Isogeny cycles and volcanoes

Mireille Fouquet

(Joint work with F. Morain)

Institut de Mathématiques de Jussieu

Université Paris 7 - Denis Diderot

fouquet@math.jussieu.fr

Overview

A little bit of history

- Kohel's work on $\mathrm{End}(E)$
- Construction of the volcano
- Application to point counting
- Looking for an isogenous curve with a given endomorphism ring

 Once upon a time ... 

Counting the number of points of an elliptic curve E defined over a finite field was long and difficult ...

Then Schoof's algorithm arrived !! But still we were stuck with using the division polynomials $f_\ell^E(X)$ of the curve.

Elkies and Atkin designed a way to use a factor of $f_\ell^E(X)$: finding this factor is equivalent to find an ℓ-isogenous curve of E.

Couveignes and Morain showed how to build an isogeny cycle to find factors of $f_{\ell^k}^E(X)$.

Questions

- Building the isogeny cycle is possible in certain cases. What about the other cases ?
- What is the relation between two curves in the same isogeny cycle ?

Goal of this talk : Describe the structure of ℓ-isogeny classes and design an efficient algorithm to compute this structure.

Means : Kohel's work on the computation of $\mathrm{End}(E)$.

Notations

Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ where $q = p^d$.

The characteristic polynomial of the Frobenius endomorphism π is $X^2 - tX + q$ and its discriminant is

$$d_\pi = t^2 - 4q.$$

$\mathrm{End}(E)$ is an order in an imaginary quadratic field K.

$f = [\mathcal{O}_K : \mathrm{End}(E)]$ conductor of $\mathrm{End}(E)$. That is if we denote d_K the discriminant of $\mathcal{O}_K$, the discriminant d_E of $\mathrm{End}(E)$ is $d_E = f^2 d_K$.

Modular equation

The modular equation $\Phi_\ell(X, Y)$ is a symmetric polynomial of degree $\ell + 1$ in each variable, with integral coefficients and with the following property:
Let E and E' two elliptic curves defined over $\mathbb{F}_q$. E and E' are ℓ-isogenous over $\mathbb{F}_q \Leftrightarrow \#E = \#E'$ and $\Phi_\ell(j(E), j(E')) = 0$.

Existence of formulas to compute the equation of a curve E' ℓ-isogenous to E from $\Phi_\ell(j(E'), j(E)) = 0$. (Vélu; Elkies, Atkin)

Number of ℓ-isogenous curves to E :

Theorem :

$$\#\text{Roots of } \Phi_\ell(X, j(E)) = \begin{cases} 0 \Rightarrow (d_\pi/\ell) = -1 \\ 2 \Rightarrow (d_\pi/\ell) = +1 \\ 1 \text{ or } \ell + 1 \Rightarrow (d_\pi/\ell) = 0 \end{cases}$$

Computing End(E) (Kohel 1996)

His hypothesis: We suppose known $\#E$ as well as the factorization of $d_\pi = t^2 - 4q = g^2 d_K$.

Our approach: $\#E$ unknown.

$\pi \in \mathrm{End}(E) \;\Rightarrow \mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$

$\Longrightarrow\;$ $f | g$ with f conductor of $\mathrm{End}(E)$ and g conductor of $\mathbb{Z}[\pi]$.

$$\begin{tikzcd}
\mathcal{O}_K \arrow[d, dash, "f"] \arrow[dd, bend right=60, dash, "g"'] & \leftrightarrow & d_K \\
\mathrm{End}(E) \arrow[d, dash, "g/f"] & \leftrightarrow & f^2 d_K \\
\mathbb{Z}[\pi] & \leftrightarrow & g^2 d_K
\end{tikzcd}$$

Goal : Locate exactly $\mathrm{End}(E)$ in this diagram.

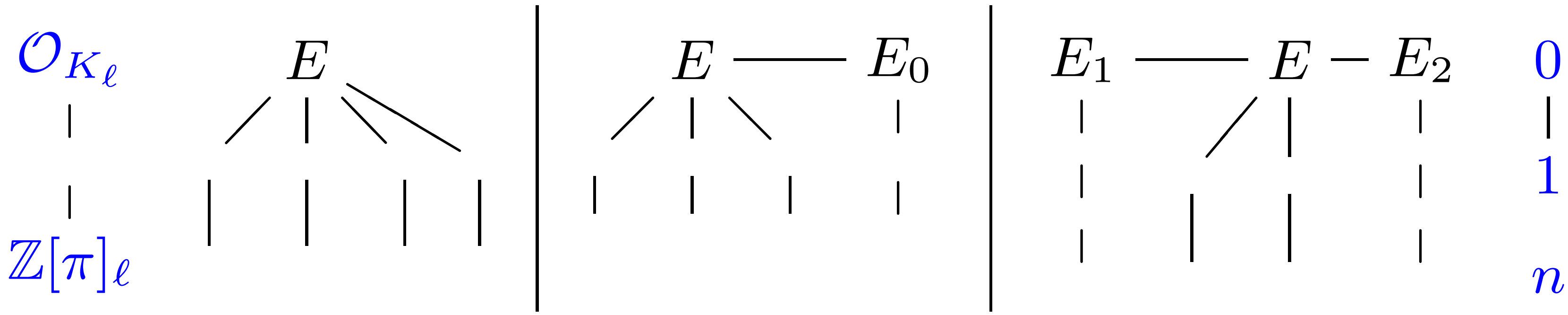
Relation between two ℓ-isogenous curves and their endomorphism rings

Theorem (Kohel) Let $\phi : E_1 \to E_2$ be an isogeny of degree $\ell \neq p$ is a prime number. Then we are in one of those three cases :

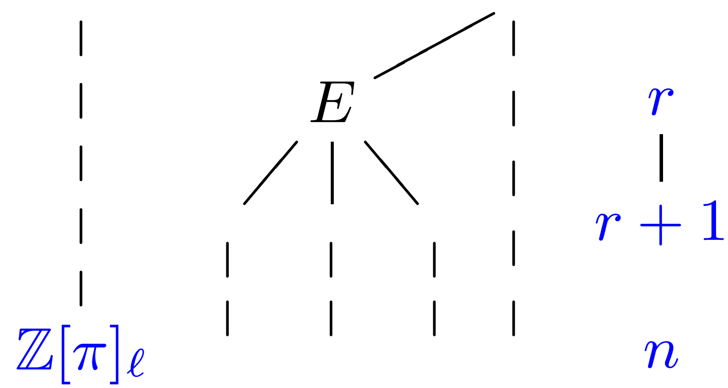
$$\begin{array}{c||c||c}
\mathcal{O}_K & \mathcal{O}_K & \mathcal{O}_K \\
| & | & | \\
\mathrm{End}(E_1) & \mathrm{End}(E_2) & \mathrm{End}(E_1) \simeq \mathrm{End}(E_2) \\
|\;\ell & |\;\ell & | \\
\mathrm{End}(E_2) & \mathrm{End}(E_1) & \mathbb{Z}[\pi] \\
| & | & \\
\mathbb{Z}[\pi] & \mathbb{Z}[\pi] & \\
\text{Descending case} & \text{Ascending case} & \text{Horizontal case}
\end{array}$$

Classification of the ℓ-isogenies (Kohel)

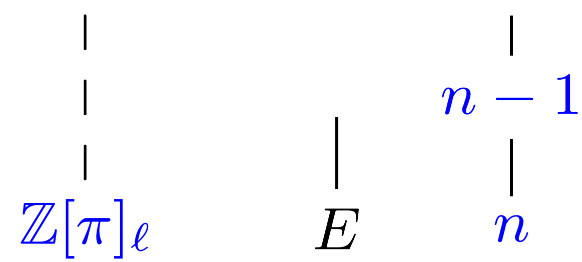
- Curves such that $\ell \nmid [\mathcal{O}_K : \mathrm{End}(E)]$: if $\ell \nmid [\mathrm{End}(E) : \mathbb{Z}[\pi]]$ then $1 + (d_K/\ell)$ ℓ-isogenies $\rightarrow$, if $\ell | [\mathrm{End}(E) : \mathbb{Z}[\pi]]$



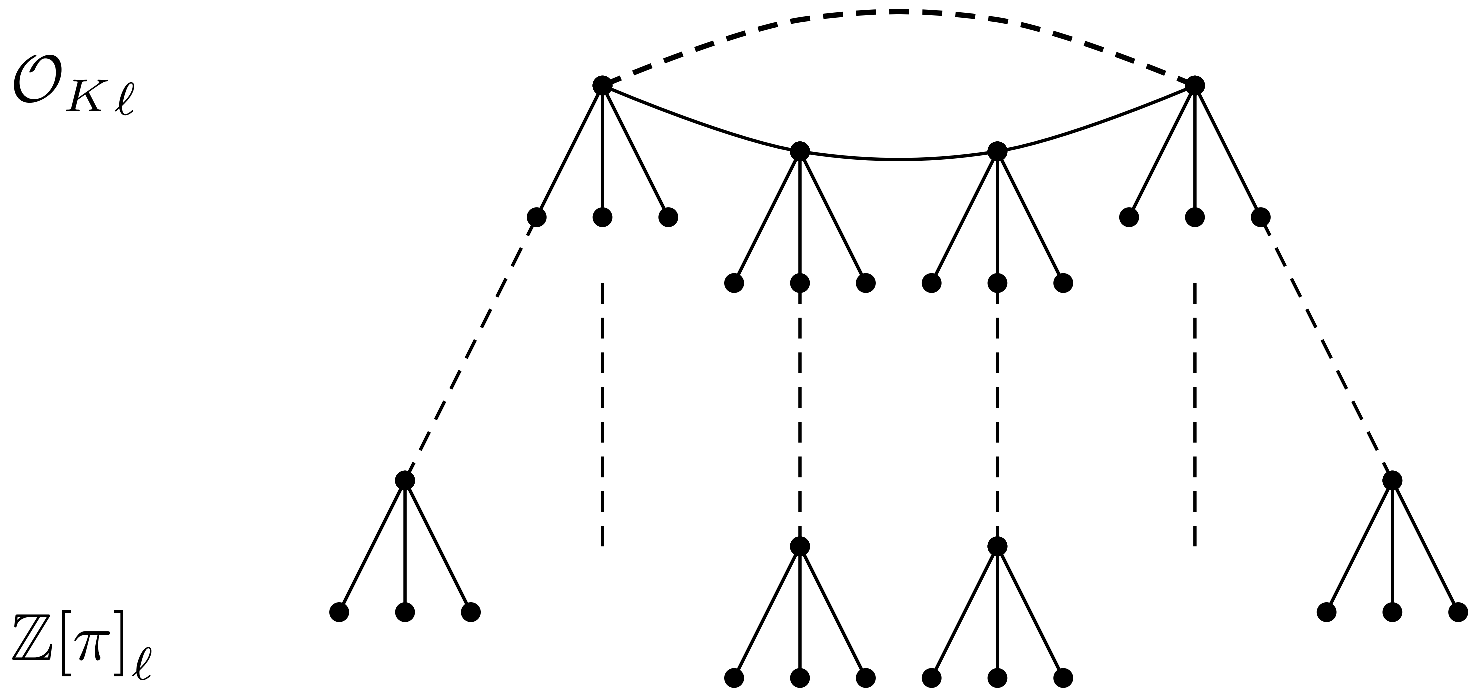
- Curves such that $\ell \mid [\mathcal{O}_K : \mathrm{End}(E)]$ and $\ell \mid [\mathrm{End}(E) : \mathbb{Z}[\pi]]$



- Curves such that $\ell \mid [\mathcal{O}_K : \mathrm{End}(E)]$ and $\ell \nmid [\mathrm{End}(E) : \mathbb{Z}[\pi]]$



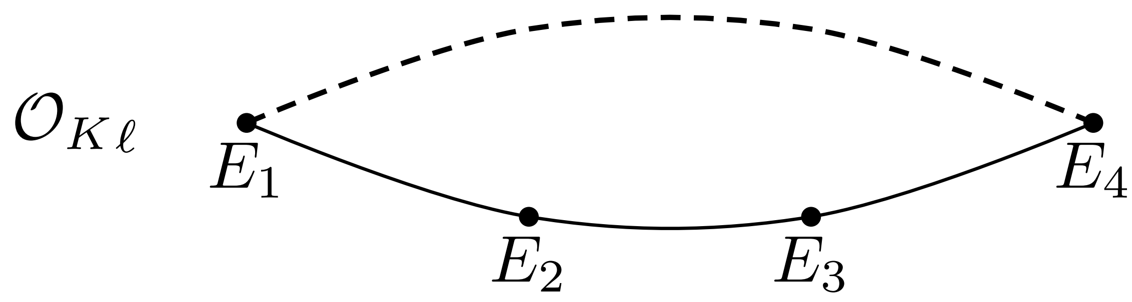
Isogeny volcano



Height of the volcano = ℓ-adic valuation of g conductor of $\mathbb{Z}[\pi]$.

Isogeny cycle : case $(d_\pi/\ell) = +1$

- No descending isogenies
- All the ℓ-isogenous curves have the same endomorphim ring



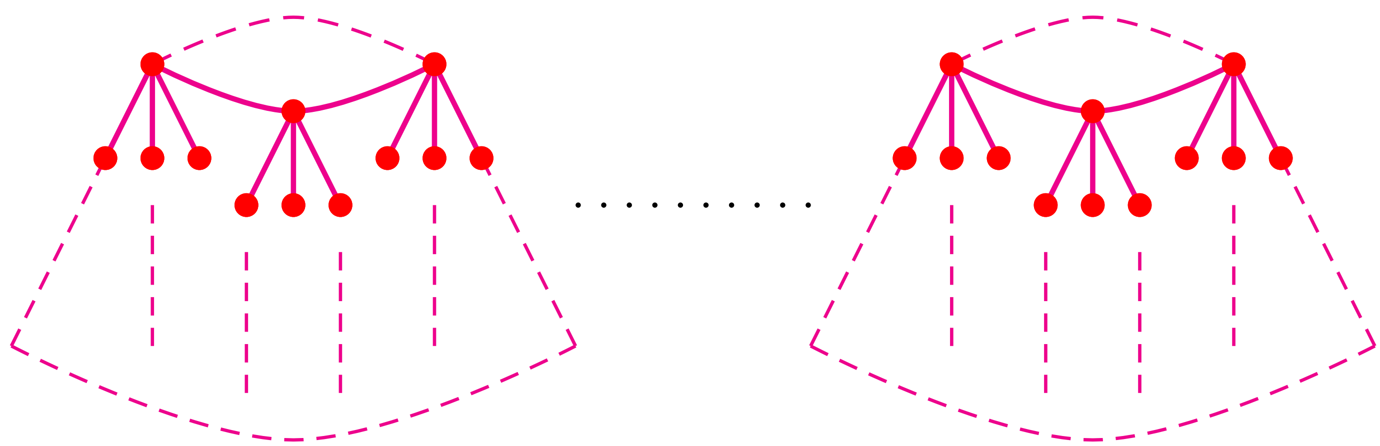
Size of the cycle = $\mathrm{ord}(\mathfrak{l})$ where $\mathfrak{l}$ is a prime ideal of norm ℓ of $\mathcal{O}_K$

Number of ℓ-isogeny volcanoes

Theorem (F.): Let f be the conductor of $\mathrm{End}(E)$ and let r be its ℓ-adic valuation. Let f' be such that $f = \ell^r f'$. Then there are

$$h({f'}^2 d_K)/\mathrm{ord}(\mathfrak{l})$$

distinct ℓ-isogeny volcanoes where $\mathfrak{l}$ is a prime ideal of norm ℓ of the order of conductor f'.



Moving in the volcano

Key point : Once we have started to go down, we keep on going down.

$$
\begin{tikzcd}
& E_1 \arrow[d, "\alpha"] & \\
& E_2 \arrow[u, bend right, "\hat{\alpha}"'] \arrow[dl] \arrow[d] \arrow[dr] & \\
{} & {} & {}
\end{tikzcd}
$$

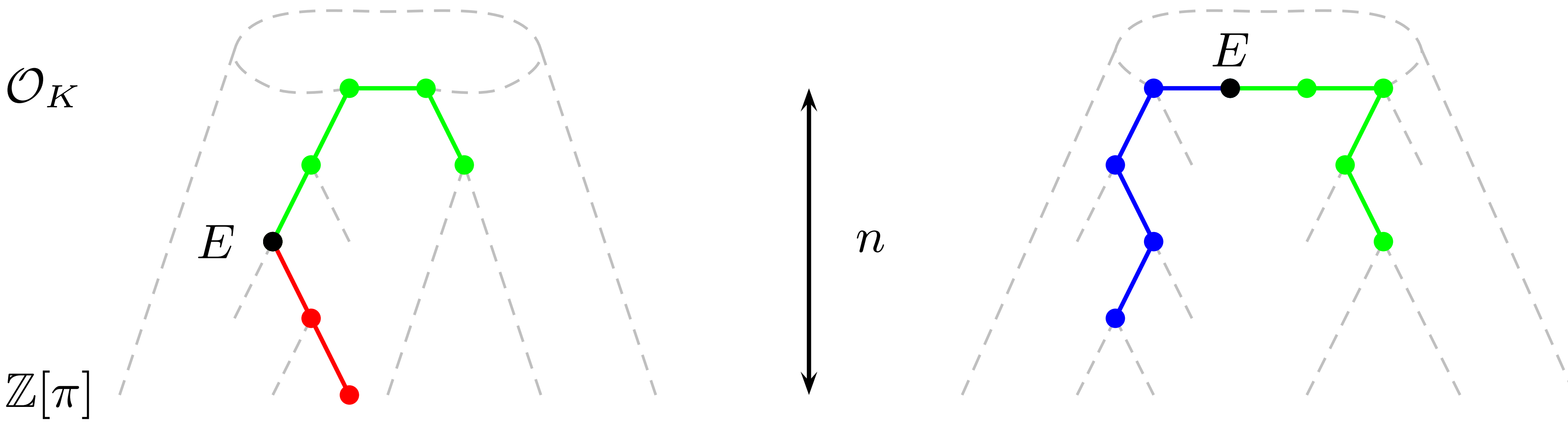
ℓ curves

$\Longrightarrow$ we can find a path of isogenous curves, starting from our curve and ending with a curve at the level of $\mathbb{Z}[\pi]$, of smallest length : a descending path.

Kohel's algorithm

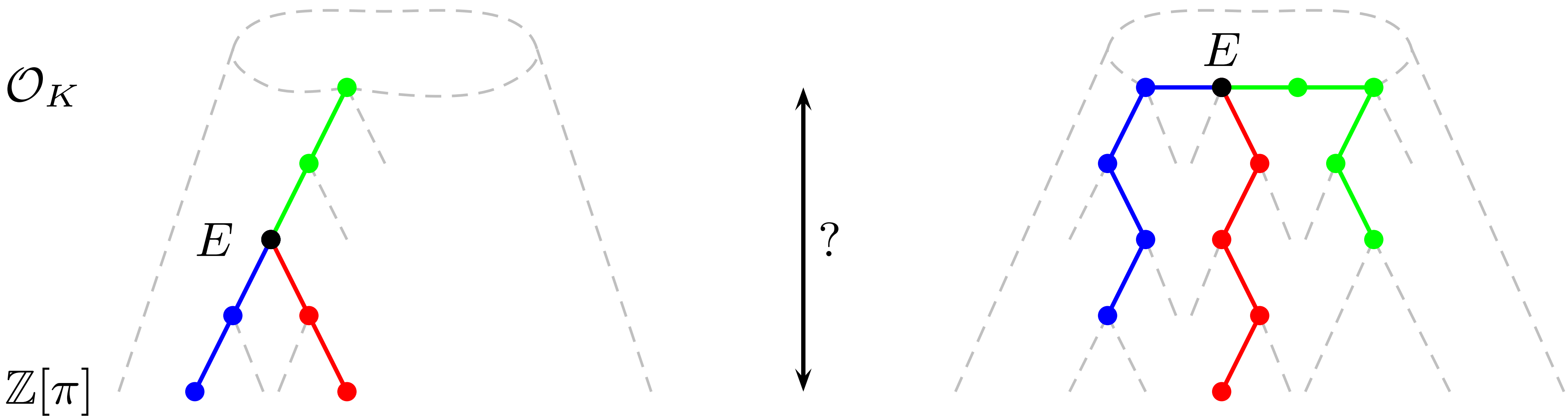
Idea: Construction of 2 random sequences of ℓ-isogenous curves of length $\leqslant n$ where $\ell^n \parallel g$.

Two possible cases:



Our approach

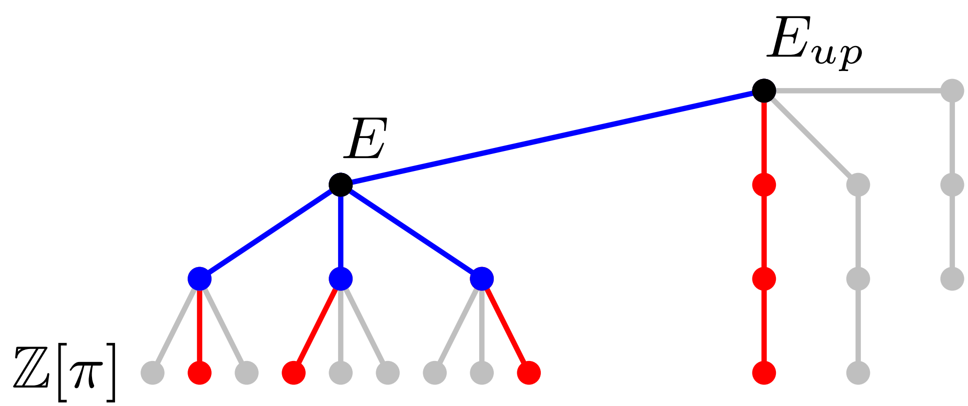
Idea: Construction of 3 random sequences of ℓ-isogenous curves in parallel.



Complexity of the computation of a descending path : $O(m\mathcal{F}_3(\ell))$ where m is such that $\ell^m \parallel g/f$ and $\mathcal{F}_3(\ell)$ = time to compute three roots of $\Phi_\ell(X, j)$.

Going up in the volcano

- Compute a descending path for each one of the $\ell + 1$ ℓ-isogenous curves to E;
- Compare their sizes and the curves with longest path are either up or horizontal.



Skeleton of the algorithm and complexity

Procedure ComputePartialVolcano
Input : An elliptic curve E and a prime number $\ell \neq p$.
Output : A full descending path and the type of the crater.

1. Test if E is in the crater;
2. If yes, compute a descending path starting from E and determine the type of the crater;
3. If not, go up in the volcano starting from E until finding the crater and then determine the type of the crater.

Complexity : $O(n^2 \ell \mathcal{F}(\ell))$ operations to compute a partial volcano, where $n \leqslant \frac{\log(|d_K|)}{2\log(\ell)}$ and $\mathcal{F}(\ell)$ is the time to compute the set of roots of $\Phi_\ell(X, j)$.

Application to point counting

Case where $d_\pi \equiv 0 \mod \ell$

Incomplete solution given by the computation of isogeny cycles (Couveignes, Dewaghe, Morain).

Solution : Isogeny volcanoes

$d_\pi = t^2 - 4q = g^2 d_K$: if $\ell^n \parallel g$ and $\ell^\epsilon \parallel d_K$

then $t^2 \equiv 4q \mod \ell^{2n+\epsilon}$.

$\Longrightarrow$ Computing n = Computing the height of the volcano and Computing ϵ = Determining the type of the crater.

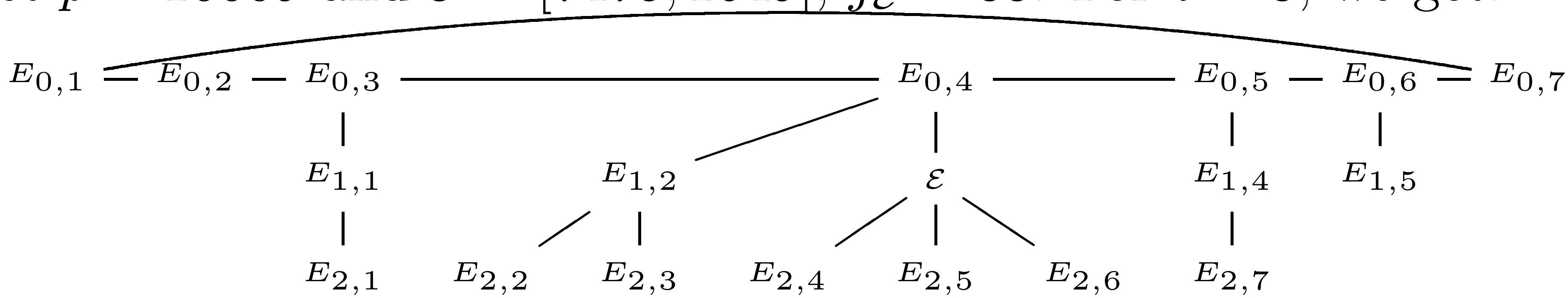
Finally compute $t \mod \ell^{2n+\epsilon}$.

Example

Implementation in Magma and in Maple

Case where $\left(\frac{d_K}{\ell}\right) = +1$

Let $p = 10009$ and $\mathcal{E} = [7478, 1649]$, $j_{\mathcal{E}} = 83$. For $\ell = 3$, we get:

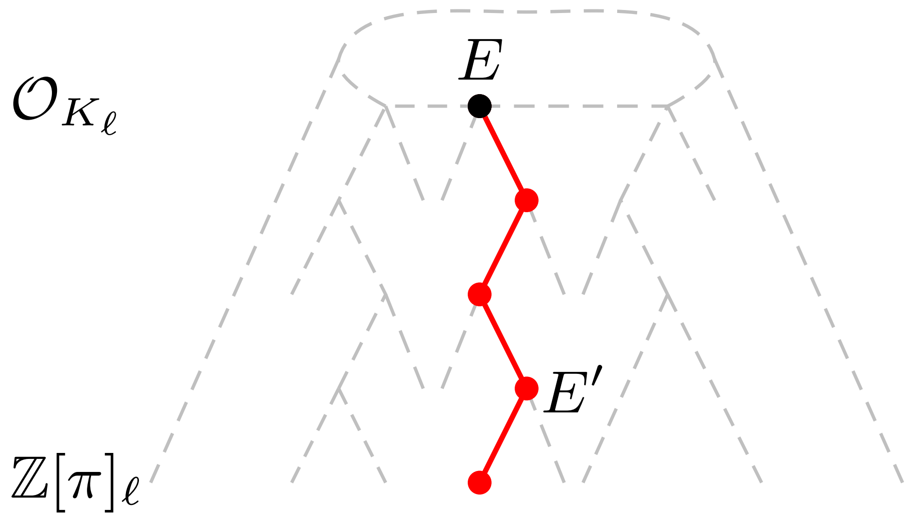


where

curve	equation	curve	equation	curve	equation	curve	equation
$E_{0,1}$	[1336, 8702]	$E_{0,6}$	[352, 4401]	$E_{1,5}$	[3659, 6441]	$E_{2,5}$	[4732, 4541]
$E_{0,2}$	[56, 8167]	$E_{0,7}$	[616, 274]	$E_{2,1}$	[5412, 9972]	$E_{2,6}$	[6203, 3741]
$E_{0,3}$	[7418, 8055]	$E_{1,1}$	[9166, 9156]	$E_{2,2}$	[9899, 274]	$E_{2,7}$	[2728, 8215]
$E_{0,4}$	[7778, 9421]	$E_{1,2}$	[5138, 6736]	$E_{2,3}$	[6796, 2230]		
$E_{0,5}$	[5051, 4157]	$E_{1,4}$	[6435, 570]	$E_{2,4}$	[8899, 8303]		

$\Rightarrow$ $n = 2$ and $\epsilon = 0$, thus $t^2 \equiv 4p \equiv 34 \mod 3^4$ and $t \equiv 22 \mod 3^4$.

Relation between two curves in a volcano



In this case :

$$f' = \ell^3 f$$

.

Looking for an isogenous curve with a given endomorphism ring

We suppose known $\#E$ and the factorization of $d_\pi = g^2 d_K$.

Goal : Given f' such that $f'|g$, find an isogenous curve E' to $E = E_0$ with endomorphism ring of conductor f'.

- Compute $\mathrm{End}(E)$.
- Determine $f = \prod_i \ell_i^{\alpha_i}$ and $f' = \prod_i \ell_i^{\beta_i}$ where ℓ_i is a prime.
- For each prime ℓ_i:
  - if $\alpha_i > \beta_i$ then compute an ascending path from E_i and take the curve E_{i+1} $(\alpha_i - \beta_i)$ steps from E_i in the path.
  - if $\alpha_i < \beta_i$ then compute a descending path from E_i and take the curve E_{i+1} $(\beta_i - \alpha_i)$ steps from E_i.
  - if $\alpha_i = \beta_i$ then $E_i = E_{i+1}$.

Improvements to compute the isogeny volcanoes for certain ℓ

Case $\ell = 2, 3$ by Miret, Moreno, Rio, Sadornil, Tena, Tomas and Valls :

- the structure of the ℓ-Sylow subgroup can be computed in a polynomial time ($O(\log^5(q))$ for $\ell = 2$);
- the structure of the ℓ-Sylow subgroup helps you determine if you are going up, down or horizontally in a lot of cases. The other cases are treated like previously.