Structure of Volcano of ℓ-isogeny applied to Couveignes's algorithm

Luca De Feo, Cyril Hugounenq, Jerome Plut, Eric Schost

Université Versailles Saint Quentin en Yvelines, Paris-Saclay

March 15, 2016

digiteo
Research in science and technology of information

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

Summary

1. Reminder on elliptic curves,
2. Endomorphism ring of elliptic curves following Kohel in 1996 [5],
3. Volcanoes of ℓ-isogenies and Frobenius endomorphism,
4. Working on ℓ-adic tower.

Reminder on elliptic curves

$\mathbb{F}_q$ a finite field of characteristic p.

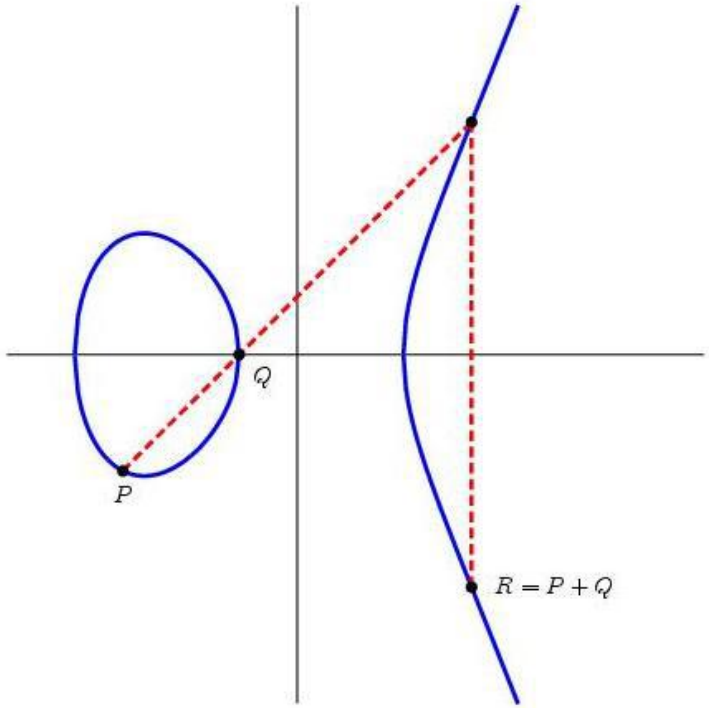
Definition

E an elliptic curve defined over $\mathbb{F}_q$, we denote by :

$$E(\mathbb{F}_q)$$

the set of rational points of E over $\mathbb{F}_q$

During all this presentation we will consider only elliptic curves on the finite field $\mathbb{F}_q$, ℓ is a prime different from p



Definition (m torsion points)

$m \in \mathbb{N}$, we denote by

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

Reminder on isogenies

Definition (isogeny)

E and E' two ellitpic curves, $\phi : E \to E'$ a surjective morphism such that $\phi(0_E) = 0_{E'}$, then ϕ is an isogeny. An isogeny is a group morphism. We say that E and E' are isogenous if there exist an isogeny ϕ between the two curves.

Proposition

E and E' two ellitpic curves, $\phi : E \to E'$ an isogeny, if ϕ is **separable**, then we have:

$$\deg \phi = |\ker(\phi)|$$

Definition

E and E' two elliptic curves and ℓ a prime number, $\phi : E \to E'$ a non constant isogeny. We say that ϕ is an ℓ-isogeny if we have $\deg \phi = \ell$

Theorem (Tate)

E and E' two elliptic curves and $\phi : E \to E'$ an isogeny. Then

$$|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$$

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

Theorem

E, E' two elliptic curves. There is a bijection between finite subgroups of E' and separable isogenies :

$$\begin{array}{ccc} (\phi : E \to E') & \mapsto & \ker \phi \\ (E \to {}^{E}/_{C}) & \leftarrow\!\shortmid & C \end{array}$$

Remark

E an elliptic curve defined over $\mathbb{F}_q$, let ℓ be a prime different from p, then we define an ℓ-isogeny by a primitive ℓ-torsion point: P

$$\phi : E \to E/\langle P \rangle$$

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

Isogeny computation

Couveignes's algorithm [1] in $O(r^2)$

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

Main steps of Couveignes's algorithm:

1. determine p^k primitive torsion points on E and E' with $p^k > 4r$,
2. since $E[p^k]$ is cyclic, the algorithm just has to interpolate p^k torsion points on p^k torsion points according to the group law,
3. test if the interpolation is good,
4. if the test is good, then return the isogeny.

Mainly used in S.E.A. for counting points

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

Isogeny computation

Other existing algorithms

1. .[BMSS] et [CCR] work only for $r \ll p$ in $O(M(r)\log(r))$
2. p-adic algorithms [Satoh] with p fixed are exponential in $\log(p)$
3. .[LS08] works for every p in $O(r^2)$

Definition (Endomorphism ring)

$\mathrm{End}(E) = \{\text{isogenies} \phi : E \to E\}$ is a ring with the addition law and composition law.

Remark

We have $\mathbb{Z} \subset \mathrm{End}(E)$

Definition (Frobenius Endomorphism)

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

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

is called Frobenius endomorphism. It belongs to $\mathrm{End}(E)$.

Remark

E an elliptic curve defined over $\mathbb{F}_q$, then we always have

$$\mathbb{Z}[\pi] \subset \mathrm{End}(E)$$

.

Proposition

E an elliptic curve defined over $\mathbb{F}_q$ is ordinary if it satisfies any of the two equivalent conditions:

1. $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$
2. $\mathrm{End}(E)$ is isomorphic to an order in a quadratic imaginary extension of $\mathbb{Q}$.

From now we will only work with ordinary elliptic curves.

Definition

An order in a quadratic imaginary number field K is a

1. subring of K
2. a $\mathbb{Z}$-modulus of rank 2

Definition

We denote by $\mathcal{O}_K$ the algebraic integers of K.

We can associate to any elliptic curve E his endomorphism ring:

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

We will denote $\mathcal{O}$ (resp. $\mathcal{O}'$) the $\mathrm{End}(E)$ (resp. $\mathrm{End}(E')$) up to isomorphism.

Remark

For an ordinary elliptic curve we have:

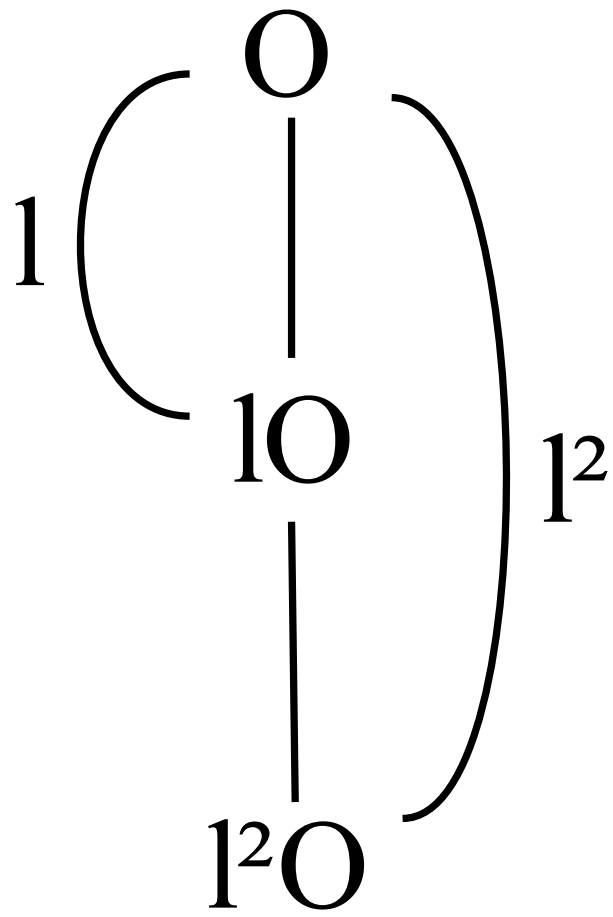
$$\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$$

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

Lemma (Kohel 1996)

E and E' two elliptic curves defined over $\mathbb{F}_q$, $\phi : E \to E'$ an ℓ-isogeny, with $\ell \neq p$. Then

1. $\ell = [\mathcal{O} : \mathcal{O}']$ we say then that ϕ is a descending isogeny,
2. $\ell = [\mathcal{O}' : \mathcal{O}]$ we say then that ϕ is an ascending isogeny,
3. $\mathcal{O} = \mathcal{O}'$ we say then that ϕ is an horizontal isogeny.



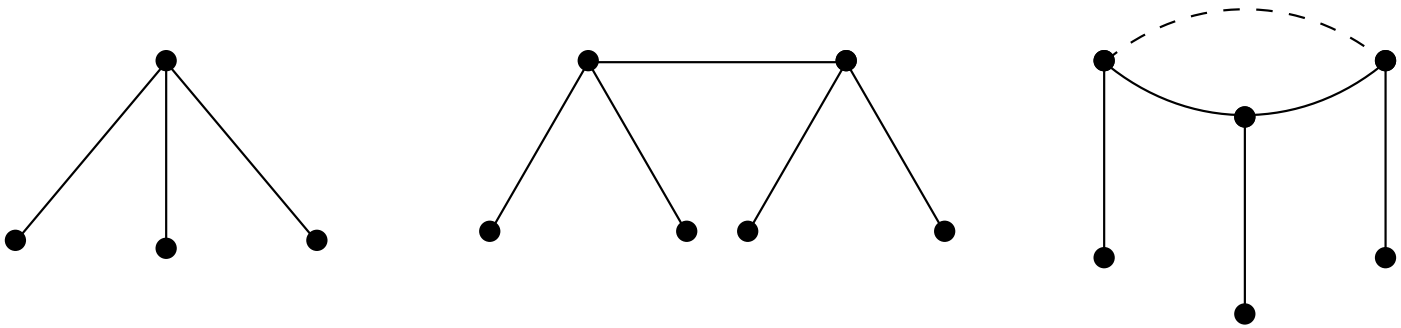


Figure: The three shapes of volcanoes of 2-isogenies

Remark

In the rest of this talk we consider only volcanoes with cyclic crater (i.e. $(d_K/\ell) = +1$), so that ℓ is an Elkies prime for these curves.
This implies that the Frobenius automorphism on $T_\ell(E)$, which we write $\pi|T_\ell(E)$, has two distinct eigenvalues $\lambda \neq \mu$.
The depth of the volcano of $\mathbb{F}_q$-rational ℓ-isogenies is $h = v_\ell(\lambda - \mu)$.

Proposition

Let E be a curve on a volcano of ℓ isogeny with cyclic crater. Then there exists a unique $a \in \{0, \ell, \ldots, \ell^{h-1}\}$ such that $\pi|T_\ell(E)$ is conjugate, over $\mathbb{Z}_\ell$, to the matrix $\left(\begin{smallmatrix} \lambda & a \\ 0 & \mu \end{smallmatrix}\right)$.
Moreover $a = 0$ if E lies on the crater.

Definition (Horizontal and diagonal bases)

Let E be a curve lying on the crater. We call a basis of $E[\ell^k]$

diagonal if π is diagonal in it;

horizontal if the basis is diagonal and both basis points generate the kernel of horizontal ℓ^k-isogenies.

Accordingly, we also call diagonal (resp. horizontal) the generators of a diagonal (resp. horizontal) basis.

Proposition

Let E be a curve lying on the crater and P be a point of $E[\ell^k]$. Then $\ell^h P$ is horizontal if, and only if, P is an eigenvector for π. If $\pi(P) = \lambda P$ then we say that $\ell^h P$ has direction λ.

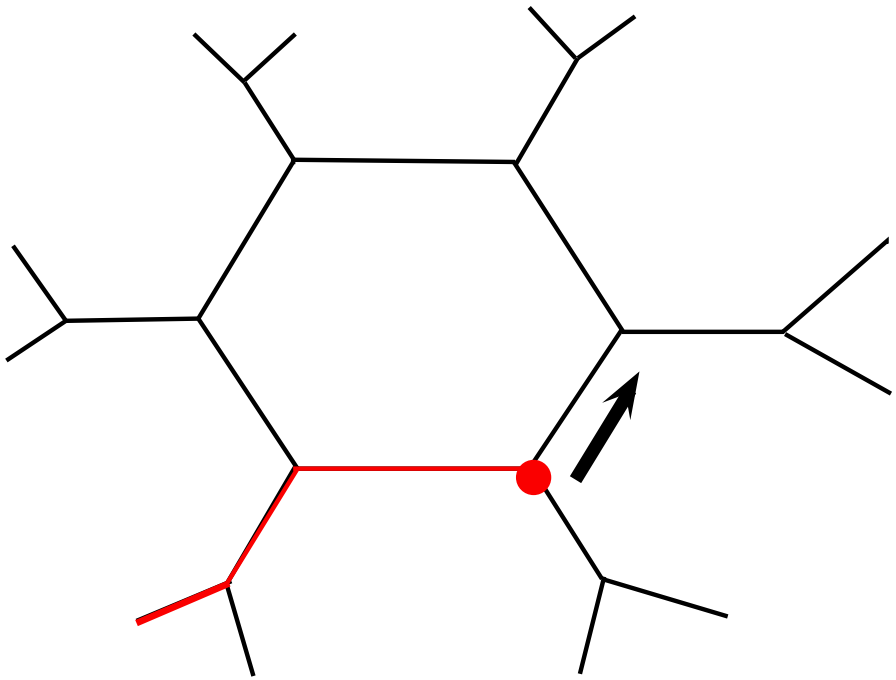
How to construct an horizontal basis

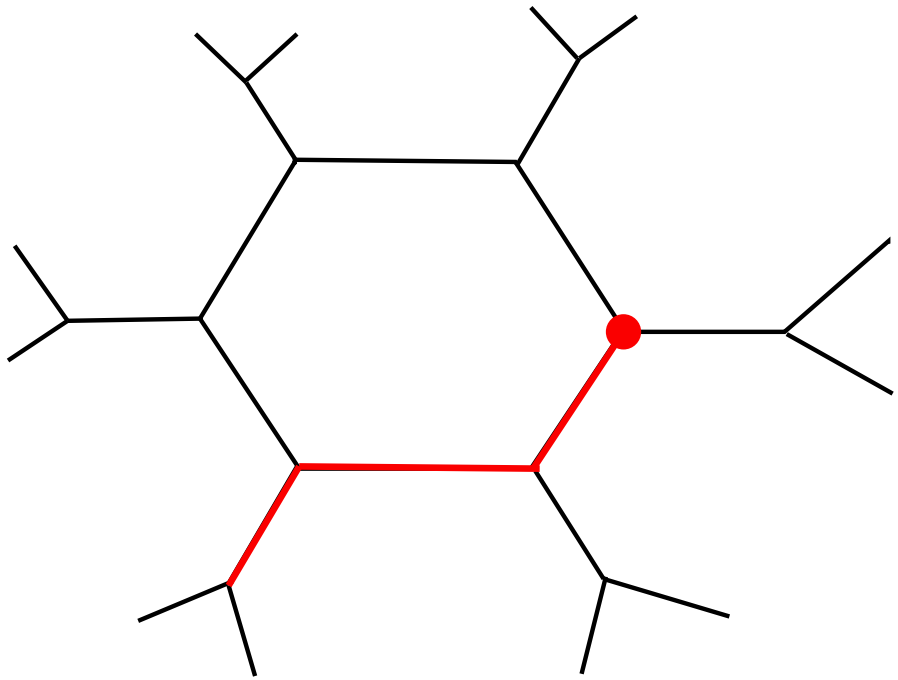
Proposition

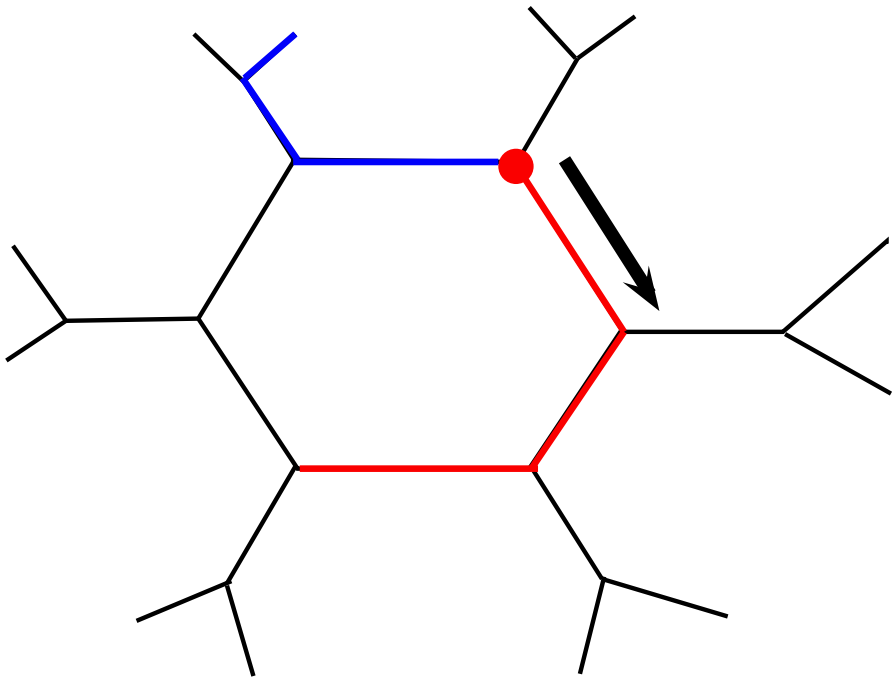
Let $\psi : E \to E'$ be a horizontal ℓ-isogeny with direction λ. For any point $Q \in E[\ell^\infty]$, if ℓQ is horizontal with direction μ, then $\psi(Q)$ is horizontal with direction μ.

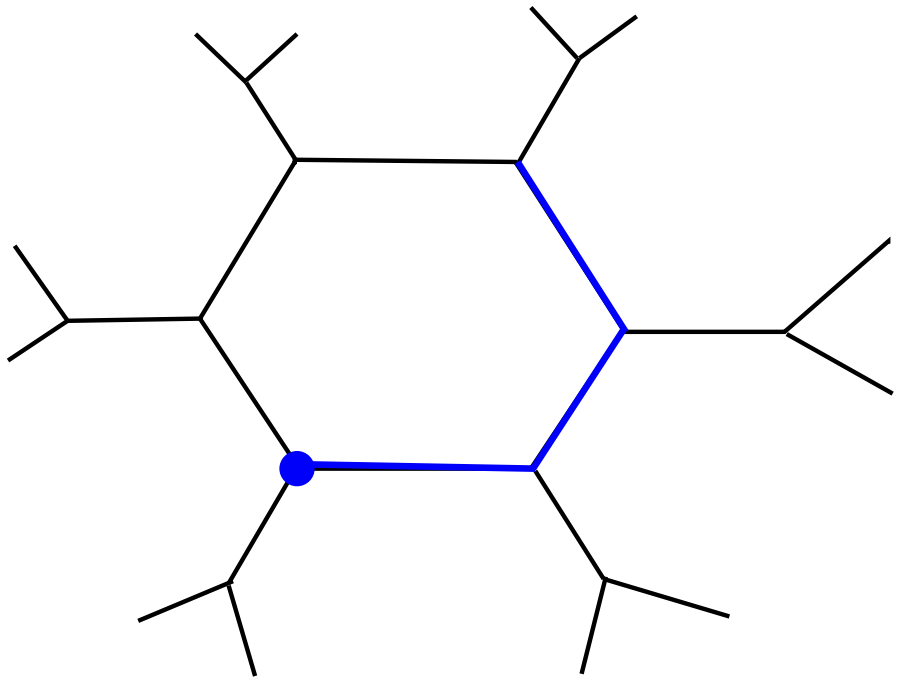
Remark

We could have computed directly an horizontal basis of the ℓ^k torsion, but it would have a cost too high implying the computation of the ℓ^{h+k} torsion.









Proposition

Let $\psi : E \to E'$ be an isogeny of degree r prime to ℓ.

1. The curves E and E' have the same depth in their ℓ-isogeny volcanoes.
2. For any point $P \in E[\ell^k]$, the isogenies with kernel $\langle P \rangle$ and $\langle \psi(P) \rangle$ have the same type (ascending, descending, or horizontal with the same direction).
3. If $P \in E[\ell]$ and $P' \in E'[\ell]$ are both ascending, or both horizontal with the same direction, then E/P and E'/P' are again r-isogenous.

Remark

In particular we have the image of an horizontal basis of E which is still an horizontal basis of E'.

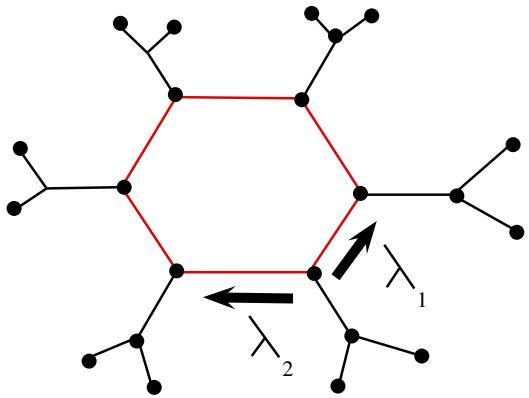
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

Advantages of the Frobenius

Remark

E an elliptic curve defined over $\mathbb{F}_q$. Thanks to the *Frobenius*,

- $\Rightarrow$ we can distinguish the two paths of length k on the crater starting from E,
- $\Rightarrow$ we can associate two set of ℓ^k primitive torsion points generating the ℓ^k isogeny,
- $\Rightarrow$ we have horizontal basis of $E[\ell^k]$.



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

ℓ-adic tower and rational ℓ-torsion points

Remark

As in Couveignes's algorithm we need to determine the image of a number N of points such that: $N > 4r$

Remark

An ℓ-adic extension of a Kummer tower permits to increase of 1 the height of the volcano and of 1 the ℓ-adic valuation of points defined on the curve.

Thus to have enough higher ℓ^k torsion points defined on the field we work, we could need to take several ℓ-adic extension.
To work efficiently on this ℓ-adic tower we work with the construction by [Doliskani-Schost '15] for $\ell = 2$ and [De Feo-Doliskani-Schost '13] for $\ell \neq 2$.

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

Improving interpolation with the Frobenius

Since the Frobenius acts on ℓ^k torsion points and the isogeny is defined over $\mathbb{F}_q$ the action of the Frobenius doesn't change the value of the isogeny thus of the interpolation polynomial.

Remark

With the action of the Frobenius we have only representative points to interpolate.

Summarizing, our algorithm for two curves on a cyclic crater of a volcano of ℓ-isogeny as follows:

1. Compute horizontal bases (P, Q) of $E[\ell^k]$ and (P', Q') of $E'[\ell^k]$;
2. Compute the polynomial T vanishing on the abscissas of $\langle P, Q \rangle$ using the method of [De Feo '07];
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 $L_{a,b}$ such that $L_{a,b}(x(uP + vQ)) = x(a\,u\,P' + b\,v\,Q')$ for all $u, v \in \mathbb{Z}/\ell^k\mathbb{Z}$;
   2. Use the *Cauchy interpolation algorithm* to compute a rational fraction $F_{a,b} = L_{a,b} \bmod T$ of degrees $(r, r-1)$;
   3. If $F_{a,b}$ defines an isogeny of degree r, return it and stop.

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

Completing the algorithm for all curves

For curves which are not on a cyclic crater of a volcano of ℓ-isogeny The entire algorithm:

1. we have to find a suitable ℓ such that the volcano of ℓ isogeny has a cyclic crater
2. find curves on the crater

$\Rightarrow$ To respond to those 2 points we have to use algorithms like the one of Fouquet-Morain.

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

Conclusion

We have seen a way to determine horizontal basis of the ℓ^k torsion through the structure of voclanoes with cyclic crater and the use of the Frobenius.
With this determination we have less points to try to interpolate.
We also have seen that the Frobenius permits us to fasten the interpolation.
We still have to

1. determine what we can do if we are not on a cyclic crater of a volcano,
2. compare with what we can do with pairings.


Jean Marc Couveignes.
Computing l-isogenies using the p-torsion.
In Henri Cohen, editor, *ANTS*, volume 1122 of *Lecture Notes in Computer Science*, pages 59–65. Springer, 1996.


Javad Doliskani and Éric Schost.
Computing in degree 2^k-extensions of finite fields of odd characteristic.
Des. Codes Cryptography, 74(3):559–569, 2015.


Mireille Fouquet.
Anneau d endomorphismes et cardinalite des courbes elliptiques.
PhD thesis, Ecole polytechnique, 2001.


Mireille Fouquet and François Morain.
Isogeny volcanoes and the sea algorithm.
In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.


David R. Kohel.
Endomorphism rings of elliptic curves over finite fields.

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