Explicit isogenies in quadratic time in any characteristic

Luca De Feo, Cyril Hugounenq, Jérôme Plût, Éric Schost

ANTS XII – Kaiserslautern

September 1, 2016

Summary

Refresher on isogenies

Isogenies

- E and E' two elliptic curves, an isogeny is a surjective morphism $\phi : E \to E'$ such that $\phi(0_E) = 0_{E'}$. Isogenies are
  - group morphisms (with finite kernel),
  - algebraic maps (of finite degree).
- If the isogeny has degree ℓ, we call it an *ℓ-isogeny*,
- We say that E and E' are *ℓ-isogenous* if there exist an ℓ-isogeny between them.
- In this talk: only *rational* isogenies (i.e. Galois-equivariant maps).

Refresher on isogenies

Isogenies

- E and E' two elliptic curves, an isogeny is a surjective morphism $\phi : E \to E'$ such that $\phi(0_E) = 0_{E'}$. Isogenies are
  - group morphisms (with finite kernel),
  - algebraic maps (of finite degree).
- If the isogeny has degree ℓ, we call it an *ℓ-isogeny*,
- We say that E and E' are *ℓ-isogenous* if there exist an ℓ-isogeny between them.
- In this talk: only *rational* isogenies (i.e. Galois-equivariant maps).

Example: Let ℓ be an integer, the *scalar multiplication map*

$$\begin{aligned}[\ell] \ : \ & E \to E \\ & P \mapsto \ell \cdot P\end{aligned}$$

is an isogeny of degree ℓ^2.

Explicit isogenies

Explicit isogenies

Separable isogenies of degree ℓ are represented by rational maps in Weierstrass form

$$(x, y) \mapsto \left(\frac{n(x)}{d(x)}, cy \left(\frac{n(x)}{d(x)} \right)' \right)$$

with $n(x)$ a polynomial of degree ℓ and $d(x)$ a polynomial of degree $\ell - 1$.

Vélu's formulas

From the knowledge of its kernel we can explicitly write down the isogeny:

- Let $G = \ker \phi$, then $d(X) = \prod_{P \in G \setminus \{0_E\}} (X - x(P))$;
- Vélu's formulas: from $d(X)$ we deduce $n(X)/d(X)$;

Motivation

Explicit isogeny computation problem

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

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].

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], [De Feo '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.

$\rightarrow$ We want to 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: $\phi : E \to E'$ 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 such that $L(x(uP)) = x(a\,u\,P')$ for all $u \in \mathbb{Z}/p^k\mathbb{Z}$; $\tilde{O}(rp^{O(1)})$
   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 such that $L(x(uP)) = x(a\,u\,P')$ for all $u \in \mathbb{Z}/p^k\mathbb{Z}$; $\tilde{O}(rp^{O(1)})$
   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.

Goal

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

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

An ℓ-adic Couveignes' algorithm?

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

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

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 $\psi : E \to E'$, i.e.

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

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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

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

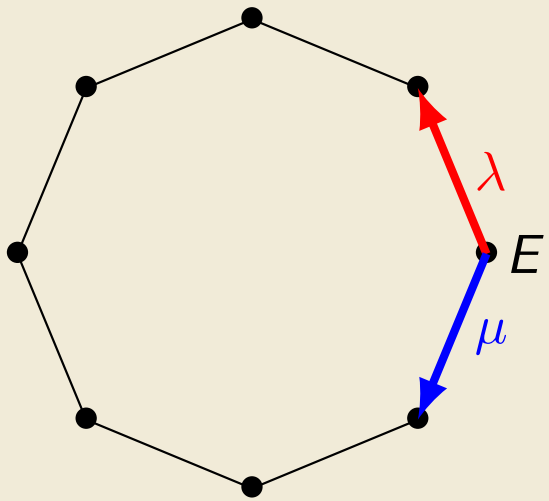
Subgroup of size ℓ	$\Leftrightarrow$	ℓ-isogeny
Subgroup of size ℓ stable by π	$\Leftrightarrow$	Rational ℓ-isogeny

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

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

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

Isogeny graph

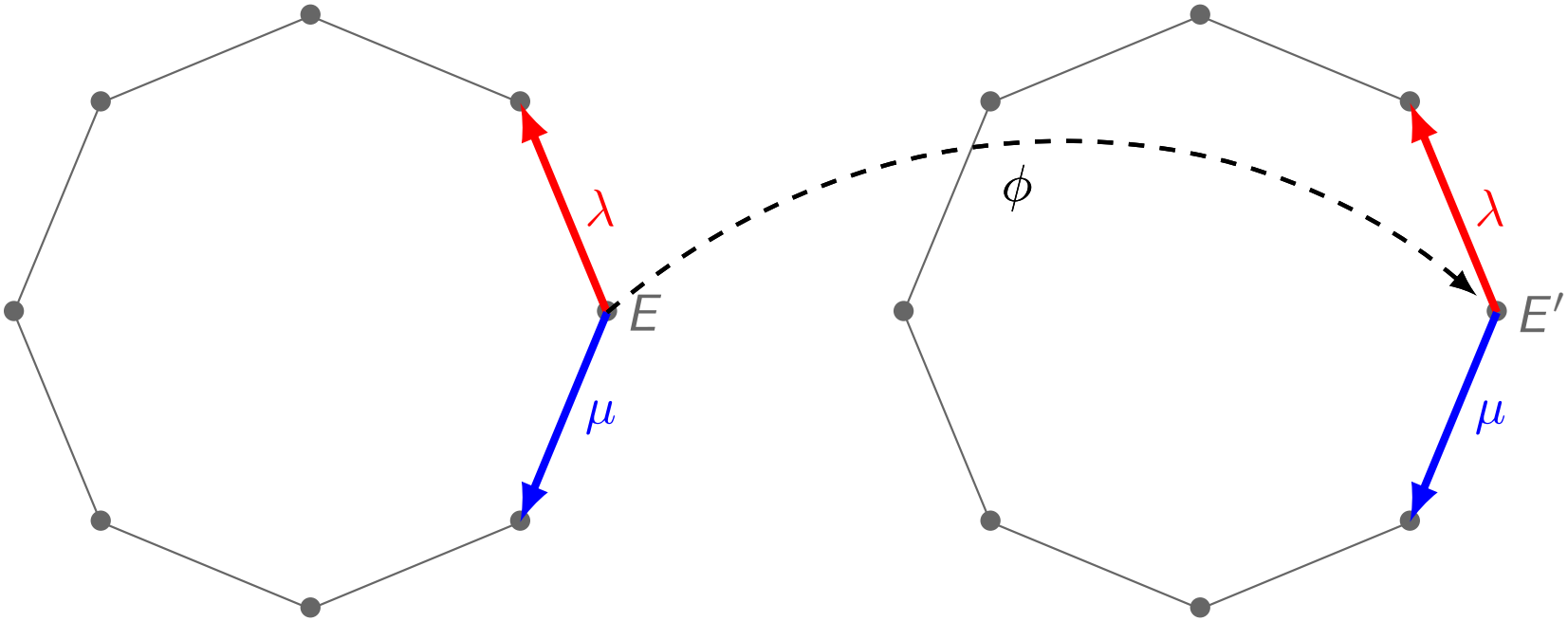


UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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.

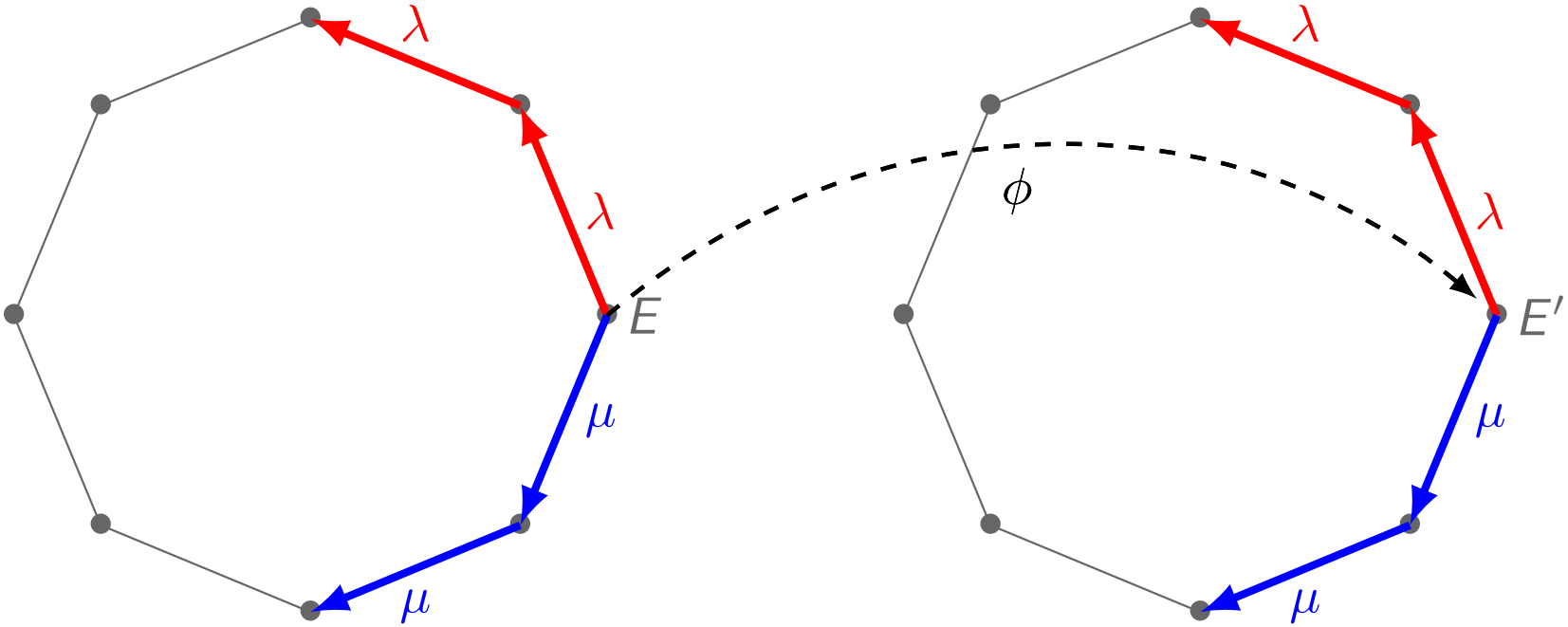


UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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.

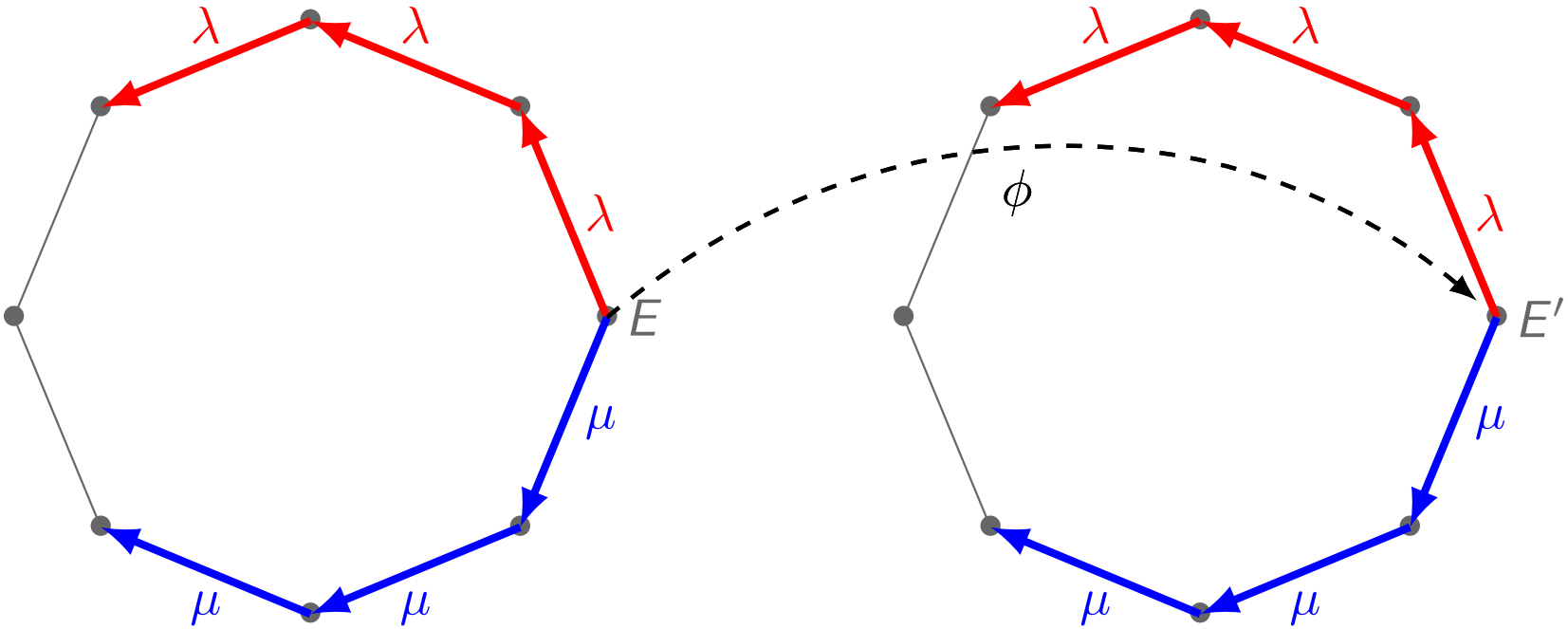


UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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].

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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.

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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

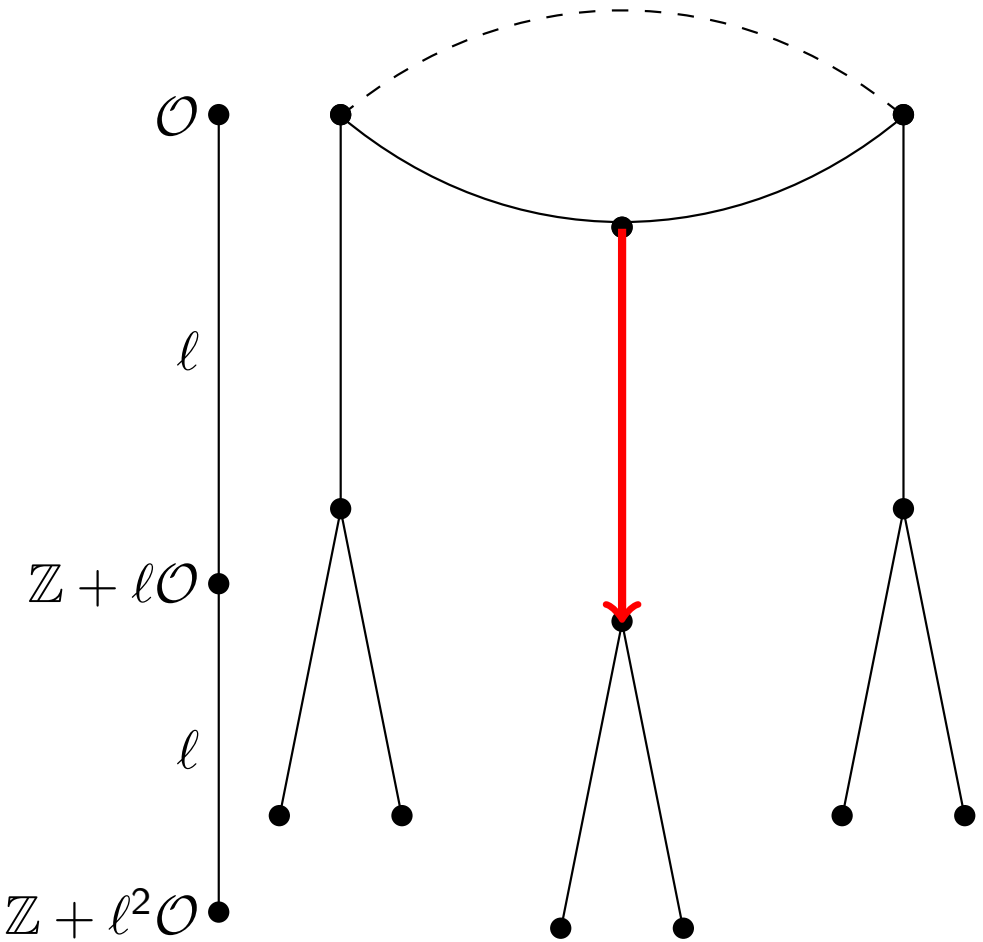
Input: E, E' two r-isogenous curves on $\mathbb{F}_q$
Output: $\phi : E \to E'$ of degree r

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 $(\mathbb{Z}/\ell^k\mathbb{Z})^{2\times 2}$: $O(r)$
   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.

The general case

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



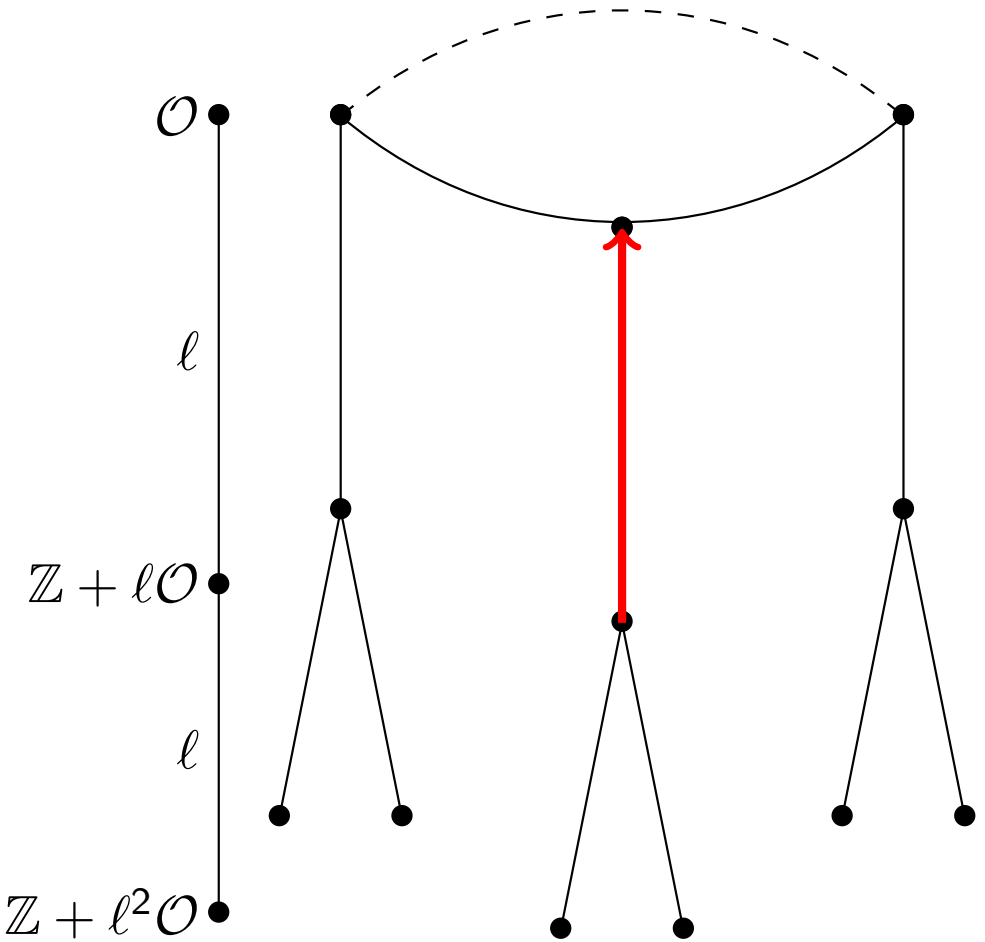
Lemma (Kohel 1996)

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 $\mathcal{O} = \mathcal{O}'$.

The general case

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



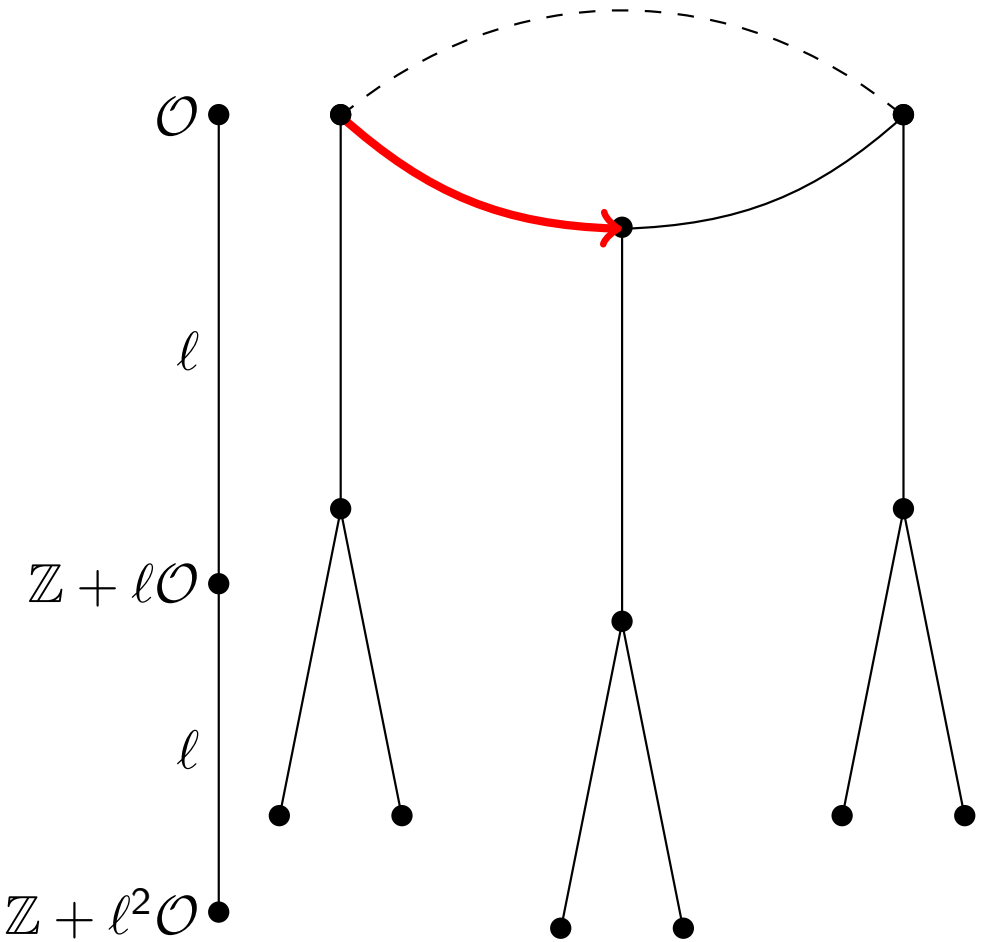
Lemma (Kohel 1996)

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 $\mathcal{O} = \mathcal{O}'$.

The general case

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

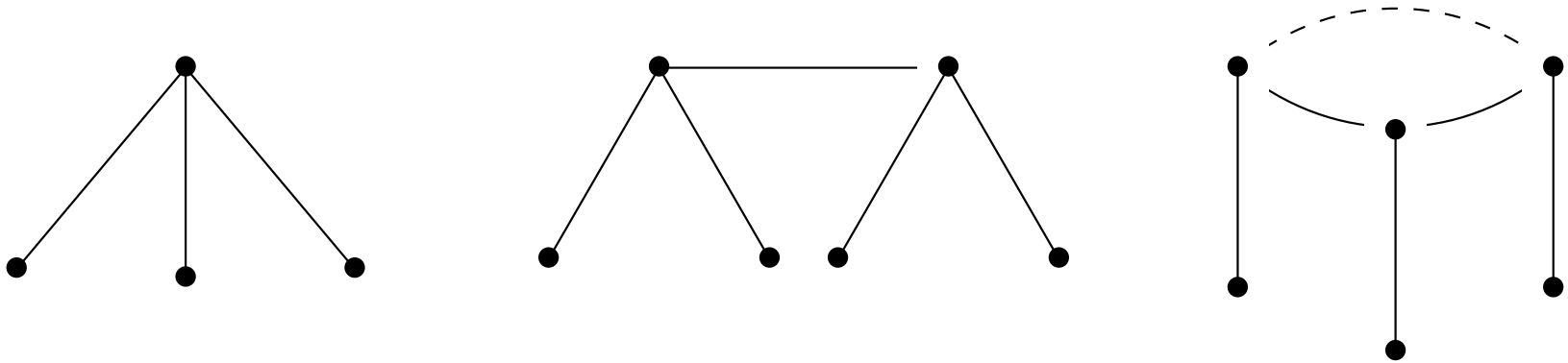


Lemma (Kohel 1996)

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



Inert prime ℓ Ramified prime ℓ Split prime ℓ

Figure: The three shapes of volcanoes of 2-isogenies

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

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

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 $\geqslant 1$.

Since for any $P \in E[\ell^h]$ we have:

$$\pi(P) = \lambda P = \mu P$$

we cannot immediately distinguish kernels of isogenies with direction λ from those with direction μ.

Thus we have to work with $E[\ell^{h+1}]$ to get $P \in E[\ell^{h+1}]_\lambda$ such that:

$$\pi(P) = \lambda P \neq \mu P$$

We must therefore now assume that $k \geqslant h + 1$.

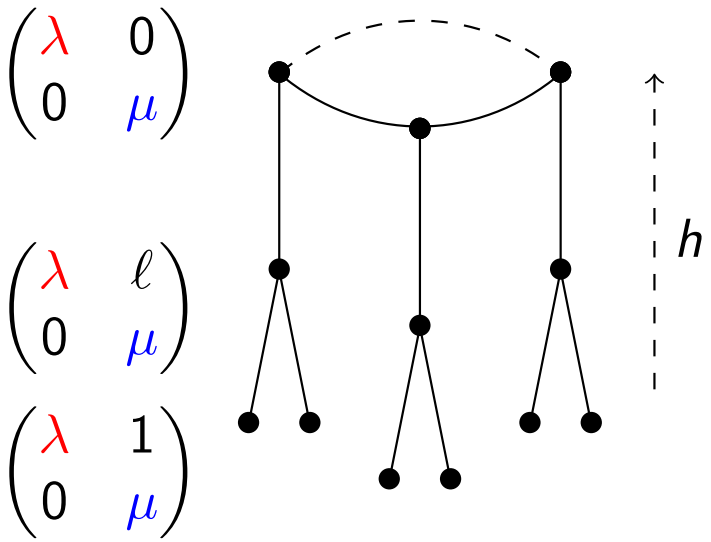
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

Proposition (De Feo, H., 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

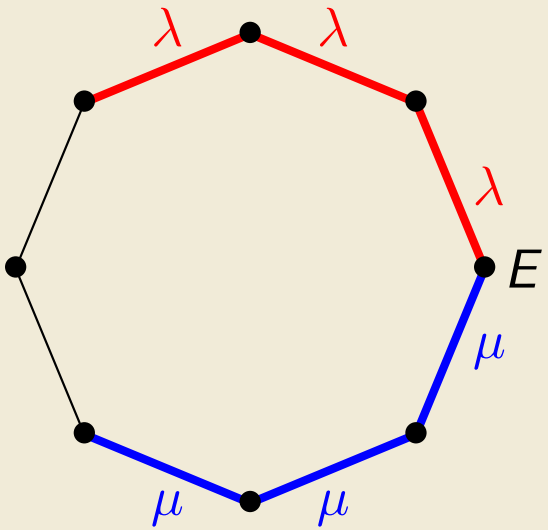
$$\begin{pmatrix} \lambda & a \\ 0 & \mu \end{pmatrix},$$

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



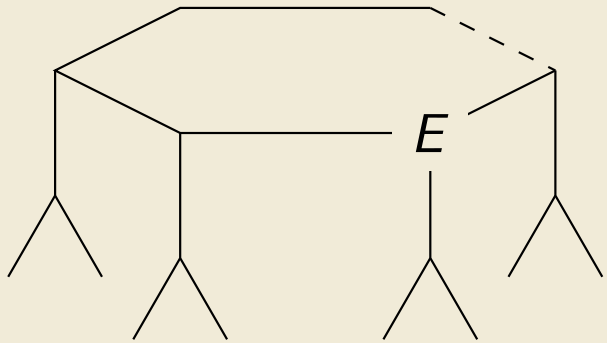
We assume that E lies on the crater (we can reduce to this case easily).

Volcano with height $h = 0$



$\ker(\pi - \mu \mid E[\ell^k])$ is a cyclic group of size ℓ^k.

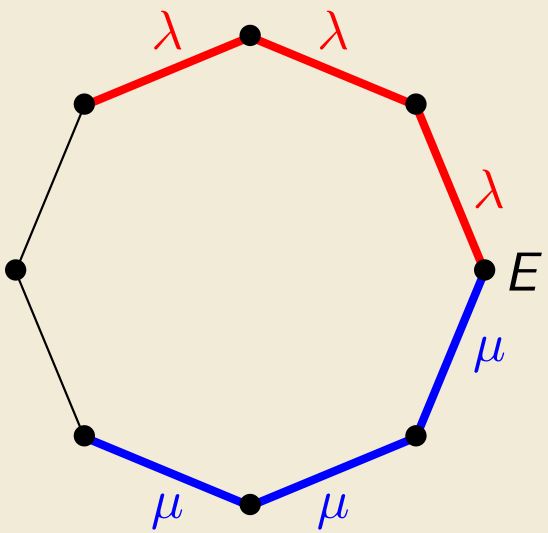
Volcano with height $h = 2$



Problem: if $h \geqslant 1$ then $\ker(\pi - \mu \mid E[\ell^k]) \simeq (\mathbb{Z}/\ell^k) \times (\mathbb{Z}/\ell^h)$ is not cyclic, and contains ℓ^h cyclic subgroups of order ℓ^k.

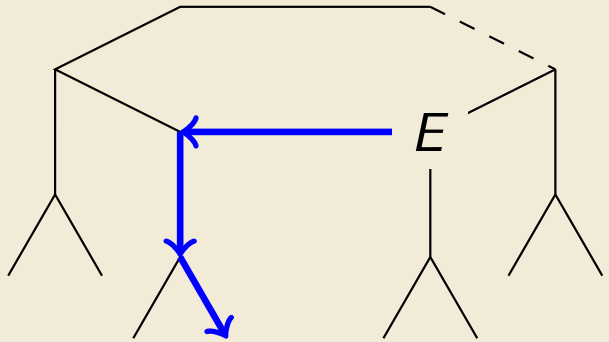
We assume that E lies on the crater (we can reduce to this case easily).

Volcano with height $h = 0$



$\ker(\pi - \mu \mid E[\ell^k])$ is a cyclic group of size ℓ^k.

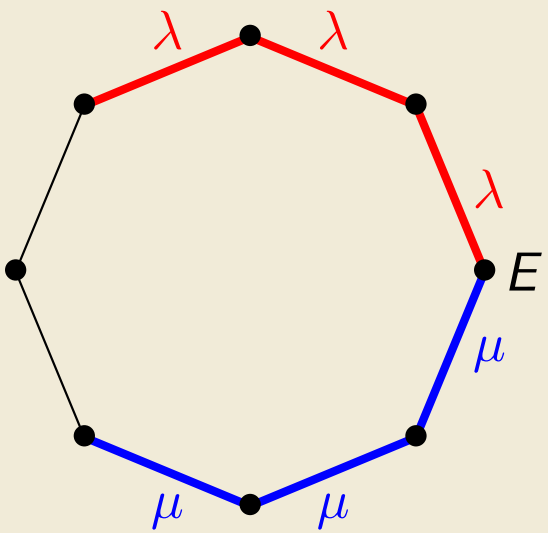
Volcano with height $h = 2$



Problem: if $h \geqslant 1$ then $\ker(\pi - \mu \mid E[\ell^k]) \simeq (\mathbb{Z}/\ell^k) \times (\mathbb{Z}/\ell^h)$ is not cyclic, and contains ℓ^h cyclic subgroups of order ℓ^k.

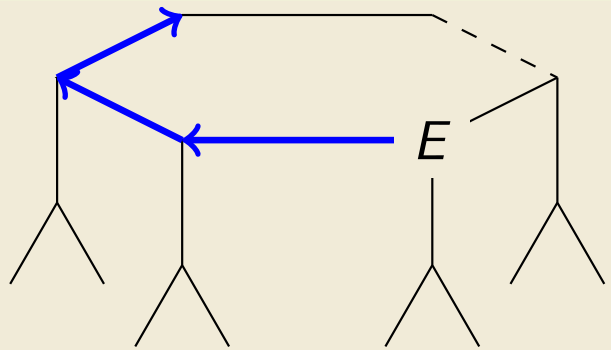
We assume that E lies on the crater (we can reduce to this case easily).

Volcano with height $h = 0$



$\ker(\pi - \mu \mid E[\ell^k])$ is a cyclic group of size ℓ^k.

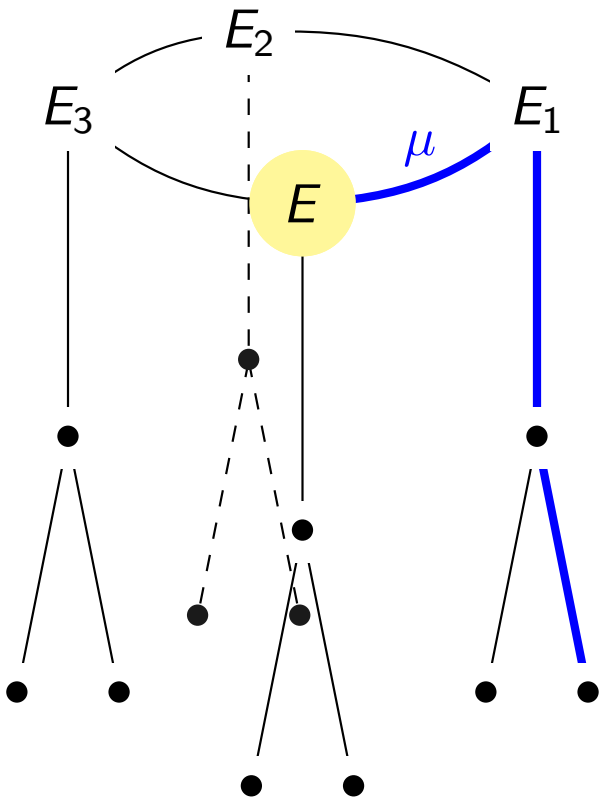
Volcano with height $h = 2$



Problem: if $h \geqslant 1$ then $\ker(\pi - \mu \mid E[\ell^k]) \simeq (\mathbb{Z}/\ell^k) \times (\mathbb{Z}/\ell^h)$ is not cyclic, and contains ℓ^h cyclic subgroups of order ℓ^k.

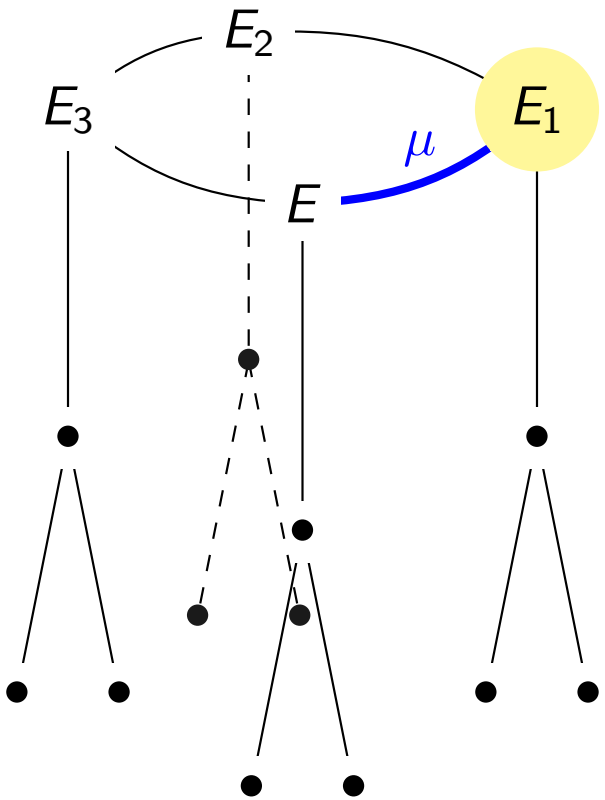
Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



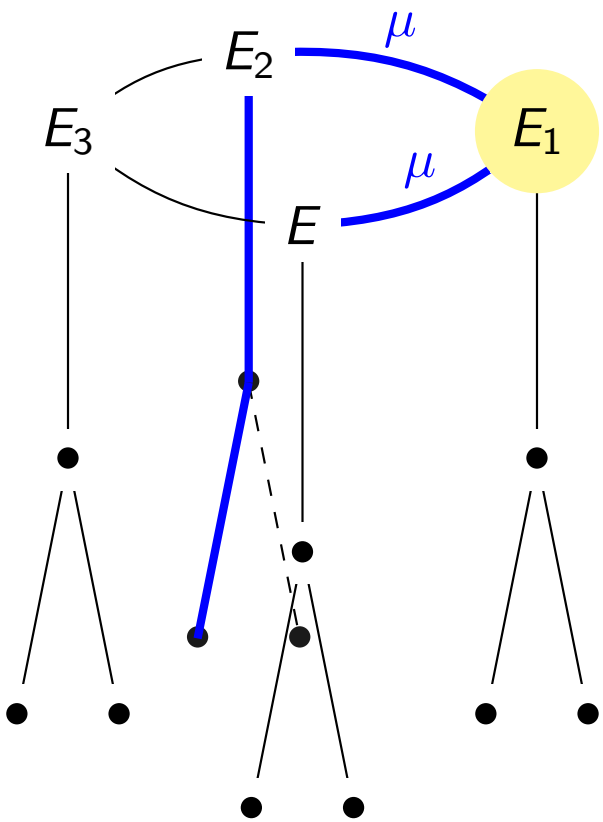
Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



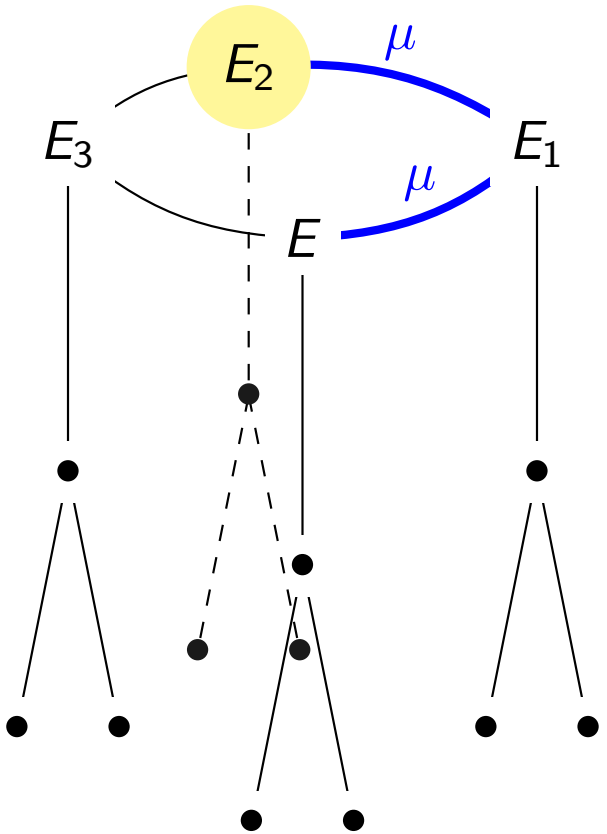
Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



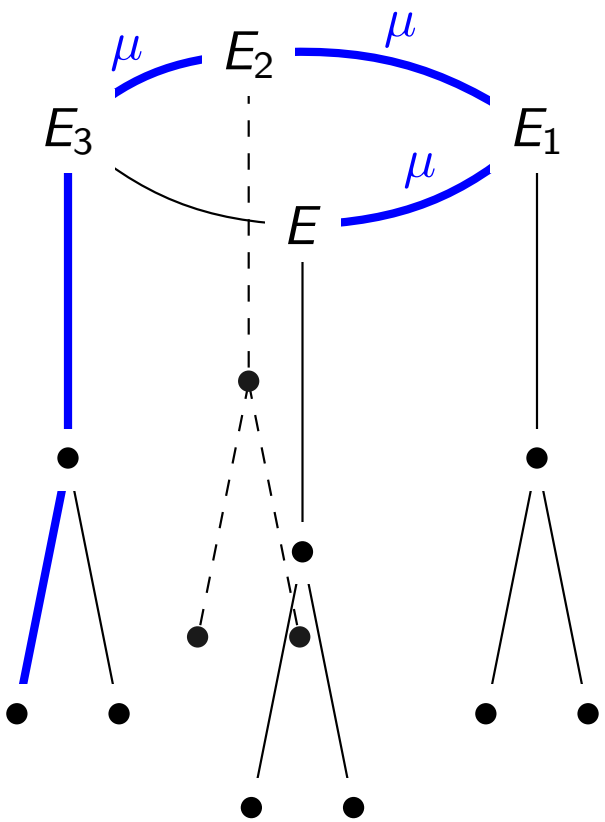
Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



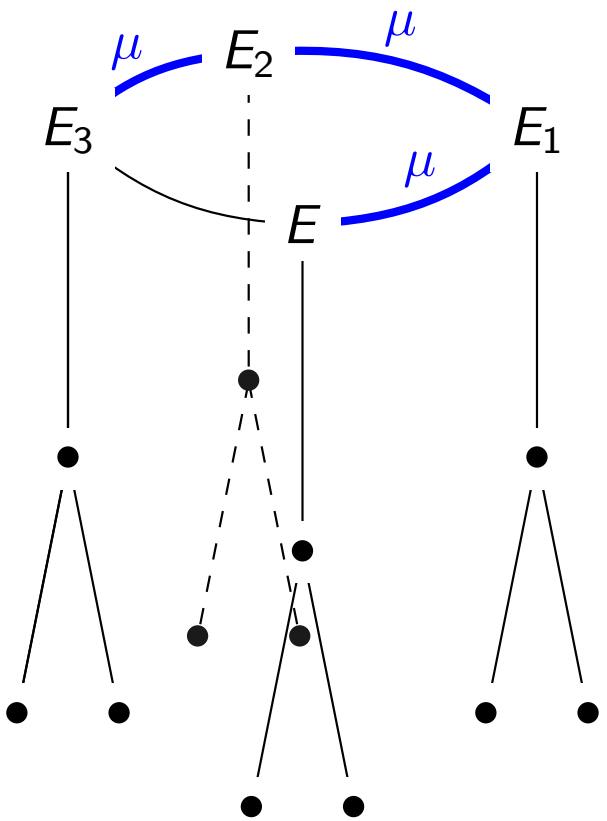
Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



Walking on the crater

Goal: compute the kernel of horizontal ℓ^k-isogenies (codomain curves lying on the crater).
We proceed step by step by walking along the volcano crater according to the direction μ.



Technical details

Computing in towers of field extensions

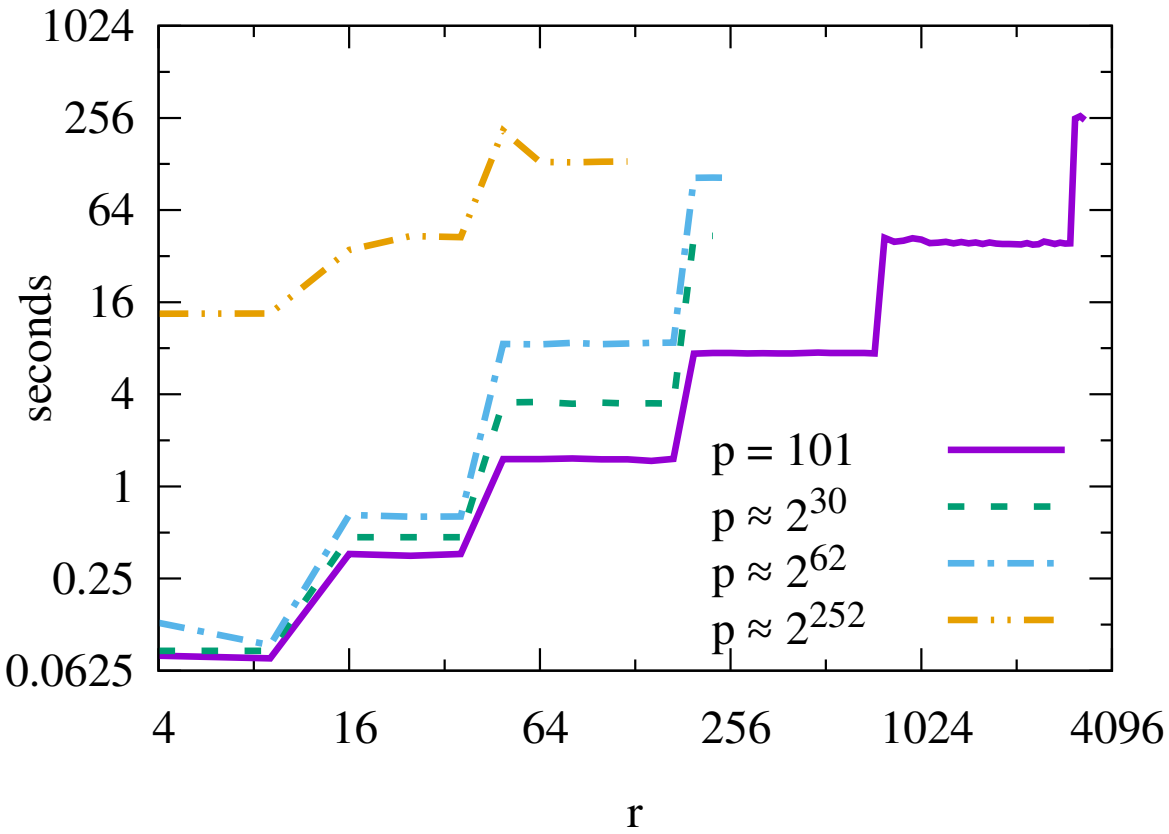
- Torsion points are not defined in $\mathbb{F}_q$, in general.
- We work in ℓ-adic extensions of $\mathbb{F}_q$ using constructions from [De Feo, Doliskani, Schost '13], [Doliskani, Schost '15] where in particular we have a fast computation of the Frobenius.

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`



UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

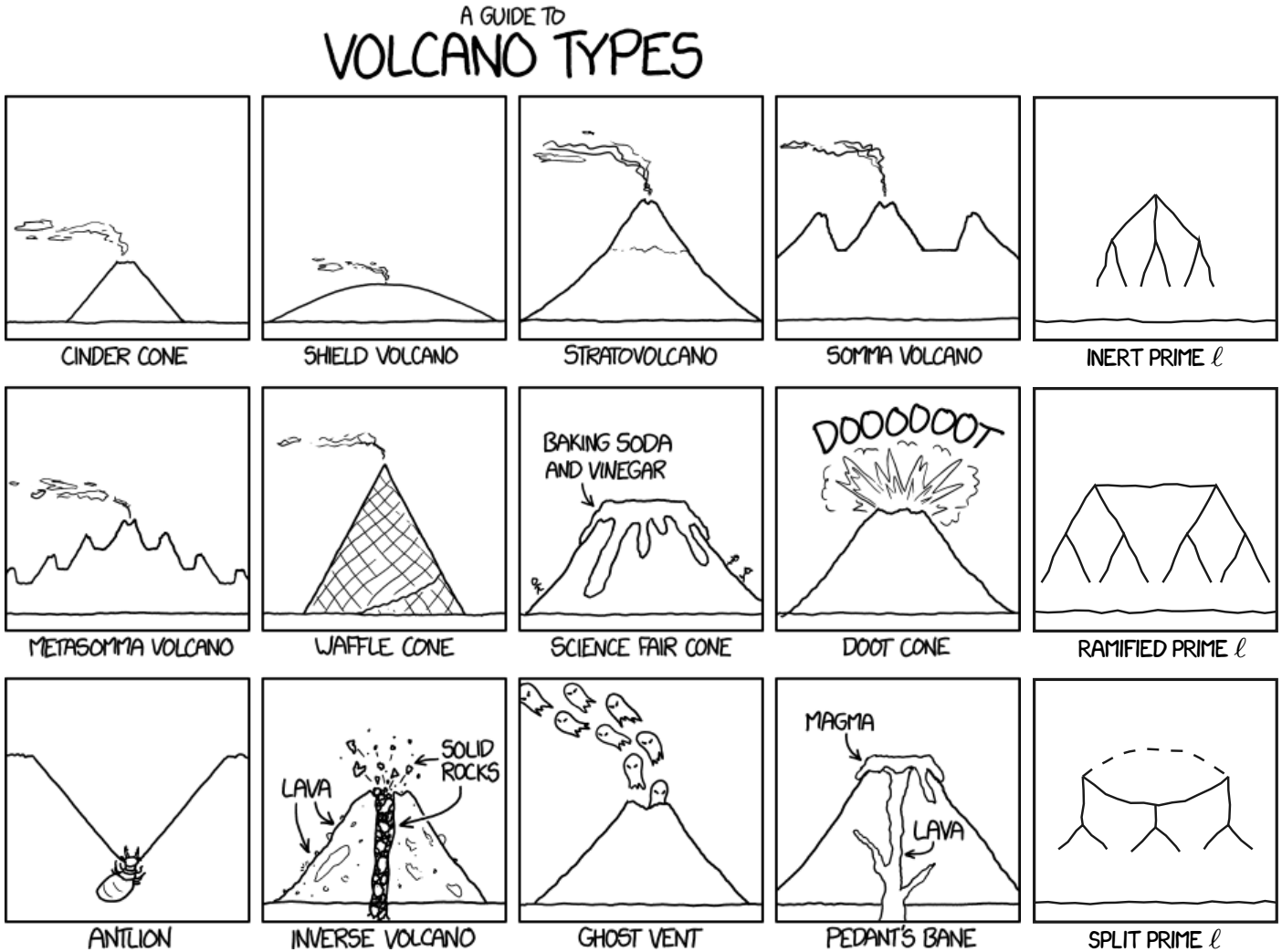
Conclusion

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