Computing modular polynomials by deformation

Sixteenth Algorithmic Number Theory Symposium (ANTS XVI)

Sabrina Kunzweiler & Damien Robert

July 15th, 2024

Inria, IMB, Bordeaux, France

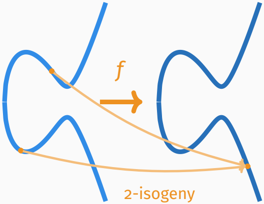
Introduction to Modular Polynomials

Elliptic curves and isogenies

An **elliptic curve** over a field k is a smooth projective curve of genus 1 with a k-rational point $\mathcal{O}$.

- The ***j*-invariant** defines a 1-1 correspondence $j : \{E \text{ elliptic curve over } k\}/\cong \ \rightarrow\ k$.

An **isogeny** is a nonzero morphism of elliptic curves $f : E \to E'$ with $f(\mathcal{O}) = \mathcal{O}$.



An **ℓ-isogeny** is an isogeny of degree ℓ with kernel $G \cong \mathbb{Z}/\ell\mathbb{Z}$.

Computing isogenies

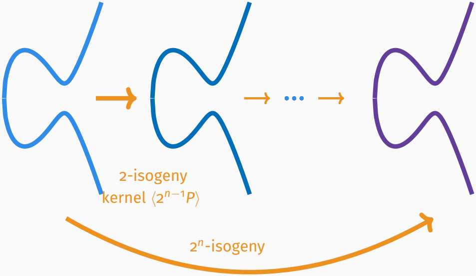
Computing an ℓ-isogenies with Vélu's formulae

- complexity: $O(\ell)$ or $\tilde{O}(\sqrt{\ell})$ (sqrt-Vélu).

⚠ The kernel G might only be defined over an extension k'/k.

Computing composite-degree isogenies

Example: N-isogeny with $N = 2^n$ and kernel $G = \langle P \rangle$.



- complexity: $O(n \log(n)) = \tilde{O}(\log(N))$ (using optimal strategies).

Modular polynomials

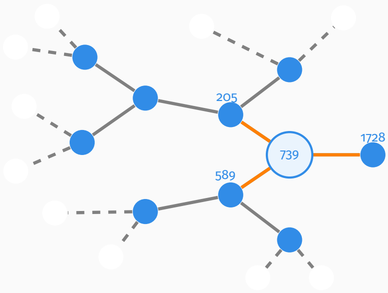
The **modular polynomial** is a polynomial $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ with the property that for E, E' elliptic curves, we have

$$\Phi_\ell(j(E), j(E')) = 0 \Leftrightarrow \text{there is an } \ell\text{-isogeny } E \to E'$$

Example $\ell = 2$

$\Phi_2(X,Y) = X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY + 8748000000X + Y^3 - 162000Y^2 + 8748000000Y - 157464000000000.$

- Elliptic curve with $j(E) = 739$ $E : y^2 = x^3 + 6x^2 + x$ over $\mathbb{F}_{2063^2}$.
- Evaluated: $\bar{\Phi}_2(X, 739) = X^3 - 459X^2 - 835X + 334 = (X - 589)(X - 205)(X - 1728)$ in $\mathbb{F}_{2063^2}[X]$.



2-isogeny graph over $\mathbb{F}_{2063^2}$

Computing modular polynomials

Properties of Φ_ℓ for primes ℓ:

- $\deg_X(\Phi_\ell) = \deg_Y(\Phi_\ell) = \ell + 1$.
- $\log(c) \leq 6\ell \log(\ell) + \ldots$ for all coefficients c.

} Total size (in bits): $O(\ell^3 \log \ell)$.

General Chinese Remainder approach

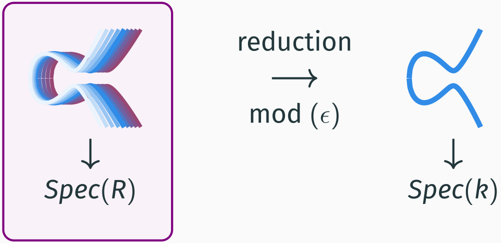
- Compute $\bar{\Phi}_\ell \in \mathbb{F}_p[X, Y]$ for many small primes (around ℓ primes with $\log \ell \approx \log p$)
- Combine the results using *Explicit CRT* to find $\Phi_\ell \in \mathbb{Z}[X, Y]$.
- used in: Charles-Lauter (2005), Bröker-Lauter-Sutherland (2010), Sutherland (2012), Leroux (2023), this work

How to compute $\bar{\Phi}_\ell \in \mathbb{F}_p[X, Y]$?
Goal: time $O(\ell^2 \log^c p)$

Deformations of Elliptic Curves

Elliptic curves over $R = k[\epsilon]/(\epsilon^{m+1})$

An **elliptic curve $\mathcal{E}$ over $R = k[\epsilon]/(\epsilon^{m+1})$** is a a group scheme $\mathcal{E} \to Spec(R)$ which is also a smooth, proper, connected curve of genus 1 over R.



We say that $\mathcal{E}$ is an m-th order **deformation** of E.

Given $\tilde{j} \in R$ with $j \neq 0, 1728 \pmod{\epsilon}$, we can compute $\mathcal{E}$ with $j(\mathcal{E}) = \tilde{j}$.

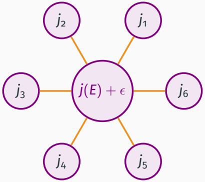
What's the connection to modular polynomials?

General idea to compute ϕ_ℓ over $\mathbb{F}_p$:
Choose an elliptic curve $E/\mathbb{F}_p$.

1. Compute the deformation $\mathcal{E}/R$ with $j(\mathcal{E}) = j(E) + \epsilon$, where $R = \mathbb{F}_p[\epsilon]/(\epsilon^{\ell+2})$
2. Compute the evaluated modular polynomial $\phi_\ell(j(E) + \epsilon, Y) \in R[Y]$.
3. Substitute $\epsilon = X - j(E)$:

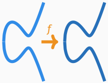
$$\phi_\ell(X, Y) \in \mathbb{F}_p[X, Y]/((X - j(E))^{\ell+2}).$$

- This is the modular polynomial, since $\deg_X(\phi_\ell) = \ell + 1$.



Deformations of isogenies

Let $f : E \to E'$ be an isogeny over k.



For any deformation $\mathcal{E}$ of E, there exists a unique (up to iso) deformation $\mathcal{E}'$ of E', so that f lifts to an isogeny $\tilde{f} : \mathcal{E} \to \mathcal{E}'$.

Computing the lift $\tilde{f}$ of an ℓ-isogeny f

1. Lift the the generator P of $\ker(f)$ to an element $\tilde{P} \in \mathcal{E}[\ell]$.
2. Compute the isogeny with kernel $\langle \tilde{P} \rangle$ using Vélu's formulae.

We will do this faster by working in dimension 2!

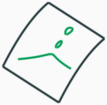
Kani's Lemma and isogenies in dimension 2

Overview of the 2-dimensional setting

Principally polarized abelian varieties *A* in dimension 2

- Product of elliptic curves.

- Jacobian of genus-2 curve *C*.

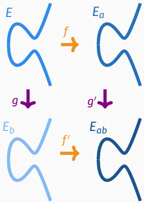


(ℓ, ℓ)**-Isogenies**

- Kernels are maximal isotropic subgroups of $A[\ell]$ and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.
- Computation is polynomial in ℓ.

Kani's Lemma

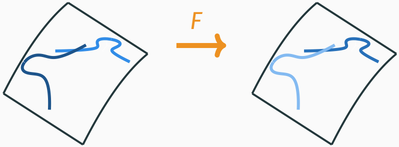
A commutative diagram of isogenies (as on the right) with $d_a = \deg(f) = \deg(f')$ and $d_b = \deg(g) = \deg(g')$ is called (d_a, d_b)-**isogeny diamond**.



Kani's Lemma

If $\gcd(d_a, d_b) = 1$, then a (d_a, d_b)-isogeny diamond gives rise to a $(d_a + d_b, d_a + d_b)$-product isogeny

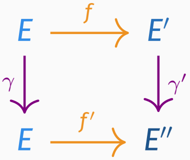
$$F : E \times E_{ab} \to E_a \times E_b \quad \text{with } \ker(F) = \{(-\hat{g}(P), f'(P)) \mid P \in E_b[d_a + d_b]\}.$$



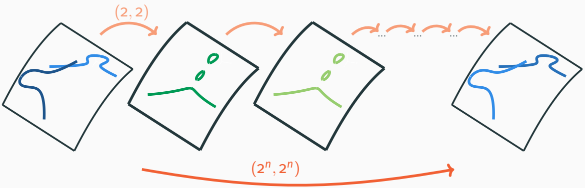
A special isogeny diamond

Let $E : y^2 = x^3 + 6x^2 + x$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$, and ℓ a prime $\ell \equiv 3 \pmod 4$.
Let $\iota : E \to E$ the isogeny with $\iota \circ \iota = [-4]$.

- Consider an ℓ-isogeny $f : E \to E'$.
- Choose n, a, b so that $2^n - \ell = a^2 + b^2$.
- Define $\gamma = [a] + [b/2]\iota$. $\Rightarrow \deg(\gamma) = a^2 + b^2$.

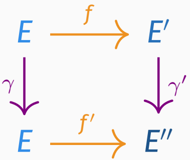


$(\ell, 2^n - \ell)$-isogeny diamond $\Rightarrow$ $(2^n, 2^n)$-product isogeny



An algorithm for computing modular polynomials

Computing $\varphi_\ell \in \mathbb{F}_p[X, Y]$



Input: A prime ℓ with $\ell \equiv 3 \pmod 4$, integers n, a, b with $2^n - \ell = a^2 + 4b^2$, and a prime $p \equiv -1 \pmod{\ell \cdot 2^n}$.

Output: $\varphi_\ell \in \mathbb{F}_p[X, Y]$.

1. $E : y^2 = x^3 + 6x^2 + x$ over $\mathbb{F}_{p^2}$, $\iota = [2i] \in \mathrm{End}(E)$.
2. Set $\mathcal{E}$ deformation with $j(\mathcal{E}) = j(E) + \epsilon \in \mathbb{F}_{p^2}[\epsilon]/(\epsilon^{\ell+2})$.
3. For each ℓ-isogeny $f_i : E \to E'$:
   (a) Construct a special $(\ell, 2^n - \ell)$-isogeny diamond (E, E', E, E'').
   (b) Lift the isogeny diamond by lifting the $(2^n, 2^n)$-product isogeny $\rightsquigarrow (\mathcal{E}, \mathcal{E}', \mathcal{E}_0, \mathcal{E}'')$. Set $j_k = j(\mathcal{E}')$.
4. $\varphi_\ell = \prod (Y - j_k)(\epsilon = X - j(E)) \in \mathbb{F}_p[X, Y]$.

Dominating step: $\ell + 1$ different $(2^n, 2^n)$-isogenies over $\mathbb{F}_{p^2}[\epsilon]/(\epsilon^{\ell+2})$.
$\Rightarrow$ complexity: $O(n \cdot \ell^2 \log^2 \ell \log\log \ell)$ when $\log(p) \approx \log(\ell)$.

Summary

This presentation

- Quasi-linear algorithm to compute Φ_ℓ, when $\ell \equiv 3 \pmod 4$, based on a mild heuristic ($\exists n \in \mathcal{O}(\log(\ell)) : 2^n - \ell = a^2 + 4b^2$).
- Key ideas:
  - Computing Φ_ℓ modulo small primes and use CRT
  - Lifting smooth-degree isogenies (in dim 2) instead of prime degree isogenies (in dim 1).

Our paper

- Generalization to arbitrary primes ℓ.
- Unconditional quasi-linear algorithm.

Thanks for your attention!