IACR Communications in Cryptology
ISSN 3006-5496, Vol. 1, No. 1, 32 pages.
https://doi.org/10.62056/abvua69p1

Computing 2-isogenies between Kummer lines

Damien Robert and Nicolas Sarkis

Univ. Bordeaux, CNRS, INRIA, Bordeaux INP, IMB, UMR 5251, INRIA CANARI team, Talence, France

Abstract. We use theta groups to study 2-isogenies between Kummer lines, with a particular focus on the Montgomery model. This allows us to recover known formulas, along with more efficient forms for translated isogenies, which require only $2\mathbf{S} + 2\mathbf{m}_0$ for evaluation. We leverage these translated isogenies to build a hybrid ladder for scalar multiplication on Montgomery curves with rational 2-torsion, which cost $3\mathbf{M}+6\mathbf{S}+2\mathbf{m}_0$ per bit, compared to $5\mathbf{M}+4\mathbf{S}+1\mathbf{m}_0$ for the standard Montgomery ladder.

Keywords: Elliptic curve cryptography · Kummer lines · Isogenies · Scalar multiplication · Montgomery ladder

1 Introduction

1.1 Motivation

Elliptic curve cryptography is widely used in the TLS layer, and its speed is determined by the scalar multiplication. Its efficiency relies on the chosen model. On a Montgomery model, Montgomery [Mon87] provided an efficient algorithm known as the Montgomery ladder to compute $x(n \cdot P)$ with only the datum of $x(P)$. This allows protocols like the Diffie-Hellman key exchange protocol to only send the coordinate $x(n \cdot P)$, thus gaining in bandwidth.

Furthermore, the equation of the elliptic curve helps to recover $y(n \cdot P)$ from $x(n \cdot P)$, up to a sign. The sign can also be determined with $x((n+1) \cdot P)$, which is also computed by the ladder, at a negligible cost. To sum up, one efficient way to do a scalar multiplication on an elliptic curve is to do it only with the x-coordinate $x(P)$, and recover $y(n \cdot P)$ at the very end.

The mathematical object on which we only keep the x-coordinate is a Kummer line, which is described by a morphism $(x(P), y(P)) \mapsto x(P)$ from the elliptic curve to the projective line. It is a degree-2 map and its ramification points are the four 2-torsion points. An interesting fact about Kummer lines is that they are entirely described by this ramification, made of 4 points. This gives a very convenient and flexible approach to build models of Kummer lines as we will see throughout the paper. Apart from scalar multiplication, Kummer lines are also used a lot for isogeny based cryptography, as in [FJP14; CLN16].

The main goal of this paper is to provide a general method to study 2-isogenies between different models of Kummer lines, and to find old and new formulas for these isogenies, and notably to also study translated isogenies. Our main objective was to better understand the isogeny formulas from isogeny based cryptography, and in particular why the Montgomery model has fast 2-isogenies, in the hope to extend these formulas to higher dimension. For dimension 1, as we will see in Appendix C, although our translated 2-isogeny formula is

E-mail: damien.robert@inria.fr (Damien Robert), nicolas.sarkis@math.u-bordeaux.fr (Nicolas Sarkis)

Received: 2024-01-09 Accepted: 2024-03-05

faster than the usual one, in practice, as shown in [CH17], it is faster to decompose a 2^n-isogeny as a product of 4-isogenies rather than a product of 2-isogenies.

Our second application is to speed up the multiplication law on the Kummer line of an elliptic curve. Indeed, composing a 2-isogeny with its dual gives the multiplication by 2 map. This approach, pioneered by [DIK06], allows writing the doubling as a composition of two polynomials of degree 2 rather than a polynomial of degree 4. Such a decomposition is already used in the fast doubling formula of the Montgomery model [Mon87] or the theta model [GL09].

1.2 Results

On the Montgomery model with full rational 2-torsion, we can evaluate a 2-isogeny, translated by a suitable 2-torsion point in $2\mathbf{S} + 1\mathbf{m}_0$, compared to $2\mathbf{M} + 1\mathbf{m}_0$ for the non translated image. Composing with the translated dual isogeny, we obtain a translated doubling formula in $4\mathbf{S} + 2\mathbf{m}_0$, compared to $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$ for a standard doubling.

Using the translated doubling in the Montgomery ladder, and keeping track of the translation by the 2-torsion point, we obtain a hybrid ladder arithmetic which costs $3\mathbf{M} + 6\mathbf{S} + 2\mathbf{m}_0$ per bit, compared to $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}_0$ for the standard ladder for the Montgomery model. Thus, if $\mathbf{m}_0$ is sufficiently small, we obtain a more efficient scalar multiplication (while retaining the standard side channel protection of the Montgomery ladder). We remark also that the ladder for the theta model costs $3\mathbf{M} + 6\mathbf{S} + 3\mathbf{m}_0$, hence our hybrid ladder is always faster than the theta ladder.

1.3 Method

We proceed to a systematic study of 2-isogenies between Kummer lines by combining two tools:

1. First, we use that a Kummer model is completely determined by its four ramification points. Keeping track of the ramification along the isogeny allows us to keep track of the model, without resorting to formal groups as in Vélu's formulas;

2. Secondly we make a systematic use of theta groups and their action on sections to find invariant sections.

As explained in Remark 2 below (Section 2), the usual Vélu formulas [Vél71] can be seen as a special case of the above strategy, applied to the theta group of a divisor D invariant by translation and where the canonical action by the symmetric elements is trivial. In this paper we rather use the action of the theta group $G(2(\mathcal{O}_{E_1}))$ associated to the divisor $2(\mathcal{O}_{E_1})$, which is not invariant by translation, hence whose associated action is not trivial.

This will allow us in future work to extend this strategy to higher dimension. Notably, we will explain in an upcoming article how to study differential additions in dimension one on Kummer lines, using the fact that differential additions can be described by a 2-isogeny in dimension two, on a product of two Kummer lines. Extending our framework to a systematic study of 2-isogenies formulas between arbitrary models of Kummer surfaces is more challenging though, because the combinatorial description of the Kummer surface is given by a $(16, 6, 2)$-design in $\mathbb{P}^3$ rather than by simply 4 points in $\mathbb{P}^1$, so is harder to keep track off.

Our paper is exhaustive as we can apply this algorithm to several known models such as Legendre curves, Montgomery curves, but also theta functions of level 2. We give several examples, along with examples when we start from one type of model and obtain a new type of model for the codomain. This allows us to recover the efficient 2-isogenies formulas already in the literature in a unified manner, showing the flexibility of the framework.

A particularity of our framework is that we do not impose the neutral point $\mathcal{O}_{E_1}$ to be the point at infinity $\infty = (1 : 0)$ on the Kummer line. This extra flexibility allows us to naturally find new efficient formulas for translated isogeny images.

In particular, we study the Montgomery models of Kummer lines in more detail. Such a model exists whenever there is a point T_1' of 4-torsion which is rational on the Kummer model (so the set $\{T_1', -T_1'\}$ is rational on the elliptic curve). Let R_1 be a 2-torsion point, and E_2 the codomain of the isogeny with kernel R_1. The curve E_2 admits a Montgomery model if R_1 is distinct from $T_1 = 2 \cdot T_1'$, or when $T_1 = R_1$ and there exists a 8-torsion point $\widetilde{T_1}$ on E above T_1'. We give explicit formulas via our framework for these isogenies and their duals in both cases, recovering well known formulas in the literature [FJP14; CH17; Ren18]. Furthermore, we also obtain the efficient translated isogeny formula on a Montgomery model mentioned above.

We mainly focus in this paper on the study of 2-isogenies between models of Kummer lines which have a specific Galois action on their 2^n-torsion (like the Legendre model, the Montgomery model and the theta model). This is indeed the most interesting situation: the isogeny interacts with the Galois action. So either we lose some of the Galois information on the codomain, which means that we can only describe another type of model on the codomain (like Theta to Montgomery, Montgomery to Legendre, or Legendre to Montgomery), or we need to assume that we are given a supplementary input. For instance, for 2-isogeny formulas from theta to theta, we need a 8-torsion point above the kernel to find a theta model of the codomain.

By contrast, a model requiring, say, a rational 3-torsion point T would not have this problem with a 2-isogeny formula, since the image of T by the isogeny would immediately give a model of the codomain. In a similar vein, handling the case of odd degree isogenies in the models mentioned above (Montgomery, Legendre, Theta), is in some sense easier since the Galois structure on the 2^n-torsion is respected through the isogeny, see Appendix E for formulas.

1.4 Notations

We work with elliptic curves and Kummer lines defined over a field of characteristic different from 2, and with separable isogenies. When the kernel of an isogeny between elliptic curves has order n, we call it an n-isogeny. An n-isogeny between Kummer lines is then the projection of an n-isogeny between elliptic curves.

We will use the following complexity notations throughout the article:

- $\mathbf{M}$ is a generic multiplication,
- $\mathbf{S}$ is a generic squaring,
- $\mathbf{m}_0$ is a multiplication by a curve constant,
- $\mathbf{c}$ is a multiplication by a small constant (i.e. less than a computer word),
- $\mathbf{a}$ is an addition / subtraction.

1.5 Similar work

In [Mor+22], the authors introduce the generalized Montgomery coordinate h on an elliptic curve E_1, which can be seen as the composition $h = x \circ f$ of an isogeny $f : E_1 \to E_2$ to an elliptic curve in Montgomery form, with the x-coordinate on E_2 [Mor+22, Thm. 13]. They then give formulas for isogenies and scalar multiplication in the generalized Montgomery coordinate.

Our work is in an orthogonal direction. If the isogeny f is of degree n, a generalized Montgomery coordinate $h = x \circ f$ is a section of a divisor of degree $2n$ on E_1. The work of [Mor+22] may thus be seen as specifying a special model associated to a section of $2n(\mathcal{O}_{E_1})$ and developing the arithmetic and isogenies on this model.

By contrast, we focus only on sections of $2(\mathcal{O}_{E_1})$ to describe models of the Kummer line, but we don't impose conditions on the model; our framework allows us to derive efficient isogeny formulas between different Kummer models, including models where the neutral point is not at infinity.

In [KS20], the authors use the theta squared coordinates on the Kummer line. One can see that their doubling formulas in their Table 2 are indeed the one we recover up to a translation by a 2-torsion point in Algorithm 1. Our ladder is however slightly faster because we are using Montgomery differential addition instead of the theta squared one, a comparison is available in Table 2 in Section 5.

1.6 Roadmap

In Section 2 we recall Kummer models and the theory of theta groups and their action on sections, which allow us to develop our isogeny framework. We apply it in Section 4 to study 2-isogenies between Montgomery models, and we apply those in Section 5 where we introduce the hybrid ladder. We briefly discuss applications to fast evaluations of 2^n-isogenies in Appendix C. In Appendix B, we provide more examples of our technique with different ramification structure to show its flexibility. Finally, in Appendix E, we explain how to deal with odd degree isogenies.

2 2-isogenies between Kummer lines

In this whole article, k is a perfect field of characteristic different from 2.

2.1 Weierstrass coordinates

Let E/k be an elliptic curve given by an affine short Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$. If D is a divisor on E, we recall that a global section is a function $f \in k(E)$ from the function field $k(E)$ of E such that $\operatorname{div} f + D \geq 0$. The set of all global sections associated to D is denoted by $\Gamma(D)$.

For instance, if $D = (\mathcal{O}_E)$, $\Gamma((\mathcal{O}_E)) = \langle 1 \rangle$, $\Gamma(2(\mathcal{O}_E)) = \langle 1, x \rangle$, $\Gamma(3(\mathcal{O}_E)) = \langle 1, x, y \rangle$. The Weierstrass coordinates x, y give an embedding of E into $\mathbb{P}^2_k$; however, since x is even $(x(-P) = x(P))$, the application $E \to \mathbb{P}^1, P \mapsto x(P), \mathcal{O}_E \mapsto \infty$ factors through $E/\pm 1$. It is not hard to show that x gives an isomorphism of curves $E/\pm 1 \simeq \mathbb{P}^1$.

It is often convenient to work with projective coordinates to avoid divisions; the elliptic curve has a projective equation $Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ in $\mathbb{P}^2$. Working in projective coordinates means we pass from the divisor point of view to the line bundle point of view. We denote by $\mathfrak{O}_E(D)$ the line bundle associated to D; this is the sheaf given by the local sections of D, i.e., such that on a Zariski open U of E, we have $\mathfrak{O}_E(D)(U) = \Gamma(U, D) = \{f \in k(E) \mid \operatorname{div} f_{|U} + D_{|U} \geq 0\}$. We have $\Gamma(\mathfrak{O}_E(\mathcal{O}_E)) = \langle Z_0 \rangle$, $\Gamma(\mathfrak{O}_E(2(\mathcal{O}_E))) = \langle X_0, Z_0^2 \rangle$, $\Gamma(\mathfrak{O}_E(3(\mathcal{O}_E))) = \langle X = X_0Z_0, Y, Z = Z_0^3 \rangle$. We remark that $x = X/Z = X_0/Z_0^2$.

Since we are only interested in models of Kummer lines in this paper, we will change notations and denote $\Gamma(\mathfrak{O}_E(2D)) = \langle X, Z \rangle$, where $Z = Z_0^2$. With this notation, the full projective Weierstrass coordinates are XZ_0, Y, ZZ_0.

As explained in the introduction, it will be convenient to have models of Kummer lines where the neutral point is not at infinity. If $x \in \Gamma(2(\mathcal{O}_E))$ is an affine Weierstrass coordinate (resp. $(X : Z)$ are projective Weierstrass coordinates) this amounts to allow working with the affine coordinate $x' = \frac{ax+b}{cx+d}$ with $c \neq 0$ (resp. $(X' : Z') = (aX + bZ : cX + dZ)$). Notice that the divisor of poles of x' is not equal to $2(\mathcal{O}_E)$ when $c \neq 0$, but to a linearly equivalent divisor, so x' is not a section of $2(\mathcal{O}_E)$, while X', Z' are still sections of $\mathfrak{O}_E(2(\mathcal{O}_E))$.

2.2 Kummer lines

Let E be an elliptic curve defined over k. We have seen that $E/\pm 1 \simeq \mathbb{P}^1$. However, the curve $\mathbb{P}^1$ by itself is not enough to recover E, so we'll reserve the term Kummer line to include slightly more information:

Definition 1. A Kummer line is the datum of a degree 2 covering of $\mathbb{P}^1$ by E with 4 distinct ramification points, one of which is rational and marked:

$$\pi : E \to \mathbb{P}^1 \text{ and } \exists \mathcal{O} \in E(k), \exists T, R, S \in E \text{ with } \#\pi^{-1}(\pi(P)) = \begin{cases} 1 & \text{if } P \in \{\mathcal{O}, T, R, S\}, \\ 2 & \text{otherwise.} \end{cases}$$

A way to reinterpret this is that the involution quotient $E \to E/\pm 1 \simeq \mathbb{P}^1$ is a degree-2 cover ramified at 4 points. Conversely, for such a degree-2 cover of $\mathbb{P}^1$, the curve on the domain is of genus 1 by the Riemann-Hurwitz formula, and marking an explicit rational point makes it an elliptic curve E. The cover gives an embedding $k(\mathbb{P}^1) \to k(E)$, hence a Galois involution, which on the level of E has to be given by $P \mapsto -P$ because the neutral point is one of the ramified points of this involution. In particular, the fibres are $\pi^{-1}(\pi(P)) = \{-P, P\}$. We will give more details in a future work on the geometry of Kummer lines.

Example 1. The marked point is denoted with a $*$. If the ramification on the Kummer line is given by

$$(1:0)^*, \qquad (\alpha_1 : 1), \qquad (\alpha_2 : 1), \qquad (\alpha_3 : 1), \tag{1}$$

(with the α_i potentially defined over an extension of k) then the corresponding elliptic curve has equation, with some $\beta \in k$:

$$E : \beta y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3). \tag{2}$$

Conversely, starting from Eq. (2), if the point at infinity is denoted $\mathcal{O}$, then the following map is a degree 2-covering with 4 ramification points which correspond to the 2-torsion:

$$\begin{aligned} E &\xrightarrow{\pi} \mathbb{P}^1 \\ (x, y) &\mapsto (x : 1), \\ \mathcal{O} &\mapsto (1 : 0). \end{aligned}$$

We remark that a Kummer line cannot distinguish between an elliptic curve E and its quadratic twist E' which amount in the previous example to a choice of $\beta \in k^*/k^{*,2}$. Denote $\pi' : E' \to \mathbb{P}^1$ a Kummer line associated to the quadratic twist. If $p \in \mathbb{P}^1$ is not a ramification point of π and π', then there are two points $P \in E$ and $P' \in E'$ of order $n > 2$ such that $\pi(P) = \pi'(P') = p$, and either $P \in E(k)$ or $P' \in E'(k)$. Thus pushing the rational point along a 2-isogeny allows keeping track of the twist on the codomain even while working on the Kummer lines.

We will describe Kummer lines only via their ramification, like in Eq. (1), and denote them by $\mathcal{K}$, where $\mathcal{K} \simeq \mathbb{P}^1$. We will also forget about the π notation when it is not ambiguous and write $[P] = \pi(P)$.

The addition law is not well-defined any more on the Kummer line π, as if one knows $\pi(P)$ and $\pi(Q)$, one retrieves $\pm P$ and $\pm Q$ on the elliptic curve and won't be able to distinguish $\pi(P + Q)$ from $\pi(P - Q)$. However, with the knowledge of $\pi(P)$, $\pi(Q)$ and $\pi(P - Q)$, it is possible to reconstruct $\pi(P + Q)$, this is differential addition and is enough to build a scalar multiplication on the Kummer line, see for instance Montgomery arithmetic in Appendix A.

Consider a Kummer line π, and since we are interested in 2-isogenies, assume there is a rational 2-torsion point $T \in E(k)$. This is a particular case of where we can define the translation by T on the line, as $T = -T$, so $\pi(P - T) = \pi(P + T)$.

Main Example 1. By taking an automorphism of $\mathbb{P}^1$, i.e a homography, we can always send T to the point $(0:1)$ and the marked point to $(1:0)$. This amounts to working on the following curve, according to Eq. (2):

$$E : \beta y^2 = x(x^2 + \mathcal{A}x + \gamma).$$

The complete ramification on the Kummer line $\mathcal{K}$ associated to E is then

$$\mathcal{O} = (1:0)^*, \qquad T = (0:1), \qquad R = (\alpha:1), \qquad S = (\gamma:\alpha) = R+T,$$

where $\alpha \in \overline{k}$ satisfies the equation $\mathcal{A} = -\alpha - \frac{\gamma}{\alpha}$, with $\mathcal{A}, \gamma \in k$.

2.3 2-isogenies between Kummer lines via an analogue of Vélu's formulas

Let E_1/k be an elliptic curve, $T_1 \in E_1[2](k)$ a 2-torsion point, $K = \{\mathcal{O}_1, T_1\}$ and $f : E_1 \to E_2 = E_1/K$ be the corresponding isogeny. Neutral elements on E_1 and E_2 are denoted $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively.

Starting from a Kummer model of E_1, with affine coordinate $x_1 \neq 1$, we want to build a Kummer model of E_2 with affine coordinate $x_2 \neq 1$. For simplicity here, we will take x_1, x_2 to be Weierstrass coordinates.

Our goal is to express x_2 as a rational function of x_1. The coordinate x_2 is a section of the divisor $2(\mathcal{O}_2)$, its pullback by f is $f^*(2(\mathcal{O}_2)) = 2(\mathcal{O}_1) + 2(T_1)$. In particular, the coordinate $x_2 \circ f$ on E_1 is a section of $2(\mathcal{O}_1) + 2(T_1)$ which is invariant by translation by T_1. Conversely, any coordinate $u \in \Gamma(2(\mathcal{O}_1) + 2(T_1))$ which is invariant by translation by T_1 is of the form $x_2 \circ f$ for some $x_2 \in \Gamma(2(\mathcal{O}_2))$, by the universal property of the quotient.

In particular, since $x_1 \in \Gamma(2(\mathcal{O}_1))$, the trace $u = x_1(\cdot) + x_1(\cdot + T_1)$ is in $\Gamma(2(\mathcal{O}_1) + 2(T_1))$ and is certainly invariant by translation, so is of the form $x_2 \circ f$.

This is exactly like the first step of Vélu's formulas (where Vélu takes traces under the kernel of the isogeny of the coordinates x and y respectively, because he works with sections of $3(\mathcal{O}_1)$). In the second step of Vélu's formulas, Vélu then uses the formal group of E_1 to recover equations for E_2.

In our case, we only need to recover a model of the Kummer line $E_2/\pm 1$; by Section 2.2 it is completely determined by the image by u of the four ramifications points of the Kummer line $E_1/\pm 1$. Since we are working with Weierstrass coordinates in our example, one of these ramification points is at infinity and is sent to infinity.

In the rest of this article, rather than working with the affine coordinates x_1, x_2, we will work directly with the projective coordinates X_1, Z_1, X_2, Z_2 (in other words, their numerators and denominators).

3 A general framework for 2-isogenies on a Kummer line

In this section, we will redo Section 2.3 but with projective coordinates directly. Although conceptually more abstract (we need to introduce Mumford's theory of the theta group), the same techniques apply to higher dimensional abelian varieties, by contrast to Vélu's method, as explained in Remark 2 below.

3.1 Theta group and isogenies

We reuse the notations of Section 2.3. We have the two projective coordinates X_1, Z_1 associated to the divisor $2(\mathcal{O}_{E_1})$, which is a shortcut to say they are sections of the line bundle $\mathfrak{O}_{E_1}(2(\mathcal{O}_{E_1}))$. Then X_1^2, X_1Z_1, Z_1^2 are sections of $4(\mathcal{O}_{E_1})$, and we would like to find, like in Section 2.3, a basis of linear combinations $aX_1^2 + bX_1Z_1 + cZ_1^2$ which descends to projective coordinates X_2, Z_2 on E_2, associated to the divisor $2(\mathcal{O}_{E_2})$.

Remark 1 (Even coordinates). Let $D_n = n(\mathcal{O}_{E_1})$. The multiplication map $\Gamma(D_n) \otimes \Gamma(D_m) \to \Gamma(D_{n+m})$ is surjective when $n, m \geq 2, n+m \geq 5$, but $\Gamma(D_2) \otimes \Gamma(D_2) \to \Gamma(D_4)$ only surjects onto even global sections: all global sections of D_2 are even, so their products have to be even.

In particular, since $\Gamma(4(\mathcal{O}_{E_1}))$ is of dimension 4, there is a fourth linearly independent projective coordinate, which is generated by an odd coordinate, because the space of even coordinates is of dimension 3.

On the other hand, the sections s we want to construct on E_2 are sections of $2(\mathcal{O}_{E_2})$, so are even, and their pullbacks f^*s are even. Hence, it is enough to look at the even sections $\Gamma^+(D_4) = \langle X_1^2, X_1Z_1, Z_1^2 \rangle$.

A first difficulty that arises is that, although $D_4 = 4(\mathcal{O}_{E_1})$ is very convenient to use to get a nice basis of the even sections subspace, it is not invariant by translation by T_1, so it does not descend to a divisor on E_2.

We first need to find a divisor D_4'' linearly equivalent to D_4 which is invariant by translation by T_1. Then sections of D_4'' invariant by translation descends to coordinates on E_2; we then need to express this translation invariance for the sections of D_4'' in terms of the sections of D_4.

Mumford's theory of the theta group answers these questions, in the general case of an abelian variety. For simplicity, we only describe the case of a divisor D on an elliptic curve E here.

Let D be a divisor. The divisor D induces the polarization $\Phi_D : E \to \hat{E}$, which is the map defined by $P \mapsto t_{-P}^* D - D \in \hat{E} = \mathrm{Pic}^0(E)$, where t_{-P}^* is the pullback of the translation by $-P$. We stress that $\Phi_D(P)$ is in $\mathrm{Pic}^0(E)$, which means that we consider the divisor $t_{-P}^* D - D$ up to linear equivalence. (The correct polarization should be the map $-\Phi_D$, but to match with the usual sign conventions on elliptic curves, we will use Φ_D in this article.) We say that two divisors D_1, D_2 are algebraically equivalent if the associated polarizations are the same: $\Phi_{D_1} = \Phi_{D_2}$. On an elliptic curve, this is equivalent to $\deg D_1 = \deg D_2$. In particular, if $\deg D = n$, to study Φ_D we may take $D = D_n$, and $\Phi_D(P) = n(P) - n(\mathcal{O}_E)$. The kernel of Φ_D is $E[n]$, since a divisor $n(P) - n(\mathcal{O}_E)$ is linearly equivalent to zero if and only if $n \cdot P = \mathcal{O}_E$.

The theta group $G(D)$ associated to the divisor D is the group of functions g_P on $k(E)$ such that $P \in E[n] = \ker(\Phi_D)$, and $\operatorname{div} g_P = t_{-P}^* D - D$. The addition law of $G(D)$ is given by $(g_P \cdot g_Q)(R) = g_P(R) g_Q(R-P)$, it is a function with divisor $t_{-P-Q}^* D - D$. We have a canonical faithful action of $G(D)$ on $\Gamma(D)$ given by $(g_P \cdot s)(R) = g_P(R) s(R-P)$.

If $D = D_n$, then since D_n is symmetric (which means that $[-1]^* D_n = D_n$), we also have an involution δ_{-1} on $G(D_n)$ given by, for $g_P \in G(D_n)$ with divisor $t_{-P}^* D_n - D_n = n(P) - n(\mathcal{O}_E)$, $(\delta_{-1} g_P)(R) = g_P(-R)$; this is a function with divisor $n(-P) - n(\mathcal{O}_E)$. A function g_P is said to be symmetric if $\delta_{-1} g_P = g_P^{-1}$.

Theorem 1 (Mumford)**.** *Let D be a symmetric divisor on E, $n = \deg D$ (with n prime to the characteristic of k), $K \subset E[n](\overline{k})$ a finite subgroup, and $E' = E/K$ the image of the isogeny f with kernel K. There is a bijection between descents of the divisor D to a divisor D' on $E' = E/K$ (meaning that $f^*D' \simeq D$) and lifts $\widetilde{K}$ of $K \subset \ker \Phi_D$ to the theta group $G(D)$. Furthermore, D' is symmetric if and only if $\widetilde{K}$ consists of symmetric elements. Finally, there is a canonical isomorphism between $\Gamma(D')$ and $\Gamma(D)^{\widetilde{K}}$.*

Proof. Let us give an idea of the proof. A descent of D to a divisor D' on E' is the same as finding a divisor D'' on E, linearly equivalent to D, which is invariant by translation by the points of the kernel: to D' we associate its pullback $D'' = f^*D'$ by the isogeny. Since

$K \subset E[n] = \ker \Phi_D$, by definition for any $P \in K$, we have that $t_{-P}^* D \simeq D$. Assume we have such a D''. Let g be a function with divisor $D'' - D$. Then the function $g(\cdot - P)$ has for divisor $D'' - t_{-P}^* D$ since D'' is invariant, hence $g''_P \coloneqq \frac{g(\cdot)}{g(\cdot - P)}$ is a function with divisor $t_{-P}^* D - D$: $g''_P \in G(D)$. Mumford's theorem says that the functions g''_P, when they are induced by such a function g form a group under the theta group law (that's the easy part).

Conversely, if for each $P \in K$ we pick up a g_P with divisor $t_{-P}^* D - D$, and these g_P form a group in $G(D)$, then they are induced by a function $g \in k(E)$, and $D'' = D + \operatorname{div} g$ is invariant. This is the hard part, which is a corollary of Grothendieck's general flat descent theory.

Let $\widetilde{K}$ be a lift of K in the theta group, and g the function induced by the $g_P \in \widetilde{K}$. If $s'' \in \Gamma(D'')$ is invariant by K, then $s'' = s/g$ is a function in $\Gamma(D)$, and since $g_P = \frac{g(\cdot)}{g(\cdot - P)}$, the action of g_P on s is given by $g_P \cdot s = s(\cdot - P) g_P = s''(\cdot - P)/g(\cdot) = s$ because s'' is invariant, so s is invariant by $\widetilde{K}$ (and conversely). □

We apply this theory to 2-isogenies, and let $K = \{\mathcal{O}_1, T_1\}$ be a kernel generated by a 2-torsion point $T_1 \in E_1[2](k)$.

First we look at the possible descents of D_2 to E_2, this amounts to finding an element $g_{T_1} \in G(D_2)$ above T_1 of order 2. Since T_1 is of 2-torsion, the divisor of $\delta_{-1} g_{T_1}$ is $2(-T_1) - 2(\mathcal{O}_1) = 2(T_1) - 2(\mathcal{O}_1)$, and we even have $\delta^{-1} g_{T_1} = g_{T_1}$ by [Mum66, Prop. 2 p.307 and Prop. 3 p.309]. So g_{T_1} is symmetric if and only if g_{T_1} is of order 2, and we see that a lift $\widetilde{K}$ of K to $G(D_2)$ corresponds to a symmetric lift g_{T_1} above T_1, and the possible descents of D_2 have to be symmetric.

Take an arbitrary lift $g_{T_1} \in G(D_2)$, then since $2 \cdot T_1 = \mathcal{O}_1$, we have $g_{T_1}^2 = \lambda_{T_1}$ for some $\lambda_{T_1} \in k^*$. The symmetric elements above T_1 are then $\pm \frac{g_{T_1}}{\sqrt{\lambda_{T_1}}}$, which live possibly over a degree-2 extension of k. Since taking another lift g_{T_1} changes λ_{T_1} by a square, we see that λ_{T_1} is well-defined in $k^*/k^{*,2}$. It is not hard to show that it is given by the non-reduced self Tate pairing $e_{T,2}(T_1, T_1)$: g_{T_1} is a function with divisor $2(T_1) - 2(\mathcal{O}_1)$, and $g_{T_1}(R) g_{T_1}(R - P) = \lambda_{T_1}$ by definition of the group law. So the class of $\lambda_{T_1} \in k^*/k^{*,2}$ is given by $g_{T_1}(R+P)/g_{T_1}(R)$, which is the self Tate pairing.

Definition 2. The element $[\lambda_{T_1}] \in k^*/k^{*,2}$ defined above is the type of T_1. We say that T_1 is of Montgomery type if λ_{T_1} is already a square over k.

From the discussion above, by Mumford's theorem, D_2 descends over k to a symmetric divisor on E_2 if and only if λ_{T_1} is a square in k, if and only if T_1 is of Montgomery type.

We can check this directly. First we remark that $D'' = f^* \mathcal{O}_2 = (T_1) + (\mathcal{O}_1)$ is not linearly equivalent to D_2, so D_2 cannot directly descend to $(\mathcal{O}_2)$. The other symmetric degree-1 divisors on E_2 are given by (T_2), (R_2), (S_2) where T_2, R_2, S_2 are the three Weierstrass points on E_2. Set R_1 and S_1 to be the other Weierstrass points of E_1 in addition to T_1, we may assume that $f(R_1) = f(S_1) = T_2$. We let T_1' be a 4-torsion point above T_1, and $T_1'' = T_1' + R_1$. We may assume that $f(T_1') = R_2$ and $f(T_1'') = S_2$. So $f^* T_2 = (R_1) + (S_1)$, $f^* R_2 = (T_1') + (T_1' + T_1)$, $f^* S_2 = (T_1'') + (T_1'' + T_1)$. Only the last two are linearly equivalent to D_2, they give the two possible symmetric descents of D_2 to E_2.

We remark that these divisors are rational if and only if $\{T_1', T_1' + T_1 = -T_1'\}$ is invariant, if and only if the cyclic degree-4 subgroup generated by T_1' is rational, if and only if $e_{T,2}(T_1, T_1)$ is a square. This explains why in general a symmetric lift g_{T_1} only lives in a degree two extension, and explains the terminology of Montgomery type: T_1 is of Montgomery type if and only if T_1 can be sent to the point $(0, 0)$ on a Montgomery model. In particular, there can be an asymmetry: D_2 may descend to a symmetric divisor on E_2 via f, while $2(\mathcal{O}_2)$ may not descend to a symmetric divisor on E_1 via the dual isogeny $\widetilde{f}$.

The situation becomes much simpler when looking at the possible descents of $D_4 = 4(\mathcal{O}_1)$ to a degree-2 divisor on E_2, which is all we need to construct a Kummer model for E_2. The tensor product gives a morphism $G(D_2) \otimes G(D_2) \to G(D_4)$, and if $\widetilde{g}_{T_1} = \pm \frac{g_{T_1}}{\sqrt{\lambda_{T_1}}}$, its tensor squared $\widetilde{g}_{T_1}^{\otimes 2} = \frac{g_{T_1}^{\otimes 2}}{\lambda_{T_1}}$ is symmetric in $G(D_4)$ and always rational. An important remark is that while the symmetric divisor $\pm\widetilde{g}_{T_1}$ above T_1 in $G(D_2)$ is only defined up to a sign, there is a canonical symmetric divisor in $G(D_4)$ given by $\widetilde{g}_{T_1}^{\otimes 2}$, which does not depend on this sign.

Since $2(R_2) \simeq 2(S_2) \simeq 2(\mathcal{O}_2)$, this canonical symmetric element encodes the descent of $D_4 = 4(\mathcal{O}_1)$ to $D_2' = 2(\mathcal{O}_2)$, we remark that $f^*(2(\mathcal{O}_2)) = 2(T_1) + 2(\mathcal{O}_1) \simeq 4(\mathcal{O}_1)$. The other symmetric descent of D_4 is induced by $-\widetilde{g}_{T_1}^{\otimes 2}$, which gives the descent of D_4 to $(T_2) + (\mathcal{O}_2)$.

By Theorem 1, we get that the global sections $\Gamma(D_2')$ are precisely the global sections in $\Gamma(D_4)$ invariant under the action by $\widetilde{g}_{T_1}^{\otimes 2}$.

We can now sketch our algorithm to compute 2-isogenies between Kummer lines:

1. Compute the action of the symmetric element $\widetilde{g}_{T_1}^{\otimes 2}$ on X^2, XZ, Z^2
2. Find a basis X', Z' of invariant functions
3. Recover the Kummer model of E' embedded by X', Z'.

We detail these steps in the next sections.

Remark 2 (Vélu's formula). By Section 2.3, we certainly do not need Theorem 1 to find a divisor linearly equivalent to D_4 and invariant by T_1: simply take $D_4'' = 2(\mathcal{O}_{E_1}) + 2(T_1)$.

The link with Vélu's formula and the theta group is as follows: since D_4'' is invariant by translation by T_1, the constant function 1 provides a canonical symmetric element $\widetilde{h''_{T_1}}$ above T_1 in $G(D_4'')$, which corresponds to the canonical descent of D_4'' to $2(\mathcal{O}_2)$. Sections of D_4'' invariant by T_1 thus corresponds by Theorem 1 to sections of $2(\mathcal{O}_2)$ on E_2.

We will see below in Main Example 3 that as expected, on E_2 these sections are exactly the same as the ones we obtain through sections of D_4 invariant by $\widetilde{h_{T_1}} = \widetilde{g_{T_1}}^{\otimes 2}$. In fact, if g is any function with divisor $D_4'' - D_4 = 2(T_1) - 2(\mathcal{O}_1)$, then one can check that the function $h_{T_1} = g(\cdot)/g(\cdot - T_1)$ defined in the proof of Theorem 1 is precisely $\widetilde{g_{T_1}}^{\otimes 2}$.

So Vélu's formula can be seen as a special case of the more general framework of descending sections and divisors through theta groups actions. The reason we work directly with theta groups is that it provides a more flexible framework to study isogenies. In particular, it is slightly more convenient to work with the divisor $D_2 = 2(\mathcal{O}_1)$ than with $(\mathcal{O}_1) + (T_1)$.

More importantly, in higher dimensions, we don't have analogues of Vélu's formula for an ℓ-isogeny. Namely, if we start with an ample divisor Θ of degree 1 associated to a principal polarization, then the traces of Θ under the points of K, a maximal isotropic subgroup of $A[\ell]$ will be an invariant divisor of degree ℓ^{g^2}, hence descends to a divisor on $B = A/K$ of degree $\ell^{g(g-1)}$, so is associated to a principal polarization if and only if $g = 1$. So taking traces of principal polarization does not work to build invariant divisors of the correct degree on A, and we need the full power of the theta group framework as developed by Mumford.

In this paper, we study 2-isogenies between Kummer lines, from which we can deduce doubling formulas (by composing with the dual isogeny). In a sequel to this paper we will extend this to differential addition formulas. This amounts to studying the dimension 2 isogeny given by $E \times E \to E \times E, (P, Q) \mapsto (P + Q, P - Q)$. The action of the theta group $G(D_2)$ on the global sections (X, Z) that we study in this paper will be crucial to extend the doubling formulas to differential additions.

3.2 Computing 2-isogenies

We reuse the notations from Section 2.2, we want to compute a 2-isogeny generated by a 2-torsion point T. We will describe in this section how to build degree 2 maps which are invariant under a translation by T on Kummer lines, and how to recover 2-isogenies from that.

Remark 3. The automorphism $\tau_T : P \mapsto P + T$ on the elliptic curve can be pushed to $\mathbb{P}^1$ via π because T is of 2-torsion. It is an involutive map, therefore it is an automorphism of $\mathbb{P}^1$, i.e. it is a homography.

First, consider the matrix $[M_T] \in \mathrm{PGL}_2(k)$ associated to the homography τ_T.

Main Example 2. In Main Example 1, with $T = (0 : 1)$, the homography τ_T is given by $\tau_T(\mathcal{O}) = T$, $\tau_T(T) = \mathcal{O}$ and $\tau_T(R) = S$. If $\tau_T(X : Z) = (aX + bZ : cX + dZ)$, we then have:

- $\tau_T(1 : 0) = (a : c) = (0 : 1)$, i.e. $a = 0$.
- $\tau_T(0 : 1) = (b : d) = (1 : 0)$, i.e. $d = 0$.
- $\tau_T(\alpha : 1) = (b : c\alpha) = (\gamma : \alpha)$, i.e. $b = c\gamma$.

So $\tau_T(X : Z) = (bZ : cX) = (\gamma Z : X)$ and the associated matrix in $\mathrm{PGL}_2(k)$ is:

$$[M_T] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = \left[\begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}\right].$$

Lift this matrix to $M_T \in \mathrm{GL}_2(k)$, by definition, since T is a 2-torsion point, $[M_T^2] = [I_2]$, so $M_T^2 = \lambda_T I_2$. This lift is associated to an explicit element g_T in the theta group $G(D_2)$. Indeed, we have a projective action of $E[2]$ on $\Gamma(D_2) \simeq k^2$ given by translation by a 2-torsion point on projective coordinates. The canonical action defined in Section 3.1 lifts this to an affine group action of $G(D_2)$ on $\Gamma(D_2)$. Since this group action is faithful, we can represent an element $g \in G(D_2)$ by the corresponding action matrix. In particular, the element λ_T associated to M_T is the same as the one we associated to g_T in Section 3.1. As mentioned there, because of the lift, λ_T is well-defined up to a square. In particular:

Lemma 1. *$[\lambda_T] \in k^*/k^{*,2}$ is the type of T, as defined in Definition 2.*

λ_T depends on the chosen lift M_T, however $\frac{1}{\sqrt{\lambda_T}} M_T$ does not (up to a sign). This is the invariant matrix of interest, corresponding to the action of a symmetric lift $\widetilde{g}_T$ of Section 3.1.

We want to build quadratic forms in (X, Z) invariant by $\frac{1}{\sqrt{\lambda}} M_T$, which will be said to be T-invariants. (Note that $\frac{1}{\sqrt{\lambda}} M_T$ is canonical and does not depend on the sign.) We will look at the action of this matrix on X^2, Z^2 and XZ.

Remark 4. If q is a quadratic form and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the action of M over q is given by:

$$M \cdot q(X, Z) = q(aX + bZ, cX + dZ).$$

Here, $\sqrt{\lambda_T}$ may be in some quadratic extension of k, but we can work around that, if $M_T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$:

$$\left(\frac{1}{\sqrt{\lambda_T}} M_T\right) \cdot q(X, Z) = q\left(\frac{aX + bZ}{\sqrt{\lambda_T}}, \frac{cX + dZ}{\sqrt{\lambda_T}}\right) = \frac{1}{\lambda_T} \left(M_T \cdot q(X, Z)\right).$$

Main Example 3. Following up with Main Example 2, we choose $M_T = \left(\begin{smallmatrix} 0 & \gamma \\ 1 & 0 \end{smallmatrix}\right)$, then $M_T^2 = \gamma I_2$ so the type of T is $[\gamma]$. We then compute the action of M_T on X^2, Z^2 and XZ, and then divide by γ:

$$\frac{1}{\gamma}\left(M_T \cdot X^2\right) = \gamma Z^2; \quad \frac{1}{\gamma}\left(M_T \cdot Z^2\right) = \frac{1}{\gamma} X^2; \quad \frac{1}{\gamma}\left(M_T \cdot XZ\right) = XZ.$$

We notice that XZ is already invariant, to build another one we can consider a trace for the matrix action on quadratic forms, for instance:

$$q_1 = X^2 + \frac{1}{\gamma}\left(M_T \cdot X^2\right) = X^2 + \gamma Z^2, \text{then } \frac{1}{\gamma}\left(M_T \cdot q_1\right) = q_1.$$

It appears that we retrieve the same invariant projective sections using Vélu's formula. By Remark 2, Vélu's formula build the invariant affine section:

$$x'(P) = x(P) + x(P+T) = x(P) + \frac{\gamma}{x(P)} = \frac{X(P)}{Z(P)} + \frac{\gamma Z(P)}{X(P)} = \frac{X^2(P) + \gamma Z^2(P)}{X(P)Z(P)}.$$

The numerator and denominators of this function are precisely the above invariant sections.

Say we have two linearly independent quadratic forms q and q' which are T_1-invariant where T_1 is a 2-torsion point on the Kummer line $\mathcal{K}_1$, and consider a basis $u, v \in \mathrm{Span}(q, q')$. Set $M_{T_1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ the matrix of τ_{T_1} and $[\lambda_{T_1}]$ the type of T_1.

$$\begin{aligned} \tau_{T_1} : \mathcal{K}_1 &\to \mathcal{K}_1 \\ P &\mapsto P + T_1. \end{aligned}$$

Set the following degree 2 map, which is well-defined by the properties of quadratic forms:

$$\begin{aligned} f : \mathcal{K}_1 &\to \mathcal{K}_2 \\ (x : z) &\mapsto (u(x,z) : v(x,z)). \end{aligned}$$

Since u and v are T_1-invariant, we get $f(P + T_1) = f(\tau_{T_1}(P)) = f(P)$. What remains to do is determining the codomain $\mathcal{K}_2$ using the extra 2-torsion points we have.

Main Example 4. We add a 1 in index of notations from Main Example 1. We found earlier in Main Example 3 that $q(X,Z) = X^2 + \gamma Z^2$ and $q'(X,Z) = XZ$ are T_1-invariant. Consider for instance $u = q$ and $v = q'$ (or any linear combination of q and q'), then $f : (X : Z) \mapsto (X^2 + \gamma Z^2 : XZ)$ can be computed in $1\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$. We have by construction of f that $f(\mathcal{O}_1) = f(T_1)$, and since $S_1 = R_1 + T_1$, we also have $f(R_1) = f(S_1)$. A quick computation yields:

$$f(\mathcal{O}_1) = (1 : 1) \text{ and } f(R_1) = (\alpha^2 + \gamma : \alpha) = (\mathcal{A} : 1).$$

We are trying to build an isogeny with kernel T_1, so $f(\mathcal{O}_1)$ is sent to $\mathcal{O}_2$, and $f(R_1)$ is a 2-torsion point on $\mathcal{K}_2$. Note that here $f(R_1)$ is rational even if R_1 may not be, this is a more general fact proven in the following lemma:

Lemma 2. *$f(R_1)$ is rational.*

Proof. Let σ be a Galois element on the field k. If R_1 is invariant by σ, so is S_1 (because $S_1 = R_1 + T_1$) and the image by f is obviously invariant by σ too. However, if R_1 is not invariant by σ, then $\sigma(R_1) \neq R_1$, so we must have $\sigma(R_1) = S_1$ because T_1 is rational. But then, since σ commutes with f:

$$\sigma(f(R_1)) = f(\sigma(R_1)) = f(S_1) = f(R_1).$$

□

To grab the final information of 2-torsion, consider a 4-torsion point T_1' above T_1 which may not be rational. Such a point can be found by solving $T_1' + T_1 = T_1'$ on the Kummer line (remember that $-T_1' = T_1'$ in this situation). If $T_1' = (X : Z)$, using the translation τ_{T_1}, this leads to:

$$(\gamma Z : X) = (X : Z) \text{ i.e. } \frac{X}{Z} = \pm\sqrt{\gamma}.$$

Then $T_1' = (\sqrt{\gamma} : 1)$ and $T_1'' = (-\sqrt{\gamma} : 1)$ are the 4-torsion points above T_1, and $f(T_1')$, $f(T_1'')$ are the remaining 2-torsion points on $\mathcal{K}_2$.

An optional step is to put $\mathcal{K}_2$ in a nice shape by a homography, but this is not mandatory and can gain some operations. We will give more details in the next section.

4 2-isogenies on Montgomery curves

We will focus on Montgomery curves in this section, which corresponds to the case $\gamma = 1$ in Main Example 1. Recall from Definition 2:

Definition 3. A 2-torsion point T is said to be of Montgomery type if its type λ_T is a square. Sending T to $(0, 0)$ and $\mathcal{O}$ to infinity, we thus obtain a Montgomery model $\beta y^2 = x(x^2 + \mathcal{A}_1 x + 1)$.

The Montgomery Kummer line is denoted $\mathcal{K}_1$ over k with constant $\mathcal{A}_1 \in k$. The ramification of our Kummer line is then:

$$\mathcal{O}_1 = (1 : 0)^*, \qquad T_1 = (0 : 1), \qquad R_1 = (A_1 : B_1), \qquad S_1 = (B_1 : A_1) = R_1 + T_1.$$

Thus, $\mathcal{A}_1 = -\frac{(A_1 - B_1)^2}{A_1 B_1}$ and:

$$d_1 = \frac{\mathcal{A}_1 + 2}{4} = \frac{-(A_1 - B_1)^2}{4A_1B_1} = \frac{(A_1 - B_1)^2}{(A_1 - B_1)^2 - (A_1 + B_1)^2}. \tag{3}$$

The constant d_1 is the important one instead of $\mathcal{A}_1$ because it is also sufficient to recover the elliptic curve up to a twist, but it is more importantly used in doubling formulas on Montgomery curves, see Algorithm 5. When the codomain of an isogeny is a Montgomery curve, we want to compute d_1 efficiently to get all the necessary information about the codomain.

We computed in Main Example 3 the type of T_1 which is 1 up to a square (T_1 is then of Montgomery type), and two T_1-invariant quadratic forms:

$$q_1(X, Z) = X^2 + Z^2, \qquad q_2(X, Z) = XZ.$$

We also have the translation by T_1 denoted $\tau_{T_1} : \mathcal{K}_1 \to \mathcal{K}_1$ computed in Main Example 2:

$$\tau_{T_1} : (X : Z) \mapsto (Z : X). \tag{4}$$

We will need the translation by R_1 later too, which is given by:

$$\tau_{R_1} : (X : Z) \mapsto (A_1 X - B_1 Z : B_1 X - A_1 Z). \tag{5}$$

Remark 5. When the curve E is fixed (as for scalar multiplication), we will count multiplication by d or $(A_1 : B_1)$ as one $\mathbf{m}_0$, since we can assume that $B_1 = 1$. For the computation of a 2^n-isogeny chain, they will be given as quotients, in which case we will count them as two multiplications, either small or generic depending on the context. See Section 5 and Appendix C.

Remark 6. The ramification of the Montgomery Kummer line is invariant under the involution $(X : Z) \mapsto (Z : X)$, corresponding to translation by T_1. If we apply the Hadamard transform $H(X : Z) = (X + Z : X - Z) = (X' : Z')$, we obtain a new model $H\mathcal{K}_1$ where the ramification becomes

$$(1 : 1), \qquad (-1 : 1), \qquad (A_1 + B_1 : A_1 - B_1), \qquad (A_1 + B_1 : B_1 - A_1),$$

which is invariant by the involution $(X' : Z') \mapsto (-X' : Z')$.

The quadratic forms invariant by the canonical affine lift of this involution are $q'_1 = {X'}^2$ and $q'_2 = {Z'}^2$. On $\mathcal{K}_1$, these quadratic forms correspond to $(X + Z)^2$ and $(X - Z)^2$, which indeed span the same vector spaces as q_1, q_2 above.

4.1 Isogeny with kernel T_1

Assume in this section that $\frac{A_1}{B_1} \in k$, so we have the full 2-torsion on our curve. Recall we have these independent 4-torsion points above T_1:

$$T'_1 = (1 : 1), \qquad T''_1 = (-1 : 1) = T'_1 + R_1.$$

We will use the following invariant quadratic forms from Remark 6, using the notations of Main Example 3:

$$u(X, Z) = (X + Z)^2 = q_1(X, Z) + 2q_2(X, Z), \; v(X, Z) = (X - Z)^2 = q_1(X, Z) - 2q_2(X, Z).$$

Set $f_0 : (X : Z) \mapsto ((X + Z)^2 : (X - Z)^2)$. By construction, $f_0(P + T_1) = f_0(P)$. Set $A_2 = A_1 + B_1$ and $B_2 = A_1 - B_1$, the image of the ramification is the following:

$$f_0(\mathcal{O}_1) = (1 : 1)^* = f_0(T_1), \qquad f_0(R_1) = (A_2^2 : B_2^2) = f_0(S_1),$$
$$f_0(T'_1) = (1 : 0), \qquad f_0(T''_1) = (0 : 1).$$

To get a Montgomery shaped ramification, we will multiply by $C : (X : Z) \mapsto (B_2 X : A_2 Z)$, set $f = C \circ f_0$, then:

$$\mathcal{O}_2 = f(T'_1) = (1 : 0), \qquad T_2 = f(T''_1) = (0 : 1),$$
$$R_2 = f(R_1) = (A_2 : B_2), \qquad S_2 = f(\mathcal{O}_1) = (B_2 : A_2)^*.$$

Up to a translation by S_2 we recover the 2-isogeny with kernel T_1 and the image is Montgomery shaped.

Theorem 2 (Translated 2-isogeny with kernel T_1)**.** *Let $g : \mathcal{K}_1 \to \mathcal{K}_2$ be the 2-isogeny with kernel T_1 on the Montgomery Kummer line $\mathcal{K}_1$ with extra 2-torsion $(A_1 : B_1)$, and assume $\frac{A_1}{B_1} \in k$. Set $(A_2 : B_2) = (A_1 + B_1 : A_1 - B_1)$, then $g = f + S_2$ where:*

$$f : (X : Z) \mapsto \left(B_2(X + Z)^2 : A_2(X - Z)^2\right).$$

f can be computed in $2\mathbf{S} + 1\mathbf{m}_0 + 2\mathbf{a}$, the codomain $\mathcal{K}_2$ is a Montgomery Kummer line and the curve constant d_2 can be computed in $2\mathbf{S} + 1\mathbf{a}$ with:

$$d_2 = \frac{B_1^2}{B_1^2 - A_1^2}.$$

Proof. The fact that g is the 2-isogeny with kernel T_1 and that the image is a Montgomery Kummer line is straight-forward from the reasoning above. The curve constant d_2 comes from the computation in Eq. (3) and that $(A_2 : B_2) = (A_1 + B_1 : A_1 - B_1)$:

$$d_2 = \frac{(A_2 - B_2)^2}{(A_2 - B_2)^2 - (A_2 + B_2)^2} = \frac{B_1^2}{B_1^2 - A_1^2}.$$

□

Proposition 1 (Translated dual isogeny)**.** *Using notation of Theorem 2, the dual isogeny of g is given by $\hat{g} = \hat{f} + S_1$ where:*

$$\hat{f} : (X : Z) \mapsto \left(B_1(X+Z)^2 : A_1(X-Z)^2\right).$$

Then $\hat{f} \circ f(P) = 2 \cdot P + R_1$ where $P \in \mathcal{K}_1$ can be computed in $4\mathbf{S} + 2\mathbf{m}_0 + 4\mathbf{a}$ as in Algorithm 1.

Proof. Because the Hadamard transform is an involution, the codomain of $\hat{f}$ is $\mathcal{K}_1$. We can then set $g_0 = \hat{f} + S_1$, which is the 2-isogeny with kernel T_2 thanks to Theorem 2. Let's check that $g_0 \circ g = [2]$, the multiplication by 2, on the Kummer line. We will use the following formula:

$$\begin{aligned} g_0(g(P)) &= g_0(f(P) + S_2) \\ &= g_0(f(P)) + g_0(S_2) \\ &= \hat{f}(f(P)) + \hat{f}(S_2) + 2 \cdot S_1 \\ g_0(g(P)) + R_1 &= \hat{f}(f(P)). \end{aligned}$$

We then study $g_0 \circ g$ on the 2-torsion:

$$\begin{aligned} g_0(g(\mathcal{O}_1)) &= \mathcal{O}_1, & g_0(g(T_1)) &= \hat{f}(S_2) + R_1 = 2 \cdot R_1 = \mathcal{O}_1, \\ g_0(g(R_1)) &= \hat{f}(R_2) + R_1 = \mathcal{O}_1, & g_0(g(S_1)) &= \hat{f}(R_2) + R_1 = \mathcal{O}_1. \end{aligned}$$

$g_0 \circ g \neq [0]$ (for instance, $g_0(g(T_1')) = T_1$), so we must have $g_0 \circ g = [2]$. Similarly, we prove $g \circ g_0 = [2]$. By uniqueness, $g_0 = \hat{g}$. The first formula then yields $\hat{f}(f(P)) = 2 \cdot P + R_1$. ☐

Algorithm 1: Doubling in Montgomery coordinates up to a 2-torsion point

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P + R_1] = (X : Z)$
Data: On $\mathcal{K}_1$ with extra 2-torsion $[R_1] = (A_1 : B_1)$,
$(A_2 : B_2) = (A_1 + B_1 : A_1 - B_1)$

Function `DoublingTranslation`$([P])$**:**
- $u \leftarrow (X_1 + Z_1)^2$;
- $v \leftarrow \frac{A_2}{B_2}(X_1 - Z_1)^2$;
- $X \leftarrow (u + v)^2$;
- $Z \leftarrow \frac{A_1}{B_1}(u - v)^2$;
- **return** $(X : Z)$;

We will be using the translated doubling of Proposition 1 in Section 5 to build a "hybrid ladder".

Remark 7. In ECC, if one always works on the same curve, it is possible to control the associated constants and make them small. That way, a multiplication by a curve constant costs way less than a multiplication by a generic number. The hybrid ladder will rely on this fact a lot. Because the translated point is S_2 and not T_2 in Theorem 2, it is not convenient to use these formulas to chain isogenies.

Remark 8. The translated doubling formula of Algorithm 1 uses exactly the same formula as the standard doubling formula in squared theta coordinates [1]. This is not a coincidence,

[1] `https//hyperelliptic.org/EFD/g1p/auto-edwards-yzsquared.html`

as remarked in [HR19], the Montgomery Kummer line and the squared theta Kummer line differ by translation by a 2-torsion point (one way to directly recover this result, using Section 2, is to look at the associated ramification points), so using the squared theta doubling formula in Montgomery coordinates gives a translated doubling. We will come back to this in an upcoming article where we explore the Galois properties of various models of Kummer lines in more details.

4.2 Isogeny with kernel R_1

Assume once again that $\frac{A_1}{B_1} \in k$, so we have full 2-torsion on our curve. Recall that we have the following ramification on our Kummer line:

$$\mathcal{O}_1 = (1:0)^*, \qquad T_1 = (0:1), \qquad R_1 = (A_1 : B_1), \qquad S_1 = (B_1 : A_1) = R_1 + T_1.$$

In this section, we further assume that there is a 4-torsion point $R_1' = (a_1' : b_1')$ above R_1. Another independent 4-torsion point above R_1 is then $R_1'' = R_1' + T_1$ which can be computed easily as $R_1'' = (b_1' : a_1')$ thanks to Eq. (4). Finally, set $(a_1 : b_1) = (a_1' + b_1' : a_1' - b_1')$. A useful relation that we will be using is the following:

$$(A_1 : B_1) = (a_1^2 + b_1^2 : a_1^2 - b_1^2) \iff (A_1 + B_1 : A_1 - B_1) = (a_1^2 : b_1^2).$$

This comes for instance from the doubling formulas in Proposition 1, because $2 \cdot R_1' + R_1 = \mathcal{O}_1$:

$$(A_1 - B_1)a_1^2 - (A_1 + B_1)b_1^2 = 0 \iff (A_1 + B_1 : A_1 - B_1) = (a_1^2 : b_1^2).$$

We will now apply the algorithm to find invariant maps by R_1. A matrix associated to τ_{R_1} is:

$$M_{R_1} = \begin{pmatrix} A_1 & -B_1 \\ B_1 & -A_1 \end{pmatrix}.$$

Since $M_{R_1}^2 = (A_1^2 - B_1^2)I_2$, the type is $\lambda_{R_1} = A_1^2 - B_1^2 = 4a_1^2b_1^2$. This is a square, so R_1 is of Montgomery type.

Set $M = \frac{M_{R_1}}{\sqrt{\lambda_{R_1}}}$, we will be looking at the action of M on the following basis of quadratic forms: $(X+Z)^2$, $(X-Z)^2$ and $(X-Z)(X+Z)$:

$$M \cdot (X+Z)^2 = \frac{a_1^2}{b_1^2}(X-Z)^2 \qquad M \cdot (X-Z)^2 = \frac{b_1^2}{a_1^2}(X+Z)^2.$$

$$M \cdot (X-Z)(X+Z) = (X-Z)(X+Z).$$

The invariant quadratic forms we will be using are then:

$$q_1(X,Z) = b_1^2(X+Z)^2 + a_1^2(X-Z)^2, \qquad q_2(X,Z) = a_1b_1(X+Z)(X-Z). \tag{6}$$

By doing linear combination of q_1 and q_2, we end up with the following formulas:

Theorem 3 (Translated 2-isogeny with kernel R_1)**.** *Let $g : \mathcal{K}_1 \to \mathcal{K}_2$ be the 2-isogeny with kernel R_1 on the Montgomery Kummer line $\mathcal{K}_1$ with extra 2-torsion $R_1 = (A_1 : B_1)$. Assume there is a 4-torsion point $R_1' = (a_1' : b_1')$ above R_1. Set $(a_1 : b_1) = (a_1' + b_1' : a_1' - b_1')$, we have the relation $(A_1 : B_1) = (a_1^2 + b_1^2 : a_1^2 - b_1^2)$. Finally, set f to be the following map:*

$$f : (X : Z) \mapsto \left((b_1(X+Z) + a_1(X-Z))^2 : (b_1(X+Z) - a_1(X-Z))^2 \right).$$

Then the ramification on the image of f is:

$$\mathcal{O}_2 = (1:0), \qquad T_2 = (0:1), \qquad R_2 = (a_1'^2 : b_1'^2)^*, \qquad S_2 = (a_1'^2 : b_1'^2) = R_2 + T_2.$$

We have $g = f + R_2$, f can be computed in $2\mathbf{S} + 1\mathbf{m}_0 + 4\mathbf{a}$, the codomain $\mathcal{K}_2$ is a Montgomery Kummer line and the curve constant d_2 can be computed in $2\mathbf{S} + 1\mathbf{a}$ with:

$$d_2 = \frac{B_1^2 - A_1^2}{B_1^2}.$$

Proof. We have $f(X : Z) = (q_1(X, Z) + 2q_2(X, Z) : q_1(X, Z) - 2q_2(X, Z))$ where q_1 and q_2 are defined in Eq. (6) and are R_1-invariant. So $f(\cdot + R_1) = f$. It is straight-forward to compute:

$$\begin{aligned} f(\mathcal{O}_1) &= (a_1'^2 : b_1'^2)^* = f(R_1), & f(T_1) &= (b_1'^2 : a_1'^2) = f(S_1), \\ f(R_1') &= (1 : 0), & f(R_1'') &= (0 : 1). \end{aligned}$$

So the image is a Montgomery Kummer line and $g = f + R_2$ with notations from the theorem.

The codomain is given by d_2 using Eq. (3):

$$d_2 = \frac{(a_1'^2 - b_1'^2)^2}{(a_1'^2 - b_1'^2)^2 - (a_1'^2 + b_1'^2)^2} \tag{7}$$

Thanks to $(A_1 : B_1) = (a_1^2 + b_1^2 : a_1^2 - b_1^2)$, we can simplify the expression of d_2:

$$\left((a_1'^2 - b_1'^2)^2 : (a_1'^2 + b_1'^2)^2\right) = \left(4a_1^2 b_1^2 : (a_1^2 + b_1^2)^2\right) = (A_1^2 - B_1^2 : A_1^2).$$

□

If we compute $g = f + R_2$ using the translation τ_{R_2} given in Eq. (4), we find back the formulas for 2-isogenies given by Renes in [Ren18, Prop. 2]. We can also recover alternative shifted doubling formulas instead of Algorithm 1, which only differ by the number of additions.

Remark 9. Unlike in Theorem 2, we have a translated isogeny by R_2, and the kernel was initially R_1. We can therefore chain such isogenies to compute 2^n-isogenies, more details are given in Appendix C.

Since the computations only involves the 4-torsion point R_1' above R_1, one could keep track only of the 4-torsion points. The codomain would then be given by Eq. (7), which costs $4\mathbf{S} + 3\mathbf{a}$.

Proposition 2 (Dual isogeny)**.** *Using notation of Theorem 3, the dual isogeny of g is given by $\hat{g}$ where:*

$$\hat{g} : (X : Z) \mapsto \left(B_1(X + Z)^2 : 4A_1 XZ\right).$$

Then $\hat{g} \circ f(P) = 2 \cdot P + R_1$ where $P \in \mathcal{K}_1$ can be computed in $4\mathbf{S} + 2\mathbf{m}_0 + 7\mathbf{a}$ as in Algorithm 2 (using $4XZ = (X + Z)^2 - (X - Z)^2$).

Proof. We know that the kernel of $\hat{g}$ is $g(\mathcal{K}_1[2]) = \langle g(T_1) \rangle = \langle T_2 \rangle$. We also have computed two T_2-invariant quadratic forms earlier, set $g_0(X : Z) = ((X + Z)^2 : XZ)$. Then $g_0(\cdot + T_2) = g_0$. The output ramification is:

$$\begin{aligned} g_0(\mathcal{O}_2) &= (1 : 0)^* = g_0(T_2), & g_0(R_2) &= \left((a_1'^2 + b_1'^2)^2 : a_1'^2 b_1'^2\right) = g_0(S_2), \\ g_0(T_2') &= (4 : 1), & g_0(T_2'') &= (0 : 1). \end{aligned}$$

Thanks to computations already done while proving Theorem 3, we have $g_0(R_2) = (4A_1^2 : B_1^2)$.

We then consider a homography $h : (X : Z) \mapsto (aX + bZ : cX + dZ)$, we want:

- $h(1:0) = (1:0)$, then $c = 0$.
- $h(0:1) = (0:1)$, then $b = 0$.
- $h(4:1) = (B_1 : A_1)$, which sets $(4a : d) = (B_1 : A_1)$.

Then, $h(4A_1^2 : B_1^2) = (4aA_1^2 : dB_1^2) = (A_1 : B_1)$. Finally, the map $h \circ g_0$ is the 2-isogeny with kernel T_2 and codomain $\mathcal{K}_1$, hence $\hat{g} = h \circ g_0$.

Since, $\hat{g}(g(P)) = 2 \cdot P = \hat{g}(f(P)) + \hat{g}(R_2)$, we get the alternative formula from $\hat{g}(R_2) = R_1$. ☐

Algorithm 2: Alternative doubling in Montgomery coordinates up to a 2-torsion point

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P + R_1] = (X : Z)$
Data: On $\mathcal{K}_1$ with extra 2-torsion $[R_1] = (A_1 : B_1)$ and $[R_1'] = (a_1' : b_1')$ of 4-torsion above $[R_1]$, $(a_1 : b_1) = (a_1' + b_1' : a_1' - b_1')$

Function `DoublingTranslation`($[P]$):
- $u \leftarrow (X_1 + Z_1)$;
- $v \leftarrow \frac{a_1}{b_1}(X_1 - Z_1)$;
- $w \leftarrow (u + v)^2$;
- $t \leftarrow (u - v)^2$;
- $u \leftarrow (w + t)^2$;
- $v \leftarrow (w - t)^2$;
- $X \leftarrow u$;
- $Z \leftarrow \frac{A_1}{B_1}(u - v)$;
- **return** $(X : Z)$;

4.3 Additional 8-torsion: another formula for the isogeny with kernel T_1

In this last section, we assume $\frac{A_1}{B_1} \notin k$, so we don't know about the full 2-torsion, but we add a hypothesis about a 8-torsion point $\widetilde{T_1} = (r : s)$ above $T_1' = (1 : 1)$ (which itself is above $T_1 = (0 : 1)$). That way, we ensure that there will still be a rational 4-torsion point on the Kummer line, so it will be Montgomery shaped.

We set $(\gamma : \delta) = (4rs : (r - s)^2)$, and because $2 \cdot \widetilde{T_1} = T_1' = (1 : 1)$, using Algorithm 5:

$$((\gamma + \delta)\delta : \gamma(\delta + d_1\gamma)) = (1 : 1) \iff d_1 = \frac{\delta^2}{\gamma^2}.$$

But we have another expression for d_1 given in Eq. (3), therefore:

$$(\delta^2 : \gamma^2) = (-(A_1 - B_1)^2 : 4A_1B_1).$$

We are looking for a 2-isogeny with kernel T_1 without the knowledge of $\frac{A_1}{B_1}$. The result will be in a similar shape to the one in Proposition 2. As before, we start by computing invariants by the matrix $M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which we already did in Main Example 3. We will consider:

$$M \cdot (X - Z)^2 = (X - Z)^2, \qquad M \cdot XZ = XZ.$$

If $f_0 : (X : Z) \mapsto ((X-Z)^2 : XZ)$, then $f_0(\cdot + T_1) = f_0$. The codomain ramification is:

$$\begin{aligned} f_0(\mathcal{O}_1) = (1:0)^* = f_0(T_1), \quad & f(R_1) = ((A_1 - B_1)^2 : A_1 B_1) = (-4\delta^2 : \gamma^2) = f(S_1), \\ f(T_1') = (0:1), \quad & \qquad\qquad\qquad\qquad f(T_1'') = (-4:1). \end{aligned}$$

To put it in a convenient shape, we consider a homography $h : (X : Z) \mapsto (aX + bZ : cX + dZ)$. We want $h(1:0) = (1:0)$ and $h(0:1) = (0:1)$, which forces $b = 0$ and $c = 0$. Then, we naturally want to send $f_0(\widetilde{T_1}) = ((r-s)^2 : rs)$ onto $(1:1)$:

$$h((r-s)^2 : rs) = (1:1) \iff (a:d) = (\gamma : 4\delta).$$

That way, we get:

$$h(-4\delta^2 : \gamma^2) = (-4\gamma\delta^2 : 4\delta\gamma^2) = (-\delta : \gamma), \qquad h(-4:1) = (-\gamma : \delta).$$

We then set $f = h \circ f_0$, we recover formulas already known in [FJP14, Eq. (19)]:

Theorem 4 (2-isogeny with kernel T_1)**.** *Let $g : \mathcal{K}_1 \to \mathcal{K}_2$ be the 2-isogeny with kernel T_1 on the Montgomery Kummer line $\mathcal{K}_1$. Assume there is a rational 8-torsion point $\widetilde{T_1} = (r:s)$ above $T_1' = (1:1)$. Set $(\gamma : \delta) = (4rs : (r-s)^2)$, then g is given by:*

$$g : (X : Z) \mapsto \left(\gamma(X-Z)^2 : 4\delta XZ\right).$$

g can be computed in $2\mathbf{S} + 1\mathbf{m}_0 + 3\mathbf{a}$ ($4XZ = (X+Z)^2 - (X-Z)^2$), the codomain $\mathcal{K}_2$ is a Montgomery Kummer line and the curve constant d_2 can be computed in $4\mathbf{S} + 6\mathbf{a}$ with:

$$d_2 = \frac{(\gamma+\delta)^2}{(\gamma+\delta)^2 - (\gamma-\delta)^2}.$$

The computation of d_2 is a direct application of Eq. (3). For completeness, we also provide the dual isogeny formula.

Proposition 3 (Dual isogeny)**.** *Using notation of Theorem 4, the dual isogeny of g is given by $\hat{g}$ where:*

$$\begin{aligned} \hat{g} : (X : Z) &\mapsto (u(X,Z) + 2\delta v(X,Z) : u(X,Z) - 2\delta v(X,Z)), \\ u(X,Z) &= (\gamma+\delta)(X+Z)^2 - (\gamma-\delta)(X-Z)^2, \\ v(X,Z) &= (X+Z)(X-Z). \end{aligned}$$

$\hat{g}$ can be computed in $1\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}_0 + 3\mathbf{a}$.

Proof. We have that $\ker \hat{g} = \langle R_2 \rangle$, we can't apply results from Theorem 3 since we don't know the 4-torsion above R_2. We have already computed the matrix M associated to τ_{R_2} and the type $\lambda = \delta^2 - \gamma^2$:

$$M = \begin{pmatrix} -\delta & -\gamma \\ \gamma & \delta \end{pmatrix}.$$

Furthermore, we have seen that $\frac{1}{\lambda}(M \cdot (X+Z)(X-Z)) = (X+Z)(X-Z)$, so we are looking for one other invariant:

$$\frac{1}{\lambda}\left(M \cdot (X+Z)^2\right) = \frac{(\gamma-\delta)^2}{\delta^2 - \gamma^2}(X-Z)^2 = -\frac{\gamma-\delta}{\gamma+\delta}(X-Z)^2.$$

Hence, the two invariant quadratic forms we will consider are:

$$\begin{aligned}u(X,Z) &= (\gamma+\delta)\left((X+Z)^2 + \frac{1}{\lambda}\left(M\cdot(X+Z)^2\right)\right)\\ &= (\gamma+\delta)(X+Z)^2 - (\gamma-\delta)(X-Z)^2\\ v(X,Z) &= (X+Z)(X-Z).\end{aligned}$$

We then set $g_0(X:Z) = (au(X,Z)+bv(X,Z) : cu(X,Z)+dv(X,Z))$, which by construction verifies $g_0(\cdot + R_2) = g_0$. Since we want it to be the dual of g, we are looking for the following equations:

- $g_0(g(\mathcal{O}_1)) = g_0(\mathcal{O}_2) = \mathcal{O}_1$, which implies $2\delta c + d = 0$.
- $g_0(g(T_1')) = g_0(T_2) = T_1$, which implies $2\delta a - b = 0$.
- $g_0(g(\widetilde{T_1})) = g_0(T_2') = T_1'$, which implies $a = c$.

We factor by a in g_0 and get the following expression:

$$g_0 : (X:Z) \mapsto (u(X,Z) + 2\delta v(X,Z) : u(X,Z) - 2\delta v(X,Z)).$$

We then check that it behaves correctly on the remaining 2-torsion:

- $g_0(g(R_1)) = g_0(R_2) = (4\delta\lambda : 0) = \mathcal{O}_1$.
- $g_0(g(T_1'')) = g_0(S_2) = (0 : 4\delta\lambda) = T_1$.

Finally, $g_0 = \hat{g}$. □

5 Hybrid ladder

Let $\pi : E \to \mathbb{P}^1 \simeq \mathcal{K}$ be a Montgomery Kummer line. Recall that if one knows $\pi(P)$, $\pi(Q)$ and $\pi(P-Q)$, then it is possible to recover $\pi(P+Q)$ using differential addition formulas which are given in Appendix A, Algorithms 4 and 5. Special formulas for doubling are necessary because the general formula do not work when $P = Q$, unlike for the theta model which uses the same formulas for doublings and differential additions. We will also use the notation $[P] = \pi(P)$ in the algorithms.

Using these formulas, one can compute $\pi(n \cdot P)$ on the Kummer line using the Montgomery ladder (Algorithm 6). The key of the ladder is that, at each step, we have $\pi(U-V) = \pi(P)$, where U and V are the two points we keep track of. It is clear that the cost of a scalar multiplication depends linearly on the cost of one differential addition and one doubling. In this paper, we focus on the doubling part. If we look at the computational cost of the doubling in Algorithm 5, we get $2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$, where $\mathbf{m}_0$ is a multiplication by a curve constant.

On the other hand, the computational cost of a doubling up to a 2-torsion point in Proposition 1 and Algorithm 1 is $4\mathbf{S} + 2\mathbf{m}_0$. Depending on the context, a square tends to be faster than a multiplication. For instance, $3\mathbf{S} = 2\mathbf{M}$ in $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ when $p \equiv 3 \bmod 4$. The comparison is given in Table 1.

For parameters where the multiplication by a curve constant is way faster than a generic multiplication, then our translated doubling is faster. This can be achieved for instance by having small constants, i.e. less than a computer word. By adapting the Montgomery ladder to take into account the additional 2-torsion point, we can build a new hybrid ladder in Algorithm 3. The major change is that, instead of having $\pi(U-V) = \pi(P)$, we allow $\pi(U-V) \in \{\pi(P), \pi(P+R_1)\}$. The correctness of our scalar multiplication is

Table 1: Comparison of doubling formulas computational cost

	Doubling	Doubling up to a 2-torsion point
Detailed cost	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{S} + 2\mathbf{m}_0$
$3\mathbf{S} = 2\mathbf{M}$, $\mathbf{m}_0 = \mathbf{M}$	$\approx 4.33\mathbf{M}$	$\approx 4.67\mathbf{M}$
$3\mathbf{S} = 2\mathbf{M}$, $5\mathbf{m}_0 = \mathbf{M}$	$\approx 3.53\mathbf{M}$	$\approx 3.07\mathbf{M}$

Algorithm 3: Scalar multiplication with hybrid ladder

Input: $n = (1, b_{\ell-2}, \ldots, b_0)$ an ℓ-bits integer, $[P]$ a point on $\mathcal{K}_1$
Output: $[n \cdot P]$
Data: On $\mathcal{K}_1$, $[Q] = [P + R_1]$ using Eq. (5)

Function `ScalarMult`$(n, [P])$**:**
  $[U] \leftarrow [P]$;
  $[V] \leftarrow$ `DoublingTranslation`$([P])$;
  for $i \leftarrow \ell - 2$ **to** 0 **do**
    $[D] \leftarrow [U - V]$; `// This is either` $[P]$ `or` $[Q]$ `which are pre-computed`
    if $b_i = 0$ **then**
      $[V] \leftarrow$ `DiffAdd`$([U], [V], [D])$;
      $[U] \leftarrow$ `DoublingTranslation`$([U])$;
    else if $b_i = 1$ **then**
      $[U] \leftarrow$ `DiffAdd`$([U], [V], [D])$;
      $[V] \leftarrow$ `DoublingTranslation`$([V])$;
    end
  end
  if $\ell \equiv 0 \bmod 2$ **or** $b_0 = 0$ **then**
    return $[U + R_1]$; `// Details in Appendix D`
  end
  return $[U]$;

explained in Appendix D, the formula for the correction step that may occur is given by Eq. (5).

Now, in the context of ECC, if we are working on a set curve like in ECDSA, we can choose a convenient one such that the associated constants are less than a computer word, and that way one can get $\mathbf{m}_0$ way smaller than $\mathbf{M}$.

Remark 10. Since we work on a set curve, some constants can be saved. Implementation-wise, constants are given as a numerator r and a denominator s, and because everything lives in a projective space a multiplication by $\frac{r}{s}$ can be put into two multiplications by r and by s. We will denote by $\mathbf{c}$ the cost of a multiplication by a small constant.

- In the doubling Algorithm 5, we directly choose d to be small, so $1\mathbf{m}_0 = 1\mathbf{c}$ for this one.
- With the additional 2-torsion point in Algorithm 1, the curve constants are $\frac{A_1}{B_1}$ and $\frac{A_2}{B_2}$. We can choose $B_1 = 1$, and that's it because the others are tied, we end up with three constants then: A_1, A_2 and B_2. In this algorithm, $2\mathbf{m}_0 = 3\mathbf{c}$.

Instead of dealing with the low level libraries' implementation of multiplication to take into account the small constants, we provide a proof of concept as well as verification scripts on GitLab[2]. The context is the following:

- We work over $\mathbb{F}_{p^{10}} = \mathbb{F}_{p^5}[i]$ where $i^2 = -1$ and $\mathbb{F}_{p^5} = \mathbb{F}_p[u]$ where $u^5 = 2$. The extension $\mathbb{F}_{p^{10}}/\mathbb{F}_{p^5}$ is to ensure that $3\mathbf{S} = 2\mathbf{M}$, and the extension $\mathbb{F}_{p^5}/\mathbb{F}_p$ is to have a large extension with trivial multiplication by u and i. A small constant corresponds to an element of $\mathbb{F}_p$. The construction obviously puts some constraints on p ($p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 5$).
- We choose $A_1 = 1 + \mu i$ and $d = \nu + i$ for some $\mu, \nu \in \mathbb{F}_p$, that way $A_2 = 2 + \mu i$ and $B_2 = \mu i$. Multiplication by these constants are faster to deal with than multiplication by generic number over $\mathbb{F}_{p^{10}}$.
- We repeated 100 times 100 random scalar multiplications.

The chosen parameters are the following:

- $p = 1485974920886612103\,1$.
- $\mu = 1141088753069104366$ such that $A_1 = 1 + \mu i$.
- $\nu = 400659849698428527$ such that $d = \nu + i$.

The results are in Table 2 and show that we achieve a 6.2% gain over the Montgomery ladder. For completeness, we also add a comparison with the theta ladder over which we achieve a 4.4%, the doubling formulas correspond to the ones from Algorithm 1, and the differential addition can be found in [KS20, Table 2].

Table 2: Timings on Intel Core i5-1145G7 @ 2.60GHz

	Montgomery ladder	Theta ladder	**Hybrid ladder**
Average (s)	2.400 ± 0.049	2.344 ± 0.009	$\mathbf{2.241 \pm 0.005}$

Remark 11. In the differential addition Algorithm 4, since in our application $\pi(U - V)$ is also a constant, it is possible to add a constraint for this one to be small too and that improves the whole time saved. However, this is not necessary for our comparison as the differential addition is the same in both ladders.

References

[Ber+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. "Twisted Edwards Curves". In: *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings.* Ed. by Serge Vaudenay. Vol. 5023. Lecture Notes in Computer Science. Springer, 2008, pp. 389–405. DOI: 10.1007/978-3-540-68164-9_26.

[CH17] Craig Costello and Hüseyin Hisil. "A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies". In: *ASIACRYPT 2017, Part II.* Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10625. LNCS. Springer, Heidelberg, Dec. 2017, pp. 303–329. DOI: 10.1007/978-3-319-70697-9_11.

[CLN16] Craig Costello, Patrick Longa, and Michael Naehrig. "Efficient Algorithms for Supersingular Isogeny Diffie-Hellman". In: *CRYPTO 2016, Part I.* Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 572–601. DOI: 10.1007/978-3-662-53018-4_21.

[DIK06] Christophe Doche, Thomas Icart, and David R. Kohel. "Efficient Scalar Multiplication by Isogeny Decompositions". In: *PKC 2006.* Ed. by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin. Vol. 3958. LNCS. Springer, Heidelberg, Apr. 2006, pp. 191–206. DOI: 10.1007/11745853_13.

[2] https://gitlab.inria.fr/nsarkis/poc-scalar-multiplication-kummer-lines

[FJP14] Luca De Feo, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *J. Math. Cryptol.* 8.3 (2014), pp. 209–247. DOI: 10.1515/JMC-2012-0015.

[GL09] Pierrick Gaudry and David Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields Their Appl.* 15.2 (2009), pp. 246–260. DOI: 10.1016/J.FFA.2008.12.006.

[HR19] Hüseyin Hisil and Joost Renes. "On Kummer Lines with Full Rational 2-torsion and Their Usage in Cryptography". In: *ACM Trans. Math. Softw.* 45.4 (2019), 39:1–39:17. DOI: 10.1145/3361680.

[KS20] Sabyasachi Karati and Palash Sarkar. "Kummer for Genus One Over Prime-Order Fields". In: *Journal of Cryptology* 33.1 (Jan. 2020), pp. 92–129. DOI: 10.1007/s00145-019-09320-4.

[Mon87] Peter L. Montgomery. "Speeding the Pollard and elliptic curve methods of factorization". English. In: *Mathematics of Computation* 48 (1987), pp. 243–264. ISSN: 0025-5718. DOI: 10.2307/2007888.

[Mor+22] Tomoki Moriya, Hiroshi Onuki, Yusuke Aikawa, and Tsuyoshi Takagi. *The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography.* Cryptology ePrint Archive, Report 2022/150. https://eprint.iacr.org/2022/150. 2022.

[Mum66] David Mumford. "On the Equations Defining Abelian Varieties. I." In: *Inventiones mathematicae* 1 (1966), pp. 287–354.

[Ren18] Joost Renes. "Computing Isogenies Between Montgomery Curves Using the Action of (0, 0)". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings.* Ed. by Tanja Lange and Rainer Steinwandt. Vol. 10786. Lecture Notes in Computer Science. Springer, 2018, pp. 229–247. DOI: 10.1007/978-3-319-79063-3_11. URL: https://doi.org/10.1007/978-3-319-79063-3%5C_11.

[Vél71] Jacques Vélu. "Isogénies entre courbes elliptiques". In: *Comptes-Rendus de l'Académie des Sciences* 273 (1971), A238–A241.

A Montgomery arithmetic on a Kummer line

We work on a Kummer line $\mathcal{K}$ associated to a Montgomery curve with constant $\mathcal{A}$. Arithmetic in Algorithms 4 and 5 was introduced by Montgomery in [Mon87]. They are used in the Montgomery ladder (Algorithm 6).

Algorithm 4: Differential addition in Montgomery xz-coordinates

Input: $[P] = (X_1 : Z_1)$, $[Q] = (X_2 : Z_2)$ and $[P - Q] = (X_0 : Z_0) \neq (1 : 0)$
Output: $[P + Q] = (X : Z)$

Function `DiffAdd(`$[P], [Q], [P - Q]$`):`
- $u \leftarrow (X_1 + Z_1)(X_2 - Z_2)$;
- $v \leftarrow (X_1 - Z_1)(X_2 + Z_2)$;
- $w \leftarrow (u + v)^2$;
- $t \leftarrow (u - v)^2$;
- $X \leftarrow w$;
- $Z \leftarrow \frac{X_0}{Z_0} t$;
- **return** $(X : Z)$;

Algorithm 5: Doubling in Montgomery xz-coordinates

Input: $[P] = (X_1 : Z_1)$
Output: $[2 \cdot P] = (X : Z)$
Data: If $\mathcal{A}$ is the Montgomery curve constant, $d = \frac{\mathcal{A}+2}{4}$

Function `Doubling(`$[P]$`):`
- $u \leftarrow (X_1 + Z_1)^2$;
- $v \leftarrow (X_1 - Z_1)^2$;
- $t \leftarrow u - v$;
- $X \leftarrow uv$;
- $Z \leftarrow t(v + dt)$;
- **return** $(X : Z)$;

B More examples of 2-isogenies: Legendre and theta models

In this section, we will look at two other classical Kummer lines models.

B.1 Legendre model

An elliptic curve is said to be in Legendre form if it has full rational 2-torsion and is then put in the following shape:

$$E : By^2 = x(x - 1)(x - \gamma), \gamma \in k.$$

In terms of Kummer lines, this is a particular case of Main Example 1. The ramification is as follows:

$$\mathcal{O} = (1 : 0)^*, \qquad T = (0 : 1), \qquad R = (1 : 1), \qquad S = (\gamma : 1).$$

We will focus on two isogenies with kernel T. Our goal is to recover the Montgomery to Legendre and Legendre to Montgomery isogeny formulas from [Ber+08, Theorem 5.1].

Algorithm 6: Scalar multiplication with Montgomery ladder

Input: $n = (1, b_{\ell-2}, \ldots, b_0)$ an ℓ-bits integer, $[P]$ a point on $\mathcal{K}_1$
Output: $[n \cdot P]$

Function `MontgomeryLadder`$(n, [P])$**:**
    $[U] \leftarrow [P]$;
    $[V] \leftarrow$ `Doubling`$([P])$;
    for $i \leftarrow \ell - 2$ **to** 0 **do**
        if $b_i = 0$ **then**
            $[V] \leftarrow$ `DiffAdd`$([U], [V], [P])$;
            $[U] \leftarrow$ `Doubling`$([U])$;
        else if $b_i = 1$ **then**
            $[U] \leftarrow$ `DiffAdd`$([U], [V], [P])$;
            $[V] \leftarrow$ `Doubling`$([V])$;
        end
    end
    return $[U]$;

Example 2 (Montgomery model to Legendre model)**.** Suppose our initial Kummer line $\mathcal{K}_1$ is a Montgomery one with the following ramification:

$$\mathcal{O}_1 = (1:0)^*, \qquad T_1 = (0:1), \qquad R_1 = (A_1 : B_1), \qquad S_1 = (B_1 : A_1).$$

$\frac{A_1}{B_1}$ may not be rational. We also know about the 4-torsion points above T_1, which are $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

We can use the invariants from Section 4.1. Set $f : (X : Z) \mapsto \Big((X+Z)^2 : (X-Z)^2\Big)$, it is T_1-invariant and the ramification on the codomain is:

- $f(\mathcal{O}_1) = f(T_1) = (1:1)^*$,
- $f(R_1) = f(S_1) = ((A_1 + B_1)^2 : (A_1 - B_1)^2)$,
- $f(T_1') = (1:0)$,
- $f(T_1'') = (0:1)$.

We notice that this is exactly a Legendre model with $\gamma_2 = \frac{(A_1+B_1)^2}{(A_1-B_1)^2}$ up to translation by a 2-torsion point. We already justified in Main Example 4 that $f(R_1) = f(S_1)$ is rational even if R_1 is not. The ramification of the codomain is:

$$\mathcal{O}_2 = (1:0), \qquad T_2 = (0:1), \qquad R_2 = (1:1)^*, \qquad S_2 = (\gamma_2 : 1).$$

The 2-isogeny is then $g = f + R_2$ and can be computed in $2\mathbf{S} + 2\mathbf{a}$, γ_2 can be computed in $2\mathbf{S} + 2\mathbf{a}$.

Another idea is to use invariants $(X+Z)^2$ and XZ via $g_0 : (X : Z) \mapsto ((X+Z)^2 : XZ)$, the ramification on the codomain this time is:

- $g_0(\mathcal{O}_1) = f_0(T_1) = (1:0)^*$,
- $g_0(R_1) = f_0(S_1) = ((A_1 + B_1)^2 : A_1 B_1)$,
- $g_0(T_1') = (4:1)$,
- $g_0(T_1'') = (0:1)$.

We have to change the shape of our ramification, we are looking for a homography h such that:

- $h(1:0) = (1:0)$,
- $h(4:1) = (1:1)$,
- $h(0:1) = (0:1)$.

We find that $h(X:Z) = (X:4Z)$ satisfies these conditions. By setting $g = h \circ g_0$ and:

$$\gamma_2 = h((A_1+B_1)^2 : A_1B_1) = \frac{(A_1+B_1)^2}{4A_1B_1}.$$

The ramification on the codomain is:

$$\mathcal{O}_2 = (1:0)^*, \qquad T_2 = (0:1), \qquad R_2 = (1:1), \qquad S_2 = (\gamma_2 : 1).$$

This can be computed in $2\mathbf{S} + 3\mathbf{a}$ using $4XZ = (X+Z)^2 - (X-Z)^2$, and γ_2 also in $2\mathbf{S} + 3\mathbf{a}$.

Example 3 (Legendre model to Montgomery model)**.** On the other hand, it is also possible to go from a Legendre model to a Montgomery one via a 2-isogeny. Suppose our initial Kummer line $\mathcal{K}_1$ is a Legendre one with the following ramification:

$$\mathcal{O}_1 = (1:0)^*, \qquad T_1 = (0:1), \qquad R_1 = (1:1), \qquad S_1 = (\gamma_1 : 1).$$

In Main Example 3, we computed the following quadratic forms that are T_1-invariant:

$$u(X,Z) = X^2 + \gamma_1 Z^2, \qquad v(X,Z) = XZ.$$

In Main Example 4, we also computed the 4-torsion above T_1:

$$T_1' = (\sqrt{\gamma_1} : 1) \qquad T_1'' = (-\sqrt{\gamma_1} : 1).$$

First, set $g_0 : (X:Z) \mapsto (X^2 + \gamma_1 Z^2 : XZ)$, it is T_1-invariant and the ramification on the codomain is:

- $g_0(\mathcal{O}_1) = f_0(T_1) = (1:0)^*$,
- $g_0(R_1) = f_0(S_1) = (1+\gamma_1 : 1)$,
- $g_0(T_1') = (2\sqrt{\gamma_1} : 1)$,
- $g_0(T_1'') = (-2\sqrt{\gamma_1} : 1)$.

To recover a Montgomery Kummer line, we also need a 4-torsion point. Set $R_1' = (r:s)$ to be a 4-torsion point above R_1'. Let σ be an element of the Galois group of our field k. Then either $[\sigma(R_1')] = [R_1']$, or $[\sigma(R_1')] = [R_1'']$ is another 4-torsion point above R_1 because $2\sigma(R_1') = \sigma(R_1) = R_1$. We can't have $R_1'' = R_1' + R_1$ because on the Kummer line $[R_1'] = [R_1' + R_1]$, therefore $R_1'' = R_1' + T_1 = R_1' + S_1$ on the Kummer line. Hence, $\sigma(g_0(R_1')) = g_0(\sigma(R_1')) = g_0(R_1' + T_1) = g_0(R_1')$. In all cases, $g_0(R_1')$ is invariant by Galois.

The translation by R_1 is given by $\tau_{R_1} : (X:Z) \mapsto (X - \gamma_1 Z : X - Z)$. Because $R_1' + R_1 = R_1'$, we find using τ_{R_1} that $r^2 + \gamma_1 s^2 = 2rs$. Then $g_0(R_1') = (2:1)$.

To go to a Montgomery model, we want a homography $h : (X:Z) \mapsto (aX + bZ : cX + dZ)$ such that:

- $h(1:0) = (1:0)$, i.e. $c = 0$,

- $h(1+\gamma_1 : 1) = (0:1)$, i.e. $b = -a(1+\gamma_1)$,
- $h(2:1) = (1:1)$, i.e. $d = 2a + b = a(1-\gamma_1)$.

This yields $h(X:Z) = (X - (1+\gamma_1)Z : (1-\gamma_1)Z)$. One can check that:

$$h(2\sqrt{\gamma_1}:1) = (\sqrt{\gamma_1}-1 : \sqrt{\gamma_1}+1) \qquad h(-2\sqrt{\gamma_1}:1) = (\sqrt{\gamma_1}+1 : \sqrt{\gamma_1}-1).$$

We end up on the following Montgomery model with the 2-isogeny $g = h \circ g_0$:

$$\mathcal{O}_2 = (1:0)^*, \qquad T_2 = (0:1), \qquad R_2 = (\sqrt{\gamma_1}-1 : \sqrt{\gamma_1}+1), \qquad S_2 = (\sqrt{\gamma_1}-1 : \sqrt{\gamma_1}+1).$$

B.2 Theta model

In this section we look at another model where the neutral point is not at infinity this time. Let $a, b \in k$ be two constants that will define our ramification:

$$\mathcal{O}_1 = (a:b)^*, \qquad T_1 = (-a:b), \qquad R_1 = (b:a), \qquad S_1 = (-b:a).$$

This is called a theta model with theta constants $(a:b)$, we will again focus on 2-isogenies with kernel T_1.

We first want to compute potential 4-torsion points, we have:

$$\tau_{T_1}(X:Z) \mapsto (-X:Z), \qquad \tau_{R_1} : (X:Z) \mapsto (Z:X), \qquad \tau_{S_1} : (X:Z) \mapsto (-Z:X).$$

If $T_1' = (X:Z)$ is a 4-torsion point above T_1, we want to solve $T_1' + T_1 = T_1'$. With a similar approach, these are the 4-torsion points on this model:

- Above T_1: $T_1' = (1:0)$ and $T_1'' = (0:1)$.
- Above R_1: $R_1' = (1:1)$ and $R_1'' = (-1:1)$.
- Above S_1: $S_1' = (i:1)$ and $S_1'' = (-i:1)$ with $i^2 = -1$.

Aside S_1' and S_1'' which may not be rational, there are always two rational independent 4-torsion points on this model: T_1' and R_1'. This is one more occurrence of a Montgomery model where this time two points of two torsion are required to be of Montgomery type. In the theta model, the ramification is then put in a way to be invariant both by $(X:Z) \to (Z:X)$ as in the Montgomery model, but also by $(X:Z) \mapsto (-X:Z)$. In particular the full 2-torsion is always rational in the theta model.

The matrix associated to τ_{T_1} is $M = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $M^2 = I_2$, so the type is 1 as expected and M acts as:

$$M \cdot X^2 = X^2 \qquad M \cdot Z^2 = Z^2 \qquad M \cdot XZ = -XZ.$$

Example 4 (Theta model to Montgomery model)**.** We will use X^2 and Z^2 as the invariants, set $f : (X:Z) \mapsto (X^2 : Z^2)$. A quick computation yields:

- $f(\mathcal{O}_1) = f(T_1) = (a^2 : b^2)^*$,
- $f(R_1) = f(S_1) = (b^2 : a^2)$,
- $f(T_1') = (1:0)$,
- $f(T_1'') = (0:1)$.

We also have $f(R_1') = (1:1)$ and $f(S_1') = (-1:1)$, the 4-torsion above $(1:0)$. The ramification is Montgomery shaped up to a translation, the 2-isogeny is then $g = f + R_2$ with:

$$\mathcal{O}_2 = (1:0), \qquad T_2 = (0:1), \qquad R_2 = (a^2:b^2)^*, \qquad S_2 = (b^2:a^2).$$

f can be computed in $2\mathbf{S}$, the codomain in $2\mathbf{S}$ too.

This can be used to find doubling formulas on the theta model. If $\hat{g}$ is the dual of g, we have that $\ker \hat{g} = \langle T_2 \rangle$. We use the same invariants as in Theorem 2 because we start on a Montgomery model, and we set $\hat{g}_0 : (X:Z) \mapsto ((X+Z)^2 : (X-Z)^2)$. One computes, with $(A^2:B^2) = (a^2+b^2 : a^2-b^2)$:

- $\hat{g}_0(\mathcal{O}_2) = \hat{g}_0(T_2) = (1:1)^*$,
- $\hat{g}_0(R_2) = \hat{g}_0(S_2) = (A^4:B^4)$,
- $\hat{g}_0(T_2') = (1:0)$,
- $\hat{g}_0(T_2'') = (0:1)$.

Because we want to compute the dual, we are aiming for the following equations:

- $\hat{g}(g(\mathcal{O}_1)) = \mathcal{O}_1$ i.e. $\hat{g}(\mathcal{O}_2) = (a:b)$,
- $\hat{g}(g(S_1')) = S_1$ i.e. $\hat{g}(T_2') = (-b:a)$,
- $\hat{g}(g(R_1')) = R_1$ i.e. $\hat{g}(T_2'') = (b:a)$,
- $\hat{g}(g(T_1')) = T_1$ i.e. $\hat{g}(R_2) = (-a:b)$.

As usual, we look for a homography h such that $\hat{g} = h \circ \hat{g}_0$. Using the first three equations, we find that:

$$h : (X:Z) \mapsto (b(B^2X + A^2Z) : a(-B^2X + A^2Z)).$$

We finally check that indeed $h(A^4:B^4) = (-a:b)$, and therefore we have $\hat{g} = h \circ \hat{g}_0$. Because $\hat{g}(g(P)) = 2 \cdot P$ and $\hat{g}(R_2) = T_1$, we can then compute $2 \cdot P + T_1 = \hat{g} \circ f(P)$ in $4\mathbf{S} + 2\mathbf{m}_0 + 2\mathbf{a}$, which is essentially $2 \cdot P$ because $\tau_{T_1}(X:Z) = (-X:Z)$.

Example 5 (Theta model to theta model)**.** We recall the theta model here:

$$\mathcal{O}_1 = (a:b)^*, \qquad T_1 = (-a:b), \qquad R_1 = (b:a), \qquad S_1 = (-b:a).$$

Assume in this example that we have a 8-torsion point $\widetilde{T_1} = (r:s)$ above T_1'. Using invariants X^2 and Z^2, we set $g_0(X:Z) = (X^2+Z^2 : X^2-Z^2)$ and once again $(A^2 : B^2) = (a^2+b^2 : a^2-b^2)$. One computes:

- $g_0(\mathcal{O}_1) = g_0(T_1) = (A^2:B^2)^*$,
- $g_0(R_1) = g_0(S_1) = (-A^2:B^2)$,
- $g_0(T_1') = (1:1)$,
- $g_0(T_1'') = (-1:1)$.

The 4-torsion is $g_0(\widetilde{T_1}) = (r^2+s^2 : r^2-s^2) := (u:v)$, $g_0(R_1') = (1:0)$ and $g_0(S_1') = (0:1)$.

By setting $h : (X:Z) \mapsto (BX : AZ)$, the ramification is put in the correct shape. It remains to check is that $(A:B)$ is indeed rational in this context. To do so, we will look at the 4-torsion on the intermediate model, set:

$$\mathcal{O}_0 = (A^2:B^2)^*, \qquad T_0 = (-A^2:B^2), \qquad R_0 = (1:1), \qquad S_0 = (-1:1).$$

We then have $T_0' = (1:0)$ and $T_0'' = (0:1)$ and $R_0' = (u:v)$ by the 2-isogeny. On this model, the translation by R_0 is $\tau_{R_0} : (X:Z) \mapsto (A^2 Z : B^2 X)$. The 4-torsion verifies $R_0' + R_0 = R_0'$, therefore:

$$(A^2 v : B^2 u) = (u:v) \iff \frac{u}{v} = \pm\frac{A}{B}.$$

Hence, $(A:B)$ is rational, so is h and $g = h \circ g_0$ which gives the following theta model:

$$\mathcal{O}_2 = (A:B)^*, \qquad T_2 = (-A:B), \qquad R_2 = (B:A), \qquad S_2 = (-B:A).$$

The 4-torsion is $T_2' = g(R_1') = (1:0)$, $T_2'' = g(S_1') = (0:1)$ and $R_2' = g(\widetilde{T_1}) = (1:1)$ when we choose $(A:B) = (u:v)$.

We recover the usual duplication formula on theta coordinates. Since the codomain is in the theta model, we can also easily compute the dual isogeny by swapping $(a:b)$ and $(A:B)$ in the formulas, and recover the doubling formulas from [GL09].

C Computing 2^n-isogenies between Montgomery models

As explained in Section 2, 2^n-isogenies can be computed via chaining 2-isogenies. Starting with a point P_0 of 2^n-torsion on an elliptic curve E_0, one can reduce its order by:

- Either computing $2 \cdot P_0$, in which case we stay on the curve E_0.
- Or computing the image of P_0 via the 2-isogeny of kernel $2^{n-1} \cdot P_0$, in which case we end up on some curve E_1

We then have two important operations: doubling and image by a 2-isogeny. One thing to keep in mind is that we have to do operations in the correct order, it is not possible to compute an image without the kernel, and it is not possible to compute a doubling without the curve constant.

As a first step, one always need to compute every $2^i \cdot P_0$. Then a naive approach would be to compute the 2-isogeny with kernel $2^{n-1} \cdot P_0$, compute every image, and repeat this process on the new curve. One could also only compute the image of P_0, compute every doubling of the new point P_1 on the new curve and repeat the process. It is convenient to represent such strategies as trees, like in Fig. 1. The leaves are 2-torsion points on the corresponding curve.

This is obviously not optimal however, too many useless points are computed, and we end up with $O(n^2)$ operations for a 2^n-isogeny. In their paper [FJP14, § 4.2.2], De Feo, Jao and Plut explain how to find optimal strategies, taking into account the relative cost of a doubling compared to an image. An example is given in Fig. 2, where using a binary tree gives $O(n \log n)$ operations for a 2^n-isogeny.

In this section, we focus on 2^n-isogenies where the intermediate Kummer lines are given by Montgomery models. We will denote them as $\mathcal{K}_i$ with $i \geq 0$, so $\mathcal{K}_0$ is the initial Kummer line, and the ramification will be denoted as follows:

$$\mathcal{O}_i = (1:0)^*, \qquad T_i = (0:1), \qquad R_i = (A_i : B_i), \qquad S_i = (B_i : A_i) = R_i + T_i.$$

As shown in Section 4, the point $R_i = (A_i : B_i)$ can be used for the translated doubling formula on $\mathcal{K}_i$. It can also be used to recover the curve constant for standard doubling, it is always rational, even if R_i and S_i are not:

$$d_i = \frac{(A_i - B_i)^2}{(A_i - B_i)^2 - (A_i + B_i)^2}.$$

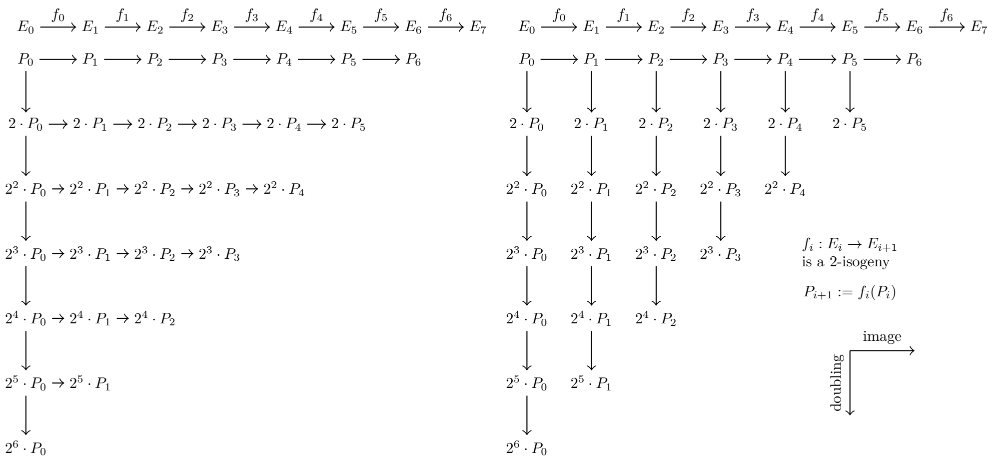

Figure 1: 2^7-isogeny $f = f_6 \circ \cdots \circ f_0$ with kernel P_0 — naive approaches

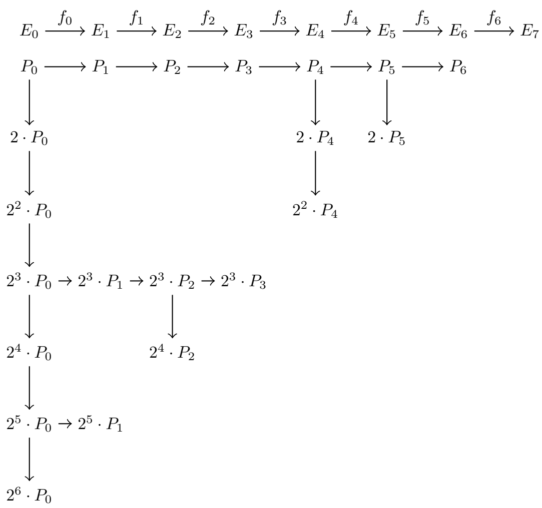

Figure 2: 2^7-isogeny $f = f_6 \circ \cdots \circ f_0$ with kernel P_0 — optimized approach

We also denoted earlier $(a'_i : b'_i)$ the 4-torsion point above R_i and $(a_i : b_i) = (a'_i + b'_i : a'_i - b'_i)$.

We will focus on the case where P_0 is above the 2-torsion point R_0, as we want to compare it to Renes formulas provided in [Ren18, Prop. 4.2], and for simplicity we neglect the cost of the additions. Recall from Section 4 that for the isogeny with kernel R_i, the translated by $f_i(R'_i) = R_{i+1} = ({a'_i}^2 : {b'_i}^2)$ isogeny formula $\mathcal{K}_i \to \mathcal{K}_{i+1}$ is given by $(X : Z) \mapsto \Big((b_i(X+Z) + a_i(X-Z))^2 : (b_i(X+Z) - a_i(X-Z))^2 \Big)$. The codomain $\mathcal{K}_{i+1}$ is represented by R_{i+1} and can be computed in $2\mathbf{S}$, and the translated image costs $2\mathbf{M}+2\mathbf{S}$.

Since $R_{i+1} = f_i(R'_i)$ is the kernel of the next isogeny f_{i+1}, computing translated images by R_{i+1} does not matter, except at the very last step where we can use the standard non translated formula instead. Thus, similarly to what was done in Section 5, we can build a hybrid algorithm which combines Montgomery doubling (standard or translated by R_i) and our translated image formula.

Remark 12. As we can see, our image formula only involves the 4-torsion point R'_i above R_i (we can also recover from it the constant d_i), so the leaves in our strategy tree will be the 4-torsion points instead of the 2-torsion ones. This also implies that if we want to compute a 2^n-isogeny, we have to assume we are given a 2^{n+1}-torsion point, or we do the last step with Renes formulas which doesn't have this constraint.

What matters now is to compare the standard costs operations from [Ren18, Prop. 4.2] with the ones provided in Section 4, this is done in Table 3. Unlike in Section 5, after the first 2-isogeny, we don't have control on curve constants any more, so $\mathbf{m}_0$ must be counted as two generic multiplications because of the numerator and the denominator.

Table 3: Comparison of operations on Kummer lines to compute 2^n-isogenies

Operation	Doubling		Image	
	[Mon87]	Proposition 1	[Ren18]	Theorem 3
Cost	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}_0$	$4\mathbf{S} + 2\mathbf{m}_0$	$2\mathbf{M} + 1\mathbf{m}_0$	$2\mathbf{S} + 1\mathbf{m}_0$
Cost ($\mathbf{m}_0 = 2\mathbf{M}$)	$4\mathbf{M} + 2\mathbf{S}$	$4\mathbf{M} + 4\mathbf{S}$	$4\mathbf{M}$	$2\mathbf{M} + 2\mathbf{S}$
Constants used	d_i	$(A_i : B_i)$, $(A_{i+1} : B_{i+1})$	$(A_i : B_i)$	$(a_i : b_i)$

We see that our formulas for images should be faster than the ones by Renes. The cost of the codomain is more tricky: Renes formulas directly give d_{i+1} in $2\mathbf{S}$. Our formulas give R_{i+1} in $2\mathbf{S}$; but from R_{i+1} we can only use our translated doubling formulas, which are in this context more expensive than the standard doubling formulas. Thus, we need to compute d_{i+1} from R_{i+1} which costs $2\mathbf{S}$ by the formula

$$d_{i+1} = \frac{(a_i'^2 - b_i'^2)^2}{(a_i'^2 - b_i'^2)^2 - (a_i'^2 + b_i'^2)^2},$$

for a total codomain cost of $4\mathbf{S}$.

Asymptotically, since there are exactly n codomains to compute, they are negligible compared to images and doublings which are in $O(n \log n)$. An implementation to compute a 2^n-isogeny using this hybrid method with SIKE$p434$ parameters is available in the same GitLab repository and shows that we do end on the same curve as the one with Renes formulas. For these parameters, our implementation shows that our hybrid method is slower, because the n considered is not large enough that the faster images compensate the slower codomains.

Another reason why this would not be viable anyway is that there exists efficient 4-isogeny formulas [CH17, § A], which saves half of the steps while having competitive costs for multiplication by 4 and images, hence are much faster. Indeed, the 4-isogeny codomain costs $4\mathbf{S}$ (computing d_{i+2} from d_i and R_i'), and a 4-isogeny image costs $6\mathbf{M} + 2\mathbf{S}$. We remark that this is the same cost as combining our translated 2-isogeny image with the standard 2-isogeny image. In particular, by composing our translated 2-isogeny image twice, there is also a translated (by a 2-torsion point) 4-isogeny image in only $4\mathbf{M} + 4\mathbf{S}$. However, to be able to use these translated images, our codomain formula would be slower.

Only in some hypothetical context where we would need to compute a lot of images, assuming we already know the codomains, then the hybrid approach would be faster.

D Correctness of the hybrid ladder

Fig. 3 shows two steps of Algorithm 3 and explains why we are cycling between 1 and 2 translated points. We want to compute $n \cdot P$, with n an ℓ-bits integer, its bits are denoted b_i. Set also $Q = P + R$ where R is the extra 2-torsion point and assume the input is $U_0 = m \cdot P$ and $V_0 = (m+1) \cdot P + R$, this corresponds to the initialization of our algorithm. According to Fig. 3, the correction to the end result is as follows:

- If we have an odd number of steps, i.e. ℓ is even, we get $U = n \cdot P + R$, so we always need to correct U.

- On the other hand, if ℓ is odd, we get $V = n \cdot P + R$ if and only if the last bit is 0, otherwise we have $U = n \cdot P$.

E Odd degree isogenies on Kummer lines

In this section, we extend the work of [Ren18] to build isogenies of odd degrees on any model of a Kummer line.

Let E be an elliptic curve, and K be a cyclic kernel of odd degree ℓ, and $f : E \to E'$ the corresponding isogeny. To build a model of the Kummer line associated to $E' = E/K$, we need to build sections of $2(\mathcal{O}_{E'})$, hence invariant sections of $f^*(2(\mathcal{O}_{E'})) = \sum_{T \in K} 2(T)$ on E.

If s is an invariant section, its associated divisor $\operatorname{div} s$ is invariant. The converse is not true, there is an obstruction coming from the Weil-Cartier pairing.

Lemma 3. *Let $D = \sum_i a_i \sum_{T \in K}(P_i + T) = \operatorname{div} s_D$ a principal divisor and $P_0 \coloneqq \sum a_i P_i$. Then s_D is invariant by translation if and only if $P_0 \in K$.*

Proof. Since $\operatorname{div} s_D$ is invariant by K, if $T \in K$, the function $s_D(P + T)$ has the same divisor as s_D, hence differ by a constant. By definition of the Weil-Cartier pairing e_f, this constant is precisely equal to $e_f(T, f(P_0))$. So s_D is invariant by K if and only if $P_0 \in E[\ell]$ is orthogonal to K, if and only if $P_0 \in K$, if and only if $f(P_0) = \mathcal{O}_{E'}$.

Another equivalent proof is to remark that s_D is invariant by translation if and only if D descends to a divisor $D' = \sum_i a_i \sum_{T \in K} f(P_i)$ on E' which is linearly equivalent to 0, which is the case if and only if $P_0 \in K$. $\square$

Example 6. Take $Q_1, Q_2 \in E(k)$, $s_D = \prod_{T \in K} \frac{x - x(Q_1+T)}{x - x(Q_2+T)}$ (we use the convention that $x - x(\mathcal{O}_E) \coloneqq 1$). Its associated divisor is

$$D = \sum_{T \in K} \left((Q_1 + T) + (-Q_1 + T) - (Q_2 + T) - (-Q_2 + T)\right).$$

Then s_D is invariant by translation and descends to $\frac{x - f(Q_1)}{x - f(Q_2)}$ on E/K, x a Weierstrass coordinate. When $Q_2 = \mathcal{O}_E$, we recover a formula from [CH17; Ren18].

As illustrated by Example 6, we can use Lemma 3 to construct divisors associated to an invariant section. From such a divisor we can use Miller's algorithm to construct the associated section s. Since the isogeny is of odd degree, it preserves the 2-torsion, so by evaluating s on the ramification point of the Kummer model of E we can efficiently recover the Kummer model of E' given by s.

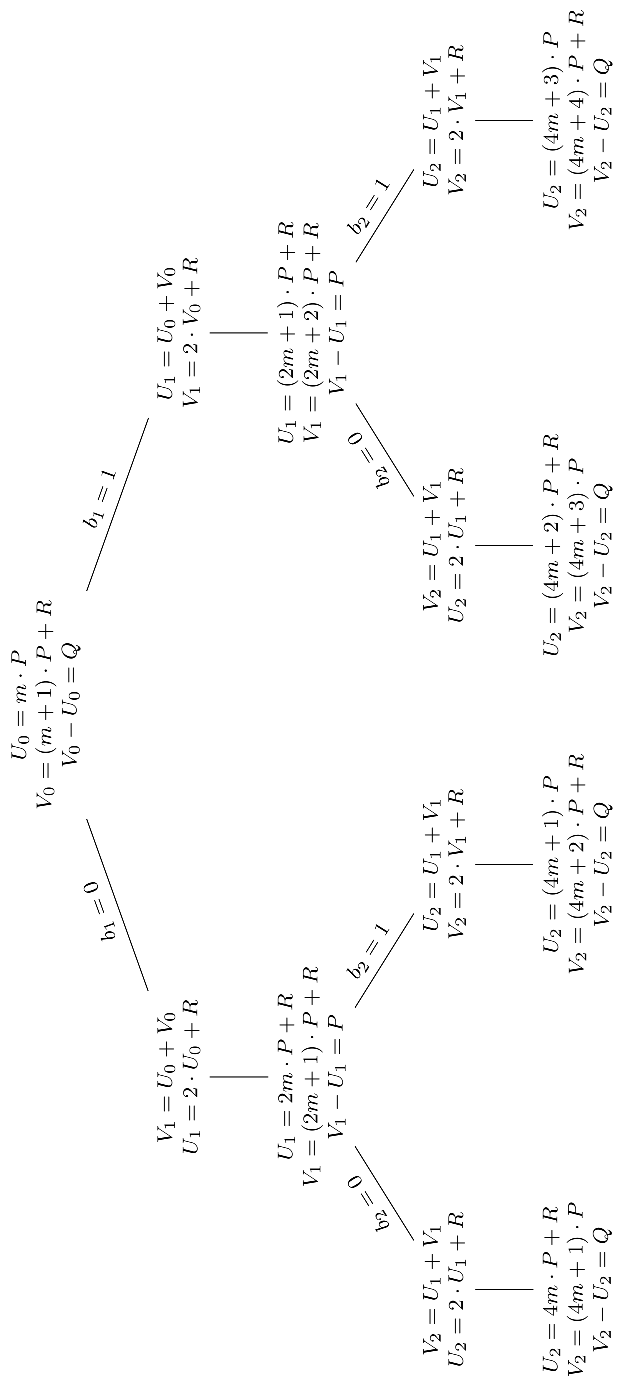

Figure 3: Two steps of scalar multiplication based on hybrid ladder