Computing isogenies between Abelian Varieties

David Lubicz, Damien Robert

Computing isogenies between abelian varieties

David Lubicz[1,2], Damien Robert[3]

[1] CÉLAR,
BP 7419, F-35174 Bruz
[2] IRMAR, Universté de Rennes 1,
Campus de Beaulieu, F-35042 Rennes
[3] LORIA, Campus Scientifique, BP 239,
F-54506 Vandœuvre-lès-Nancy

Abstract

We describe an efficient algorithm for the computation of isogenies between abelian varieties represented in the coordinate system provided by algebraic theta functions. We explain how to compute all the isogenies from an abelian variety whose kernel is isomorphic to a given abstract group. We also describe an analog of Vélu's formulas to compute an isogenis with prescribed kernels. All our algorithms rely in an essential manner on a generalization of the Riemann formulas.

In order to improve the efficiency of our algorithms, we introduce a point compression algorithm that represents a point of level 4ℓ of a g dimensional abelian variety using only $g(g+1)/2 \cdot 4^g$ coordinates. We also give formulas to compute the Weil and commutator pairing given input points in theta coordinates. All the algorithms presented in this paper work in general for any abelian variety defined over a field of odd characteristic.

Contents

List of Algorithms

List of Notations

Notation	Description	Page List
$Z(\overline{n})$	$\mathbb{Z}^g/n\mathbb{Z}^g$	9
$\mathscr{M}_{\overline{n}}$	The moduli space of theta null points of level n.	7
A_k	$(A_k, \mathscr{L}, \Theta_{A_k})$ is a polarized abelian variety with a theta structure of level ℓn.	9
B_k	$(B_k, \mathscr{L}_0, \Theta_{B_k})$ is an abelian variety ℓ-isogenous to A_k with a theta structure of level n.	10
ϑ_i	$(\vartheta_i)_{i\in Z(\overline{\ell n})}$ are the canonical projective coordinates on A_k given by the theta structure.	9
0_{A_k}	The theta null $0_{A_k} = \vartheta_i(0_{A_k})_{i\in Z(\overline{\ell n})}$.	10
0_{B_k}	The theta null $0_{B_k} = \vartheta_i(0_{B_k})_{i\in Z(\overline{n})}$.	10
$G(\mathscr{L})$	The Theta group of $(A_k, \mathscr{L})$	9
$K(\mathscr{L})$	$K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$ is the decomposition of the kernel of the polarization $\mathscr{L}$ induced by the Theta structure Θ_A	9
$H(\delta)$	The Heisenberg group of type δ.	9
$s_{K_1(\mathscr{L})}$	The natural section $K_1(\mathscr{L}) \to G(\mathscr{L})$ induced by the Theta structure.	9
$\widetilde{\rho}^*_{\mathscr{L}}$	The affine action of $G(\mathscr{L})$ on $\widetilde{A}_k$.	10
$\rho^*_{\mathscr{L}}$	The projective action of $K(\mathscr{L})$ on A_k.	10
$\widetilde{A}_k$	The affine cone of A_k.	10
$\widetilde{B}_k$	The affine cone of B_k.	11
$\widetilde{\vartheta}_i$	$(\widetilde{\vartheta}_i)_{i\in Z(\overline{\ell n})}$ are the affine coordinates on $\widetilde{A}_k$.	10
$\widetilde{0}_{B_k}$	An affine lift of 0_{B_k}.	15
$\widetilde{0}_{A_k}$	The affine lift of 0_{A_k} such that $\widetilde{\pi}(\widetilde{0}_{A_k}) = \widetilde{0}_{B_k}$.	15
π	The ℓ-isogeny $\pi : A_k \to B_k$.	10
$\widetilde{\pi}$	$\widetilde{\pi}(\widetilde{\vartheta}_i(\widetilde{x})_{i\in Z(\overline{\ell n})}) = \widetilde{\vartheta}_i(\widetilde{x})_{i\in Z(\overline{n})}$ is the affine lift of π to $\widetilde{A}_k \to \widetilde{B}_k$.	11
$\widetilde{\pi}_i$	$\widetilde{\pi}_i = \widetilde{\pi} \circ (1, i, 0) = \widetilde{\vartheta}_{i+j}(\cdot)_{j\in Z(\overline{n})}$.	14
$\widetilde{P}_i$	$\widetilde{P}_i = (1, i, 0).\widetilde{0}_{A_k} = (\vartheta_{i+j}(\widetilde{0}_{A_k}))_{j\in Z(\overline{\ell n})}$.	16
$\widetilde{R}_i$	$\widetilde{R}_i = \widetilde{\pi}_i(\widetilde{0}_{A_k}) = \widetilde{\pi}(\widetilde{P}_i)$.	16
$(e_1, \ldots, e_g)$	A basis of $Z(\overline{\ell n})$	28
$(d_1, \ldots, d_g)$	$d_i = ne_i$	28
$\mathscr{S}$	$\mathscr{S} = Z(\overline{\ell})$ (When $\ell \wedge n = 1$)	14
$\mathfrak{S}$	$\mathfrak{S} = \{d_1, d_2, \ldots, d_g, d_1 + d_2, \ldots d_1 + d_g, d_2 + d_3, \ldots d_{g-1} + d_g\}$ (When $\ell \wedge n = 1$)	28
e'_ℓ	The extended commutator pairing on $B_k[\ell]$	16

Notation	Description	Page List
e_W	The Weil pairing.	41
e_c	The canonical pairing on $Z(\overline{n}) \times \hat{Z}(\overline{n})$.	9
$\widetilde{B_k}'$	the affine cone of $(B_k, \mathscr{M}_0, \Theta_{B_k,\mathscr{M}_0})$ where $\mathscr{M}_0 = [\ell]^*\mathscr{L}_0$ and $\Theta_{B_k,\mathscr{M}_0}$ is a theta structure on $(B_k, \mathscr{M}_0)$ compatible with Θ_{B_k}.	16
$\widetilde{[\ell]}$	$\widetilde{[\ell]} : \widetilde{B_k}' \to \widetilde{B}_k$ is the morphism lifting $[\ell] : B_k \to B_k$.	16
`chaine_add`	An addition chain	18
`chaine_multadd`	A multiplication chain	21

1 Introduction

In this paper, we are interested in some algorithmic aspects of isogeny computations between abelian varieties. Computing isogenies between abelian varieties may be seen as different kind of computational problems depending on the expected input and output of the algorithm. These problems are:

- Given an abelian variety A_k and an abstract finite abelian group K compute all the abelian varieties B_k such that there exists an isogeny $A_k \to B_k$ whose kernel is isomorphic to K, and compute these isogenies.
- Given an abelian variety A_k and a finite subgroup K of A_k, recover the quotient abelian variety $B_k = A_k/K$ as well as the isogeny $A_k \to B_k$.
- Given two isogenous abelian varieties, A_k and B_k, compute explicit equations for an isogeny map $A_k \to B_k$.

Here, we are concerned with the first two problems. In the case that the abelian variety is an elliptic curve, efficient algorithms have been described that solve all the aforementioned problems [Ler]. For higher-dimensional abelian varieties much less is known. Richelot's formulas [Mes01, Mes02] can be used to compute $(2,2)$-isogenies between abelian varieties of dimension 2. The paper [Smi09] also introduced a method to compute certain isogenies of degree 8 between Jacobian of curves of genus three. In this paper, we present an algorithm to compute $(\ell,\dots,\ell)$-isogenies between abelian varieties of dimension g for any $\ell \geqslant 2$ and $g \geqslant 1$. Possible applications of our algorithm includes:

- The transfer the discrete logarithm from an abelian variety to another abelian variety where the discrete logarithm is easy to solve [Smi08]
- The computation of isogeny graph to obtain a description the endomorphism ring of an Abelian variety.

By Torelli's theorem there is a one on one correspondence between principally polarized abelian varieties of dimension 2 and Jacobians of genus 2 hyperelliptic curves. Thus the modular space of principally polarized abelian varieties of dimension 2 is parametrized by the three Igusa invariants, and one can define modular polynomials between these invariants much in the same way as in the genus-one case [BL09]. However the height of these modular polynomials explodes with the order, making their computations impractical: only those are known [Plo29]. In order to circumvent this problem, in the article [FLR09], we have defined a modular correspondence between abelian varieties in the moduli of marked abelian varieties. This moduli space is well-suited for computating modular correspondences since the associated modular polynomials have their coefficients in $\{1,-1\}$, and there is no explosion as before.

In this paper, we explain how, given a solution to this modular correspondence (provided for instance by the algorithm described in [FLR09]), one can compute the associated isogeny. Once such a modular point is obtained, the isogeny can be computed using only simple addition formulas of algebraic theta functions, so in practice, the computation of the isogeny takes

much less time than the computation of a point provided by the modular correspondence. Note that this is similar to the genus-one case. For elliptic curves, the computation of a root of the modular polynomial is not mandatory if the points in the kernel of the isogeny are given, since this is the input taken by Vélu's formulas. Here, we explain how to recover the equations of an isogeny given the points of its kernel, yielding a generalization of Vélu's formulas.

Our generalization introduces however a difference compared to the usual genus-1 case. For elliptic curves, the modular polynomial of order ℓ give the moduli space of ℓ-isogenous elliptic curves. In our generalized setting, the modular correspondence in the coordinate system of theta null points gives ℓ^g-isogenous abelian varieties with a theta structure of different level. As a consequence, a point in this modular space corresponds to an ℓ^g-isogeny, together with a symplectic structure of level ℓ. Another method would be to describe a modular correspondence between abelian varieties with theta structures of the same level, see [BGL09] for an example with $\ell = 3$ and $g = 2$.

The paper is organized as follow. In Section 2 we recall Vélu's formulas and outline our algorithms. In Section 3, we recall the definition of the modular correspondence given in [FLR09], and we study the relationship between isogenies and the action of the theta group. We recall the addition relations, which play a central role in this paper in Section 4. We then explain how to compute the isogeny associated to a modular point in Section 5. If the isogeny is given by theta functions of level 4ℓ, it requires $(4\ell)^g$ coordinates. We give a point compression algorithm in Section 5.1, showing how to express such an isogeny with only $g(g+1)/2 \cdot 4^g$ coordinates. In Section 6 we give a full generalization of Vélu's formulas that constructs an isogenous modular point with prescribed kernel. This algorithm is more efficient than the special Gröbner basis algorithm from [FLR09]. There is a strong connection between isogenies and pairings, and we use the above work to explain how one can compute the commutator pairing and how it relates to the usual Weil pairing in Section 7.

2 Computing Isogenies

In this section, we recall how one can compute isogenies between elliptic curves. We then outline our algorithm to compute isogenies between abelian varieties.

2.1 Elliptic curves and Vélu's formulas

Let $(E_k, \widetilde{0}_{E_k})$ be an elliptic curve given by a Weierstrass equation $y^2 = f(x)$ with f a degree-3 monic polynomial. Vélu's formulas rely on the intrinsic characterization of the coordinate system (x, y) giving the Weierstrass model of E_k as:

$$\begin{aligned} v_{\widetilde{0}_{E_k}}(x) &= -3 \qquad v_P(x) \geqslant 0 \quad \text{if } P \neq \widetilde{0}_{E_k} \\ v_{\widetilde{0}_{E_k}}(y) &= -2 \qquad v_P(y) \geqslant 0 \quad \text{if } P \neq \widetilde{0}_{E_k} \\ y^2/x^3(\widetilde{0}_{E_k}) &= 1, \end{aligned} \tag{1}$$

where v_Q denotes the valuation of the local ring of E_k in the closed point Q.

Theorem 2.1 (Vélu):
Let $G \subset E_k(k)$ be a finite subgroup. Then E_k/G is given by $Y^2 = g(X)$ with g a degree 3 monic polynomial where

$$X(P) = x(P) + \sum_{Q \in G \setminus \{\tilde{0}_{E_k}\}} x(P+Q) - x(Q)$$
$$Y(P) = y(P) + \sum_{Q \in G \setminus \{\tilde{0}_{E_k}\}} y(P+Q) - y(Q)$$

Proof: Indeed, X and Y are in $k(E_k)^G$, and it is easily seen that they satisfy the relations (1).■

A consequence of the that theorem is that, given a finite subgroup G of cardinality ℓ of an elliptic curve E_k an equation $y^2 = f(x)$ with f a degre 3 polynomial, it is possible to compute the Weierstrass equation of the quotient E_k/G at the cost of $O(\ell)$ additions in E_k.

The modular curve $X_0(\ell)$ parametrizes the set of isomorphism classes of elliptic curves together with a ℓ-torsion subgroup. For instance $X_0(1)$ is just the line of j-invariants. Let $\Phi_\ell(x,y) \in \mathbb{Z}[x,y]$ be the order ℓ modular polynomial. It is well known that the roots of $\Phi_\ell(j(E_k),\cdot)$ give the j-invariants of the elliptic curves ℓ-isogenous to E_k. Since an ℓ-isogeny is given by a finite subgroup of E_k of order ℓ, we see that $\Phi_\ell(x,y)$ cuts out a curve isomorphic to $X_0(\ell)$ in $X_0(1) \times X_0(1)$.

Given an elliptic curve E_k with j-invariant j_{E_k}, the computation of isogenies can be done in two steps:

- First, find the solutions of $\Phi_\ell(j_{E_k}, X)$ where $\Phi_\ell(X,Y)$ is the order ℓ modular polynomial; then recover from a root $j_{E'_k}$ the equation of the corresponding curve E'_k which is ℓ-isogenous to E_k.
- Next, using Vélu's formulas, compute the isogeny $E_k \to E'_k$.

For some applications such as isogeny-graph computation, only the first step is required, while for other applications it is necessary to obtain the explicit equations describing the isogeny. Note that the first step is unnecessary if one already know the points in the kernel of the isogeny.

2.2 Isogenies on abelian varieties

Let A_k be an abelian variety of dimension g over a field k and denote by $K(A_k)$ its function field. An isogeny is a finite surjective map of abelian varieties. In the following we only consider separable isogenies i.e. isogenies $\pi : A_k \to B_k$ such that the function field $K(A_k)$ is a finite separable extension of $K(B_k)$. A separable isogeny is uniquely determined by its kernel, which is a finite subgroup of $A_k(\overline{k})$. In that case, the cardinality of the kernel is the degree of the isogeny. In the rest of this paper, by ℓ-isogeny for $\ell > 0$, we always mean a $(\ell,\cdots,\ell)$-isogeny where $(\ell,\cdots,\ell) \in \mathbb{Z}^g$.

We have seen that it is possible to define a modular correspondence between the Igusa invariants, parameterizing the set of dimension 2 principally polarized abelian varieties, but the coefficients explosion of the related modular polynomials makes it computationally inefficient. In order to mitigate this problem and obtain formulas suitable for general g-dimensional abelian varieties, we use the moduli space of marked abelian varieties.

Let $g \in \mathbb{N}^*$ and let $n \in \mathbb{N}$ be such that $2|n$. Let $\overline{n} = (n, n, \ldots, n) \in \mathbb{Z}^g$, and $Z(\overline{n}) = \mathbb{Z}^g/n\mathbb{Z}^g$. We denote $\mathscr{M}_{\overline{n}}$ the modular space of marked abelian varieties $(A_k, \mathscr{L}, \Theta_{A_k})$ where $\mathscr{L}$ is a polarization and Θ_{A_k} is symmetric theta structure Θ_{A_k} of type $Z(\overline{n})$ (see [Mum66]). The forgetting map $(A_k, \mathscr{L}, \Theta_{A_k}) \mapsto (A_k, \mathscr{L})$ is a finite map from $\mathscr{M}_{\overline{n}}$ to the moduli space of abelian varieties with a polarization of type $Z(\overline{n})$.

We recall [Mum67a] that if $4|n$, then $\mathscr{M}_{\overline{n}}$ is open in the projective variety described by the following equations in $\mathbb{P}(k(Z(\overline{n})))$:

$$\begin{aligned}\Big(\sum_{t\in Z(\overline{2})} \chi(t) a_{x+t} a_{x+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) a_{u+t} a_{u+t}\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t) a_{z-x+t} a_{z-y+t}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) a_{z-u+t} a_{z-v+t}\Big) \qquad (2)\\ a_x = a_{-x}\end{aligned}$$

for all $x, y, u, v \in Z(\overline{n})$, such that $x + y + u + v = 2z$ and all $\chi \in \hat{Z}(\overline{2})$.

In [FLR09], we have described a modular correspondence $\varphi : \mathscr{M}_{\overline{\ell n}} \to \mathscr{M}_{\overline{n}} \times \mathscr{M}_{\overline{n}}$ for $\ell \in \mathbb{N}^*$, which can be seen as a generalization of the modular correspondence $X_0(\ell) \to X_0(1) \times X_0(1)$ for elliptic curves. Let p_1 and p_2 be the corresponding projections $\mathscr{M}_{\overline{n}} \times \mathscr{M}_{\overline{n}} \to \mathscr{M}_{\overline{n}}$, and let $\varphi_1 = p_1 \circ \varphi$, $\varphi_2 = p_2 \circ \varphi$. The map $\varphi_1 : \mathscr{M}_{\overline{\ell n}} \to \mathscr{M}_{\overline{n}}$ is such that $(x, \varphi_1(x))$ are modular points corresponding to ℓ-isogenous varieties We recall that φ_1 is defined by $\varphi_1\left((a_i)_{i\in Z(\overline{\ell n})}\right) = (a_i)_{i\in Z(\overline{n})}$ where $Z(\overline{n})$ is identified as a subgroup of $Z(\overline{\ell n})$ by the map $x \mapsto \ell x$.

Suppose that we are given a modular point $(b_i)_{i\in Z(\overline{n})}$ corresponding to the marked abelian variety $(B_k, \mathscr{L}_0, \Theta_{B_k})$. If B_k is the Jacobian variety of an hyperelliptic curve, one may recover the associated modular point for $n = 4$ via Thomae formulas [Mum84].

Suppose for now that $4|n$ and that ℓ is prime to n. Our algorithm works in two steps:

1. **Modular computation** Compute a modular point $(a_i)_{i\in Z(\overline{\ell n})} \in \varphi_1^{-1}\left((b_i)_{i\in Z(\overline{n})}\right)$. This can be done via the specialized Gröbner basis algorithm described in [FLR09], but see also Section 6 for a more efficient method.

2. **Vélu's like formulas** Use the addition formula in B_k to compute the isogeny $\hat{\pi} : B_k \to A_k$ associated to the modular point solution. Here $(A_k, \mathscr{L}, \Theta_{A_k})$ is the marked abelian variety corresponding to $(a_i)_{i\in Z(\overline{\ell n})}$. This step is described in Section 5.

We can also compute an isogeny given by its kernel K by using the results of Section 6.1 to construct the corresponding modular point $(a_i)_{i\in Z(\overline{\ell n})}$ from K. We thus have a complete generalization of Vélu's formulas for higher dimensional abelian varieties since the reconstruction of the modular point $(a_i)_{i\in Z(\overline{\ell n})}$ from the kernel K only requires the addition formulas

in B_k (together with the extraction of ℓ^{th}-roots). In Section 6.3 we explain how to use this to speed up Step 1 of our algorithm (we call this Step 1').

If the kernel of the isogeny is unknown, the most time-consuming part of our algorithm is the computation of a maximal subgroup of rank g of the ℓ-torsion, which means that currently, with $g = 2$ we can go up to $\ell = 31$ relying on the current state-of-the-art implementation [GS08]. In order to speed up Step 2, which requires $O(\ell^g)$ additions to be performed in B_k, and compute with a compact representation, it is important to consider the smallest possible n. If $n = 2$, we cannot prove that the modular system to be solved in Step 1 is of dimension 0. However Step 1', which is faster, does not require a modular solution but only the kernel of the isogeny, so our algorithm works with $n = 2$ too. Note, however, that some care must be taken when computing additions on B_k, since the algebraic theta functions only give an embedding of the Kummer variety of B_k for $n = 2$.

For an actual implementation the case $n = 2$ is critical (it allows for a more compact representation of the points than $n = 4$: we gain a factor 2^g, it allows for a faster addition chain, see Section 5.1.1, but most importantly it reduces the most consuming part of our algorithm, the computation of the points of ℓ-torsion, since there are half as much such points on the Kummer variety). For each algorithm that we use, we give an explanation on how to adapt it for the level 2 case: see Section 4.2.1 and the end of Sections 5.2, 6.1, 6.3 and 7.2.

The assumption that n is prime to ℓ is not necessary either but there is one important difference in this case. Suppose that we are given $B_k[\ell]$. Since B_k is given by a theta structure of level n, we also have $B_k[n]$. If ℓ is prime to n, this gives us $B_k[\ell n]$, and we can use Step 1' to reconstitute a modular point of level ℓn. If ℓ is not prime to n, we have to compute $B_k[\ell n]$ directly.

It is also possible to compute more general types of isogenies via our algorithm. With the notations of Section 3, let $\delta_0 = (\delta_1, \dots, \delta_g)$ be a sequence of integers such that $\delta_i | \delta_{i+1}$, and let $(b_i)_{i \in Z(\delta_0)} \in \mathcal{M}_{\delta_0}$ be a modular point corresponding to an abelian variety B_k. Let $\delta' = (\ell_1, \dots, \ell_g)$ (where $\ell_i | \ell_{i+1}$) and define $\delta = (\delta_1 \ell_1, \dots, \delta_g \ell_g)$. Let $(a_i)_{i \in Z(\delta)} \in \mathcal{M}_\delta$ be such that $\varphi\left((a_i)_{i \in Z(\delta)}\right) = (b_i)_{i \in Z(\delta_0)}$. The theta null point $(a_i)_{i \in Z(\delta)}$ corresponds to an abelian variety A_k, such that there is a $(\ell_1, \cdots, \ell_g)$-isogeny $\pi : A_k \to B_k$, which can be computed by the isogeny theorem [Mum66] (see Section 3.2). The isogeny we compute in Step 2 is the contragredient isogeny $\hat{\pi} : B_k \to A_k$ of type $(\ell_g/\ell_1, \ell_g/\ell_2, \cdots, 1, \ell_g, \ell_g, \cdots, \ell_g)$. Using the modular correspondence φ to go back to a modular point of level δ_0 (see Section 3.3) gives an isogeny of type $(\ell_g/\ell_1, \ell_g/\ell_2, \cdots, 1, \ell_1\ell_g, \ell_2\ell_g, \cdots, \ell_g\ell_g)$. For the clarity of the exposition, we will stick to the case $\delta_0 = \overline{n}$ and $\delta = \overline{\ell n}$ and we leave to the reader the easy generalization.

Let us make some remarks on our algorithm. First note that to compute ℓ-isogenies, we start from a theta null point of level n to get a theta null point of level ℓn. We can then go back to a point of level n (see Section 3.3), but in this case we are computing ℓ^2-isogenies. A second remark is that all our computations are geometric, not arithmetic, since the projective embedding given by theta functions of level ℓn is not rational. A last remark is that since we use different moduli spaces, our method is not a straight-up generalization of the genus-1 case. In particular, computing a modular point solution $(a_i)_{i \in Z(\overline{\ell n})}$ is the same as choosing an ℓ-isogeny **and** a theta structure of level ℓ, so there are many more modular solutions than there is ℓ-isogenies. Hence, as noted in the introduction, the most efficient method in our

cases is to compute the points of ℓ-torsion to reconstitute the modular point.

3 Modular correspondences and theta null points

In this section, we recall some results of [FLR09] and notations that we will use in the rest of the paper. In Section 3.1 we recall the definition of a theta structure and the associated theta functions [Mum66]. In Section 3.2 we recall the isogeny theorem, which give a relations between the theta functions of two isogenous abelian varieties. In Section 3.3 we explain the modular correspondence defined in [FLR09]. In Section 3.4 we study the connection between isogenies and the action of the theta group.

3.1 Theta structures

Let A_k be a g dimensional abelian variety over a field k. Let $\mathscr{L}$ be a degree-d ample symmetric line bundle on A_k. We suppose that d is prime to the characteristic of k or that A_k is ordinary. Denote by $K(\mathscr{L})$ the kernel of the isogeny $\varphi_{\mathscr{L}} : A_k \to \hat{A}_k$, defined on geometric points by $x \mapsto \tau_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ where τ_x is the translation by x. Let $\delta = (\delta_1, \ldots, \delta_g)$ be the sequence of integers satisfying $\delta_i | \delta_{i+1}$ such that, as group schemes $K(\mathscr{L}) \simeq \bigoplus_{i=1}^g (\mathbb{Z}/\delta_i\mathbb{Z})_k^2$. We say that δ is the type of $\mathscr{L}$. In the following we let $Z(\delta) = \bigoplus_{i=1}^g (\mathbb{Z}/\delta_i\mathbb{Z})_k$, $\hat{Z}(\delta)$ be the Cartier dual of $Z(\delta)$, and $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$.

Let $G(\mathscr{L})$ and $\mathscr{H}(\delta)$ be respectively the theta group of $(A_k, \mathscr{L})$ and the Heisenberg group of type δ [Mum66]. In this article, elements of $G(\mathscr{L})$ will be written as (x, ψ_x) with $x \in K(\mathscr{L})$ and $\psi_x : \mathscr{L} \to \tau_x^*\mathscr{L}$ is an isomorphism. We know that $G(\mathscr{L})$ and $\mathscr{H}(\delta)$ are central extensions of $K(\mathscr{L})$ and $K(\delta)$ by $\mathbb{G}_m$. By definition, a theta structure Θ_{A_k} on $(A_k, \mathscr{L})$ is an isomorphism of central extensions from $\mathscr{H}(\delta)$ to $G(\mathscr{L})$. We denote by $e_{\mathscr{L}}$ the commutator pairing [Mum66] on $K(\mathscr{L})$ and by $e_{c,\delta}$ the canonical pairing on $Z(\delta) \times \hat{Z}(\delta)$ (We often drop the indice δ in e_δ when there is no risk of confusion). We remark that a theta structure Θ_{A_k} induces a symplectic isomorphism $\overline{\Theta}_{A_k}$ from $(K(\delta), e_{c,\delta})$ to $(K(\mathscr{L}), e_{\mathscr{L}})$. We denote by $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ the decomposition into maximal isotropic subspaces induced by $\overline{\Theta}_{A_k}$. The sections $Z(\delta) \to \mathscr{H}(\delta)$ and $\hat{Z}(\delta) \to \mathscr{H}(\delta)$ defined on geometric points by $x \mapsto (1, x, 0)$ and $y \mapsto (1, 0, y)$ can be transported by the theta structure to obtain natural sections $s_{K_1(\mathscr{L})} : K_1(\mathscr{L}) \to G(\mathscr{L})$ and $s_{K_2(\mathscr{L})} : K_2(\mathscr{L}) \to G(\mathscr{L})$ of the canonical projection $\varkappa : G(\mathscr{L}) \to K(\mathscr{L})$. Recall [Mum66, pp. 291] that a level subgroup $\widetilde{K}$ of $G(\mathscr{L})$ is a subgroup such that $\widetilde{K}$ is isomorphic to its image by $\varkappa$. We define the maximal level subgroups $\widetilde{K}_1$ over $K_1(\mathscr{L})$ and $\widetilde{K}_2$ over $K_2(\mathscr{L})$ as the image by Θ_{A_k} of the subgroups $(1, x, 0)_{x \in Z(\delta)}$ and $(1, 0, y)_{y \in \hat{Z}(\delta)}$ of $\mathscr{H}(\delta)$.

Let $V = \Gamma(A_k, \mathscr{L})$. The theta group $G(\mathscr{L})$ acts on V by $v \mapsto \psi_x^{-1}\tau_x^*(v)$ for $v \in V$ and $(x, \psi_x) \in G(\mathscr{L})$. This action can be transported via Θ_{A_k} to an action of $\mathscr{H}(\delta)$ on V. It can be shown that there is a unique (up to a scalar factors) basis $(\vartheta_i)_{i \in Z(\delta)}$ of V such that this action is given by:

$$(\alpha, i, j).\vartheta_h^{\Theta_{A_k}} = \alpha.e_{c,\delta}(-i-h, j).\vartheta_{h+i}^{\Theta_{A_k}}. \tag{3}$$

(see [Mum67b, BL04] for a connection between algebraic theta functions and the classical, analytic theta functions.) If there is no ambiguity, in this paper, we will sometimes drop the superscript Θ_{A_k} in the notation $\vartheta_k^{\Theta_{A_k}}$. We briefly recall the construction of this basis: let A_k^0 be the quotient of A_k by $K_2(\mathscr{L})$ and $\pi : A_k \to A_k^0$ be the natural projection. By Grothendieck descent theory, the data of $\widetilde{K}_2$ is equivalent to the data of a couple $(\mathscr{L}_0, \lambda)$ where $\mathscr{L}_0$ is a degree-one ample line bundle on A_k^0 and λ is an isomorphism $\lambda : \pi^*(\mathscr{L}_0) \to \mathscr{L}$. Let s_0 be the unique global section of $\mathscr{L}_0$ up to a constant factor and let $s = \lambda(\pi^*(s_0))$. We have the following proposition (see [Mum66])

Proposition 3.1:
For all $i \in Z(\delta)$, let $(x_i, \psi_i) = \Theta_{A_k}((1, i, 0))$. We set $\vartheta_i^{\Theta_{A_k}} = (\psi_x^{-1}\tau_x^*(s))$. The elements $(\vartheta_i^{\Theta_{A_k}})_{i\in Z(\delta)}$ form a basis of the global sections of $\mathscr{L}$; it is uniquely determined (up to a multiplicative factor independent of i) by Θ_{A_k}.

This basis gives a projective embedding $\varphi_{\Theta_{A_k}} : A_k \to \mathbb{P}_k^{d-1}$ which is uniquely defined by the theta structure Θ_{A_k}. The point $(a_i)_{i\in Z(\delta)} := \varphi_{\Theta_{A_k}}(0_{A_k})$ is called the theta null point associated to the theta structure. Mumford proves [Mum66] that if $4|\delta$, $\varphi_{\Theta_{A_k}}(A_k)$ is the closed subvariety of $\mathbb{P}_k^{d-1}$ defined by the homogeneous ideal generated by the Riemann equations:

Theorem 3.2 (Riemann equations):
For all $x, y, u, v \in Z(2\delta)$ that are congruent modulo $Z(\bar{2})$, and all $\chi \in \hat{Z}(\bar{2})$, we have

$$\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{x+y+t}\vartheta_{x-y+t}\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)a_{u+v+t}a_{u-v+t}\Big) = \\ = \Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{x+u+t}\vartheta_{x-u+t}\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)a_{y+v+t}a_{y-v+t}\Big). \quad (4)$$

Let $p_{\mathbb{A}_k(V)} : \mathbb{A}_k(V) \to \mathbb{P}_k(V)$ be the canonical projection. Let $\widetilde{A}_k = p_{\mathbb{A}_k(V)}^{-1}(A_k)$ be the affine cone of A_k and denote by $p_{A_k} : \widetilde{A}_k \to A_k$, the application induced by $p_{\mathbb{A}_k(V)}$. Since this affine cone will play a central role in this paper, we take the following convention: if $(\vartheta_i)_{i\in Z(\delta)}$ is a homogeneous coordinate system on $\mathbb{P}(V)$ then we denote by $(\widetilde{\vartheta}_i)_{i\in Z(\delta)}$ the associated affine coordinate system of $\mathbb{A}(V)$. For instance, p_{A_k} is given by $(\widetilde{\vartheta}_i(x))_{i\in Z(\delta)} \mapsto (\vartheta_i(x))_{i\in Z(\delta)}$. It should be remarked that, for $i \in Z(\delta)$, $\widetilde{\vartheta}_i$ is a well defined function on $\widetilde{A}_k$ and for any geometric point $x \in \widetilde{A}_k$, we denote by $\widetilde{\vartheta}_i(x)$ its values in x.

Since the action of $G(\mathscr{L})$ on V is affine, the action (3) gives an action $\widetilde{\rho}_{\mathscr{L}}^*$ on $\widetilde{A}_k$. This action descends to a projective action $\rho_{\mathscr{L}}^*$ of $K(\mathscr{L})$ on A_k which is simply the action by translation. We will use the same notations for the action of $\mathscr{H}(\delta)$ (resp. of $K(\delta)$) induced by Θ_{A_k}.

3.2 Isogenies compatible with a theta structure

Let $\delta' \in \mathbb{Z}^g$ be such that $2|\delta'|\delta$, and write $\delta = \delta' \cdot \delta''$. In the following we consider $Z(\delta')$ as a subgroup of $Z(\delta)$ via the map $\varphi : (x_i)_{i\in[1..g]} \in Z(\delta') \mapsto (\delta''_i x_i)_{i\in[1..g]} \in Z(\delta)$. From now on, when we write $Z(\delta') \subset Z(\delta)$, we always refer to this map. Let K be the subgroup $\overline{\Theta}_{A_k}(\hat{Z}(\delta''))$ of $K_2(\mathscr{L})$ and let π_K be the isogeny $A_k \to B_k = A_k/K$. By Grothendieck descent theory, the level subgroup $\widetilde{K} := s_{K_2(\mathscr{L})}(K)$ induces a polarization $\mathscr{L}_0$ on B_k, such that $\mathscr{L} \simeq \pi_K^*(\mathscr{L}_0)$. The theta group $G(\mathscr{L}_0)$ is isomorphic to $\mathscr{Z}(\widetilde{K})/\widetilde{K}$ where $\mathscr{Z}(\widetilde{K})$ is the centralizer of $\widetilde{K}$ in $G(\mathscr{L})$ [Mum66]. Let Θ_{B_k} be the unique theta structure on B_k compatible with the theta structure on A_k [FLR09, Sec. 3]. We have [FLR09, Prop. 4]:

Proposition 3.3 (Isogeny theorem for compatible theta structures): *Let $\varphi : Z(\delta') \to Z(\delta)$ be the canonical embedding. Let $(\vartheta_i^{\Theta_{A_k}})_{i\in Z(\delta)}$ (resp. $(\vartheta_i^{\Theta_{B_k}})_{i\in Z(\delta')}$) be the canonical basis of $\mathscr{L}$ (resp. $\mathscr{L}_0$) associated to Θ_{A_k} (resp. Θ_{B_k}). There exists some $\omega \in \overline{k}^*$ such that for all $i \in Z(\delta')$*

$$\pi_K^*(\vartheta_i^{\Theta_{A_k}}) = \omega \vartheta_{\varphi(i)}^{\Theta_{B_k}}. \tag{5}$$

In particular, the theta null point of B_k is given by

$$(b_i)_{i\in Z(\delta')} = (a_{\varphi(i)})_{i\in Z(\delta')} \tag{6}$$

The above proposition is a particular case of the more general isogeny theorem [Mum66, Th. 4].

On the affine cones this proposition shows that, given the theta null point $(a_i)_{i\in Z(\delta)}$, the morphism

$$\begin{aligned} \widetilde{\pi}_K : \widetilde{A}_k &\to \widetilde{B}_k \\ (\widetilde{\vartheta})_{i\in Z(\delta)} &\mapsto (\widetilde{\vartheta})_{i\in\varphi(Z(\delta'))} \end{aligned}$$

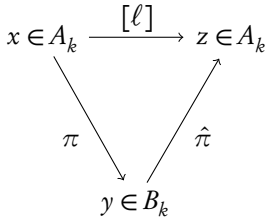
makes the following diagram commutative:

$$\begin{array}{ccc} \widetilde{A}_k & \xrightarrow{p_{A_k}} & A_k \\ \downarrow{\scriptstyle \widetilde{\pi}} & & \downarrow{\scriptstyle \pi} \\ \widetilde{B}_k & \xrightarrow{p_{B_k}} & B_k \end{array}$$

For the sake of simplicity, we set from now on $\delta_0 = \overline{n}$, and $\delta' = \overline{\ell}$ so that $\delta = \overline{\ell n}$ (we stated Proposition (3.3) in a more general form because we can use it to compute the ℓ-torsion on B_k, see Section 6.3). Let $(b_i)_{i\in Z(\overline{n})}$ be a theta null point associated to a triple $(B_k, \mathscr{L}_0, \Theta_{B_k})$; we want to compute an ℓ-isogeny $B_k \to A_k$. Since n is fixed, we cannot apply the isogeny theorem directly since it requires $\ell|n$. However, if $(a_i)_{i\in Z(\overline{\ell n})} \in \mathscr{M}_{\overline{\ell n}}$ is a theta null point

corresponding to a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ where the theta structure Θ_{A_k} is compatible with Θ_{B_k} (this is equivalent to $(a_i)_{i\in Z(\overline{\ell n})}$ satisfying (6)), then Proposition 3.3 gives an (explicit) isogeny $\pi : A_k \to B_k$. So to the modular point $(a_i)_{i\in Z(\overline{\ell n})}$ we may associate the isogeny $\hat{\pi} : B_k \to A_k$ and this is the isogeny we compute in Step 2 of our algorithm (Section 2.2).

We have the following diagram



This diagram shows that it is possible to obtain an explicit description of the rational map $z = \hat{\pi}(y)$ by eliminating the variables x in the ideal generated by $(y = \pi(x), z = \ell \cdot x)$. This can be done using a Gröbner basis algorithm. In Section 5 gives a much faster algorithm which uses the addition formulas in B_k to find the equations of $\hat{\pi}$ directly.

3.3 Modular correspondences

In the previous section, we have shown how to compute an isogeny with a prescribed kernel $K \subset K_2(\mathscr{L})[\ell]$ that is isotropic for the commutator pairing. Now let $K \subset A_k[\ell]$ be any isotropic subgroup such that we can write $K = K_1 \times K_2$ with $K_i \subset K_i(\mathscr{L})$. Let $B_k = A_k/K$ and π be the associated isogeny. Let Θ_{B_k} and Θ_{A_k} be π-compatible theta structures in the sense of Mumford [Mum66]. We briefly explain this notion: if two abelian varieties $(A_k, \mathscr{L}, \Theta_{A_k})$ and $(B_k, \mathscr{L}_0, \Theta_{B_k})$ have π-compatible marked theta structures, it means that we have $\pi^*(\mathscr{L}_0) = \mathscr{L}$. By Grothendieck descent theory, this define a level subgroup $\widetilde{K} \subset G(\mathscr{L})$ of the kernel of π. We have seen in Section 3.2 that we have $G(\mathscr{L}_0) = \mathscr{Z}(\widetilde{K})/\widetilde{K}$ where $\mathscr{Z}(\widetilde{K})$ is the centralizer of $\widetilde{K}$. The structures Θ_{A_k} and Θ_{B_k} are said to be compatible if they respect this isomorphism. The isogeny theorem ([Mum66, Theorem 4]) then gives a way to compute $(\pi^*(\vartheta_i^{\Theta_{B_k}}))_{i\in Z(\overline{n})}$ given $(\vartheta_i^{\Theta_{A_k}})_{i\in Z(\overline{\ell n})}$.

We recall briefly how this works: if $K_1 = 0$, we say that π is an isogeny of type 1, and if $K_2 = 0$ that π is an isogeny of type 2. In the paper [FLR09] we have studied the case of isogenies of type 1 and 2; in fact, the notion of compatible isogenies we had defined in these cases is nothing but a particular case of the notion of compatible isogenies described above. Obviously, by composing isogenies, we only need to study the case of compatible theta structures between isogenies of type 1 or 2. We have already seen the case of isogenies of type 1 in the previous Section. Now let $\mathfrak{I}_0$ be the automorphism of the Heisenberg group $\mathscr{H}(\overline{\ell n})$ that permutes $Z(\overline{\ell n})$ and $\hat{Z}(\overline{\ell n})$: $\mathfrak{I}_0(\alpha, x, y) = (\alpha, y, x)$. We define $\mathfrak{I}_{A_k} = \Theta_{A_k} \circ \mathfrak{I}_0 \circ \Theta_{A_k}^{-1}$, where $\mathfrak{I}_{A_k}$ is the automorphism of the Theta group of A_k that permutes $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$. (There is a similar automorphism $\mathfrak{I}_{B_k}$ of the theta group of B_k; we will usually note these

automorphisms $\mathfrak{I}$ since the theta group is clear from the context.) If π_2 is a compatible isogeny of type 2 between $(A_k, \mathscr{L}, \Theta_{A_k})$ and $(B_k, \mathscr{L}_0, \Theta_{B_k})$, then π_2 is a compatible isogeny of type 1 between $(A_k, \mathscr{L}, \mathfrak{I}_{A_k} \circ \Theta_{A_k})$ and $(B_k, \mathscr{L}, \mathfrak{I}_B \circ \Theta_{B_k})$.

Since the action of $\mathfrak{I}$ is given by [FLR09, Section 5]

$$\vartheta_i^{\mathfrak{I}_{A_k} \circ \Theta_{A_k}} = \sum_{j \in \hat{Z}(\overline{\ell n})} e(i,j) \vartheta_j^{\Theta_{A_k}}, \tag{7}$$

we see that we have for all $i \in Z(\overline{n})$

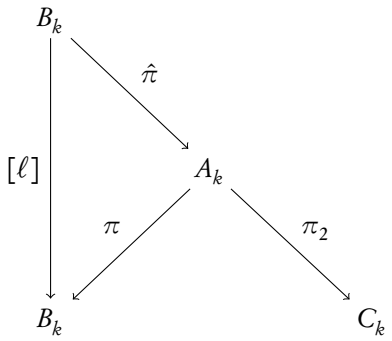
$$\pi^*(\vartheta_i^{\Theta_{B_k}}) = \sum_{j \in Z(\overline{\ell})} \vartheta_{i+nj}^{\Theta_{A_k}}.$$

In the following, we focus on isogenies of type 1 but it is easy to adapt the following to isogenies of type 2 (and hence more generally to compatible isogenies between theta structures) using the action of $\mathfrak{I}$. Considering both types of isogenies can be useful, see Section 4.3 or Section 6.3. The modular correspondence described in Section 2.2 is given by

$$\varphi : \mathscr{M}_{\overline{\ell n}} \to \mathscr{M}_{\overline{n}} \times \mathscr{M}_{\overline{n}}, (a_i)_{i \in Z(\overline{\ell n})} \mapsto ((a_i)_{i \in Z(\overline{n})}, (\sum_{j \in Z(\overline{\ell})} a_{i+nj})_{i \in Z(\overline{n})}).$$

Let φ_1 (resp. φ_2) be the composition of φ with the first (resp. second) projection. Let $(a_i)_{i \in Z(\overline{\ell n})}$ be the theta null point of $(A, \mathscr{L}, \Theta_{A_k})$, and put $(b_i)_{i \in Z(\overline{\ell})} = \varphi_1\left((a_i)_{i \in Z(\overline{\ell})}\right)$, and $(c_i)_{i \in Z(\overline{\ell})} = \varphi_2\left((a_i)_{i \in Z(\overline{\ell})}\right)$. Then $(b_i)_{i \in Z(\overline{\ell})}$ is the theta null point corresponding to the variety $B_k = A_k / K_2(\mathscr{L})[\ell]$, and $(c_i)_{i \in Z(\overline{\ell})}$ corresponds to $C_k = A_k / K_1(\mathscr{L})[\ell]$.

The following diagram shows that the composition $\pi_2 \circ \hat{\pi} : B_k \to C_k$ is an ℓ^2-isogeny:



3.4 The action of the theta group on the affine cone and isogenies

For the rest of the article, we suppose given an abelian variety with a theta structure $(B_k, \mathscr{L}_0, \Theta_{B_k})$ with associated theta null point $(b_i)_{i \in Z(\overline{n})}$, and a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$

associated to a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ such that Θ_{B_k} and Θ_{A_k} are compatible [FLR09]. Let $\widetilde{\pi} : \widetilde{A}_k \to \widetilde{B}_k$ be the morphism such that $\pi^*(\vartheta_i^{\Theta_{B_k}}) = \vartheta_i^{\Theta_{A_k}}$ for $i \in Z(\overline{n})$. Note that the isogeny $\pi : A_k \to B_k$ lifts to the affine cone as $\widetilde{\pi}$.

Let $\{e_i\}_{i\in[1..g]}$ be the canonical "basis" of $Z(\overline{\ell n})$, and $\{f_i\}_{i\in[1..g]}$ be the canonical "basis" of $\hat{Z}(\overline{\ell n})$ so that $\{e_i, f_i\}_{i\in[1..g]}$ is the canonical symplectic basis of $K(\overline{\ell n})$. For $i \in Z(\overline{\ell n})$, we let $P_i = \overline{\Theta}_{A_k}(i, 0))$ and for $i \in \hat{Z}(\overline{\ell n})$ we let $Q_i = \overline{\Theta}_{A_k}(0, i)$. The points $\left\{P_{e_i}, Q_{f_i}\right\}_{i\in[1..g]}$ form a symplectic basis of $K(\mathscr{L})$ for the commutator pairing induced by the theta structure: we have for $i, j \in [1..g]$ $e_{\mathscr{L}}(P_{e_i}, Q_{f_j}) = \delta^i_j$ where δ^i_j is the Kronecker symbol.

We have seen (see Section 3.1) that the theta structure Θ_{A_k} induces a section $s = s_{K(\mathscr{L})} : K(\mathscr{L}) \to G(\mathscr{L})$ of the canonical projection $x : G(\mathscr{L}) \to K(\mathscr{L})$. The kernel K_π of the isogeny $\pi : A_k \to B_k$ is $\overline{\Theta}_{A_k}(\hat{Z}(\overline{\ell}))$. Let $\widetilde{K}_\pi = s(K_\pi)$ and recall (see Section 3.2) that $G(\mathscr{L}_0) = \mathscr{Z}(\widetilde{K}_\pi)/\widetilde{K}_\pi$. In particular, we have $K(\mathscr{L}_0) = \mathscr{Z}(K_\pi)/K_\pi$ where $\mathscr{Z}(K_\pi) = x(\mathscr{Z}(\widetilde{K}_\pi))$ is the orthogonal of K_π for the commutator pairing $e_{\mathscr{L}}$. Explicitly, we have: $K_\pi = \{Q_i\}_{i\in Z(\overline{\ell})}$ and $\mathscr{Z}(K_\pi) = \{P_i\}_{i\in Z(\overline{n})} \times \{Q_i\}_{i\in Z(\overline{\ell n})}$ so that $K(\mathscr{L}_0) = \{\pi(P_i)\}_{i\in Z(\overline{n})} \times \pi(\{Q_i\}_{i\in Z(\overline{\ell n})})$.

In the following, if X_k is an abelian variety, we denote by $\mathrm{Aut}^*(X_k)$ the group of isomorphisms of X_k seen as an algebraic variety, in particular an element of $\mathrm{Aut}^*(X_k)$ does not necessarily fix the point 0 of X_k. The action by translation $\rho^*_{\mathscr{L}} : K(\mathscr{L}) \to \mathrm{Aut}^*(A_k)$ induces an action $\rho^*_{\mathscr{L}} : K(\mathscr{L}) \to \mathrm{Aut}^*(B_k)$ via π: if $x \in K(\mathscr{L})$, the action of $\rho^*_{\mathscr{L}}(x)$ on B_k is the translation by $\pi(x)$. This action extends the action by translation $\rho^*_{\mathscr{L}_0} : K(\mathscr{L}_0) \to \mathrm{Aut}^*(B_k)$. We recall that the action of $G(\mathscr{L})$ on $V = \Gamma(A_k, \mathscr{L})$ is given by $(x, \psi_x).v = \psi_x^{-1}\tau_x^*(v)$ for $(x, \psi_x) \in G(\mathscr{L})$ and $v \in V$ from which we derive an action of $G(\mathscr{L})$ on $\mathbb{A}_k(V)$. By restriction, we obtain an action $\widetilde{\rho}^*_{\mathscr{L}} : G(\mathscr{L}) \to \mathrm{Aut}^*(\widetilde{A}_k)$. Similarly, we define an action $\widetilde{\rho}^*_{\mathscr{L}_0} : G(\mathscr{L}_0) \to \mathrm{Aut}^*(\widetilde{B}_k)$. (Note that $\widetilde{\pi}$ does not induce an action from $G(\mathscr{L})$ on $\widetilde{B}_k$ via $\widetilde{\rho}^*_{\mathscr{L}}$; see Corollary 3.5). Still, we would like to be able to recover $\widetilde{\rho}^*_{\mathscr{L}}$ from $\widetilde{\rho}^*_{\mathscr{L}_0}$ and the theta structure Θ_{B_k}. First, we have:

Proposition 3.4:
Let $g \in \mathscr{Z}(\widetilde{K}_\pi)$ and note $\overline{g}$ its image in $\mathscr{Z}(\widetilde{K}_\pi)/\widetilde{K}_\pi$. We have $\widetilde{\rho}^*_{\mathscr{L}_0}(\overline{g}) = \widetilde{\pi} \circ \widetilde{\rho}_{\mathscr{L}}(g)$.

Proof: This is as an immediate consequence of the fact that the two theta structures Θ_{A_k} and Θ_{B_k} are compatible. ■

For $g \in G(\mathscr{L})$, we can define a mapping $\widetilde{\pi}_g : \widetilde{A}_k \to \widetilde{B}_k$ given on geometric points by $\widetilde{x} \mapsto \widetilde{\pi}(\widetilde{\rho}^*_{\mathscr{L}}(g).\widetilde{x})$. If $g \in \mathscr{Z}(\widetilde{K}_\pi)$; Proposition 3.4 then shows that $\widetilde{\pi}_g = \widetilde{\rho}^*_{\mathscr{L}_0}(\overline{g}) \circ \widetilde{\pi}$, hence $\widetilde{\pi}_g$ can be recovered from $\widetilde{\pi}$ and the theta structure Θ_{B_k}. Since $\mathscr{Z}(\widetilde{K}_\pi) \supset s(K_2(\mathscr{L}))$, we only have to study the mappings $\widetilde{\pi}_i = \widetilde{\pi}_{s(P_i)}$ for $i \in Z(\overline{\ell n})$. They are given on geometric points by

$$\widetilde{\pi}_i((\widetilde{\vartheta}_j(\widetilde{x}))_{j\in Z(\overline{\ell n})}) = (\widetilde{\vartheta}_{i+\ell.j}(\widetilde{x}))_{j\in Z(\overline{n})}.$$

Corollary 3.5:

1. *Let $\mathcal{S}$ be a subset of $Z(\overline{\ell n})$, such that $\mathcal{S} + Z(\overline{n}) = Z(\overline{\ell n})$. Then $\widetilde{x} \in \widetilde{A}_k$ is uniquely determined by $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathcal{S}}$.*

2. *Let $\widetilde{y} \in \widetilde{A}_k$ be such that $\widetilde{\pi}(\widetilde{y}) = \widetilde{\pi}(\widetilde{x})$. Then there exists $j \in \hat{Z}(\overline{\ell}) \subset \hat{Z}(\overline{\ell n})$ such that $\widetilde{y} = (1, 0, j).\widetilde{x}$ and*
$$\widetilde{\pi}_i(\widetilde{y}) = e_{\overline{\ell n}}(i, j)\widetilde{\pi}_i(\widetilde{x}).$$
In particular $\widetilde{\pi}_i(\widetilde{y})$ and $\widetilde{\pi}_i(\widetilde{x})$ differ by an ℓ^{th}-root of unity.

Proof:

1. Since $\widetilde{\pi}_i((\widetilde{\vartheta}_j(\widetilde{x}))_{j\in Z(\overline{\ell n})}) = (\widetilde{\vartheta}_{i+\ell.j}(\widetilde{x}))_{j\in Z(\overline{n})}$, from $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathcal{S}}$ one can obtain the values $\left\{\widetilde{\vartheta}_j(\widetilde{x})\right\}_{j\in\mathcal{S}+Z(\overline{n})}$. If $\mathcal{S} + Z(\overline{n}) = Z(\overline{\ell n})$ this shows that we can recover $\widetilde{x} = (\widetilde{\vartheta}_j(\widetilde{x}))_{j\in Z(\overline{\ell n})}$.

2. If $\widetilde{\pi}(\widetilde{y}) = \widetilde{\pi}(\widetilde{x})$, then $p_{A_k}(\widetilde{y}) - p_{A_k}(\widetilde{x}) \in K_\pi$. So there exists $j \in \hat{Z}(\overline{\ell})$ and $\alpha \in \overline{k}^*$ such that $\widetilde{y} = (\alpha, 0, j).\widetilde{x}$. Hence $\widetilde{\vartheta}_i(\widetilde{y}) = \alpha e_{\overline{\ell n}}(i, j)\widetilde{\vartheta}_i(\widetilde{x})$. Since $\widetilde{\pi}(\widetilde{x}) = \widetilde{\pi}(\widetilde{y})$, $\alpha = 1$. Moreover, as $j \in \hat{Z}(\overline{\ell})$, $e_{\overline{\ell n}}(i + k, j) = e_{\overline{\ell n}}(i, j)$ if $k \in Z(\overline{n})$ so that $\widetilde{\pi}_i(\widetilde{x}) = e_{\overline{\ell n}}(i, j)\widetilde{\pi}_i(\widetilde{y})$. ■

Example 3.6:

- If ℓ is prime to n, the canonical mappings $Z(\overline{n}) \to Z(\overline{\ell n})$ and $Z(\overline{\ell}) \to Z(\overline{\ell n})$ induce an isomorphism $Z(\overline{n}) \times Z(\overline{\ell}) \xrightarrow{\sim} Z(\overline{\ell n})$, and one can take $\mathcal{S} = Z(\overline{\ell})$ in Corollary 3.5.
- If ℓ is not prime to n, a possible choice for $\mathcal{S}$ is
$$\mathcal{S} = \{\sum_{i\in[1..g]} \lambda_i e_i | \lambda_i \in [0..\ell - 1]\}.$$

4 The addition relations

In this section we study the addition relations and introduce the notion of addition chain on the affine cone of an abelian variety. This chain addition will be our basic tool for our isogenies computation in Section 5 and Vélu's like formula in Section 6.

In Section 4.1 we introduce the concept of extended commutator pairing. The importance of this pairing comes from the fact that the isogenies we compute with our algorithm (see Section 2.2) correspond to subgroups that are isotropic for this extended commutator pairing [FLR09]. We explain in Section 7 how to use addition chains to compute this pairing. In Section 4.2 we prove in an algebraic setting the Riemann relations, and we deduce from them the addition relations. In Section 4.3 we use the results of Section 3.4 to study the properties of the addition chain.

4.1 Evaluation of algebraic theta functions at points of ℓ-torsion

For the rest of this article, we suppose that we have fixed a $\widetilde{0}_{B_k} \in p_{B_k}^{-1}(0_{B_k})$. This give us a canonical way to fix an affine lift of 0_{A_k}: we denote $\widetilde{0}_{A_k}$ the unique point in $p_{A_k}^{-1}(0_{A_k})$ such that $\widetilde{0}_{B_k} = \widetilde{\pi}(\widetilde{0}_{A_k})$. We recall that the theta structure Θ_{A_k} gives a section $s_{K(\mathscr{L})} : K(\mathscr{L}) \to G(\mathscr{L})$. This means that the map $x \in K(\mathscr{L}) \mapsto s_{K(\mathscr{L})}(x).\widetilde{0}_{A_k} \in \widetilde{A}_k$ induces a section $K(\mathscr{L}) \to \widetilde{A}_k$ of the map $p_{A_k} : \widetilde{A}_k \to A_k$. We remark that the choice of $\widetilde{0}_{A_k} \in p_{A_k}^{-1}(0_{A_k}) \subset \widetilde{A}_k$ is equivalent to the choice of an evaluation isomorphism: $\varepsilon_0 : \mathscr{L}(0) \simeq k$. For any $x \in K(\mathscr{L})$, let $s_{\mathscr{L}}(x) = (x, \psi_x)$, we define $\widetilde{\vartheta}_i(x) = \varepsilon_0(s_{\mathscr{L}}(x).\vartheta_i) = \varepsilon_0 \circ \psi_x^{-1} \circ \tau_x^*(\vartheta_i)$. Then the section $K(\mathscr{L}) \to \widetilde{A}_k$ is given by:

$$s_{K(\mathscr{L})}(x).\widetilde{0}_{A_k} = (\widetilde{\vartheta}_i(x))_{i \in Z(\overline{\ell n})}.$$

Thus we have a canonical way to fix an affine lift for any geometric point in $K(\mathscr{L})$. For $i \in Z(\overline{\ell n})$, let $\widetilde{P}_i = (1, i, 0).\widetilde{0}_{A_k}$, and for $j \in \hat{Z}(\overline{\ell n})$, let $\widetilde{Q}_j = (1, 0, j).\widetilde{0}_{A_k}$. We also put $\widetilde{R}_i = \widetilde{\pi}(\widetilde{P}_i) = \widetilde{\pi}_i(\widetilde{0}_{A_k})$, and $R_i = p_{B_k}(\widetilde{R}_i)$. We remark that $\{R_i\}_{i \in Z(\bar{\ell})}$ is the kernel $K_{\hat{\pi}}$ of $\hat{\pi}$ which explains the primordial role the points $\widetilde{R}_i$ will play for the rest of this paper.

More generally, we can define an affine lift for any point of $B_k[\ell]$ by considering the isogeny given by $[\ell]$ rather than by π: let $\mathscr{M}_0 = [\ell]^*\mathscr{L}_0$ on B_k. As $\mathscr{L}_0$ is symmetric, we have that $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$ [Mum70] and so $K(\mathscr{M}_0)$, the kernel of $\mathscr{M}_0$ is isomorphic to $K(\overline{\ell^2 n})$. Let $\Theta_{B_k,\mathscr{M}_0}$ be a theta structure on $(B_k, \mathscr{M}_0)$ compatible with the theta structure Θ_{B_k} on $(B_k, \mathscr{L}_0)$. We note $\widetilde{B_k}'$ the affine cone of $(B_k, \mathscr{M}_0)$, and $\widetilde{[\ell]}$ the morphism $\widetilde{B_k}' \to \widetilde{B}_k$ induced by $[\ell]$.

We recall that there is a natural action of $G(\mathscr{M}_0)$ on $H^0(\mathscr{M}_0)$ which can be transported via $\Theta_{B_k,\mathscr{M}_0}$ to an action of $\mathscr{H}(\overline{\ell^2 n})$ on $H^0(\mathscr{M}_0)$. We note $\widetilde{0}_{\widetilde{B_k}'}$ the affine lift of the theta null point of $\widetilde{B_k}'$ such that $\widetilde{[\ell]}\widetilde{0}_{\widetilde{B_k}'} = \widetilde{0}_{B_k}$. We can then generalize the definition of the $\widetilde{R}_i$ by looking at the points:

$$\{\widetilde{[\ell]}(1, i, j).\widetilde{0}_{\widetilde{B_k}'} | i, j \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})\}.$$

Let $H = \{(1, i, j) | i, j \in Z(\bar{\ell})\}$. H is a commutative subgroup of $\mathscr{H}(\overline{\ell^2 n})$ such that $\widetilde{[\ell]}\widetilde{x}_1 = \widetilde{[\ell]}\widetilde{x}_2$ if and only if $x_1 = h.x_2$ where $h \in H$. We see that the section of a point in $B_k[\ell]$ is only defined up to an ℓ^{th}-root of unity. (This is also the case for the lift $\widetilde{R}_i$ of R_i: if we change the theta structure on A_k, it changes the $\widetilde{R}_i$ by an ℓ^{th}-root of unity. See also Corollary 3.5 and Example 6.8). The geometric meaning of these affine lifts is explained in Section 6.2.

The polarization $\mathscr{M}_0$ induces a commutator pairing $e_{\mathscr{M}_0}$ ([Mum66]) on $K(\mathscr{M}_0)$ and as $\mathscr{M}_0$ descends to $\mathscr{L}_0$ via the isogeny $[\ell]$, we know that $e_{\mathscr{M}_0}$ is trivial on $B_k[\ell]$. For $x_1, x_2 \in B_k[\ell]$, let $x_1', x_2' \in B_k[\ell^2]$ be such that $\ell.x_i' = x_i$ for $i = 1, 2$. We remark that x_1' and x_2' are defined up to an element of $B_k[\ell]$. As a consequence, $e_{\mathscr{M}_0}(x_1', x_2) = e_{\mathscr{M}_0}(x_1, x_2') = e_{\mathscr{M}_0}(x_1', x_2')^\ell$, does not depend on the choice of x_1' and x_2' and if we put $e'_\ell(x_1, x_2) = e_{\mathscr{M}_0}(x_1', x_2)$, we obtain a well defined bilinear application $e'_\ell : B_k[\ell n] \times B_k[\ell n] \to \overline{k}$. We call e'_ℓ the extended commutator pairing. It

extends the commutator pairing $e_{\mathscr{L}_0}$ since if $x,y \in B_k[n]$ we have $e'_\ell(x,y) = e_{\mathscr{L}_0}(x,y)^\ell$. When we speak of isotropic points in $B_k[\ell]$, we always refer to isotropic points with respect to e'_ℓ. We quote the following important result from [FLR09]: the modular points $\varphi_1^{-1}(b_i)_{i\in Z(\overline{n})}$ that we compute in Section 2.2 correspond to isogenies whose kernel are isotropic for e'_ℓ.

4.2 The general Riemann relations

The Riemann relations (2) for $\mathscr{M}_{\overline{\ell n}}$ and the Riemann equations (4) for A_k are all particular case of more general Riemann relations, which we will use to get the addition relations on A_k. An analytic proof of these relations can be found in [Mum83].

Theorem 4.1 (Generalized Riemann Relations):
Let $x_1,y_1,u_1,v_1,z \in A_k$ be such that $x_1+y_1+u_1+v_1 = 2z$. Let $x_2 = z-x_1$, $y_2 = z-y_1$, $u_2 = z-u_1$ and $v_2 = z-v_1$. Then there exist $\widetilde{x}_1 \in p_{A_k}^{-1}(x_1)$, $\widetilde{y}_1 \in p_{A_k}^{-1}(y_1)$, $\widetilde{u}_1 \in p_{A_k}^{-1}(u_1)$, $\widetilde{v}_1 \in p_{A_k}^{-1}(v_1)$, $\widetilde{x}_2 \in p_{A_k}^{-1}(x_2)$, $\widetilde{y}_2 \in p_{A_k}^{-1}(y_2)$, $\widetilde{u}_2 \in p_{A_k}^{-1}(u_2)$, $\widetilde{v}_2 \in p_{A_k}^{-1}(v_2)$ that satisfy the following relations: for any $i,j,k,l,m \in Z(\overline{\ell n})$ such that $i+j+k+l = 2m$, let $i' = m-i$, $j' = m-j$, $k' = m-k$ and $l' = m-l$, then for all $\chi \in \hat{Z}(\overline{2})$, we have

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(\widetilde{x}_1)\vartheta_{j+t}(\widetilde{y}_1)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(\widetilde{u}_1)\vartheta_{l+t}(\widetilde{v}_1)\Big) = \Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i'+t}(\widetilde{x}_2)\vartheta_{j'+t}(\widetilde{y}_2)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(\widetilde{u}_2)\vartheta_{l'+t}(\widetilde{v}_2)\Big). \quad (8)$$

Proof: If $x = y = u = v = 0_A$, the preceding result gives the algebraic Riemann relations, a proof of these relations can be found in [Mum66]. We just need to adapt the proof of Mumford for the general case.

Let p_1 and p_2 be the first and second projections from $A_k \times A_k$ to A_k. Let $\mathscr{M} = {p_1}^*(\mathscr{L}) \otimes {p_2}^*(\mathscr{L})$. The theta structure Θ_{A_k} induces a theta structure $\Theta_{A_k\times A_k}$ such that for $(i,j) \in Z(\overline{\ell n}) \times Z(\overline{\ell n})$ we have $\vartheta_{i,j}^{\Theta_{A\times A}} = \vartheta_i^{\Theta_{A_k}} \otimes \vartheta_j^{\Theta_{A_k}}$. (see [Mum66, Lemma 1 p. 323].) Consider the isogeny $\xi : A_k \times A_k \to A_k \times A_k, (x,y) \mapsto (x+y, x-y)$. We have $\xi^*(\mathscr{M}) = \mathscr{M}^2$. Since Θ_{A_k} is a symmetric theta structure Θ_{A_k} it induces a theta structure on $\mathscr{L}^2$ and on $\mathscr{M}^2$. One can check that this theta structure is compatible with the isogeny ξ. Applying the isogeny theorem (see [Mum66, p324]), we obtain that there exists $\lambda \in \overline{k}^*$ such that for all $i,j \in Z(\overline{\ell n})$ and $x,y \in A_k(\overline{k})$:

$$(\vartheta_i^{\mathscr{L}} \otimes \vartheta_j^{\mathscr{L}})(\xi(x,y)) = \lambda \sum_{\substack{u,v\in Z(\overline{2\ell n})\\ u+v=i\\ u-v=j}} (\vartheta_u^{\mathscr{L}^2} \otimes \vartheta_v^{\mathscr{L}^2})(x,y) \quad (9)$$

In the preceding equation, in order to evaluate the sections of $\mathscr{M}$ or $\mathscr{M}^2$ at a geometric point of $x \in A_k \times A_k$ we just choose any isomorphism between $\mathscr{M}_x$ or $\mathscr{M}^2_x$ and $\mathscr{O}_{A_k\times A_k,x}$

where $\mathcal{O}_{A_k \times A_k}$ is the structural sheaf of $A_k \times A_k$. To simplify the notations, we suppose in the following that $\lambda = 1$.

Using equation (9) we compute for all $i, j \in Z(\overline{2\ell n})$ which are congruent modulo $Z(\overline{\ell n})$ and $x, y \in A_k(\overline{k})$:

$$\begin{aligned}\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(x+y)\vartheta^{\mathcal{L}}_{i-j+t}(x-y) &= \sum_{\substack{t\in Z(\bar{2})\\ u,v\in Z(\overline{2ln})\\ u+v=i+j+t\\ u-v=i-j+t}} \chi(t)\vartheta^{\mathcal{L}^2}_{u}(x)\vartheta^{\mathcal{L}^2}_{v}(y)\\ &= \sum_{t_1,t_2\in Z(\bar{2})} \chi(t_1+t_2)\vartheta^{\mathcal{L}^2}_{i+t_1}(x)\vartheta^{\mathcal{L}^2}_{j+t_2}(y)\\ &= \left(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{i+t}(x)\right)\cdot\left(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{j+t}(y)\right)\end{aligned}$$

So we have:

$$\begin{aligned}&\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(x+y)\vartheta^{\mathcal{L}}_{i-j+t}(x-y)\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}}_{k+l+t}(u+v)\vartheta^{\mathcal{L}}_{k-l+t}(u-v)\Big) =\\ &\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{i+t}(x)\Big)\cdot\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{j+t}(y)\Big)\cdot\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{k+t}(u)\Big)\cdot\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}^2}_{l+t}(v)\Big) =\\ &\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+l+t}(x+v)\vartheta^{\mathcal{L}}_{i-l+t}(x-v)\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta^{\mathcal{L}}_{k+j+t}(u+y)\vartheta^{\mathcal{L}}_{k-j+t}(u-y)\Big) \quad (10)\end{aligned}$$

Now if we let $x = x_0 + y_0$, $y = x_0 - y_0$, $u = u_0 + v_0$ and $v = u_0 - v_0$, we have $x+y+u+v = 2(x_0+u_0)$ so we can choose $z = x_0 + u_0$, so that $z - x = u_0 - y_0$, $z - y = u_0 + y_0$, $z - u = x_0 - v_0$, $z - v = x_0 + v_0$. By doing the same variable change for i, j, k, l we see that the theorem is just a restatement of Equation (10). (see [Mum66, p334]). ■

From the generalized Riemann relations it is possible to derive addition relations. First remark that since the theta structure Θ_{A_k} is symmetric there exists a constant $\lambda \in \overline{k}^*$ such that for all $i \in Z(\overline{\ell n})$, $\vartheta_i(-x) = \lambda.\vartheta_{-i}(x)$. In particular if $\widetilde{x} \in \widetilde{A}_k$, we put $-\widetilde{x} = (\widetilde{\vartheta}_{-i}(\widetilde{x}))_{i\in Z(\overline{\ell n})}$.

Theorem 4.2 (Addition Formulas):
Let $x, y \in A_k(\overline{k})$ and suppose that we are given $\widetilde{x} \in p_{A_k}^{-1}(x)$, $\widetilde{y} \in p_{A_k}^{-1}(y)$, $\widetilde{x-y} \in p_{A_k}^{-1}(x-y)$, then there is a unique point $\widetilde{x+y} \in \widetilde{A}_k(\overline{k})$ verifying for $i, j, k, l \in Z(\overline{\ell n})$

$$\begin{aligned}&\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{i+t}(\widetilde{x+y})\vartheta_{j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{k+t}(\widetilde{0}_{A_k})\vartheta_{l+t}(\widetilde{0}_{A_k})\Big) =\\ &\qquad\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{-i'+t}(\widetilde{y})\vartheta_{j'+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{k'+t}(\widetilde{x})\vartheta_{l'+t}(\widetilde{x})\Big), \quad (11)\end{aligned}$$

and we have $p_{A_k}(\widetilde{x+y}) = x+y$.

Thus the addition law on A_k *extends to a pseudo addition law on* $\widetilde{A}_k$*; we call it an addition chain and we note* $\widetilde{x+y} = \texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})$.

Proof: We apply the Riemann relations (8) to $x+y, x-y, 0_A, 0_A$. We have $2x = (x+y)+(x-y)+0_A+0_A$, $-y = x-(x+y)$, $y = x-(x-y)$, $x = x-0_A$, $x = x-0_A$ so Theorem 4.1 shows that there exist a point $\widetilde{x+y} \in \widetilde{A}_k(\overline{k})$ satisfying the addition relations (11).

It remains to show that this point is unique. But first we reformulate the addition formulas (see [Mum66, p334]). Let $H = Z(\overline{\ell n}) \times \hat{Z}(\overline{2})$, and for $(i,\chi) \in H$ define

$$\widetilde{u}_{i,\chi}(\widetilde{x}) = \sum_{t \in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{i+t}(\widetilde{x}).$$

Then we have for all $i,j,k,l,m \in H$ such that $2m = i+j+k+l$

$$\widetilde{u}_i(\widetilde{x+y})\widetilde{u}_j(\widetilde{x-y})\widetilde{u}_k(\widetilde{0}_{A_k})\widetilde{u}_l(\widetilde{0}_{A_k}) = \frac{1}{2^{2g}} \sum_{\xi \in H, 2\xi = \in Z(\overline{2})\times 0} (m_2+\xi_2)(2\xi_1)\widetilde{u}_{i-m+\xi}(\widetilde{y})\widetilde{u}_{m-j+\xi}(\widetilde{y})\widetilde{u}_{m-k+\xi}(\widetilde{x})\widetilde{u}_{m-l+\xi}(\widetilde{x}) \quad (12)$$

It is easy to see that $(\widetilde{\vartheta}_i(\widetilde{x}))_{i \in Z(\overline{\ell n})}$, is determined by $(\widetilde{u}_i(\widetilde{x}))_{i \in H}$. That means there is a $j \in H$ such that $\widetilde{u}_j(\widetilde{x-y}) \neq 0$ otherwise we would have $\widetilde{\vartheta}_i(\widetilde{x-y}) = 0$ for all $i \in Z(\overline{\ell n})$. Now for all $i \in H$, we need to find $k,l \in H$ such that $i+j+k+l = 2m$ and $\widetilde{u}_k(\widetilde{0}) \neq 0$, $\widetilde{u}_l(\widetilde{0}) \neq 0$. In that case equation (12) allows us to compute $\widetilde{u}_i(\widetilde{x+y})\widetilde{u}_j(\widetilde{x-y})\widetilde{u}_k(0)\widetilde{u}_l(0)$ from $(\widetilde{u}_i(\widetilde{x}))_{i \in H}$ and $(\widetilde{u}_i(\widetilde{y}))_{i \in H}$, so we can obtain $\widetilde{u}_i(\widetilde{x+y})$.

In [Mum66, p. 339], Mumford prove that for any $i \in H$, there is an $\alpha \in 2Z(\overline{\ell n})$ such that $\widetilde{u}_{i+(\alpha,0)}(0) \neq 0$. So we can choose $k = i$, $l = j$, we have $i+j+k+l = 2m$, and if necessary we add an element of $2Z(\overline{\ell n})$ to k and l. ■

Algorithm 4.3 (Addition chain):
Input $\widetilde{x},\widetilde{y}$ and $\widetilde{x-y}$ such that $p_{A_k}(\widetilde{x}) - p_{A_k}(\widetilde{y}) = p_{A_k}(\widetilde{x-y})$.
Output $\widetilde{x+y} = \texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})$.
Step 1 For all $i \in Z(\overline{\ell n})$, $\chi \in \hat{Z}(\overline{2})$ and $X \in \{\widetilde{x+y}, \widetilde{x}, \widetilde{y}, \widetilde{0}_{A_k}\}$ compute

$$\widetilde{u}_{i,\chi}(X) = \sum_{t \in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{i+t}(X).$$

Step 2 For all $i \in Z(\overline{\ell n})$ choose $j,k,l \in Z(\overline{\ell n})$ such that $i+j+k+l = 2m$, $\widetilde{u}_j(\widetilde{x-y}) \neq 0$,

$\widetilde{u}_k(\widetilde{0}_{A_k}) \neq 0$, $\widetilde{u}_l(\widetilde{0}_{A_k}) \neq 0$ and compute

$$\widetilde{u}_i(\widetilde{x+y}) = \frac{1}{2^{2g}\widetilde{u}_j(\widetilde{x-y})\widetilde{u}_k(\widetilde{0}_{A_k})\widetilde{u}_l(\widetilde{0}_{A_k})} \sum_{\xi \in H, 2\xi = \in Z(\bar{2})\times 0} (m_2+\xi_2)(2\xi_1)\widetilde{u}_{i-m+\xi}(\widetilde{y})\widetilde{u}_{m-j+\xi}(\widetilde{y})\widetilde{u}_{m-k+\xi}(\widetilde{x})\widetilde{u}_{m-l+\xi}(\widetilde{x}). \quad (13)$$

Step 3 For all $i \in Z(\overline{\ell n})$ output

$$\widetilde{\vartheta}_i(\widetilde{x+y}) = \frac{1}{2^g} \sum_{\xi \in \hat{Z}(\bar{2})} \widetilde{u}_{i,\chi}(\widetilde{x+y}).$$

♢

Complexity Analysis 4.4:
We use a linear transformation between the $\widetilde{\vartheta}$ coordinates and the $\widetilde{u}$ coordinates in the Steps 1 and 3 because we have seen in the proof of Theorem 4.2 that the latter are more suited for additions.

As $\widetilde{u}_{i+t,\chi} = \chi(t)\widetilde{u}_{i,\chi}$ we only need to consider $(\ell n)^g$ coordinates and the linear transformation between $\widetilde{u}$ and $\widetilde{\vartheta}$ can be computed at the cost of $(2n\ell)^g$ additions in k. We also have $\widetilde{u}_{i,\chi}(-\widetilde{x}) = \widetilde{u}_{-i,\chi}(\widetilde{x})$.

Using the fact that for $t \in Z(\bar{2})$ the right hand terms of (13) corresponding to $\xi = (\xi_1+t, \xi_2)$ and to $\xi = (\xi_1, \xi_2)$ are the same up to a sign, one can compute the left hand side of (13) with $4 \cdot 4^g$ multiplications and 4^g additions in k. In total one can compute an addition chain in $4.(4\ell n)^g$ multiplications, $(4\ell n)^g$ additions and $(\ell n)^g$ divisions in k. We remark that in order to compute several additions using the same point, there is no need to convert back to the $\widetilde{\vartheta}$ at each step so we only need to perform Step 2.

The addition chain formula is a basic step for our isogenies computations, and in the sequel we consider it as our basic unit for the complexity analysis. In some cases it is possible to greatly speed up this computation. See for instance [Gau07] which uses the duplication formula between theta functions to speed up the addition chain of level two (in genuses 1 and 2). See also Section 5.1 where it is explained how to use isogenies to compute the addition chain for a general level by using only addition chains of level two, so that we can use the speed up of [Gau07] in every level. ♢

Remark 4.5:
The addition formulas can also be used to compute the usual addition law in A_k by choosing $j = 0$ in Equation (13) for every i.

It is also possible to use directly the ϑ coordinates as follows: if $x, y \in A_k(\bar{k})$ and $i \in Z(\overline{\ell n})$, for every $\chi \in \hat{Z}(\bar{2})$, one can choose $k, l \in Z(\overline{\ell n})$ such that $i+k+l$ is divisible by 2 and

$$\Big(\sum_{t \in Z(\bar{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) \neq 0.$$

So one can use (11) to compute

$$a_{i,\chi} := \Big(\sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i+t}(P+Q) \vartheta_{0+t}(P-Q) \Big),$$

and recover $\vartheta_i(P+Q)$ by inversing a matrix. For instance we have $\vartheta_i(x) = \dfrac{1}{2^g} \sum_{\chi \in \hat{Z}(\bar{2})} a_{\chi,i}$ ♢

The addition chain law on $\widetilde{A}_k$ induces a multiplication by a scalar law which reduces via p_{A_k} to the usual multiplication by a scalar law deduced from the group structure of A_k. Let $\widetilde{x}, \widetilde{y} \in \widetilde{A}_k$ and $\widetilde{x+y} \in p_{A_k}^{-1}(x+y)$, then we can compute $\widetilde{2x+y} := \texttt{chaine\_add}(\widetilde{x+y}, \widetilde{x}, \widetilde{y})$. More generally there is a recursive algorithm to compute for every $m \geqslant 2$:

$$\widetilde{mx+y} := \texttt{chaine\_add}(\widetilde{(m-1)x+y}, \widetilde{x}, \widetilde{(m-2)x+y})$$

We put $\texttt{chaine\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y}) := \widetilde{mx+y}$ and define $\texttt{chaine\_mult}(m, \widetilde{x}) := \texttt{chaine\_multadd}(m, \widetilde{x}, \widetilde{x}, \widetilde{0}_{A_k})$. We have $p_{A_k}(\texttt{chaine\_mult}(m, \widetilde{x})) = m.p_{A_k}(\widetilde{x})$. We call `chaine_multadd` a multiplication chain.

Algorithm 4.6 (Multiplication chain):
Input $m \in \mathbb{N}$, $\widetilde{x+y}, \widetilde{x}, \widetilde{y} \in \widetilde{A}_k$.
Output $\texttt{chaine\_multadd}(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y})$.
Step 1 Compute the binary decomposition of $m := \sum_{i=0}^{I} b_i 2^i$. Set $m' := 0$, $\mathtt{xy}_0 := \widetilde{y}$, $\mathtt{xy}_{-1} := \texttt{chaine\_add}(\widetilde{y}, -\widetilde{x}, \widetilde{x+y})$, $\mathtt{x}_0 := \widetilde{0}_{A_k}$ and $\mathtt{x}_1 := \widetilde{x}$.
Step 2 For i in $[I..0]$ do
If $b_i = 0$ then compute

$$\begin{gathered} \mathtt{x}_{2m'} := \texttt{chaine\_add}(\mathtt{x}_{m'}, \mathtt{x}_{m'}, \mathtt{x}_0) \\ \mathtt{x}_{2m'+1} := \texttt{chaine\_add}(\mathtt{x}_{m'+1}, \mathtt{x}_{m'}, \mathtt{x}_1) \\ \mathtt{xy}_{2m'} := \texttt{chaine\_add}(\mathtt{xy}_{m'}, \mathtt{x}_{m'}, \mathtt{xy}_0) \\ m' := 2m'. \end{gathered}$$

Else compute

$$\begin{gathered} \mathtt{x}_{2m'+1} := \texttt{chaine\_add}(\mathtt{x}_{m'+1}, \mathtt{x}_{m'}, \mathtt{x}_1) \\ \mathtt{x}_{2m'+2} := \texttt{chaine\_add}(\mathtt{x}_{m'+1}, \mathtt{x}_{m'+1}, \mathtt{x}_0) \\ \mathtt{xy}_{2m'+1} := \texttt{chaine\_add}(\mathtt{xy}_{m'}, \mathtt{x}_{m'}, \mathtt{xy}_{-1}) \\ m' := 2m' + 1. \end{gathered}$$

Step 3 Output $\mathtt{xy}_m$. ♢

Correction and Complexity Analysis 4.7:
In Corollary 4.13 we show that multiplication chains are associative, so we can use a Lucas sequence to compute them. In order to do as few division as possible, we use a Montgomery ladder for our Lucas sequence, hence the algorithm.

We see that a multiplication chain requires $O(\log(m))$ addition chains. ♢

Lemma 4.8:
For $\lambda_x, \lambda_y, \lambda_{x-y} \in \overline{k}^*$ and $\widetilde{x}, \widetilde{y} \in A_k(\overline{k})$, we have:

$$\texttt{chaine\_add}(\lambda_x\widetilde{x}, \lambda_y\widetilde{y}, \lambda_{x-y}\widetilde{x-y}) = \frac{\lambda_x^2\lambda_y^2}{\lambda_{x-y}}\,\texttt{chaine\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}), \tag{14}$$

$$\texttt{chaine\_multadd}(n, \lambda_{x+y}\widetilde{x+y}, \lambda_x\widetilde{x}, \lambda_y\widetilde{y}) = \frac{\lambda_x^{n(n-1)}\lambda_{x+y}^n}{\lambda_y^{n-1}}\,\texttt{chaine\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y}), \tag{15}$$

$$\texttt{chaine\_mult}(n, \lambda_x\widetilde{x}) = \lambda_x^{n^2}\,\texttt{chaine\_mult}(n, \widetilde{x}). \tag{16}$$

Proof: Formula (14) is an immediate consequence of the addition formulas (11). The rest of the lemma follows by an easy recursion. ■

4.2.1 The case $n = 2$

Let x be the generic point of A_k. Then the Riemann equations (17) come from the following addition formula:

$$x = \texttt{chaine\_add}(x, 0_A, x). \tag{17}$$

We suppose here that $n = 2$ and $\ell = 1$. We have for all $i \in Z(\overline{2})$, $(-1)^*\vartheta_i = \vartheta_i$, where (-1) is the inverse automorphism on A_k. As a consequence, $\mathscr{L}$ gives an embedding of the Kummer variety $K_A = A/\pm 1$. The equations (17) are trivial, so that Riemann equations does not give the projective equations of this embedding (except when $g = 1$). Nonetheless, one can recover these equations by considering more general addition relations.

Let $p : A_k \to K_A$ be the natural projection. If $x, y \in K_A$, let $x_0 \in p^{-1}(x)$ and $y_0 = p^{-1}(y)$, we have $p(p^{-1}(x) + p^{-1}(y)) = p(\pm x_0 \pm y_0) = \{p(x_0 + y_0), p(x_0 - y_0)\}$. As a consequence, there is no properly defined addition law on K_A: from $\pm x \in K_A$ and $\pm y \in K_A$, we may compute $\pm x \pm y$ which give two points on K_A. However, if we are also given $\pm(x - y) \in K_A$, then we can identify $\pm(x + y) \in \{\pm x \pm y\}$. Thus the addition chain law from Theorem 4.2 extends to a pseudo addition on the Kummer variety. We remark that our addition chain is a generalization of the pseudo addition law on the Kummer variety.

Let $x, y \in K_A$. To compute $\pm x \pm y$ without $\pm(x - y)$ we can proceed as follows: let $X = (X_i)_{i \in Z(\overline{2})}$, $Y = (Y_i)_{i \in Z(\overline{2})}$ be the two projections of the generic point on $K_A \times K_A$. Then the addition relations $\texttt{chaine\_add}(X, x, y, Y)$ describe a system of degree 2 in $K_A \times K_A$, whose solutions are $(\pm(x + y), \pm(x - y))$ and $(\pm(x - y), \pm(x + y))$. From this system, it is easy to recover the points $\{\pm(x + y), \pm(x - y)\}$, but this involves a square root in k. (The preceding

claims will be proved on an upcoming paper). Coming back to isogenies computations, it means that when working with $n = 2$, we have to avoid computing normal additions, since they require a square root and are much slower than addition chains.

We make a last remark concerning additions on the Kummer variety. Suppose that we are given $x, y, z \in K_A$, together with $\pm(x+y)$, $\pm(y+z)$. We want to find $\pm(x+z)$. Using the addition relations, we can compute $S = \{\pm(x+z), \pm(x-z)\}$. Let $A \in S$, then the solutions of the addition relations $\texttt{chaine\_add}(X, x+y, A, Y)$ are $\{\pm(2x+y+z), \pm(y-z)\}$ if $A = \pm(x+z)$, and $\{\pm(2x+y-z), \pm(y+z)\}$ if $A = \pm(x-z)$. This allows to find $\pm(y+z) \in S$ if $2x \neq 0, 2y \neq 0, 2z \neq 0, 2(x+y+z) \neq 0$. We call this the compatible addition relation, and we can use this to compute $\pm(x+z)$ directly without taking a square root (by computing the gcd between the two systems of degree two given by the addition relations).

4.3 Theta group and addition relations

In this Section, we study the action of the theta group on the addition relations. We use this action to find the addition relations linking the coordinates of the points $\{\widetilde{R}_i\}_{i \in Z(\overline{\ell n})}$. By considering different isogenies $\pi : A_k \to B_k$, we can then understand the addition chains between any isotropic subgroup of $B_k[\ell]$ (see Section 4.1). In particular we exploit this to show that we can compute the chain multiplication by ℓ in $O(\log(\ell))$ addition chains.

Lemma 4.9:
Suppose that $\widetilde{x}_1, \widetilde{y}_1, \widetilde{u}_1, \widetilde{v}_1, \widetilde{x}_2, \widetilde{y}_2, \widetilde{u}_2, \widetilde{v}_2 \in \widetilde{A}_k$ satisfy the general Riemann relations (8).

- *For every $g \in G(\mathscr{L})$, $g.\widetilde{x}_1, g.\widetilde{y}_1, g.\widetilde{u}_1, g.\widetilde{v}_1, g.\widetilde{x}_2, g.\widetilde{y}_2, g.\widetilde{u}_2, g.\widetilde{v}_2$ also satisfy the Riemann relations.*
- *For every isogeny $\pi : (A, \mathscr{L}, \Theta_{A_k}) \to (B, \mathscr{L}_0, \Theta_{B_k})$ such that Θ_{B_k} is π-compatible of type 1 with Θ_{A_k}, then $\widetilde{\pi}(\widetilde{x}_1), \widetilde{\pi}(\widetilde{y}_1), \widetilde{\pi}(\widetilde{u}_1), \widetilde{\pi}(\widetilde{v}_1), \widetilde{\pi}(\widetilde{x}_2), \widetilde{\pi}(\widetilde{y}_2), \widetilde{\pi}(\widetilde{u}_2), \widetilde{\pi}(\widetilde{v}_2) \in \widetilde{B}_k$ also satisfy the Riemann relations.*

Proof: This is an immediate computation. ■

Lemma 4.10:
Let $(\alpha, i, j) \in \mathscr{H}(\overline{\ell n})$. Let $\widetilde{x} = (\alpha, i, j).\widetilde{0}_{A_k} \in \widetilde{A}_k$. Then we have $-\widetilde{x} = (\alpha, -i, -j).\widetilde{0}_{A_k}$.

More generally, if $\widetilde{x} \in \widetilde{A}_k$, then $-(\alpha, i, j).\widetilde{x} = (\alpha, -i, -j).-\widetilde{x}$, and we have $\widetilde{\pi}(-x) = -\widetilde{\pi}(x)$.

Proof: If $\widetilde{x} = (x_i)_{i \in Z(\overline{\ell n})}$, we recall that we have defined $-\widetilde{x} = (x_{-i})_{i \in Z(\overline{\ell n})}$. Let $\widetilde{0}_{A_k} = (a_i)_{i \in Z(\overline{\ell n})}$, if $u \in Z(\overline{\ell n})$ we have by (3): $x_u = ((\alpha, i, j).\widetilde{0}_{A_k})_u = \alpha j(-u-i)a_{u+i}$, $((\alpha, -i, -j).\widetilde{0}_{A_k})_{-u} = \alpha(-j)(u+i)a_{-u-i} = a_{u+i} = x_u$.

The generalization and the rest of the lemma is trivial. ■

An interesting property of the addition formulas, is that they are compatible with the action $s_{K_1(\mathscr{L})} : K_1(\mathscr{L}) \to \widetilde{A}_k$:

Proposition 4.11 (Compatibility of the pseudo-addition law):
For $\widetilde{x},\widetilde{y},\widetilde{x-y}\in\widetilde{A}_k$, and $i,j\in Z(\ell n)$, we have:

$$(1,i+j,0).\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})=\texttt{chaine\_add}((1,i,0).\widetilde{x},(1,j,0).\widetilde{y},(1,i-j,0).\widetilde{x-y}) \tag{18}$$

In particular if we set $\widetilde{P}_i=(1,i,0).\widetilde{0}_{A_k}$ we have:

$$\widetilde{P}_{i+j}=\texttt{chaine\_add}(\widetilde{P}_i,\widetilde{P}_j,\widetilde{P}_{i-j})$$

Proof: Let $\widetilde{x+y}=\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})$. By Theorem 4.2, we have for every $a,b,c,d,e\in Z(\overline{\ell n})$ such that $a+b+c+d=2e$:

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{a+t}(\widetilde{x+y})\vartheta_{b+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big)=$$
$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{-e+a+t}(\widetilde{y})\vartheta_{e-b+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{e-c+t}(\widetilde{x})\vartheta_{e-d+t}(\widetilde{x})\Big). \tag{19}$$

Applying (19) to $a'=a+i+j, b'=b+i-j, c'=c, d'=d, e'=e+i$, it comes:

$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+j+a+t}(\widetilde{x+y})\vartheta_{b+i-j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big)=$$
$$\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{-j-e+a+t}(\widetilde{y})\vartheta_{j+e-b}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\bar{2})}\chi(t)\vartheta_{i+e-c+t}(\widetilde{x})\vartheta_{i+e-d+t}(\widetilde{x})\Big). \tag{20}$$

Thus $(1,i+j,0).\widetilde{x+y}$, $(1,i,0).\widetilde{x}$, $(1,j,0).\widetilde{y}$ and $(1,i-j,0).\widetilde{x-y}$ satisfy the additions relations. ■

By applying $\widetilde{\pi}$, we obtain the following corollary:

Corollary 4.12:

$$\widetilde{\pi}_{i+j}(\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y}))=\texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}),\widetilde{\pi}_j(\widetilde{y}),\widetilde{\pi}_{i-j}(\widetilde{x-y}))$$

Proof: Remember that by definition $\widetilde{\pi}_i(\widetilde{x})=\widetilde{\pi}((1,i,0).\widetilde{x})$. The lemma is then a trivial consequence of Proposition 4.11 and Lemma 4.9. ■

We discuss two consequences of the preceding corollary. The first is that we can recover the point $\widetilde{x}=(\vartheta_i(\widetilde{x}))_{i\in Z(\overline{\ell n})}$ from only a subset of its coordinates $\{\vartheta_i(\widetilde{x})\}_{i\in Z(\overline{\ell n})}$ (see Section 5.1).
The second application is the computation of the dual isogeny $\hat{\pi}$ (see Section 5.2).

But first we remark that by setting $\widetilde{x}=\widetilde{y}=\widetilde{0}_{A_k}$ in Corollary 4.12, we find

$$\widetilde{R}_{i+j}=\texttt{chaine\_add}(\widetilde{R}_i,\widetilde{R}_j,\widetilde{R}_{i-j}).$$

By considering different isogenies $\pi : A_k \to B_k$, we can use Corollary 4.12 to study the associativity of chain additions:

Corollary 4.13:
Let $x \in B_k[\ell]$ and $y \in B_k$. Choose any affine lifts $\widetilde{x}$, $\widetilde{y}$ and $\widetilde{x+y}$ of respectively x, y and $x+y$.

1. *Let $\widetilde{nx+y}=\texttt{chaine\_multadd}(n,\widetilde{x+y},\widetilde{x},\widetilde{y})$ and $\widetilde{nx}=\texttt{chaine\_mult}(n,\widetilde{x})$.*
   We have
   $$\widetilde{(n_1+n_2)x+y}=\texttt{chaine\_add}(\widetilde{n_1x+y},\widetilde{n_2x},\widetilde{(n_1-n_2)x+y}) \tag{21}$$
   In particular, we see that we can compute $\widetilde{nx+y}$ in $O(\log(n))$ addition chains by using a Montgomery ladder [Plo29].
2. $-\widetilde{nx+y}=\texttt{chaine\_add}(n,-(\widetilde{x+y}),-\widetilde{x},-\widetilde{y})$

Proof: We prove the two assertions.

1. Let K be a maximal isotropic group containing x, and let $A_k=B_k/K$. Let $\pi : A_k \to B_k$ be the contragredient isogeny, and choose any theta structure on $(A_k,\pi^*\mathscr{L}_0)$ compatible with π. There exist $i \in Z(\overline{\ell})$ and $\lambda_i \in \overline{k}^*$ such that $\widetilde{x}=\lambda_i\widetilde{\pi}_i(\widetilde{0}_{A_k})$. If $\lambda_i=1$, then Corollary 4.13 is a consequence of Corollary 4.12. But it is easy (see Lemma 4.8) to see that (21) is homogeneous in λ_i, hence the result.

2. Once again, let $i \in Z(\overline{\ell})$ be such that $\widetilde{x}=\lambda_i\widetilde{\pi}\left((1,i,0).\widetilde{0}_{A_k}\right)$, and let $\widetilde{y}'$ be any point in $\widetilde{\pi}^{-1}(\widetilde{y})$. By homogeneity we may suppose that $\lambda_i=1$. By Corollary 4.12 and Proposition 4.11, we have $\widetilde{nx+y}=\widetilde{\pi}\left((1,n.i,0).\widetilde{y}'\right)$. Now by Lemma 4.10, we have $-\widetilde{nx+y}=\widetilde{\pi}\left(-(1,n.i,0).\widetilde{y}'\right)=\widetilde{\pi}\left((1,-n.i,0).-\widetilde{y}'\right)=\texttt{chaine\_add}(n,-(\widetilde{x+y}),-\widetilde{x},-\widetilde{y})$. ■

We make a last remark concerning Corollary 4.12 namely a useful fact for studying the case ℓ not prime to n:

Remark 4.14:
Let $\widetilde{x} \in \widetilde{A}_k$, $i \in Z(\overline{\ell n})$ and let $\widetilde{y}=\widetilde{\pi}(\widetilde{x})$. Let $m \in \mathbb{Z}$ such that $\ell | m$. By Proposition 4.11 and Corollary 4.12, we have

$$\widetilde{\pi}((1,mi,0).\widetilde{x})=\texttt{chaine\_multadd}(m,\widetilde{\pi}_i(\widetilde{x}),\widetilde{R}_i,\widetilde{y})$$

But if $\ell | m$, then $mi \in Z(\overline{n}) \subset Z(\overline{\ell n})$, by Proposition 3.4 we have $\widetilde{\pi}((1,mi,0).\widetilde{x})=(1,mi,0).\widetilde{y}$, and $(1,mi,0).\widetilde{y}$ can be computed with the formulas (3). Hence

$$(1,mi,0).\widetilde{y}=\texttt{chaine\_multadd}(m,\widetilde{\pi}_i(\widetilde{x}),\widetilde{R}_i,\widetilde{y})$$

♢

For the purpose of Section 6.2, we have to study the addition relations between the points in $B_k[\ell]$ which does not necessarily belong to $K(\mathscr{L}_0)$. From Section 4.1, we see that we need to understand the link between the addition relations and the isogeny $\widetilde{[\ell]}$. More generally, for the rest of this section we will study the relationship between the addition relations and a general isogeny. First we take a closer look at the action of $s_{K_2(\mathscr{L})}$ on the addition relations. Let $\mathfrak{I}$ be the automorphism of the Theta group from Section 3.3 that permutes K_1 and K_2. Since $s_{K_2(\mathscr{L})} = \mathfrak{I} \circ s_{K_1(\mathscr{L})} \circ \mathfrak{I}$ we see that it suffices to study the action of $\mathfrak{I}$ on the addition relations.

Proposition 4.15:
Suppose that $x, y, u, v, x', y', u', v' \in \widetilde{A}_k$ satisfy the general Riemann equations (8). Then $\mathfrak{I}.x$, $\mathfrak{I}.y$, $\mathfrak{I}.u$, $\mathfrak{I}.v$, $\mathfrak{I}.x'$, $\mathfrak{I}.y'$, $\mathfrak{I}.u'$, $\mathfrak{I}.v'$ also satisfy (8).

Proof: If $x = (x_i)_{i \in Z(\overline{\ell n})}$ we recall (see (7)) that

$$\mathfrak{I}.x = \Big(\sum_{j \in Z(\overline{\ell n})} e(i,j) x_j \Big)_{i \in Z(\overline{\ell n})}$$

where $e = e_{\mathscr{L}}$ is the commutator pairing.

By hypothesis, we have for $i, j, k, l \in Z(\overline{\ell n})$ such that $i + j + k + l = 2m$:

$$\Big(\sum_{t \in Z(\bar{2})} \vartheta_{i+t}(x) \vartheta_{j+t}(y) \Big) . \Big(\sum_{t \in Z(\bar{2})} \vartheta_{k+t}(u) \vartheta_{l+t}(v) \Big) = \Big(\sum_{t \in Z(\bar{2})} \vartheta_{i'+t}(x') \vartheta_{j'+t}(y') \Big) . \Big(\sum_{t \in Z(\bar{2})} \vartheta_{k'+t}(u') \vartheta_{l'+t}(v') \Big). \quad (22)$$

Let $A_{\chi,x,y,i,j} = \big(\sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i+t}(x) \vartheta_{j+t}(y) \big)$. We have if $I, J, K, L \in Z(\overline{\ell n})$ are such that $I + J + K + L = 2M$:

$$\begin{aligned} A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J} &= \sum_{T \in Z(\bar{2})} \chi(T) \Big(\sum_{i \in Z(\overline{\ell n})} e(I+T,i) \vartheta_i(x) \Big) \Big(\sum_{j \in Z(\overline{\ell n})} e(J+T,j) \vartheta_j(x) \Big) \\ &= \sum_{T \in Z(\bar{2}), i,j \in Z(\overline{\ell n})} \chi(T) e(T, i+j) e(I,i) e(J,j) \vartheta_i(x) \vartheta_j(y) \end{aligned}$$

$$\begin{aligned} & A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J} A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L} = \\ & \sum_{\substack{T_1,T_2 \in Z(\bar{2}) \\ i,j,k,l \in Z(\overline{\ell n})}} \chi(T_1+T_2) e(T_1, i+j) e(T_2, k+l) e(I,i) e(J,j) e(K,k) e(L,l) \vartheta_i(x) \vartheta_j(y) \vartheta_k(u) \vartheta_l(v) \\ &= \sum_{i,j,k,l \in Z(\overline{\ell n})} e(I,i) e(J,j) e(K,k) e(L,l) \vartheta_i(x) \vartheta_j(y) \vartheta_k(u) \vartheta_l(v) \\ &\qquad \Big(\sum_{T_1,T_2 \in Z(\bar{2})} \chi(T_1+T_2) e(T_1, i+j) e(T_2, k+l) \Big) \end{aligned}$$

But

$$\Big(\sum_{T_1,T_2\in Z(\bar{2})}\chi(T_1+T_2)e(T_1,i+j)e(T_2,k+l)\Big)=\begin{cases}4^g & \text{if } e(\cdot,i+j)=e(\cdot,k+l)=\chi\\ 0 & \text{otherwise}\end{cases}$$

and $e(\cdot,i+j)=e(\cdot,k+l)$ (as characters on $Z(\bar{2})$) iff there exists $m\in Z(\overline{\ell n})$ such that $i+j+k+l=2m$. Now since $I+J+K+L=2M$ we have $e(I+J,\cdot)=e(K+L,\cdot)$ so we have:

$$\lambda\sum_{t_1,t_2\in Z(\bar{2})}e(I,i+t_1)e(J,j+t_1)e(K,k+t_2)e(L,l+t_2)\vartheta_{i+t_1}(x)\vartheta_{j+t_1}(y)\vartheta_{k+t_2}(u)\vartheta_{l+t_2}(v)=$$
$$\lambda e(I,i)e(J,j)e(K,k)e(L,l)\sum_{t_1,t_2\in Z(\bar{2})}\vartheta_{i+t_1}(x)\vartheta_{j+t_1}(y)\vartheta_{k+t_2}(u)\vartheta_{l+t_2}(v)=$$
$$\lambda e(I,i)e(J,j)e(K,k)e(L,l)\sum_{t_1,t_2\in Z(\bar{2})}\vartheta_{i'+t_1}(x')\vartheta_{j'+t_1}(y')\vartheta_{k'+t_2}(u')\vartheta_{l'+t_2}(v)=$$
$$\lambda e(I',i')e(J',j')e(K',k')e(L',l')\sum_{t_1,t_2\in Z(\bar{2})}\vartheta_{i'+t_1}(x')\vartheta_{j'+t_1}(y')\vartheta_{k'+t_2}(u')\vartheta_{l'+t_2}(v)$$

where $\lambda=4^g$ if $i+j+k+l=2m$ and $\lambda=0$ otherwise. By combining these relations we find that

$$A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J}A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L}=A_{\chi,\mathfrak{I}.x',\mathfrak{I}.y',I',J'}A_{\chi,\mathfrak{I}.u',\mathfrak{I}.v',K,L}$$

which concludes the proof. (We remark that we did not need to use the general Riemann relations with characters on our proof. By considering $\mathfrak{I}\circ\mathfrak{I}$, this shows that the general Riemann relations with characters are induced by the general Riemann relations without characters.) ■

Corollary 4.16:
Let $\widetilde{x},\widetilde{y},\widetilde{x-y}\in\widetilde{A}_k$, and let $i,j\in Z(\overline{\ell n})$, $k,l\in\hat{Z}(\overline{\ell n})$. Then we have:

$$(1,i+j,k+l).\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})=\texttt{chaine\_add}((1,i,k).\widetilde{x},(1,j,l).\widetilde{y},(1,i-j,k-l).\widetilde{x-y})$$

Proof: By Propositions 4.11 and 4.15 we have

$$s_2(k+l).\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})=\texttt{chaine\_add}(s_2(k).\widetilde{x},s_2(l).\widetilde{y},s_2(k-l).\widetilde{x-y}) \quad (23)$$

Now since $(1,i,k)=s_1(i)s_2(k)$, we conclude by combining Equations (18) and (23). ■

Corollary 4.17:
Suppose that $\widetilde{x}_1,\widetilde{y}_1,\widetilde{u}_1,\widetilde{v}_1,\widetilde{x}_2,\widetilde{y}_2,\widetilde{u}_2,\widetilde{v}_2\in\widetilde{A}_k$ satisfy the Riemann relations (8).

If $\pi:(A,\mathscr{L},\Theta_{A_k})\to(B,\mathscr{L}_0,\Theta_{B_k})$ is an isogeny such that Θ_{B_k} is π-compatible with Θ_{A_k}, then $\widetilde{\pi}(\widetilde{x}_1)$, $\widetilde{\pi}(\widetilde{y}_1)$, $\widetilde{\pi}(\widetilde{u}_1)$, $\widetilde{\pi}(\widetilde{v}_1)$, $\widetilde{\pi}(\widetilde{x}_2)$, $\widetilde{\pi}(\widetilde{y}_2)$, $\widetilde{\pi}(\widetilde{u}_2)$, $\widetilde{\pi}(\widetilde{v}_2)\in\widetilde{B}_k$ also satisfy the general Riemann Relations.

In particular we have

$$\widetilde{\pi}(\texttt{chaine\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})=\texttt{chaine\_add}(\widetilde{\pi}(\widetilde{x}),\widetilde{\pi}(\widetilde{y}),\widetilde{\pi}(\widetilde{x-y}))$$

Proof: By Lemma 4.9, this is the case for compatible isogenies of type 1. By Proposition 4.15 this is also the case for compatible isogenies of type 2, which concludes since every compatible isogeny is a composition of isogenies of type 1 or 2. ■

5 Application of the addition relations to isogenies

In this Section we apply the results of Section 4 to the computation of isogenies (see Section 5.2). More precisely, we present an algorithm to compute the isogeny $\hat{\pi} : B_k \to A_k$ from the knowledge of the modular point $\widetilde{0}_{A_k}$. We give in Section 6 algorithms to compute $\widetilde{0}_{A_k}$ from the kernel of $\hat{\pi}$.

Since the embedding of A_k that we consider is given by a theta structure of level $\overline{\ell n}$, a point $\hat{\pi}(x)$ is given by $(\ell n)^g$ coordinates, which get impractical when ℓ is high. In order to mitigate this problem, in Section 5.1, we give a point compression algorithm such that the number of coordinates of a compressed point does not depend on ℓ.

We recall that we have chosen in Section 4.1 $\widetilde{0}_{A_k} = (a_i)_{i \in Z(\overline{\ell n})}$ thus that $\widetilde{\pi}(\widetilde{0}_{A_k}) = \widetilde{0}_{B_k}$, and that we have defined for $i \in Z(\overline{\ell n})$ $\widetilde{R}_i = (a_{i+j})_{j \in Z(\overline{n})}$.

5.1 Point compression

Suppose that ℓ is prime to n. We know that $\widetilde{x} \in \widetilde{A}_k$ can be recovered from $(\widetilde{\pi}_i(\widetilde{x}))_{i \in Z(\overline{\ell})}$, by $(\widetilde{x})_{ni+\ell j} = (\widetilde{\pi}_i(\widetilde{x}))_j$. If $(d_1, \cdots, d_g)$ is a basis of $Z(\overline{\ell})$, we can prove that $\widetilde{x}$ can be easily computed from just $(\widetilde{\pi}_{d_i}(\widetilde{x}))_{i \in [1..g]}$ and $(\widetilde{\pi}_{d_i+d_j}(\widetilde{x}))_{i,j \in [1..g]}$. If $(e_1, \cdots, e_g)$ is the canonical basis of $Z(\overline{\ell n})$, in the following, we take as a basis of $Z(\overline{\ell})$ the $d_i = ne_i$ if $i \in [1..g]$.

Proposition 5.1:

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x})).$$

Proof: We apply Corollary 4.12 with $\widetilde{y} = \widetilde{0}_{A_k}$, $\widetilde{x - y} = \widetilde{x}$, so that we have $\texttt{chaine\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x - y}) = \widetilde{x}$. We obtain:

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_{A_k}), \widetilde{\pi}_{i-j}(\widetilde{x})).$$ ■

Definition 5.2:
Let $S \subset G$ be a subset of a finite abelian group G such that $0_G \in S$. We note S' the inductive subset of G defined by $S' = S \bigcup \{x + y | x \in S', y \in S', x - y \in S'\}$. We say that S is a chain basis of G if $S' = G$.

Example 5.3:
Let $G = Z(\overline{\ell})$. Let $\{e_1, \cdots, e_g\}$ be the canonical basis of G. There are two cases to consider to get a chain basis of G:

- If ℓ is odd, then one can take

$$S = \{0_G, e_i, e_i + e_j\}_{i,j\in[1..g],i<j}$$

- If ℓ is even, we use

$$S = \{0_G, e_{i_1}, e_{i_1} + e_{i_2}, \cdots, e_{i_1} + \cdots + e_{i_g}\}_{i_1,\cdots,i_g\in[1..g],i_1<\cdots<i_g}$$

In each case, the chain basis S is minimal, we call it the canonical chain basis $\mathfrak{S}(G)$ of G.

We recall that we have defined a section $\mathscr{S} \subset Z(\overline{\ell n})$ of $Z(\overline{\ell n}) \to Z(\overline{n})$ in Example 3.6. To this set we associate a canonical chain basis $\mathfrak{S} \subset \mathscr{S}$ as follow: if ℓ is prime to n, then $\mathscr{S} = Z(\overline{\ell}) \subset Z(\overline{\ell n})$, and we define $\mathfrak{S} = \mathfrak{S}(Z(\overline{\ell})) = \{d_1, \cdots, d_g, d_1 + d_g, \cdots, d_{g-1} + d_g\}$. Otherwise we will take $\mathfrak{S} = \mathfrak{S}(Z(\overline{\ell n}))$.

Theorem 5.4 (Point compression):
Let $\widetilde{x} \in \widetilde{A}_k$. Then $\widetilde{x}$ is uniquely determined by $\widetilde{0}_{A_k}$ and $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathfrak{S}}$.
$\widetilde{0}_{A_k}$ is uniquely determined by $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}} = \{\widetilde{R}_i\}_{i\in\mathfrak{S}}$.

Proof: By Proposition 4.11 we have $\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_{A_k}), \widetilde{\pi}_{i-j}(\widetilde{x}), \widetilde{0}_{B_k})$. So by induction, from $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}}$ we can compute every $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}'}$. Since $\mathfrak{S}' = \mathscr{S}$ (or contains $\mathscr{S}$ if n is not prime to ℓ), Corollary 3.5 shows that $\widetilde{x}$ is entirely determined by $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}}$ and $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}}$.

In particular, $\widetilde{0}_{A_k}$ is entirely determined by $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}}$. But $\widetilde{\pi}_i(\widetilde{0}_{A_k}) = \widetilde{\pi}(\widetilde{P}_i)$. by Proposition 3.4 which concludes. ■

In the description of the algorithms, we suppose that ℓ is prime to n, so that $\mathscr{S} = Z(\overline{\ell}) \subset Z(\overline{\ell n})$.

Algorithm 5.5 (Point compression):
Input $\widetilde{x} = (\widetilde{\vartheta}_i(\widetilde{x}))_{i\in Z(\overline{\ell n})} \in \widetilde{A}_k$
Output The compressed coordinates $(\widetilde{\pi}_i(\widetilde{x}))_{i\in\mathfrak{S}}$.
Step 1 For each $i \in \mathfrak{S}$, output $(\widetilde{\pi}_i(\widetilde{x})) = (\widetilde{\vartheta}_{ni+\ell j}(\widetilde{x}))_{j\in Z(\overline{n})}$ ♢

Algorithm 5.6 (Point decompression):
Input The compressed coordinates $\widetilde{\pi}(\widetilde{x})_{i\in\mathfrak{S}}$ of $\widetilde{x}$.
Ouput $\widetilde{x} = (\widetilde{\vartheta}_i(\widetilde{x}))_{i\in Z(\overline{\ell n})} \in \widetilde{A}_k$.
Step 1 Set $\mathscr{S}' := \mathfrak{S}$.
Step 2 While $\mathscr{S}' \neq \mathscr{S}$, choose $i, j \in \mathscr{S}'$ such that $i + j \in \mathscr{S} \setminus \mathscr{S}'$ and $i - j \in \mathscr{S}'$.
Compute $\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x}))$.
$\mathscr{S}' := \mathscr{S}' \bigcup \{i + j\}$.

Step 3 For all $i \in Z(\overline{\ell n})$, write $i = ni_0 + \ell j$ and output $\widetilde{\vartheta}_i(x) = \left(\widetilde{\pi}_{i_0}(\widetilde{x})\right)_j$. ♢

Correction and Complexity Analysis 5.7:
By using repeatedly the formula from Proposition 4.11:

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x}), \widetilde{0}_{B_k})$$

we can reconstitute every $\widetilde{\pi}_i(\widetilde{x})$ for $i \in Z(\overline{\ell})$ in Step 2 since $\mathfrak{S}$ is a chain basis of $Z(\overline{\ell})$. We can then trivially recover the coordinates of $\widetilde{x}$ in Step 3 since they are just a permutation of the coordinates of the $\{\widetilde{\pi}_i(\widetilde{x}), i \in Z(\overline{\ell})\}$ (see Section 3.5).

To recover $\widetilde{x}$, we need to do $\#\mathscr{S} - \#\mathfrak{S} = O(\ell^g)$ chain additions. The compressed point $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathfrak{S}}$ is given by $\#\mathfrak{S} \times n^g$ coordinates.

If $\ell n = 2n_0$ and n_0 is odd we see that we can store a point in $\widetilde{A}_k$ with $2^g(1 + g(g+1)/2)$ coordinates (4^g if n_0 is even) rather than $(2n_0)^g$. ♢

5.1.1 Addition chains with compressed coordinates

Let $\widetilde{x}$, $\widetilde{y}$ and $\widetilde{x-y} \in \widetilde{A}_k$. Suppose that we have the compressed coordinates $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathfrak{S}}$, $\{\widetilde{\pi}_i(\widetilde{y})\}_{i\in\mathfrak{S}}$, $\{\widetilde{\pi}_i(\widetilde{x-y})\}_{i\in\mathfrak{S}}$. Then if $i \in \mathfrak{S}$ we have by Corollary 4.12

$$\widetilde{\pi}_i(\widetilde{x+y}) = \texttt{chaine\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_0(\widetilde{y}), \widetilde{\pi}_i(\widetilde{x-y}),$$

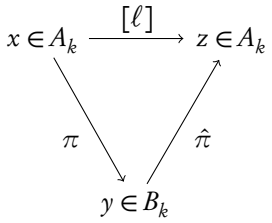
hence we may recover the compressed coordinates of $\widetilde{x+y}$.

We can compare this with an addition chain with the full coordinates (of level ℓn). By the formulas from Theorem 4.2, since $2|n$ and the formulas sum over points of 2-torsion, we see that we are doing $\#\mathscr{S}$ addition chains in B_k of level n. This mean that we are doing the same addition chains in B_k when we use a chain addition with compressed coordinates and then use the point decompression algorithm. But if we just need the compressed coordinates, the chain additions with compressed coordinates are much faster since we need to do only $\#\mathfrak{S}$ addition chains of level n. In particular, since we can compute the multiplication by m with chain additions, we see that the cost of a multiplication by m is $O(\#\mathfrak{S}\log(m))$ addition chains of level n.

Since we can take $n = 2$, this mean that the additions formulas of level 2 allows us to compute addition chains of any level. In particular the speed up for these formulas given by [Gau07] affects all levels.

5.2 Computing the dual isogeny

We recall that we have the following diagram:



Let $\widetilde{y} \in p_{B_k}^{-1}(y)$ and let $\widetilde{x} \in \widetilde{A}_k$ be such that $\widetilde{\pi}(\widetilde{x}) = \widetilde{y}$. Let $i \in Z(\overline{\ell})$. In this section, we describe an algorithm to compute $\widetilde{\pi}_i(\ell.\widetilde{x})$. By using this algorithm for $i \in \{d_1, \cdots, d_g, d_1 + d_2, \cdots d_{g-1} + d_g\}$, we can then recover $\hat{\pi}(y) = p_{A_k}(\ell.\widetilde{x})$ (see Theorem 5.4, $\{d_i\}_{i\in[1..g]}$ is the basis of $Z(\overline{\ell})$ defined in Section 5.1). We know that $\pi_i(x) = y + R_i$. For $i \in Z(\overline{\ell})$, we choose a point $\pi_i^a(x) \in p_A^{-1}(y + R_i)$ so that for each $i \in Z(\overline{\ell})$ there exists $\lambda_i \in \overline{k}^*$ such that $\widetilde{\pi}_i(\widetilde{x}) = \lambda_i \pi_i^a(x)$. If $\widetilde{x}'$ is another point in $\widetilde{\pi}^{-1}(y)$, then we have $\widetilde{\pi}_i(\widetilde{x}') = \lambda_i' \pi_i^a(x)$, with $\lambda_i' = \zeta\lambda_i$, ζ a ℓ-root of unity. As a consequence, it is possible to recover λ_i only up to an ℓ^{th}-root of unity, but this information is sufficient to compute $\widetilde{\pi}_i(\ell.\widetilde{x})$:

Theorem 5.8:
For all $i \in Z(\overline{\ell})$,

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \lambda_i^\ell \, \texttt{chaine\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, \widetilde{R}_i)),$$

where λ_i^ℓ is determined by:

$$\widetilde{y} = \lambda_i^\ell \, \texttt{chaine\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}).$$

Proof: By Proposition 4.11 and Lemma 4.8 we have:

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \texttt{chaine\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}(\widetilde{x}), \widetilde{\pi}(\widetilde{P}_i)) = \lambda_i^\ell \, \texttt{chaine\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, R_i).$$

Now we only need to find the λ_i^ℓ for $i \in Z(\overline{\ell})$. But by Proposition 4.11 and an easy recursion, we have $\widetilde{x} = s_{K_1(\mathscr{L})}(i)^\ell.\widetilde{x}$ so that by Corollary 4.12 and Lemma 4.8

$$\widetilde{\pi}(\widetilde{x}) = \texttt{chaine\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), R_i, \widetilde{y}) = \lambda_i^\ell . \texttt{chaine\_multadd}(\ell, \pi_i^a(x), R_i, \widetilde{y}) \quad \blacksquare$$

Algorithm 5.9 (The image of a point by the isogeny):
Input $y \in B_k$.
Output The compressed coordinates of $\hat{\pi}(y) \in A_k$.
Step 1 For each $i \in \mathfrak{S}$ compute $y + R_i$ and choose an affine lift y_i of $y + R_i$.
Step 2 For each $i \in \mathfrak{S}$, compute $\texttt{ylR}_i := \texttt{chaine\_multadd}(\ell, y_i, \widetilde{R}_i, y_0)$ and λ_i such that $y_0 = \lambda_i \texttt{ylR}_i$.
Step 3 For each $i \in \mathfrak{S}$, compute $\widetilde{\pi}(\hat{\pi}(y_0))_i = \lambda_i \, \texttt{chaine\_multadd}(\ell, y_i, \widetilde{y}, \widetilde{R}_i))$. $\diamondsuit$

Correction and Complexity Analysis 5.10:
In Step 3 we compute $\widetilde{\pi}_i(\hat{\pi}(y)) = \lambda_i^\ell$ `chaine_multadd`$(\ell, y_i, \widetilde{y}, \widetilde{R}_i))$ where λ_i^ℓ is given in Step 2 by by $\widetilde{y} = \lambda_i^\ell$ `chaine_multadd`$(\ell, y_i, \widetilde{R}_i, \widetilde{y})$.

We can easily recover $\hat{\pi}(y)$ from the $\widetilde{\pi}_i(\hat{\pi}(y)), i \in Z(\overline{\ell})$, but we note that it is faster to only compute the $\widetilde{\pi}_i(\hat{\pi}(y))$ only for $i \in \mathfrak{S}$ (with the notations of Example 5.3 in the preceding section), and then do a point decompression (see Algorithm 5.7). This last step is of course unnecessary if the compressed coordinates of $\hat{\pi}(y)$ are sufficient.

To compute $\widetilde{\pi}_i(\ell.x)$, we need to do two multiplication chains of length ℓ. We obtain the compressed coordinates of $\ell.x$ after $g(g+1)/2$ such operations. In total we can compute the compressed coordinates of a point in $O(\frac{1}{2}g(g+1)\log(\ell))$ additions in B_k (with $\frac{1}{2}g(g+1)n^g$ divisions in k) and the full coordinates in $O(\ell^g)$ additions in B_k. We recover the equations of the isogeny by applying this algorithm to the generic point of B_k. ♢

The case $(n,\ell) > 1$ In this case we have to use $\mathfrak{S} = \{e_1, \cdots, e_g, e_1 + e_2, \cdots\}$, and in this case if $i \in \mathfrak{S}$, $\widetilde{R}_i$ is a point of ℓn-torsion. But we have by Remark 4.14

$$(1, \ell i, 0).\widetilde{y} = \lambda_i^\ell \texttt{ chaine\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}),$$

so that we can still recover λ_i^ℓ.

The case $n = 2$ The only difficult part here is the ordinary additions $y + R_i$, since the addition chains do not pose any problems with $n = 2$. In particular, we first choose one of the two points $\pm(x \pm R_{e_1})$, which requires a square root. Now, since we have $\widetilde{0}_{A_k}$ given by a theta structure of degree $\ell n > 2$, we have the coordinates of $R_{e_1} + R_i$ on B_k. This means that we can compute the compatible additions $x + R_i$ from $x + R_{e_1}$ and $R_{e_1} + R_i$.

5.3 Computation of the kernel of the isogeny

We know that the kernel of the isogeny $\hat{\pi} : B \to A$ is the subgroup K generated by $\{R_{d_i}\}_{i \in [1..g]}$. Let $\widetilde{y} \in \widetilde{B}_k[\ell]$, up to a projective factor, we may suppose that `chaine_mult`$(\ell, \widetilde{y}) = \widetilde{0}_{B_k}$. Then y is in K if and only if for all $i \in Z(\overline{\ell})$ we have $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y})) = \widetilde{R}_i$. Let $\widetilde{y + R_i}$ be any affine point above $y + R_i$. Since y and R_i are points of ℓ-torsion, for all $i \in Z(\overline{\ell})$, there exist $\alpha_i, \beta_i \in \overline{k}^*$ such that `chaine_multadd`$(\ell, \widetilde{y + R_i}, \widetilde{y}, \widetilde{R}_i)) = \alpha_i \widetilde{R}_i$ `chaine_multadd`$(\ell, \widetilde{y + R_i}, \widetilde{R}_i, \widetilde{y}) = \beta_i \widetilde{y}$. By Theorem 5.8, we know that $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y})) = \frac{\alpha_i}{\beta_i}\widetilde{R}_i$. In particular $y \in K$ if and only if $\frac{\alpha_i}{\beta_i} = 1$ for all $i \in Z(\overline{\ell n})$.

In fact, we will show in Section 7 that $\alpha_i/\beta_i = e'_\ell(y, R_i)$ where e'_ℓ is the extended commutator pairing from Section 4.1. We obtain that y is in K if and only if $e_W(y, R_i) = 1$ for $i \in \{d_1, \cdots, d_g\}$.

6 The computation of a modular point

In the Section 6.1 we explain how to compute the theta null point $\widetilde{0}_{A_k}$ from the knowledge of the kernel of $\hat{\pi}$. This section introduces the notion of a "true" point of ℓ-torsion, which is an affine lift of a point of ℓ-torsion that satisfy Equation (27). We study this notion in Section 6.2, and we use these results in Section 6.3 where we study the computation of all (or just one) modular points.

6.1 An analog of Vélu's formulas

We have seen in Section 4 how to use the addition formula to compute the isogeny $\hat{\pi} : B_k \to A_k$. For this computation, we need to know the theta null point $(a_i)_{i\in Z(\overline{\ell n})}$ corresponding to A_k. In this section, we explain how to recover the theta null point $(a_i)_{i\in Z(\overline{\ell n})}$, given the kernel $K = \{T_i\}_{i\in Z(\overline{\ell})}$ of $\hat{\pi}$, by using only the addition relations. This gives an analog to Vélu's formulas for higher genus. As in the course of the algorithm we have to take ℓ^{th}-root in k, we suppose that k is algebraically closed. (If $k = \mathbb{F}_q$, with $\ell | q-1$ so that we have the ℓ-root of unity, we only have to work over an extension of degree ℓ of k).

Let $\{T_{d_1}, \cdots, T_{d_g}\}$ be a basis of K. Let $(a_i)_{i\in Z(\overline{\ell n})}$ be the theta null point corresponding to any theta structure on A_k compatible with the theta structure on B_k. The compatible automorphisms of the theta structure on A_k allows us to recover all the theta null point of the compatibles theta structures on A_k, via the actions:

$$\{\widetilde{R}_i\}_{i\in Z(\overline{\ell})} \mapsto \{\widetilde{R}_{\psi_1(i)}\}_{i\in Z(\overline{\ell})}, \tag{24}$$

$$\{\widetilde{R}_i\}_{i\in Z(\overline{\ell})} \mapsto \{e(\psi_2(i), i)\widetilde{R}_i\}_{i\in Z(\overline{\ell})}, \tag{25}$$

where ψ_1 is an automorphism of $Z(\overline{\ell})$ and ψ_2 is a symmetric endomorphism of $Z(\overline{\ell})$ (see [FLR09, Prop. 7]). The $\widetilde{R}_i$ were defined in Section 4.1, and we recall they determine $\widetilde{0}_{A_k}$ entirely. In fact the results of Section 5.1 show that $\widetilde{0}_{A_k}$ is completely determined by $\{\widetilde{R}_{d_i}, \widetilde{R}_{d_i+d_j}\}_{i,j\in[1..g]}$ where $d_1, \cdots, d_g$ is a basis of $Z(\overline{\ell})$.

Up to an action (24) we may suppose that $\widetilde{0}_{A_k}$ is such that $\widetilde{\pi}_{d_i}(\widetilde{0}_{A_k}) = T_{d_i}$. Fix $i \in Z(\overline{\ell})$. Let $\widetilde{T}_i$ be any affine point above T_i, we have $\widetilde{R}_i = \lambda_i \widetilde{T}_i$. Write $\ell = 2\ell' + 1$, since R_i is a point of ℓ-torsion, we have $(1, \ell'+1, 0).\widetilde{R}_i = -(1, \ell', 0).\widetilde{R}_i$. By Proposition 4.11 and Lemma 4.8, we have

$$\begin{aligned}
\texttt{chaine_mult}(\ell'+1, \widetilde{R}_i) &= -\texttt{chaine_mult}(\ell', \widetilde{R}_i),\\
\lambda_i^{(\ell'+1)^2}\texttt{chaine_mult}(\ell'+1, \widetilde{T}_i) &= -\lambda_i^{\ell'^2}\texttt{chaine_mult}(k, \widetilde{T}_i),\\
\lambda_i^{\ell}\texttt{chaine_mult}(\ell'+1, \widetilde{T}_i) &= -\texttt{chaine_mult}(\ell', \widetilde{T}_i).
\end{aligned} \tag{26}$$

Hence we may find λ_i up to an ℓ^{th}-root of unity. If we apply this method for $i \in$

$\{d_1,\cdots,d_g,d_1+d_2,\cdots,d_{g-1}+d_g\}$, we find $\widetilde{R}_i$ up to an ℓ^{th}-root of unity. But the action (25) shows that every choice of $\widetilde{R}_i$ comes from a valid theta null point $\widetilde{0}_{A_k}$.

Algorithm 6.1 (Vélu's like formula):

Input $T_{d_1},\cdots T_{d_g}$ a basis of the kernel K of $\hat{\pi}$.

Output The compressed coordinates of $\widetilde{0}_{A_k}$, the theta null point of level ℓn corresponding to $\hat{\pi}$.

Step 1 For $i,j\in[1..g]$ compute the points $T_{d_i}+T_{d_j}$. Let $\mathfrak{S}=\{d_1,\cdots,d_g,d_1+d_2,\cdots d_{g-1}+d_g\}$.

Step 2 For each $i\in\mathfrak{S}$ choose any affine lift T_i' of T_i, and compute $(\beta^i_j)_{j\in\mathbb{Z}(\overline{n})}:=\texttt{chaine\_mult}(\ell',T_i')$, and $(\gamma^i_j)_{j\in\mathbb{Z}(\overline{n})}:=\texttt{chaine\_mult}(\ell'+1,T_i')$.

Step 3 For each $i\in\mathfrak{S}$ compute α_i such that $(\gamma^i_j)_{j\in\mathbb{Z}(\overline{n})}=\alpha_i(\beta^i_{-j})_{j\in\mathbb{Z}(\overline{n})}$.

Step 4 For each $i\in\mathfrak{S}$, output $\widetilde{R}_i:=(\alpha_i)^{\frac{1}{\ell}}\cdot T_i'$. ♢

Correction and Complexity Analysis 6.2:

In Step 4 we compute $\widetilde{R}_i$ be any of the ℓ affine lift of T_i such that: $\texttt{chaine\_mult}(\ell'+1,\widetilde{R}_i)=-\texttt{chaine\_mult}(\ell',\widetilde{R}_i)$. Then $\{\widetilde{R}_i\}_{i\in\mathfrak{S}}$ give the compressed coordinates of $\widetilde{0}_{A_k}$, we can then recover $\widetilde{0}_{A_k}$ by doing a point decompression (see Algorithm 5.7).

To find $\widetilde{R}_i$, we need to do two chain multiplications of length $\ell/2$, and then take an ℓ^{th}-root of unity. After $g(g+1)/2$ such operations, we obtain the compressed coordinates of a $\widetilde{0}_{A_k}$, and we may recover the full coordinates of the corresponding $\widetilde{0}_{A_k}$ using the point decompression algorithm 5.7. We remark that we only need the compressed coordinates of $\widetilde{0}_{A_k}$ to compute the compressed coordinates of $\hat{\pi}$. In total we need to compute $g(g+1)/2$ ℓ^{th}-roots of unity and $O(\frac{1}{2}g(g+1)\log(\ell))$ additions in B_k to recover the compressed coordinates of $\widetilde{0}_{A_k}$. We can then recover the full coordinates of $\widetilde{0}_{A_k}$ at the cost of $O(\ell^g)$ additions in B_k. ♢

Remark 6.3:

Each choice of the $g(g+1)/2$ ℓ^{th}-roots of unity give a theta null point corresponding to the same Abelian variety $A_k=B_k/K$. However, each such point comes from a different theta structure on A_k, and hence give a different decomposition of the ℓ-torsion $A[\ell]=K_1(\ell)\oplus K_2(\ell)$. Since $B_k=A_k/K_2(\ell)$, $K_2(\ell)=K$ is fixed so that each point gives a different $K_1(\ell)$. This mean that if $C_k=A_k/K_1(\ell)$ we can recover different ℓ^2-isogeny $B_k\to C_k$ from such choices (see Section 3.3). By looking at the action (25), we see that there is a bijection between the $\ell^{g(g+1)/2}$ choices and the ℓ^2 isogenies whose kernel $\mathfrak{K}\subset B_k$ is such that $\mathfrak{K}[\ell]=K$. ♢

The case $(n,\ell)>1$. In this case once again we have to recover $\widetilde{R}_i$ for $i\in\mathfrak{S}=\{e_1,\cdots,e_g,e_1+e_2,\cdots,e_1+e_g\}$. Suppose that we have $\{T_i\}_{i\in\mathbb{Z}(\overline{\ell})}$, ℓ^g points of ℓn-torsion such that $\ell.T_i=(1,\ell i,0).0_B$. Once again if $i\in\mathfrak{S}$, we may suppose that $\widetilde{R}_i=\lambda_i\widetilde{T}_i$.

We have if $\ell = 2\ell' + 1$ is odd:

$$\lambda_i^{\ell}\, \texttt{chaine\_mult}(\ell'+1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\, \texttt{chaine\_mult}(\ell', \widetilde{T}_i)$$

so that once again we can find λ_i^{ℓ}.

The kernel of $\hat{\pi}$ is then $K = \{nT_i\}_{i \in Z(\bar{\ell})}$. Even if K is isotropic, the $\{T_i\}_{i \in Z(\bar{\ell})}$ may not be, so some care must be taken when we choose the $\{T_i\}_{i \in Z(\bar{\ell})}$.

If $\ell = 2\ell'$ is even, we have:

$$\lambda_i^{2\ell}\, \texttt{chaine\_mult}(\ell'+1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\, \texttt{chaine\_mult}(\ell'-1, \widetilde{T}_i)$$

so we can recover only $\lambda_i^{2\ell}$. But every choice still corresponds to a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$, because when $2|\ell$, to the actions (24) and (25) we have to add the action given by the change of the maximal symmetric level structure [FLR09, Proposition 7].

The case $n = 2$ Once again, the only difficulty rest in the standard additions. Using standard additions, we may compute $R_{e_1} \pm R_{e_2}, \cdots, R_{e_1} \pm R_{e_g}$, making a choice each time. Then we can compute $R_{e_i} + R_{e_j}$ by doing an addition compatible with $R_{e_1} + R_{e_i}$ and $R_{e_1} + R_{e_j}$.

6.2 Theta group and ℓ-torsion

Let $\widetilde{x} \in \widetilde{B}_k$ be such that $p_{B_k}(x)$ is a point of ℓ-torsion. We say that x is a "true" point of ℓ-torsion if $\widetilde{x}$ satisfy (see (26)):

$$\texttt{chaine\_mult}(\ell'+1, \widetilde{x}) = -\,\texttt{chaine\_mult}(\ell', \widetilde{x}). \tag{27}$$

Remark 6.4:
If $\widetilde{x}$ is a "true" point of ℓ-torsion, then Lemma 4.8 shows it is also the case for $\lambda\widetilde{x}$ for any λ an ℓ^{th}-root of unity. ♢

We have seen in the preceding Section the importance of taking lifts that are "true" points of ℓ-torsion. The aim of this section is to use the results of Section 4.3 to show that the addition chain of "true" points of ℓ-torsion is again a "true"-point of ℓ-torsion. We will use this in Section 6.3 to compute "true" affine lifts of $B_k[\ell]$ by taking as few ℓ^{th}-roots as possible.

We will use the affine lifts of points in $B_k[\ell]$ that we have introduced in Section 4.1 to study this notion. Let $\mathscr{M}_0 = [\ell]^* \mathscr{L}_0$ on B_k and $\Theta_{B_k, \mathscr{M}_0}$ a theta structure for $\mathscr{M}_0$ compatible with Θ_{B_k}. Recall that we note $\widetilde{B_k}'$ the affine cone of $(B_k, \mathscr{M}_0)$, and $\widetilde{[\ell]}$ the morphism $\widetilde{B_k}' \to \widetilde{B}_k$ induced by $[\ell]$. Since $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$, the natural action of $G(\mathscr{M}_0)$ on $H^0(\mathscr{M}_0)$ give via $\Theta_{B_k, \mathscr{M}_0}$ an action of $\mathscr{H}(\overline{\ell^2 n})$ on $H^0(\mathscr{M}_0)$.

Lemma 6.5:
Let $y \in B_k[\ell], \widetilde{y} \in p_{B_k}^{-1}(y)$ and $\widetilde{x} \in \widetilde{[\ell]}^{-1}(\widetilde{y})$. Then there exists $(\alpha, ni, nj) \in k^\ell \times Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$ such that $\widetilde{x} = (\alpha, ni, nj).0_{\widetilde{B_k}'}$. Moreover, $\widetilde{y}$ is a true point of ℓ-torsion if and only if $\alpha = \lambda_{i,j}\mu$ where μ is an ℓ^{th}-root of unity and $\lambda_{i,j} = e_c(i,-j)^{\ell' n(\ell-1)}$.

(If $x' \in \widetilde{B_k}'$, then $x' \in \widetilde{[\ell]}^{-1}(y)$ if and only if $x' = (1, \ell i', \ell j').x$ where $(i', j') \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$), so the class of α in $k^*/k^{*\ell}$ does not depend on $\widetilde{x}$ but only on $\widetilde{y}$).

Proof: Since $p_{\widetilde{B_k}'}(\widetilde{x}) \in B_k[\ell^2]$, there is an element $h \in \mathscr{H}(\overline{\ell^2 n})$ such that $\widetilde{x} = h.0_{\widetilde{B_k}'}$, with $h = (\alpha, ni, nj)$. By Remark 6.4, we only need to check that $(\lambda_{i,j}, ni, nj).0_{\widetilde{B_k}'}$ is a "true" point of ℓ-torsion. Let $m \in \mathbb{Z}$, and let $\widetilde{x}_m = \texttt{chaine\_mult}(m, \widetilde{x})$, $\widetilde{y}_m = \texttt{chaine\_mult}(m, \widetilde{y})$. By Corollary 4.16 we have $\widetilde{x}_m = (1, m\cdot i, m\cdot j).0_{\widetilde{B_k}'}$, and by Corollary 4.16 $\widetilde{y}_m = \widetilde{[\ell]}(1, m\cdot i, m\cdot j).0_{\widetilde{B_k}'}$. So by Lemma 4.10 $\widetilde{y}_{\ell'} = \widetilde{[\ell]}(1, \ell'\cdot i, \ell'\cdot j).0_{\widetilde{B_k}'} = e_c(ni, \ell n(\ell-1)j)\widetilde{[\ell]}(1, \ell'\cdot i + \ell n(\ell-1), \ell'\cdot j + \ell n(\ell-1)).0_{\widetilde{B_k}'} = \lambda_{i,j}^{-\ell}\widetilde{[\ell]}(1, -(\ell'+1)\cdot i, -(\ell'+1)\cdot j).0_{\widetilde{B_k}'} = \lambda_{i,j}^{-\ell}\widetilde{[\ell]}(-\widetilde{x}_{\ell'+1}) = -\lambda_{i,j}^{-\ell}\widetilde{y}_{\ell'+1}$. ■

Proposition 6.6:
Let $\widetilde{y}_1, \widetilde{y}_2, \widetilde{y_1 - y_2} \in \widetilde{B}_k$ be points of "true" ℓ-torsion. Then $\widetilde{y_1 + y_2} := \texttt{chaine\_add}(\widetilde{y}_1, \widetilde{y}_2, \widetilde{y_1 - y_2})$ is a "true" point of ℓ-torsion.

Proof: Let $(\alpha_1, i_1, j_1) \in \mathscr{H}(\overline{\ell^2 n})$, $(\alpha_2, i_2, j_2) \in \mathscr{H}(\overline{\ell^2 n})$, $(\alpha_3, i_3, j_3) \in \mathscr{H}(\overline{\ell^2 n})$, be such that

$$\widetilde{[\ell]}(\alpha_1, i_1, j_1).0_{\widetilde{B_k}'} = \widetilde{y}_1, \quad \widetilde{[\ell]}(\alpha_2, i_2, j_2).0_{\widetilde{B_k}'} = \widetilde{y}_2, \quad \widetilde{[\ell]}(\alpha_3, i_3, j_3).0_{\widetilde{B_k}'} = \widetilde{y_1 - y_2}$$

By the Remark at the end of Lemma 6.5, we may suppose that $i_3 = i_1 - i_2$, $j_3 = j_1 - j_2$. Since $\widetilde{y}_1, \widetilde{y}_2$ and $\widetilde{y_1 - y_2}$ are "true" points of ℓ-torsion, by Remark 6.4 and Lemma 6.5 we may suppose that $\alpha_1 = \lambda_{i_1, j_1}$, $\alpha_2 = \lambda_{i_2, j_2}$ and $\alpha_3 = \lambda_{i_1 - i_2, j_1 - j_2}$.

By Corollary 4.16 and Lemma 4.8, we have

$$\widetilde{y_1 + y_2} = \frac{\lambda_{i_1,j_1}^2 \lambda_{i_2,j_2}^2}{\lambda_{i_1 - i_2, j_1 - j_2}}(1, i_1 + i_2, j_1 + j_2).0_{\widetilde{B_k}'} = (\lambda_{i_1+i_2, j_1+j_2}, i_1 + i_2, j_1 + j_2).0_{\widetilde{B_k}'},$$

so $\widetilde{y_1 + y_2}$ is indeed a "true" point of ℓ-torsion by Lemma 6.5. ■

6.3 Improving the computation of a modular point

In [FLR09], to compute the modular points $\widetilde{0}_{A_k}$, the following algorithm was used: write the Riemann relations of level ℓn to get a system in which we plug the known coordinates $\widetilde{0}_{B_k}$. We obtain a system S of with a finite number of solutions, that can be solved using a Gröbner basis algorithm. But even for $g = 2$ and $\ell = 3$, the system was too hard to be solved with a general Gröbner basis algorithm, so we had to design a specific one.

In this section we explain how, using the "Vélu's"-like formulas of Section 6.1, it is possible to recover every modular point $\widetilde{0}_{A_k}$ solution of the system S from the knowledge of the ℓ-torsion of B_k. We then discuss different methods to compute the ℓ-torsion in B_k.

Algorithm 6.7 (Computing all modular points):
Input $T_1, \cdots, T_{2g}$ a basis of the ℓ-torsion of B_k.
Output All ℓ-isogenies.

We only give an outline of the algorithm, since we give a detailed description in Example 6.8: Compute any affine "true" ℓ-torsion lifts $\widetilde{T}_1, \cdots, \widetilde{T}_{2g}, \widetilde{T_1+T_2}, \cdots, \widetilde{T_{g-1}+T_g}$, and then use addition chains to compute affine lifts $\widetilde{T}$ for every point $T \in B_k[\ell]$. By Proposition 6.6 $\widetilde{T}$ is a "true" point of ℓ-torsion.

For every isotropic subgroup $K \subset B_k[\ell]$, take the corresponding lifts and use them to reconstitute the corresponding theta null point $\widetilde{0}_{A_k}$ (see Section 6.1). ♢

Example 6.8:
Suppose that $\{T_1, \ldots, T_{2g}\}$ is a symplectic basis of $B_k[\ell]$. (A symplectic basis is easy to obtain from a basis of the ℓ-torsion, we just need to compute the discrete logarithms of some of the pairings between the points, and we can use Algorithm 7.5 to compute these).

Let $\Theta_{B_k,\mathscr{M}_0}$ be any theta structure of level $\ell^2 n$ on B_k compatible with Θ_{B_k}, and $\widetilde{0}'_{B_k}$ be the corresponding theta null point (see Section 4.1). We may suppose (see Section 6.1) that $\widetilde{T}_1 = \widetilde{[\ell]}(1,(n,0,\cdots,0),0).\widetilde{0}'_{B_k}$, $\widetilde{T}_2 = \widetilde{[\ell]}(1,(0,n,\cdots,0),0).\widetilde{0}'_{B_k}, \ldots, \widetilde{T_{g+1}} = \widetilde{[\ell]}(1,0,(n,0,\cdots,0)).\widetilde{0}'_{B_k}$, $\widetilde{T_{g+2}} = \widetilde{[\ell]}(1,0,(0,n,\cdots,0)).\widetilde{0}'_{B_k}, \ldots, \widetilde{T_1+T_{g+2}} = \widetilde{[\ell]}(1,(n,0,\cdots,0),(0,n,0,\cdots,0)).\widetilde{0}'_{B_k}, \ldots$

Then by Corollary 4.16, using Algorithm 6.7, we compute the following affine lifts of the ℓ-torsion:

$$\{\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k} : i,j \in \{0,1,\cdots,\ell-1\}^g \subset Z(\ell^2 n)\}. \tag{28}$$

Now if $K \subset B_k[\ell]$ is an isotropic group, in the reconstruction algorithm 6.1 we need to compute points of the form $\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k}$ for $i,j \in Z(\ell^2 n)$. But we have

$$\begin{aligned}\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k} &= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1,\ell\alpha n,\ell\beta n).(1,(i-\ell\alpha)n,(j-\ell\beta)n).\widetilde{0}'_{B_k}\\ &= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1,(i-\ell\alpha)n,(j-\ell\beta)n).\widetilde{0}'_{B_k},\end{aligned}$$

where $\alpha, \beta \in Z(\ell^2 n)$, and ζ is a $(\ell^2 n)^{th}$-root of unity. As a consequence, we can always go back to a point computed in (28) up to an ℓ^{th}-root of unity.

We give a detailed example with $g = 1$, $\ell = 3$, $n = 4$. Let B_k be an elliptic curve, with a theta structure Θ_{B_k} of level n. Let T_1, T_2 be a basis of $B_k[\ell]$, and choose "true" affine lifts $\widetilde{T}_1, \widetilde{T}_2, \widetilde{T_1+T_2}$. Let $\Theta_{B_k,\mathscr{M}_0}$ be any theta structure of level $\ell^2 n$ compatible with Θ_{B_k}, and $\widetilde{0}'_{B_k}$ be the corresponding theta null point (see Section 4.3). We take $\Theta_{B_k,\mathscr{M}_0}$ such that $\widetilde{T}_1 = \widetilde{[\ell]}(1,n,0).\widetilde{0}'_{B_k}$, $\widetilde{T}_2 = \widetilde{[\ell]}(1,0,n).\widetilde{0}'_{B_k}$, and $\widetilde{T_1+T_2} = \widetilde{[\ell]}(1,n,n).\widetilde{0}'_{B_k}$.

We have seen in (28) that in the Algorithm 6.7 we compute the points: $\widetilde{[\ell]}(1, in, jn).\widetilde{0}'_{B_k}$ for $i, j \in 0, 1, \cdots, \ell - 1 \subset \mathbb{Z}/\ell^2 n\mathbb{Z}$.

Now let $T = \widetilde{[\ell]}(1, n, 2n).\widetilde{0}'_{B_k}$, $K =< p_{B_k}(T) >$ is an isotropic subgroup of $B_k[\ell]$. Let $A_k = B_k/K$, choose a compatible theta structure Θ_{A_k} on A, and let $\widetilde{0}_{A_k}$ be the associated theta null point.

As usual, we define $\widetilde{R}_i = \widetilde{\pi}_i(\widetilde{0}_{A_k})$ if $i \in \mathbb{Z}/\ell Z \subset \mathbb{Z}/\ell n\mathbb{Z}$, and we may suppose (Section 6.1) that Θ_{A_k} is such that $R_1 = T$. More explicitly, if $n = 4$ we have $\widetilde{0}_{A_k} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$, $\widetilde{\pi}((x_i)_{i\in\mathbb{Z}/12\mathbb{Z}}) = (x_0, x_3, x_6, x_9)$ so that $\widetilde{R}_0 = (a_0, a_3, a_6, a_9) = \widetilde{0}_{B_k}$ (Remember that we always choose $\widetilde{0}_{A_k}$ such that $\widetilde{\pi}(\widetilde{0}_{A_k}) = \widetilde{0}_{B_k}$), $\widetilde{R}_1 = (a_4, a_7, a_{10}, a_1)$ and $\widetilde{R}_2 = (a_8, a_{11}, a_2, a_5)$. Now by Theorem 5.4 we know that $\widetilde{0}_{A_k}$ is entirely determined by $\widetilde{R}_1$ (and $\widetilde{0}_{B_k}$), in fact we have: $\widetilde{R}_2 = \texttt{chaine\_add}(R_1, R_1, \widetilde{0}_{B_k})$. By Corollary 4.16, we have

$$\widetilde{R}_2 = \widetilde{[\ell]}(1, 2n, 4n).\widetilde{0}'_{B_k} = \widetilde{[\ell]}\zeta^{2n\cdot 3n}(1, 0, 3n).(1, 2n, n).\widetilde{0}'_{B_k} = \zeta^{2n\cdot 3n}\widetilde{[\ell]}(1, 2n, n).\widetilde{0}'_{B_k},$$

where ζ is a $(\ell^2 n)^{th}$-root of unity.

This shows that in the reconstruction step, we have to multiply the point $\widetilde{[\ell]}(1, 2n, n).\widetilde{0}'_{B_k}$ which we have already computed by the ℓ-root of unity $\zeta^{2n\cdot\ell n}$.

Complexity Analysis 6.9:
To compute an affine lift $\widetilde{T}_i$, we have to compute an ℓ^{th}-root of unity (and do some addition chains but we can reuse the results for the next step). Once we have computed the $\ell(2\ell + 1)$-root, we compute the whole (affine lifts of) ℓ-torsion by using $O(\ell^{2g})$ addition chains. We can now compute the pairings $e(T_i, T_j)$ with just one division since we have already computed the necessary addition chain (see Section 7). From these pairings we can compute a symplectic basis of $B_k[\ell]$. This requires to compute the discrete logarithm of the pairings and can be done in $O(\ell)$. Using this basis, we can enumerate every isotropic subgroup $K \subset B_k[\ell]$, and reconstruct the corresponding theta null point with $O(\ell^g)$ multiplications by an ℓ^{th}-root of unity. ♢

The case $(n, \ell > 1)$ In this case, the only difference is that we have to compute $B_k[\ell n]$ rather than $B_k[\ell]$, and when T_i is a point of ℓn-torsion, we compute an affine lift $\widetilde{T}_i$ such that:

$$\texttt{chaine\_mult}(\ell' + 1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\,\texttt{chaine\_mult}(\ell', \widetilde{T}_i).$$

The case $n = 2$: This works as in Section 6.1, once we have computed the $\widetilde{T_{e_1}} + \widetilde{T_{e_i}}$, we have to take compatible additions to compute the $\widetilde{T_{e_i}} + \widetilde{T_{e_j}}$.

Computing the points of ℓ-torsion in B_k: The first method is to use the Riemann relations of level $\delta = (n, n, n, \cdots, \ell n)$. Let $\varphi : Z(\overline{n}) \to Z(\delta)$ be the canonical injection. Let $\mathscr{M}_\delta$ be the modular space of theta null points of level δ, and V_J the subvariety defined by the ideal J generated by $a_{\varphi(i)} = b_i$ for $i \in Z(\overline{n})$.

Then to every (non degenerate) point solution correspond an isogeny $\pi : A_k \to B_k$. The kernel of the contragredient of π is then of the form $\{0_{B_k}, T, 2T, \cdots, (\ell-1)T\}$ where T is a primitive point of ℓ-torsion. We may recover T as follows: if $i \in \mathbb{Z}/\ell\mathbb{Z}$, let $\pi_i = \pi \circ s_1(0, 0, \cdots, ni)$, then we have $\pi_i(\widetilde{0}_{A_k}) = i \cdot T$.

By using this method for every point solution (even the degenerate ones), we find all the points of ℓ-torsion (the degenerate point solutions giving points of ℓ-torsion that are not primitive [FLR09, Theorem 4]).

When we look at the equations of V_J, we see that we can reformulate them as follows. Let $R_1, \cdots, R_{\ell-1}$ be the $\ell - 1$ projections of the generic point of $\widetilde{B}_k \times \widetilde{B}_k \times \cdots \times \widetilde{B}_k$ and let $R_0 = \widetilde{0}_{B_k}$. Then the equations on B_k comes from the addition relations: for all $i, j \in Z(\overline{\ell})$,

$$R_{i+j} = \texttt{chaine\_add}(R_i, R_j, R_{i-j}).$$

We see that we can describe the system with less unknowns and equations by looking only at equations of the form:

$$R_{2i} = \texttt{chaine\_add}(R_i, R_i, R_0),$$
$$R_{2i+1} = \texttt{chaine\_add}(R_{i+1}, R_i, R_0).$$

This requires $n^g O(\log(\ell))$ variables, and each equations is of degree 4.

A second method is to work directly over the variety B_k. The Riemann relations (11) allows us to compute the ideal of ℓ-division in B_k. Here we have n^g unknown, but the equations are of degree ℓ^{2g}. Contrary to the first method, we recover projective points of ℓ-torsion, so we have to compute an ℓ^{th}-root of unity to compute a "true" affine lift of ℓ-torsion. But this mean that the degree of our system is ℓ^{2g} rather than ℓ^{2g+1}, so a generic Gröbner basis algorithm will finish faster. In genus 2, using a Core 2 with 4 GB of RAM, this allows us to compute up to $\ell = 13$.

In general we prefer to work over the Kummer surface (so with $n = 2$), since it cuts the degree of the system by two. In genus 2, Gaudry and Schost [GS08] have an algorithm to compute the ℓ-torsion on the Kummer surface using resultants rather than a general purpose Gröbner-based algorithm. The points are given in Mumford coordinates, but we can use the results of Wamelen [Wam99] to have them in theta coordinates. With this algorithm, we can go up to $\ell = 31$. This algorithm is in $\widetilde{O}(\ell^6)$ (where we use the notation $\widetilde{O}$ to mean we forget about the log factors). The computation of the "true" affine points of ℓ-torsion from Algorithm 6.7 is in $\widetilde{O}(\ell^4)$, and each of the $O(\ell^3)$ isogeny requires $O(\ell^2)$ multiplication by an ℓ^{th}-root of unity. In total we see that we can compute all (ℓ, ℓ)-isogenies in $\widetilde{O}(\ell^6)$ in genus 2.

Lastly, if we know the zeta function of B_k (for instance if B_k comes from complex multiplication), we can recover a point of ℓ-torsion by taking a random point of B_k and multiplying it by the required factor.

Isogenies graph:

Usually when we compute every isogenies, this is to build isogenies graph. However, our Vélu's like algorithm from Section 6.1 gives us a theta null point 0_{A_k} of level ℓn from a point of level n. We can use the Modular correspondence from Section 3.3 to go back to a theta null point 0_{C_k} of level n, but the corresponding isogeny $B_k \to C_k$ is a ℓ^2 isogeny, so with our method we can only draw ℓ^2-isogenies graphs.

There is however one advantage of using the intermediate step 0_{A_k}: since it is a theta null point of level ℓn, we have all the ℓ-torsion on A_k. Let $\pi_2 : A_k \to C_k$ be the corresponding isogeny, $K_2 := \pi_2(A_k[\ell])$ gives us half the ℓ-torsion of C_k. (to get an explicit description of K_2, just apply $\mathfrak{I}$ to the results of Section 3.4). Since K_2 is the kernel of the dual isogeny $C_k \to A_k$, this allows us to build an isogeny graph of ℓ^2 isogenies where the composition of two such isogenies give an ℓ^4-isogeny and not (for instance if $g = 2$) a $(1, \ell^2, \ell^2, \ell^4)$-isogeny (it suffices to consider the isotropic subgroups of $C_k[\ell]$ that intersect K_2 trivially). The knowledge of K_2 also allows us to speed up the computation of $C_k[\ell]$: In the following section, we will give an algorithm to compute the extended commutator pairing e on $C_k[\ell]$. Let $(G_1, \cdots, G_g)$ be a basis of K_2, and consider the system of degree ℓ^{g+1} given by the ideal of ℓ-torsion and the relations $e(G_i, \cdot) = 1$ for $i \in [2..g]$. Let H_1 be a point in this system different from $< G_1 >$ (it suffices to check that $e(G_1, H_1) \neq 1$. We can now construct the system of degree ℓ^g given by the ideal of ℓ-torsion and the relations $e(G_i, \cdot) = 1$ for $i \neq 2$ and $e(H_1, \cdot) = 1$; and look for a solution H_2 such that $e(G_2, H_2) \neq 1$. We see that we can construct a basis $G_1, \cdots, G_g, H_1, \cdots, H_g$ of $C_k[\ell]$ by solving a system of degree ℓ^{g+1}, then of degree ℓ^g, ..., then of degree ℓ^2. This is faster than solving the ideal of ℓ-torsion which is a system of degree ℓ^{2g}.

7 Pairing computations

In this section, we explain how to use the addition chains introduced in Section 4.2 in order to compute the commutator, Weil and Tate pairings on Abelian varieties. We suppose here that B_k is provided with a polarization $\mathscr{L}_0$ which is the n^{th} power of a principal polarization. This allows us to make the link between the extended commutator pairing and the Weil pairing in Section 7.1. We then give an algorithm to compute the extended commutator pairing in Section 7.2.

7.1 Weil pairing and commutator pairing

We recall the definition of the extended commutator pairing from Section 4.1: Let $\mathscr{M}_0 = [\ell]^*\mathscr{L}_0$ on B_k. As $\mathscr{L}_0$ is symmetric, we have that $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$ and as a consequence $K(\mathscr{M}_0)$, the kernel of $\mathscr{M}_0$ is isomorphic to $K(\overline{\ell^2 n})$. The polarization $\mathscr{M}_0$ induces a commutator pairing $e_{\mathscr{M}_0}$ ([Mum66]) on $K(\mathscr{M}_0)$ and as $\mathscr{M}_0$ descends to $\mathscr{L}_0$ via the isogeny $[\ell]$, we know that $e_{\mathscr{M}_0}$ is trivial on $B_k[\ell]$. For $x_1, x_2 \in B_k[\ell]$, let $x_1', x_2' \in B_k[\ell^2]$ be such that $\ell.x_i' = x_i$ for $i = 1, 2$. The extended commutator pairing is then $e'_\ell(x_1, x_2) = e_{\mathscr{M}_0}(x_1', x_2) = e_{\mathscr{M}_0}(x_1, x_2')$, this is a well defined bilinear application $e'_\ell : B_k[\ell] \times B_k[\ell] \to \overline{k}$. As $e_{\mathscr{M}_0}$ is a perfect pairing, for

any $x_1' \in B_k[\ell^2]$ there exits $x_2' \in B_k[\ell^2]$ such that $e_{\mathscr{M}_0}(x_1', x_2')$ is a primitive ℓ^{2th} root of unity. As a consequence, for any $x_1 \in B_k[\ell]$ there exists $x_2 \in B_k[\ell]$ such that $e'_\ell(x_1, x_2)$ is a primitive ℓ^{th} root of unity and e'_ℓ is also a perfect pairing.

As the kernel of $\mathscr{L}_0$ is $B_k[n]$, we have an isogeny $B_k \to \hat{B}_k$ with kernel $B_k[n]$ and by composing this isogeny on the right side of e'_ℓ, we obtain a perfect pairing $e'_W : B_k[\ell] \times \hat{B}_k[\ell] \to \mu_\ell$ where μ_ℓ is the subgroup of ℓ^{th}-roots of unity of $\overline{k}$.

We have

Proposition 7.1:
The pairing e'_W is the Weil pairing e_W.

Proof: For $y \in \hat{B}_k[\ell]$, we denote by Λ_y the degree-0 line bundle on B_k associated to y. We first recall a possible definition of the Weil pairing e_W. Let $(x, y) \in B_k[\ell] \times \hat{B}_k[\ell]$. Let $\mathscr{O}_{B_k}$ be the structural sheaf of B_k, and as $y \in \hat{B}_k[\ell]$ there is an isomorphism $\psi'_y : [\ell]^*\Lambda_y \simeq \mathscr{O}_{B_k}$. As a consequence, Λ_y is obtained as the quotient of the trivial bundle $B_k \times \mathbb{A}^1_k$ over B_k by an action g of $B_k[\ell]$ on $B_k \times \mathbb{A}^1_k$ given by $g_x(t, \alpha) = (t + x, \chi(x).\alpha)$ where $(t, \alpha) \in (B_k \times \mathbb{A}^1_k)(\overline{k})$, $x \in B_k[\ell]$ and χ is a character of $B_k[\ell]$. By definition [Mum70], we have $e_W(x, y) = \chi(x)$.

In order to give another formulation of this definition, we chose an isomorphism $\mathscr{O}_{B_k}(0) \simeq k$ from which we deduce via ψ'_y (resp. $\tau_x^*\psi'_y$) an isomorphism $\psi_0 : [\ell]^*\Lambda_y(0) \simeq k$ (resp. $\psi_1 : \tau_x^*[\ell]^*\Lambda_y(0) \simeq k$). There exists a unique isomorphism $\psi_x : [\ell]^*\Lambda_y \to \tau_x^*[\ell]^*\Lambda_y$ compatible on the 0 fiber with ψ_0 and ψ_1, i.e. we have that $\psi_1 \circ \psi_x \circ \psi_0^{-1}$ is the identity of k. Then, the following diagram commutes up to a multiplication by $e_W(x, y)$:

$$\begin{array}{ccc} [\ell]^*\Lambda_y & \xrightarrow{\psi'_y} & \mathscr{O}_{B_k} \\ \downarrow{\scriptstyle \psi_x} & & \| \\ \tau_x^*[\ell]^*\Lambda_y & \xrightarrow{\tau_x^*\psi'_y} & \tau_x^*\mathscr{O}_{B_k} \end{array} \qquad e_W(x, y)$$

The polarization $\mathscr{L}_0$ gives the natural isogeny $\varphi_{\mathscr{L}_0}$, defined on geometric points by

$$\begin{aligned} \varphi_{\mathscr{L}_0}(\overline{k}) : B_k(\overline{k}) &\to \hat{B}_k(\overline{k}) \\ y &\mapsto \Lambda_y = \mathscr{L}_0 \otimes (\tau_y^*\mathscr{L}_0)^{-1}. \end{aligned}$$

As a consequence, for $y \in \hat{B}_k[\ell]$ there exists $y_0 \in B_k(\overline{k})$ such that $\Lambda_y = \mathscr{L}_0 \otimes (\tau_{y_0}^*\mathscr{L}_0)^{-1}$. Let $y' \in B_k[\ell^2]$ be such that $\ell.y' = y_0$. As $[\ell]^*\mathscr{L}_0 = \mathscr{M}_0$, we have $[\ell]^*\Lambda_y = [\ell]^*(\mathscr{L}_0 \otimes (\tau_{y_0}^*\mathscr{L}_0)^{-1}) = \mathscr{M}_0 \otimes (\tau_{y'}^*\mathscr{M}_0)^{-1}$. We remark that the isomorphism $\psi'_y : [\ell]^*\Lambda_y = \mathscr{M}_0 \otimes (\tau_{y'}^*\mathscr{M}_0)^{-1} \to \mathscr{O}_{B_k}$ gives by tensoring on the right by $\tau_{y'}^*\mathscr{M}_0$ an isomorphism $\psi_{y'} : \mathscr{M}_0 \to \tau_{y'}^*\mathscr{M}_0$. Thus, the following diagram is commutative up to a multiplication by $e_W(x, y)$:

$$\begin{array}{ccc} \mathscr{M}_0 & \xrightarrow{\psi_{y'}} & \tau_{y'}^*\mathscr{M}_0 \\ \downarrow{\scriptstyle \psi_x} & & \downarrow{\scriptstyle \tau_{y'}^*\psi_x} \\ \tau_x^*\mathscr{M}_0 & \xrightarrow{\tau_x^*\psi_{y'}} & \tau_{x+y'}^*\mathscr{M}_0 \end{array}$$

■

But this is exactly the definition of $e'_W(x,y)$ thus we have $e'_W(x,y) = e_W(x,y)$.

7.2 Commutator pairing and addition chains

In this paragraph, we explain how to compute the pairing e'_ℓ using addition chains. From Section 7.1 this give a different algorithm to compute the Weil pairing than the usual Miller loop [Mil04]. We chose a theta structure $\Theta_{B_k,\mathscr{M}_0}$ for $\mathscr{M}_0$ compatible with Θ_{B_k} (see Section 3.3) from which we deduce a decomposition $K(\mathscr{M}_0) = K_1(\mathscr{M}_0) \times K_2(\mathscr{M}_0)$ of $K(\mathscr{M}_0)$ into isotropic subspaces for the commutator pairing and a basis $(\vartheta_i)_{i \in Z(\overline{\ell^2 n})}$ of $H^0(\mathscr{M}_0)$. We recall that there is a natural action of $G(\mathscr{M}_0)$ on $H^0(\mathscr{M}_0)$ which can transported via $\Theta_{B_k,\mathscr{M}_0}$ to an action of $\mathscr{H}(\overline{\ell^2 n})$ on $H^0(\mathscr{M}_0)$. Let $x, y \in B_k[\ell]$, and $x', y' \in B_k[\ell^2]$ be such that $\ell.x' = y$ and $\ell.y' = y$. We put $x' = x'_1 + x'_2$ and $y' = y'_1 + y'_2$ with $x'_i, y'_i \in K_i(\mathscr{M}_0)$, for $i = 1,2$. Let $\varkappa : G(\mathscr{M}_0) \to K(\mathscr{M}_0)$ be the natural projection and let $(\alpha_1,\alpha_2),(\beta_1,\beta_2) \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$ be such that $\varkappa(\Theta_{B_k,\mathscr{M}_0}(\alpha_i)) = x'_i$ and $\varkappa(\Theta_{B_k,\mathscr{M}_0}(\beta_i)) = y'_i$. This mean that we have $x' = (1,\alpha_1,\alpha_2).0_{A_k}$ and $y' = (1,\beta_1,\beta_2).0_{A_k}$.

Lemma 7.2:
Let $i \in Z(\ell^2 n)$ and put

$$s(1) = \frac{((1,\alpha_1,0).(1,\beta_1,0).\vartheta_i)(\widetilde{0}_{B_k})}{((1,\alpha_1,0).\vartheta_i)(\widetilde{0}_{B_k})} \cdot \frac{\vartheta_i(\widetilde{0}_{B_k})}{((1,\beta_1,0).\vartheta_i)(\widetilde{0}_{B_k})}.$$

For all $k \in \mathbb{N}$, we have

$$s(k) = \frac{((1,\alpha_1,0).(1,k.\beta_1,0).\vartheta_i)(\widetilde{0}_{B_k})}{((1,\alpha_1,0).\vartheta_i)(\widetilde{0}_{B_k})} \cdot \frac{\vartheta_i(\widetilde{0}_{B_k})}{((1,k.\beta_1,0).\vartheta_i)(\widetilde{0}_{B_k})} = s(1)^k. \tag{29}$$

Proof: Consider the degree-0 line bundle $\Lambda = \tau_{y'_1}^*\mathscr{M}_0 \otimes \mathscr{M}_0^{-1}$. We remark that as $y'_1 \in K(\mathscr{M}_0)$, Λ is isomorphic to the trivial line bundle on B_k. Let K be the subgroup of $K_1(\mathscr{M}_0)$ generated by x'_1 and let C_k be the quotient of B_k by K. The line bundle Λ descends to a line bundle Λ' over C_k. As Λ' has degree 0, it is the quotient of $B_k \times \mathbb{A}^1_k$ by an action of the form $g'_x(t,\alpha) = (t+x, \chi_0(x).\alpha)$, where $(t,\alpha) \in B_k \times \mathbb{A}^1_x$, $x \in K$, and χ_0 is a character of K.

As $\vartheta_i \in H^0(\mathscr{M}_0)$, we remark that $f = ((1,\beta_1,0).\vartheta_i)/(\vartheta_i)$ is a section of Λ. Thus, we have $s(k) = f(k.x'_1)/f(0_{B_k}) = \chi_0(k)$ and $s(k) = s(1)^k$. ■

Remark 7.3:
We remark that in the preceding lemma, α_1 and β_1 play the same role and as a consequence can be permuted. ♢

We keep the notation of the beginning of this paragraph to state the

Proposition 7.4:
We put:

$$L = \frac{((1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\vartheta_i)(\widetilde{0}_{B_k})}{((1,\beta_1,\beta_2)\vartheta_i)(\widetilde{0}_{B_k})}.\frac{\vartheta_i(\widetilde{0}_{B_k})}{((1,\ell.\alpha_1,\ell.\alpha_2)\vartheta_i)(\widetilde{0}_{B_k})}.$$

$$R = \frac{((1,\alpha_1+\ell.\beta_1,\alpha_2+\ell.\beta_2)\vartheta_i)(\widetilde{0}_{B_k})}{((1,\alpha_1,\alpha_2)\vartheta_i)(\widetilde{0}_{B_k})}.\frac{\vartheta_i(\widetilde{0}_{B_k})}{((1,\ell.\beta_1,\ell.\beta_2)\vartheta_i)(\widetilde{0}_{B_k})}.$$

We have :

$$e'_\ell(x,y) = L^{-1}.R. \tag{30}$$

Proof: In order to clarify the notations we denote by e_c the canonical pairing between $Z(\overline{\ell^2 n})$ and $\hat{Z}(\overline{\ell^2 n})$. First, we compute L. We have:

$$\begin{aligned}(1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\vartheta_i &= e_c(\ell.\alpha_1+\beta_1,-\ell.\alpha_2-\beta_2)(1,\ell.\alpha+\beta_1,0)(1,0,\ell.\alpha_2+\beta_2)\vartheta_i\\ &= e_c(\ell.\alpha_1+\beta_1,-\ell.\alpha_2-\beta_2)(1,\ell.\alpha_1+\beta_1,0)\vartheta_i.\end{aligned}$$

In the same way, we have:

$$\begin{aligned}(1,\beta_1,\beta_2)\vartheta_i &= e_c(\beta_1,-\beta_2)(1,\beta_1,0)\vartheta_i,\\ (1,\ell.\alpha_1,\ell.\alpha_2)\vartheta_i &= e_c(\ell.\alpha_1,-\ell.\alpha_2)(1,\ell.\alpha_1,0)\vartheta_i.\end{aligned}$$

Taking the product, we obtain that

$$L = e_c(\ell.\alpha_1,-\beta_2).L',$$

with

$$L' = \frac{((1,\beta_1,0).(1,\ell.\alpha_1,0)\vartheta_i)(\widetilde{0}_{B_k})}{(1,\beta_1,0)\vartheta_i(\widetilde{0}_{B_k})}\frac{\vartheta_i(\widetilde{0}_{B_k})}{(1,\ell.\alpha_1,0)\vartheta_i(\widetilde{0}_{B_k})}.$$

In the same manner, we have:

$$R = e_c(\ell.\beta_1,-\alpha_2).R',$$

with

$$R' = \frac{((1,\alpha_1,0).(1,\ell.\beta_1,0)\vartheta_i)(\widetilde{0}_{B_k})}{(1,\alpha_1,0)\vartheta_i(\widetilde{0}_{B_k})}\frac{\vartheta_i(\widetilde{0}_{B_k})}{(1,\ell.\beta_1,0)\vartheta_i(\widetilde{0}_{B_k})}.$$

Using lemma 7.2 and the fact that $(1,\alpha_1,0)$ commutes with $(1,\beta_1,0)$ we get that $L' = R'$. Therefore,

$$L^{-1}.R = e_c(\ell.\alpha_1,\beta_2).e_c(\ell.\alpha_2,\beta_1) = e'_\ell(x,y).$$ ■

The preceding proposition gives us an algorithm to compute the pairing:

Algorithm 7.5 (Pairing computation):
Input $P, Q \in B_k[\ell]$
Output $e'_\ell(P,Q)$

Let $P, Q \in B_k[\ell]$, and choose any affine lift $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$, we can compute the following via addition chains:

$$\begin{array}{cccc} \widetilde{0}_{B_k} & \widetilde{P} & 2\widetilde{P} & \dots & \ell\widetilde{P} = \lambda_P^0 \widetilde{0}_{B_k} \\ \widetilde{Q} & \widetilde{P+Q} & 2\widetilde{P}+\widetilde{Q} & \dots & \ell\widetilde{P}+\widetilde{Q} = \lambda_P^1 \widetilde{Q} \\ 2\widetilde{Q} & \widetilde{P}+2\widetilde{Q} & & & \\ \dots & \dots & & & \\ \ell\widetilde{Q} = \lambda_Q^0 \widetilde{0}_{B_k} & \widetilde{P}+\ell\widetilde{Q} = \lambda_Q^1 P & & & \end{array}$$

Namely we compute:

$$\ell\widetilde{P} := \texttt{chaine\_mult}(\ell, \widetilde{P}) \quad \ell\widetilde{Q} := \texttt{chaine\_mult}(\ell, \widetilde{Q})$$
$$\ell\widetilde{P}+\widetilde{Q} := \texttt{chaine\_multadd}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}) \quad \widetilde{P}+\ell\widetilde{Q} := \texttt{chaine\_multadd}(\ell, \widetilde{P+Q}, \widetilde{Q}, \widetilde{P}).$$

Then we have:

$$e'_\ell(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_Q^1 \lambda_P^0} \tag{31}$$
♢

Proof: Assume that $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$ are such that $\widetilde{P} = \widetilde{[\ell]}(1, \alpha_1, \beta_1)\widetilde{0}'_{B_k}$, $\widetilde{Q} = \widetilde{[\ell]}(1, \alpha_2, \beta_2)\widetilde{0}'_{B_k}$, and $\widetilde{P+Q} = \widetilde{[\ell]}(1, \alpha_1+\alpha_2, \beta_1+\beta_2)\widetilde{0}'_{B_k}$. Then by Corollary 4.16, we find that $\lambda_P^0 = \frac{\vartheta_i(0)}{((1,\ell.\alpha_1,\ell.\alpha_2)\vartheta_i)(0)} = 1$ and that $\lambda_P^1 = \frac{((1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\vartheta_i)(0)}{((1,\beta_1,\beta_2)\vartheta_i)(0)}$, so that by Proposition 7.4, we have:

$$e'_\ell(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_Q^1 \lambda_P^0}$$

Now by Lemma 4.8, it is easy to see that (31) is homogeneous and does not depend on the affine lifts $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$, which concludes the proof. ■

Complexity Analysis 7.6:
By using a Montgomery ladder, we see that we can compute $e'_\ell(P,Q)$ with four fast addition chains of length ℓ, hence we need $O(\log(\ell))$ additions. It should be noted that we can reuse a lot of computation between the addition chains $P, 2P, 4P, \dots$ and $P+Q, 2P+Q, 4P+Q, \dots$ since we always add the same point at the same time between the two chains. ♢

The case $n = 2$ Let $\pm P, \pm Q \in K_B$, then we have $e'_\ell(\pm P, \pm Q) = \{e'_\ell(P,Q), e'_\ell(P,Q)^{-1}\}$. Thus the pairing on the Kummer variety is a bilinear pairing $K_B \times K_B \to k^{*,\pm}$ where $k^{*,\pm} = k^*/\{x = 1/x\}$. We represent a class $\overline{x} \in k^{*,\pm}$ by $x + 1/x \in k$, and we define the symmetric pairing $e'_s(\pm P, \pm Q) = e'_\ell(P,Q) + e'_\ell(P,-Q)$. We can use the addition relations to compute $P \pm Q$ and then use Algorithm 7.5 to compute $e'_\ell(P,Q)$, $e'_\ell(P,-Q)$, but since e'_s is symmetric there should be a method to compute it without solving the degree-2 system given by the addition relations. This will be the object of a future article.

8 Conclusion

We have described an algorithm that give a modular point from an isotropic kernel, and another one that can compute the isogeny associated to a modular point. By combining these two algorithms, we can compute any isogeny between abelian varieties. However, the level of the modular space that we use depend on the degree of the isogeny. That means that a point in this modular space $\mathcal{M}_{\overline{\ell n}}$ corresponds to an isogeny and to the choice of a symplectic basis of $B_k[\ell]$. So in our case it is easier to compute directly the points of ℓ-torsion in B_k than to compute directly the modular points in $\mathcal{M}_{\overline{\ell n}}$ since the degree of this latter system is higher. These remarks mean that we cannot use our algorithm to speed up Schoof point counting algorithm, like in the genus-one case (see for instance [Elk98]). A solution would be to have an efficient characterization of $\mathcal{M}_{\overline{\ell n}}$ modulo the action by the symplectic group of order ℓ.

Still, we can go back to a modular point of level n by using the modular correspondence introduced in [FLR09]. This mean that we can compute isogeny graphs if we restrict to ℓ^2-isogenies. We have also introduced a point compression algorithm, that allows to drastically reduce the number of coordinates of a projective embedding of level 4ℓ. This new representation can be useful when one has to work with such a projective embedding, rather than the usual one of level 4 (for instance if one need a quick access to the translation by a point of ℓ-torsion).

We have also described a new way to compute the Weil pairing, that use addition chains rather than a Miller loop. We remark that our new algorithm apply to any abelian variety, so it extends the range of pairings accessible for cryptography.

References

[BGL09] Reinier Broker, David Gruenewald, and Kristin Lauter. Explicit cm-theory in dimension 2, October 2009.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BL09] Reinier Broker and Kristin Lauter. Modular polynomials for genus 2, February 2009.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[FLR09] Jean-Charles Faugère, David Lubicz, and Damien Robert. Computing modular correspondences for abelian varieties, October 2009.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007.

[GS08] P. Gaudry and E. Schost. Hyperelliptic curve point counting record: 254 bit jacobian, 06 2008. Available at `http://webloria.loria.fr/ gaudry/record127/`.

[Ler] R. Lercier. Algorithmique des courbes elliptiques dans les corps finis. These, LIX–CNRS, juin 1997.

[Mes01] Jean-François Mestre. Lettre à Gaudry et Harley, 2001. Available at `http://www.math.jussieu.fr/mestre`.

[Mes02] Jean-François Mestre. Notes of a talk given at the cryptography seminar Rennes, 2002. Available at `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`.

[Mil04] Victor S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum67a] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum67b] D. Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3:215–244, 1967.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum83] David Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum84] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Plo29] Ploum. *Plim*. Plom. Plam, 1729.

[Smi08] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. Smart, Nigel (ed.), Advances in cryptology – EUROCRYPT 2008. 27th annual international conference on the theory and applications of cryptographic techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 4965, 163-180 (2008)., 2008.

[Smi09] Benjamin Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves, February 2009.

[Wam99] P. Wamelen. Equations for the Jacobian of a hyperelliptic curve. *AMS*, 350(8):3083–3106, August 1999.