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 $\text{End}(E)$

• 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 $\ell$-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 \( \ell \)-isogeny classes and design an efficient algorithm to compute this structure.

Means: Kohel’s work on the computation of \( \text{End}(E) \).
Notations

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

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

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

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

$f = [\mathcal{O}_K : \text{End}(E)]$ conductor of $\text{End}(E)$. That is if we denote $d_K$ the discriminant of $\mathcal{O}_K$, the discriminant $d_E$ of $\text{End}(E)$ 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 $\ell$-isogenous over $\mathbb{F}_q \iff \#E = \#E'$ and $\Phi_\ell(j(E), j(E')) = 0$.

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

Number of $\ell$-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 $\text{End}(E)$ (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.

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

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

![Diagram showing the relationships between $\mathcal{O}_K$, $\mathbb{Z}[\pi]$, $\text{End}(E)$, $f$, and $g$]

**Goal:** Locate exactly $\text{End}(E)$ in this diagram.
Relation between two $\ell$-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:

- **Descending case**
  
  \[
  \mathcal{O}_K \quad \downarrow \quad \text{End}(E_1) \quad \uparrow \quad \text{End}(E_2) \quad \downarrow \quad \mathbb{Z}[\pi]
  \]

- **Ascending case**
  
  \[
  \mathcal{O}_K \quad \downarrow \quad \text{End}(E_2) \quad \uparrow \quad \text{End}(E_1) \quad \downarrow \quad \mathbb{Z}[\pi]
  \]

- **Horizontal case**
  
  \[
  \mathcal{O}_K \quad \downarrow \quad \text{End}(E_1) \quad \uparrow \quad \text{End}(E_2) \quad \downarrow \quad \mathbb{Z}[\pi]
  \]

\[
\text{Descending case} \quad \text{Ascending case} \quad \text{Horizontal case}
\]
Classification of the $\ell$-isogenies (Kohel)

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

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

\[ \begin{array}{c}
\mathcal{O}_K \quad E \\
\downarrow \quad \downarrow \\
\mathbb{Z}[\pi]_\ell \quad \downarrow \\
\end{array} \quad \begin{array}{ccc}
E & \rightarrow & E_0 \\
\downarrow & & \downarrow \\
E_1 & \rightarrow & E - E_2 \\
\downarrow & & \downarrow \\
0 & & 1 \\
\end{array} \quad \begin{array}{c}
\downarrow \\
r \downarrow \\
r + 1 \\
\downarrow \\
\mathbb{Z}[\pi]_\ell \\
\end{array} \quad \begin{array}{c}
\downarrow \\
n \\
\end{array} \]
• Curves such that $\ell \mid \mathcal{O}_K : \text{End}(E)$ and $\ell \nmid \text{End}(E) : \mathbb{Z}[\pi]$
Height of the volcano = \( \ell \)-adic valuation of \( g \) conductor of \( \mathbb{Z}[\pi] \).
Isogeny cycle: case $(d_π/\ell) = +1$

- No descending isogenies
- All the $\ell$-isogenous curves have the same endomorphism ring

Size of the cycle $= \text{ord}(t)$ where $t$ is a prime ideal of norm $\ell$ of $\mathcal{O}_K$
**Number of \( \ell \)-isogeny volcanoes**

**Theorem (F.):** Let \( f \) be the conductor of \( \text{End}(E) \) and let \( r \) be its \( \ell \)-adic valuation. Let \( f' \) be such that \( f = \ell^r f' \).

Then there are

\[
h(f'^2 d_K) / \text{ord}(\mathfrak{l})
\]

distinct \( \ell \)-isogeny volcanoes where \( \mathfrak{l} \) is a prime ideal of norm \( \ell \) of the order of conductor \( f' \).
Moving in the volcano

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

\[ E_1 \xleftarrow{\alpha} \xrightarrow{\hat{\alpha}} E_2 \]

\[ \ell \text{ curves} \]

\[ \Rightarrow \] 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 $\ell$-isogenous curves of length $\leq n$ where $\ell^n \mid g$.

Two possible cases:
Our approach

Idea: Construction of 3 random sequences of \( \ell \)-isogenous curves in parallel.

\[ \mathcal{O}_K \]

\[ \mathbb{Z} [\pi] \]

Complexity of the computation of a descending path: \( O(mF_3(\ell)) \) where \( m \) is such that \( \ell^m \parallel g/f \) and \( F_3(\ell) = \) time to compute three roots of \( \Phi_\ell(X, j) \).
Going up in the volcano

• Compute a descending path for each one of the $\ell + 1$ $\ell$-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 $n \leq \frac{\log(|d_K|)}{2\log(\ell)}$ 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

\[
d_\pi = t^2 - 4q = g^2d_K: \text{ if } \ell^n \parallel g \text{ and } \ell^\epsilon \parallel d_K
\]

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

\[\implies \text{ Computing } n = \text{ Computing the height of the volcano and Computing } \epsilon = \text{ Determining the type of the crater.} \]

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

\[
\begin{align*}
E_{0,1} & \quad E_{0,2} \quad E_{0,3} \quad E_{0,4} \quad E_{0,5} \quad E_{0,6} \quad E_{0,7} \\
E_{1,1} & \quad E_{1,2} & \quad \mathcal{E} & \quad E_{1,4} & \quad E_{1,5} \\
E_{2,1} & \quad E_{2,2} & \quad E_{2,3} & \quad E_{2,4} & \quad E_{2,5} & \quad E_{2,6} & \quad E_{2,7}
\end{align*}
\]

where

<table>
<thead>
<tr>
<th>curve</th>
<th>equation</th>
<th>curve</th>
<th>equation</th>
<th>curve</th>
<th>equation</th>
<th>curve</th>
<th>equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E_{0,1} )</td>
<td>[1336, 8702]</td>
<td>( E_{0,2} )</td>
<td>[56, 8167]</td>
<td>( E_{0,3} )</td>
<td>[7418, 8055]</td>
<td>( E_{0,4} )</td>
<td>[7778, 9421]</td>
</tr>
<tr>
<td>( E_{0,6} )</td>
<td>( E_{0,7} )</td>
<td>( E_{1,1} )</td>
<td>[9166, 9156]</td>
<td>( E_{1,2} )</td>
<td>[5138, 6736]</td>
<td>( E_{1,3} )</td>
<td>[6435, 570]</td>
</tr>
<tr>
<td>( E_{1,5} )</td>
<td>( E_{2,1} )</td>
<td>( E_{2,2} )</td>
<td>[9899, 274]</td>
<td>( E_{2,3} )</td>
<td>[6796, 2230]</td>
<td>( E_{2,4} )</td>
<td>[8899, 8303]</td>
</tr>
<tr>
<td>( E_{2,6} )</td>
<td>( E_{2,7} )</td>
<td>( E_{2,7} )</td>
<td>[2728, 8215]</td>
<td>( E_{2,7} )</td>
<td>[2728, 8215]</td>
<td>( E_{2,7} )</td>
<td>[2728, 8215]</td>
</tr>
</tbody>
</table>

\[ \Rightarrow n = 2 \text{ and } \epsilon = 0, \text{ thus } t^2 \equiv 4p \equiv 34 \mod 3^4 \text{ and } t \equiv 22 \mod 3^4. \]
Relation between two curves in a volcano

\[ \mathcal{O}_{K_{\ell}} \]

\[ \mathbb{Z}[\pi]_{\ell} \]

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 \( \text{End}(E) \).
- Determine \( f = \prod_i \ell_i^{\alpha_i} \) and \( f' = \prod_i \ell_i^{\beta_i} \) where \( \ell_i \) is a prime.
- For each prime \( \ell_i \):
  - 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 $\ell$

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

- the structure of the $\ell$-Sylow subgroup can be computed in a polynomial time ($O(\log^5(q))$ for $\ell = 2$);
- the structure of the $\ell$-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.