Computing the trace of elliptic curve endomorphisms via p-adic lifting

Alessandro Sferlazza
Joint work with Lorenz Panny, Damien Robert

Technical University of Munich

02 December 2025
Isogeny Club

Motivation: computing traces

Main characters:

- Elliptic curves over a finite field $\mathbb{F}_q$, $\quad q = p^m$.
- An endomorphism $\varphi \in \mathrm{End}(E)$, over $\mathbb{F}_q$ as well.

Abstractly, $\mathrm{End}(E) \cong \mathcal{O}$ isomorphic to an order in a quadratic/quaternion algebra over $\mathbb{Q}$.
Problem: how to make this isomorphism explicit?

Endomorphisms $\varphi \in \mathrm{End}(E)$ are *quadratic integers*: they satisfy

$$\varphi^2 - [t]\varphi + [d] = 0, \qquad t = \mathrm{tr}(\varphi), \quad d = \deg(\varphi).$$

- The degree $d = \deg \varphi$ is usually intrinsic to the representation of φ on a computer.
- Together with the trace $t = \mathrm{tr}\, \varphi \qquad \rightsquigarrow$ complete description of $\varphi \in \mathcal{O}$. ✓

Cost of computing $\mathrm{tr}\, \varphi$ on a curve $E/\mathbb{F}_{p^m}$, where φ is stored in $n = O(\log pd)$ field elements

[BCEMP18] arXiv 1804.04063	$\widetilde{O}(n^7)$	ordinary, supersingular
[MPSW25] arXiv 2501.16321	$O(n^4 \log(n)^2)$	supersingular
this work	$\widetilde{O}(n^3)$	ordinary, supersingular

Inspiration: point counting algorithms

Classical problem in number theory: Given $E/\mathbb{F}_q$ with $q = p^m$, compute $\#E(\mathbb{F}_q)$.

How to solve? Take $\pi\colon (x, y) \mapsto (x^q, y^q)$ the q-Frobenius endomorphism on E.

- Satisfies quadratic equation

$$\Phi(\pi) = \pi^2 - t\pi + q = 0, \qquad t = \mathrm{tr}(\pi),\ |t| \leq 2\sqrt{q}$$

- The number of q-rational points is

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

Point counting $\longleftrightarrow$ computing the trace of Frobenius.

- SEA algorithm (Schoof 1985, Elkies, Atkin 1990s, ...):
  - computes $\mathrm{tr}(\pi) \bmod \ell$ for many small primes ℓ, combine via Chinese Remainder Theorem

  $\rightsquigarrow$ state-of-the-art trace computation algorithms are variants of SEA.

- Satoh's algorithm (Satoh 2000, ...): different approach $\leftsquigarrow$ we adapt this one!
  - p-adic lifting of curves and endomorphisms
  - action of morphisms on invariant differentials

Ingredient #1: differential scaling factors

We look at $E: \; y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ locally.

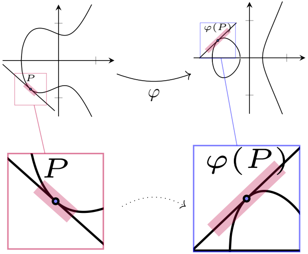
- E is a smooth curve: the tangent space at $P \in E$ is a line $\cong \mathbb{F}_q$.
- algebraic group: translations $Q \mapsto Q + P$ induce isomorphisms on tangent spaces
  $\rightsquigarrow$ there's a translation-invariant differential $\omega_E = dx/y$ on E

Morphisms $\varphi \colon E \to E'$ interact with differentials:

$$\varphi^* \omega_{E'} = \omega_{E'} \circ \varphi = c \cdot \omega_E, \qquad c \in \mathbb{F}_q.$$

where as a rational map, φ looks like:

$$\varphi(x, y) = \big(f(x),\; c^{-1} \cdot y \cdot f'(x)\big).$$



Wanna find c explicitly?

× can't generally store $f(x)$ on a computer, too large.

✓ scaling factors are multiplicative: given a chain $\varphi = \varphi_n \circ \ldots \circ \varphi_1$

- Small steps φ_i can be written explicitly $\rightsquigarrow$ recover scaling factor c_i
- We can combine the scaling factors: $\quad c_\varphi = c_{\varphi_1} \cdots c_{\varphi_n}.$

Interaction: $\mathrm{End}(E)$ and invariant differentials

We saw that $\mathrm{End}(E)$ acts on differentials:

$$\varphi^*\omega_E = c_\varphi\,\omega_E \text{ for some } c_\varphi \in k.$$

More precisely, the following is a ring homomorphism:

$$\mathrm{End}(E) \to k, \quad \varphi \mapsto c_\varphi.$$

$$\varphi^2 - [t]\varphi + [d] = 0$$
$$\rightsquigarrow$$
$$c_\varphi^2 - tc_\varphi + d = 0.$$

💡 c_φ is also quadratic, with the same trace as φ $\rightsquigarrow$ $\mathrm{tr}(\varphi) = c_\varphi + d/c_\varphi$.

- ✗ If $c_\varphi \in \mathbb{F}_q$, then $c_\varphi + d/c_\varphi$ is the image of an integer in $\mathbb{F}_q$: $\rightsquigarrow$ only get $\mathrm{tr}(\varphi) \bmod p$.
- ✓ Replace $(E/\mathbb{F}_q, \varphi)$ with a lift $(\widetilde{E}, \widetilde{\varphi})$ over a characteristic-0 ring R.
  Lifting preserves algebraic relations: $\mathrm{tr}(\widetilde{\varphi}) = \mathrm{tr}(\varphi)$.
  $\rightsquigarrow$ Now $\mathrm{tr}(\widetilde{\varphi})$ lies in $\mathbb{Z} \hookrightarrow R$, i.e., an actual integer!

Problems to solve:
- ▷ Computing c_φ easy if φ is a chain of steps of small degree. ✓
- ▷ Lifting (E, φ): let's see how!

Background digression: p-adic lifting

Useful tool: p-adics

Def Let p be a prime. The ring of p-adic integers

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i\, p^i \,\middle|\, a_i \in \{0, \ldots, p-1\} \right\}.$$

is a ring of characteristic 0, with a natural projection on $\mathbb{F}_p$: $\quad \sum_i a_i p^i \mapsto a_0 \in \mathbb{F}_p$.

Idea: $\mathbb{Z}_p \approx$ "series in p" with coefficients in $\mathbb{F}_p$.

- minor edits, defining $\mathbb{Z}_q \approx$ "series in p" with coefficients in an extension $\mathbb{F}_q$
  $\rightsquigarrow$ characteristic-0 ring $\mathbb{Z}_q$ projecting onto $\mathbb{F}_q = \mathbb{Z}_q / p\mathbb{Z}_q$

$$\sum_j (a_j + ib_j)p^j$$
$$\Uparrow$$
$$(a_0 + ib_0) \in \mathbb{F}_{p^2}$$

⚠ On a computer, limited space $\rightsquigarrow$ we truncate elements to finite precision k:

$$x \in \mathbb{Z}_q \quad \rightsquigarrow \quad x = x_0 + x_1 p + \ldots + x_{k-1} p^{k-1} + O(p^k)$$

- We can see the residue field $\mathbb{F}_q = \mathbb{Z}_q / p\mathbb{Z}_q$ as p-adic integers of precision 1.

Hensel-lifting: polynomial roots

Problem: Given $a \in \mathbb{F}_q$ with certain properties, can we (efficiently) build $\widetilde{a} \in \mathbb{Z}_q$ that

- is a lift: $\widetilde{a} \pmod p = a$
- satisfies the same properties?

✓ Yes! for roots of polynomials and polynomial systems.

Hensel's lemma:

(stated for $p > 2$)

> Let $f \in \mathbb{Z}_q[x]$ a polynomial, and $a \in \mathbb{Z}_q$ a simple root modulo p:
> $$f(a) = 0 \pmod p, \qquad f'(a) \neq 0 \pmod p.$$
> We can lift a uniquely to $\widetilde{a} \in \mathbb{Z}_q$ with $\widetilde{a} \equiv a \pmod p$ and $f(\widetilde{a}) = 0$.

Hensel generalizes to systems of polynomial equations:

- Replace f by a polynomial map $F(x) = (f_1(x), \ldots, f_n(x)) \colon \mathbb{Z}_q^m \to \mathbb{Z}_q^n$.
- Instead of $f'(a) \neq 0$, we ask $DF(a)$ surjective.

and to f any differentiable function $\mathrm{Frac}(\mathbb{Z}_q) = \mathbb{Q}_q \to \mathbb{Q}_q$! calculus works on p-adic fields!

Hensel lifting, algorithmically

Goal: given $f \in \mathbb{Z}_q[x]$, and $f(a) = 0 \pmod p$, find a lift $\widetilde{a}$ with $f(\widetilde{a}) = 0 \in \mathbb{Z}_q$.

Newton iterations make Hensel lifting constructive:

Lift $f(a) = 0 \pmod{p^k}$ to double precision p^{2k}: $\widetilde{a} = a + tp^k$

$$f(a + tp^k) = f(a) + t \cdot f'(a) \cdot p^k + O(p^{2k}) \stackrel{?}{=} 0 \pmod{p^{2k}}$$

Linear equation: if $f(a), f'(a)$ are known, solve for t.

$\ldots$

$a_4 \bmod p^4$

$a_2 \bmod p^2$

$a \bmod p$

Example: given $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_p$, lift a torsion point $P = (x_P, 0) \in E[2]$

- fix a lift $\widetilde{E} : y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}/p^2\mathbb{Z}$.
- we want $\widetilde{P} = (\widetilde{x_P}, 0) \in \widetilde{E}[2]$ $\rightsquigarrow$ lift a root of $f(x) = x^3 + Ax + B$.

The lift is $\widetilde{x_P} = x_P + tp$, $\qquad t = -\dfrac{f(x_P)/p}{f'(x_P)} = -\dfrac{(x_P^3 + Ax_P + B)/p}{3x_P^2 + A}$.

Now, what if we want to lift a point $Q \in E[2^{128}]$? The division poly ψ is quite large...

Hensel-lifting from black-box algorithms

Problem: given $a \in \mathbb{Z}_q/p^k\mathbb{Z}_q$ root of $f(x)$ at precision k, lift it to double precision.

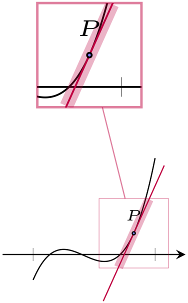
Strategy: solve linear equation $f(a) + t \cdot f'(a)\, p^k \equiv 0 \pmod{p^{2k}}$.

⚠ We need $f(a), f'(a)$ at precision k. What if we can't store f' explicitly?

✓ a black-box $a \mapsto f(a)$ is sufficient.

Evaluate two different lifts:

$$\begin{array}{rcllr} a & \mapsto & f(a) & & + O(p^{2k}) \\ a + p^k & \mapsto & f(a) & + f'(a)p^k & + O(p^{2k}) \end{array}$$



When we ignore multiples of p^{2k}, the function f looks affine-linear.

The slope of f around a is its derivative $\rightsquigarrow$

with two black-box evaluations of f in precision $2k$,
we get the value of $f'(a)$ at precision k.

Back to our friends: Isogenies 🥰

Canonical lifts: Serre–Tate's theory

We can lift roots of polynomials. But would you like to lift some ELLIPTIC CURVES?

Theorem (Serre–Tate–Grothendieck–Messing–Gross + tweaks)
Let $E/\mathbb{F}_q$ an elliptic curve, $\varphi \in \mathrm{End}_{\mathbb{F}_q}(E) \setminus \mathbb{Z}$ a separable endomorphism.
There is a unique lift $(\widetilde{E}, \widetilde{\varphi})$ over $\mathbb{Z}_q$ with $\mathrm{End}(\widetilde{E}) = \mathbb{Z}_q[\widetilde{\varphi}]$.

Special case: when E is ordinary, lifting E with the dual $\widehat{\pi}$ of its Frobenius
$\rightsquigarrow$ canonical lift $(\widetilde{E}, \widetilde{\widehat{\pi}})$ satisfying $\mathrm{End}(\widetilde{E}) \cong \mathrm{End}(E)$.

The $\bmod p$ projection induces a ring hom $\mathrm{End}(\widetilde{E}) \hookrightarrow \mathrm{End}(E)$.
$\rightsquigarrow$ characteristic polynomials ($\rightsquigarrow$ traces too!) are preserved by lifting.

Can we lift (E, φ) algorithmically?

- Lifting curve = lifting coefficients. $y^2 = x^3 + ax + b \quad \rightsquigarrow \quad y^2 = x^3 + \widetilde{a}x + \widetilde{b}$
- Lifting φ = ? ...depends on the algorithmic representation of φ.

Isogeny representations

Given a separable $\varphi\colon E \to E'$ isogeny, how do we represent it?

Isogeny chain: When φ has smooth degree $N = \prod_i \ell_i$, then it factors into small steps:

$$E = E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_r} E_n = E', \qquad \varphi: E_0 \to E_n$$

Represent φ_i via a kernel point: $\ker \varphi_i = \langle P_i \rangle, \quad P_i \in E_{i-1}[\ell_i]$.

$\rightsquigarrow$ from the tuple $(E, P_1, \dots, P_n)$, via Vélu's formulas, we can efficiently compute:

- the codomain E_n,
- given any $R \in E$, the image $\varphi(R)$.

$\rightsquigarrow$ We call $(E, P_1, \dots, P_n)$ an efficient representation of φ.

Other possibilities:

- Chain of j-invariants: $(E, j(E_1), \dots, j(E_n))$
- Radical isogenies: $(E, \varepsilon_1, \dots, \varepsilon_n)$ with a choice of "direction" ε_i for each step
- HD representation (coming in a bit!)

Lifting a single isogeny step

Let $E_i : y^2 = x^3 + a_i x + b_i$ over $\mathbb{F}_q$ for $i = 0, 1$, $\varphi\colon E_0 \to E_1$ an ℓ-isogeny, ℓ small.

First lift the domain curve to $\widetilde{E_0} : y^2 = x^3 + \widetilde{a}_0 x + \widetilde{b}_0$.

(sqrt)Vélu: Say $\ker\varphi = \langle P \rangle$. How do we lift to $\widetilde{P}$?

- $\widetilde{P}$ is of order ℓ: lift root of division polynomial $\psi_{\widetilde{E},\ell}(x)$, get $x_P \rightsquigarrow \widetilde{x_P}$
  - better: $\psi_{\widetilde{E},\ell}$ depends polynomially on the curve: $\psi_\ell(a, b, x)$.
    $\rightsquigarrow$ compute partial derivatives wrt a, b, x $\rightsquigarrow$ linear dependency between $\widetilde{a}_0, \widetilde{b}_0, \widetilde{x_P}$
- $\widetilde{P}$ lies on $\widetilde{E}$: lift root of defining polynomial $y^2 - x^3 - \widetilde{a}x - \widetilde{b}$
  $\rightsquigarrow$ linear dependency between $\widetilde{a}, \widetilde{b}, \widetilde{x_P}, \widetilde{y_P}$

j-invariants: if we've got $(E_0, j(E_1))$, instead of a kernel point?

$\rightsquigarrow$ BMSS, 2008, computes E_1 with the correct j, and $\varphi\colon E_0 \to E_1$.

✓ The computation is algebraic: rational fn of the input

⚠ problems when $j(E_0)$ or $j(E_1)$ are in $\{0, 1728\}$... as usual

- φ non unique
- non-smooth map $j(E) \to E$

Note both this algo and Vélu compute a normalized φ (i.e. scaling factor $= 1$)

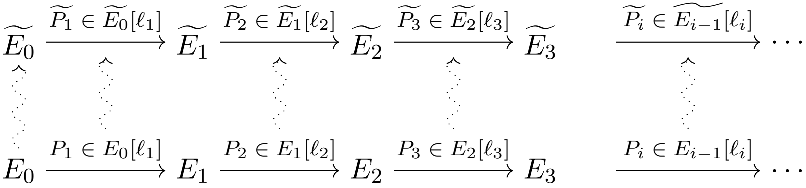
Lifting an isogeny chain

<u>Goal</u>: Lift an isogeny chain $\varphi = \varphi_n \circ \ldots \circ \varphi_1 \colon E_0 \to E_n$, with $\varphi_i \colon E_{i-1} \to E_i = E_{i-1}/\langle P_i \rangle$.
$\rightsquigarrow$ $(E, P_1, \ldots, P_n)$ efficient representation of φ as a chain of Vélu isogenies.

Choose $\widetilde{E_0}$ a lift of E_0. At each step:

- Hensel-lift P_i: get $(x(\widetilde{P_i}), y(\widetilde{P_i}))$ roots of polynomial constraints:
  (a) $\widetilde{P_i}$ lies on $\widetilde{E_{i-1}}$ (b) $\widetilde{P_i}$ has order $\ell_i = \deg \varphi_i$
- Compute lifted Vélu step: define $\widetilde{E_i} = \widetilde{E_{i-1}}/\widetilde{P_i}$.

The same strategy works when the steps are $\sqrt{\text{é}}$lu, radical isogenies, ...



Lifting iso-, lifting endo- morphisms

Isomorphisms Let E_0, E_1 be two isomorphic elliptic curves. Then they look like

$$E_0 : y^2 = x^3 + ax + b, \qquad E_1 : y^2 = x^3 + (u^4 a)x + (u^6 b) \qquad \text{for some } u \in \overline{\mathbb{F}_q}.$$

and the isomorphism (! up to sign!) is $\theta \colon E_0 \to E_1$ described by $(x, y) \mapsto (u^2 x, u^3 y)$.

The scaling factor of θ is $c = u^{-1}$. lifting θ = lifting u.

Endomorphisms Consider now $\psi \colon E \to E$. Wanna lift it to an endo $\widetilde{\psi} \colon \widetilde{E} \to \widetilde{E}$.

We know how to get an isogeny $\widetilde{\psi}_{\text{isog}} \colon \widetilde{E}_1 \to \widetilde{E}_2$. $\rightsquigarrow$ now lift extra algebraic constraint:

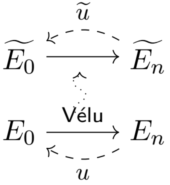
$$(\text{domain} = \text{codomain}) \qquad E = \psi(E) \quad \rightsquigarrow \quad \widetilde{E} = \widetilde{\psi}(\widetilde{E})$$

Efficient rep of a smooth endomorphism: $(E_0 : (a_0, b_0), P_0, \dots, P_n, u)$

where the P_i compute a Vélu chain $E_0 \to E_n$, and u an isomorphism $E_n \xrightarrow{\sim} E_0$.

Suppose we're given $((a_0, b_0), (P_i)_i, u)$ over $\mathbb{F}_q$ ($\rightsquigarrow$ sign choice for u)

- Endo-constraint: lifts of a_0, b_0 must satisfy $j(\widetilde{E_n}) = j(\widetilde{E_0})$
- Lift final isomorphism: find $\widetilde{u}$ s.t. $a(\widetilde{E_0}) = \widetilde{u}^4 \cdot a(\widetilde{E_n})$. ✓

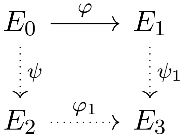


Time for some higher-dimensional fun :DD

Lifting higher-dimensional representations

Embedding Lemma Let $\varphi\colon E_0 \to E_1$ be separable of odd degree d.
One can build a 2D polarized 2^e-isogeny $\Phi\colon E_0 \times E_3 \to E_1 \times E_2$ s.t.

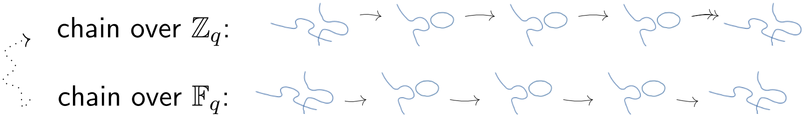
$$\varphi \quad \text{equals the composition} \quad E_0 \hookrightarrow E_0 \times E_3 \xrightarrow{\Phi} E_1 \times E_2 \twoheadrightarrow E_1.$$



The tuple (E_0, E_3, P, Q) gives an efficient representation for φ, where $\langle P, Q\rangle = \ker \Phi \subseteq (E_0 \times E_3)[2^e]$. To lift the 2D-rep, make sure:

- both P and Q lie on the domain product surface and have order 2^e
- the 2D isogeny with kernel P, Q lands on a product
- (extra constraint if we're lifting an endo): $j(E_0) = j(E_1)$

} all algebraic



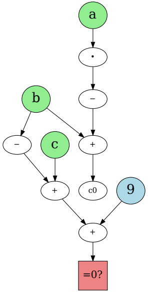
Same strategy generalizes to 4D, 8D representations.

Lifting different representations

What if φ is computed via minimal polynomials? as a sum? ENDLESS POSSIBILITIES...

If we've got a representation, Hensel lifting works, as long as

1. the isogeny computation from $(E, \text{extra data})$ is regular enough.
   e.g. in case of algebraic computation: the algo only uses $(+, \cdot, -, /)$.
   This implicitly describes a rational function with coeffs in $\mathbb{Z}$.
2. the given input is not a critical point of the constraint system i.e. $f'(x) \neq 0$
   Concrete requirement for isogenies: be separable.



In principle, we're not restricted to isogenies or polynomials!

- Lift a branch of square root $x \mapsto \sqrt{x}$:
  away from 0, can make a consistent sign choice, continuous wrt p-adic topology
- duals, inverse maps, P with small x and special properties...

Scaling factors and how to catch them

Problem left to solve: computing the scaling factor of a given isogeny

Known case: if we're given φ as composition of small-degree steps and isomorphisms:

- Vélu's formulas, √élu, BMSS output normalized isogenies: $c = 1$
- isomorphism $(x, y) \mapsto (u^2x, u^3y)$: directly represented via $u = c^{-1}$

General case: we've got an efficient representation of φ.

$\rightsquigarrow$ given $P = (x_P, y_P)$, can efficiently output $\varphi(P) = (x', y')$.

- Neat trick: any isogeny φ acts as $\varphi(P) = (f(x_P), c^{-1} \cdot y_P \cdot f'(x_P))$.
  Via Hensel-lifting, we can compute $f(x_P), f'(x_P)$.
  - cost: two evaluations of φ in precision 2 (i.e., over $\mathbb{Z}_q/p^2\mathbb{Z}_q$).

$\rightsquigarrow$ find c by division!

RECAP! Computing traces: the steps

Main problem: given (E, φ) over $\mathbb{F}_q$ with $\varphi \in \mathrm{End}(E)$, compute $\operatorname{tr}\varphi$.

- Give an upper bound for the trace: if $\deg\varphi = d$, then $|\operatorname{tr}\varphi| \leq \sqrt{4d}$ ($\approx$ Hasse-Weil)

$\rightsquigarrow$ p-adic precision goal: need the smallest k s.t. $p^k > 2 \cdot \sqrt{4d}$

- Hensel-lift (E, φ) to precision $\geq k$ $\rightsquigarrow$ $(\widetilde{E}, \widetilde{\varphi})$ defined over $\mathbb{Z}_q/p^k\mathbb{Z}_q$
- Compute the scaling factor of $\widetilde{\varphi}$ as seen above $\rightsquigarrow c_{\widetilde{\varphi}} \in \mathbb{Z}_q/p^k\mathbb{Z}_q$.
- Obtain the trace modulo p^k: $\quad t \bmod p^k = c_{\widetilde{\varphi}} + d/c_{\widetilde{\varphi}} \in \mathbb{Z}/p^k\mathbb{Z}$

  Choose repr t in $\mathbb{Z} \cap [-p^k/2, p^k/2]$. From the bound, $\operatorname{tr}(\varphi) = t \in \mathbb{Z}$.

Bulk of the computation: lifting to the highest precision.
i.e., $\approx$ re-evaluating the isogeny a handful of times (3-6) at precision k.

Complexity when φ isogeny chain:
(# steps) $\times$ (cost of a step) $\times$ (cost of multiplications in highest precision: $\mathbb{Z}_q/p^k\mathbb{Z}_q$) $=$

$$n \cdot O(\ell) \cdot \widetilde{O}(k^2) = \widetilde{O}(n^3), \qquad k \approx \log d \approx n, \quad \ell = O(1)$$

Summary

What we've got:

- An algorithm to lift isogeny representations
  - Actually works on general arithmetic computations
    with sage implementation! ✓
  - Some problems (+ workarounds) for $j = 0, 1728$
- Byproduct: constructive existence proof of Serre–Tate lifting theory
- Algorithm to compute scaling factor of any isogeny
- Trace computation in the case of smooth chains, HD, radical isogenies
  - with sage implementation! ✓
- Eprint: coming soon. STAY TUNED!

Thank you for your attention :D

Questions?