endomoprhism algebra

The **endomorphism algebra** of an elliptic curve E is the algebra over $\mathbb{Q}$ defined by

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Therefore $\mathrm{End}^0(E) := \{r\alpha : r \in \mathbb{Q} \text{ and } \alpha \in \mathrm{End}(E)\}$.

Setting $\widehat{r\alpha} = r\hat{\alpha}$, we can extend the notions of reduced norm and trace to $\mathrm{End}^0(E)$. So for every $\gamma \in \mathrm{End}^0(E)$ we have:

- reduced norm: $\mathrm{Nrd}(\gamma) = \gamma \circ \hat{\gamma} \in \mathbb{Q}$;
- reduced trace $\mathrm{Trd}(\gamma) = \gamma + \hat{\gamma} \in \mathbb{Q}$.

Then γ and $\hat{\gamma}$ are roots of the quadratic polynomial

$$(x - \gamma)(x - \hat{\gamma}) = x^2 - \mathrm{Trd}(\gamma)\, x + \mathrm{Nrd}(\gamma) \in \mathbb{Q}[x].$$

In particular, if $\gamma \notin \mathbb{Q}$, $\mathbb{Q}[\gamma]$ is a quadratic extension of $\mathbb{Q}$.

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

The endomorphism ring lies inside $\mathrm{End}^0(E)$ as a free $\mathbb{Z}$-module of rank $r = \dim_{\mathbb{Q}} \mathrm{End}^0(E)$ containing $\mathbb{Z}$.

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

The endomorphism ring lies inside $\mathrm{End}^0(E)$ as a free $\mathbb{Z}$-module of rank $r = \dim_{\mathbb{Q}} \mathrm{End}^0(E)$ containing $\mathbb{Z}$. Therefore:

- If $r = 1$, then $\mathrm{End}(E) = \mathbb{Z}$,

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

The endomorphism ring lies inside $\mathrm{End}^0(E)$ as a free $\mathbb{Z}$-module of rank $r = \dim_{\mathbb{Q}} \mathrm{End}^0(E)$ containing $\mathbb{Z}$. Therefore:

- If $r = 1$, then $\mathrm{End}(E) = \mathbb{Z}$,
- If $r = 2$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha \subseteq \mathbb{Q}(\sqrt{D})$,

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

The endomorphism ring lies inside $\mathrm{End}^0(E)$ as a free $\mathbb{Z}$-module of rank $r = \dim_{\mathbb{Q}} \mathrm{End}^0(E)$ containing $\mathbb{Z}$. Therefore:

- If $r = 1$, then $\mathrm{End}(E) = \mathbb{Z}$,
- If $r = 2$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha \subseteq \mathbb{Q}(\sqrt{D})$,
- If $r = 4$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma \subseteq B$.

Structure of the endomorphism algebra

Let E be an elliptic curve defined over a field K. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- $\mathbb{Q}$;
- an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with $D < 0$;
- a quaternion algebra over $\mathbb{Q}$, i.e. a $\mathbb{Q}$-algebra B that has a $\mathbb{Q}$-basis of $\{1, i, j, ij\}$ such that $i^2, j^2 \in \mathbb{Q} \setminus \{0\}$ and $ij = -ji$.

The endomorphism ring lies inside $\mathrm{End}^0(E)$ as a free $\mathbb{Z}$-module of rank $r = \dim_{\mathbb{Q}} \mathrm{End}^0(E)$ containing $\mathbb{Z}$. Therefore:

- If $r = 1$, then $\mathrm{End}(E) = \mathbb{Z}$,
- If $r = 2$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha \subseteq \mathbb{Q}(\sqrt{D})$,
- If $r = 4$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma \subseteq B$.

If $\mathrm{End}(E) \neq \mathbb{Z}$, we say that E has complex moltiplication (CM).

When K is a number field

Let E be an elliptic curve defined over a **number field**. Then:

- either $\mathrm{End}^0(E) \simeq \mathbb{Q}$ and in this case $\mathrm{End}(E) \simeq \mathbb{Z}$;
- or $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$ with $D < 0$ and in this case $\mathrm{End}(E)$ is isomoprhic to an order in $\mathbb{Q}(\sqrt{D})$.

When K is a number field

Let E be an elliptic curve defined over a **number field**. Then:

- either $\mathrm{End}^0(E) \simeq \mathbb{Q}$ and in this case $\mathrm{End}(E) \simeq \mathbb{Z}$;
- or $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$ with $D < 0$ and in this case $\mathrm{End}(E)$ is isomoprhic to an order in $\mathbb{Q}(\sqrt{D})$.

In most of the cases $\mathrm{End}(E) \simeq \mathbb{Z}$, so when K is a number field, complex multiplication is the exception.

From now on K will be a finite field of characteristic p:

$$K = \mathbb{F}_q,$$

with q a power of a prime number p.

Ordinary and supersingular elliptic curves

Let E be an elliptic curves defined over $\mathbb{F}_q$, with $q = p^r$.
The p-torsion subgroup of E is

$$E[p] := \{Q \in E(\overline{\mathbb{F}}_q) : pQ = O_E\}.$$

Ordinary and supersingular elliptic curves

Let E be an elliptic curves defined over $\mathbb{F}_q$, with $q = p^r$.
The p-torsion subgroup of E is

$$E[p] := \{Q \in E(\overline{\mathbb{F}}_q) : pQ = O_E\}.$$

There are two possibilities:

- $E[p] \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} \Leftrightarrow E$ is ordinary

Ordinary and supersingular elliptic curves

Let E be an elliptic curves defined over $\mathbb{F}_q$, with $q = p^r$.
The p-torsion subgroup of E is

$$E[p] := \{Q \in E(\overline{\mathbb{F}}_q) : pQ = O_E\}.$$

There are two possibilities:

- $E[p] \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} \Leftrightarrow E$ is ordinary
- $E[p] \simeq \{O_E\} \Leftrightarrow E$ is supersingular

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

Indeed π_E is a root of the characteristic polynomial:

$$x^2 - \mathrm{tr}(\pi_E)x + q \in \mathbb{Z}[x].$$

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x,y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

Indeed π_E is a root of the characteristic polynomial:

$$x^2 - \mathrm{tr}(\pi_E)x + q \in \mathbb{Z}[x].$$

So $\pi_E \in \mathbb{Z} \Leftrightarrow \mathrm{tr}(\pi_E)^2 = 4q$.

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x,y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

Indeed π_E is a root of the characteristic polynomial:

$$x^2 - \mathrm{tr}(\pi_E)x + q \in \mathbb{Z}[x].$$

So $\pi_E \in \mathbb{Z} \Leftrightarrow \mathrm{tr}(\pi_E)^2 = 4q$. This implies that E is supersingular and q is a square.

The Frobenius endomorphism

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x,y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

Indeed π_E is a root of the characteristic polynomial:

$$x^2 - \mathrm{tr}(\pi_E)x + q \in \mathbb{Z}[x].$$

So $\pi_E \in \mathbb{Z} \Leftrightarrow \mathrm{tr}(\pi_E)^2 = 4q$. This implies that E is supersingular and q is a square.

In particular, if E is ordinary, then $\mathbb{Z} \subsetneq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$.

Elliptic curves over finite fields have always complex multiplication

Let E be an elliptic curve defined over a finite field of characteristic p.

Elliptic curves over finite fields have always complex multiplication

Let E be an elliptic curve defined over a finite field of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

Elliptic curves over finite fields have always complex multiplication

Let E be an elliptic curve defined over a finite field of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

- If E is supersingular then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and in this case $\mathrm{End}(E)$ is a maximal order inside it.

Elliptic curves over finite fields have always complex multiplication

Let E be an elliptic curve defined over a finite field of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

- If E is supersingular then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and in this case $\mathrm{End}(E)$ is a maximal order inside it.

In any case $\mathrm{End}(E) \neq \mathbb{Z}$, so E has complex multiplication.

Elliptic curves over finite fields have always complex multiplication

Let E be an elliptic curve defined over a finite field of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

- If E is supersingular then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and in this case $\mathrm{End}(E)$ is a maximal order inside it.

In any case $\mathrm{End}(E) \neq \mathbb{Z}$, so E has complex multiplication.

Over finite fields:
E is ordinary $\Leftrightarrow$ $\mathrm{End}(E)$ is commutative
E is supersingular $\Leftrightarrow$ $\mathrm{End}(E)$ is non-commutative

Example

Let $p \equiv 3 \pmod 4$. Let us consider the supersingular elliptic curve

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_p.$$

Example

Let $p \equiv 3 \pmod 4$. Let us consider the supersingular elliptic curve

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_p.$$

Recall

$$\mathrm{End}^0(E) \simeq B_{p,\infty}.$$

Example

Let $p \equiv 3 \pmod 4$. Let us consider the supersingular elliptic curve

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_p.$$

Recall

$$\mathrm{End}^0(E) \simeq B_{p,\infty}.$$

(Pizer): If $p \equiv 3 \pmod 4$

$$B_{p,\infty} = \left(\frac{-1, -p}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

with $i^2 = -1, j^2 = -p$ and $ij = -ji$.

Example

Let $p \equiv 3 \pmod 4$. Let us consider the supersingular elliptic curve

$$E : y^2 = x^3 + x \text{ over } \mathbb{F}_p.$$

Recall

$$\mathrm{End}^0(E) \simeq B_{p,\infty}.$$

(Pizer): If $p \equiv 3 \pmod 4$

$$B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

with $i^2 = -1, j^2 = -p$ and $ij = -ji$.

We exibith an isomorphism between $\mathrm{End}^0(E)$ and $\left(\frac{-1,-p}{\mathbb{Q}}\right)$.

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x, y) & \mapsto & (-x, \sqrt{-1}y), \end{array}$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x, y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x, y) & \mapsto & (x^p, y^p). \end{array}$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x, y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x, y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 :$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x,y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 : (x,y) \stackrel{\varphi}{\to} (-x, \sqrt{-1}y)$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x,y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 : (x,y) \stackrel{\varphi}{\to} (-x, \sqrt{-1}y) \stackrel{\varphi}{\to} (x,-y)$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x,y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 : (x,y) \stackrel{\varphi}{\to} (-x, \sqrt{-1}y) \stackrel{\varphi}{\to} (x,-y) \Rightarrow \varphi^2 = [-1],$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x,y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 : (x,y) \stackrel{\varphi}{\to} (-x, \sqrt{-1}y) \stackrel{\varphi}{\to} (x,-y) \Rightarrow \varphi^2 = [-1],$$

$$\pi^2 = [-p], \text{ since } \operatorname{tr}(\pi) = 0.$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

Let us consider the following two endomorphisms of E:

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x,y) & \mapsto & (-x, \sqrt{-1}y), \end{array} \qquad \begin{array}{rccc} \pi : & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

We have:

$$\varphi^2 : (x,y) \xrightarrow{\varphi} (-x, \sqrt{-1}y) \xrightarrow{\varphi} (x,-y) \Rightarrow \varphi^2 = [-1],$$

$$\pi^2 = [-p], \text{ since } \operatorname{tr}(\pi) = 0.$$

Moreover:

$$\pi \circ \varphi = [-1] \circ \varphi \circ \pi.$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

So we obtain

$$\begin{array}{ccc} \mathrm{End}^0(E) & \xrightarrow{\simeq} & B_{p,\infty} \\ \varphi & \mapsto & i \\ \pi & \mapsto & j. \end{array}$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

So we obtain

$$\begin{array}{ccc} \mathrm{End}^0(E) & \xrightarrow{\simeq} & B_{p,\infty} \\ \varphi & \mapsto & i \\ \pi & \mapsto & j. \end{array}$$

We also obtained $\mathbb{Z} + \mathbb{Z}\varphi + \mathbb{Z}\pi + \mathbb{Z}\varphi\pi \subseteq \mathrm{End}(E)$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

So we obtain

$$\begin{array}{ccc} \mathrm{End}^0(E) & \xrightarrow{\simeq} & B_{p,\infty} \\ \varphi & \mapsto & i \\ \pi & \mapsto & j. \end{array}$$

We also obtained $\mathbb{Z} + \mathbb{Z}\varphi + \mathbb{Z}\pi + \mathbb{Z}\varphi\pi \subseteq \mathrm{End}(E)$ and one can show that

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\pi + \mathbb{Z}\left(\frac{\varphi - \pi}{2}\right) + \mathbb{Z}\left(\frac{1 + \varphi\pi}{2}\right),$$

Example

$$E/\mathbb{F}_p : y^2 = x^3 + x, \qquad p \equiv 3 \pmod 4$$

So we obtain

$$\begin{array}{ccc} \mathrm{End}^0(E) & \xrightarrow{\simeq} & B_{p,\infty} \\ \varphi & \mapsto & i \\ \pi & \mapsto & j. \end{array}$$

We also obtained $\mathbb{Z} + \mathbb{Z}\varphi + \mathbb{Z}\pi + \mathbb{Z}\varphi\pi \subseteq \mathrm{End}(E)$ and one can show that

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\pi + \mathbb{Z}\left(\frac{\varphi - \pi}{2}\right) + \mathbb{Z}\left(\frac{1 + \varphi\pi}{2}\right),$$

i.e. $\left\{1, \pi, \frac{\varphi-\pi}{2}, \frac{1+\varphi\pi}{2}\right\}$ is a $\mathbb{Z}$-basis of $\mathrm{End}(E)$.

The endormorphism ring problem for elliptic curves

Endomorphism ring problem

Given an elliptic curve defined over a finite field, compute all its endomorphisms.

The endormorphism ring problem for elliptic curves

Endomorphism ring problem

Given an elliptic curve defined over a finite field, compute all its endomorphisms.

Two variants of this problem:

The endormorphism ring problem for elliptic curves

Endomorphism ring problem

Given an elliptic curve defined over a finite field, compute all its endomorphisms.

Two variants of this problem:

- Given an elliptic curve E defined over a finite field, find an explicit set of endomorphisms (in an efficient representation) that generate E as a $\mathbb{Z}$-module.

The endormorphism ring problem for elliptic curves

Endomorphism ring problem

Given an elliptic curve defined over a finite field, compute all its endomorphisms.

Two variants of this problem:

- Given an elliptic curve E defined over a finite field, find an explicit set of endomorphisms (in an efficient representation) that generate E as a $\mathbb{Z}$-module.
- Given an elliptic curve E defined over a finite field, find an "abstract ring" $\mathcal{O}$ isomorphic to $\mathrm{End}(E)$.

A not so chronological historical overview of this problem

The beginning of the story

1996 - D. Kohel

Endomorphism rings of elliptic curves over finite fields.
PhD thesis, University of California, Berkeley.

▶ First to deal with the problem of computing the endomorphism ring of elliptic curves over finite fields, both in the ordinary and supersingular case. Both algorithms have exponential complexity.

Ordinary elliptic curves

2011 - G. Bisson and A.V. Sutherland

Computing the endomorphism ring of an ordinary elliptic curve over a finite field.

J. Number Theory 113, 815–831.

▶ Two algorithms that, under suitable heuristic assumptions, have subexponential complexity.

2022 - D. Robert

Some applications of higher dimensional isogenies to elliptic curves (overview of results).

▶ A deterministic polynomial time algorithm to compute the endomorphism ring, provided that we are given the factorisation of the discriminant of the Frobenius. In particular, the full endomorphism ring computation can be done in quantum polynomial time.

The advent of isogeny-based cryptography

Isogeny-based cryptography deals with any cryptosystem based on some variants of the following problem:

Isogeny problem

Given two isogenous elliptic curves E_1 and E_2 defined over a finite field, find an isogeny

$$\varphi : E_1 \to E_2.$$

The advent of isogeny-based cryptography

Isogeny-based cryptography deals with any cryptosystem based on some variants of the following problem:

Isogeny problem

Given two isogenous elliptic curves E_1 and E_2 defined over a finite field, find an isogeny

$$\varphi : E_1 \to E_2.$$

1997 - J.-M. Couveignes

Hard Homogeneous Spaces.

Unpublished note.

▶ First to bring the isogeny problem into cryptography, using ordinary elliptic curves.

Supersingular curves appear into isogeny-based cryptography

2009 - D. X. Charles, K. E. Lauter and E. Z. Goren
Cryptographic Hash Functions from Expander Graphs.
Journal of Cryptology 22, 93–113.

▶ Present a cryptographic hash function whose preimage resistance relies on the hardness of computing isogenies of degree a power of a small prime between supersingular elliptic curves.

Supersingular curves appear into isogeny-based cryptography

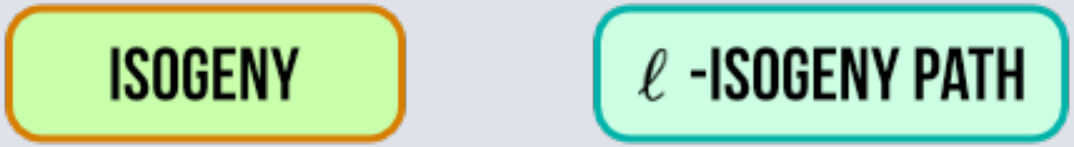
2009 - D. X. Charles, K. E. Lauter and E. Z. Goren
Cryptographic Hash Functions from Expander Graphs.
Journal of Cryptology 22, 93–113.

▶ Present a cryptographic hash function whose preimage resistance relies on the hardness of computing isogenies of degree a power of a small prime between supersingular elliptic curves.

Several other cryptosystems based on the problem of computing isogenies between supersingular elliptic curves would later follow. Among them:

- **SIDH** (2011) - Broken;
- **CSIDH** (2018);
- **SQISign** (2020).

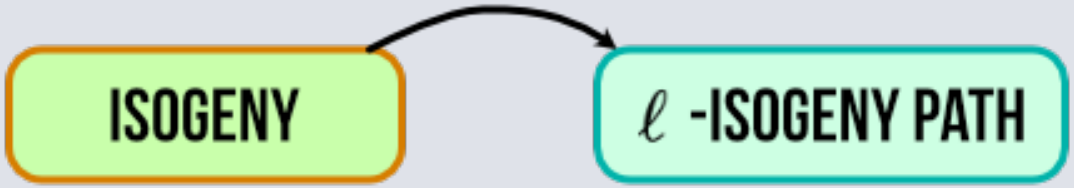
Supersingular isogeny problems



ISOGENY: Given two supersingular elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

ℓ-ISOGENY PATH: Given two supersingular elliptic curves E_1 and E_2 and a prime number ℓ, find an isogeny $\varphi : E_1 \to E_2$ of degree a power of ℓ.

Supersingular isogeny problems



ISOGENY: Given two supersingular elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

ℓ-ISOGENY PATH: Given two supersingular elliptic curves E_1 and E_2 and a prime number ℓ, find an isogeny $\varphi : E_1 \to E_2$ of degree a power of ℓ.

Deuring's correspondence

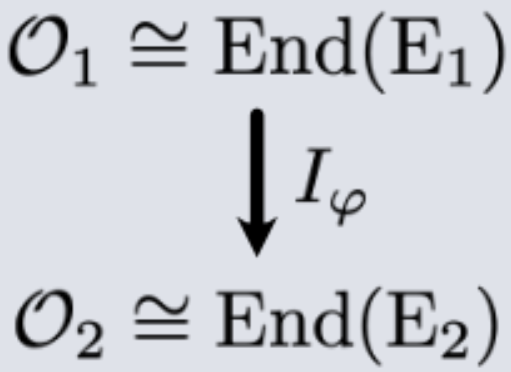
Deuring's correspondence

$\mathcal{O}_1 \cong \mathrm{End}(\mathrm{E}_1)$

$\mathcal{O}_2 \cong \mathrm{End}(\mathrm{E}_2)$

Elliptic curves	**Quaternion algebras**
$E/\overline{\mathbb{F}}_p$ supersingular elliptic curves up to Galois conjugacy	$\mathcal{O} \cong \mathrm{End}(E)$ maximal orders in $B_{p,\infty}$ up to isomorphism

Deuring's correspondence



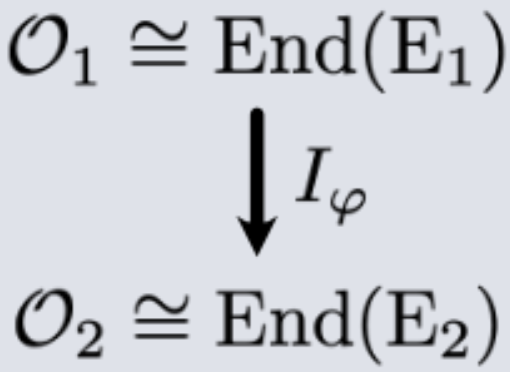
Elliptic curves	**Quaternion algebras**
$E/\overline{\mathbb{F}}_p$ supersingular elliptic curves up to Galois conjugacy	$\mathcal{O} \cong \mathrm{End}(E)$ maximal orders in $B_{p,\infty}$ up to isomorphism
$\varphi : E \to E'$ isogeny of $\deg(\varphi) = n$	$I_\varphi = \mathrm{Hom}(\mathrm{E}_2, \mathrm{E}_1)\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal of norm n

The quaternion ℓ-isogeny path problem

2014 - D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol
On the quaternion ℓ-isogeny path problem.
LMS Journal of Computation and Mathematics, 17:418–432

▶ A probabilistic algorithm to solve the quaternion version of the supersingular ℓ-isogeny path problem, i.e. given a maximal quaternion order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ determine a ℓ-power norm left $\mathcal{O}$-ideal in the class of a given left $\mathcal{O}$-ideal I. Conditional on heuristics on expected distributions of primes, it runs in expected polynomial time.

Connections with the supersingular endomorphism ring problem

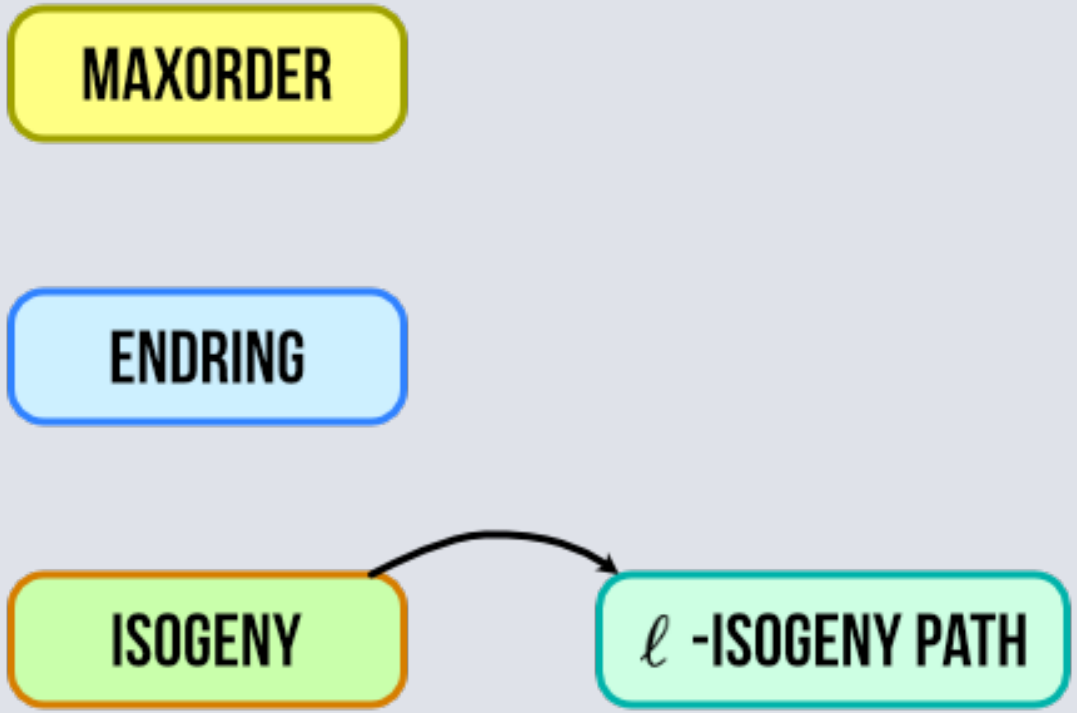


Connections with the supersingular endomorphism ring problem

Connections with the supersingular endomorphism ring problem

2018 - K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit
Supersingular isogeny graphs and endomorphism rings: Reductions and solutions.
Advances in Cryptology – EUROCRYPT 2018, pages 329–368, Cham, 2018.

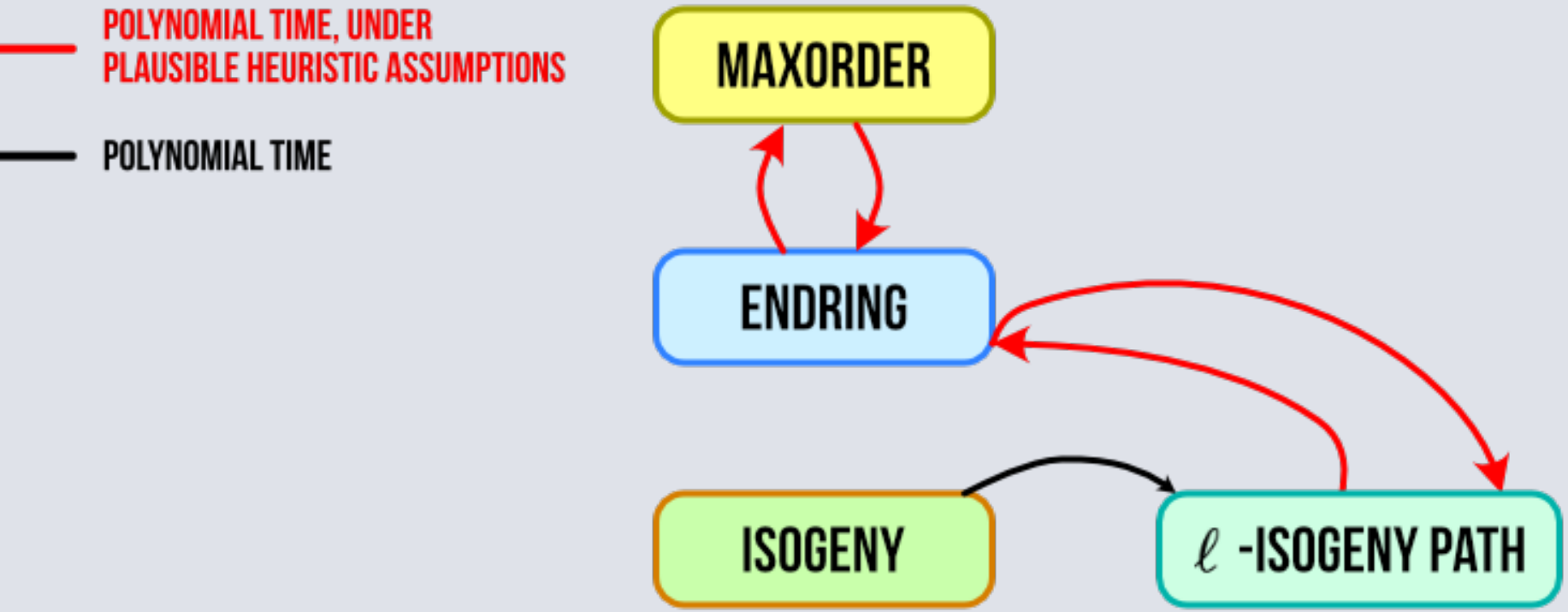
Interconnected supersingular computational problems



ENDRING: Given a supersingular elliptic curve E, compute a $\mathbb{Z}$-basis of the endomorphism ring $\mathrm{End}(E)$.

MAXORDER: Given a supersingular elliptic curve E, find an abstract representation of its endomorphism ring, that is find a maximal order $\mathcal{O}$ in a quaternion algebra $B_{p,\infty}$ isomorphism to $\mathrm{End}(E)$.

Interconnected supersingular computational problems



ENDRING: Given a supersingular elliptic curve E, compute a $\mathbb{Z}$-basis of the endomorphism ring $\mathrm{End}(E)$.

MAXORDER: Given a supersingular elliptic curve E, find an abstract representation of its endomorphism ring, that is find a maximal order $\mathcal{O}$ in a quaternion algebra $B_{p,\infty}$ isomorphism to $\mathrm{End}(E)$.

Computing supersingular endomorphism rings

2020 - K. Eisentraeger, S. Hallgren, C. Leonardi, T. Morrison and J. Park

Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs

ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium, volume 4 of Open Book Ser., pages 215–232. Math. Sci. Publ., Berkeley, CA

2025 - J. Fuselier, A. I., M. Kozek, T. Morrison and C. Namoijam

Computing supersingular endomorphism rings using inseparable endomorphisms

Journal of Algebra, Volume 668, pp 145–189

We'll come back to this later!

Removing heuristics

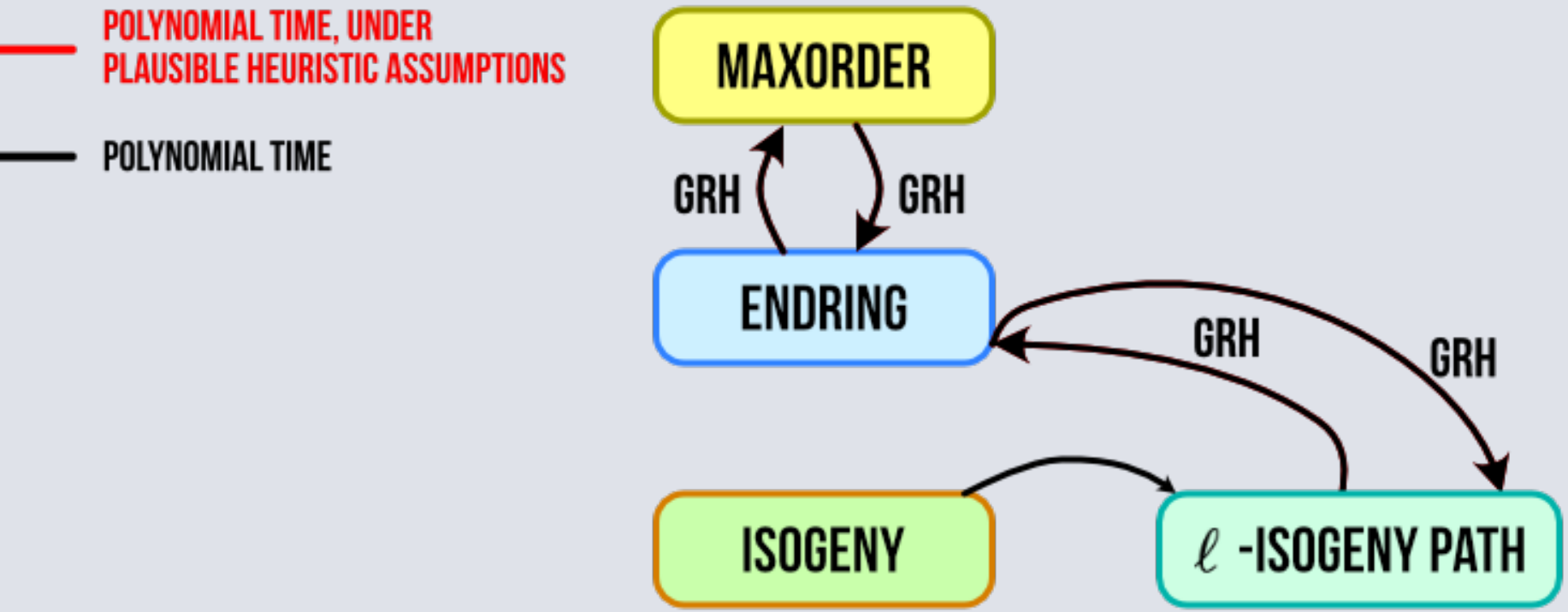
2022 - B. Wesolowski

The supersingular isogeny path and endomorphism ring problems are equivalent

2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)

▶ Proves that the ℓ-isogeny path, EndRing and MaxOrder are equivalent under reductions of polynomial expected time, assuming only the generalised Riemann hypothesis (GRH).

Interconnected supersingular computational problems



Why GRH?

The **generalized Riemann hypothesis (GRH)** asserts that the nontrivial zeros of all Dirichlet L-functions lie on the line $\mathrm{Re}(s) = 1/2$ in the complex plane.

Why GRH?

The **generalized Riemann hypothesis (GRH)** asserts that the nontrivial zeros of all Dirichlet L-functions lie on the line $\mathrm{Re}(s) = 1/2$ in the complex plane.

Actually GRH is never used in this original form, but rather through some of its proven consequences. For instance:

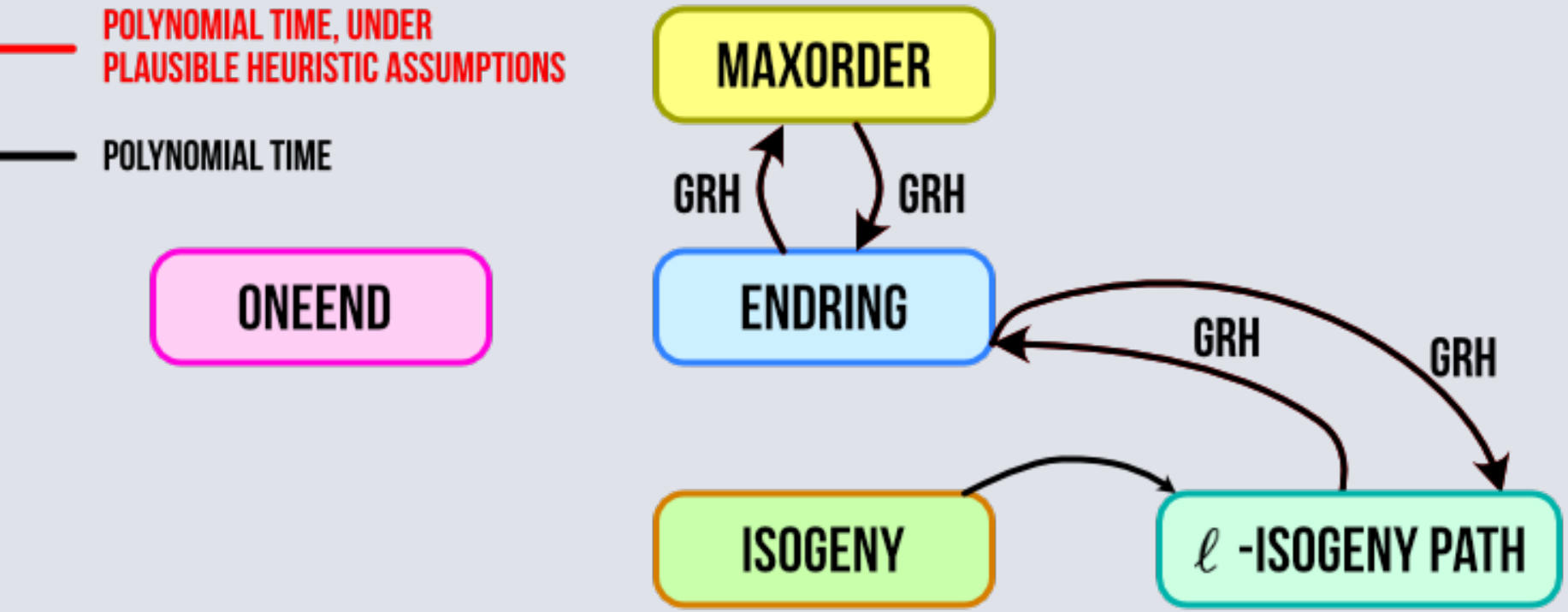
- GRH guarantees the existence of special integral elements of small norm $q = \mathcal{O}((\log p)^2)$ in a certain quaternion algebra.
- GRH gives explicit upper bounds on the class number of an imaginary quadratic field.
- GRH appears in other technical results that rely on primes to behave in various expected ways.

One Endomorphism Problem

2024 - A. Page and B. Wesolowski
The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent
Advances in Cryptology – EUROCRYPT 2024

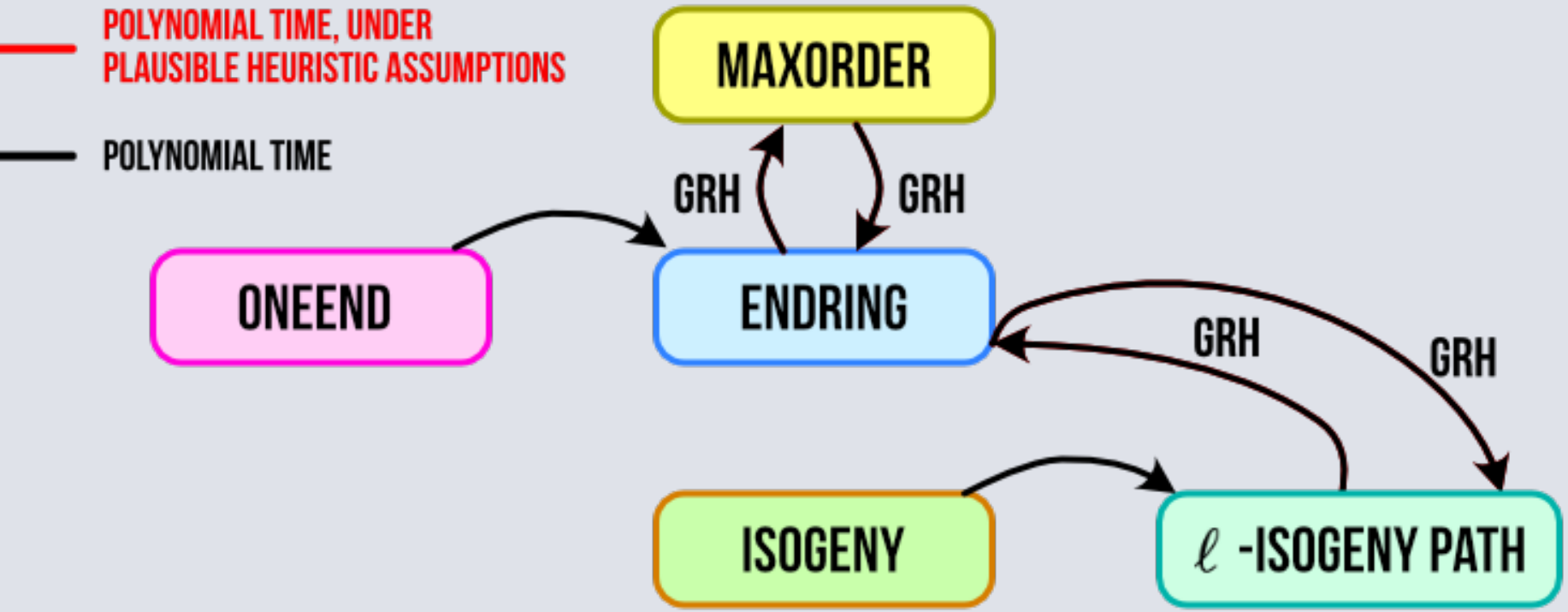
▶ They introduce the One Endomorphism problem, i.e. the problem of computing only a single non-scalar endomorphism of a supersingular elliptic curve, and prove that it is equivalent to the Supersingular Endomorphism Ring, under probabilistic polynomial time reductions. Moreover they prove the existence of an unconditional probabilistic algorithm to solve the endomorphism ring problem in time $\tilde{\mathcal{O}}(\sqrt{p})$.

Interconnected supersingular computational problems



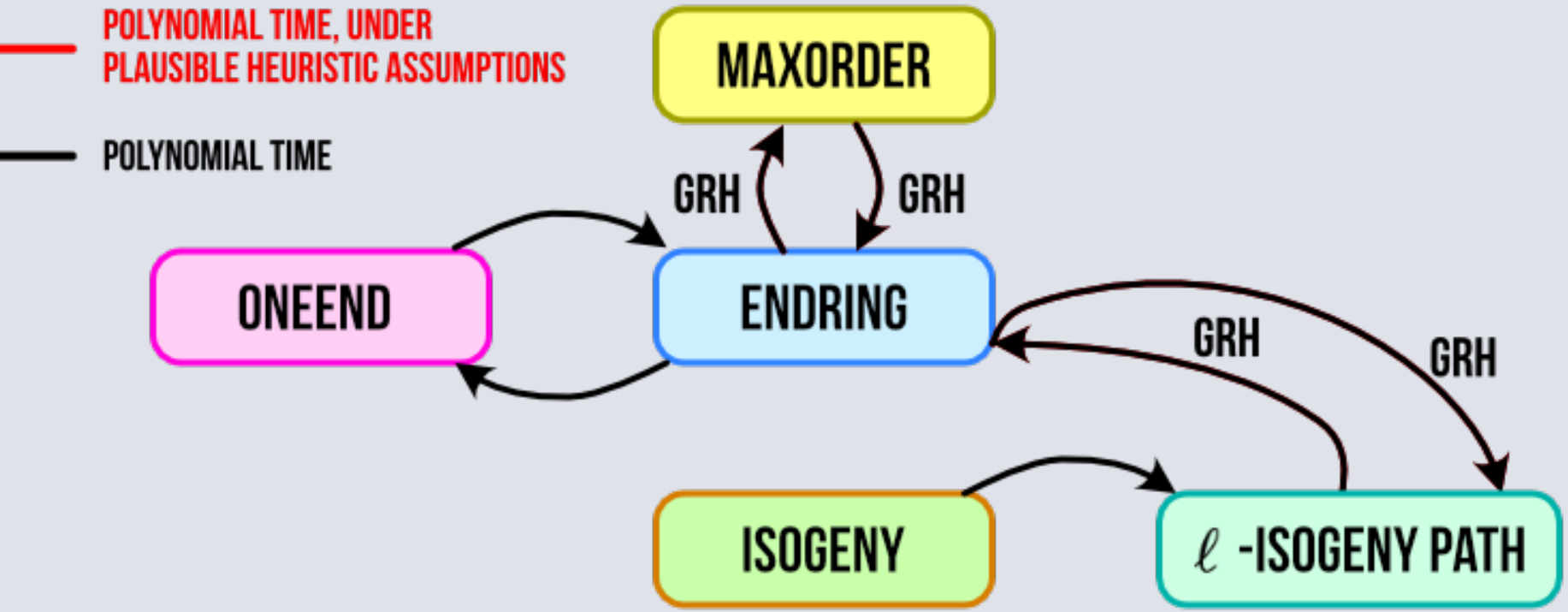
ONEEND: Given a supersingular elliptic curve E, find an endomorphism that is not a scalar multiplication, i.e. find an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.

Interconnected supersingular computational problems



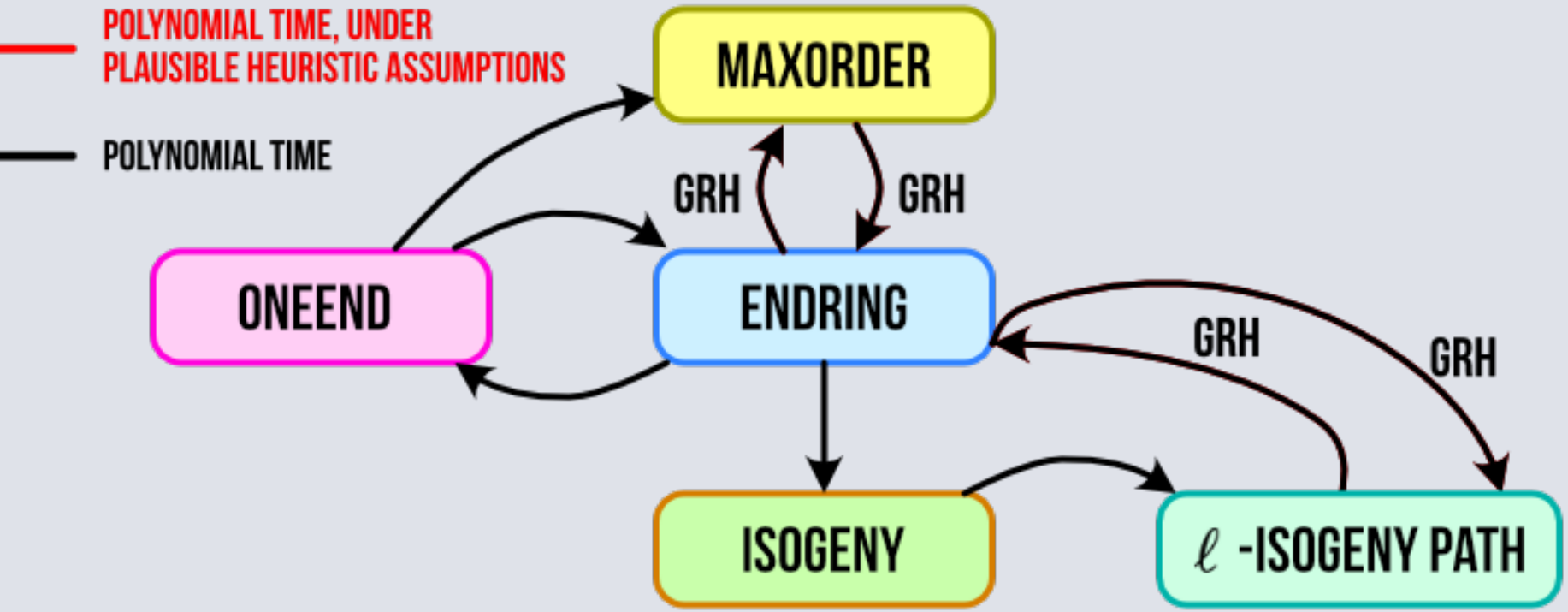
ONEEND: Given a supersingular elliptic curve E, find an endomorphism that is not a scalar multiplication, i.e. find an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.

Interconnected supersingular computational problems



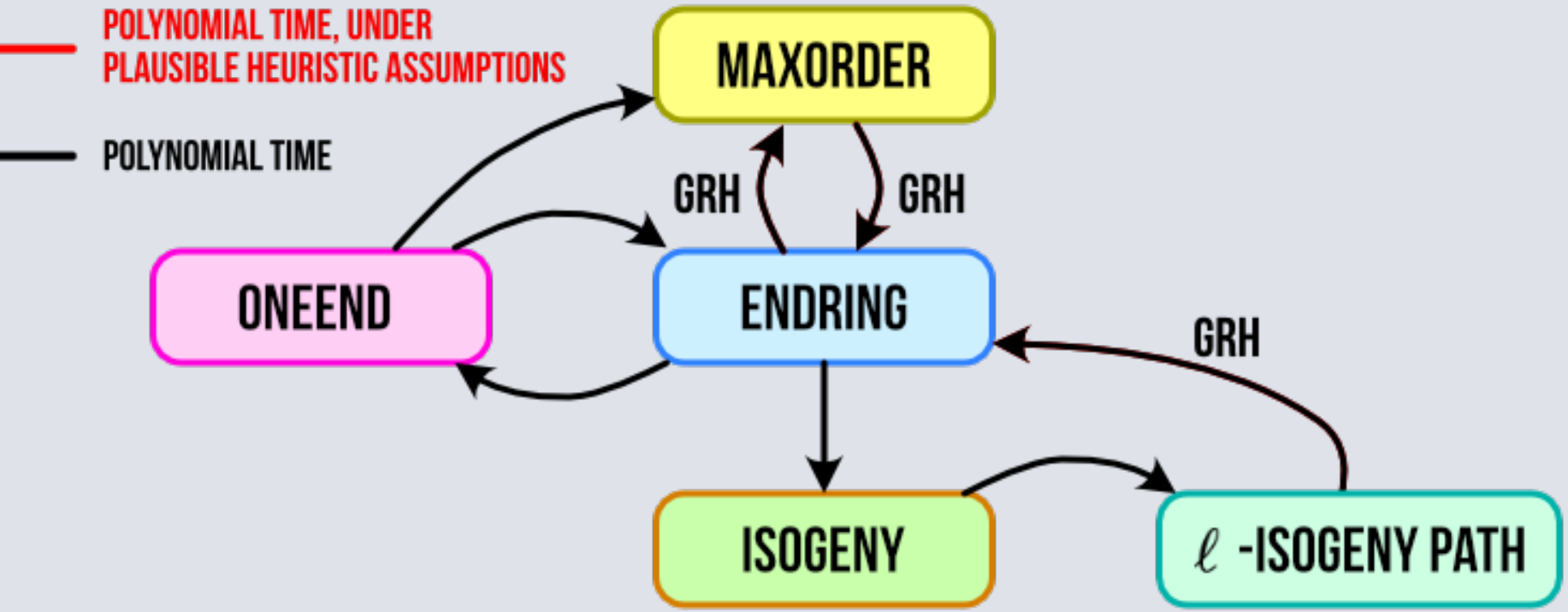
ONEEND: Given a supersingular elliptic curve E, find an endomorphism that is not a scalar multiplication, i.e. find an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.

Interconnected supersingular computational problems



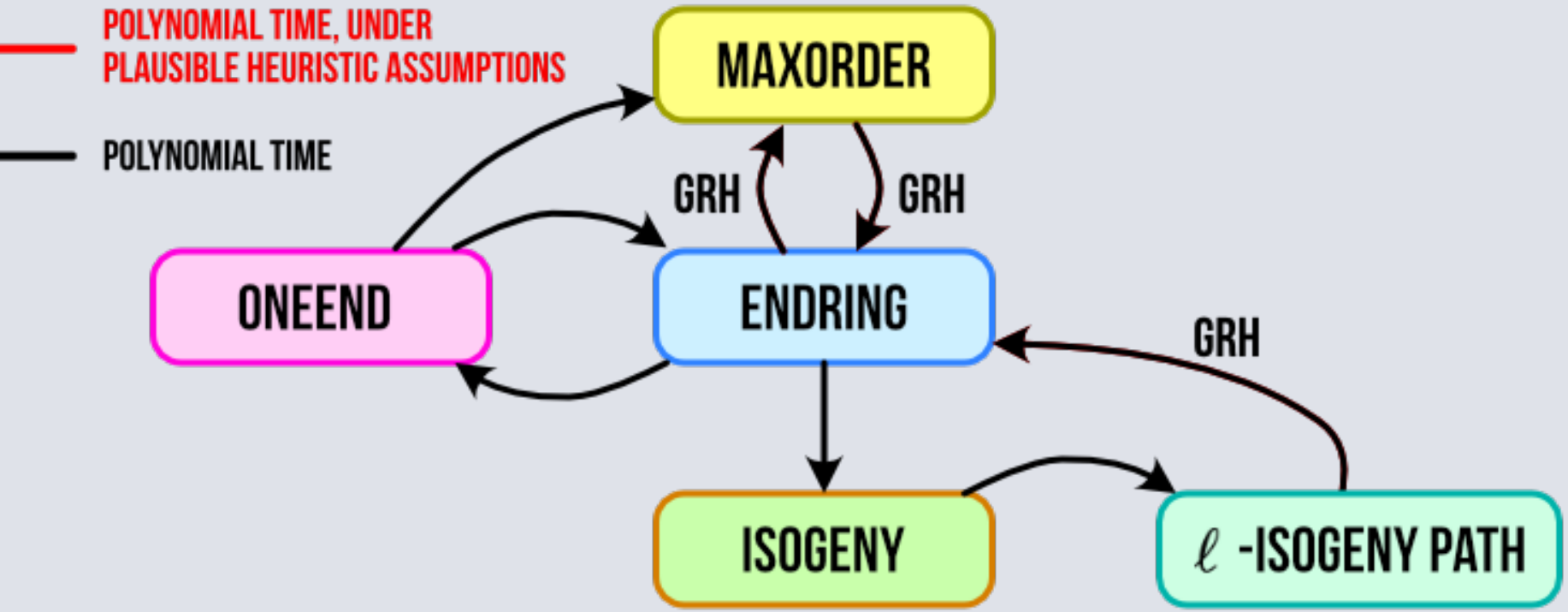
ONEEND: Given a supersingular elliptic curve E, find an endomorphism that is not a scalar multiplication, i.e. find an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.

Interconnected supersingular computational problems



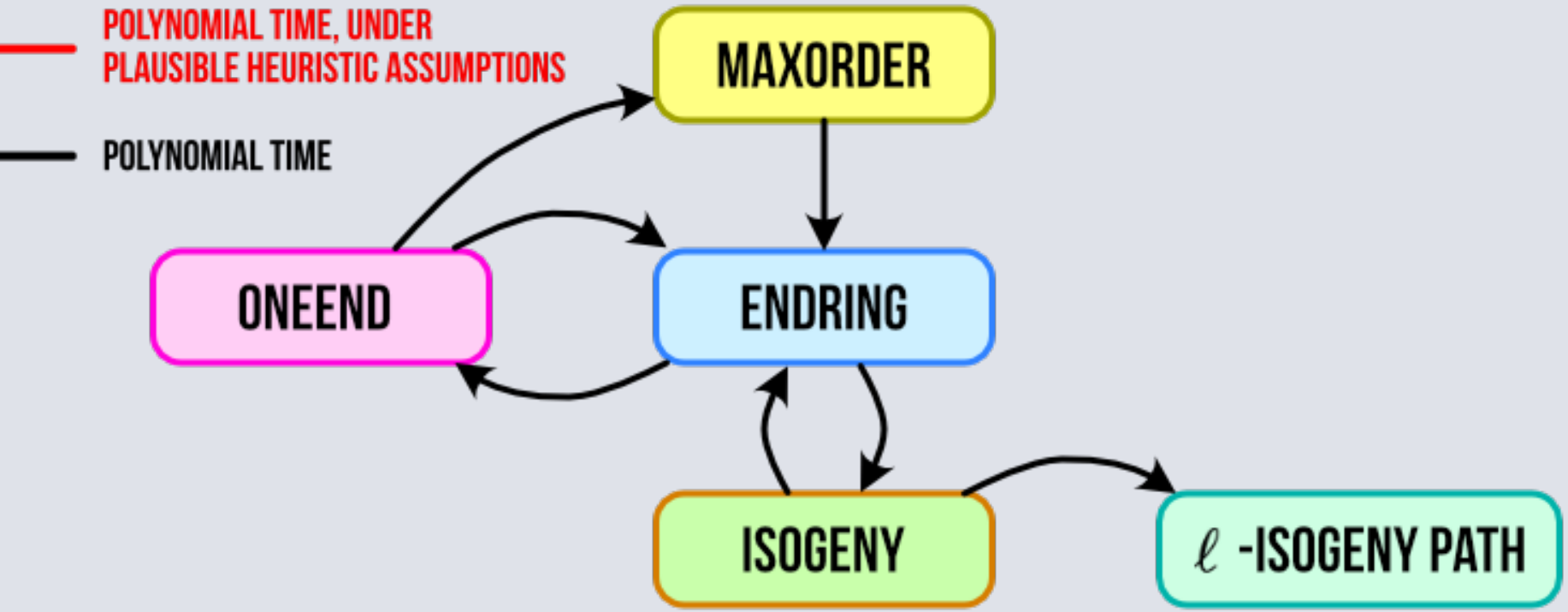
ONEEND: Given a supersingular elliptic curve E, find an endomorphism that is not a scalar multiplication, i.e. find an element of $\mathrm{End}(E) \setminus \mathbb{Z}$.

Interconnected supersingular computational problems



2025 - A. H. Le Merdy and B. Wesolowski
Unconditional foundations for supersingular isogeny-based cryptography
Preprint

Interconnected supersingular computational problems



2025 - A. H. Le Merdy and B. Wesolowski
Unconditional foundations for supersingular isogeny-based cryptography
Preprint

Take home-message

Given the applications in isogeny-based cryptography, current research on endomorphism rings of elliptic curves over finite fields is primarily focused on supersingular elliptic curves.
In my opinion, we can identify **three main research directions**:

Take home-message

Given the applications in isogeny-based cryptography, current research on endomorphism rings of elliptic curves over finite fields is primarily focused on supersingular elliptic curves.
In my opinion, we can identify **three main research directions**:

1) Developing more efficient algorithms to compute the endomorphism ring of a supersingular elliptic curve.

Take home-message

Given the applications in isogeny-based cryptography, current research on endomorphism rings of elliptic curves over finite fields is primarily focused on supersingular elliptic curves.
In my opinion, we can identify **three main research directions**:

1) Developing more efficient algorithms to compute the endomorphism ring of a supersingular elliptic curve.

2) Investigating reductions of computational problems related to the isogeny problem.

Take home-message

Given the applications in isogeny-based cryptography, current research on endomorphism rings of elliptic curves over finite fields is primarily focused on supersingular elliptic curves.
In my opinion, we can identify **three main research directions**:

1) Developing more efficient algorithms to compute the endomorphism ring of a supersingular elliptic curve.

2) Investigating reductions of computational problems related to the isogeny problem.

3) Designing methods for randomly sampling supersingular elliptic curves without leaking information about their endomorphism rings.

Take home-message

Given the applications in isogeny-based cryptography, current research on endomorphism rings of elliptic curves over finite fields is primarily focused on supersingular elliptic curves.
In my opinion, we can identify **three main research directions**:

1) Developing more efficient algorithms to compute the endomorphism ring of a supersingular elliptic curve.

2) Investigating reductions of computational problems related to the isogeny problem.

3) Designing methods for randomly sampling supersingular elliptic curves without leaking information about their endomorphism rings.

In the second part, we will delve deeper into the first research direction.

Talk 2

Computing the endomorphism ring of low-dimensional abelian varieties over finite fields

Annamaria Iezzi

Université Grenoble Alpes

CAIPI : *Endomorphisms and invariants of some abelian varieties*

Nancy - April 7, 2025

Recall from talk 1

Let E be an elliptic curve defined over a **finite field** of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

- If E is supersingular then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and in this case $\mathrm{End}(E)$ is a maximal order inside it.

Recall from talk 1

Let E be an elliptic curve defined over a **finite field** of characteristic p.

- If E is ordinary then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

  where $\mathcal{O}_L$ is the integer ring of L.

- If E is supersingular then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and in this case $\mathrm{End}(E)$ is a maximal order inside it.

Differently from quaternion algebras, number fields contains a unique maximal order, the ring of integers.

Ordinary endomorphism rings

Let $\mathcal{O}$ be an order in a quadratic field L of discriminant D_L. Then $\mathcal{O}$ has finite index in $\mathcal{O}_L$, and if $u = [\mathcal{O}_L : \mathcal{O}]$ is the conductor of $\mathcal{O}$, then

$$\mathcal{O} = \mathbb{Z} + u\mathcal{O}_L.$$

Ordinary endomorphism rings

Let $\mathcal{O}$ be an order in a quadratic field L of discriminant D_L. Then $\mathcal{O}$ has finite index in $\mathcal{O}_L$, and if $u = [\mathcal{O}_L : \mathcal{O}]$ is the conductor of $\mathcal{O}$, then

$$\mathcal{O} = \mathbb{Z} + u\mathcal{O}_L.$$

So, computing $\mathrm{End}(E)$ boils down to computing the conductor $u = [\mathcal{O}_L : \mathrm{End}(E)]$.

Ordinary endomorphism rings

Let $\mathcal{O}$ be an order in a quadratic field L of discriminant D_L. Then $\mathcal{O}$ has finite index in $\mathcal{O}_L$, and if $u = [\mathcal{O}_L : \mathcal{O}]$ is the conductor of $\mathcal{O}$, then

$$\mathcal{O} = \mathbb{Z} + u\mathcal{O}_L.$$

So, computing $\mathrm{End}(E)$ boils down to computing the conductor $u = [\mathcal{O}_L : \mathrm{End}(E)]$.

Moreover, since $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L$, then u divides $v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]]$. So there are only a finite set of possibilities for $\mathrm{End}(E)$.

Ordinary endomorphism rings

Recall

$$\mathbb{Z}[\pi_E] \subseteq \mathsf{End}(E) \subseteq \mathcal{O}_L,$$

$$u = [\mathcal{O}_L : \mathsf{End}(E)], \qquad v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]] \qquad \text{and} \qquad u \mid v.$$

Ordinary endomorphism rings

Recall

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

$$u = [\mathcal{O}_L : \mathrm{End}(E)], \qquad v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]] \qquad \text{and} \qquad u \mid v.$$

2011 - G. Bisson and A.V. Sutherland

Computing the endomorphism ring of an ordinary elliptic curve over a finite field.

J. Number Theory 113, 815–831.

Ordinary endomorphism rings

Recall

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

$$u = [\mathcal{O}_L : \mathrm{End}(E)], \qquad v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]] \qquad \text{and} \qquad u \mid v.$$

2011 - G. Bisson and A.V. Sutherland
Computing the endomorphism ring of an ordinary elliptic curve over a finite field.
J. Number Theory 113, 815–831.

For every prime p dividing v, Bisson and Sutherland determine the largest prime power p^k dividing u.

Ordinary endomorphism rings

Recall

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

$$u = [\mathcal{O}_L : \mathrm{End}(E)], \qquad v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]] \qquad \text{and} \qquad u \mid v.$$

2011 - G. Bisson and A.V. Sutherland
Computing the endomorphism ring of an ordinary elliptic curve over a finite field.
J. Number Theory 113, 815–831.

For every prime p dividing v, Bisson and Sutherland determine the largest prime power p^k dividing u. This is done:

- by isogeny climbing (Kohel's thesis) for small primes;
- by counting the number of relations holding in certain ideal class groups, for larger primes.

Ordinary endomorphism rings

Recall

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_L,$$

$$u = [\mathcal{O}_L : \mathrm{End}(E)], \qquad v = [\mathcal{O}_L : \mathbb{Z}[\pi_E]] \qquad \text{and} \qquad u \mid v.$$

2011 - G. Bisson and A.V. Sutherland
Computing the endomorphism ring of an ordinary elliptic curve over a finite field.
J. Number Theory 113, 815–831.

For every prime p dividing v, Bisson and Sutherland determine the largest prime power p^k dividing u. This is done:

- by isogeny climbing (Kohel's thesis) for small primes;
- by counting the number of relations holding in certain ideal class groups, for larger primes.

Under heuristic assumptions (including, but not limited to, the GRH), they achieve subexponential running times

Supersingular endomorphism rings

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

Supersingular endomorphism rings

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, then

$$\mathrm{End}(E) \simeq \mathcal{O},$$

where $\mathcal{O}$ is a maximal order in the quaternion algebra $B_{p,\infty}$.

Supersingular endomorphism rings

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, then

$$\mathrm{End}(E) \simeq \mathcal{O},$$

where $\mathcal{O}$ is a maximal order in the quaternion algebra $B_{p,\infty}$.

In particular it is a $\mathbb{Z}$-lattice of rank 4 containing $\mathbb{Z}$, so we have

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma,$$

where $\alpha, \beta, \gamma \in \mathrm{End}(E)$ are non trivial endomorphisms.

The Supersingular Endomorphism Ring problem

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ compute $\mathrm{End}(E)$.

Two approaches:

The Supersingular Endomorphism Ring problem

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ compute $\mathrm{End}(E)$.

Two approaches:

- Compute endomorphisms of E until finding a generating set of $\mathrm{End}(E)$.

The Supersingular Endomorphism Ring problem

Fact

Let $q = p^n$. If $E/\mathbb{F}_q$ is supersingular then $E \simeq E'/\mathbb{F}_{p^2}$ and $j_E \in \mathbb{F}_{p^2}$.

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ compute $\mathrm{End}(E)$.

Two approaches:

- Compute endomorphisms of E until finding a generating set of $\mathrm{End}(E)$.
- Compute a suborder $\Lambda \subseteq \mathrm{End}(E)$ with specific properties and recover $\mathrm{End}(E)$ from Λ.

?

How to find non-trivial endomorphisms of E?

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

  $\left\{ \text{ supersingular elliptic curves over } \mathbb{F}_{p^2}, \text{ up to isomorphism } \right\}$

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

$$\left\{ \text{ supersingular elliptic curves over } \mathbb{F}_{p^2}, \text{ up to isomorphism } \right\}$$

$$\updownarrow$$

$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

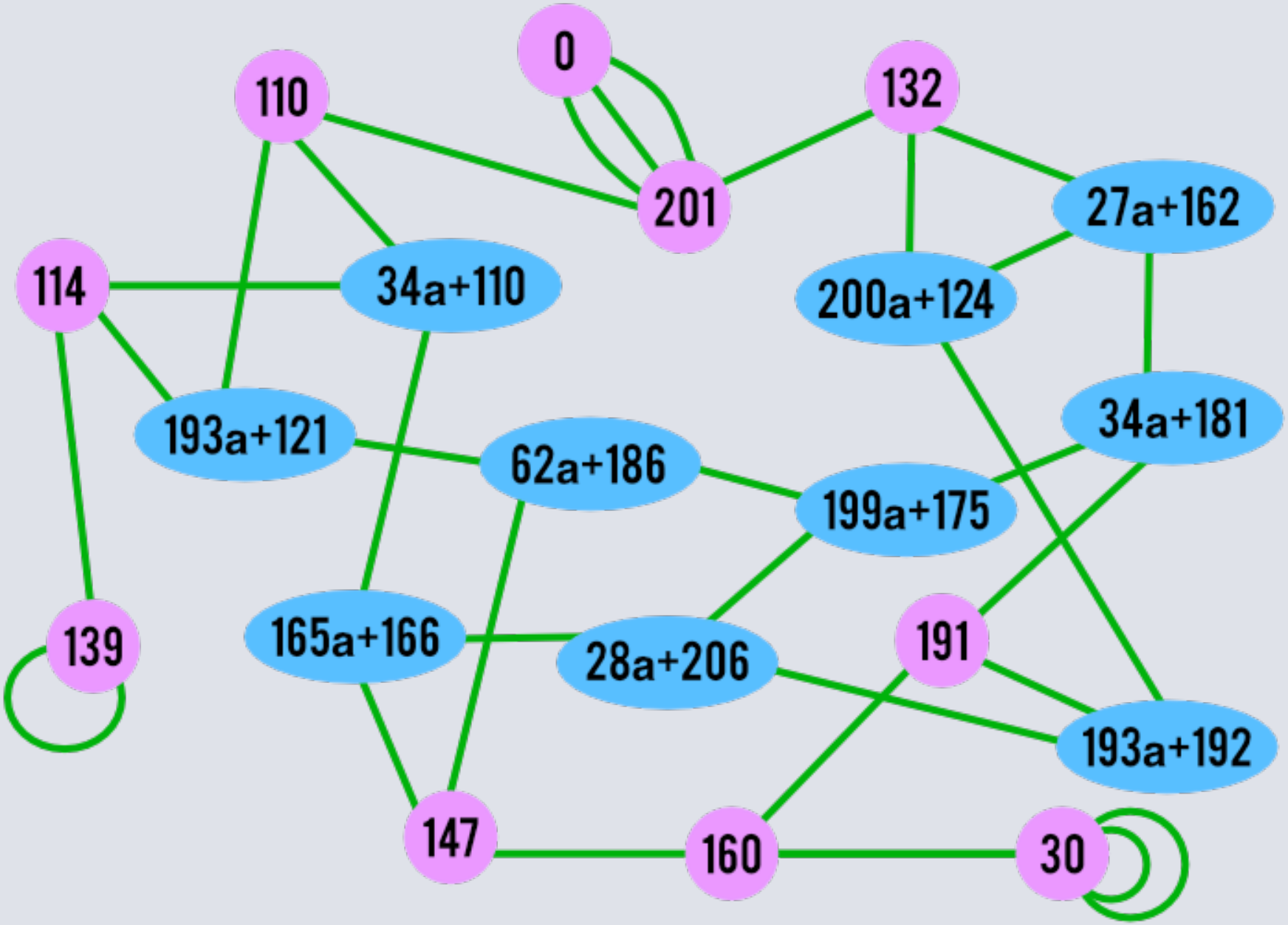
$$\left\{ \text{ supersingular elliptic curves over } \mathbb{F}_{p^2}, \text{ up to isomorphism } \right\}$$

$$\updownarrow$$

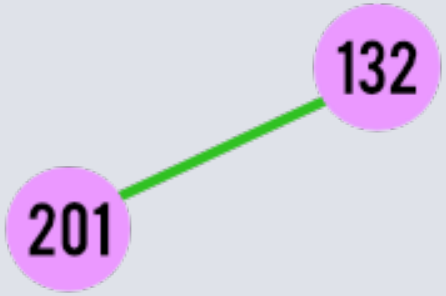
$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

- **Edges:** isogenies of degree ℓ.

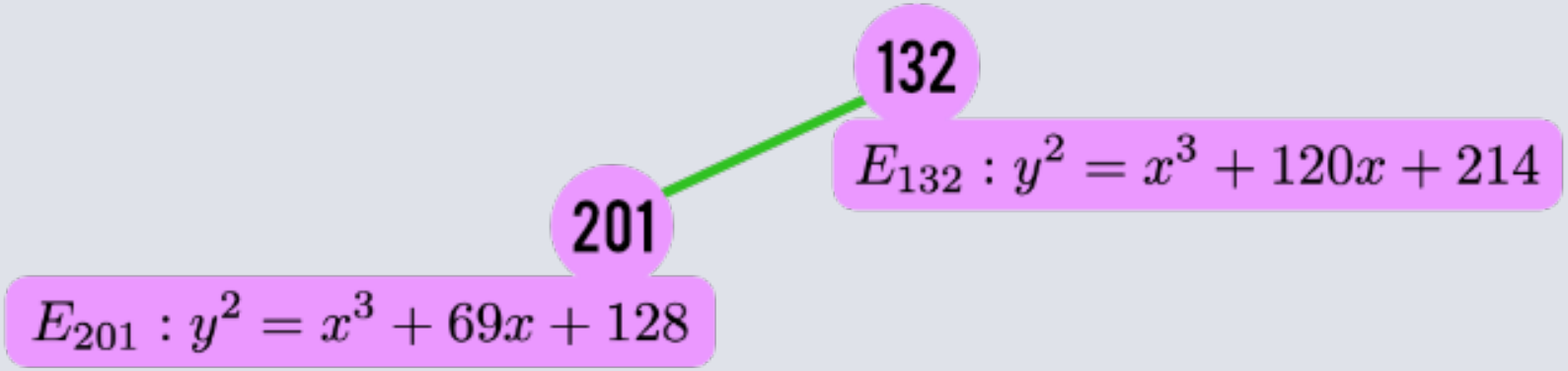
A toy example: $\mathcal{G}_2(\overline{\mathbb{F}}_{227})$



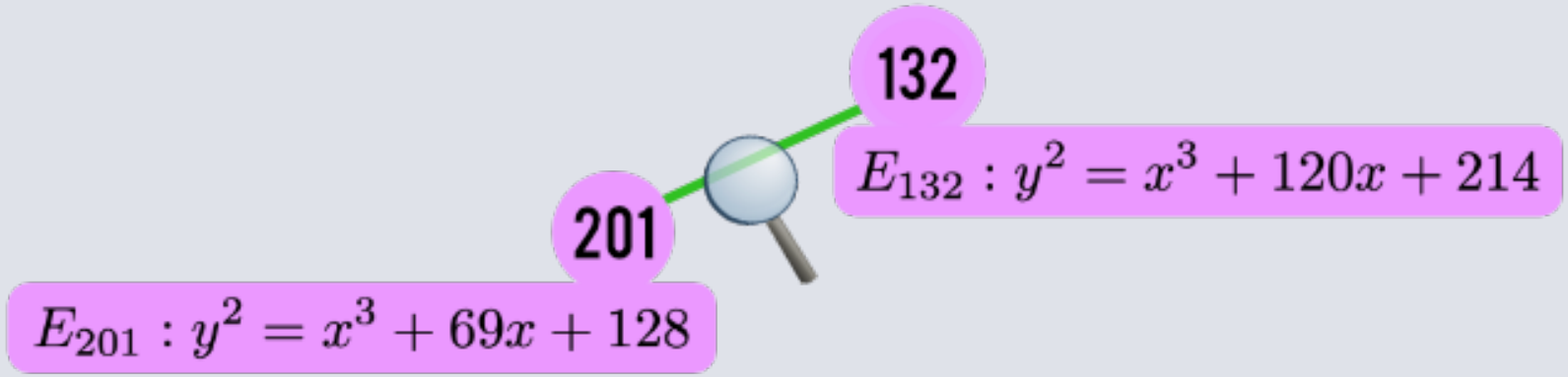
A toy example: $\mathcal{G}_2(\overline{\mathbb{F}}_{227})$



A toy example: $\mathcal{G}_2(\overline{\mathbb{F}}_{227})$

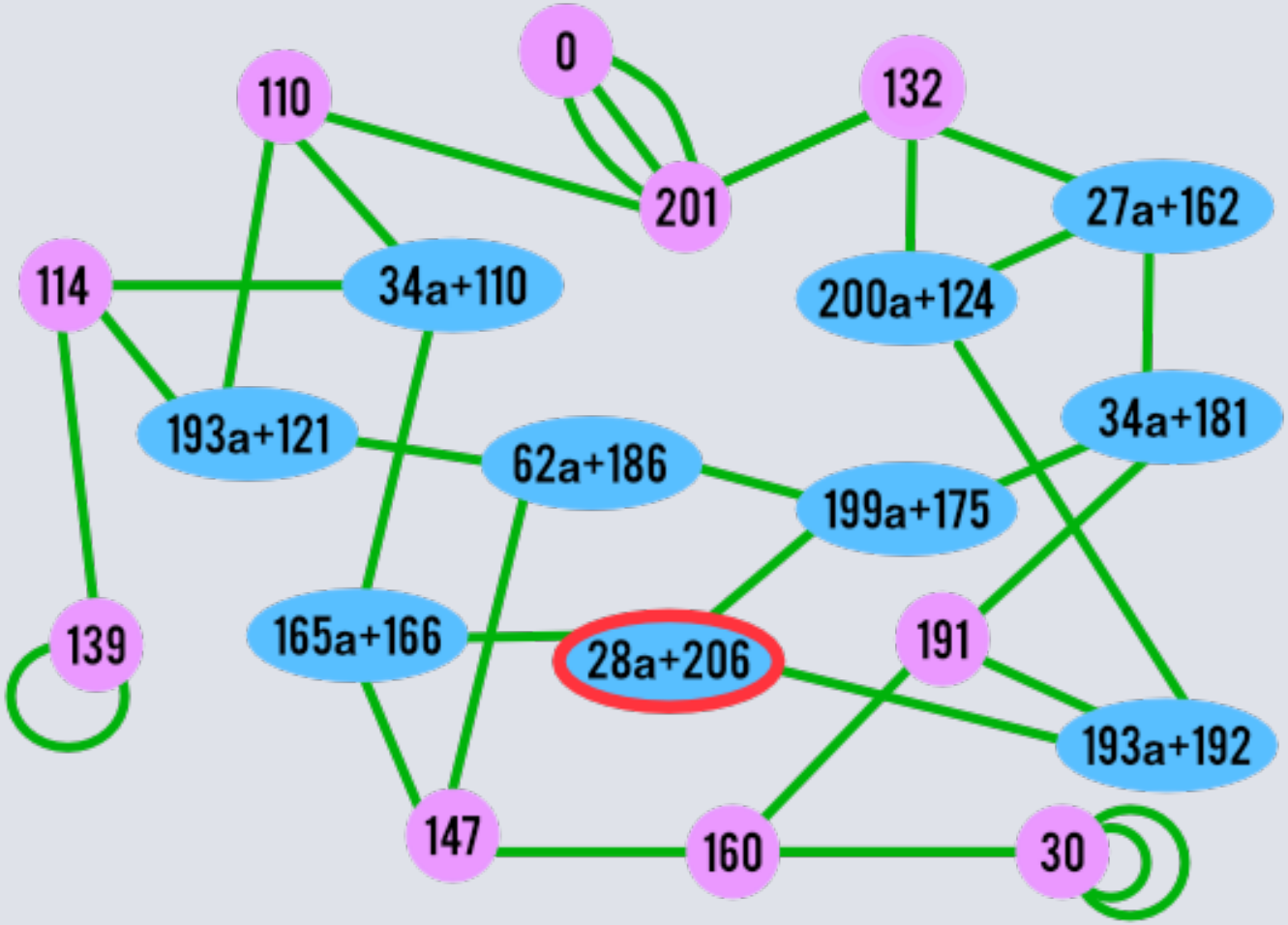


A toy example: $\mathcal{G}_2(\overline{\mathbb{F}}_{227})$

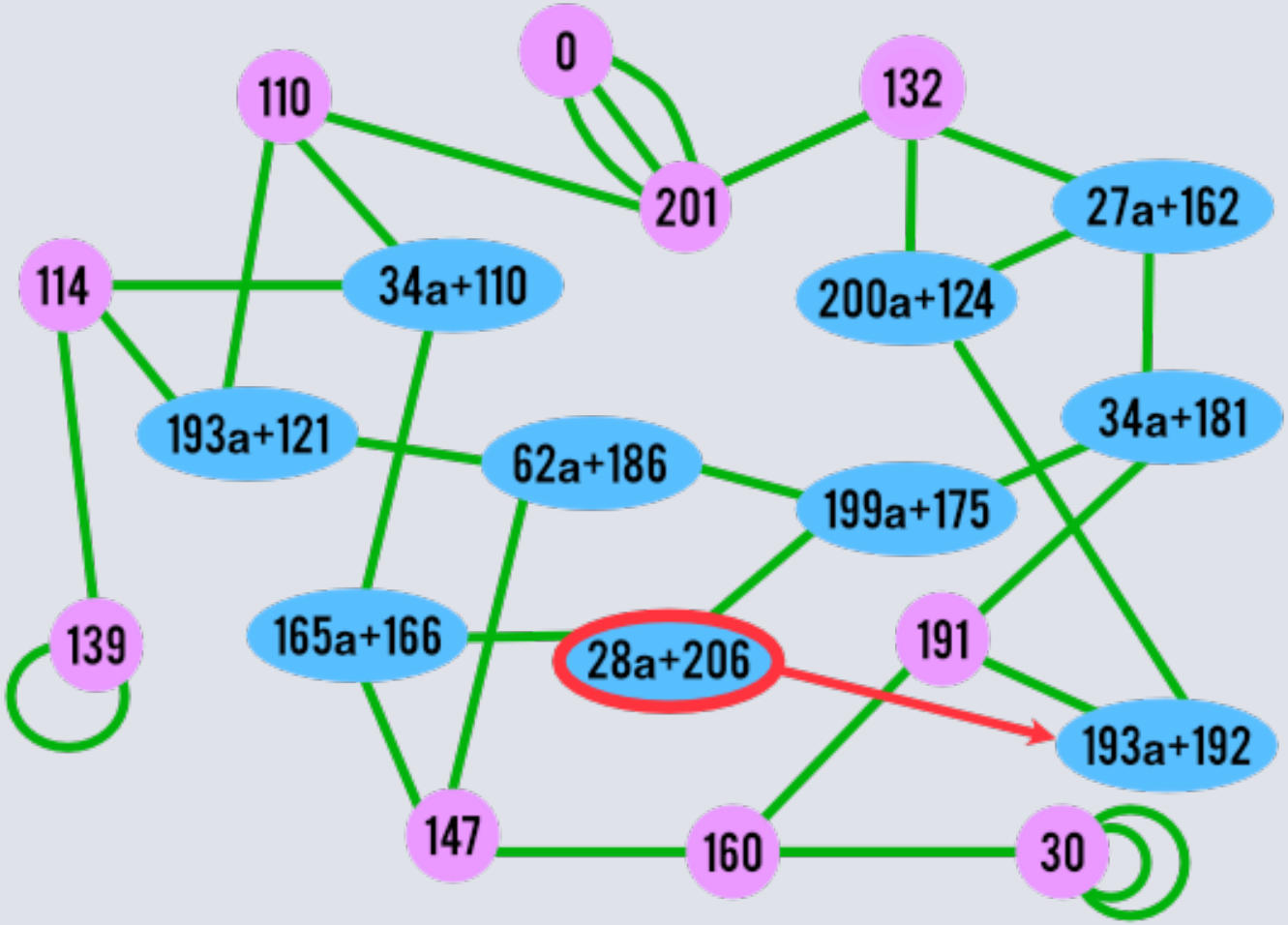


$$\begin{array}{rccc} \varphi : & E_{201} & \to & E_{132} \\ & (x, y) & \mapsto & \left(\frac{x^2+84x-101}{x+84}, y\frac{x^2-59x-107}{x^2-59x+19} \right) \end{array}$$

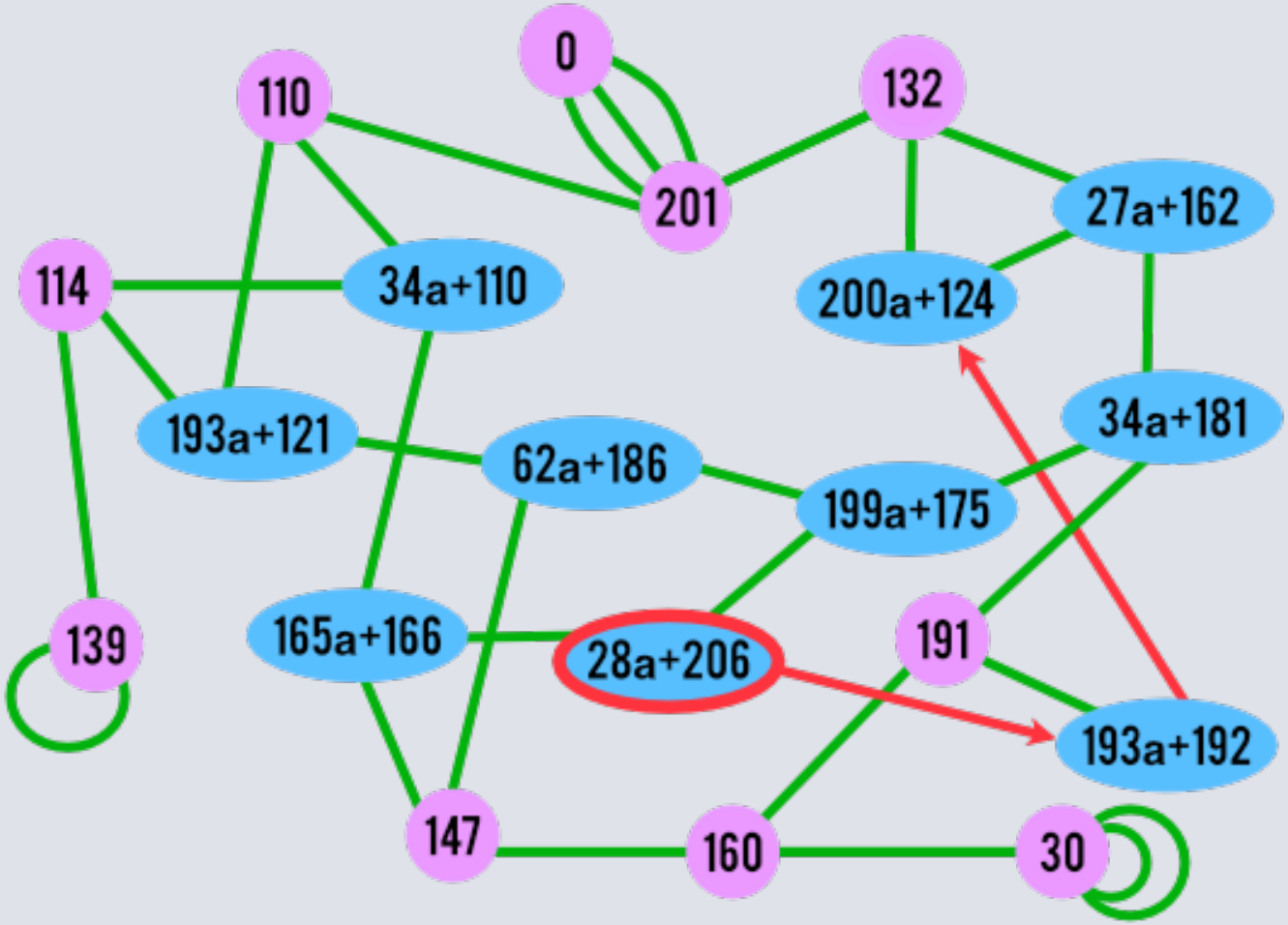
An endomorphism in the graph



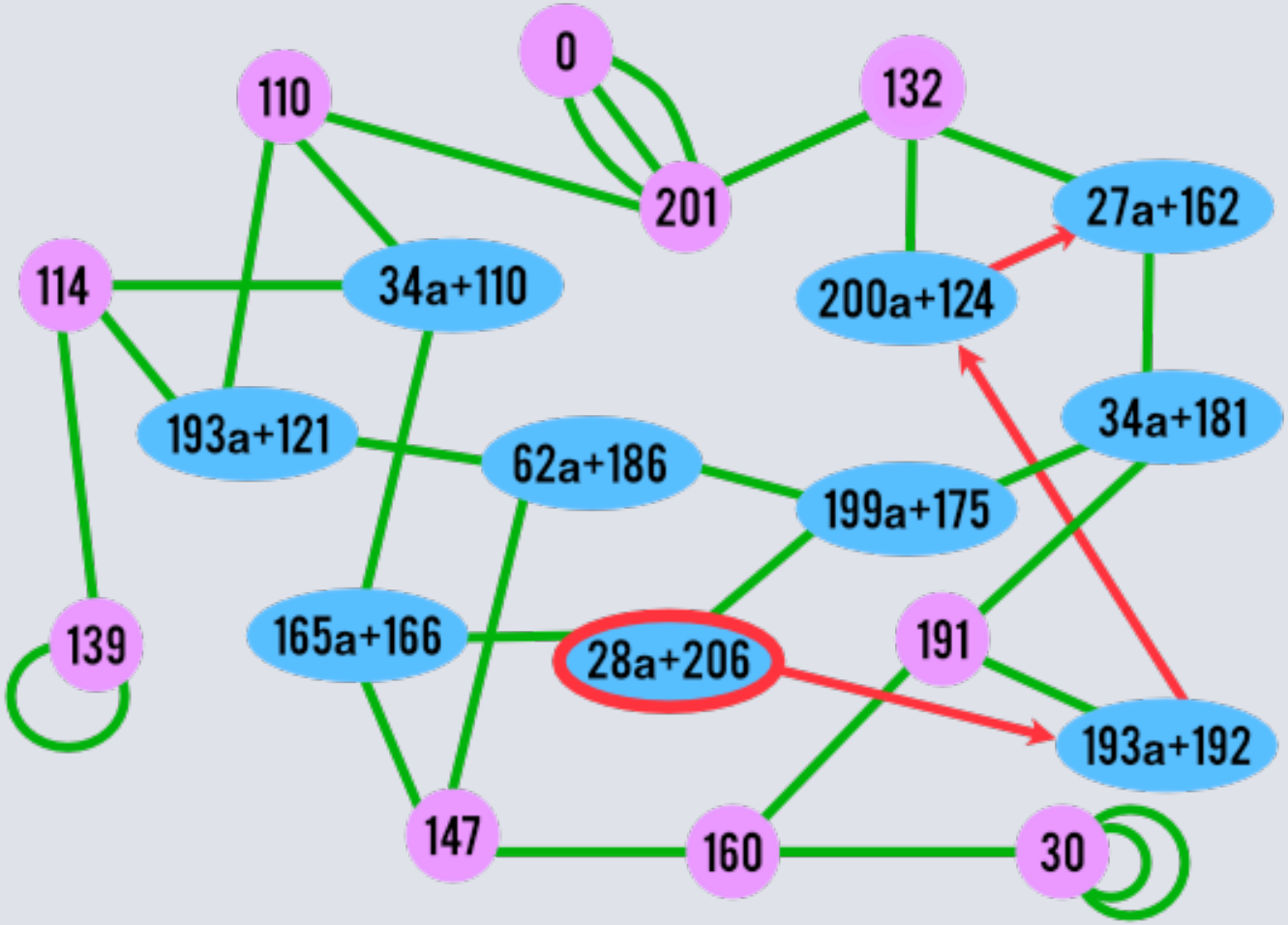
An endomorphism in the graph



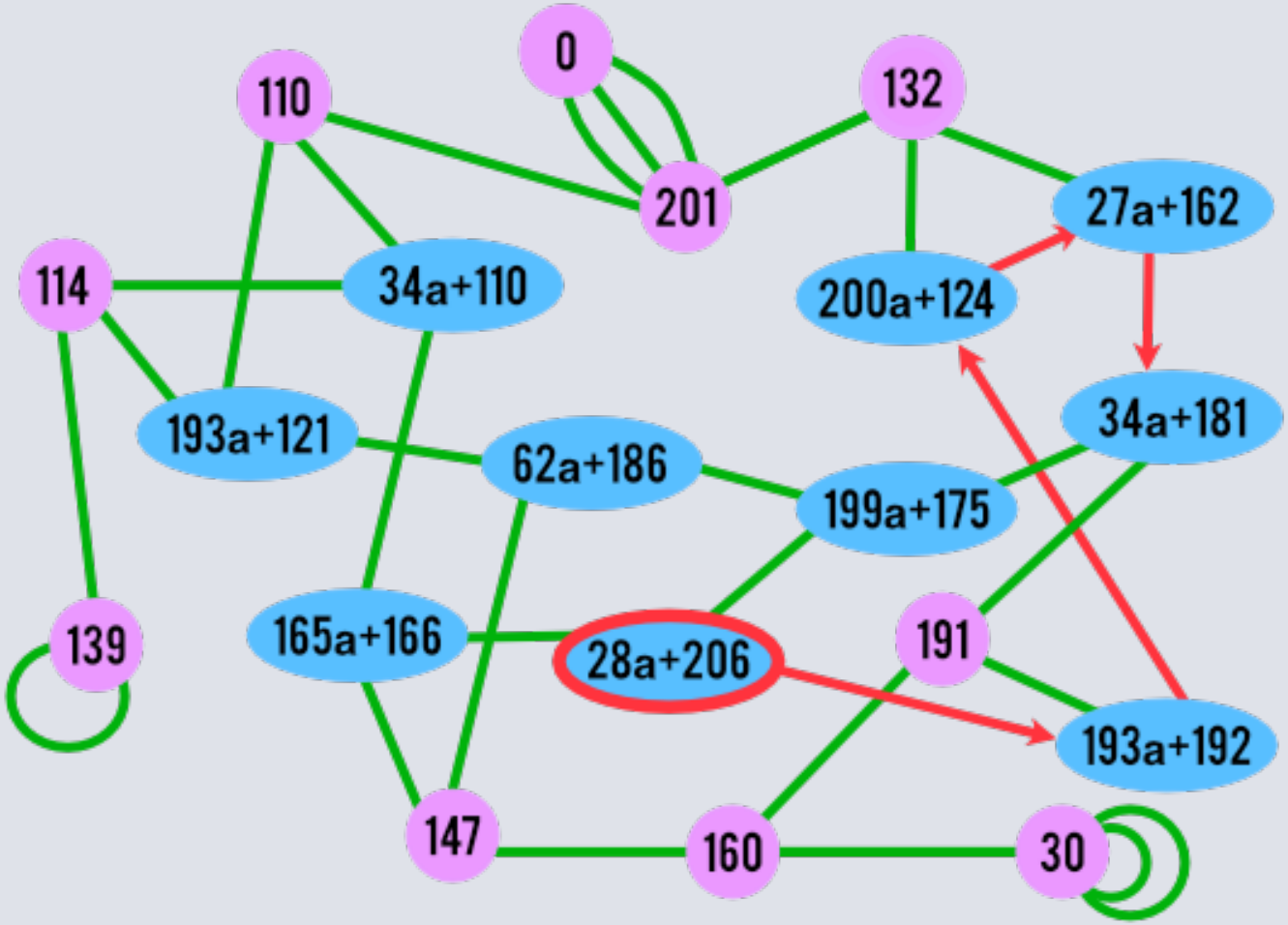
An endomorphism in the graph



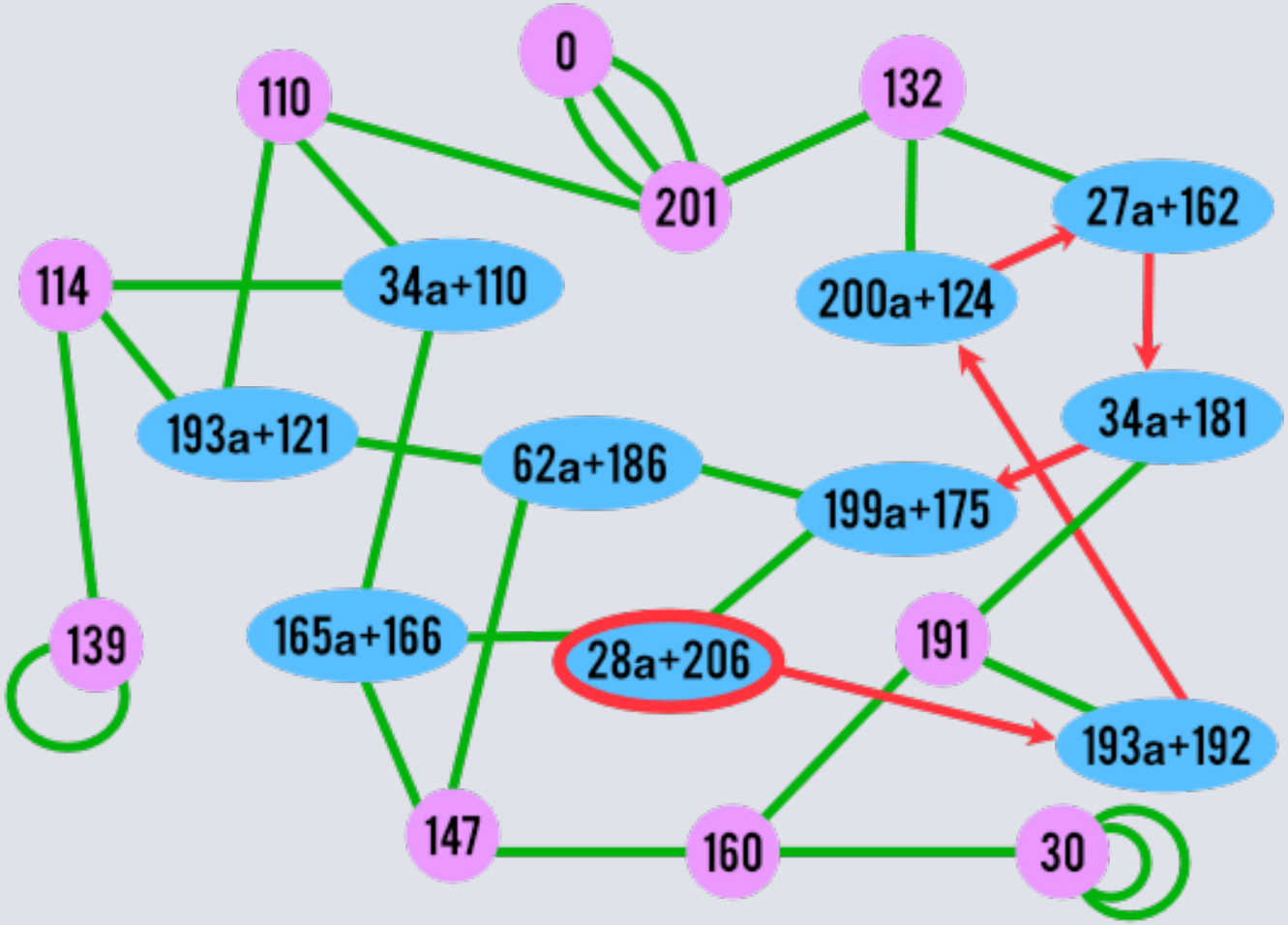
An endomorphism in the graph



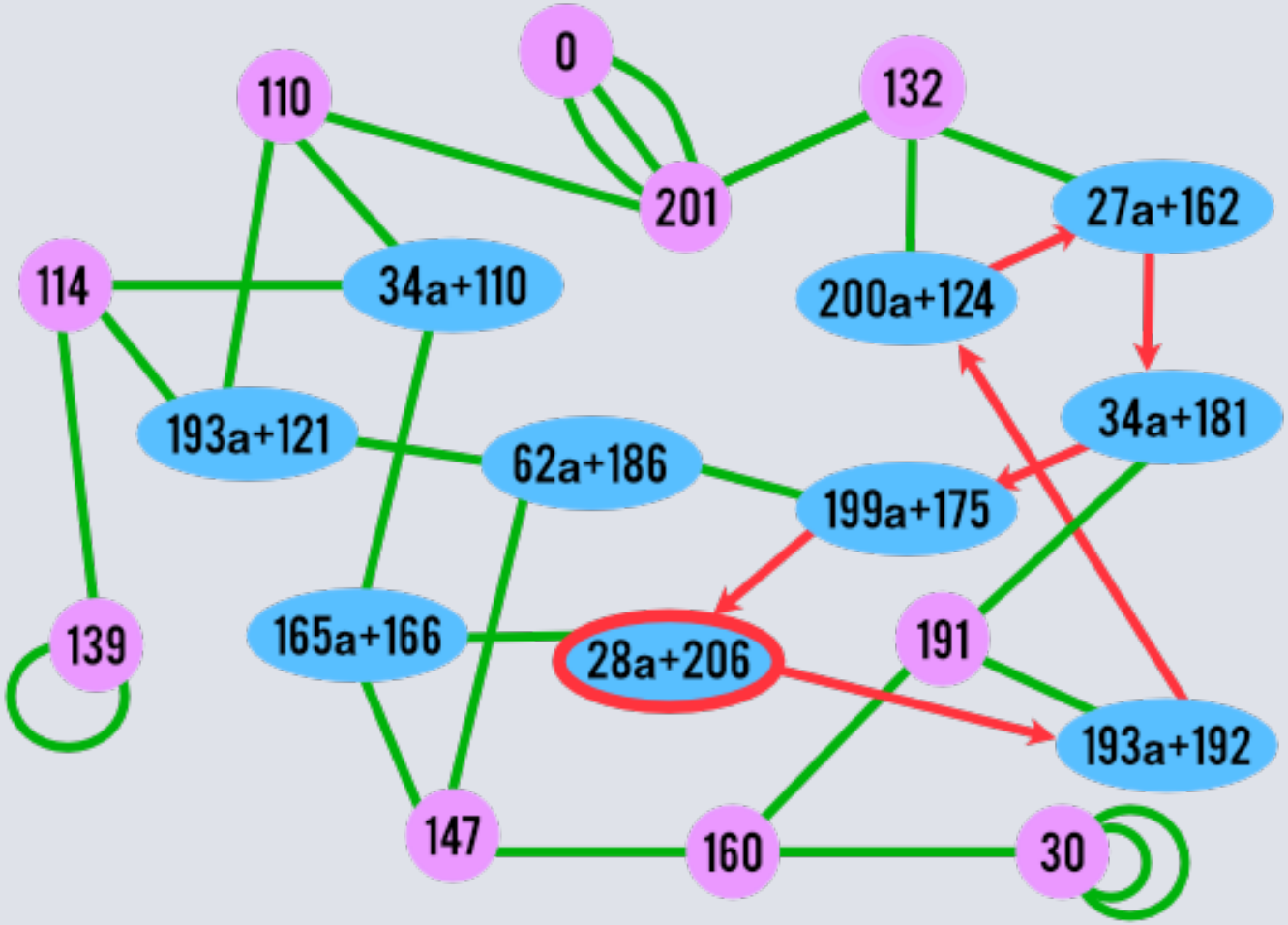
An endomorphism in the graph



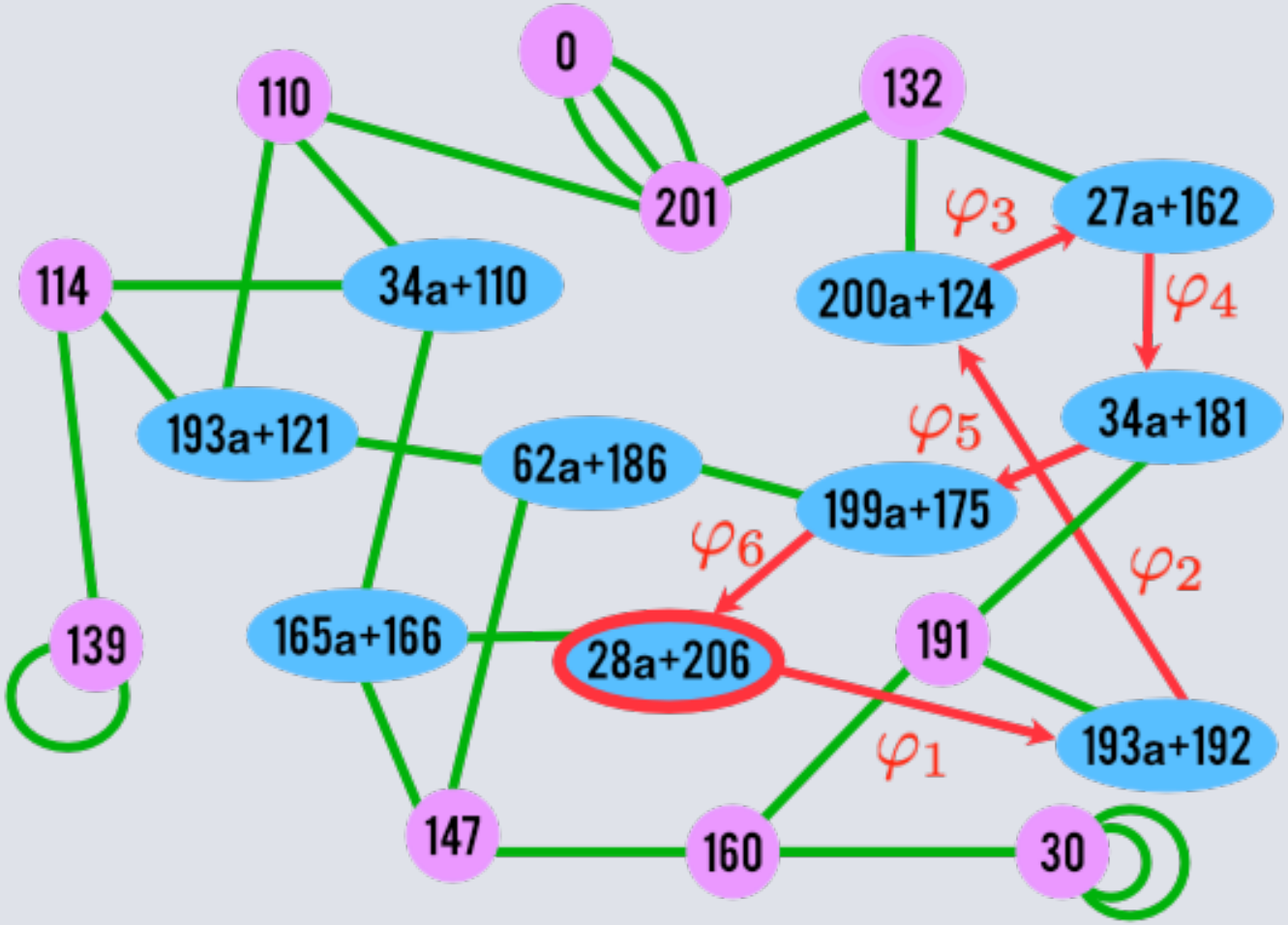
An endomorphism in the graph



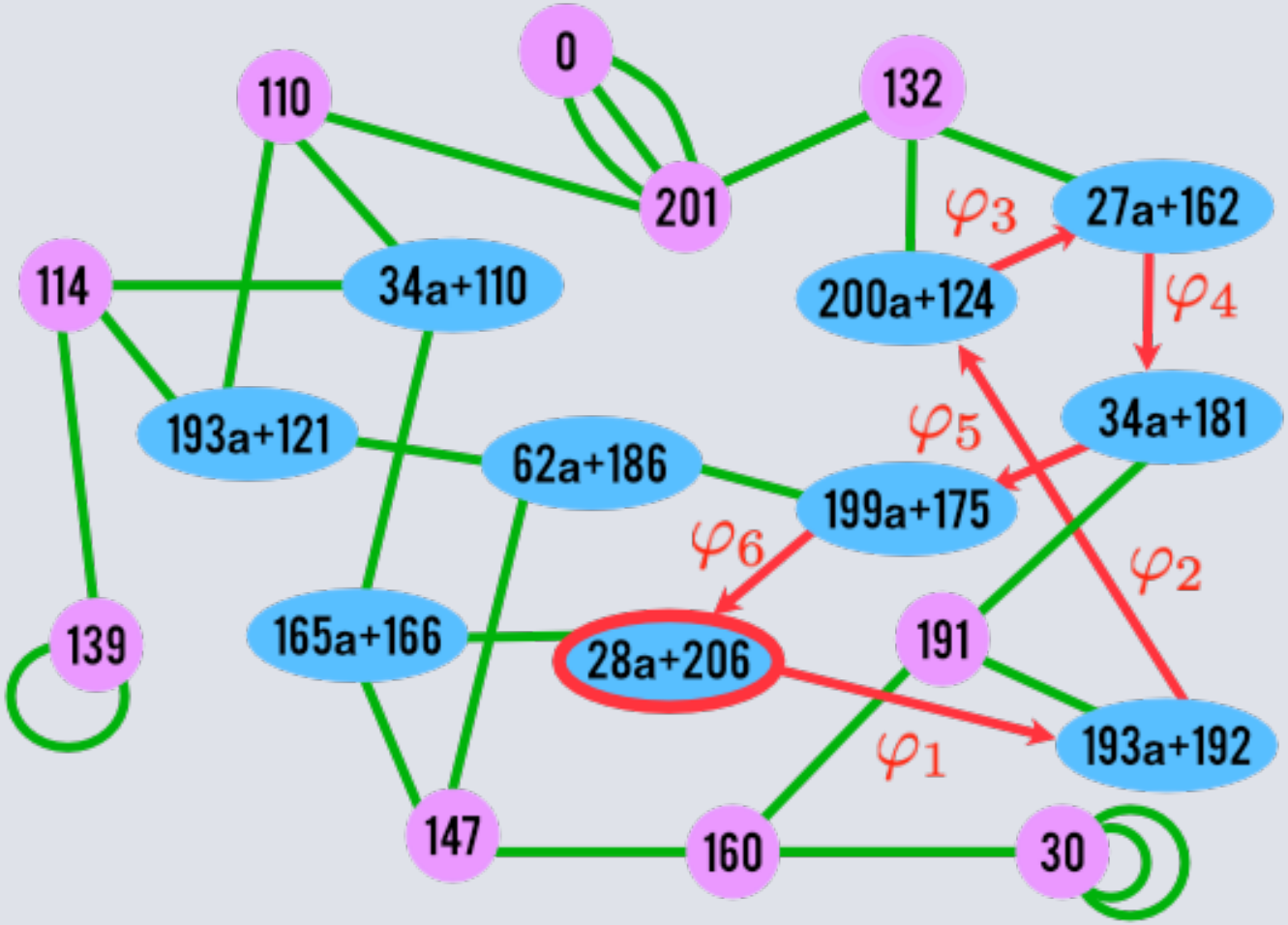
An endomorphism in the graph



An endomorphism in the graph



An endomorphism in the graph



$$\varphi_6 \circ \varphi_5 \circ \cdots \circ \varphi_1 \in \mathrm{End}(E_{28a+206}).$$

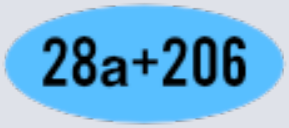
1996

D. Kohel

Endomorphism rings of elliptic curves over finite fields.

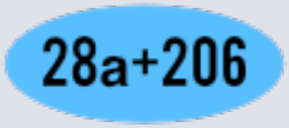
PhD thesis, University of California, Berkeley, (1996).

Kohel's idea



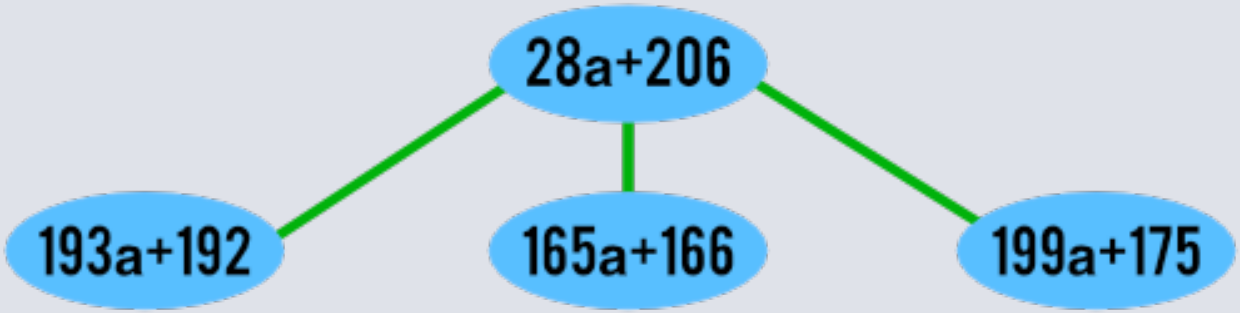
Kohel's idea

Kohel first builds a spanning tree with root E



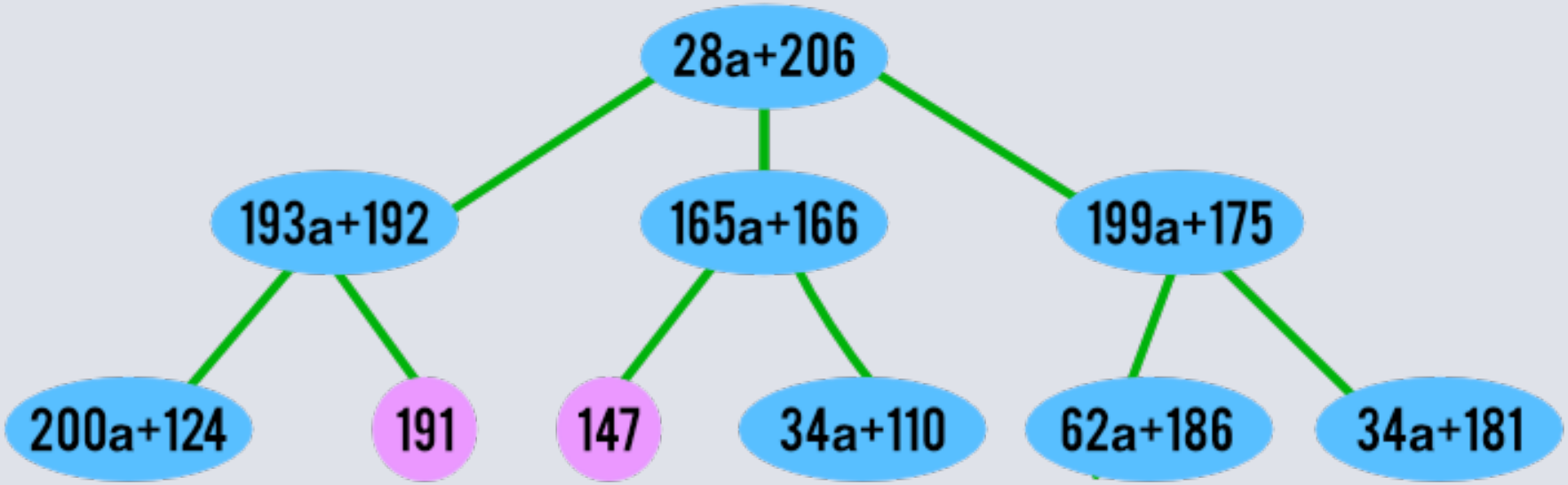
Kohel's idea

Kohel first builds a spanning tree with root E



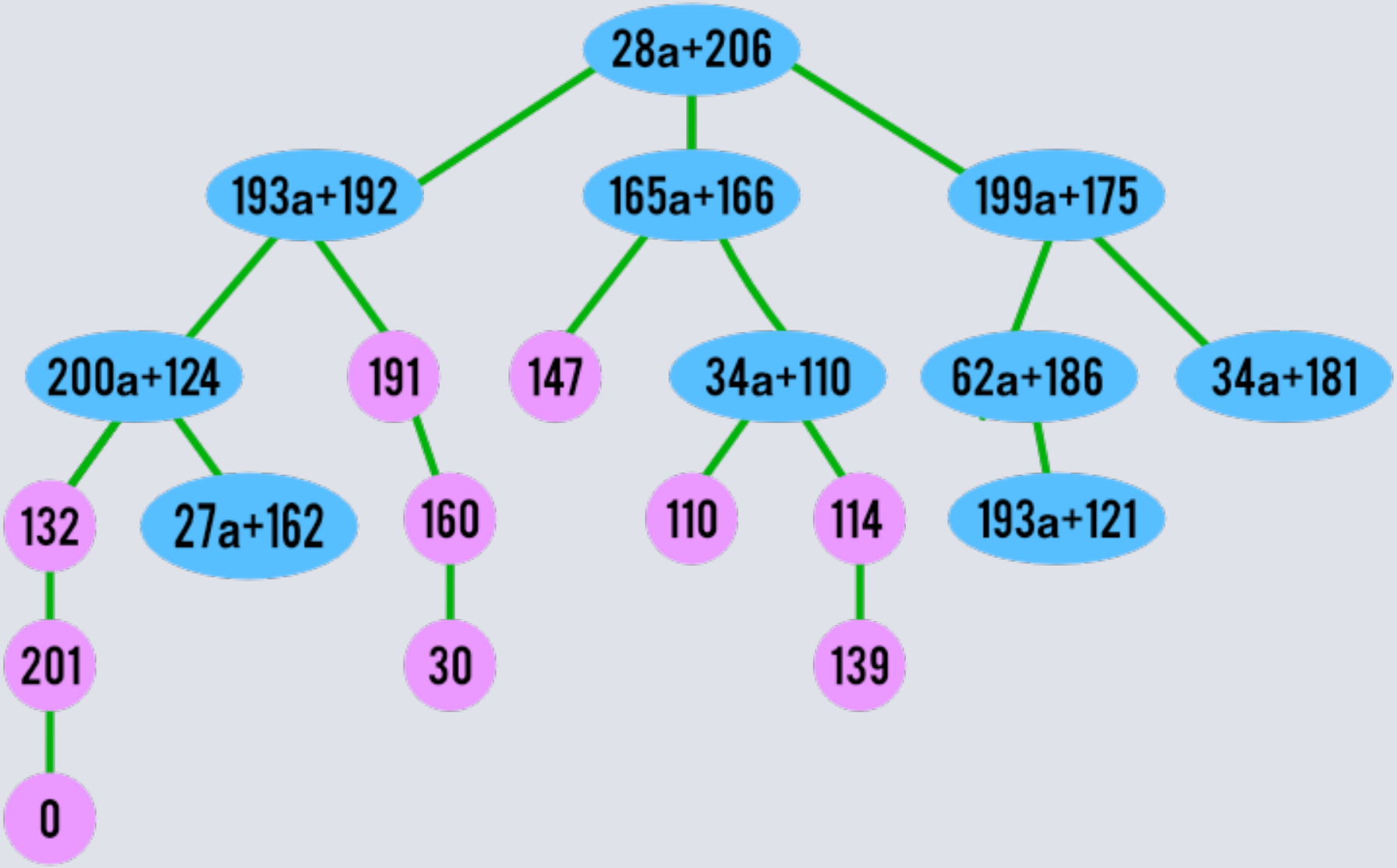
Kohel's idea

Kohel first builds a spanning tree with root E



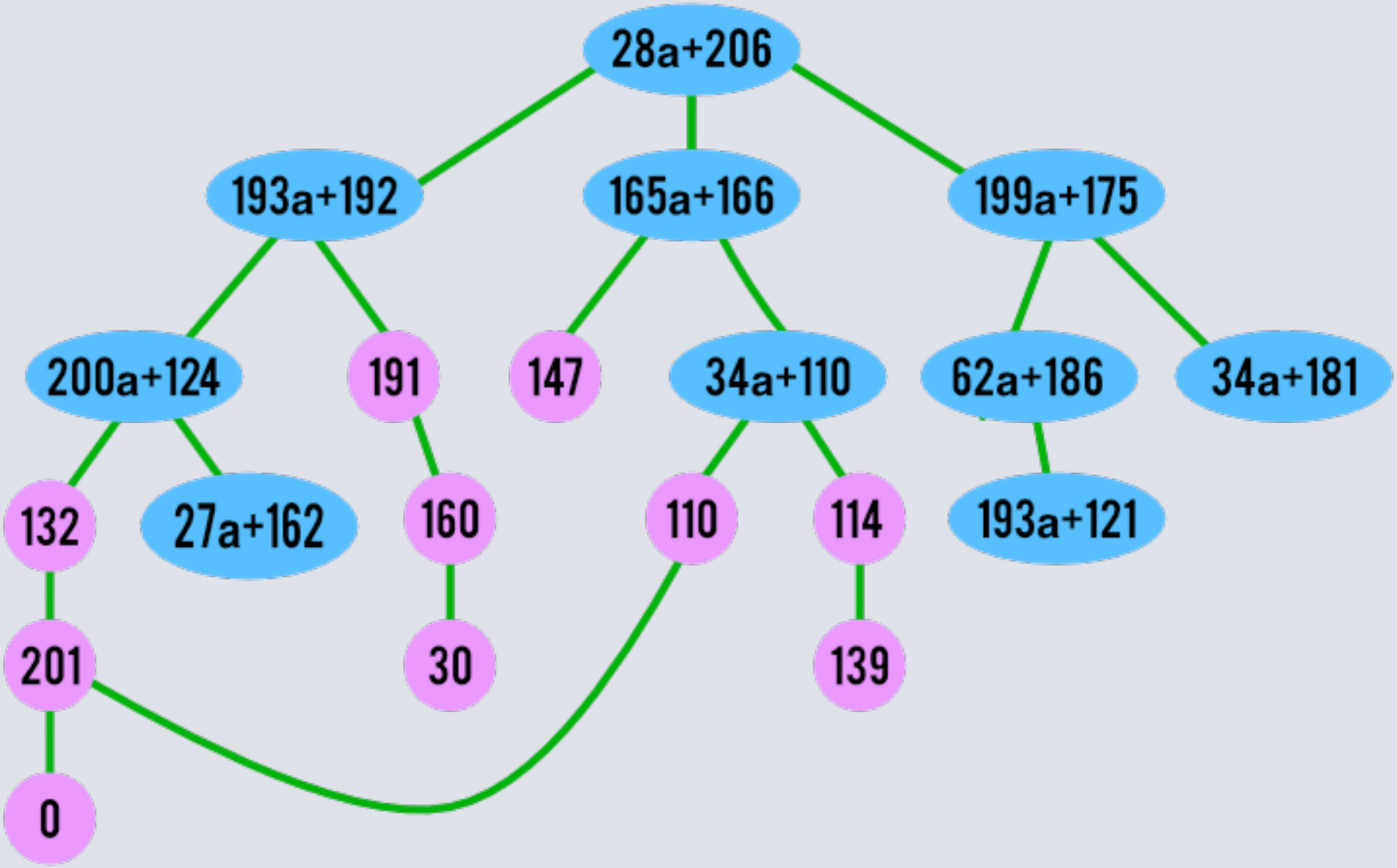
Kohel's idea

Kohel first builds a spanning tree with root E



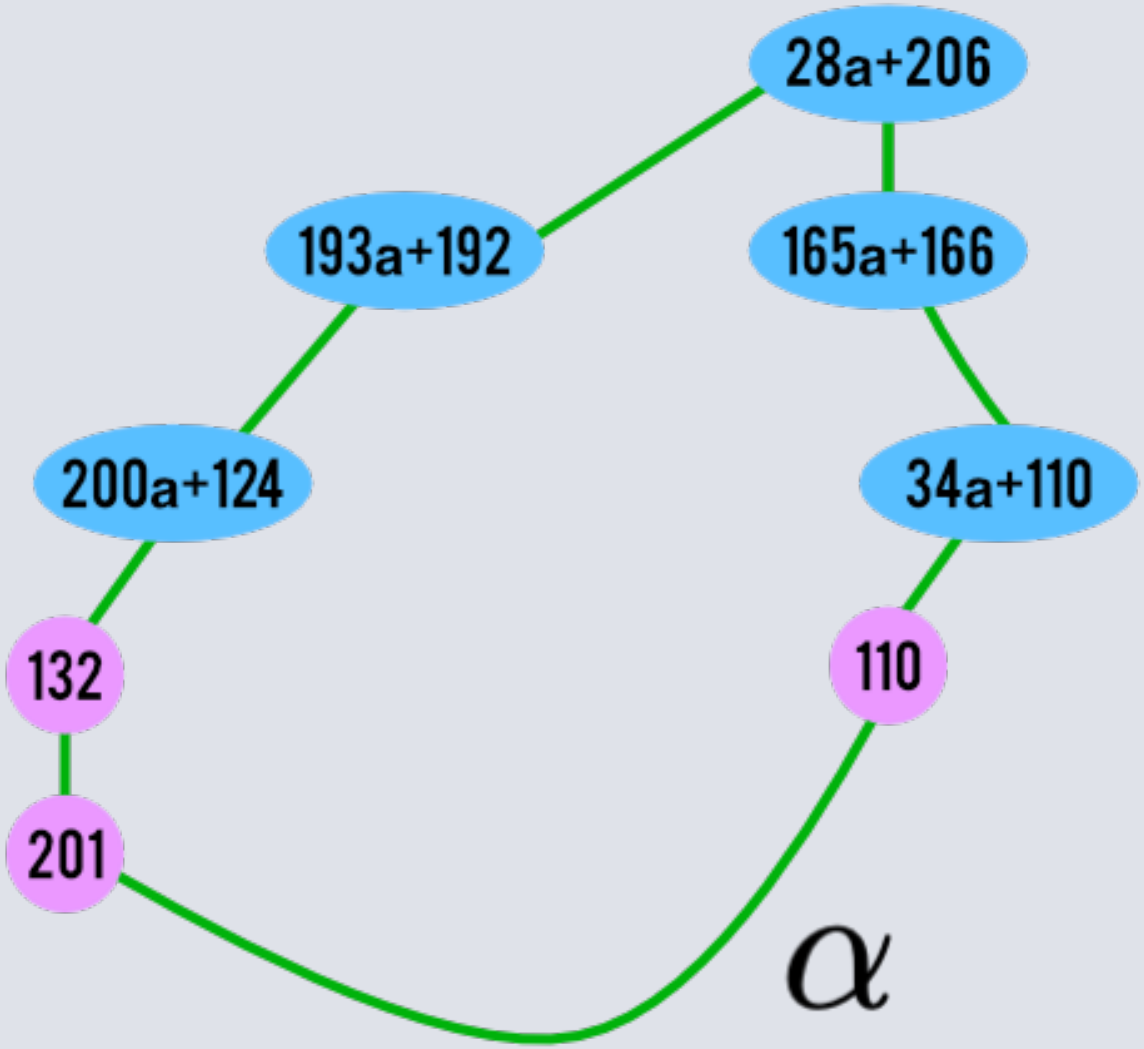
Kohel's idea

Then adds an absent edge to get a cycle through E



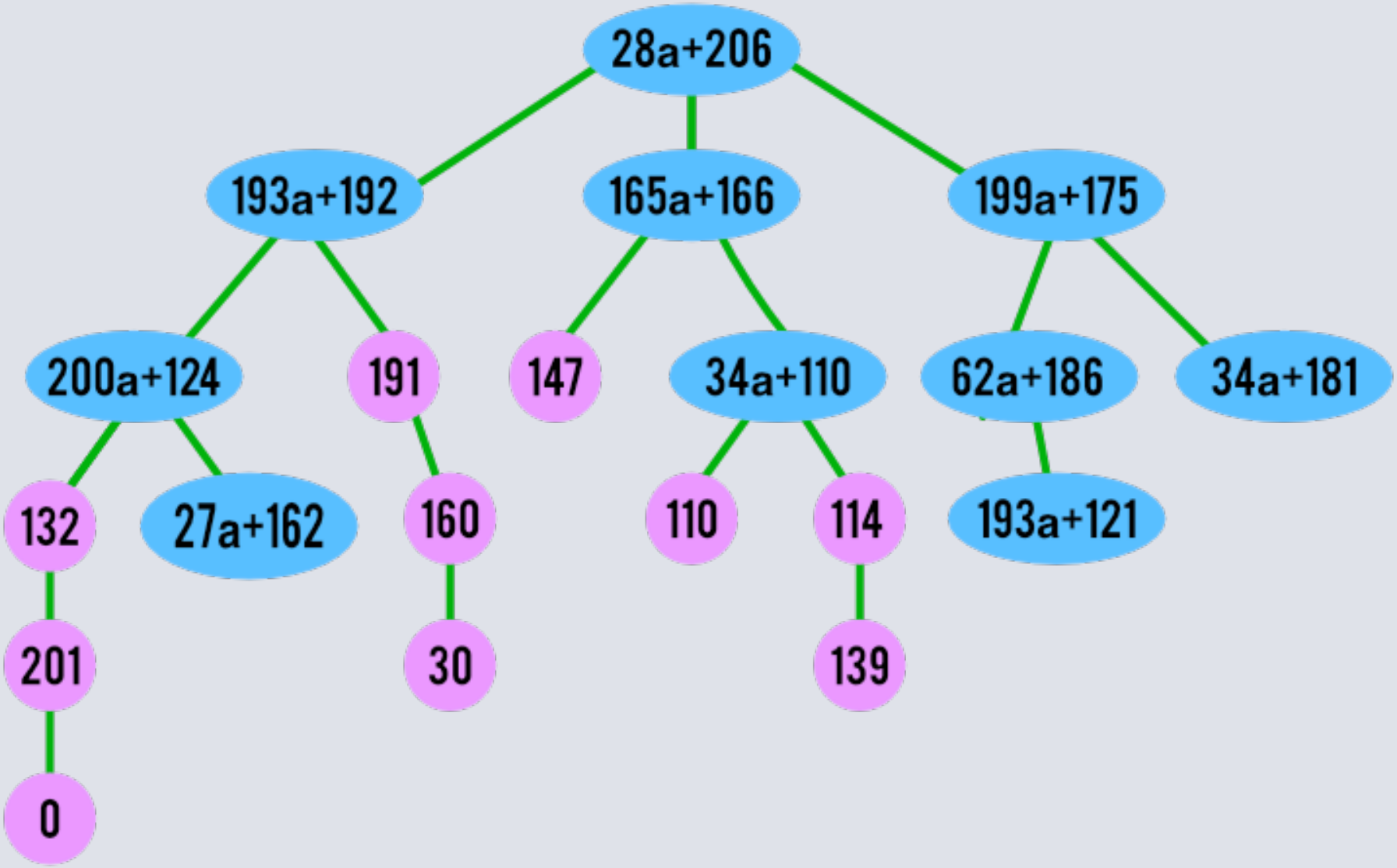
Kohel's idea

Then adds an absent edge to get a cycle through E



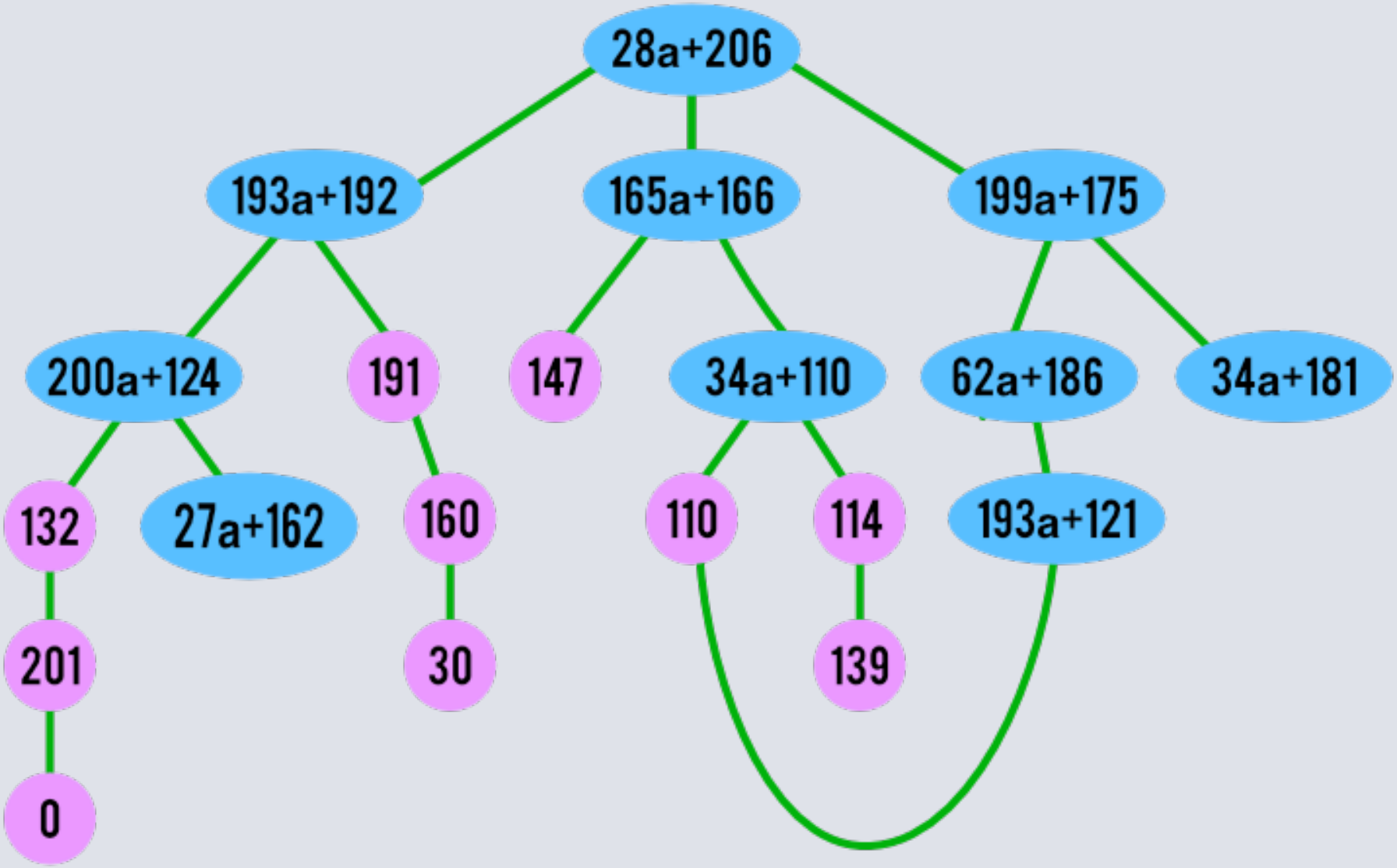
Kohel's idea

Then adds an absent edge to get a cycle through E



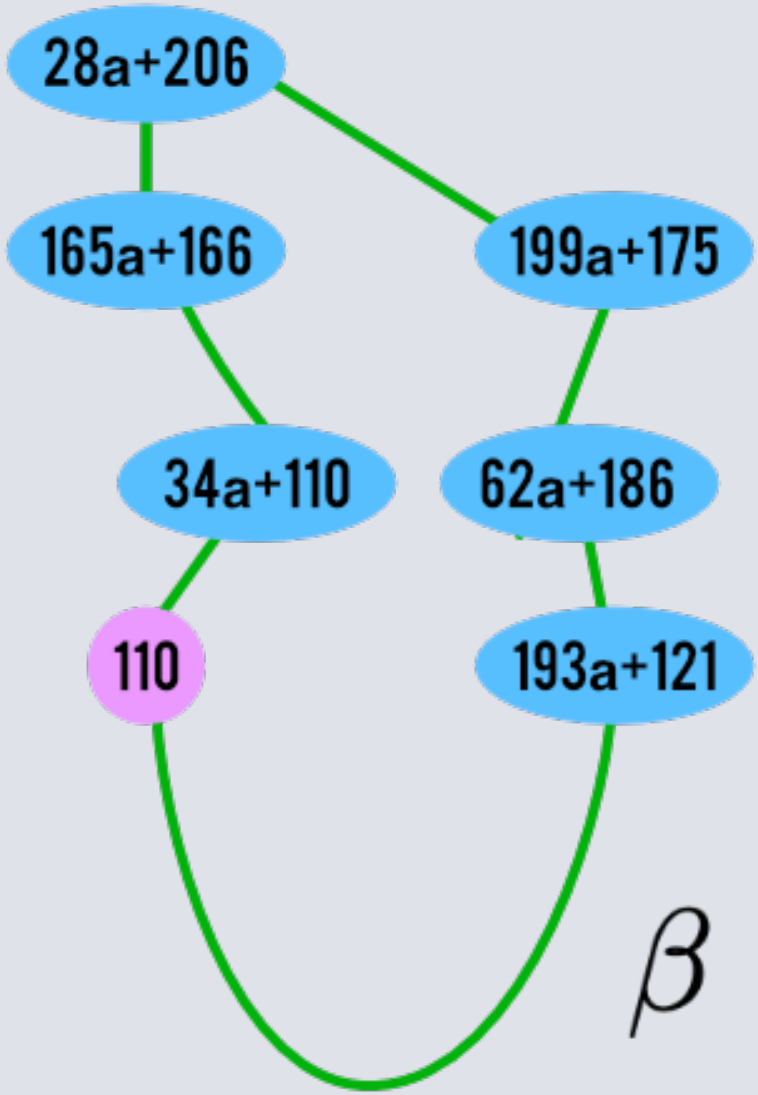
Kohel's idea

Then adds an absent edge to get a cycle through E



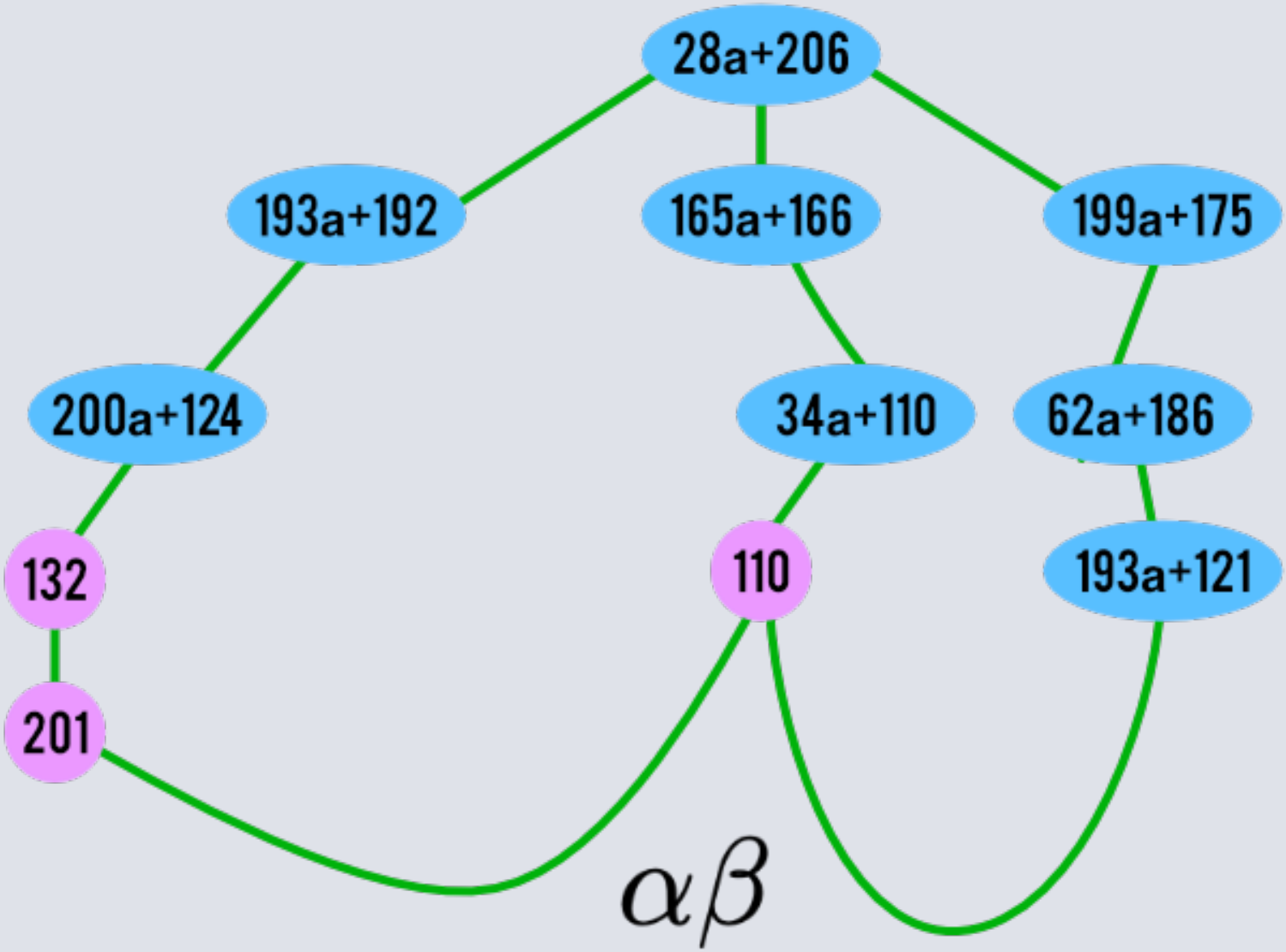
Kohel's idea

Then adds an absent edge to get a cycle through E



Kohel's idea

Then adds an absent edge to get a cycle through E



So Kohel computes four endomorphisms in $\mathrm{End}(E)$ which are linearly independent over $\mathbb{Z}$:

$$1, \alpha, \beta, \alpha\beta.$$

So Kohel computes four endomorphisms in $\mathrm{End}(E)$ which are linearly independent over $\mathbb{Z}$:

$$1, \alpha, \beta, \alpha\beta.$$

Therefore he computes the following suborder of $\mathrm{End}(E)$:

$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$$

So Kohel computes four endomorphisms in $\mathrm{End}(E)$ which are linearly independent over $\mathbb{Z}$:

$$1, \alpha, \beta, \alpha\beta.$$

Therefore he computes the following suborder of $\mathrm{End}(E)$:

$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$$

Theorem (Theorem 75)

There exists an algorithm that given any supersingular elliptic curve E over a finite field k computes **four endomorphisms in** $\mathrm{End}(E)$ **which are linearly independent over** $\mathbb{Z}$. *For any* $\epsilon > 0$ *the algorithm terminates* **deterministically in** $O(p^{3/2+\epsilon})$ *operations in the field k and* **probabilistically with expected** $O(p^{1+\epsilon})$ *operations in k, where p is the characteristic of k.*

2020

K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park.
Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs.
Proceedings of the Fourteenth Algorithmic Number Theory Symposium, pages 215–232, (2020).

A limitation of quaternion algebras

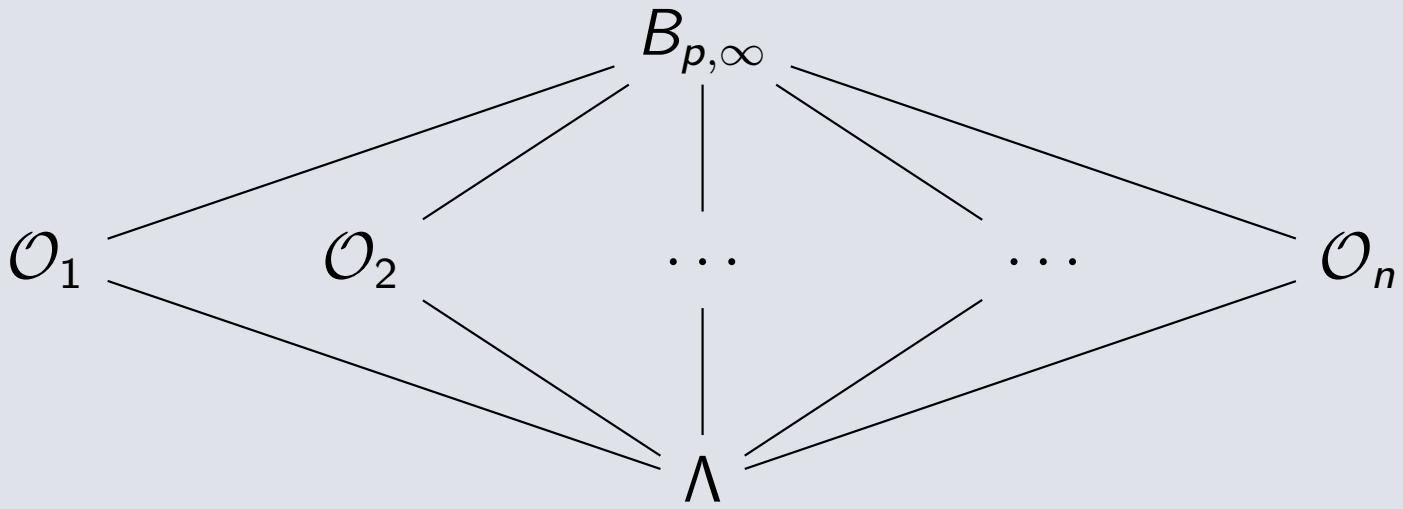
If we have a suborder $\Lambda \subseteq B_{p,\infty}$, then there can be exponentially in $\log(\mathrm{disc}(\Lambda))$ many pairwise non-isomorphic maximal orders which contain Λ.

$$B_{p,\infty}$$

$$\Lambda$$

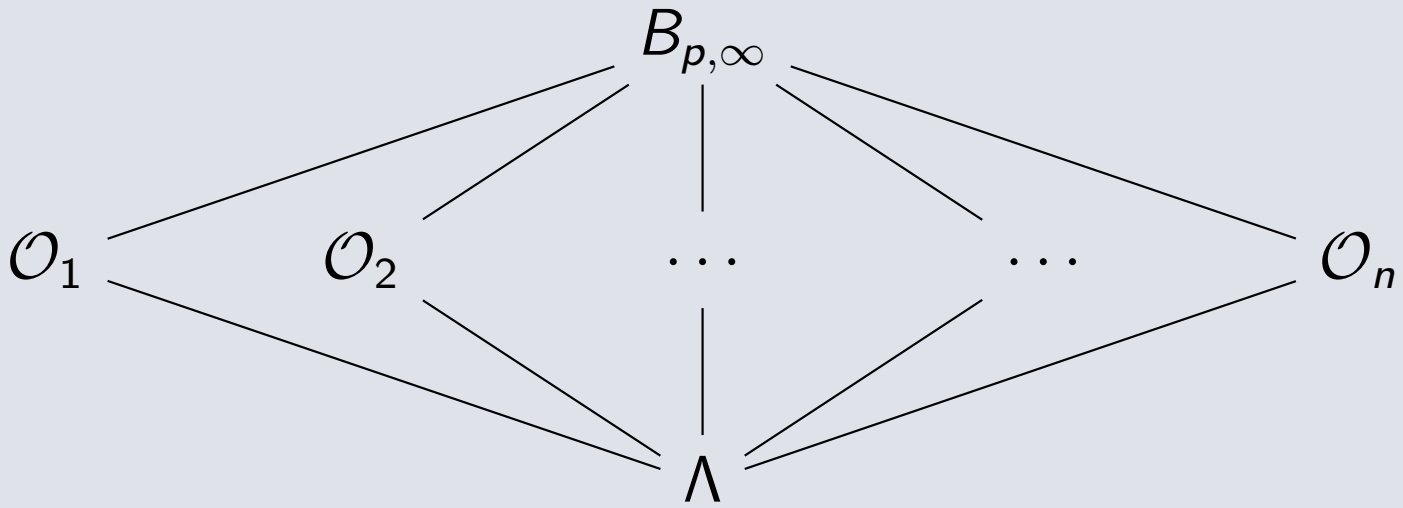
A limitation of quaternion algebras

If we have a suborder $\Lambda \subseteq B_{p,\infty}$, then there can be exponentially in $\log(\mathrm{disc}(\Lambda))$ many pairwise non-isomorphic maximal orders which contain Λ



A limitation of quaternion algebras

If we have a suborder $\Lambda \subseteq B_{p,\infty}$, then there can be exponentially in $\log(\mathrm{disc}(\Lambda))$ many pairwise non-isomorphic maximal orders which contain Λ



Which one is $\mathrm{End}(E)$?

Eisenträger et al.'s idea

Find endomorphisms $\alpha, \beta, \gamma \in \mathrm{End}(E)$ such that

$$\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

is a **Bass suborder** of $\mathrm{End}(E)$.

Eisenträger et al.'s idea

Find endomorphisms $\alpha, \beta, \gamma \in \mathrm{End}(E)$ such that

$$\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

is a **Bass suborder** of $\mathrm{End}(E)$.

Definition(s):

- An order $\mathcal{O}$ in a quaternion algebra B is *Bass* if every order $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein.

Eisenträger et al.'s idea

Find endomorphisms $\alpha, \beta, \gamma \in \mathrm{End}(E)$ such that

$$\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

is a **Bass suborder** of $\mathrm{End}(E)$.

Definition(s):

- An order $\mathcal{O}$ in a quaternion algebra B is *Bass* if every order $\mathcal{O}' \supseteq O$ is Gorenstein.
- An order $\mathcal{O}$ in a quaternion algebra B is *Gorenstein* if the codifferent is invertible.

Eisenträger et al.'s idea

Find endomorphisms $\alpha, \beta, \gamma \in \mathrm{End}(E)$ such that

$$\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

is a **Bass suborder** of $\mathrm{End}(E)$.

Definition(s):

- An order $\mathcal{O}$ in a quaternion algebra B is *Bass* if every order $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein.
- An order $\mathcal{O}$ in a quaternion algebra B is *Gorenstein* if the codifferent is invertible.
- The *codifferent* of an order $\mathcal{O}$ is $\mathrm{codiff}(\mathcal{O}) = \ldots\ldots$

Eisenträger et al.'s idea

Find endomorphisms $\alpha, \beta, \gamma \in \mathrm{End}(E)$ such that

$$\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

is a **Bass suborder** of $\mathrm{End}(E)$.

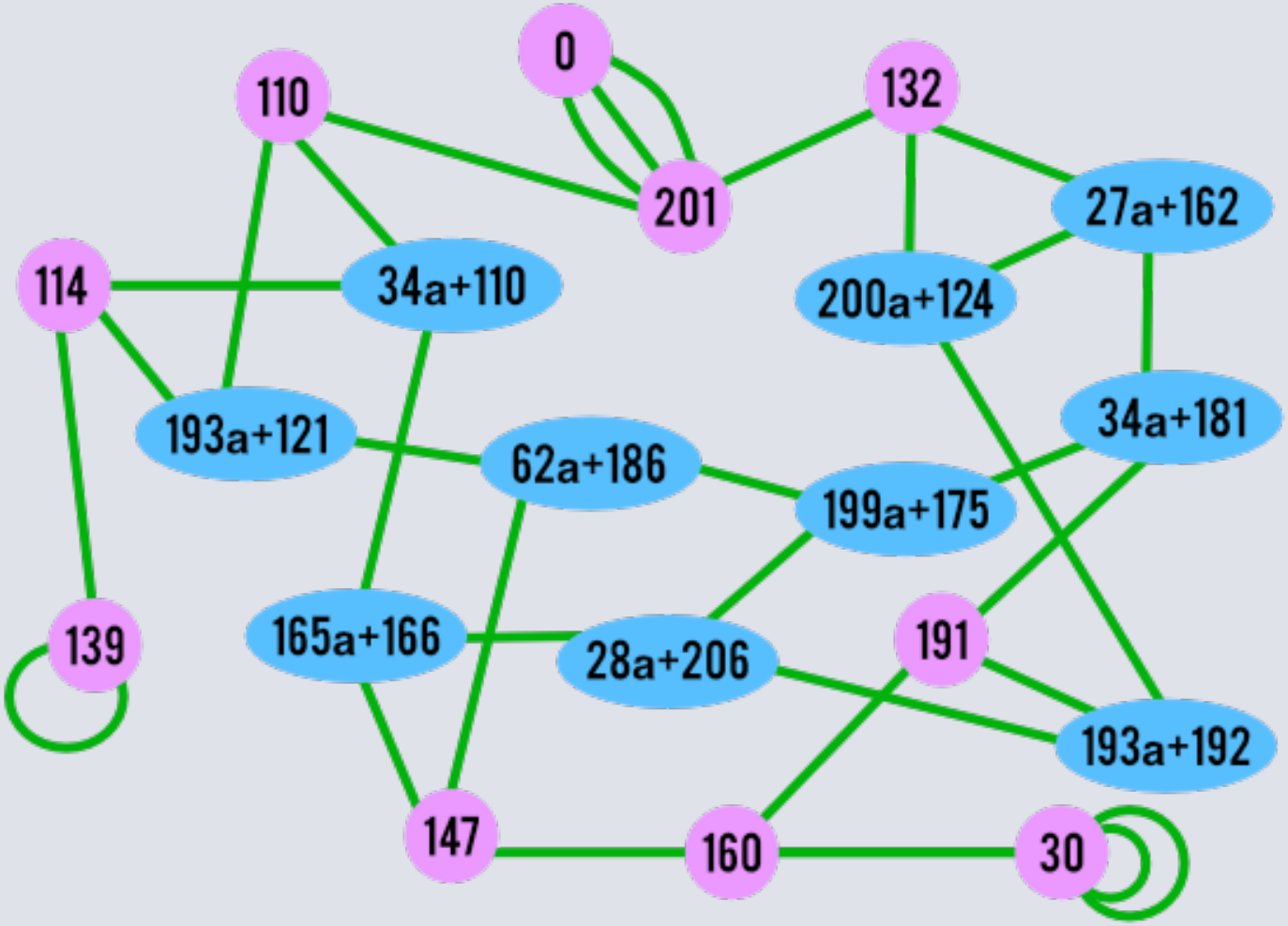
Definition(s):

- An order $\mathcal{O}$ in a quaternion algebra B is *Bass* if every order $\mathcal{O}' \supseteq O$ is Gorenstein.
- An order $\mathcal{O}$ in a quaternion algebra B is *Gorenstein* if the codifferent is invertible.
- The *codifferent* of an order $\mathcal{O}$ is $\mathrm{codiff}(\mathcal{O}) = \ldots\ldots$

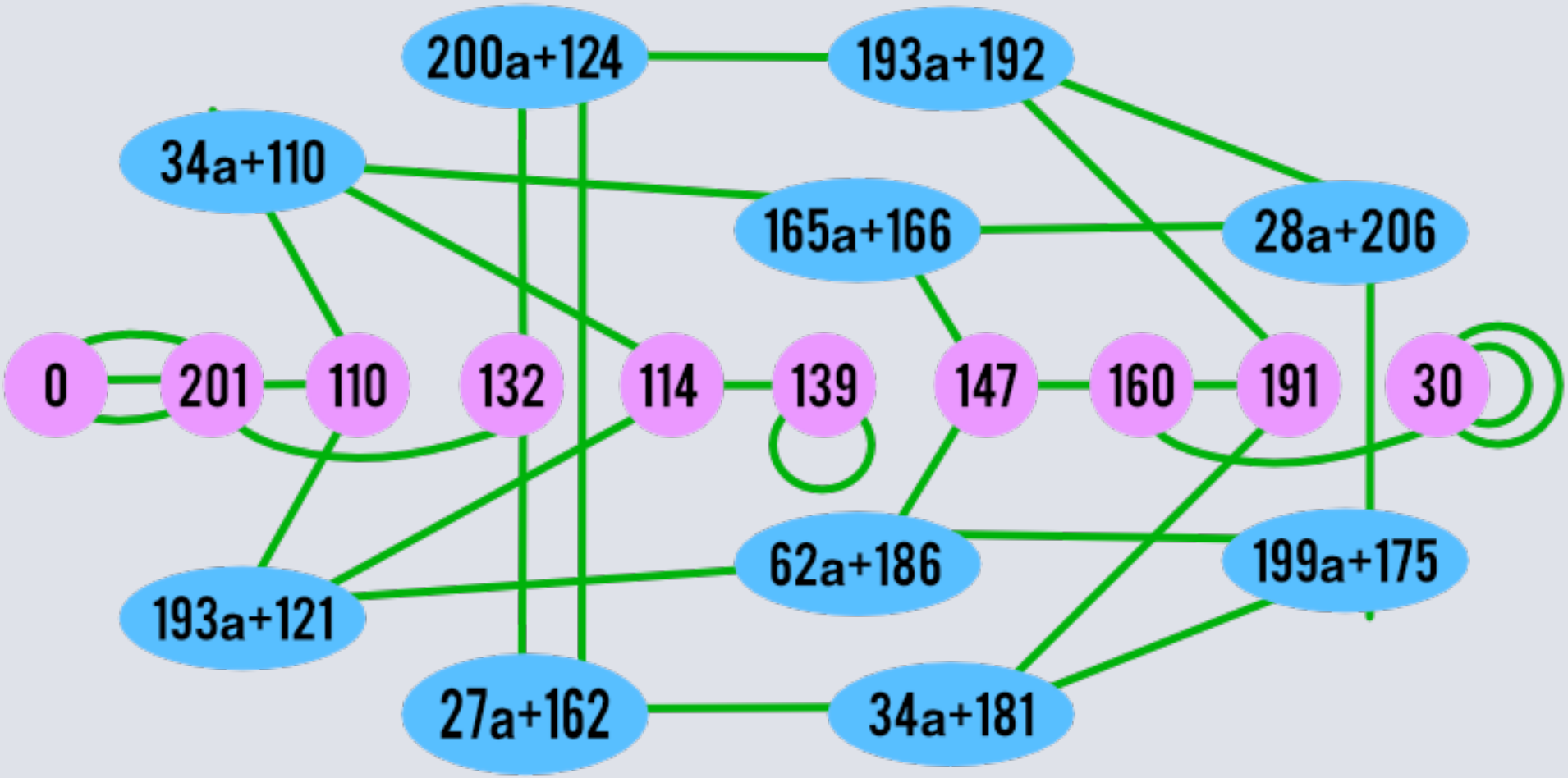
Key property: Bass orders only have $O(p^\epsilon)$ maximal orders containing them for any $\epsilon > 0$.

The mirror involution

The mirror involution



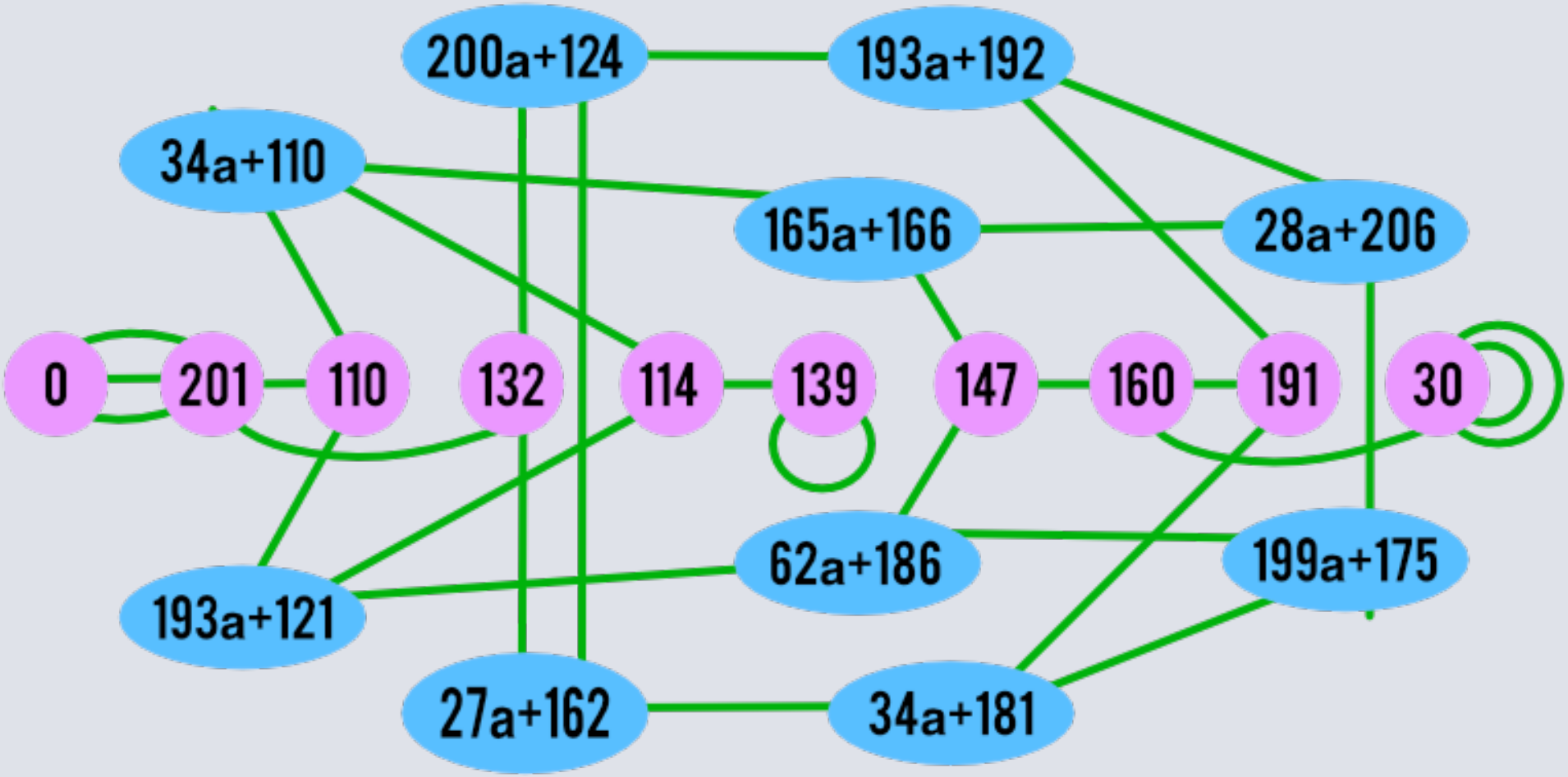
The mirror involution



The mirror involution

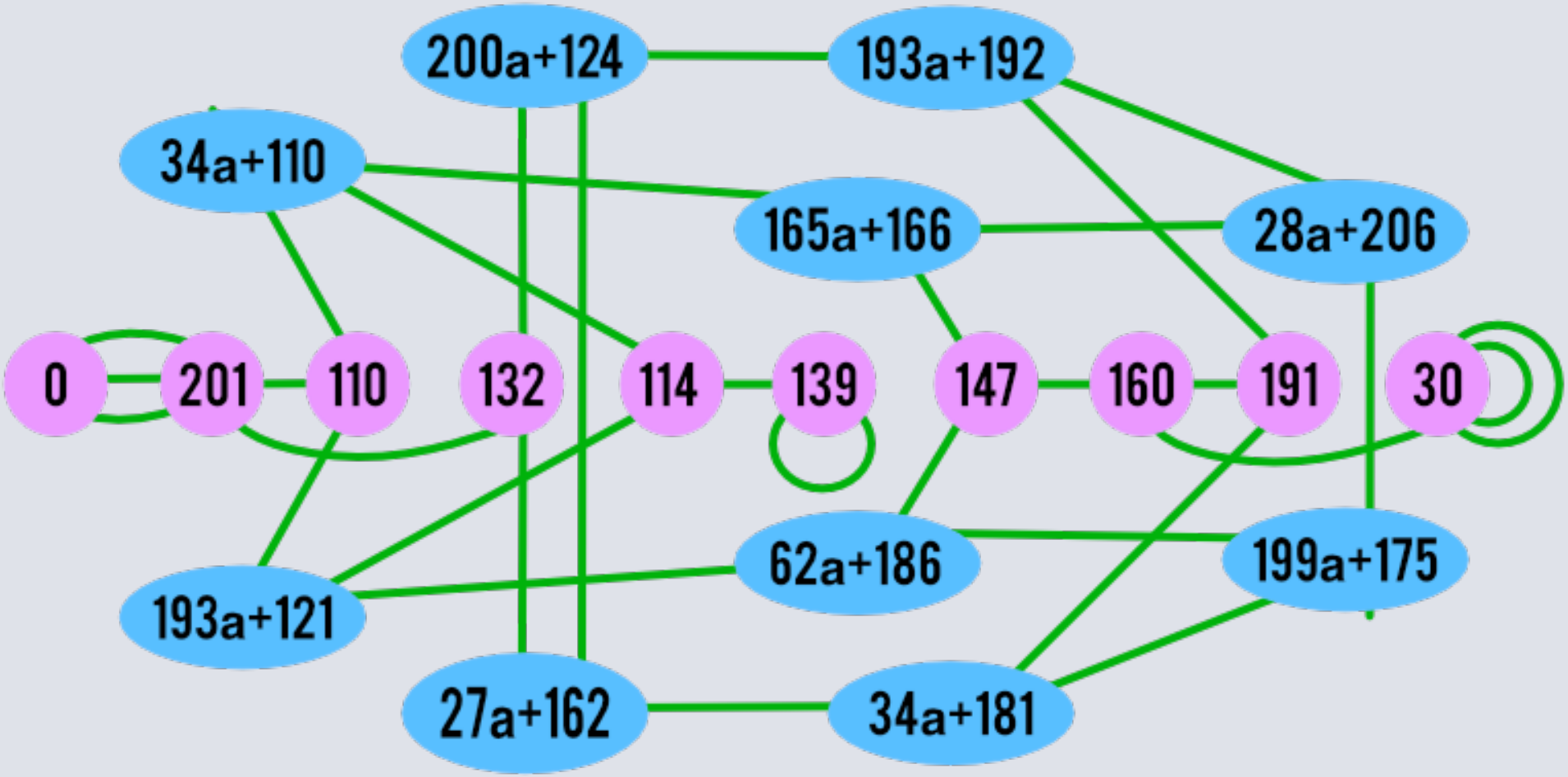
$E : y^2 = x^3 + Ax + B \quad \Leftrightarrow \quad E^{(p)} : y^2 = x^3 + A^p x + B^p$

is supersingular — is supersingular

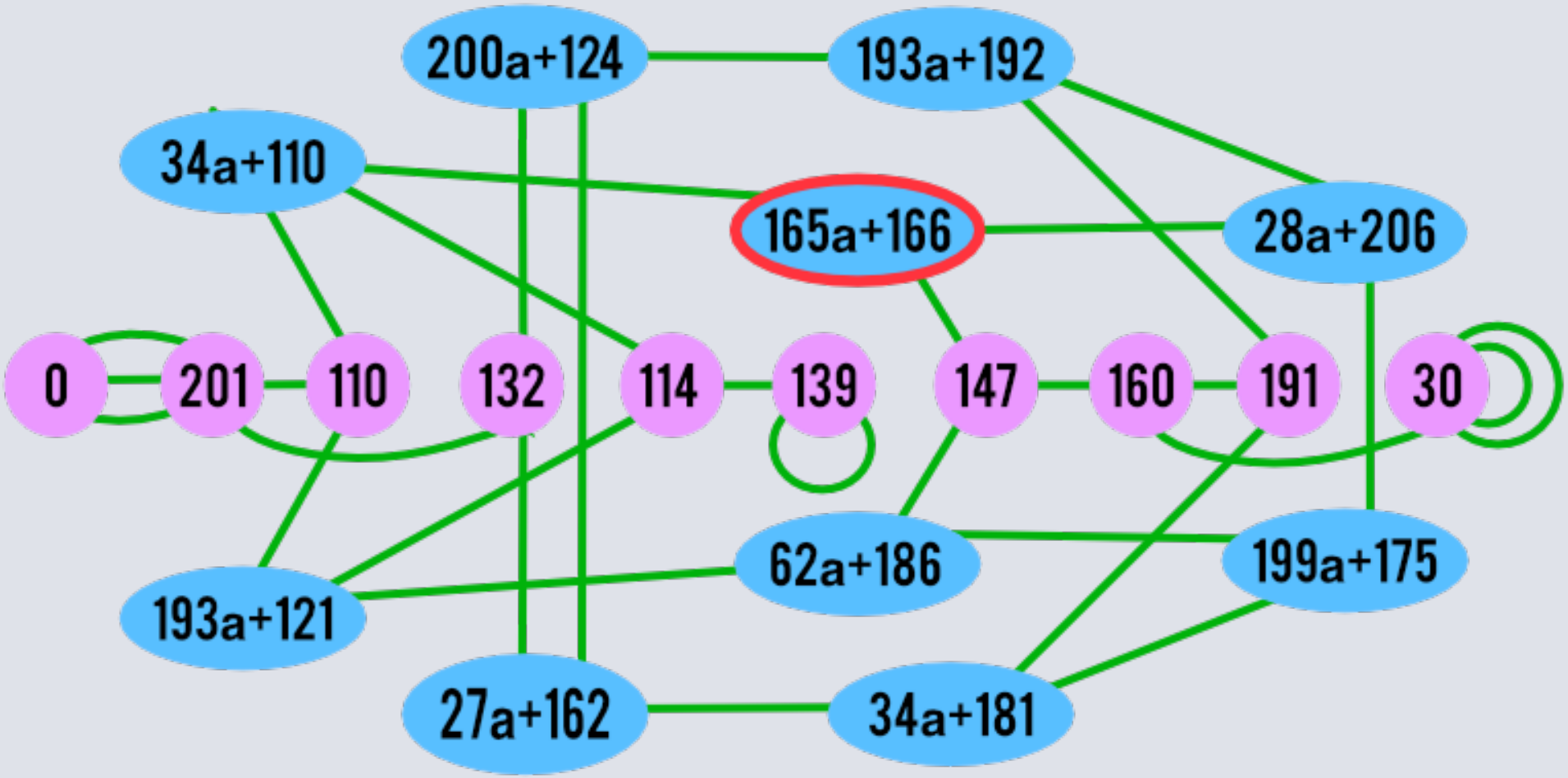


The mirror involution

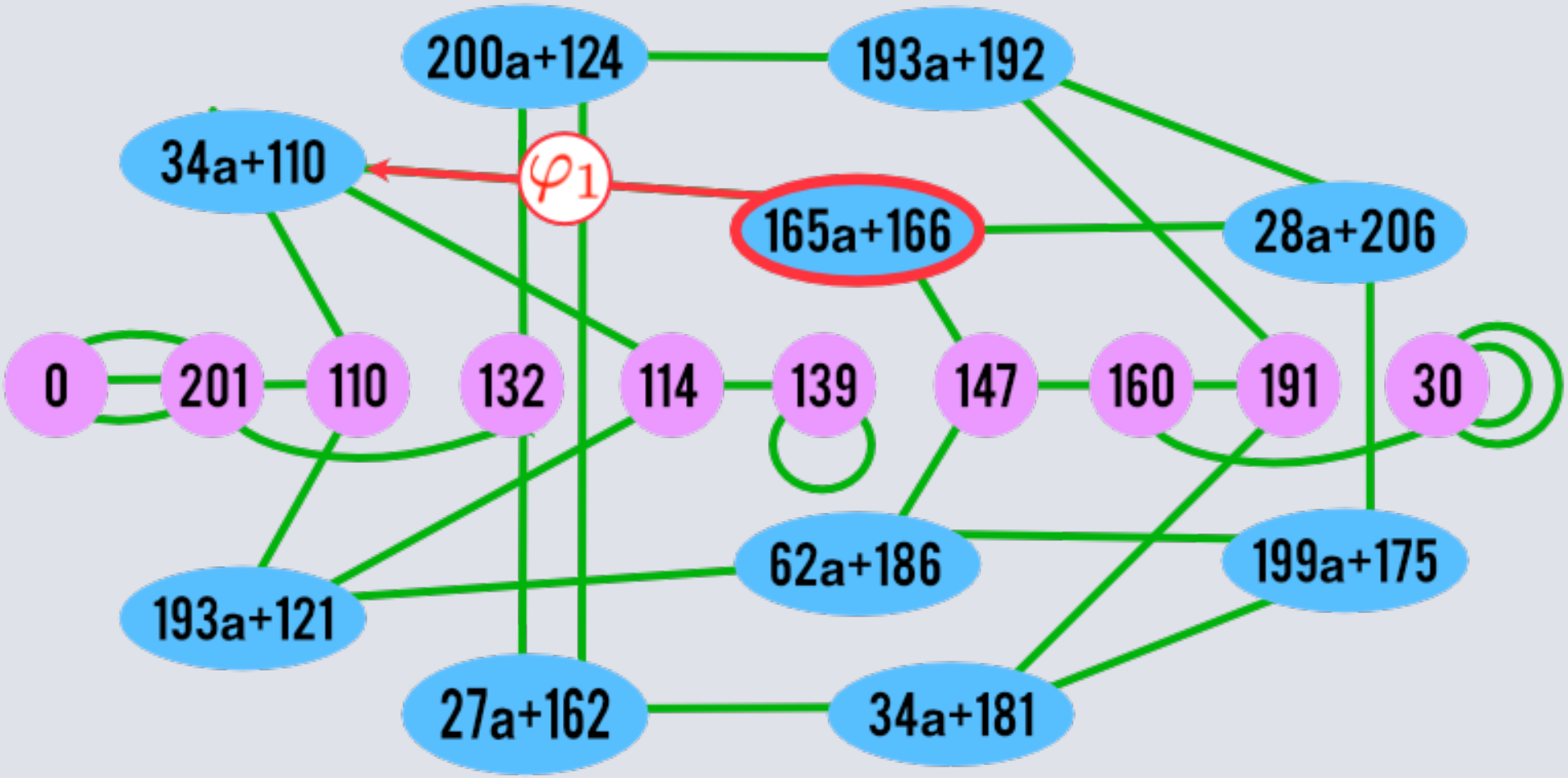
$$\varphi : E_1 \to E_2,\ \deg(\varphi) = \ell \quad \Leftrightarrow \quad \varphi^{(p)} : E_1^{(p)} \to E_2^{(p)},\ \deg(\varphi^{(p)}) = \ell$$



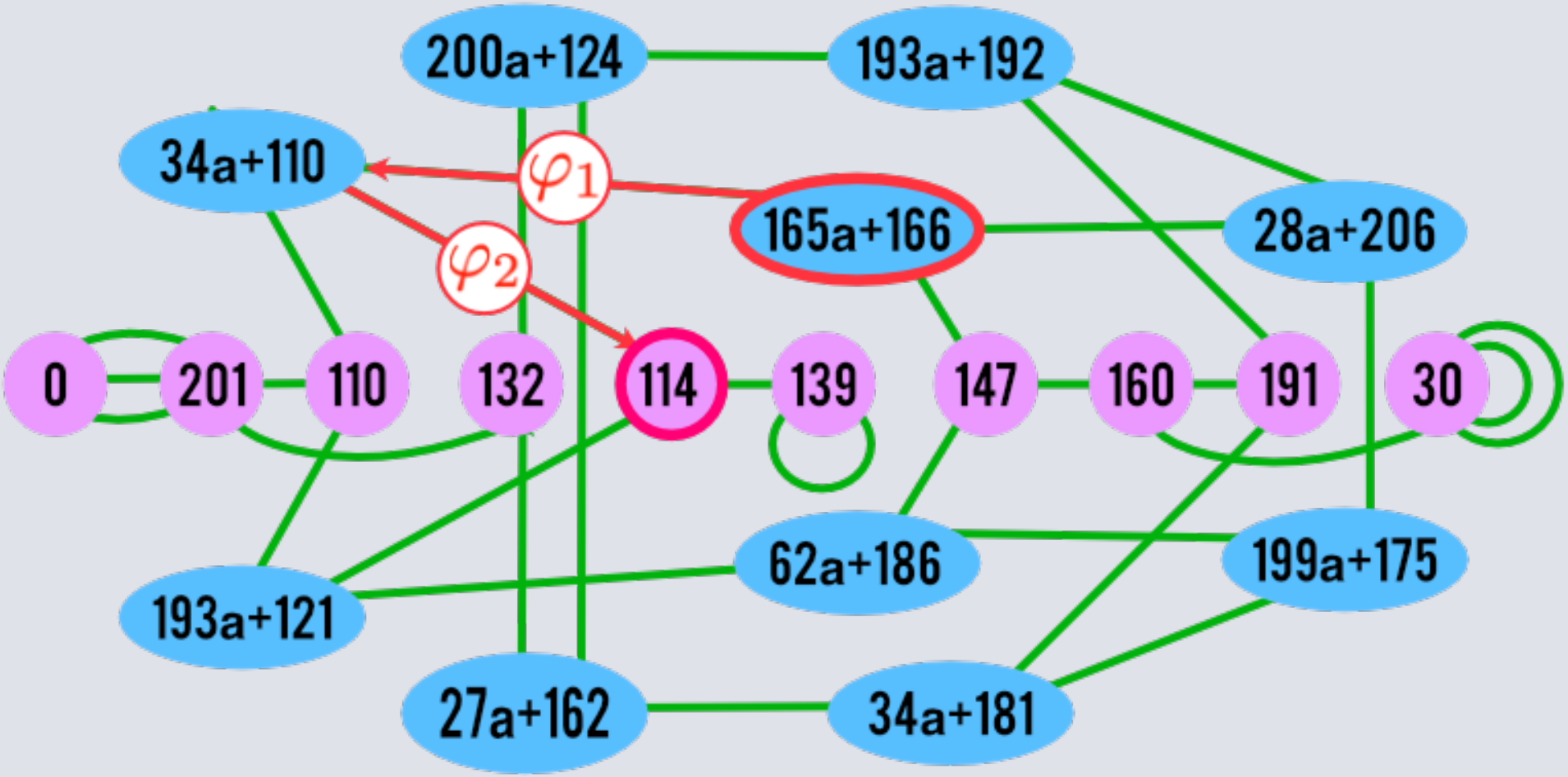
Finding cycles in the graph (Eisenträger et al.)



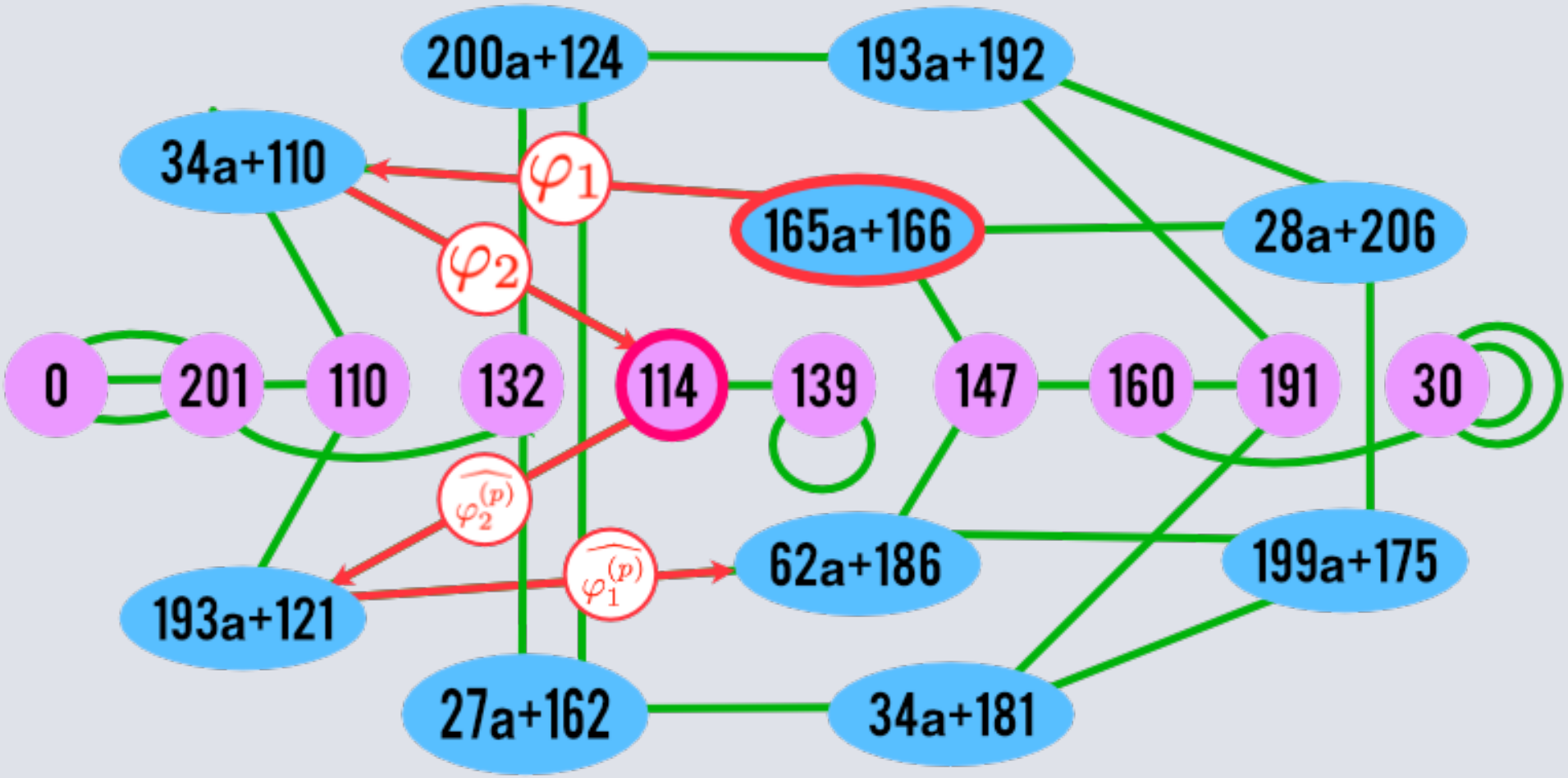
Finding cycles in the graph (Eisenträger et al.)



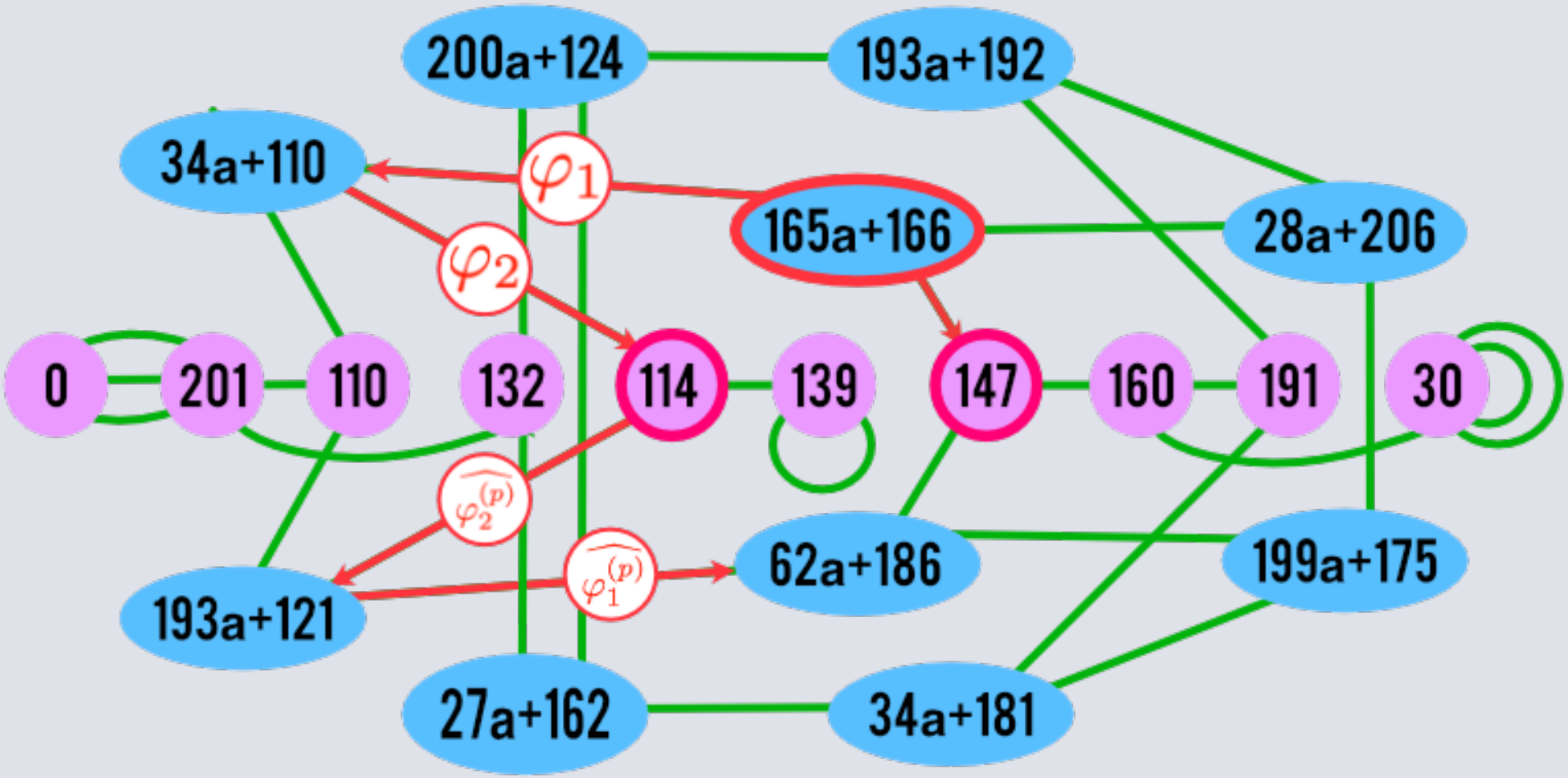
Finding cycles in the graph (Eisenträger et al.)



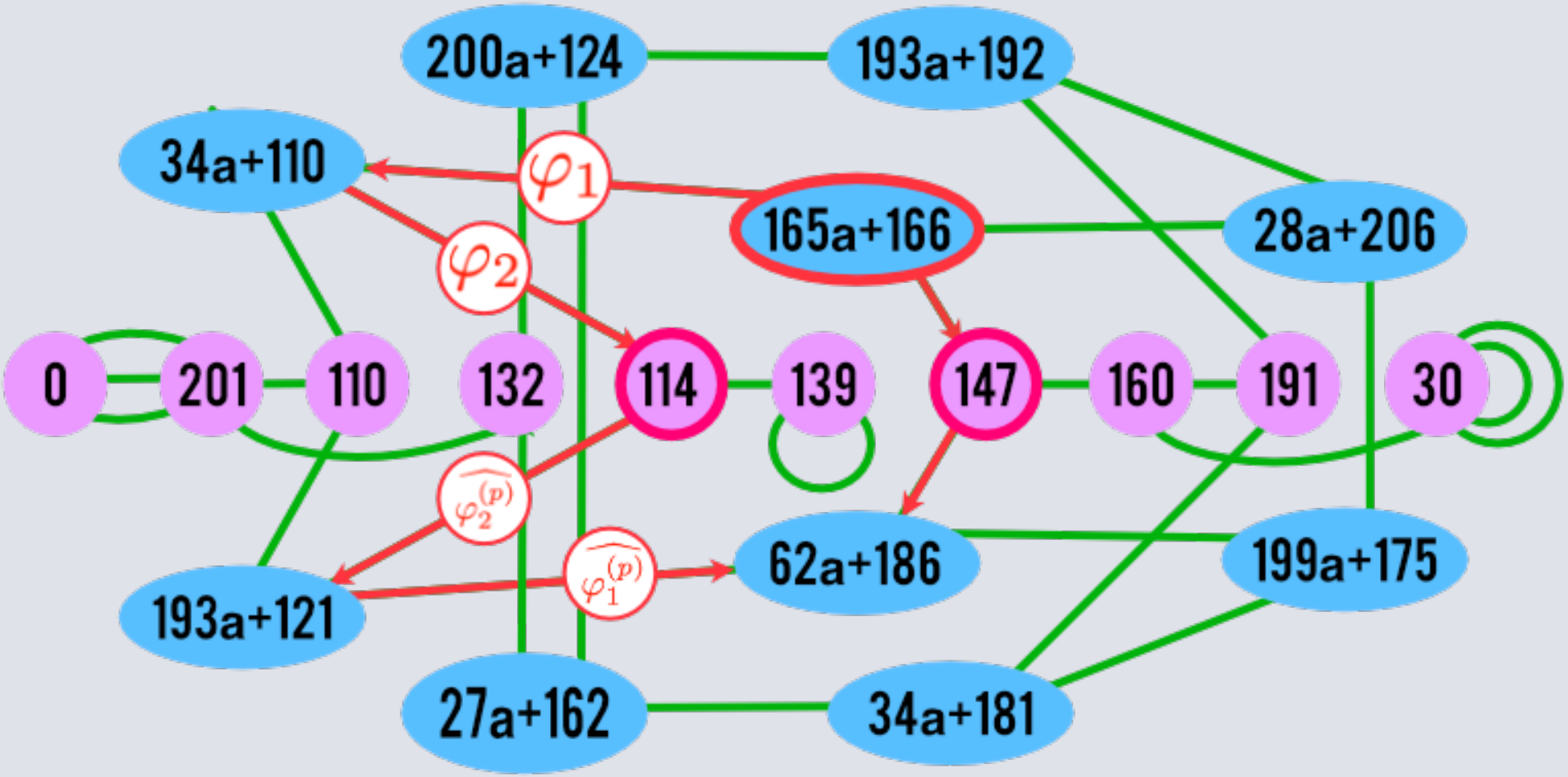
Finding cycles in the graph (Eisenträger et al.)



Finding cycles in the graph (Eisenträger et al.)



Finding cycles in the graph (Eisenträger et al.)



Algorithm (Eisenträger et al.)

Algorithm (Eisenträger et al.)

1) Compute two cycles α, β through $j(E)$ in $G(p, \ell)$ using the mirror involution.

Algorithm (Eisenträger et al.)

1) Compute two cycles α, β through $j(E)$ in $G(p, \ell)$ using the mirror involution.
2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

Algorithm (Eisenträger et al.)

1) Compute two cycles α, β through $j(E)$ in $G(p, \ell)$ using the mirror involution.
2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

- α and β do not commute with probability $1 - O\left(\frac{1}{p}\right)$.
- Λ is Bass whenever the discriminants of α and β are coprime.
  Heuristic 1: the discriminants are distributed like random integers, which are coprime with probability $\frac{6}{\pi^2}$.

Algorithm (Eisenträger et al.)

1) Compute two cycles α, β through $j(E)$ in $G(p, \ell)$ using the mirror involution.

2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

   - α and β do not commute with probability $1 - O\left(\frac{1}{p}\right)$.
   - Λ is Bass whenever the discriminants of α and β are coprime.
     Heuristic 1: the discriminants are distributed like random integers, which are coprime with probability $\frac{6}{\pi^2}$.

3) If Λ is a Bass order, then enumerate the maximal orders containing Λ and check which one is isomorphic to $\mathrm{End}(E)$.

Algorithm (Eisenträger et al.)

1) Compute two cycles α, β through $j(E)$ in $G(p, \ell)$ using the mirror involution.

2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

   - α and β do not commute with probability $1 - O\left(\frac{1}{p}\right)$.
   - Λ is Bass whenever the discriminants of α and β are coprime.
     Heuristic 1: the discriminants are distributed like random integers, which are coprime with probability $\frac{6}{\pi^2}$.

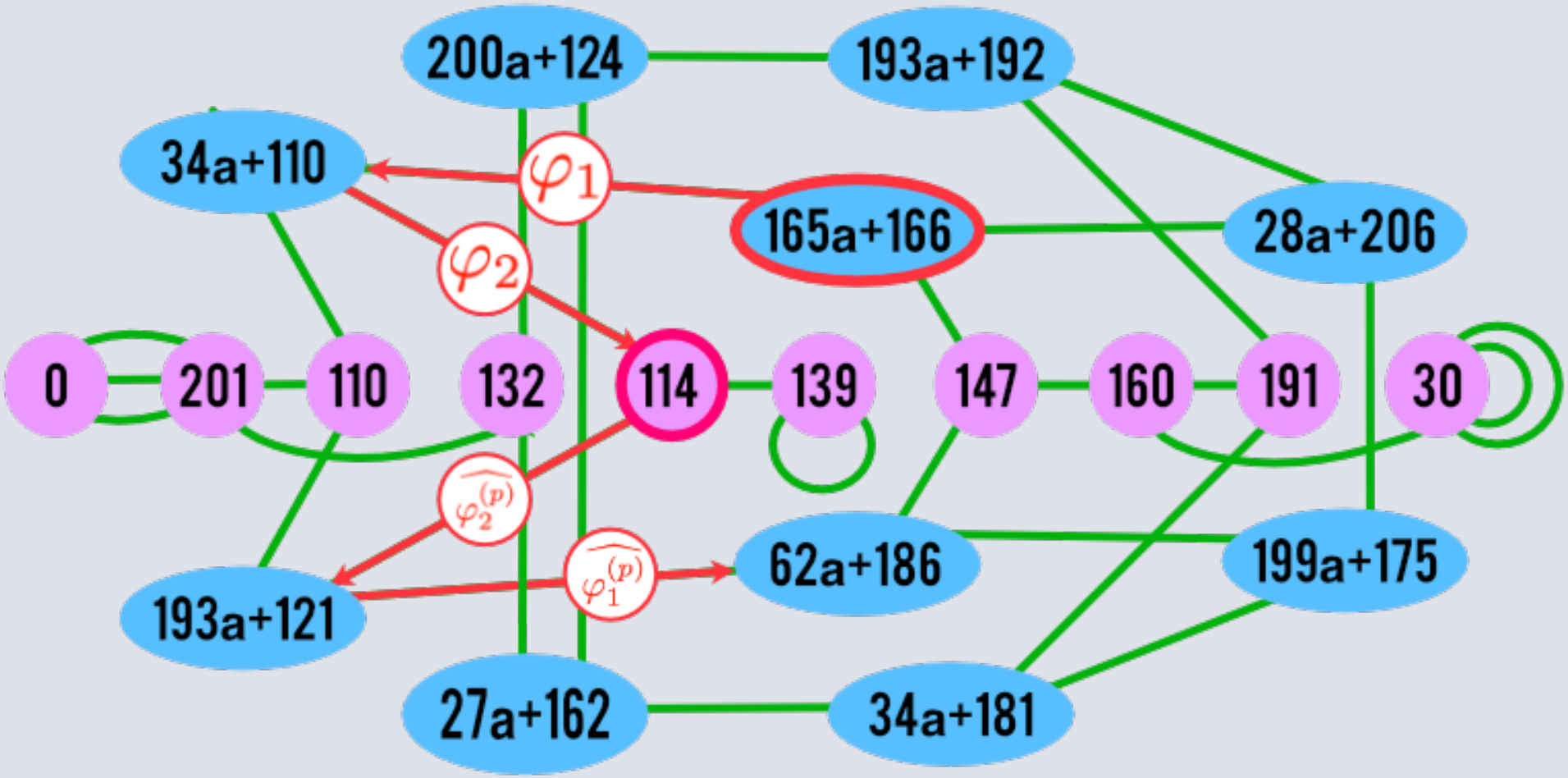
3) If Λ is a Bass order, then enumerate the maximal orders containing Λ and check which one is isomorphic to $\mathrm{End}(E)$.

Complexity: $O((\log p)^2\sqrt{p})$, under GRH and Heuristic 1.

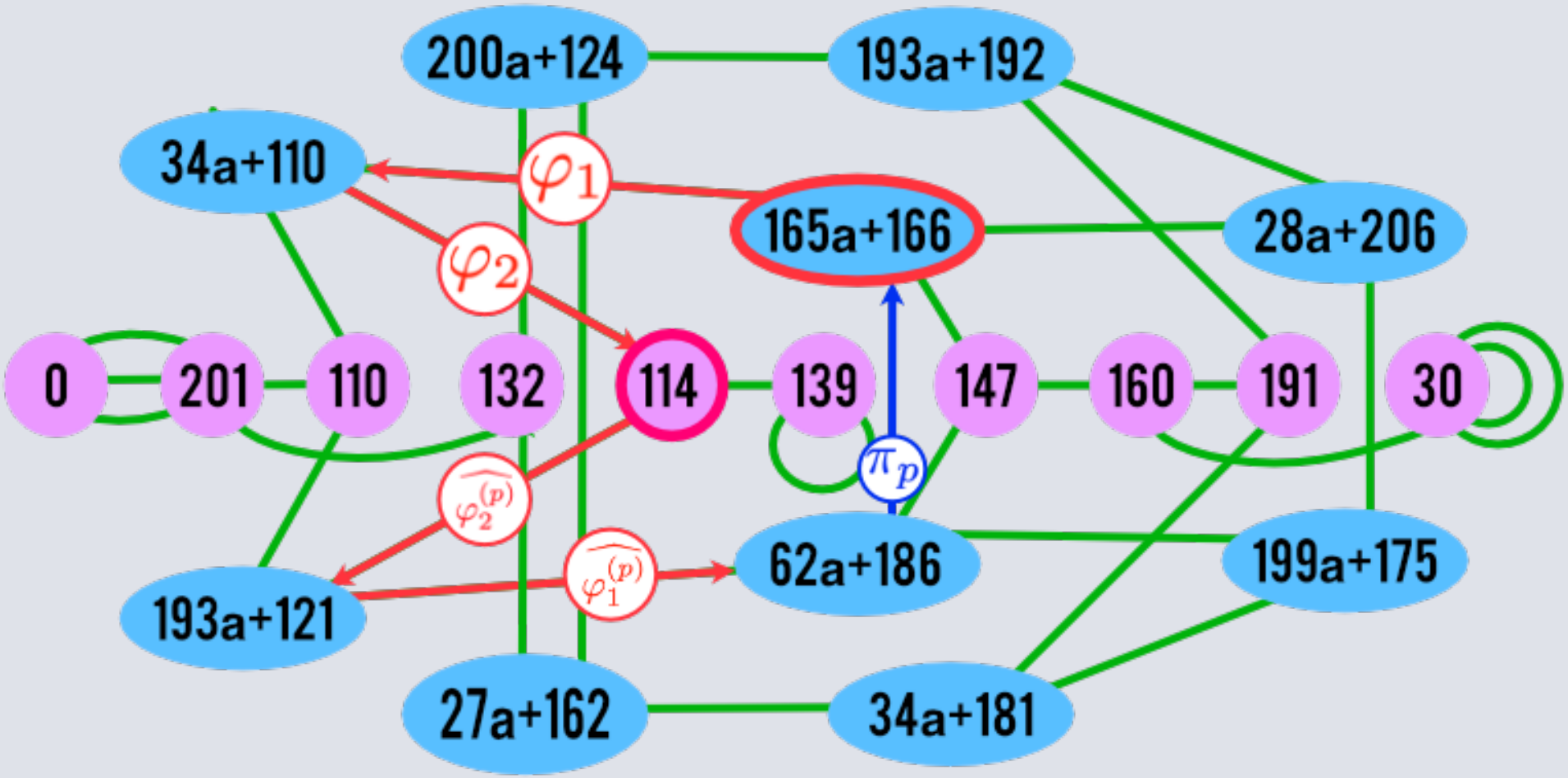
2025

J. Fuselier, A. I., M. Kozek, T. Morrison, and C. Namoijam
Computing supersingular endomorphism rings using inseparable endomorphisms.
Journal of Algebra, Volume 668, pp 145–189.

Finding cycles in the graph (our approach)

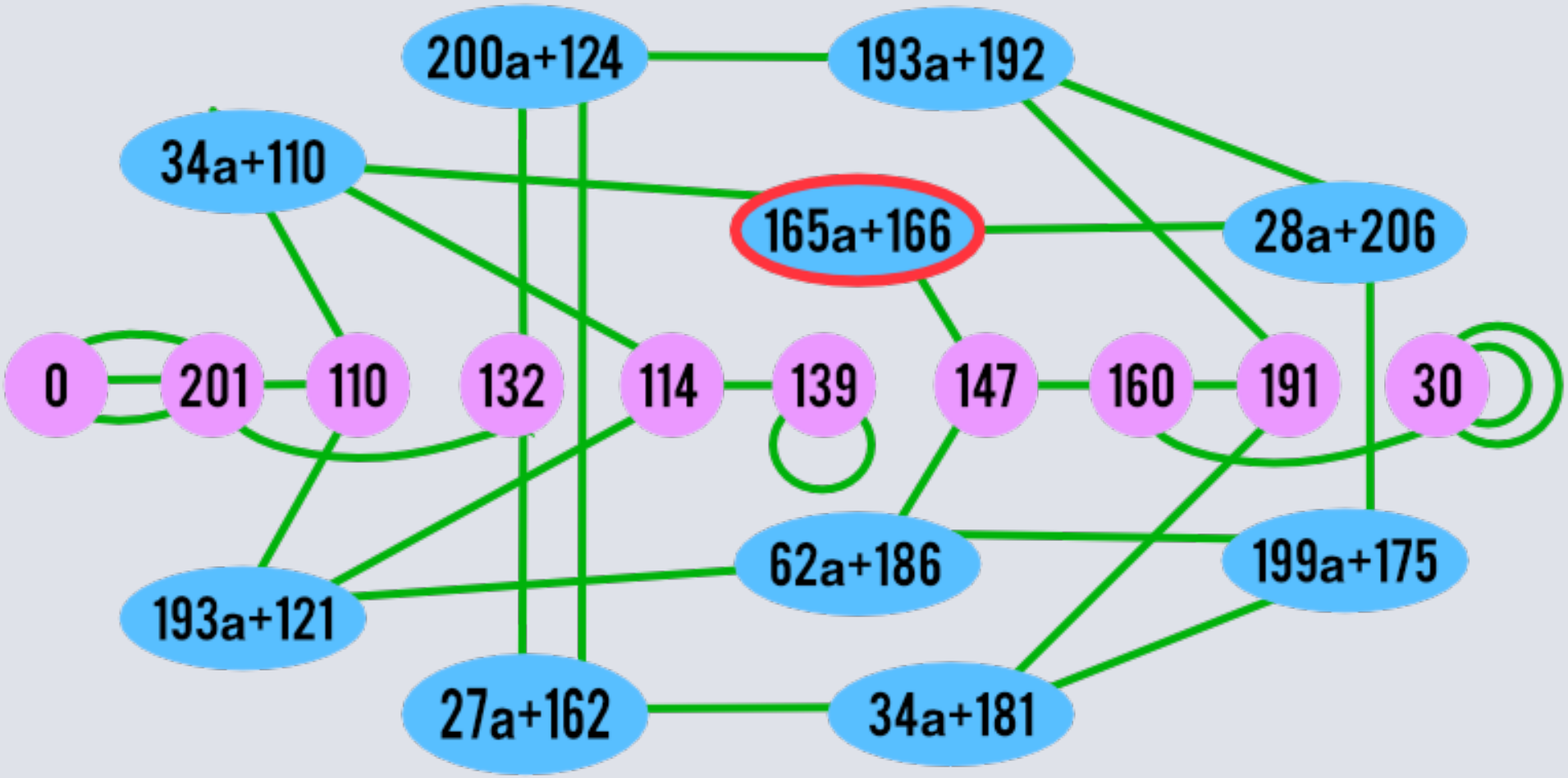


Finding cycles in the graph (our approach)

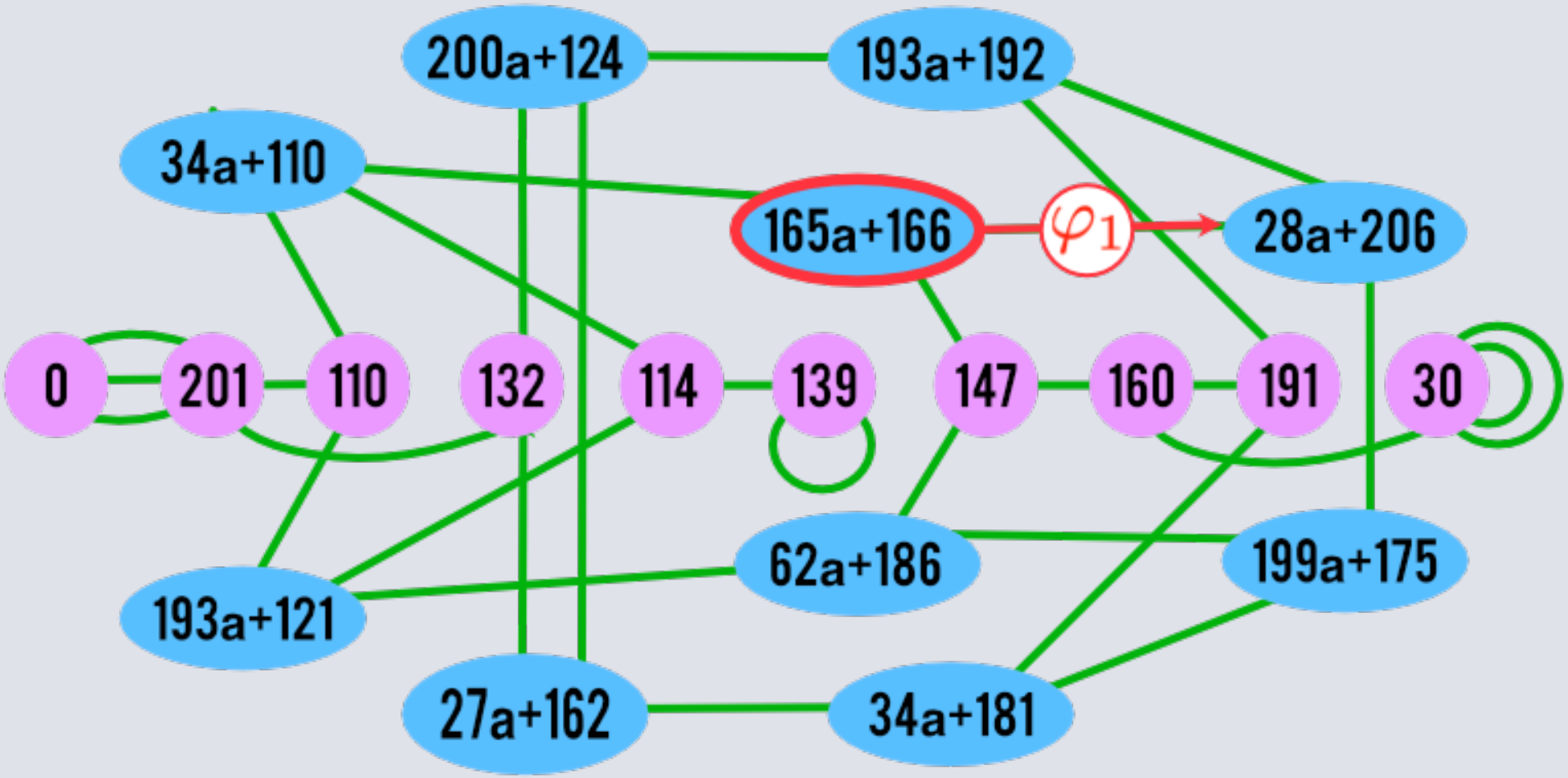


$$\pi_p : \begin{array}{ccc} E & \to & E^{(p)} \\ (x,y) & \mapsto & (x^p, y^p). \end{array}$$

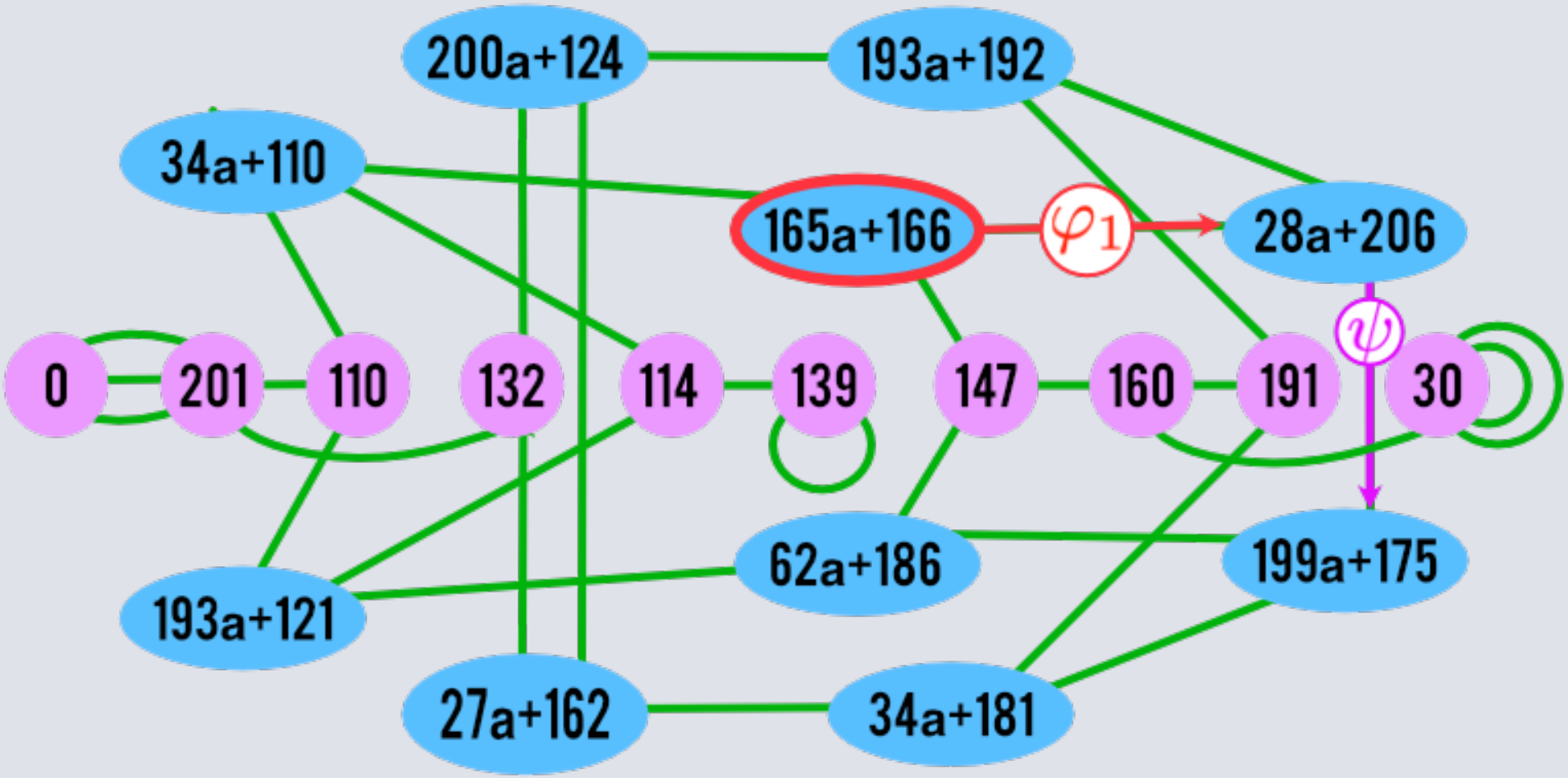
Finding cycles in the graph (our more general approach)



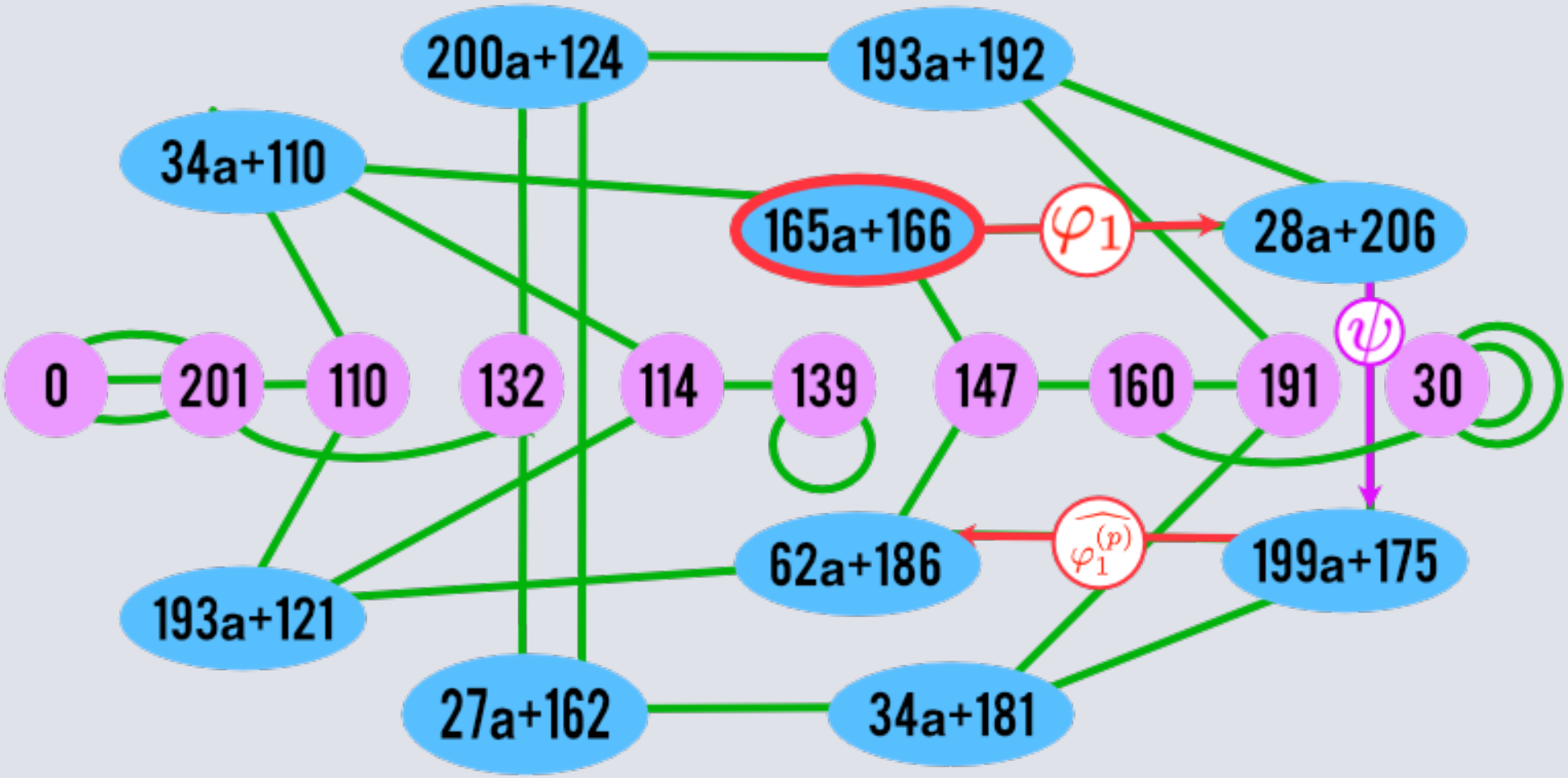
Finding cycles in the graph (our more general approach)



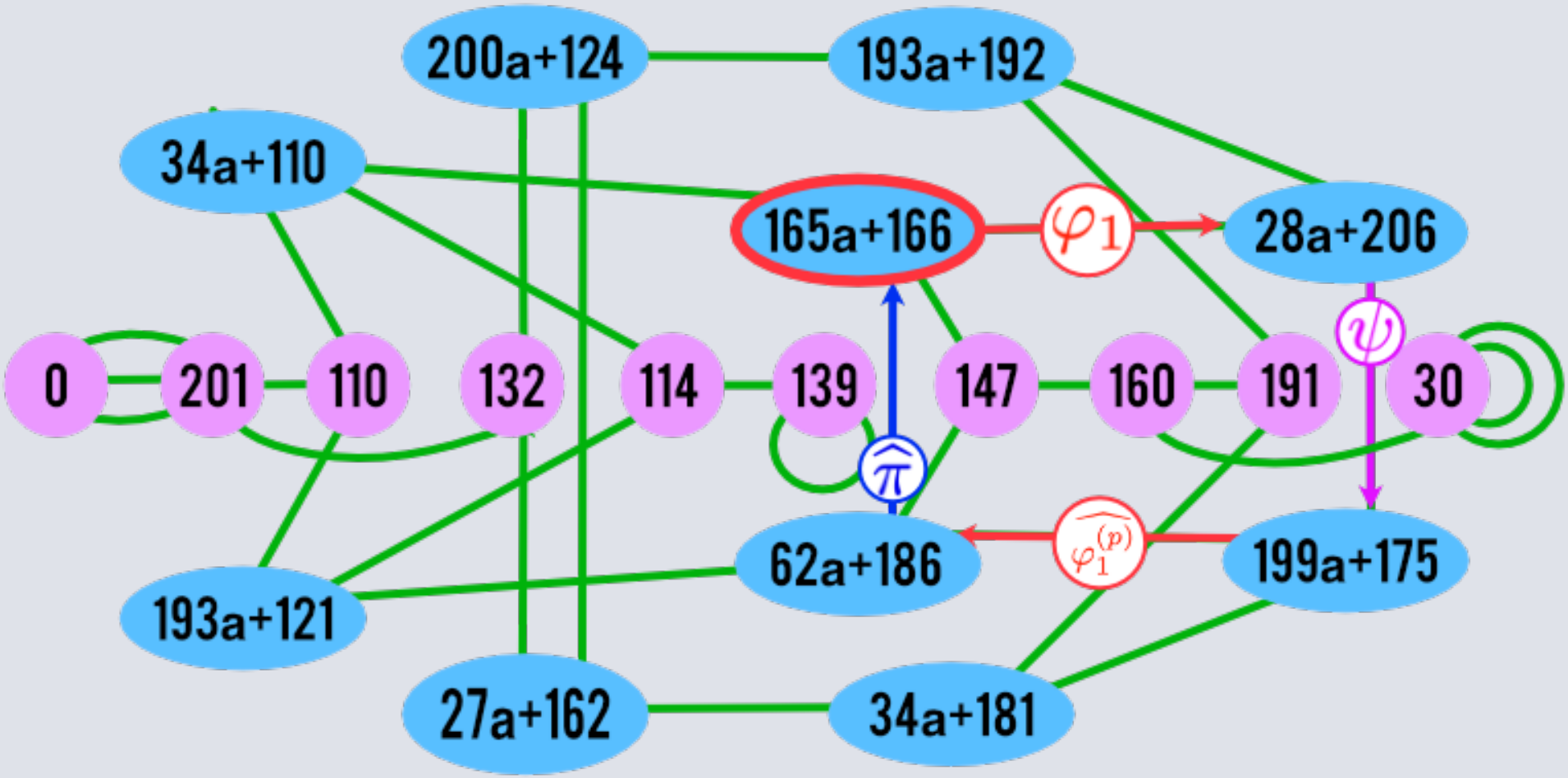
Finding cycles in the graph (our more general approach)



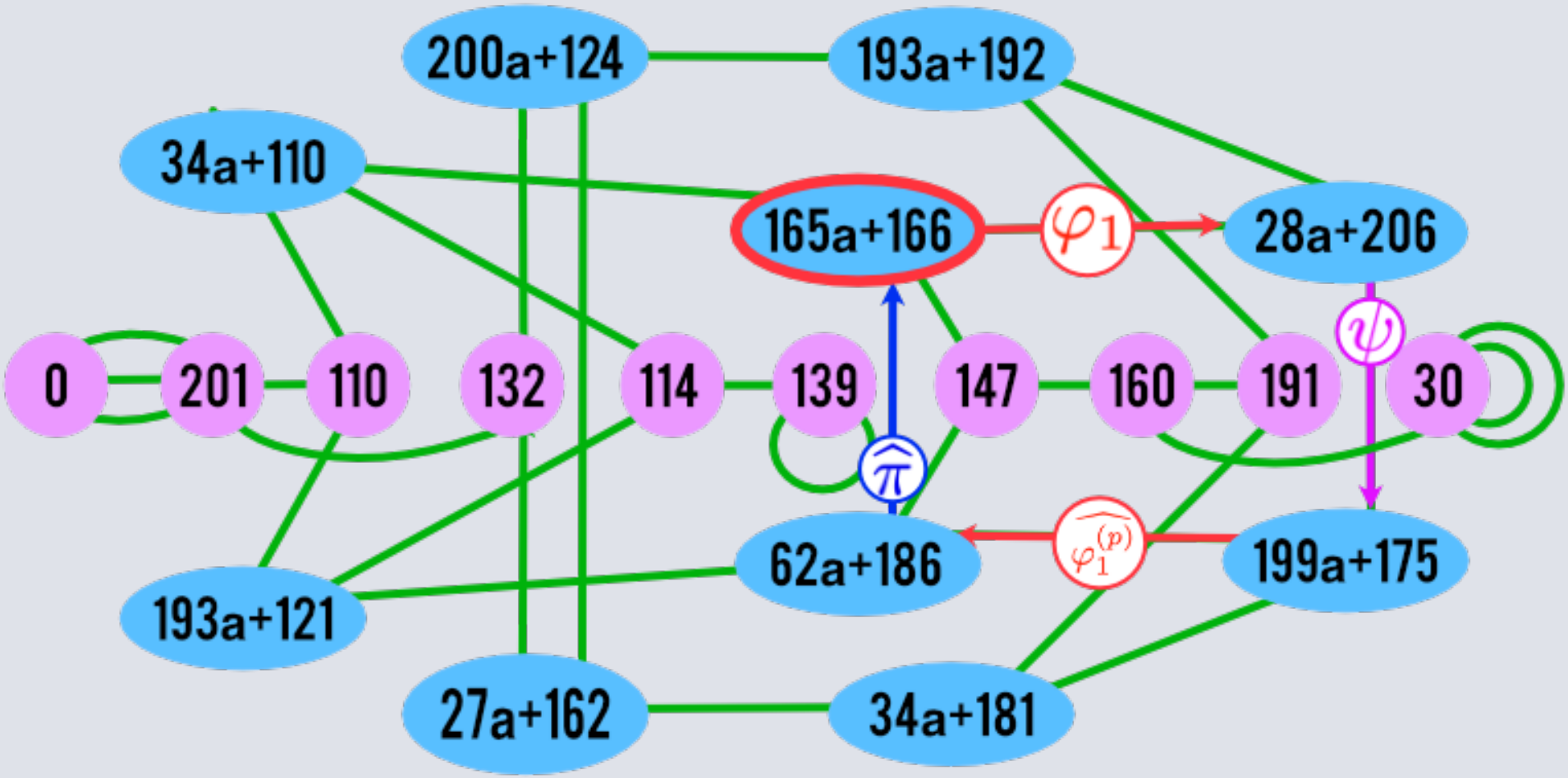
Finding cycles in the graph (our more general approach)



Finding cycles in the graph (our more general approach)

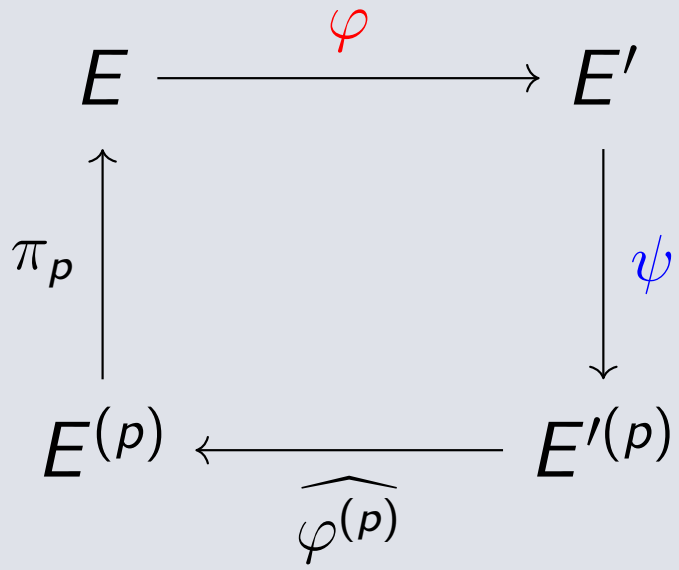


Finding cycles in the graph (our more general approach)

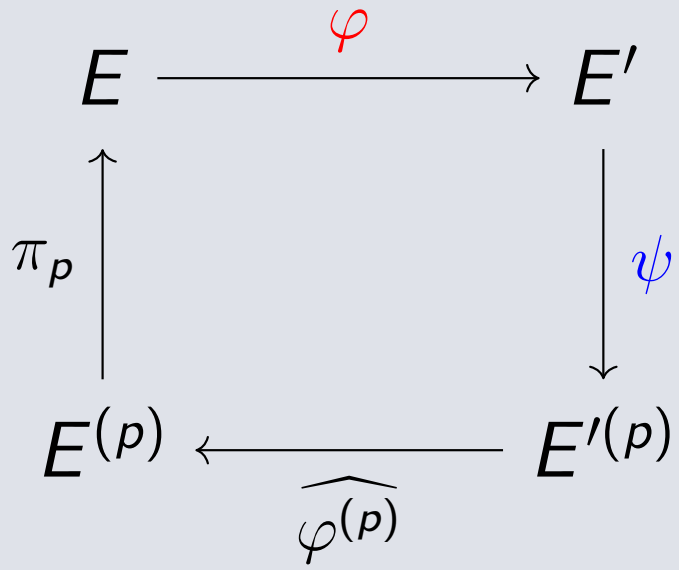


We call $\pi_p \circ \widehat{\varphi_1^{(p)}} \circ \psi \circ \varphi_1$ an *inseparable reflection*.

Inseparable reflections

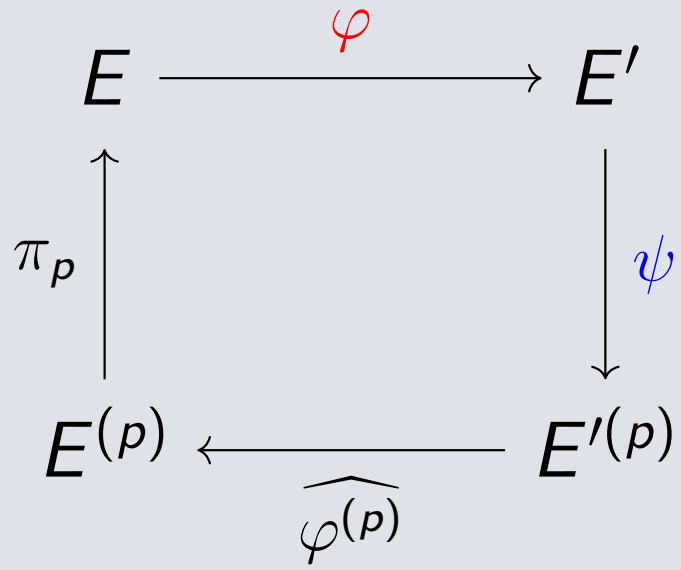


Inseparable reflections



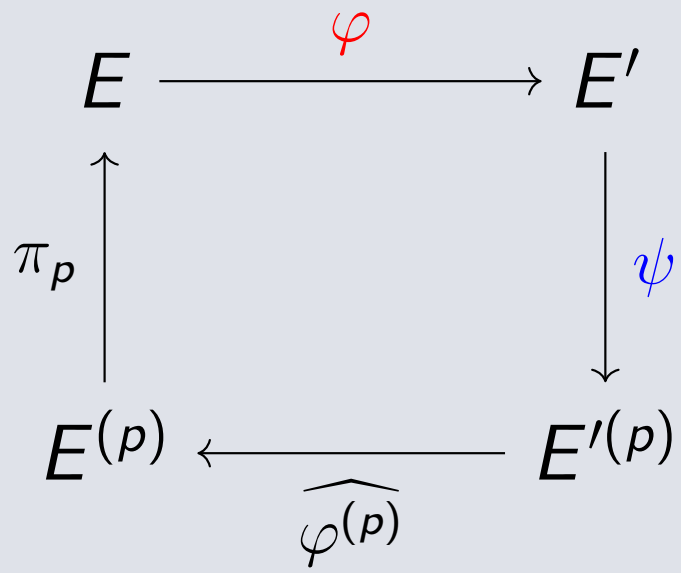
- $\varphi\colon E \to E'$ is a cyclic isogeny of degree ℓ^t,

Inseparable reflections



- $\varphi\colon E \to E'$ is a cyclic isogeny of degree ℓ^t,
- $\psi\colon E' \to E'^{(p)}$ is an isogeny of degree d,

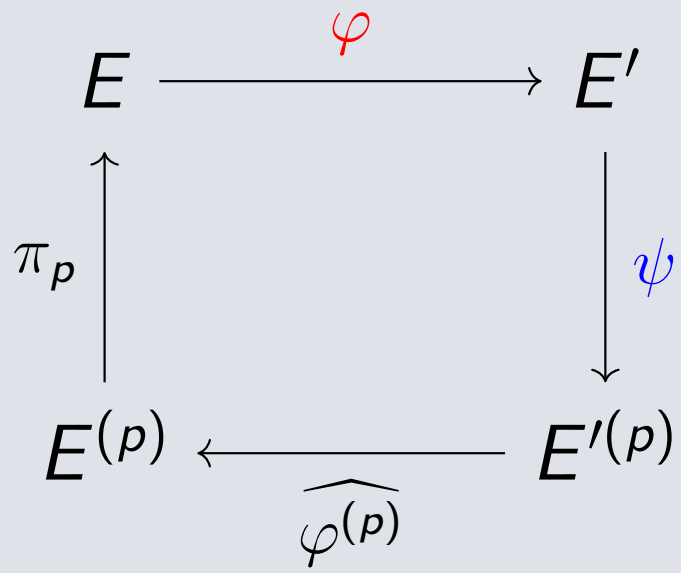
Inseparable reflections



- $\varphi\colon E \to E'$ is a cyclic isogeny of degree ℓ^t,
- $\psi\colon E' \to E'^{(p)}$ is an isogeny of degree d,

where ℓ is prime, and d is square-free and coprime with ℓ.

Inseparable reflections



- $\varphi\colon E \to E'$ is a cyclic isogeny of degree ℓ^t,
- $\psi\colon E' \to E'^{(p)}$ is an isogeny of degree d,

where ℓ is prime, and d is square-free and coprime with ℓ.

$$\alpha := \pi_p \circ \widehat{\varphi^{(p)}} \circ \psi \circ \varphi$$

is an **inseparable reflection** of degree $dp\ell^{2t}$.

Concretely, what do we do?

We take random walks of a given length t and for the endpoint E' we test whether $\Phi_d(j(E'), j(E')^p) = 0$.

Concretely, what do we do?

We take random walks of a given length t and for the endpoint E' we test whether $\Phi_d(j(E'), j(E')^p) = 0$.

How many supersingular j-invariant are d-isogenous to their Galois conjugate?

Concretely, what do we do?

We take random walks of a given length t and for the endpoint E' we test whether $\Phi_d(j(E'), j(E')^p) = 0$.

How many supersingular j-invariant are d-isogenous to their Galois conjugate?

Let X be the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ which are d-isogenous to their Galois conjugate.

Concretely, what do we do?

We take random walks of a given length t and for the endpoint E' we test whether $\Phi_d(j(E'), j(E')^p) = 0$.

How many supersingular j-invariant are d-isogenous to their Galois conjugate?

Let X be the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ which are d-isogenous to their Galois conjugate.
Then

$$X \approx h_K, \quad \text{où } K = \mathbb{Q}(\sqrt{-pd}),$$

Concretely, what do we do?

We take random walks of a given length t and for the endpoint E' we test whether $\Phi_d(j(E'), j(E')^p) = 0$.

How many supersingular j-invariant are d-isogenous to their Galois conjugate?

Let X be the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ which are d-isogenous to their Galois conjugate.
Then

$$X \approx h_K, \quad \text{où } K = \mathbb{Q}(\sqrt{-pd}),$$

and, under GRH,

$$h_K = \Omega(\sqrt{p}/\log\log(p)).$$

Cost for finding an endomorphism

Cost for finding an endomorphism

One can show that the probability that a non-backtracking walk of a certain length t lands in X is

$$\Omega\left(\frac{1}{\sqrt{p}\log\log(p)}\right).$$

Cost for finding an endomorphism

One can show that the probability that a non-backtracking walk of a certain length t lands in X is

$$\Omega\left(\frac{1}{\sqrt{p}\log\log(p)}\right).$$

Multiplying the expected number of walks by the expected number of bit operations per walk, one gets a total cost for computing a non trivial endomorphism of

$$O(\sqrt{p}(\log p)^2(\log\log p)^3).$$

Cost for finding an endomorphism

One can show that the probability that a non-backtracking walk of a certain length t lands in X is

$$\Omega\left(\frac{1}{\sqrt{p}\log\log(p)}\right).$$

Multiplying the expected number of walks by the expected number of bit operations per walk, one gets a total cost for computing a non trivial endomorphism of

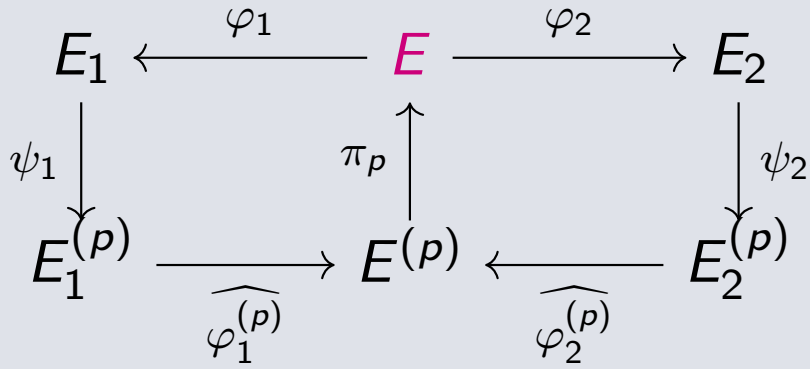
$$O(\sqrt{p}(\log p)^2(\log\log p)^3).$$

Storage: $O((\log p)^2)$.

Properties of inseparable reflections

Assume we have

$\alpha := \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1$



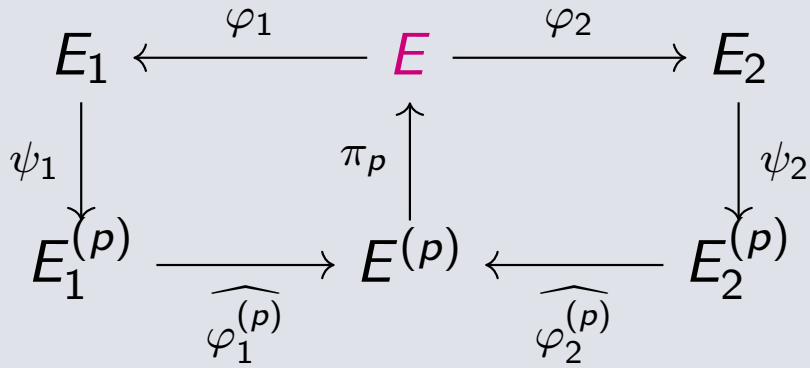
$\beta := \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2$

two inseparable reflections of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$.

Properties of inseparable reflections

Assume we have

$\alpha := \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1$



$\beta := \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2$

two inseparable reflections of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$.

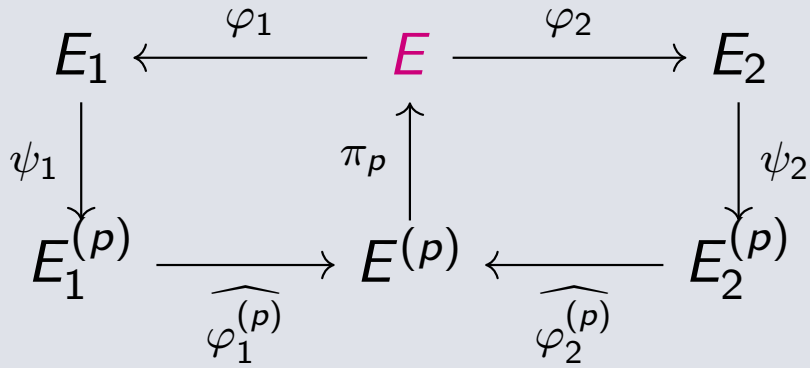
Theorem (Fuselier, I., Kozek, Morrison and Namoijam)

Assume that d, ℓ_1, ℓ_2 are three pairwise coprime integers, with d square-free and such that $-dp \not\equiv 1 \pmod 4$.
Then

Properties of inseparable reflections

Assume we have

$\alpha := \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1$



$\beta := \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2$

two inseparable reflections of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$.

Theorem (Fuselier, I., Kozek, Morrison and Namoijam)

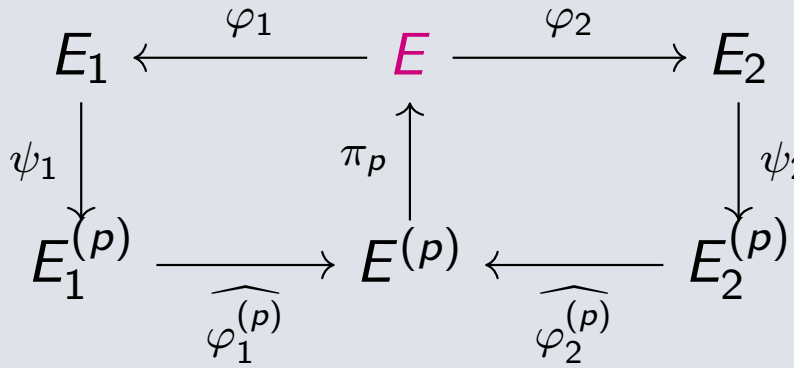
Assume that d, ℓ_1, ℓ_2 are three pairwise coprime integers, with d square-free and such that $-dp \not\equiv 1 \pmod 4$.
Then

- *α and β do not commute.*

Properties of inseparable reflections

Assume we have

$\alpha := \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1$



$\beta := \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2$

two inseparable reflections of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$.

Theorem (Fuselier, I., Kozek, Morrison and Namoijam)

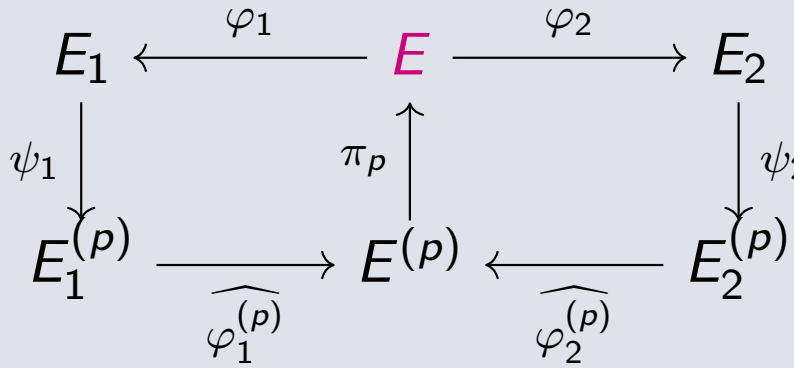
Assume that d, ℓ_1, ℓ_2 are three pairwise coprime integers, with d square-free and such that $-dp \not\equiv 1 \pmod 4$.
Then

- *α and β do not commute.*
- *the endomorphisms $1, \alpha, \beta, \alpha\beta$ generate a suborder of $\mathrm{End}(E)$ and this suborder is Bass.*

Properties of inseparable reflections

Assume we have

$\alpha := \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1$



$\beta := \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2$

two inseparable reflections of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$.

Theorem (Fuselier, I., Kozek, Morrison and Namoijam)

Assume that d, ℓ_1, ℓ_2 are three pairwise coprime integers, with d square-free and such that $-dp \not\equiv 1 \pmod 4$ (e.g. d=2).
Then

- *α and β do not commute.*
- *the endomorphisms $1, \alpha, \beta, \alpha\beta$ generate a suborder of $\mathrm{End}(E)$ and this suborder is Bass.*

Our algorithm

1) Set

$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$

Our algorithm

1) Set

$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$

and compute **two inseparable reflections** of E

$$\alpha = \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1, \qquad \beta = \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2,$$

of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$

Our algorithm

1) Set

$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$

and compute **two inseparable reflections** of E

$$\alpha = \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1, \qquad \beta = \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2,$$

of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$

2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

Our algorithm

1) Set
$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$
and compute **two inseparable reflections** of E
$$\alpha = \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1, \qquad \beta = \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2,$$
of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$
2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

By our theorem Λ is a Bass order.

Our algorithm

1) Set
$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$
and compute **two inseparable reflections** of E
$$\alpha = \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1, \qquad \beta = \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2,$$
of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$

2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

   By our theorem Λ is a Bass order.

3) Enumerate the maximal orders containing Λ and check which one is isomorphic to $\mathrm{End}(E)$.

Our algorithm

1) Set
$$\ell_1 = 3,\ \ell_2 = 5 \text{ and } d = 2$$
and compute **two inseparable reflections** of E
$$\alpha = \pi_p \widehat{\varphi_1^{(p)}} \psi_1 \varphi_1, \qquad \beta = \pi_p \widehat{\varphi_2^{(p)}} \psi_2 \varphi_2,$$
of degree respectively $dp\ell_1^{2t_1}$ and $dp\ell_2^{2t_2}$

2) Set $\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$.

   By our theorem Λ is a Bass order.

3) Enumerate the maximal orders containing Λ and check which one is isomorphic to $\mathrm{End}(E)$.

Complexity: $O(\sqrt{p}(\log p)^2(\log\log p)^3)$, under GRH.

2nd approach:

2nd approach:

Compute endomorphisms of E until finding a generating set of $\mathrm{End}(E)$.

Our inseparable reflections will never generate $\mathrm{End}(E)$ since they all live inside the ideal of inseparable endomorphisms:

$$P := \pi_p \circ \mathrm{Hom}(E, E^{(p)}).$$

Our inseparable reflections will never generate $\mathrm{End}(E)$ since they all live inside the ideal of inseparable endomorphisms:

$$P := \pi_p \circ \mathrm{Hom}(E, E^{(p)}).$$

This is the (unique) two-sided ideal in $\mathrm{End}(E)$ of norm p.

An interesting suborder

Let us consider $\mathbb{Z} + P$.

An interesting suborder

Let us consider $\mathbb{Z} + P$.

Proposition

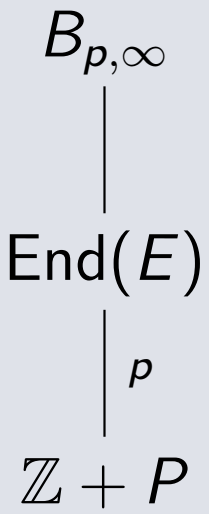
$\mathbb{Z} + P$ is a sub-order of $\mathrm{End}(E)$ *of index p and* $\mathrm{End}(E)$ *is the unique maximal order that contains $\mathbb{Z} + P$.*

An interesting suborder

Let us consider $\mathbb{Z} + P$.

Proposition

$\mathbb{Z} + P$ is a sub-order of $\mathrm{End}(E)$ of index p and $\mathrm{End}(E)$ is the unique maximal order that contains $\mathbb{Z} + P$.

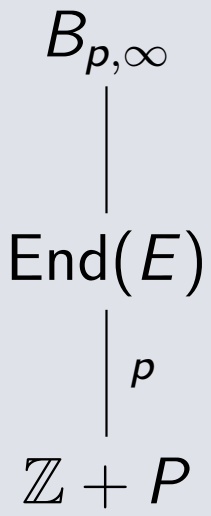


An interesting suborder

Let us consider $\mathbb{Z} + P$.

Proposition

$\mathbb{Z} + P$ is a sub-order of $\mathrm{End}(E)$ of index p and $\mathrm{End}(E)$ is the unique maximal order that contains $\mathbb{Z} + P$.



Note that $\mathrm{discrd}(\mathbb{Z} + P) = p^2$.

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$)

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set

$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set
$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$
2) While discrd(Λ) $\neq p^2$, find $\gamma \in P$ and set
$$\Lambda \leftarrow \Lambda + \gamma\mathbb{Z}.$$

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set
$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$
2) While discrd(Λ) $\neq p^2$, find $\gamma \in P$ and set
$$\Lambda \leftarrow \Lambda + \gamma\mathbb{Z}.$$

3) Now $\Lambda = \mathbb{Z} + P$. So compute the unique maximal order $\mathcal{O}$ which contains Λ (Voight, 2013).

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set
$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$
2) While discrd(Λ) $\neq p^2$, find $\gamma \in P$ and set
$$\Lambda \leftarrow \Lambda + \gamma\mathbb{Z}.$$

How many endomorphisms do we need to generate $\mathbb{Z} + P$?

3) Now $\Lambda = \mathbb{Z} + P$. So compute the unique maximal order $\mathcal{O}$ which contains Λ (Voight, 2013).

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set
$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$
2) While discrd(Λ) $\neq p^2$, find $\gamma \in P$ and set
$$\Lambda \leftarrow \Lambda + \gamma\mathbb{Z}.$$

How many endomorphisms do we need to generate $\mathbb{Z} + P$?

3) Now $\Lambda = \mathbb{Z} + P$. So compute the unique maximal order $\mathcal{O}$ which contains Λ (Voight, 2013).

Complexity: $O(\sqrt{p}(\log p)^2(\log\log p)^3)$ (under GRH), if we need not too many endomorphisms to generate $\mathbb{Z} + P$.

Computing End(E) from $\mathbb{Z} + P$

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$.
Output: The endormorphism ring End(E).

1) Find $\alpha, \beta \in P$ (inseparable reflections with $d = 1$, $\ell_1 = 2$ and $\ell_2 = 3$) and set
$$\Lambda = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}.$$
2) While discrd(Λ) $\neq p^2$, find $\gamma \in P$ and set
$$\Lambda \leftarrow \Lambda + \gamma\mathbb{Z}.$$

How many endomorphisms do we need to generate $\mathbb{Z} + P$?

3) Now $\Lambda = \mathbb{Z} + P$. So compute the unique maximal order $\mathcal{O}$ which contains Λ (Voight, 2013).

Complexity: $O(\sqrt{p}(\log p)^2(\log\log p)^3)$ (under GRH), if we need not too many endomorphisms to generate $\mathbb{Z} + P$.

Our implementation of this algorithm is available at https://github.com/travismo/inseparables.

How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

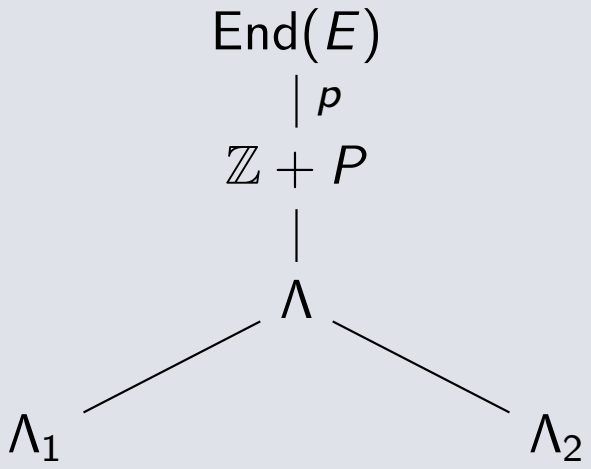
Let Λ be the order in $\mathrm{End}(E)$ generated by the bases of Λ_1, Λ_2.

How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

Let Λ be the order in $\mathrm{End}(E)$ generated by the bases of Λ_1, Λ_2.

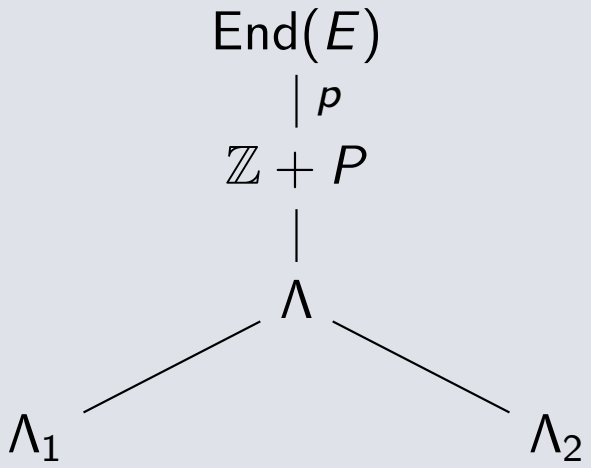


How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

Let Λ be the order in $\mathrm{End}(E)$ generated by the bases of Λ_1, Λ_2.



Therefore, if $\rho_1 = \frac{\alpha_1 \alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3 \alpha_4}{p}$,

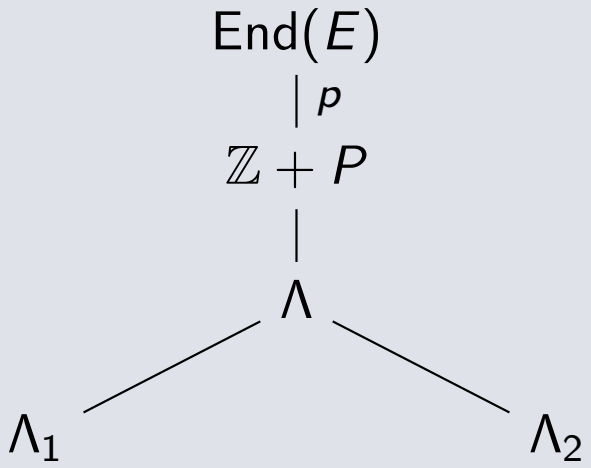
$$[\mathbb{Z} + P : \Lambda] \text{ divides } \gcd(\mathrm{disc}(\rho_1), \mathrm{disc}(\rho_2)).$$

How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

Let Λ be the order in $\mathrm{End}(E)$ generated by the bases of Λ_1, Λ_2.



Therefore, if $\rho_1 = \frac{\alpha_1 \alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3 \alpha_4}{p}$,

$$[\mathbb{Z} + P : \Lambda] \text{ divides } \gcd(\mathrm{disc}(\rho_1), \mathrm{disc}(\rho_2)).$$

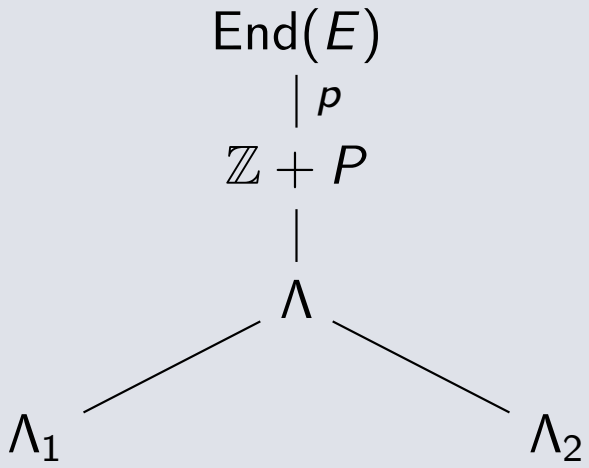
How often $\mathrm{disc}(\rho_1)$ **and** $\mathrm{disc}(\rho_2)$ **are coprime?**

How many endomorphisms do we need?

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be inseparable reflections of E. Consider

$$\Lambda_1 := \langle \alpha_1, \alpha_2 \rangle, \qquad \Lambda_2 := \langle \alpha_3, \alpha_4 \rangle.$$

Let Λ be the order in $\mathrm{End}(E)$ generated by the bases of Λ_1, Λ_2.

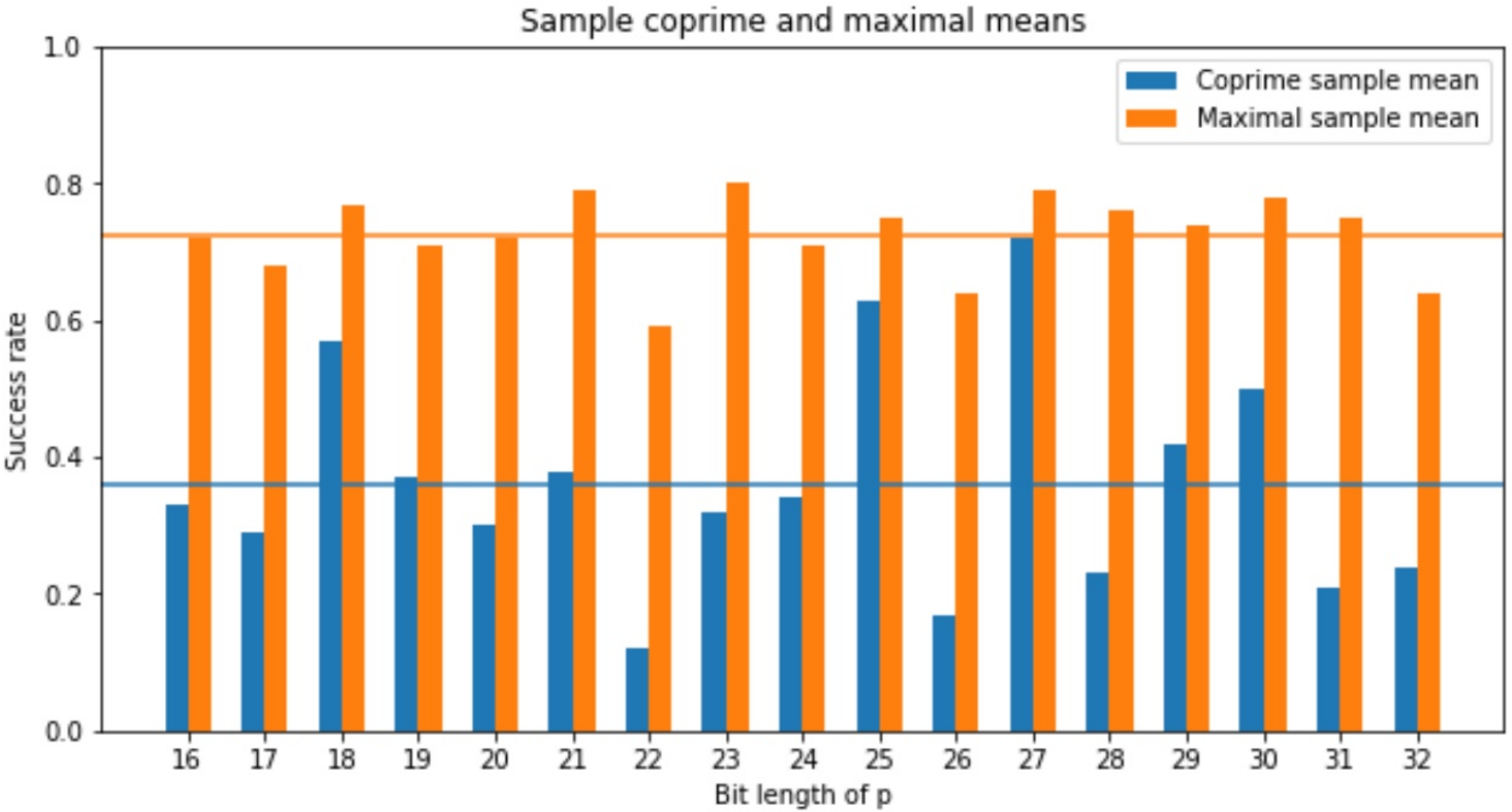


Therefore, if $\rho_1 = \frac{\alpha_1 \alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3 \alpha_4}{p}$,

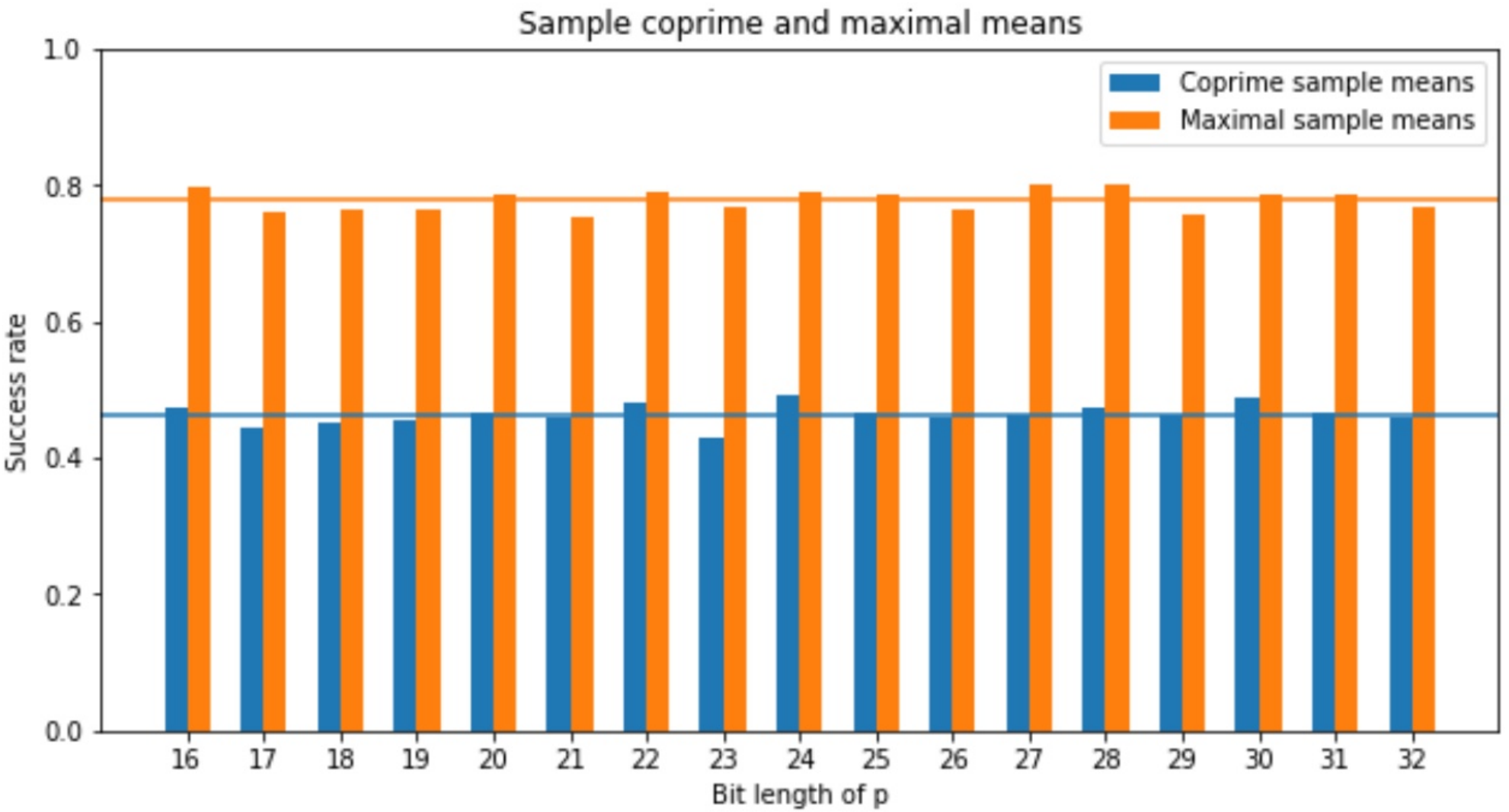
$$[\mathbb{Z} + P : \Lambda] \text{ divides } \gcd(\mathrm{disc}(\rho_1), \mathrm{disc}(\rho_2)).$$

How often $\mathrm{disc}(\rho_1)$ **and** $\mathrm{disc}(\rho_2)$ **are coprime?**
If their distribution was following the same distribution as two random integers, then they are coprime with probability approximately $6/\pi^2 \approx 0.6...$

Using 4 random inseparable reflections.



ρ_1 and ρ_2 sampled randomly in $\mathbb{Z} + P$.



More recent results about EndRing

2024 - A. Page and B. Wesolowski

The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent

Advances in Cryptology – EUROCRYPT 2024

▶ There is an unconditional probabilistic algorithm to solve the endomorphism ring problem in time $\tilde{\mathcal{O}}(\sqrt{p})$.

More recent results about EndRing

2024 - A. Page and B. Wesolowski

The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent

Advances in Cryptology – EUROCRYPT 2024

▶ There is an unconditional probabilistic algorithm to solve the endomorphism ring problem in time $\tilde{\mathcal{O}}(\sqrt{p})$.

2024 - K. Eisentraeger, G. Scullard

Connecting Kani's Lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings

Preprint

▶ They give a deterministic polynomial time algorithm to compute the endomorphism ring of a supersingular elliptic curve, provided that one is given two noncommuting endomorphisms and the factorization of the discriminant of the ring they generate.

More recent results about EndRing

2025 - M. Mukhopadhyay

Experimentally studying path-finding problem between conjugates in supersingular isogeny graphs: Optimizing primes and powers to speed-up cycle finding

Preprint

▶ They study the problem of finding a path between conjugate supersingular elliptic curves over $\mathbb{F}_{p^2}$.

More recent results about EndRing

2025 - M. Mukhopadhyay

Experimentally studying path-finding problem between conjugates in supersingular isogeny graphs: Optimizing primes and powers to speed-up cycle finding

Preprint

▶ They study the problem of finding a path between conjugate supersingular elliptic curves over $\mathbb{F}_{p^2}$.

2025 - M. Chen and C. Petit

Computing the endomorphism ring of a supersingular elliptic curve from a full rank suborder

Accepted at Eurocrypt 2025

▶ They study the problem of computing the endomorphism ring of a supersingular elliptic curve given the knowledge of a full rank suborder and provide a polynomial time quantum algorithm to solve it.

The End, thank you!