Isogeny Computations in the Level-4 Mumford Model

Dania Lazzarini, Université Libre de Bruxelles

BRISONS, 22 June 2026

Joint (ongoing) work with T. Decru, S. Kunzweiler, T. Lange and L. Maino

Work carried out at Okinawa Institute of Science and Technology (OIST).
Funded by a FRIA fellowship of the F.R.S.-FNRS.

Motivation & Context

The Isogeny Landscape

Efficient isogeny evaluation is central in various number-theoretic applications, including isogeny-based post-quantum cryptography.

Currently, algorithmic efficiency is tied to specific curve models, like:

- Montgomery curves;
- Twisted Edwards/Hesse curves.

However, relying on a narrow set of curve families limits our algebraic flexibility and design space.

The Challenge

- **Performance Bottleneck:** Computing isogenies and scalar multiplications can require *heavy* finite field arithmetic.
- **Core Metric:** We measure success by minimizing the number of field multiplications (**M**) and squarings (**S**).

To optimize these counts, we don't just optimize algorithms - we look for alternative geometric models of elliptic curves that possess favorable arithmetic properties.

The State of the Art

The description of N-isogeny formulas becomes particularly simple when working with a level-N model.

- SoTA mainly focuses on level-2 and -3 models.

The Study Case: Level-4

Reasearch Question: can we find a model that supports level-4 structures *efficiently* provides an alternative mathematical foundation?

Aim of Our Work: determine whether the new interpretation of degree-4 isogeny formulas leads to improvements of the arithmetic in this model.

An Exploratory Work

Elliptic curves in level-4 Mumford model
and the Kummer quotient(s)

$\downarrow$

4-isogenies

$\downarrow$

Radical 4-isogenies and multiplication-by-4

$\downarrow$

...

The Level-4 Mumford Model & The Quotients

How a Theta Structure Induces a Model

A **level-N theta structure** *acts* transforming abstract group geometry into concrete polynomial equations.

The mechanism operates in various steps, including:

- identifying the projective embedding

$$P \mapsto [\theta_0(P) : \theta_1(P) : \cdots : \theta_{N-1}(P)] \in \mathbb{P}^{N-1};$$

- inducing the equations (the model).

The coefficients of the resulting model are entirely determined by evaluating the theta functions at the neutral element.

From the Mumford-4 Model to the Kummer Line

As a direct consequence of this machinery, a level-4 theta structure induces a model of an elliptic curve E (over $\mathrm{char}(p) \neq 2$) in $\mathbb{P}^3$ as the intersection of two quadrics:

$$E = E_{(a:b)} : \begin{cases} b\left(x_1^2 + x_3^2\right) = 2ax_0x_2 \\ b\left(x_0^2 + x_2^2\right) = 2ax_1x_3 \end{cases}$$

for some projective coefficient
$(a : b) \notin \{(1 : \pm 1), (1 : \pm i), (1 : 0), (0 : 1)\}$.

From the Mumford-4 Model to the Kummer Line

Computing directly on the full curve can be slow and inefficient, so we project down to:

- the Kummer line $E/\langle \pm 1 \rangle$,
- a degree-2 quotient of the Kummer line,

in order to successfully derive formulas for $4 \cdot P$ bypassing the full curve arithmetic.

From the Mumford-4 Model to the Kummer Line

Multiplication by $[-1]$ on E in Mumford form acts by a permutation of the coordinates:

$$\begin{aligned}[-1] : E &\longmapsto E \\ (x_0 : x_1 : x_2 : x_3) &\longmapsto (x_0 : x_3 : x_2 : x_1).\end{aligned}$$

The *Kummer* coordinates $u_0 = x_0,\ u_1 = x_1 + x_3,\ u_2 = x_2$ are invariant by multiplication with $[-1]$.

They are related by the quadratic *Kummer* equation

$$\mathcal{K} : abu_1^2 = 2a^2 u_0 u_2 + b^2(u_0^2 + u_2^2).$$

From the Kummer line to a special quotient [name tbd]

In addition to this model of the Kummer line, we are further interested in the *special* quotient of E

$$\overline{\mathcal{K}} = \mathcal{K}/\langle \pm u_1 \rangle \cong \mathbb{P}^1.$$

The doubling formulas for E descend to this quotient as well, and are remarkably similar to doubling formulas for level-2 theta functions.

4-isogenies

The 4-torsion and symplectic transformations

If $0_E = (t_0 : t_1 : t_2 : t_1)$ is the neutral element of E, then $E[4] = \langle P, Q \rangle$ with

$$P = (t_1 : t_2 : t_1 : t_0), \quad Q = (t_0 : it_1 : -t_2 : -it_1)$$

the *canonical basis* of $E[4]$.

Having an explicit description of the 4-torsion points allows us to:

- describe the action of P, Q on a generic point $X \in E$;
- characterize certain 8-torsion points;
- provide symplectic transformations of $\mathbb{P}^3$ acting on this 4-torsion basis.

The 4-torsion and symplectic transformations

Symplectic transformations are linear transformations that define isomorphisms of elliptic curves in Mumford form;
specifically, fixed a primitive 8-th root of unity ζ, the matrices

$$D = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}, \quad M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \zeta \end{bmatrix},$$

viewed as linear transformations of $\mathbb{P}^3$, define those isomorphisms:

$$\begin{aligned} f_D : E_{(a:b)} &\to E_{(a+b:a-b)}, \\ x &\mapsto D \cdot x \end{aligned} \qquad \begin{aligned} f_M : E_{(a:b)} &\to E_{(ia:b)}, \\ x &\mapsto M \cdot x. \end{aligned}$$

The 4-torsion and symplectic transformations

Moreover, the action on the canonical 4-torsion bases is given by

$$F_D = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad F_M = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

These transformations will be useful when we want to transform the kernel of a 4-isogeny into a specific form:

- there are 6 outgoing 4-isogenies at $E_{(a:b)}$ with kernels

  $$\langle P \rangle, \quad \langle P+Q \rangle, \quad \langle P+2Q \rangle, \quad \langle P+3Q \rangle, \quad \langle Q \rangle, \quad \langle Q+2P \rangle;$$

- They are respectively transformed via the following transformations to a canonical form:

  $$D,\ DM,\ DM^2,\ DM^3,\ Id,\ MD^{-2}M^{-1}.$$

In order to describe 4-isogenies, we introduce the following:

- $\mathcal{F}$: discrete Fourier transform;
- $\mathcal{C}_\lambda$ with $\lambda = (\lambda_0 : \lambda_1 : \lambda_2) \in \mathbb{P}^2$: coordinate-wise scaling $\mathcal{C}_\lambda(x) = (\lambda_0 x_0 : \lambda_1 x_1 : \lambda_2 x_2 : \lambda_1 x_3)$;
- $\odot^4$: coordinate-wise fourth powers $\odot^4(x) \mapsto (x_0^4 : x_1^4 : x_2^4 : x_3^4)$.

If $R \in E[32]$ is s.t. $8 \cdot R = Q$ and $(r_0 : r_1 : r_2 : r_3) = \mathcal{F} \circ \odot^4(R)$, then

$$\phi = \mathcal{F} \circ \mathcal{C}_\lambda \circ \mathcal{F} \circ \odot^4 : E \to E'$$

with $\lambda = (r_1 r_2 : r_0 r_2 : r_0 r_3)$ defines a 4-isogeny with kernel $\langle Q \rangle$. Moreover, the codomain E' is in level-4 Mumford form, and the canonical 4-torsion basis is given by $(\phi(P), 2 \cdot \phi(R))$.

4-isogenies on the Kummer line

The maps $\odot^4, \mathcal{F}, \mathcal{C}_\lambda$ descend on the Kummer line as follows:

$$\begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix} \overset{\widetilde{\odot^4}}{\longmapsto} \begin{pmatrix} 2a^2b^2u_0^4 \\ 8a^4u_0^2u_2^2 - b^4(u_0^2+u_2^2)^2 \\ 2a^2b^2u_2^4 \end{pmatrix},$$

$$\begin{pmatrix} u_0' \\ u_1' \\ u_2' \end{pmatrix} \overset{\widetilde{\mathcal{F}}}{\longmapsto} \begin{pmatrix} u_0'+u_1'+u_2' \\ 2(u_0'-u_2') \\ u_0'-u_1'+u_2' \end{pmatrix}, \quad \begin{pmatrix} u_0'' \\ u_1'' \\ u_2'' \end{pmatrix} \overset{\widetilde{\mathcal{C}_\lambda}}{\longmapsto} \begin{pmatrix} \lambda_0 u_0'' \\ \lambda_1 u_1'' \\ \lambda_2 u_2'' \end{pmatrix}.$$

The 4-isogeny $\widetilde{\phi} : \mathcal{K} \to \mathcal{K}'$ is given by $\widetilde{\mathcal{F}} \circ \widetilde{\mathcal{C}_\lambda} \circ \widetilde{\mathcal{F}} \circ \widetilde{\odot}^4$, and the evaluation of a 4-isogeny on the Kummer line costs $4\mathsf{S} + 16\mathsf{a} + 7\mathsf{m}$.

4-isogenies from the special quotient (work in progress)

In analogous way to the Kummer line, we find an isogeny on the *special* quotient that lifts to the 4-isogeny ϕ, and is explicitly defined through the use of 16-torsion and the following maps $\mathbb{P}^1 \to \mathbb{P}^1$:

- $\mathcal{H}$: Hadamard transform;
- $\mathcal{C}_\lambda$ with $\lambda = (\lambda_0 : \lambda_2) \in \mathbb{P}^1$: coordinate-wise scaling $\mathcal{C}_\lambda(x) = (\lambda_0 x_0 : \lambda_2 x_2)$;
- $\odot^2$: coordinate-wise squaring $\odot^2(x) \mapsto (x_0^2 : x_2^2)$.

Radical 4-isogenies and multiplication-by-4

Radical isogenies

A *radical N-isogeny formula* takes as input an elliptic curve E together with a point P of order N. The output consists of:

- an elliptic curve E' which is the codomain of an N-isogeny $\phi : E \to E'$ with kernel $\ker(\phi) = \langle P \rangle$;
- a point $P' \in E'[N]$ which is a point of order N defining an isogeny $\phi' : E' \to E'/\langle P' \rangle$ with the property that $\phi' \circ \phi$ is an N^2-isogeny.

The formula itself consists of algebraic expressions in the coefficients of E and the coordinates of P, as well as one N-th root.

Radical 4-isogenies

Note: the neutral element $(t_0 : t_1 : t_2 : t_1)$ already encodes all information about the elliptic curve, and a 4-torsion basis, so we only have to provide:

- the coordinates of the neutral element on the domain,
- the codomain of a 4-isogeny.

Radical 4-isogenies (theorem)

Let E be an elliptic curve in level-4 Mumford form with neutral element $0_E = (t_0 : t_1 : t_2 : t_1)$. And consider the elliptic curve E' with

$$0_{E'} = (t_0 + \alpha : t_2 : t_0 - \alpha : t_2), \quad \text{with } \alpha = \sqrt[4]{t_0^4 - t_2^4}.$$

Further, let (P, Q) and (P', Q') be the canonical bases of $E[4]$ and $E'[4]$, respectively.

Then there exists a 4-isogeny with $\phi : E \to E'$ with kernel $\ker(\phi) = \langle Q \rangle$, and the kernel of the dual isogeny is given by $\ker(\hat{\phi}) = \langle P' \rangle$.

In particular, the above is a *radical isogeny formula*.

Multiplcation-by-4 (theorem)

Let E be an elliptic curve in level-4 Mumford form with neutral element $0_E = (t_0 : t_1 : t_2 : t_1)$. Set $\lambda = (\lambda_0 : \cdots : \lambda_3)$ and $\lambda' = (\lambda'_0 : \cdots : \lambda'_3)$ with

$$\begin{cases} \lambda_0 := (t_0^3 - t_2^3)^4 (t_0^4 - t_2^4)^3, \\ \lambda_1 := (t_0^6 - t_2^6)^4, \\ \lambda_2 := (t_0^3 + t_2^3)^4 (t_0^4 - t_2^4)^3, \\ \lambda_3 := (t_0^6 - t_2^6)^4, \end{cases} \qquad \begin{cases} \lambda'_0 := 4 t_2 t_1^3 (3t_0^2 + t_2^2), \\ \lambda'_1 := t_0 t_2 (3t_0^2 + t_2^2)(t_0^2 + 3t_2^2), \\ \lambda'_2 := 4 t_0 t_1^3 (t_0^2 + 3t_2^2), \\ \lambda'_3 := t_0 t_2 (3t_0^2 + t_2^2)(t_0^2 + 3t_2^2). \end{cases}$$

Then the multiplication-by-4 map $[4] : E \to E$ can be decomposed into simple operations as follows:

$$[4] = C_{\lambda'} \circ \mathcal{F} \circ C_{\lambda} \circ \odot^4 \circ \mathcal{F} \circ \odot^4.$$

Conclusion & Open Directions

Future Applications & Open Problems

This model serves as a new baseline. Where do we go from here?

- **Twisted Mumford Form:** cheaper multiplication-by-4
- **Higher Dimension:** $(4, 4)$-isogenies
- tbd :)

Thank You!

Questions?