Graph structure of isogeny on elliptic curves

Hugounenq Cyril

Université Versailles Saint Quentin en Yvelines

October 23, 2014

Outline of the talk

1. Reminder about elliptic curves,
2. Endomorphism ring of elliptic curves following Kohel in 1996 [4],
3. Volcanoes of ℓ-isogenies following Fouquet and Morain in 2001 [1] , [2],
4. Group structure of the ℓ-torsion in the volcano, following Miret and al. [5] in 2005 and Ionica and Joux [3] in 2010,
5. Study of the action of the Frobenius on ℓ torsion points.

Reminder on elliptic curves

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

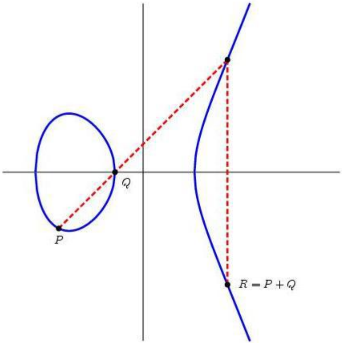
Definition

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)

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, $\phi : E \rightarrow E'$ 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, $\phi : E \rightarrow E'$ 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

E and E' two elliptic curves and ℓ a prime number, $\phi : E \to E'$ an ℓ isogeny. Then

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

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

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

Definition (Endomorphism ring)

$\mathrm{End}(E) = \{\mathrm{isogenies} \phi : E \to E\}$ 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:

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

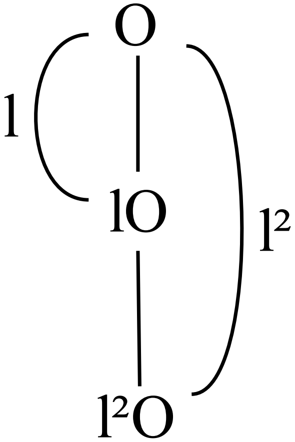
Lemma (Kohel 1996)

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

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

Definition

The index $f = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of $\mathcal{O}$.



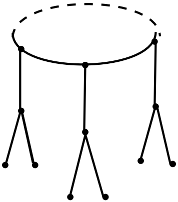


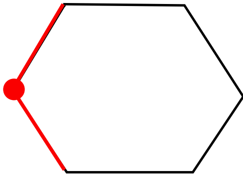
Figure : Volcano with cyclic crater

Figure : Volcano with one point on the crater, and two points

Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	•
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		



Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	•
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		

Proposition (Kohel 1996)

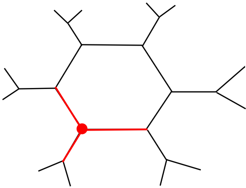
Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	$\bullet$
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		

Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

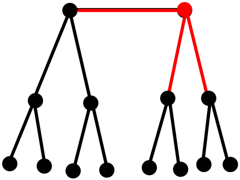
Case	Case	Case	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	•
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		



Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

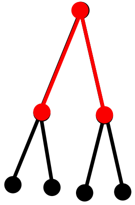
Case	Case	Case	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	•
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		



Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

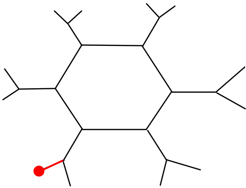
Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	•
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		



Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

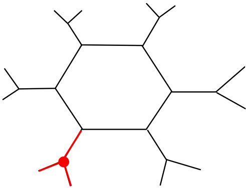
Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		•
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		



Proposition (Kohel 1996)

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$ depending on wether l splits, is ramified or inert in $\mathcal{O}$:

Case	Case	Case	Draw
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ splits	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is ramified	
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$	ℓ is inert	
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$		$\bullet$



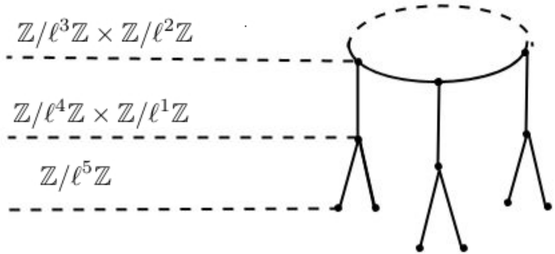
Structure of the ℓ-torsion on the volcano

Proposition

The structure of ℓ-torsion of an ordinary elliptic curve defined over $\mathbb{F}_q$ is:

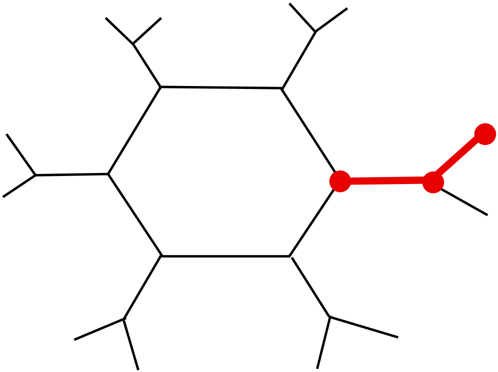
$$E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^h\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$$

with $h \geqslant j \geqslant 0$, $h + j = \nu_\ell(|E(\mathbb{F}_q)|)$ et $j \leqslant \nu_\ell(q-1)$



Motivation

From now we will work with $\ell = 2$. Our goal is to have a way to determine a descending path on the volcano.



Study of the action of the Frobenius endomorphism

Line of work

E an elliptic curve defined over $\mathbb{F}_q$ and ℓ a prime different from p, such that:

$$E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^h\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$$

with $h \geqslant j+1$. We will now focus on the action of the Frobenius endomorphism on the ℓ^{j+1}-torsion points.

P and Q two points such that : $E[\ell^{j+1}] = \langle P, Q \rangle$, with $P \in E(\mathbb{F}_q), Q \notin E(\mathbb{F}_q)$.

Proposition

The matrix of the Frobenius action in the basis (P, Q) has shape:

$$\pi(P, Q) = \begin{pmatrix} 1 & \alpha \\ 0 & q \end{pmatrix} \bmod \ell^{j+1}$$

We focus now on the ℓ-isogenies generated by $\ell^j Q$ according to the shape of the matrix.

Curves on the crater

We remind that we work with curve with the following type of ℓ structure:

$$E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^h\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$$

with $h \geqslant j+1$

Diagonal Matrix

$$\pi(P,Q) = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \bmod \ell^{j+1}$$

The points Q associated to a diagonal matrix are the ones such that $\ell^j(Q)$ generates a unique ℓ-isogeny.
This ℓ-isogeny is horizontal if the volcano has a cyclic shaped crater.

Remark

We work with parameters such that $q \neq 1 \bmod \ell^{j+1}$

We remind that we work with curves with the following type of ℓ structure:

$$E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^h\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$$

with $h \geqslant j+1$

Triangular matrix

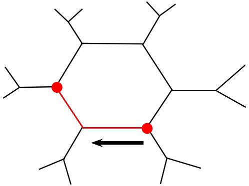
$$\pi(P,Q) = \begin{pmatrix} 1 & \alpha \\ 0 & q \end{pmatrix} \text{ mod } \ell^{j+1}, \alpha \neq 0$$

Proposition

Q points for which we have a triangular matrix are distributed such that the $\ell - 1$ descending isogenies of degree ℓ are generated by a same number of points $\ell^j(Q)$.

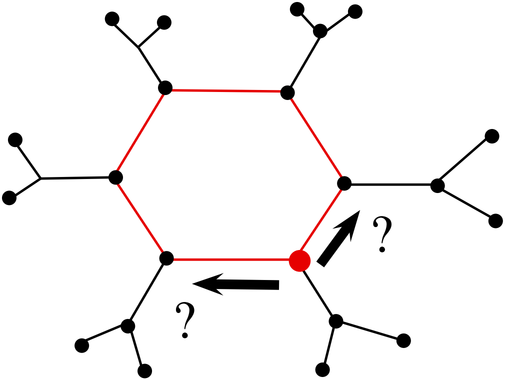
Proposition

The ℓ-isogeny generated by $\ell^j(P)$ is horizontal except if the crater is reduced to a unique point.



Fact

By determining a path of length j on the crater we associate a set of points P of order ℓ^j to this path. Because the path is associated to an ℓ^j-isogeny then to the group generated by a primitive ℓ^j torsion point.

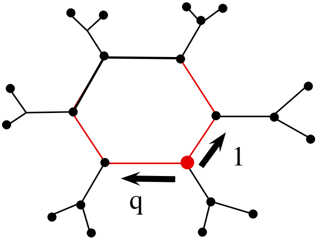


Remark

We need to give a way to the horizontal isogeny we choose.

Benefit of the Frobenius

We can distinguish two paths of length j on the volcano one for each of the "eigenvalues" we have for the Frobenius endomorphism modulo ℓ^j.



Remark

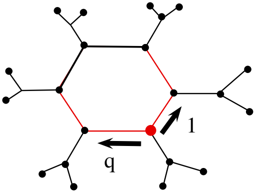
We can always do that if the Frobenius is diagonalizable with two different "eigenvalues".
We associate the "left way" to the eigenvalue q of the Frobenius endomorphism, thus we associate the "right way" to the eigenvalue 1.

What is the interest of this path?

Remark

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

- $\Rightarrow$ we will be able to distinguish the two paths of length j on the crater starting from E,
- $\Rightarrow$ we can associate two restricted set of ℓ^j primitive torsion points generating the ℓ^j isogeny,
- $\Rightarrow$ we have a "canonical" basis of $E[\ell^j]$.



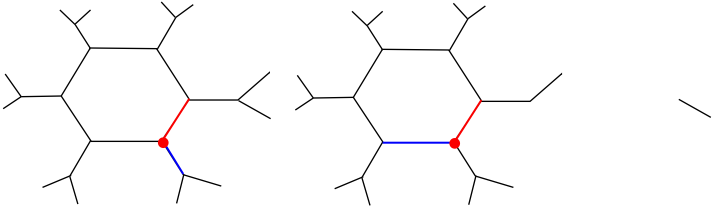
How do we do that?

Compute $\langle P, Q\rangle = E[2^j]$

Require: $E : Y^2 = X^3 + A * X + B, k$
Ensure: $P, Q \in E$ such that $\langle P, Q\rangle = E[2^j]$

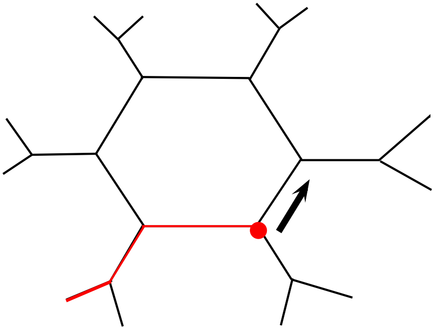
Rectify basis

Require: $\langle P, Q\rangle = E[2^j]$
Ensure: $P \in \mathbb{F}_q,\ Q, \pi(Q) = qQ, \langle P, Q\rangle = E[2^j]$



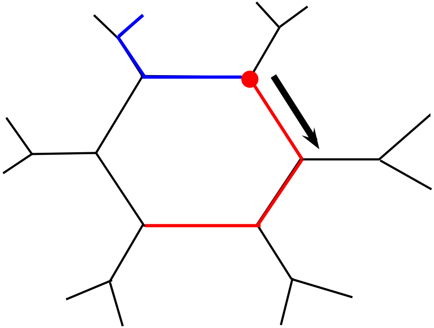
Go to the "right"

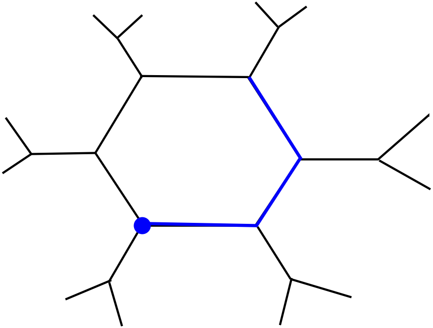
$(P, Q) \leftarrow E[2^j]$
for $i = 1$ to $j - 1$ **do**
  $(P, Q) \leftarrow$ **Rectify basis** (P, Q)
  $\phi \leftarrow E \rightarrow E/\langle [2^{j-1}]P \rangle$
  $Q \leftarrow \phi(Q)$
  $P \leftarrow \phi(P)/2$
end for
return P, Q



Go back "to the left"

1: $\phi \leftarrow E \rightarrow E/\langle Q \rangle$
2: $P \leftarrow \phi(P)$
3: **return** P





Entire algorithm

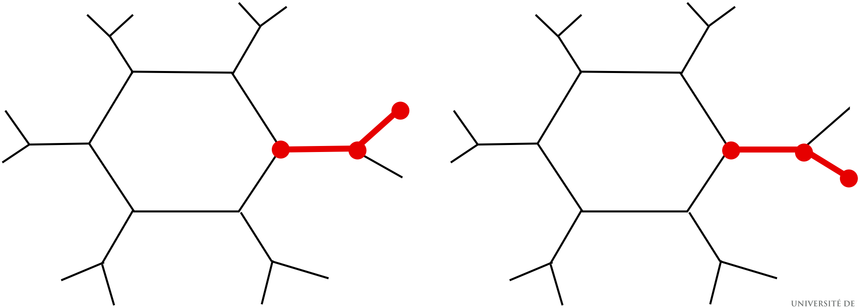
Require: E an elliptic curve defined over $\mathbb{F}_q$
Ensure: $\langle P, Q \rangle = E[2^j]$ such that P, Q generates two distinct paths of length j on the crater.

1: $(P_0, Q_0) \leftarrow$ **Compute basis of** $E[2^j]$
2: $(P, Q) \leftarrow$ **Go to the left** (P_0, Q_0)
3: $(Q_1) \leftarrow$ **Go-back to the right** (P, Q)
4: $(P, Q) \leftarrow$ **Go to the right** (P_0, Q)
5: $(P_1) \leftarrow$ **Go-back to the left** (P, Q)
6: **return** P_1, Q_1

Why couldn't we use other paths?

Remark

The same reasoning can't be done for other paths since we are not able to distinguish two descending isogeny.



Why do we want to use descending paths?

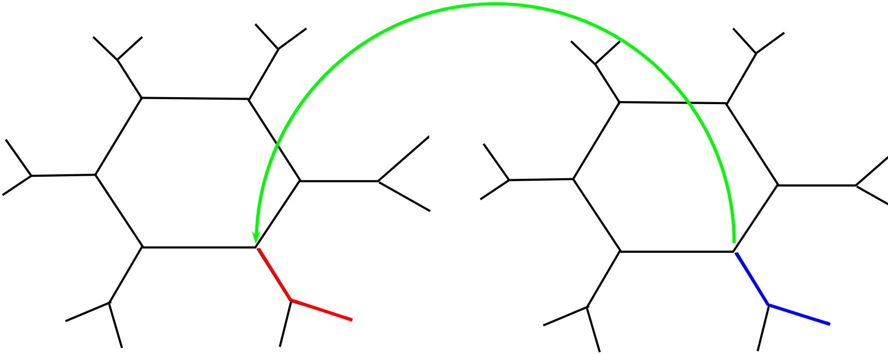


Figure : Two descents on volcanoes of 2isogeny related by an odd isogeny

The next result by [5] gives us also way to determine a path along the crater.

Remark

We denote by χ the unique non-trivial quadratic character in $\mathbb{F}_q^*$

Proposition (Miret, Moreno, Rio, Valls 2005)

Let $E : y^2 = x(x^2 + \alpha x + \beta)$ be an elliptic curve, with $\nu_2(q-1) \geqslant 2$ with $\chi(\beta) = \chi(\alpha^2 - 4\beta) = 1$. $E(\mathbb{F}_q)[2^\infty] = \mathbb{Z}/\ell^h\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}$, $h > j > 0$. P and Q points of $E(\mathbb{F}_q)[\ell^\infty]$ of order ℓ^h and ℓ^j respectively such that $Q \notin \{P\}$.

1. the isogeny generated by $\ell^{h-1}P$ is horizontal if $\chi(P_x) = 1$, otherwise the isogney is horizontal or ascending if $h = j+1$ or $h \geqslant j+2$ respectively,
2. the isogeny generated by $\ell^{j-1}Q$ is horizontal if $\chi(P_x) = 1$, otherwise the isogney is descending.

Conclusion

We have seen a way to determine ℓ^j primitive torsion points through the structure of voclanoes with cyclic crater.
We still have to

1. determine a way to label a descending path in the volcano
2. determine what can we do if we are not on a cyclic volcano
3. implement this using fast arithmetic on SAGE

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.

Sorina Ionica and Antoine Joux.
Pairing the volcano.
In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *ANTS*, volume 6197 of *Lecture Notes in Computer Science*, pages 201–218. Springer, 2010.

David R. Kohel.
Endomorphism rings of elliptic curves over finite fields.
PhD thesis, University of California, 1996.

Josep M. Miret, Ramiro Moreno, A. Rio, and Magda Valls.
Determining the 2-sylow subgroup of an elliptic curve over a finite