Explicit isogenies in quadratic time in any characteristic

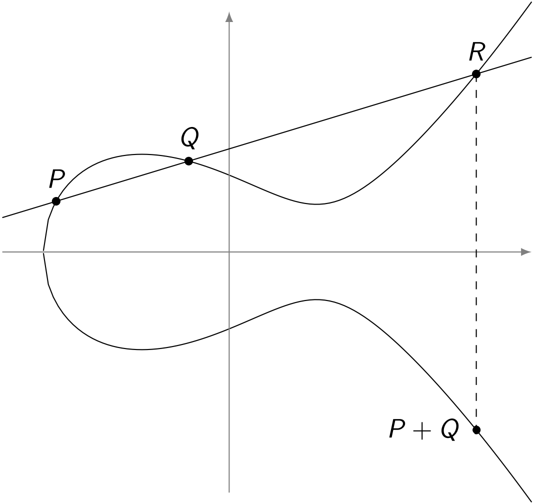
Luca De Feo
joint work with Cyril Hugounenq, Jérôme Plût, Éric Schost

Université de Neuchâtel

September 28, 2016

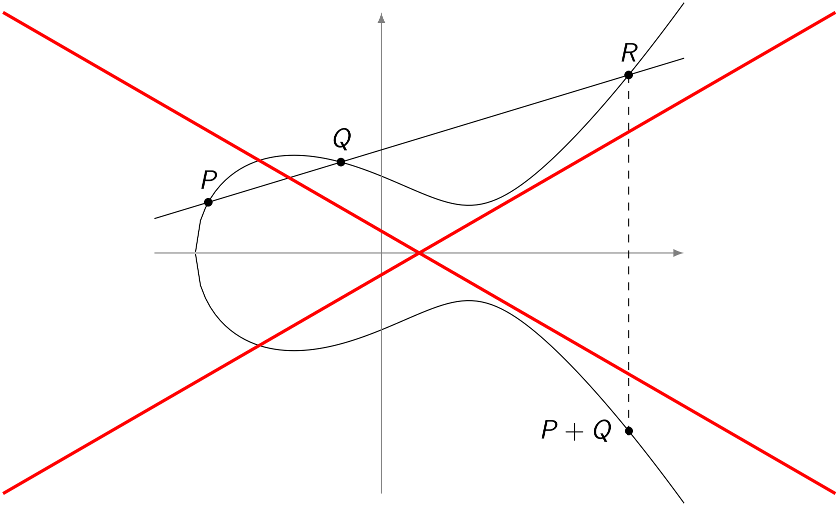
Elliptic curves

Let E be an elliptic curve. . .

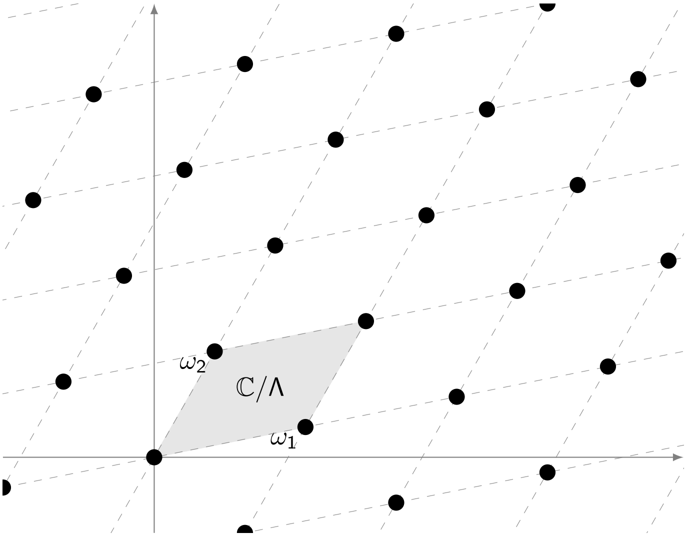


Elliptic curves

Let E be an elliptic curve... forget it!



Elliptic curves

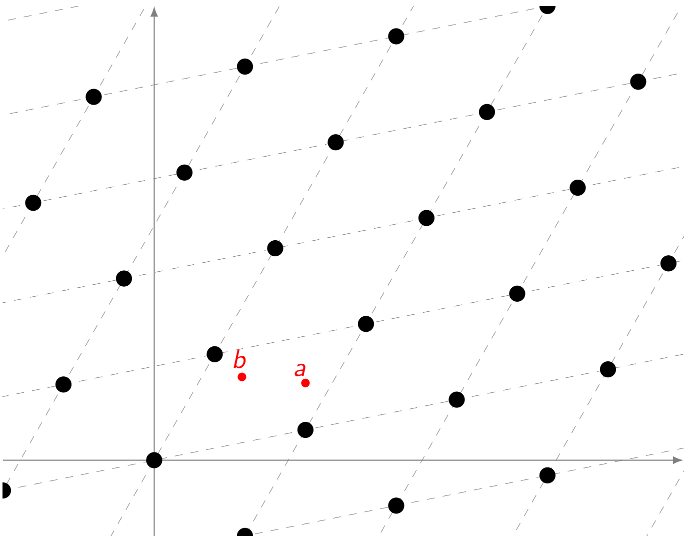


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

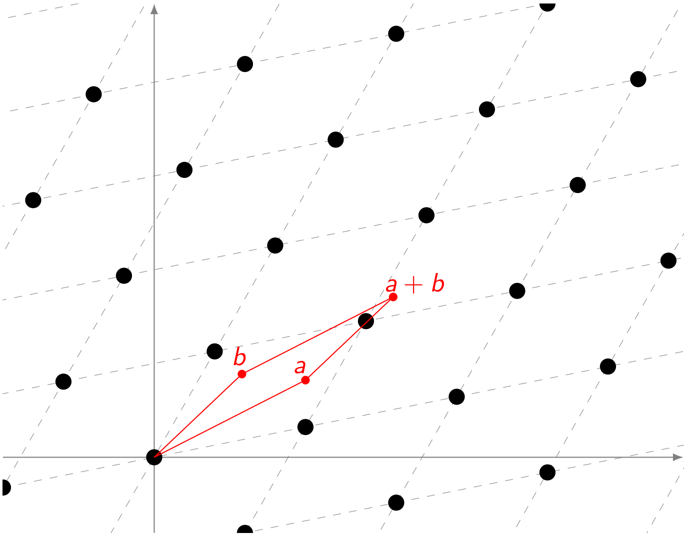
$\mathbb{C}/\Lambda$ is an elliptic curve.

Elliptic curves



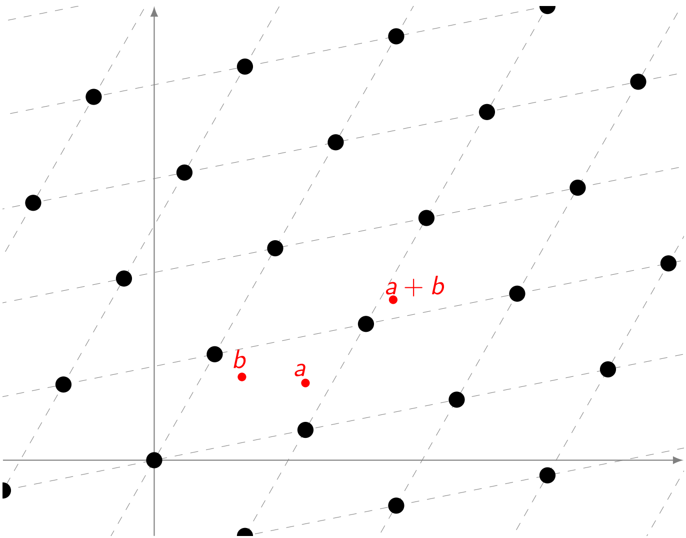
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



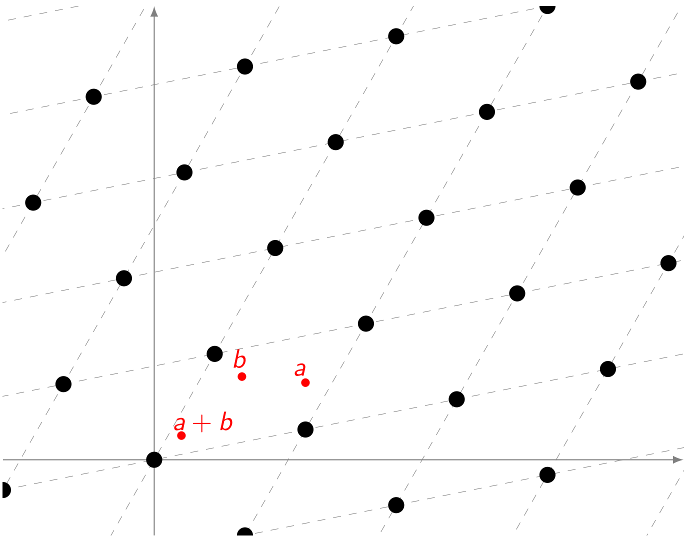
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



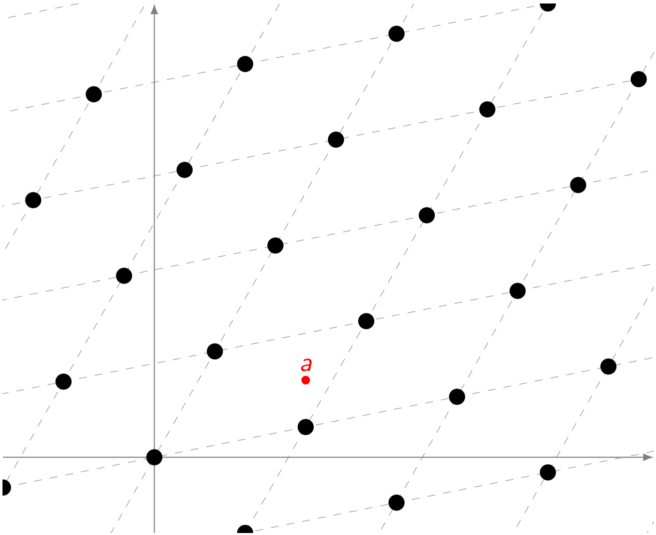
Addition law induced by addition on $\mathbb{C}$.

Elliptic curves



Addition law induced by addition on $\mathbb{C}$.

Isomorphism classes

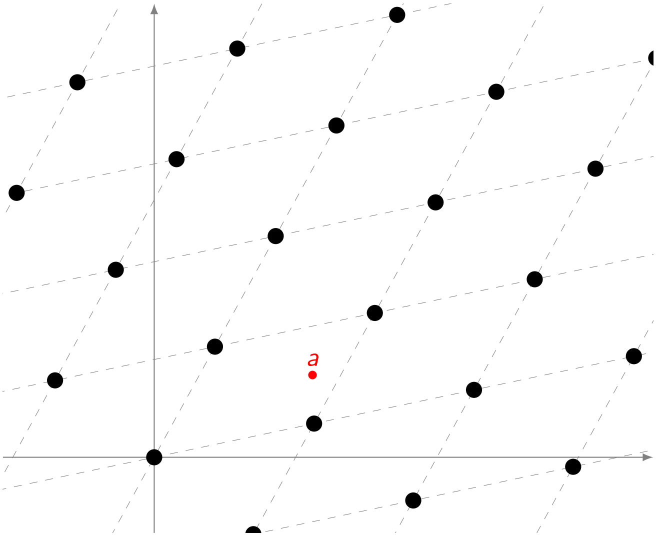


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

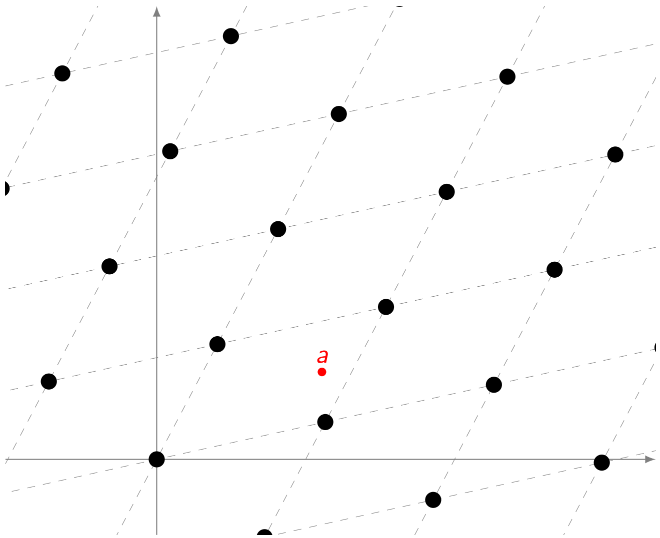


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

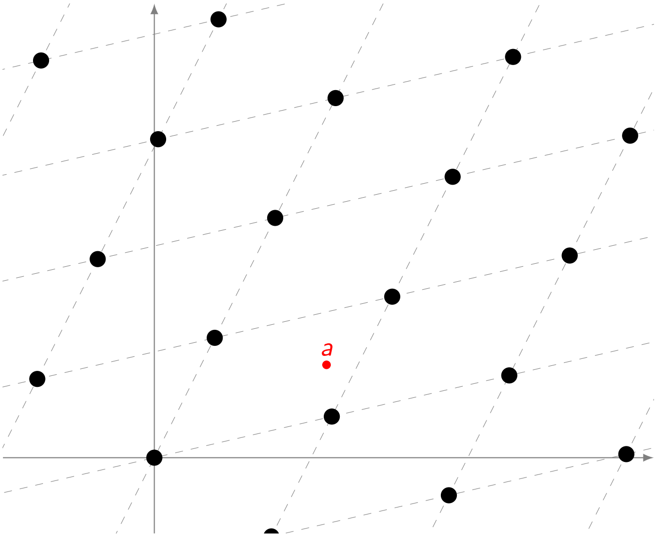


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

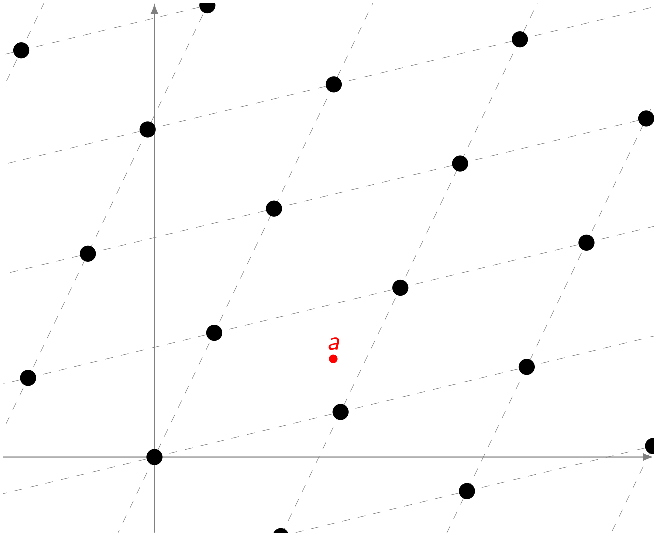


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

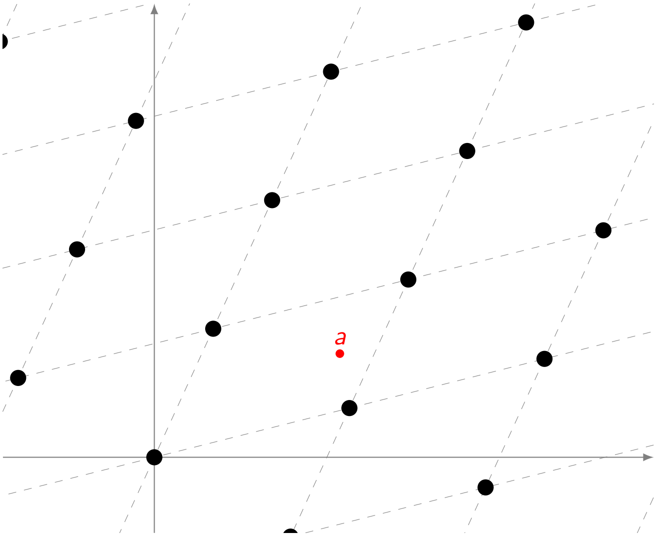


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

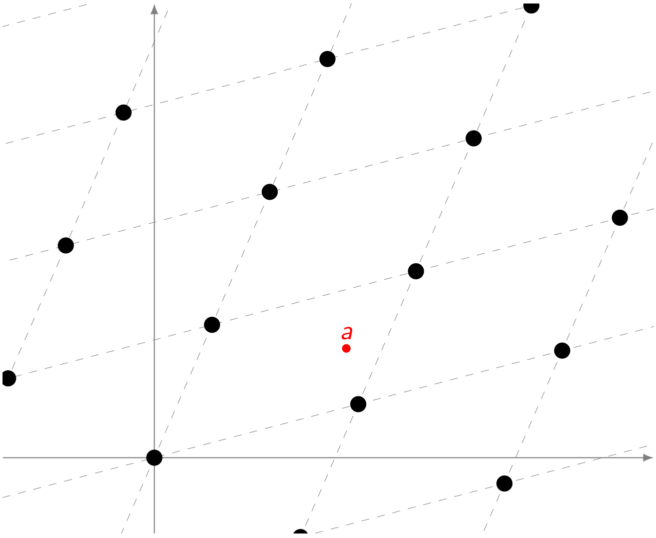


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

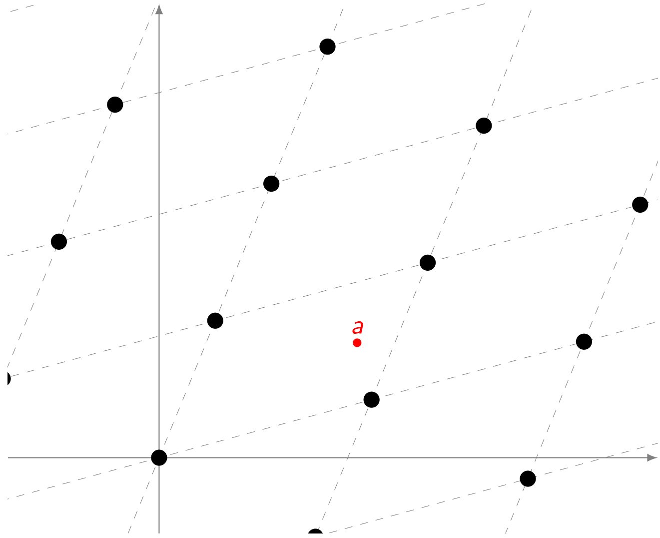


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

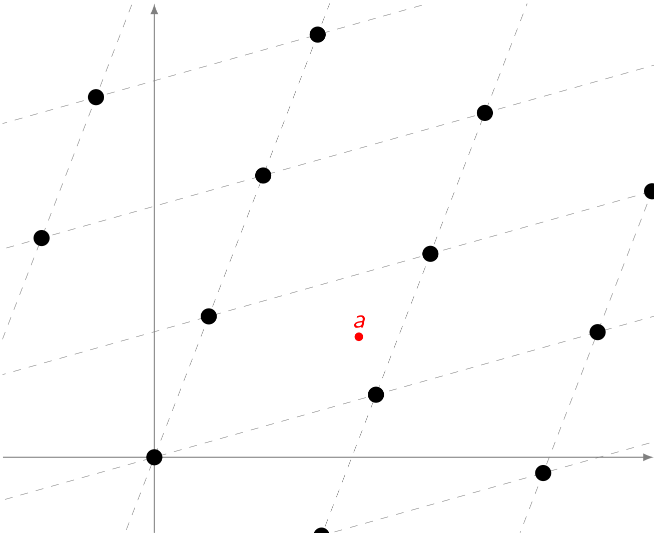


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

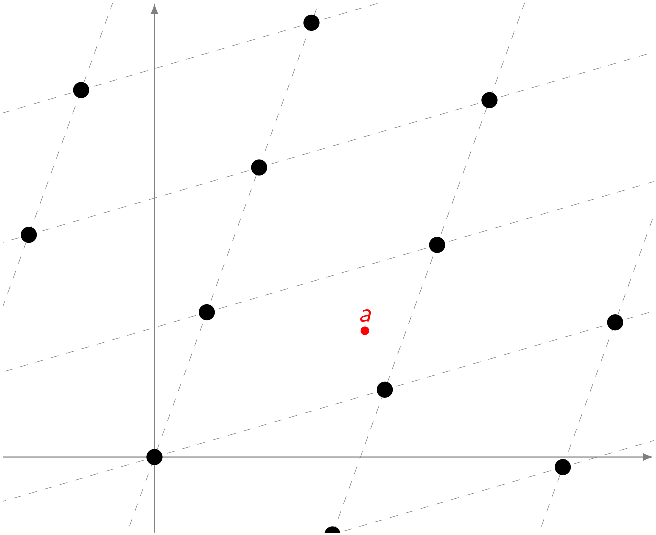


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

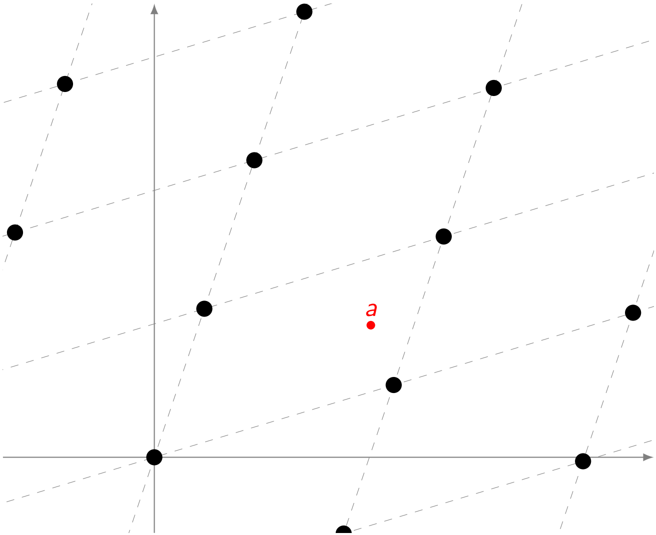


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

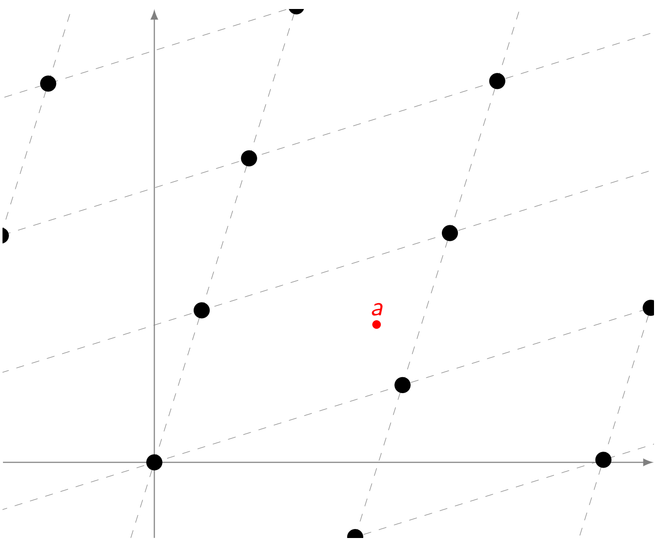


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

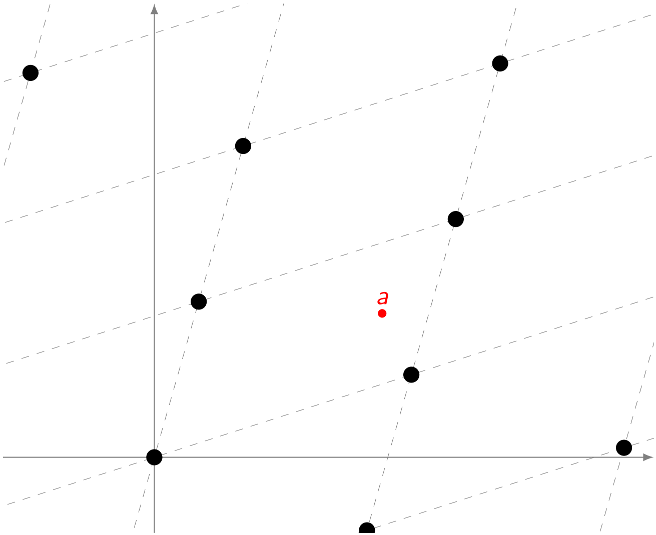


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

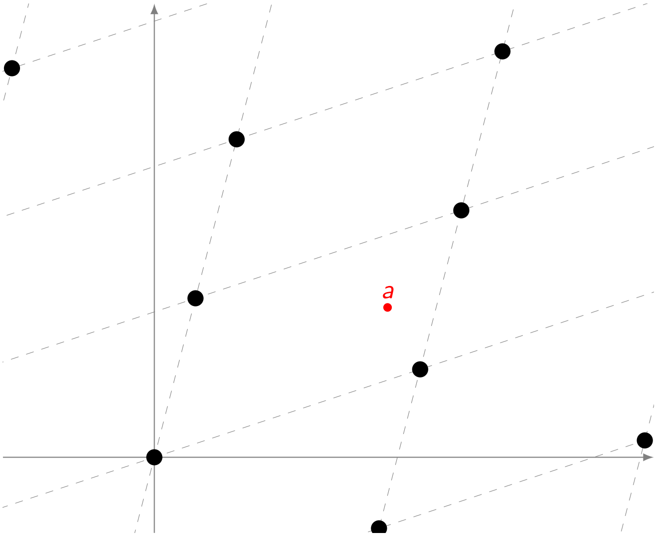


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

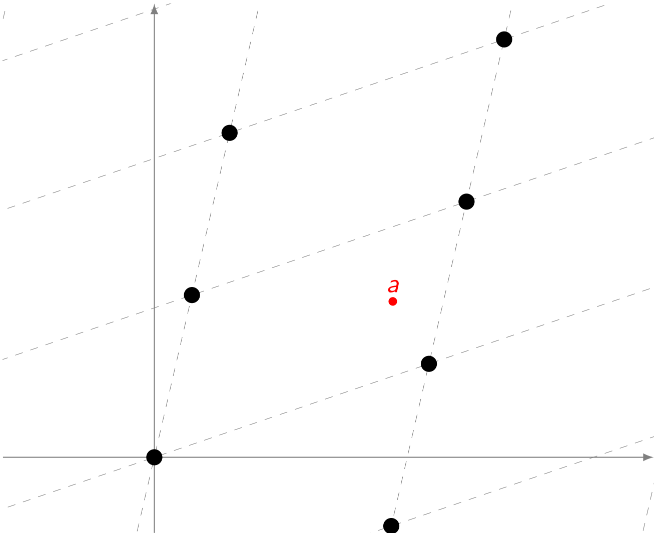


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

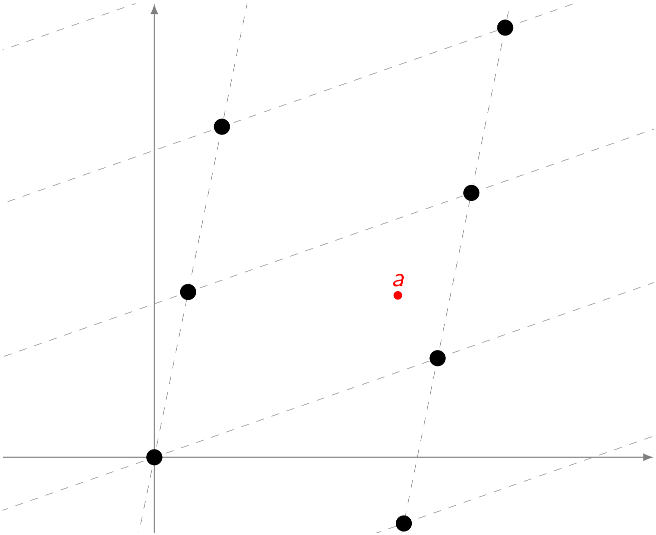


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha \Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

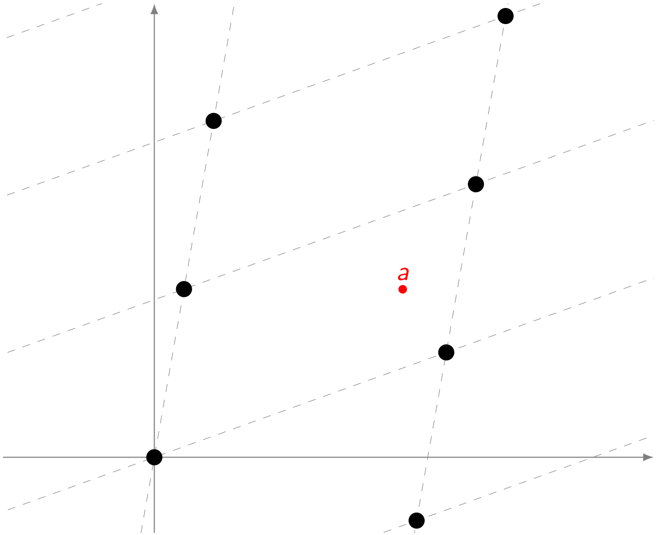


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

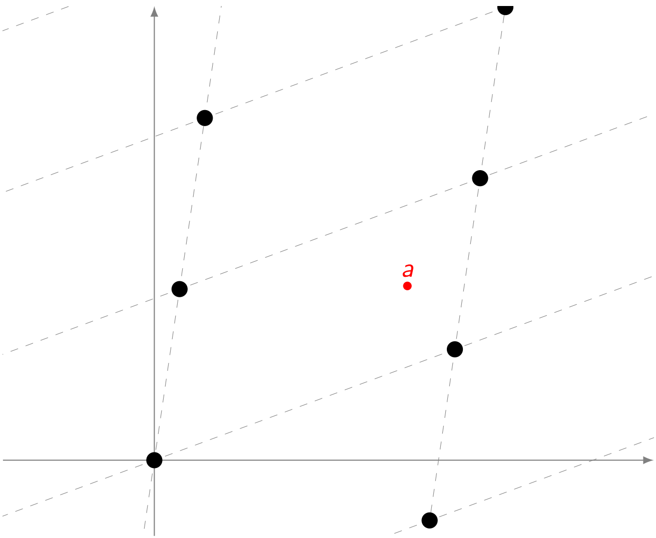


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

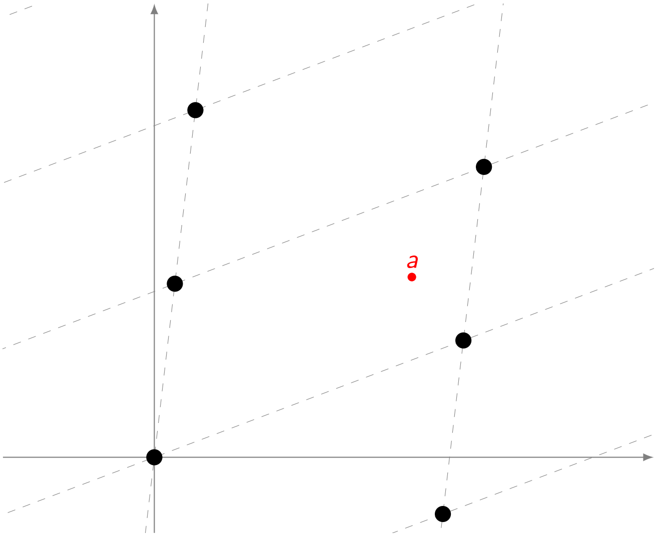


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

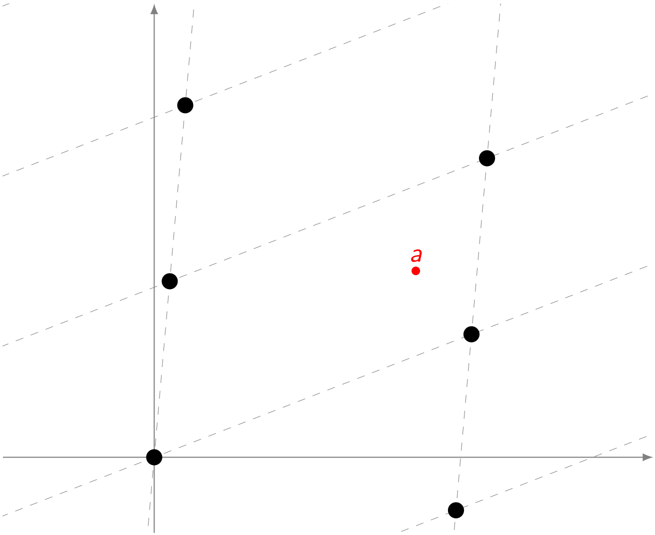


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

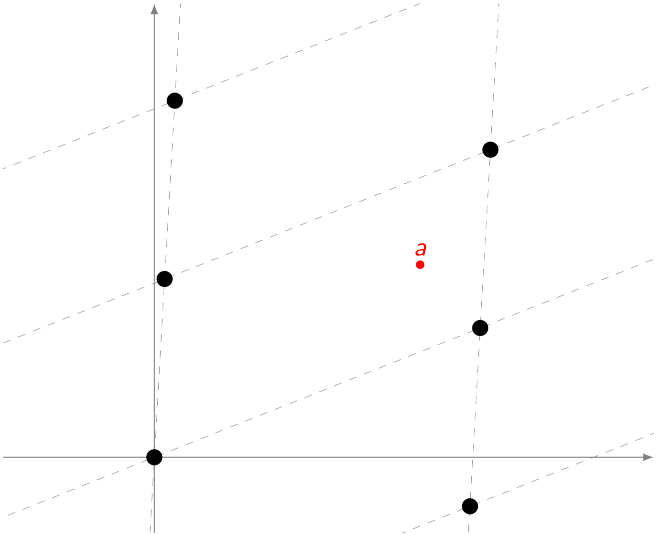


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

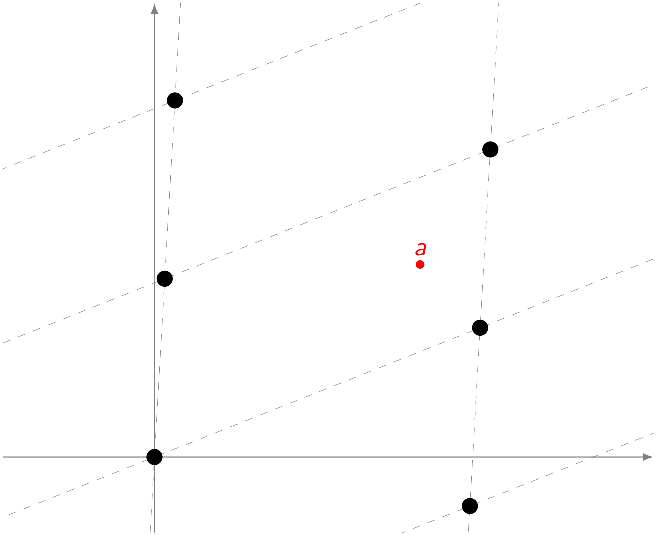


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

Isomorphism classes

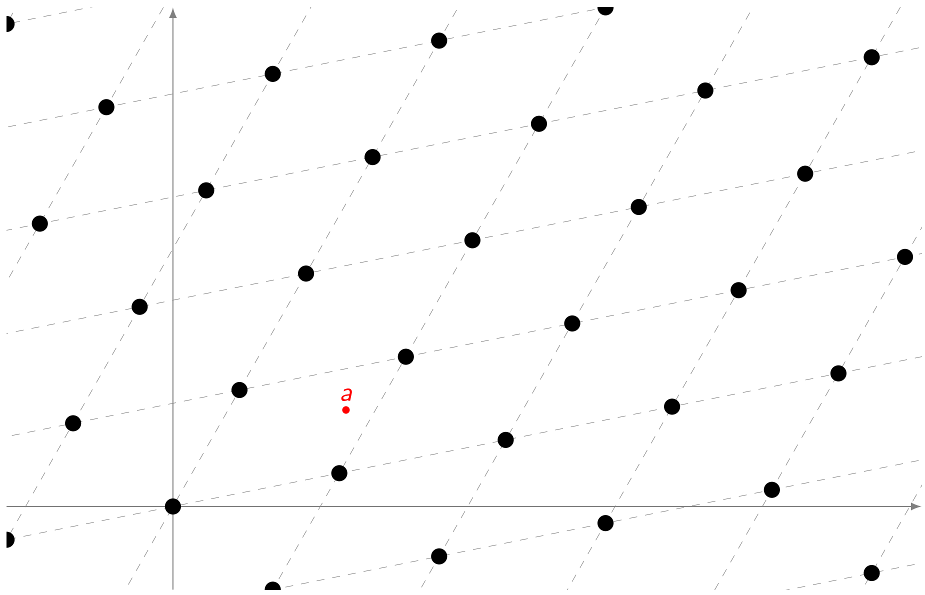


Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

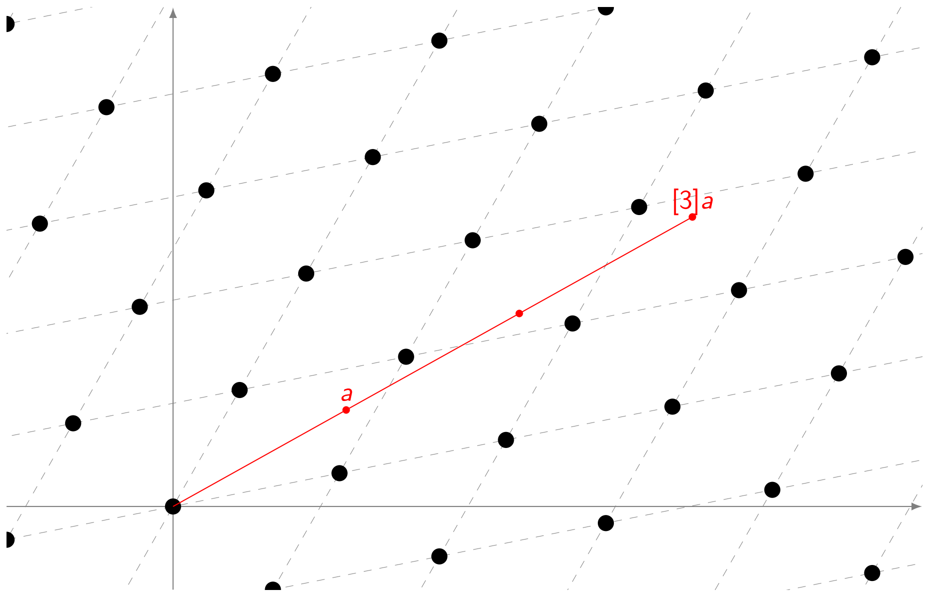
$$\alpha\Lambda_1 = \Lambda_2$$

The *j*-invariant $j(\Lambda)$ classifies elliptic curves up to homothety (isomorphism).

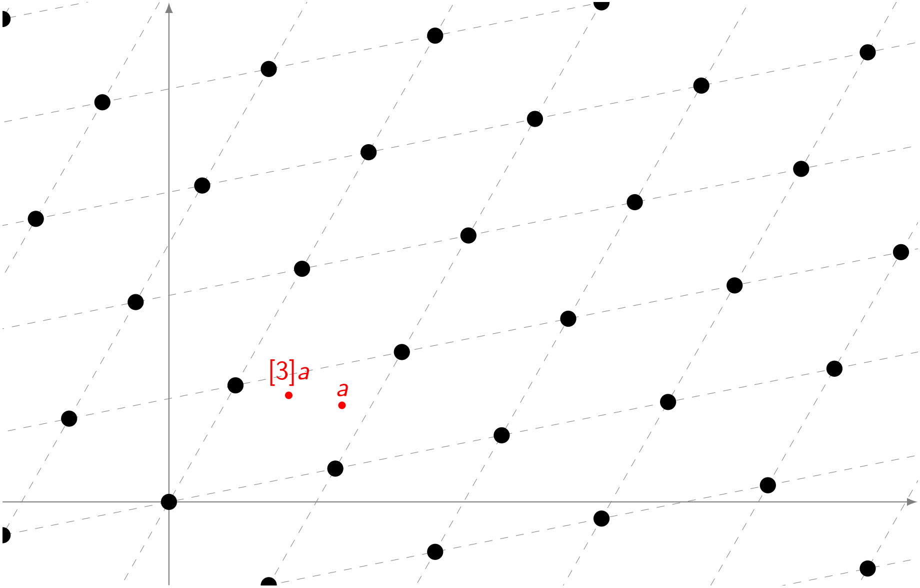
Multiplication



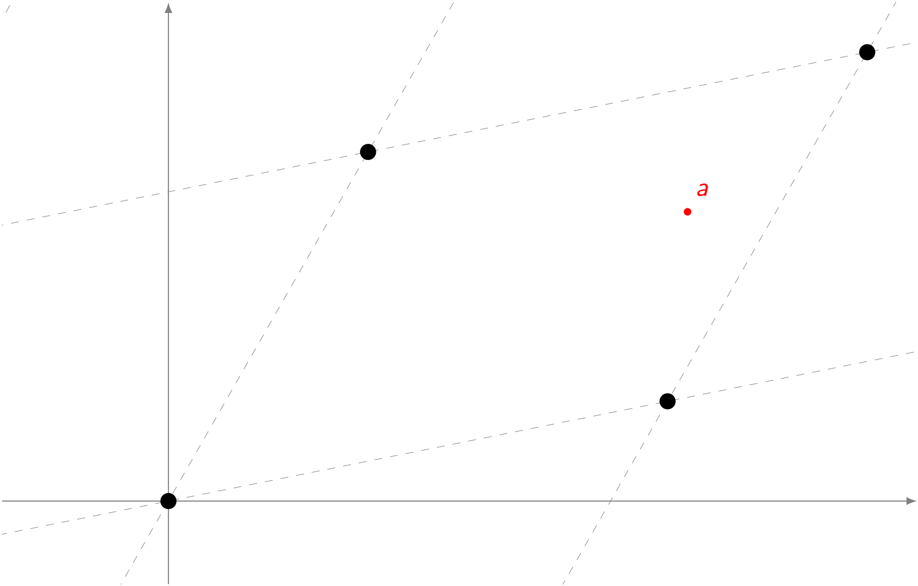
Multiplication



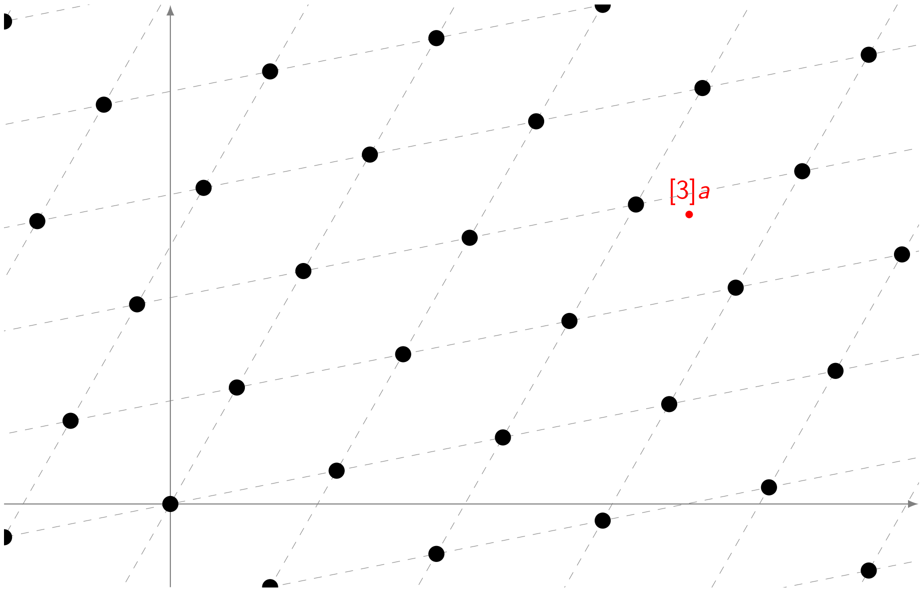
Multiplication



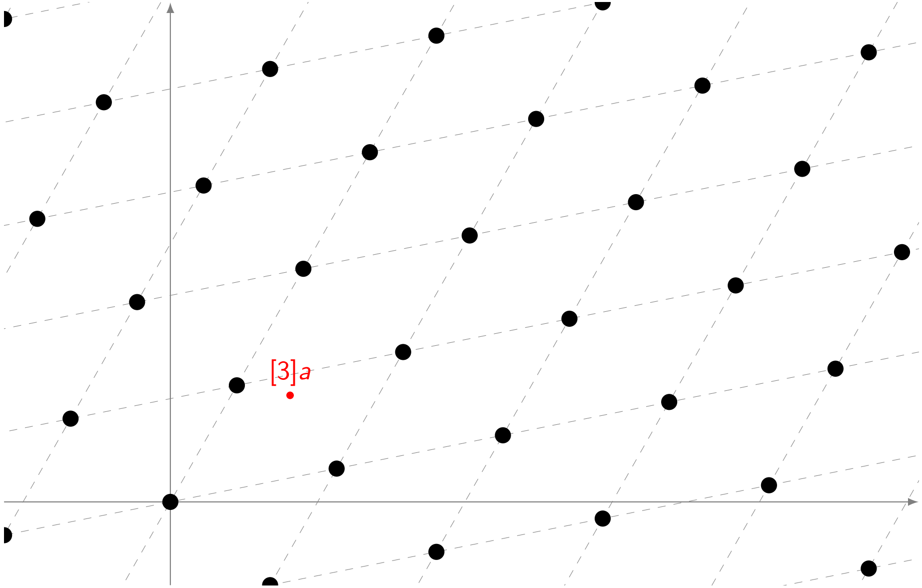
Multiplication + homothety



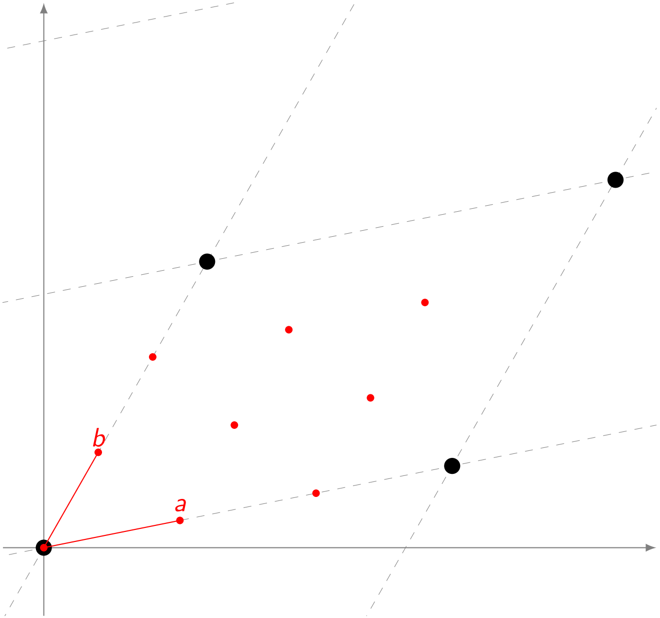
Multiplication + homothety



Multiplication + homothety



Torsion subgroups



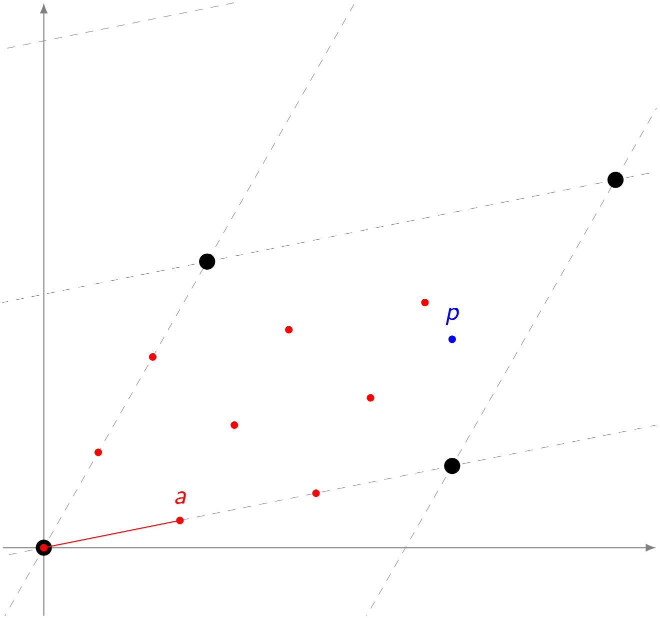
The ℓ-torsion subgroup is made up by the points

$$\left(\frac{i\omega_1}{\ell}, \frac{j\omega_2}{\ell}\right)$$

It is a group of rank two

$$E[\ell] = \langle a, b \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

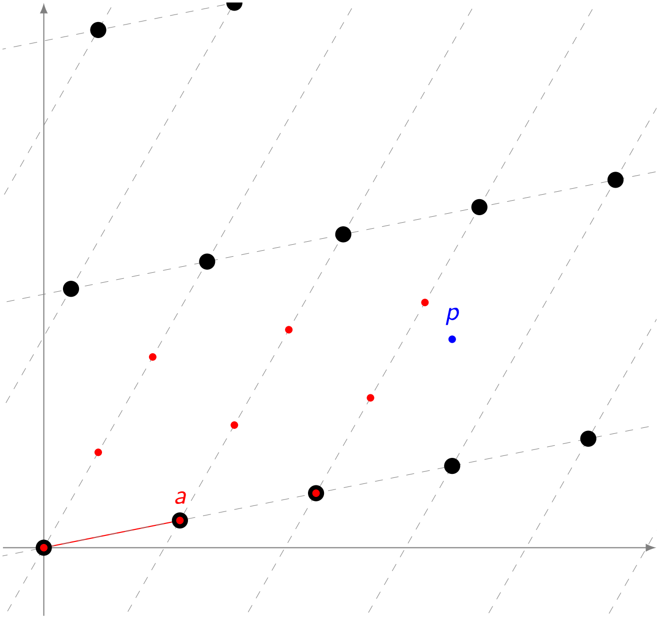
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

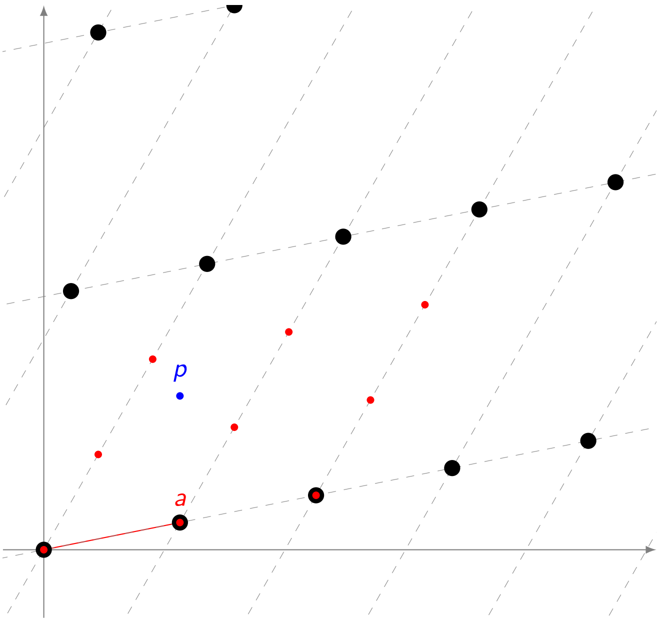
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

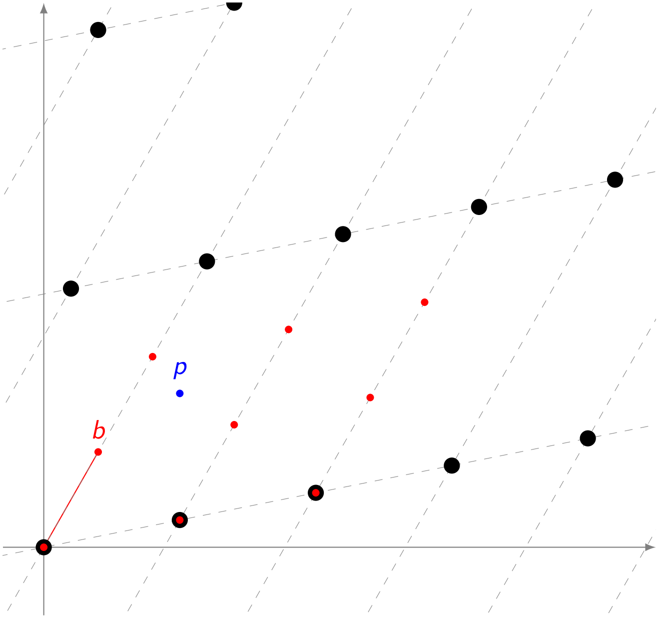
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies

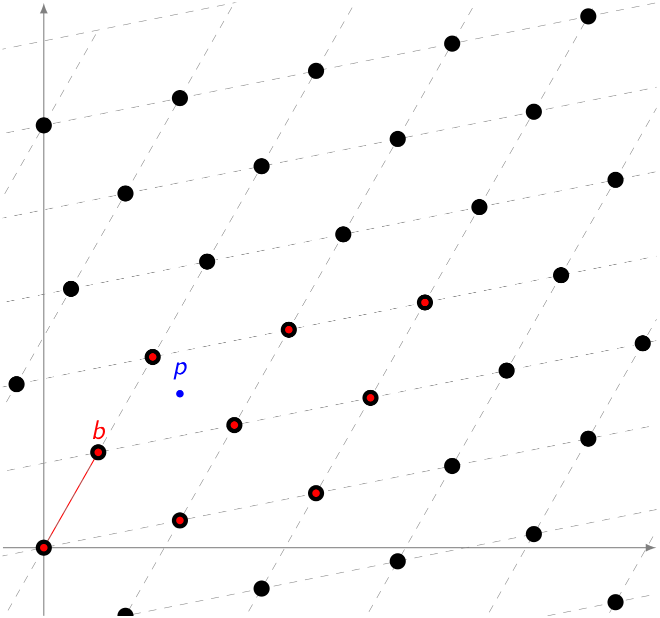


Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies

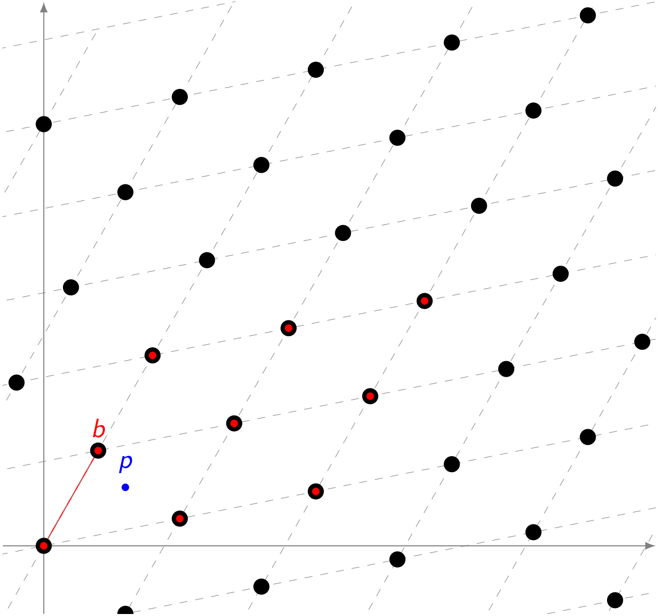


Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies over arbitrary fields

Isogenies are just the right notion of morphism for elliptic curves

- Surjective group morphisms.
- Algebraic maps (i.e., defined by polynomials).

$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

The kernel H determines the image curve E' up to isomorphism

$$E/H \stackrel{\text{def}}{=} E'.$$

Isogeny degree

Neither of these definitions is quite correct, but they *nearly* are:

- The degree of ϕ is the cardinality of $\ker \phi$.
- (Bisson) the degree of ϕ is the time needed to compute it.

The computational point of view

In practice: an isogeny ϕ is just a rational fraction (or maybe two)

$$\frac{N(x)}{D(x)} = \frac{x^r + \cdots + n_1 x + n_0}{x^{r-1} + \cdots + d_1 x + d_0} \in k(x), \qquad \text{with } \ell = \deg \phi,$$

and $D(x)$ vanishes on $\ker \phi$.

Vélu's formulas

Input: The *kernel polynomial* $D(x)$.

Output: The curve E/H and the rational fraction N/D.

Complexity: $\tilde{O}(r)$.

Sidenote: we are only interested in *rational* isogenies, i.e. such that N/D has coefficients in the base field (i.e. ϕ is Galois invariant).

Motivation

Explicit isogeny problem

Let $\mathbb{F}_q$ be a finite field of characteristic p. Given an integer r and two r-isogenous elliptic curves E, E' defined over $\mathbb{F}_q$, compute an r-isogeny $\phi : E \to E'$.

Special instances of this problem appear in various applications:

- Schoof-Elkies-Atkin point counting algorithm,
- ECC cryptanalysis: [Gaudry, Hess, Smart '02],
- Hash functions: [Charles, Goren, Lauter '07],
- Trapdoors: [Teske '06],
- Post quantum cryptography: [Rotostev, Stolbunov '06], [De Feo, Jao, Plût '11].

1

Motivation

Explicit isogeny problem

Let $\mathbb{F}_q$ be a finite field of characteristic p. Given an integer r and two r-isogenous elliptic curves E, E' defined over $\mathbb{F}_q$, compute an r-isogeny $\phi : E \to E'$.

Special instances of this problem appear in various applications:

- Schoof-Elkies-Atkin point counting algorithm,
- ECC cryptanalysis: [Gaudry, Hess, Smart '02],
- Hash functions: [Charles, Goren, Lauter '07],
- Trapdoors: [Teske '06],
- Post quantum cryptography: [Rotostev, Stolbunov '06], [De Feo, Jao, Plût '11].

Disclaimer: however, the general version we are going to solve here does not improve the theoretical complexity[1] of any of these!

[1] It possibly gives a minor practical speed-up for SEA in *medium* characteristic, though :)

Previous work

Let p be the characteristic of $\mathbb{F}_q$.

- [Elkies '92/'98], [Bostan, Morain, Salvy, Schost '08] use $\tilde{O}(r)$ operations in $\mathbb{F}_q$, work only for $r < 2p$. Specific to the SEA case.
- [Couveignes '94] any characteristic, $\tilde{O}(r^3 p^{O(1)})$ operations.
- [Lercier '97] only $p = 2$.
- [Couveignes '96], [LDF '10] any characteristic, $\tilde{O}(r^2 p^{O(1)})$ operations.
- [Lercier, Sirvent '08], [Lairez, Vaccon '16] works for every p using $\tilde{O}(r^2)$ operations in $\mathbb{F}_q$. Specific to the SEA case.

Our goal: modify Couveignes' algorithm to obtain an algorithm with complexity $\tilde{O}(r^2)$ but with no exponential dependency in $\log(p)$.

Torsion points of elliptic curves

Torsion points

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $m > 0$

$$E[m] = \{P \in E(\bar{\mathbb{F}}_q), mP = 0_E\}$$

For ordinary elliptic curves

$$E[\ell^k] \simeq \mathbb{Z}/\ell^k\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z} \quad \textit{with } \ell \neq p$$
$$E[p^k] \simeq \mathbb{Z}/p^k\mathbb{Z}$$

Torsion points of elliptic curves

Torsion points

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $m > 0$

$$E[m] = \{P \in E(\bar{\mathbb{F}}_q), mP = 0_E\}$$

For ordinary elliptic curves

$$E[\ell^k] \simeq \mathbb{Z}/\ell^k\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z} \quad \textit{with } \ell \neq p$$

$$E[p^k] \simeq \mathbb{Z}/p^k\mathbb{Z}$$

Couveignes' algorithm (compute an r-isogeny $\phi : E \to E'$)

Compute ϕ by interpolation over $E[p^k]$:

- Compute generators P, P' of $E[p^k], E'[p^k]$;
- Interpolate ϕ, assuming it maps $uP \mapsto uP'$ for all $u \in \mathbb{Z}/p^k\mathbb{Z}$;
- Test whether ϕ is an isogeny.
  In case it is not, replace P' with a multiple aP' and start again.

Couveignes algorithm (1996)

Input: E, E' two r-isogenous curves on $\mathbb{F}_{p^n}$,
Output: $\phi : E \rightarrow E'$ of degree r.

1. Select the least k such that $p^k > 4r$;
2. Compute generators P of $E[p^k]$ and P' of $E'[p^k]$;
3. Compute $T = \prod(X - x(uP))$ with $1 \leq u \leq \frac{p^k-1}{2}$;
4. For each $a \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$: $O(r)$
   1. Compute the interpolation polynomial $L : x(uP) \mapsto x(a\,(uP'))$; $\tilde{O}(rp^{O(1)})$
   2. Use a rational reconstruction algorithm to compute a rational fraction $F = L \bmod T$ of degrees $(r, r-1)$; $\tilde{O}(r)$
   3. If F defines an isogeny of degree r, return it and stop.

Couveignes algorithm (1996)

Input: E, E' two r-isogenous curves on $\mathbb{F}_{p^n}$,
Output: $\phi : E \to E'$ of degree r.

1. Select the least k such that $p^k > 4r$;
2. Compute generators P of $E[p^k]$ and P' of $E'[p^k]$;
3. Compute $T = \prod(X - x(uP))$ with $1 \leq u \leq \frac{p^k-1}{2}$;
4. For each $a \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$: $O(r)$
   1. Compute the interpolation polynomial $L : x(uP) \mapsto x(a\,(uP'))$; $\tilde{O}(rp^{O(1)})$
   2. Use a rational reconstruction algorithm to compute a rational fraction $F = L \bmod T$ of degrees $(r, r-1)$; $\tilde{O}(r)$
   3. If F defines an isogeny of degree r, return it and stop.

Our brilliant idea!

Replace $E[p^k]$ by $\boldsymbol{E[\ell^k]}$ for a small prime $\ell \neq p$.

An ℓ-adic Couveignes' algorithm?

Our goal is to work with $\boldsymbol{E[\ell^k]} \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^{\mathbf{2}}$ instead of $E[p^k]$ to remove the polynomial dependency in p.

- $E[p^k] = \langle P \rangle \simeq (\mathbb{Z}/p^k\mathbb{Z})$ with $p^k \approx r$
- $E[\ell^k] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell^k\mathbb{Z}) \times (\mathbb{Z}/\ell^k\mathbb{Z})$ with $\ell^{2k} \approx r$

An ℓ-adic Couveignes' algorithm?

Our goal is to work with $\boldsymbol{E[\ell^k]} \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^2$ instead of $E[p^k]$ to remove the polynomial dependency in p.

- $E[p^k] = \langle P \rangle \simeq (\mathbb{Z}/p^k\mathbb{Z})$ with $p^k \approx r$
- $E[\ell^k] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell^k\mathbb{Z}) \times (\mathbb{Z}/\ell^k\mathbb{Z})$ with $\ell^{2k} \approx r$

p-adic

Let $P \in E$ and $P' \in E'$

$$P \mapsto aP' \qquad a \in (\mathbb{Z}/p^k\mathbb{Z})^*$$

$\Rightarrow O(r)$ possibilities.

ℓ-adic

Let $P, Q \in E$ and $P', Q' \in E'$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P' \\ Q' \end{pmatrix}$$

with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ invertible.

$\Rightarrow O(r^2)$ possibilities.

An ℓ-adic Couveignes' algorithm?

Our goal is to work with $\boldsymbol{E[\ell^k]} \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^2$ instead of $E[p^k]$ to remove the polynomial dependency in p.

- $E[p^k] = \langle P \rangle \simeq (\mathbb{Z}/p^k\mathbb{Z})$ with $p^k \approx r$
- $E[\ell^k] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell^k\mathbb{Z}) \times (\mathbb{Z}/\ell^k\mathbb{Z})$ with $\ell^{2k} \approx r$

p-adic

Let $P \in E$ and $P' \in E'$

$$P \mapsto aP' \qquad a \in (\mathbb{Z}/p^k\mathbb{Z})^*$$

$\Rightarrow O(r)$ possibilities.

ℓ-adic

Let $P, Q \in E$ and $P', Q' \in E'$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P' \\ Q' \end{pmatrix}$$

with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ invertible.

$\Rightarrow O(r^2)$ possibilities.

Not so brilliant, after all?

Frobenius vs isogenies

Definition (Frobenius Endomorphism)

E an ordinary elliptic curve defined over $\mathbb{F}_q$. The function

$$\pi : (x, y) \mapsto (x^q, y^q)$$

is called Frobenius endomorphism. It satisfies a quadratic equation

$$\pi^2 - t_\pi \pi + q = 0.$$

We are only working with rational isogenies $\phi : E \to E'$, i.e.

$$\pi_{E'} \circ \phi = \phi \circ \pi_E.$$

Subgroup of size ℓ $\Leftrightarrow$ ℓ-isogeny

Subgroup of size ℓ	$\Leftrightarrow$	ℓ-isogeny
Subgroup of size ℓ stable by π	$\Leftrightarrow$	Rational ℓ-isogeny

Subgroup of size ℓ	$\Leftrightarrow$	ℓ-isogeny
Subgroup of size ℓ stable by π	$\Leftrightarrow$	Rational ℓ-isogeny

Assume that π splits modulo ℓ: i.e. its minimal polynomial factors as

$$(\pi - \lambda)(\pi - \mu) \quad \text{with} \quad \lambda \neq \mu \bmod \ell$$

Subgroup of size ℓ ⇔ ℓ-isogeny

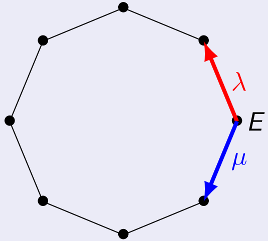
Subgroup of size ℓ stable by π ⇔ Rational ℓ-isogeny

Assume that π splits modulo ℓ: i.e. its minimal polynomial factors as

$$(\pi - \lambda)(\pi - \mu) \quad \text{with} \quad \lambda \neq \mu \bmod \ell$$

Two eigenspaces in $E[\ell]$ $\ker(\pi - \lambda), \ker(\pi - \mu)$ ⇒ Two rational ℓ-isogenies of direction λ, μ

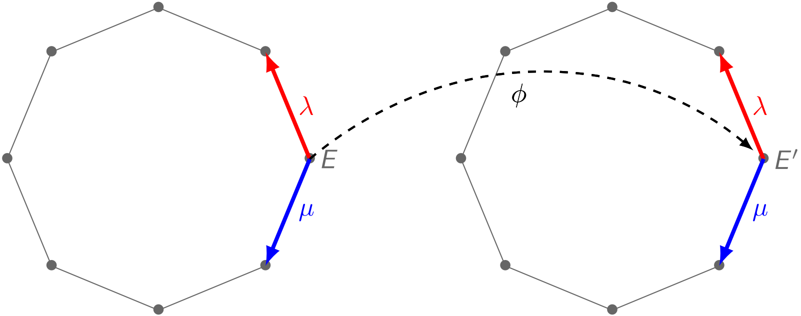
Isogeny graph



Fact

Let ϕ be an r-isogeny with $\ell \nmid r$, then ϕ preserves the kernels of the ℓ-isogenies of direction λ, μ.

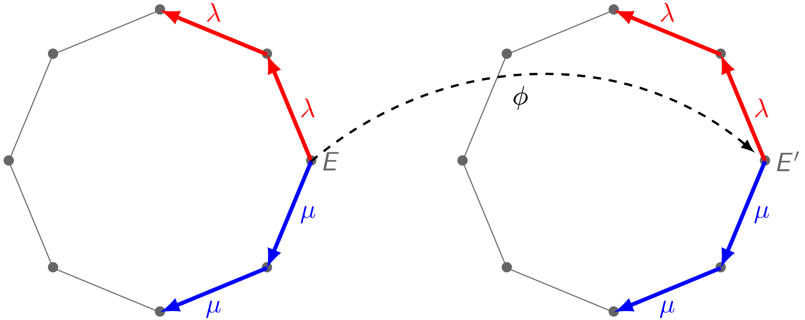
To interpolate ϕ over $E[\ell^k]$, we want to compute two cyclic ℓ^k-subgroups of direction λ, μ.



Fact

Let ϕ be an r-isogeny with $\ell \nmid r$, then ϕ preserves the kernels of the ℓ-isogenies of direction λ, μ.

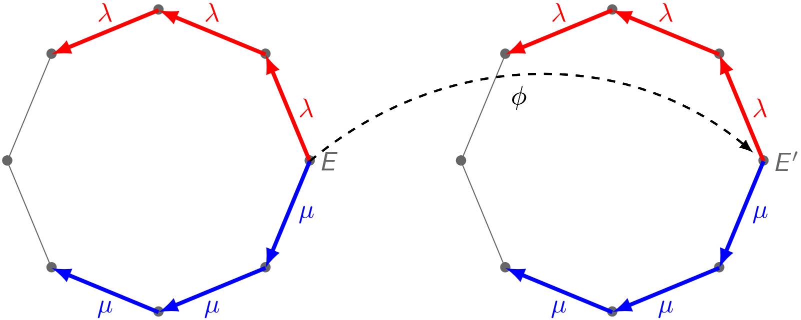
To interpolate ϕ over $E[\ell^k]$, we want to compute two cyclic ℓ^k-subgroups of direction λ, μ.



Fact

Let ϕ be an r-isogeny with $\ell \nmid r$, then ϕ preserves the kernels of the ℓ-isogenies of direction λ, μ.

To interpolate ϕ over $E[\ell^k]$, we want to compute two cyclic ℓ^k-subgroups of direction λ, μ.



- We call $E[\ell^k]_\lambda \oplus E[\ell^k]_\mu$ a horizontal decomposition;
- SEA literature calls this an isogeny cycle [Couveignes, Morain '94].

Towards an ℓ-adic Couveignes' algorithm (π splits modulo ℓ)

Input: E, E' two r-isogenous curves on $\mathbb{F}_q$,

Output: $\phi : E \to E'$ of degree r.

Fact: ϕ maps $E[\ell^k]_\lambda \to E'[\ell^k]_\lambda$ and $E[\ell^k]_\mu \to E'[\ell^k]_\mu$.

1. Select the least k such that $\ell^{2k} > 4r$.
2. Compute $\langle P, Q\rangle = E[\ell^k]_\lambda \oplus E[\ell^k]_\mu$ and $\langle P', Q'\rangle = E'[\ell^k]_\lambda \oplus E'[\ell^k]_\mu$
3. For each **invertible diagonal** matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ in $(\mathbb{Z}/\ell^k\mathbb{Z})^{2\times 2}$:
    1. Compute the interpolation polynomial L sending $P \mapsto aP'$ and $Q \mapsto bQ'$;
    2. Use a rational reconstruction algorithm to compute a rational fraction F of degrees $(r, r-1)$;
    3. If F defines an isogeny of degree r, return it and stop.

Towards an ℓ-adic Couveignes' algorithm (π splits modulo ℓ)

Input: E, E' two r-isogenous curves on $\mathbb{F}_q$,

Output: $\phi : E \to E'$ of degree r.

Fact: ϕ maps $E[\ell^k]_\lambda \to E'[\ell^k]_\lambda$ and $E[\ell^k]_\mu \to E'[\ell^k]_\mu$.

1. Select the least k such that $\ell^{2k} > 4r$.
2. Compute $\langle P, Q\rangle = E[\ell^k]_\lambda \oplus E[\ell^k]_\mu$ and $\langle P', Q'\rangle = E'[\ell^k]_\lambda \oplus E'[\ell^k]_\mu$
3. For each **invertible diagonal** matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ in $(\mathbb{Z}/\ell^k\mathbb{Z})^{2\times 2}$: $O(r)$
   1. Compute the interpolation polynomial L sending $P \mapsto aP'$ and $Q \mapsto bQ'$; $\tilde{O}(r\ell^{O(1)})$
   2. Use a rational reconstruction algorithm to compute a rational fraction F of degrees $(r, r-1)$; $\tilde{O}(r)$
   3. If F defines an isogeny of degree r, return it and stop.

I'm done. Thanks.

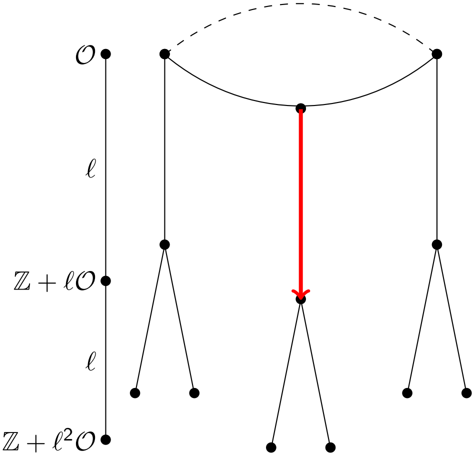
Questions?

No?

Ok, wait, I'm not done yet!

Towards the general case

Denote by $\mathcal{O}$ (resp. $\mathcal{O}'$) the endomorphism ring of E (resp. E')



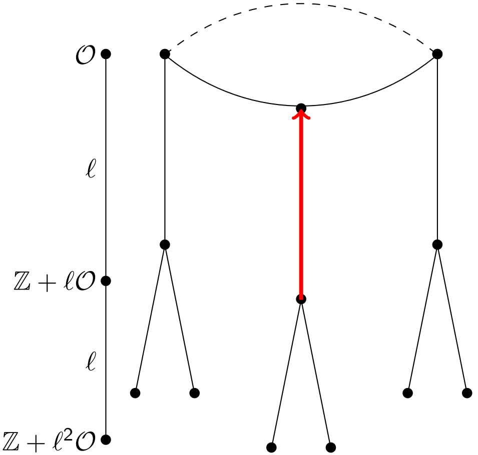
Lemma (Kohel 1996)

E and E' two elliptic curves defined over $\mathbb{F}_q$, $\psi : E \to E'$ an ℓ-isogeny. Then we say that ψ is

1. **descending** if $\ell = [\mathcal{O} : \mathcal{O}']$
2. ascending if $\ell = [\mathcal{O}' : \mathcal{O}]$,
3. horizontal if $\mathcal{O} = \mathcal{O}'$.

Towards the general case

Denote by $\mathcal{O}$ (resp. $\mathcal{O}'$) the endomorphism ring of E (resp. E')



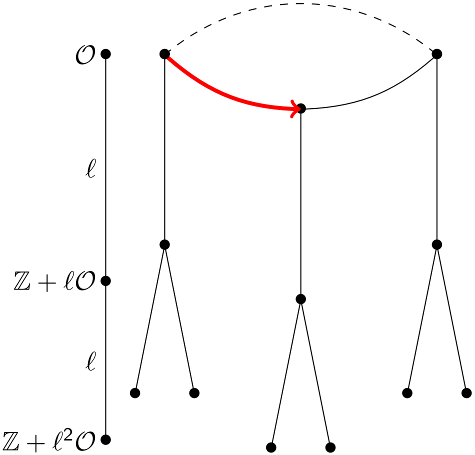
Lemma (Kohel 1996)

E and E' two elliptic curves defined over $\mathbb{F}_q$, $\psi : E \to E'$ an ℓ-isogeny. Then we say that ψ is

1. descending if $\ell = [\mathcal{O} : \mathcal{O}']$
2. **ascending** if $\ell = [\mathcal{O}' : \mathcal{O}]$,
3. horizontal if $\mathcal{O} = \mathcal{O}'$.

Towards the general case

Denote by $\mathcal{O}$ (resp. $\mathcal{O}'$) the endomorphism ring of E (resp. E')



Lemma (Kohel 1996)

E and E' two elliptic curves defined over $\mathbb{F}_q$, $\psi : E \to E'$ an ℓ-isogeny. Then we say that ψ is

1. descending if $\ell = [\mathcal{O} : \mathcal{O}']$
2. ascending if $\ell = [\mathcal{O}' : \mathcal{O}]$,
3. **horizontal** if $\mathcal{O} = \mathcal{O}'$.

A guide to volcano types

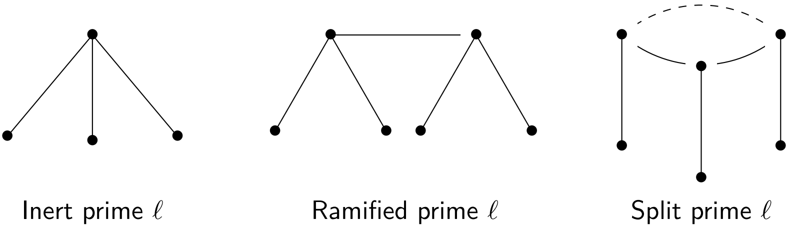


Figure: The three shapes of volcanoes of 2-isogenies

In the rest of this talk we consider only volcanoes with cyclic crater (Elkies case).

The Elkies case

Elkies prime

We say that ℓ is an Elkies prime if the characteristic polynomial of π factors over $\mathbb{Z}_\ell$ as

$$\pi^2 - t_\pi \pi + q = (\pi - \lambda)(\pi - \mu), \quad \text{with } \lambda \neq \mu,$$

where $h = v_\ell(\lambda - \mu)$ can be $\geqslant 1$.

Note: $h = v_\ell(\lambda - \mu)$ is the height of the ℓ-volcano.

Problem: as long as $k \leq h$, the two eigenvalues are undistinguishable:

$$\pi(P) = \lambda P = \mu P \quad \text{for any } P \in E[\ell^h].$$

From now on, we assume[2] that $k \geqslant h + 1$.

[2] This has no impact on the complexity as the isogeny degree grows, indeed $k \approx \log(r)$.

Proposition (LDF, Hugounenq, Plût, Schost)

In the Elkies case the action of the Frobenius endomorphism π on $E[\ell^{h+1}]$ is conjugate, over $\mathbb{Z}_\ell$, to a unique matrix

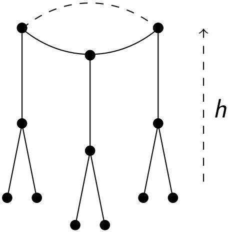
$$\begin{pmatrix} \lambda & a \\ 0 & \mu \end{pmatrix},$$

with $a \in \{1, \ell, \ldots, \ell^{h-1}, 0\}$, and $a = 0$ iff E lies on the crater.

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

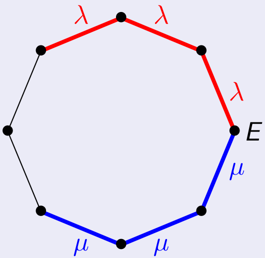
$$\begin{pmatrix} \lambda & \ell \\ 0 & \mu \end{pmatrix}$$

$$\begin{pmatrix} \lambda & 1 \\ 0 & \mu \end{pmatrix}$$



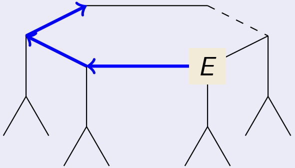
Suppose that E lies on the crater (we can reduce to this case easily).

Volcano with height $h = 0$



- $\ker(\pi - \mu \mid E[\ell^k])$ is cyclic of size ℓ^k;
- Interpolation maps a cyclic group to a cyclic group;
- $O(\ell^k)$ choices. Happiness!

Volcano with height $h = 2$

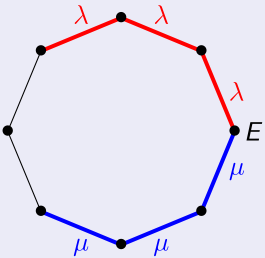


Problem:

- $\ker(\pi - \mu \mid E[\ell^k]) \simeq (\mathbb{Z}/\ell^k) \times (\mathbb{Z}/\ell^h)$;
- It contains ℓ^h cyclic subgroups of order ℓ^k;
- Each cyclic subgroup is associated to an isogeny that **starts** horizontal;
- $O(\ell^{k+h})$ choices. Sadness.

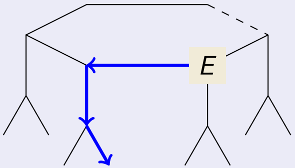
Suppose that E lies on the crater (we can reduce to this case easily).

Volcano with height $h = 0$



- $\ker(\pi - \mu \mid E[\ell^k])$ is cyclic of size ℓ^k;
- Interpolation maps a cyclic group to a cyclic group;
- $O(\ell^k)$ choices. Happiness!

Volcano with height $h = 2$



Problem:

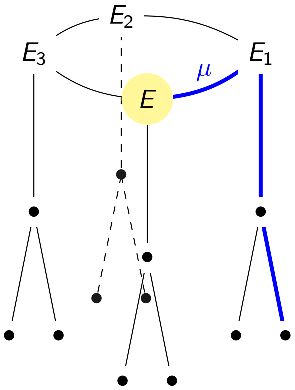
- $\ker(\pi - \mu \mid E[\ell^k]) \simeq (\mathbb{Z}/\ell^k) \times (\mathbb{Z}/\ell^h)$;
- It contains ℓ^h cyclic subgroups of order ℓ^k;
- Each cyclic subgroup is associated to an isogeny that **starts** horizontal;
- $O(\ell^{k+h})$ choices. Sadness.

Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h+1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.

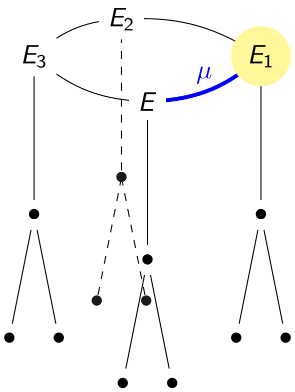


Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h + 1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.

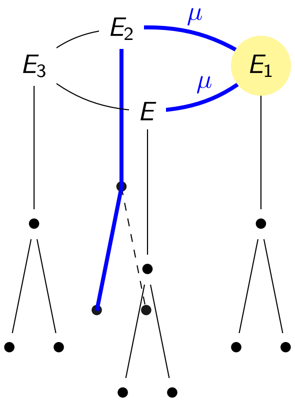


Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h+1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.

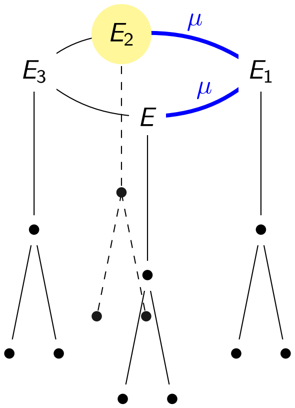


Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h+1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.

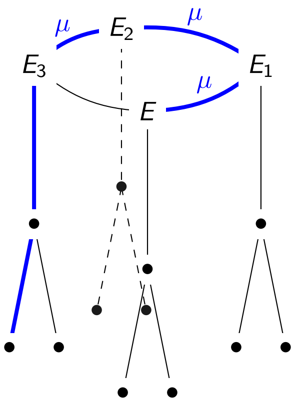


Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h + 1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.

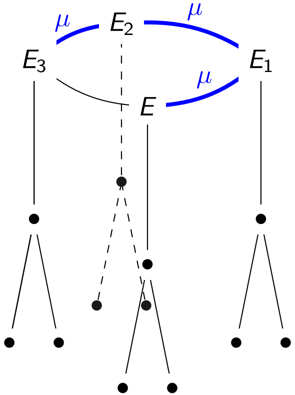


Walking on the crater

Trivial fix: compute a basis of $E[\ell^{k+h}]$, only to obtain only a horizontal decomposition of $E[\ell^k]$.

Much better:

1. Start with **any** walk of length $k \geq h + 1$;
2. First step is horizontal, use it to move to the next curve;
3. Compute again a walk of length k (actually only requires computing one step);
4. etc.



Details I glossed over

Computing in towers of field extensions

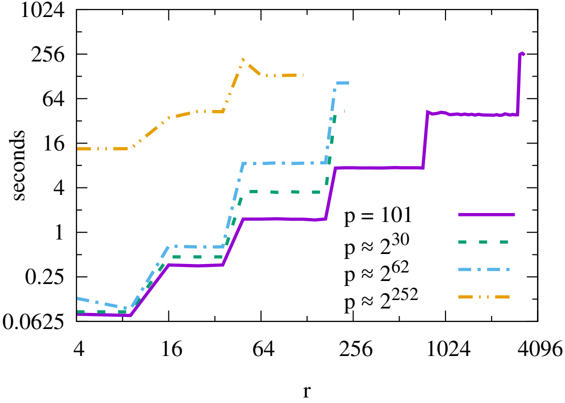
- Torsion points are not defined in $\mathbb{F}_q$, in general.
- We work in ℓ-adic extensions of $\mathbb{F}_q$ using constructions from [LDF, Doliskani, Schost '13], [Doliskani, Schost '15] where in particular we have a fast computation of the Frobenius.

Finding an Elkies prime ℓ

- The complexity depends polynomially on the auxiliary prime ℓ.
- Ideally we would like to work with $\ell = 2$.
- In practice half of all ℓ are expected to be Elkies primes.
- In theory we can only prove $\ell \leq O(\log(q))$ for almost all q and curves E, E' (see [Shparlinski, Sutherland '14]).

Experiments

The algorithm has been implemented on SageMath v7.1 for the case of $\ell = 2$, the code is available on GitHub:
`https://github.com/Hugounenq-Cyril/Two_curves_on_a_volcano`



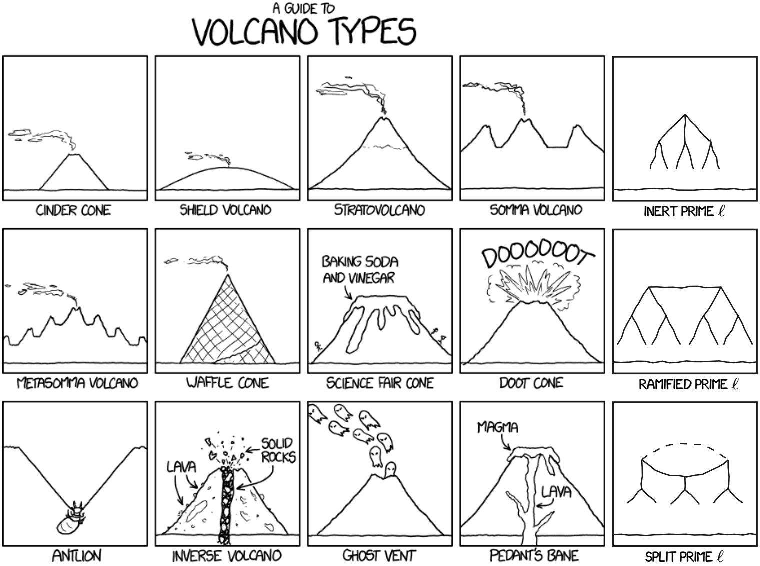
Conclusion

Contribution

- New tools for navigating isogeny volcanoes.
- A faster variant of Couveignes' algorithm.

Future work

- Compare implementation to other algorithms (esp. Lercier-Sirvent).
- Give an analogous algorithm for Atkin primes.
- Analyze our techniques to navigate the volcano in other settings: point counting, computation of endomorphism rings, Hilbert class polynomials, modular polynomials.



Modified from xkcd.com/1714