# Computing modular polynomials by deformation

Caipi Symposium

Sabrina Kunzweiler & Damien Robert

April 30th, 2024

Inria, IMB, Bordeaux, France

# Introduction to Modular Polynomials

# Elliptic Curves and $j$-invariants

An **elliptic curve** over a field $k$ is a smooth projective curve of genus 1 with a $k$-rational point $\mathcal{O}$.
In our algorithms: We work with curves in short[1] Montgomery form $E_A : y^2 = x^3 + Ax^2 + x.$[2]

The $j$-**invariant** defines a 1-1 correspondence

$$j : \{E \text{ elliptic curve over } k\}/\cong \ \to \ k.$$

We have

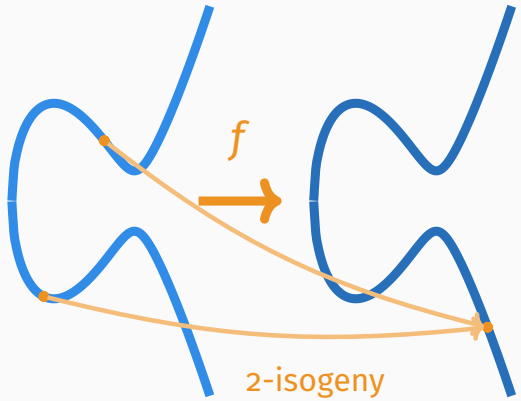
- $j(E_A) = 256\frac{(A^2-3)^3}{A^2-4}$, we denote $j(A) = j(E_A)$.
- The curves with $j$-invariant $j(E) \in \{0, 1728\}$, i.e. $A = 0, \pm\sqrt{3}$ have extra automorphisms.

[1] Here, short means that we ignore twists, i.e. $B = 1$.
[2] Not every elliptic curves over $k$ can be written in Montgomery form.

# Isogenies of Elliptic Curves

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

$G = \langle (\alpha, 0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$



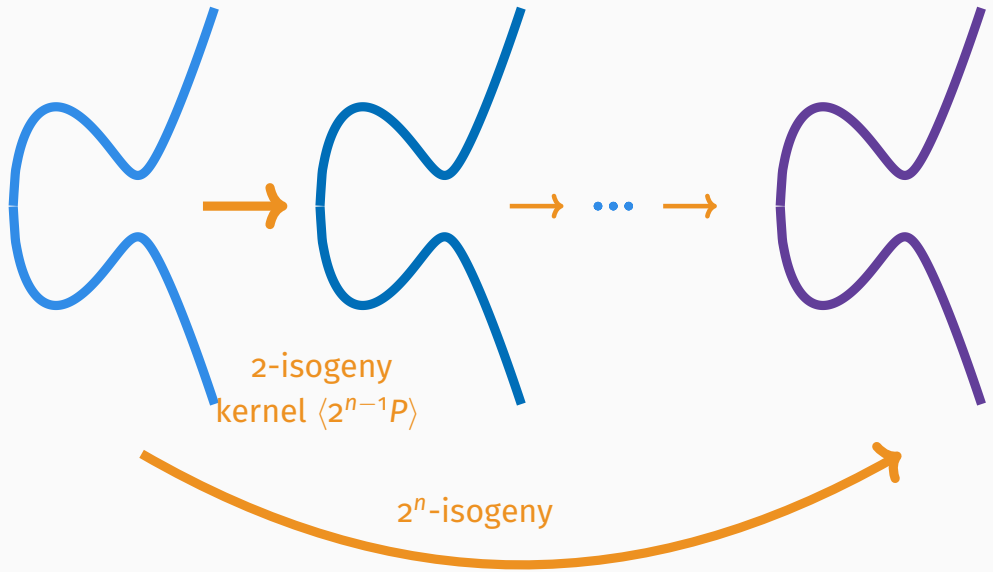

An $\ell$**-isogeny** is an isogeny of degree $\ell$ with kernel $G \cong \mathbb{Z}/\ell\mathbb{Z}$.

Given a kernel group $G$ with $\mathbb{Z}/\ell\mathbb{Z} \cong G \subset E(\bar{k})$, we can compute $f$ via Velu's formulae.

- complexity: $\tilde{O}(\sqrt{\ell})$ (sqrt-Vélu).
- ⚠ The kernel $G$ might only be defined over an extension field $k'$, we have $[k' : k] \leq \ell^2 - 1$.

# Isogenies of elliptic curves (composite degree)

Computing an $N$-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

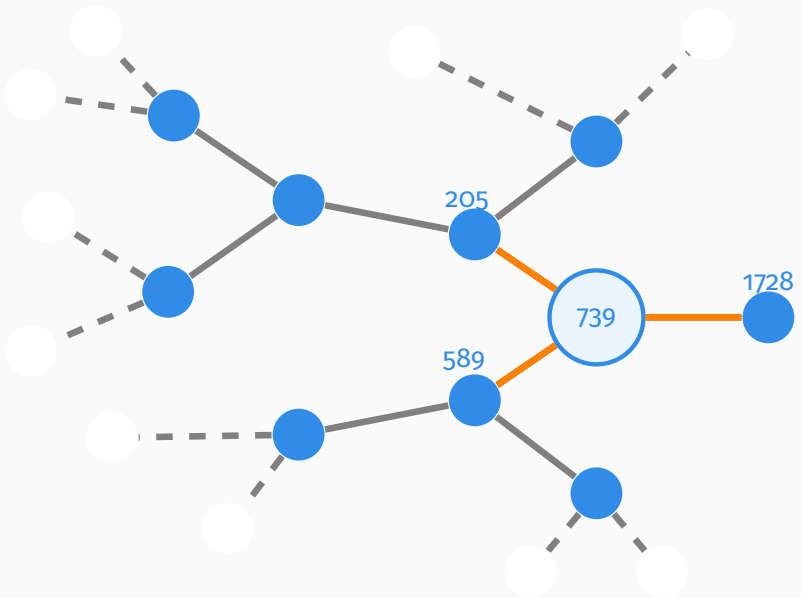
The **modular polynomial** is a polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ with the property that for $E, E'$ elliptic curves, we have

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

**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 modular polynomial $\bar{\Phi}_2(X, 739) = X^3 - 459X^2 - 835X + 334 = (X - 589)(X - 205)(X - 1728)$ in $\mathbb{F}_{2063^2}[X]$.




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

# Computing modular polynomials

**Properties** of $\Phi_\ell$ for primes $\ell$:

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

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

**General Chinese Remainder approach**

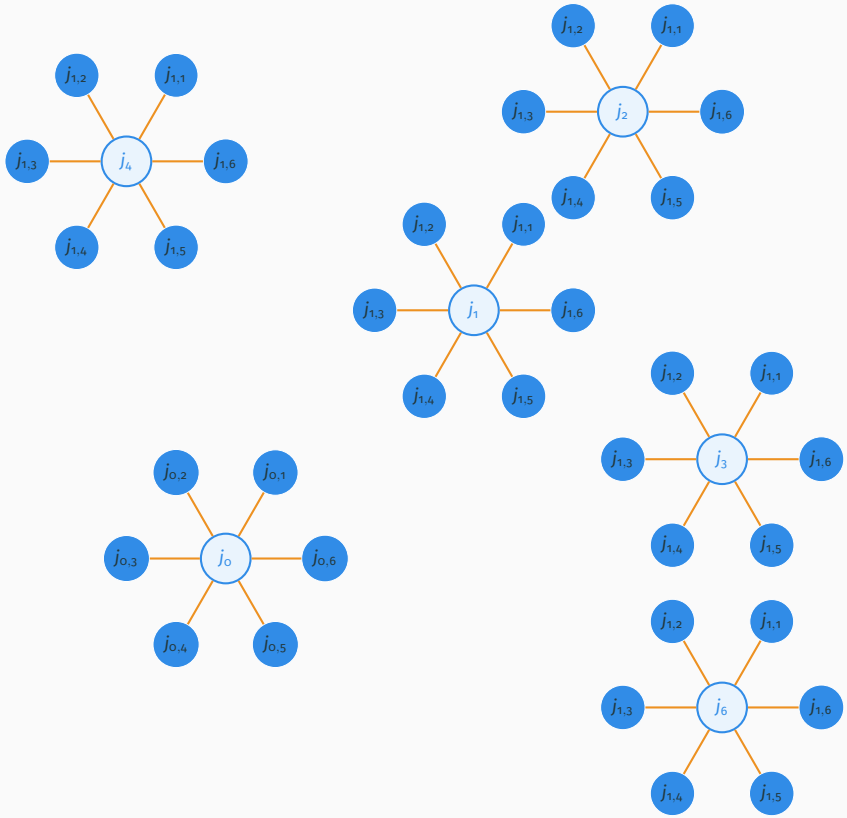
- Compute the modular polynomial $\bar{\Phi}_\ell \in \mathbb{F}_p[X, Y]$ for many small primes (around $\ell$ primes of bitsize $O(\log(\ell))$).
- Combine the results using *Explicit CRT* to find $\Phi_\ell \in \mathbb{Z}[X, Y]$

- For example: Charles-Lauter (2005), Bröker-Lauter-Sutherland (2010), Sutherland (2012), Leroux (2023), this work

# Computing modular polynomials over $\mathbb{F}_p$

**An interpolation approach** (warm-up)[1]

1. Choose $\ell + 1$ different elliptic curves $E_i$ over $\mathbb{F}_p$ with $j$-invariants $j_i$.
2. For each $j_i = j(E_i)$:
   (a) Compute the $\ell + 1$ different $\ell$-isogenies $f_{ik} : E_i \to E_{ik}$.
   (b) Evaluate $\varphi_i = \varphi_\ell(X, j_i) = \prod_{i=0}^{\ell}(X - j(E_{ik}))$.
3. Compute $\varphi_\ell$ as the interpolation of $\varphi_0, \ldots, \varphi_\ell$ in $\mathbb{F}_p[X][Y]$.



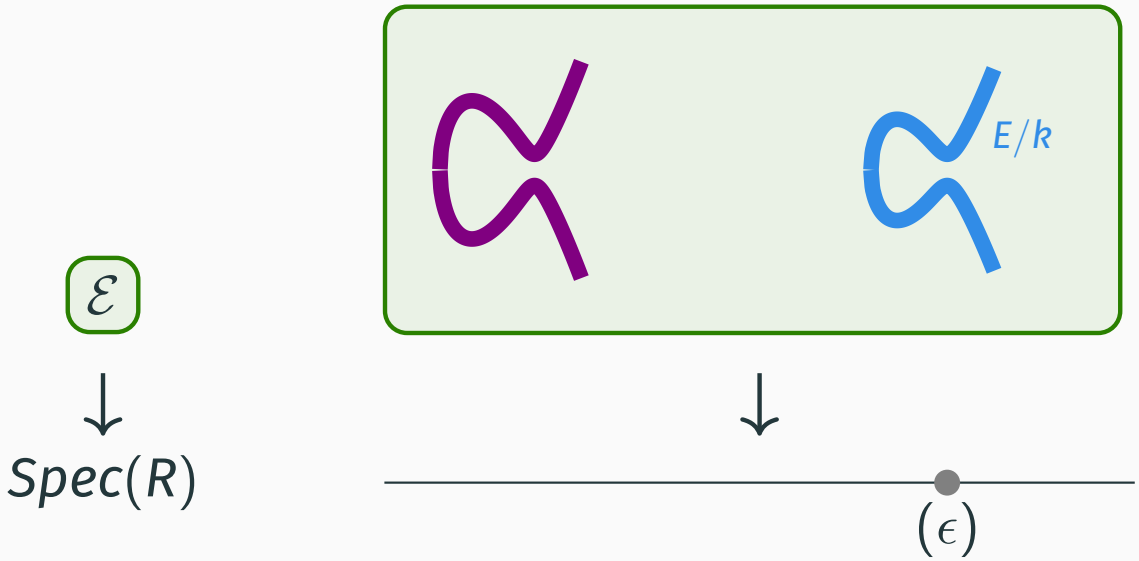

This work: Deformations of elliptic curves to $k[\epsilon]/(\epsilon^{\ell+2})$ to avoid repeating (2.) for all $j_i$.

[1] This is not the fastest approach.

# 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 $R$.



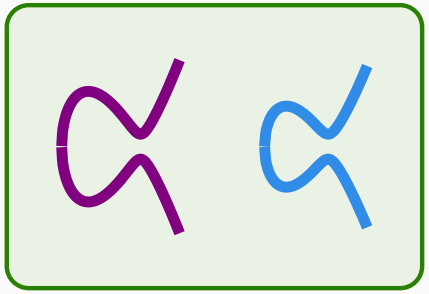

Concretely: We work with affine equations in Montgomery form

$$\mathcal{E} : y^2 = x^3 + A \cdot x^2 + x \quad \text{with } A \in R.$$

- Standard formulae apply for addition, the $j$-invariant, ...

# Deformations

For $R = k[\epsilon]/(\epsilon^{m+1})$, let $\mathcal{E}/R$ be an elliptic curve and $E/k$ the reduction modulo $(\epsilon)$.



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

**Fact:** Let $j(E) \neq 0, 1728$, and $\tilde{j} \in R$ with $\tilde{j} \equiv j(E) \pmod{\epsilon}$
$\Rightarrow \exists\, \mathcal{E}$ deformation of $E$ with $j(\mathcal{E}) = \tilde{j}$.

- We call $\lambda = j(\mathcal{E}) - j(E) \in (\epsilon)$ the **deformation parameter** of $\mathcal{E}$.
- Concretely: $\mathcal{E} : y^2 = x^3 + ax + b$ with $a = b = \frac{27(j(E)+\lambda)}{4(1728-j(E)-\lambda)}$ has $j$-invariant $j(\mathcal{E}) = j(E) + \lambda$.

# What's the connection to modular polynomials?

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

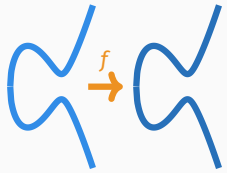
1. Compute the deformation $\mathcal{E}/R$ with $\tilde{j} = j(\mathcal{E}) = j(E) + \epsilon$, where $R = \mathbb{F}_p[\epsilon]/(\epsilon^{\ell+2})$
2. Compute the evaluated modular polynomial $\phi_\ell(\tilde{j}, Y) \in R[Y]$.
3. Substitute $\epsilon = X - j(E)$:

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

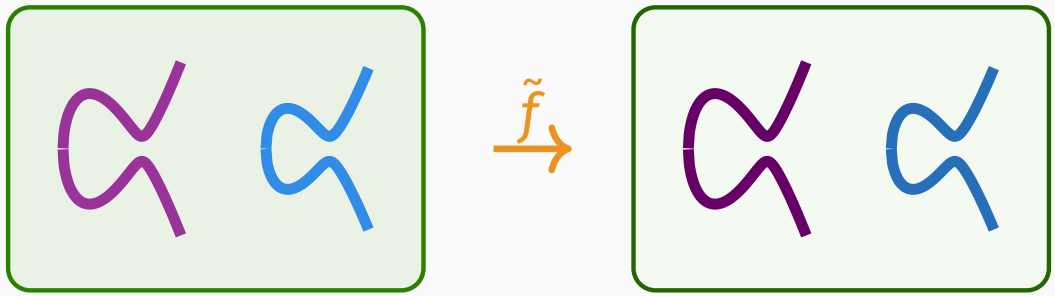
- This is the modular polynomial, since $\deg_X(\phi_\ell) = \ell + 1$.

# 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 $\ell$-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

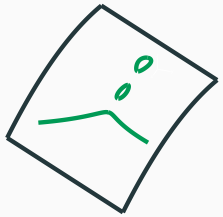
# Overview of the 2-dimensional setting

**Principally polarized abelian varieties $A$ in dimension 2**

- Product of elliptic curves.

- $\chi_{10} = 0$

- Jacobian of genus-2 curve $C$.



- $\chi_{10} = \mathrm{disc}(C)$

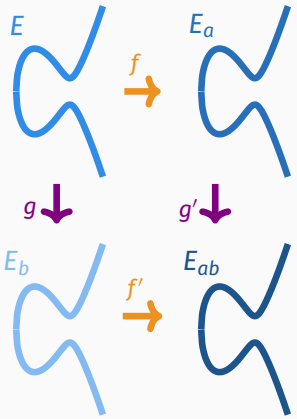
($\chi_{10}$ is a weight-10 cusp form.)

**$(\ell, \ell)$-Isogenies**

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

# Kani's Lemma

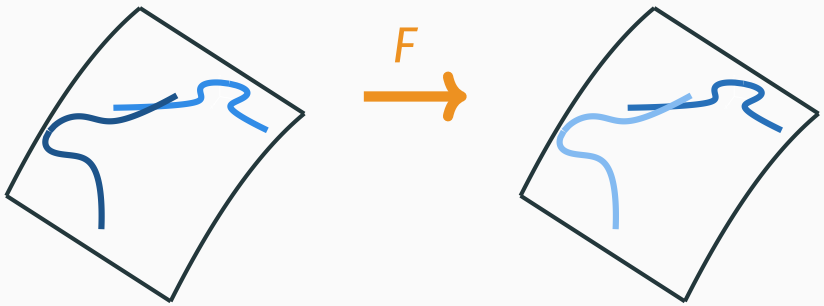
A commutative diagram of isogenies (as on the right) with $d_a = \deg(f) = \deg(f')$ and $d_b = \deg(g) = \deg(g')$ is called $(d_a, d_b)$-**isogeny diamond**.




**Kani's Lemma**

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

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



# Lifting an isogeny diamond

Let $F : A \to A'$ be an isogeny of p.p. abelian surfaces over $k$.

$\mathcal{A}$ deformation of $A$ $\quad\Rightarrow\quad$ $\exists$ unique $\tilde{A}$ deformation of $A'$ and a lift $\tilde{F} : \mathcal{A} \to \mathcal{A}'$.

---

Let $(E, E_a, E_b, E_{ab})$ be the vertices of an isogeny diamond, and $F : E \times E_{ab} \to E_a \times E_b$ the induced product isogeny.

$\mathcal{E}$ a deformation of $E$ $\quad\Rightarrow\quad$ $\exists$ unique $\mathcal{E}_a, \mathcal{E}_b, \mathcal{E}_{ab}$ and a lift to a *product* isogeny $\tilde{F} : \mathcal{E} \times \mathcal{E}_{ab} \to \mathcal{E}_a \times \mathcal{E}_b$.

(?) How to find $\mathcal{E}_{ab}$ without lifting the elliptic curve isogenies?

# Lifting product isogenies

**Proposition**

Let $(E, E_a, E_b, E_{ab})$ and $F$ as before all defined over $k$, and $\mathcal{E}$ a fixed deformation of $E$.

For an arbitrary 1st-order deformation $\mathcal{E}_{ab}$ of $E$ with deformation parameter $\lambda_{ab}$, we denote $\tilde{F} : \mathcal{E} \times \mathcal{E}_{ab} \to A$ for the lifted (normalized) isogeny.

Then there exist $\alpha, \beta \in k$ so that

$$\chi_{10}(A) = \alpha\epsilon + \beta\lambda_{ab}$$

for all $\lambda_{ab} \in (\epsilon)$.

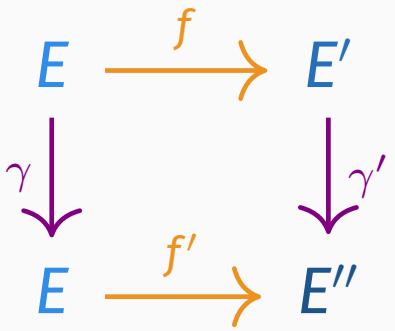
**Finding the deformation that splits**

1. Compute $\tilde{F}$ for two arbitrary parameters, e.g. $\lambda_{ab} = 0, \epsilon$.
   $\to$ Determine $\alpha, \beta$.
2. Compute the "correct" $\lambda_{ab}$ so that $\chi_{10}(A) = 0$.

- Deformation to $R = k[\epsilon]/(\epsilon^n)$ in $\log_2(n)$ steps.

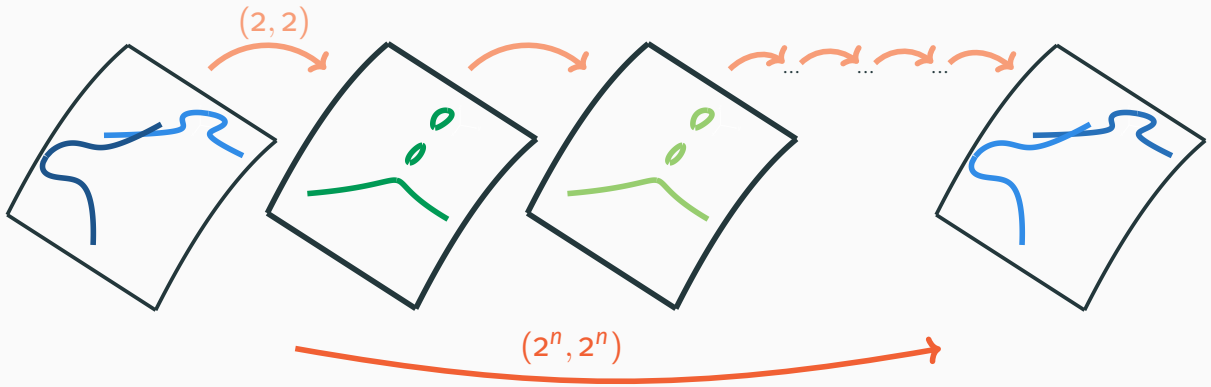
# A special isogeny diamond

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




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

This is an $(\ell, 2^n - \ell)$-isogeny diamond and induces a $(2^n, 2^n)$-product isogeny.

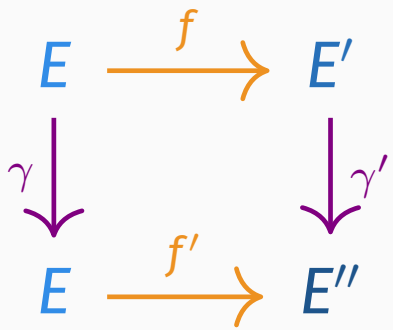


# An algorithm for computing modular polynomials

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

**Input:** A prime $\ell$ 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 $j(\mathcal{E}) = j(E) + \epsilon \in k[\epsilon]/(\epsilon^{\ell+2})$.
3. For each $\ell$-isogeny $f_i : E \to E'$:
   (a) Construct a special $(\ell, a^2 + 4b^2)$-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. $\varphi_\ell = \prod (Y - j_k)(\epsilon = X - j(E)) \in \mathbb{F}_p[X, Y]$.

# Computing $\Phi_\ell \in \mathbb{Z}[X, Y]$

**Input:** A prime $\ell$ with $\ell \equiv 3 \pmod 4$.

**Output:** $\Phi_\ell \in \mathbb{Z}[X, Y]$

1. Choose $n \in O(\log(\ell))$ and $a, b$ so that $2^n - \ell = a^2 + 4b^2$.
2. $B = 6\ell \log(\ell) + 16\ell + \min(2\ell, 14\sqrt{\ell}\log(\ell))$.
3. $P = 1$, $p = 1$, $\Phi = 0$.
4. `While` $\log(P) < B$:
   (a) $p = \texttt{next\_prime}(p)$ with $p \equiv -1 \pmod{\ell \cdot 2^n}$, and $P \leftarrow P \cdot p$.
   (b) Compute $\varphi_\ell \in \mathbb{F}_p[X, Y]$ (previous slide).
   (c) $\Phi = \mathrm{CRT}(\Phi, \varphi_\ell) \in \mathbb{Z}/P\mathbb{Z}[X, Y]$
5. Deduce the polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$

# Complexity of our algorithm

| | |
|---|---|
| We compute $\varphi_\ell \in \mathbb{F}_p[X, Y]$ for about $\ell$ primes of bitsize $O(\log(\ell))$. | $\ell$ |
| • For each $\varphi_\ell$: deformation of $\ell+1$ isogenies to $\mathbb{F}_{p^2}[\epsilon]/(\epsilon^{\ell+2})$. | $\ell$ |
| • Costliest step for each deformation: $2^{O(\log(\ell))}$-isogeny over $\mathbb{F}_{p^2}[\epsilon]/(\epsilon^{\ell+2})$. | $\log(\ell)$ |
| Cost of multiplications in $\mathbb{F}_{p^2}[\epsilon]/(\epsilon^{\ell+2})$. | $\ell \log(\ell)^2 \log\log(\ell)$ |

**Total cost:** $O(\ell^3 \log(\ell)^3 \log\log(\ell))$.

# An unconditional version

# Heuristic assumption

**Mild heuristic**: There exists $n \in \mathcal{O}(\log(\ell))$ so that $2^n - \ell = a^2 + 4b^2$ for some integers $a, b$.

$\Rightarrow$ used in the runtime analysis of the 2-dimensional version of our algorithm

**Unconditional**: There exist $a, b, c, d \in \mathbb{Z}$ so that $2^n - \ell = a^2 + b^2 + c^2 + d^2$ for any $n$ (in particular $n = \lceil \log(\ell) \rceil$).

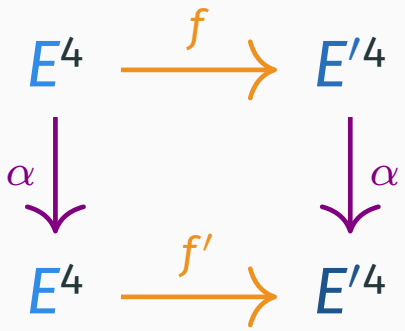
$\Rightarrow$ construct an unconditional 8-dimensional version of our algorithm

# A special isogeny diamond in dimension 8

Let $f : E \to E'$ over $\mathbb{F}_p$ an $\ell$-isogeny.

Write $2^n - \ell = a^2 + b^2 + c^2 + d^2$ and

$$\alpha = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}.$$




$\Rightarrow$ defines an
$a^2 + b^2 + c^2 + d^2$-endomorphism $\alpha : E^4 \to E^4$.

This is an $(\ell, 2^n - \ell)$-isogeny diamond and induces a $2^n$-isogeny [3]

$$F : E^4 \times E'^4 \to E^4 \times E'^4.$$

Similar to before this is used to deform isogenies efficiently.

[3] notation from before: $(2^n, \ldots, 2^n)$-isogeny.

# Summary

# Summary

**Quasi-linear algorithm to compute $\Phi_\ell$**

- Heuristic version:
  - Deforming smooth-degree isogenies (in dim 2) instead of prime degree isogenies (in dim 1).
  - Sagemath implementation: `https://github.com/sabrinakunzweiler/modular-polynomials`
- Unconditional version:
  - Deforming smooth-degree isogenies (in dim 8) instead of prime degree isogenies (in dim 1).
  - Expected to be slower in practice.
  - First unconditional quasi-linear algorithm.

**Thanks for your attention!**