A Vélu's like formula for computing isogenies on Abelian Varieties

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

[1]CÉLAR

[2]IRMAR, Université de Rennes 1

[3]Nancy Université, CNRS, Inria Nancy Grand Est

Octobre 2010, Réunion CHIC

Vélu's formula

Théorème

Let $E : y^2 = f(x)$ *be an elliptic curve. Let* $G \subset E(k)$ *be a finite subgroup. Then* E/G *is given by* $Y^2 = g(X)$ *where*

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} x(P+Q) - x(Q)$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} y(P+Q) - y(Q)$$

- Uses the fact that x and y are characterised in $k(E)$ by

$$\begin{aligned} v_{0_E}(x) &= -3 \qquad v_P(x) \geq 0 \quad \text{if } P \neq 0_E \\ v_{0_E}(y) &= -2 \qquad v_P(y) \geq 0 \quad \text{if } P \neq 0_E \\ y^2/x^3(O_E) &= 1 \end{aligned}$$

- No such characterisation in genus $g \geq 2$.

Vélu's formula

Théorème

Let $E : y^2 = f(x)$ *be an elliptic curve. Let* $G \subset E(k)$ *be a finite subgroup. Then* E/G *is given by* $Y^2 = g(X)$ *where*

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} x(P+Q) - x(Q)$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} y(P+Q) - y(Q)$$

- Uses the fact that x and y are characterised in $k(E)$ by

$$\begin{aligned} v_{0_E}(x) &= -3 & v_P(x) &\geq 0 \quad \text{if } P \neq 0_E \\ v_{0_E}(y) &= -2 & v_P(y) &\geq 0 \quad \text{if } P \neq 0_E \\ y^2/x^3(O_E) &= 1 \end{aligned}$$

- No such characterisation in genus $g \geq 2$.

The modular polynomial

Définition

- The modular polynomial is a polynomial $\varphi_n(x, y) \in \mathbb{Z}[x, y]$ such that $\varphi_n(x, y) = 0$ iff $x = j(E)$ and $y = j(E')$ with E and E′ n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\varphi_n(j(E), .)$ $\Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes : $\varphi_2 = 50$ MB.

$\Rightarrow$ Use the moduli space given by theta functions.

$\Rightarrow$ Fix the form of the isogeny and look for coordinates compatible with the isogeny.

The modular polynomial

Définition

- The modular polynomial is a polynomial $\varphi_n(x, y) \in \mathbb{Z}[x, y]$ such that $\varphi_n(x, y) = 0$ iff $x = j(E)$ and $y = j(E')$ with E and E′ n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\varphi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes : $\varphi_2 = 50$ MB.

$\Rightarrow$ Use the moduli space given by theta functions.

$\Rightarrow$ Fix the form of the isogeny and look for coordinates compatible with the isogeny.

The modular polynomial

Définition

- The modular polynomial is a polynomial $\varphi_n(x,y) \in \mathbb{Z}[x,y]$ such that $\varphi_n(x,y) = 0$ iff $x = j(E)$ and $y = j(E')$ with E and E′ n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\varphi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes : $\varphi_2 = 50$ MB.

$\Rightarrow$ Use the moduli space given by theta functions.

$\Rightarrow$ Fix the form of the isogeny and look for coordinates compatible with the isogeny.

The modular polynomial

Définition

- The modular polynomial is a polynomial $\varphi_n(x, y) \in \mathbb{Z}[x, y]$ such that $\varphi_n(x, y) = 0$ iff $x = j(E)$ and $y = j(E')$ with E and E′ n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\varphi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes : $\varphi_2 = 50$ MB.

$\Rightarrow$ Use the moduli space given by theta functions.

$\Rightarrow$ Fix the form of the isogeny and look for coordinates compatible with the isogeny.

The modular polynomial

Définition

- The modular polynomial is a polynomial $\varphi_n(x, y) \in \mathbb{Z}[x, y]$ such that $\varphi_n(x, y) = 0$ iff $x = j(E)$ and $y = j(E')$ with E and E′ n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\varphi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes : $\varphi_2 = 50$ MB.

$\Rightarrow$ Use the moduli space given by theta functions.

$\Rightarrow$ Fix the form of the isogeny and look for coordinates compatible with the isogeny.

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on $\mathbb{C}^g$.

$$\vartheta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i n' \Omega n + 2\pi i n' z}$$

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = e^{\pi i a' \Omega a + 2\pi i a'(z+b)} \vartheta(z + \Omega a + b, \Omega) \; a, b \in \mathbb{Q}^g$$

- The quasi-periodicity is given by

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z + m + \Omega n, \Omega) = e^{2\pi i (a'm - b'n) - \pi i n' \Omega n - 2\pi i n' z} \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega)$$

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on $\mathbb{C}^g$.

$$\vartheta(z,\Omega) = \sum_{n\in\mathbb{Z}^g} e^{\pi i n'\Omega n + 2\pi i n' z}$$

$$\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z,\Omega) = e^{\pi i a'\Omega a + 2\pi i a'(z+b)}\vartheta(z+\Omega a + b, \Omega) \; a,b\in\mathbb{Q}^g$$

- The quasi-periodicity is given by

$$\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z+m+\Omega n,\Omega) = e^{2\pi i(a'm-b'n)-\pi i n'\Omega n - 2\pi i n' z}\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z,\Omega)$$

Projective embeddings given by theta functions

Théorème

- *Let* $\mathcal{L}_\ell$ *be the space of analytic functions* f *satisfying :*

$$f(z+n) = f(z)$$
$$f(z+n\Omega) = \exp(-\ell \cdot \pi i n'\Omega n - \ell \cdot 2\pi i n' z) f(z)$$

- *A basis of* $\mathcal{L}_\ell$ *is given by*

$$\left\{ \vartheta \begin{bmatrix} 0 \\ b \end{bmatrix} (z, \Omega/\ell) \right\}_{b \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g}$$

- *Let* $\mathcal{Z}_\ell = \mathbb{Z}^g/\ell\mathbb{Z}^g$. *If* $i \in \mathcal{Z}_\ell$ *we define* $\vartheta_i = \vartheta \begin{bmatrix} 0 \\ i/\ell \end{bmatrix} (., \Omega/\ell)$. *If* $l \geq 3$ *then*

$$z \mapsto (\vartheta_i(z))_{i \in \mathcal{Z}_\ell}$$

is a projective embedding $A \to \mathbb{P}_{\mathbb{C}}^{\ell^g - 1}$.

Projective embeddings given by theta functions

Théorème

- *Let* $\mathcal{L}_\ell$ *be the space of analytic functions* f *satisfying :*

$$f(z+n) = f(z)$$
$$f(z+n\Omega) = \exp(-\ell \cdot \pi i n'\Omega n - \ell \cdot 2\pi i n' z) f(z)$$

- *A basis of* $\mathcal{L}_\ell$ *is given by*

$$\left\{ \vartheta \begin{bmatrix} 0 \\ b \end{bmatrix} (z, \Omega/\ell) \right\}_{b \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g}$$

- *Let* $\mathcal{Z}_\ell = \mathbb{Z}^g/\ell\mathbb{Z}^g$. *If* $i \in \mathcal{Z}_\ell$ *we define* $\vartheta_i = \vartheta \begin{bmatrix} 0 \\ i/\ell \end{bmatrix} (., \Omega/\ell)$. *If* $l \geq 3$ *then*

$$z \mapsto (\vartheta_i(z))_{i \in \mathcal{Z}_\ell}$$

is a projective embedding $A \to \mathbb{P}_{\mathbb{C}}^{\ell^g - 1}$.

The action of the Theta group

- The point $(a_i)_{i\in\mathcal{Z}_\ell} := (\vartheta_i(0))_{i\in\mathcal{Z}_\ell}$ is called the theta null point of level ℓ of the Abelian Variety $A := \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- $(a_i)_{i\in\mathcal{Z}_\ell}$ determines the equations of the projective embedding of A of level ℓ.
- The symplectic basis $\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g$ induce a decomposition into isotropic subgroups for the commutator pairing :

$$\begin{aligned} A[\ell] &= A[\ell]_1 \oplus A[\ell]_2 \\ &= \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \oplus \frac{1}{\ell}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g \end{aligned}$$

  This decomposition can be recovered by $(a_i)_{i\in\mathcal{Z}_\ell}$.
- The action by translation is given by

$$\vartheta_k\left(z - \frac{i}{\ell} - \Omega\frac{j}{\ell}\right) = e_{\mathcal{L}_\ell}(i+k, j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}_\ell}(x,y) = e^{2\pi i/\ell \cdot x' y}$ is the commutator pairing.

The action of the Theta group

- The point $(a_i)_{i \in \mathcal{Z}_\ell} := (\vartheta_i(0))_{i \in \mathcal{Z}_\ell}$ is called the theta null point of level ℓ of the Abelian Variety $A := \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- $(a_i)_{i \in \mathcal{Z}_\ell}$ determines the equations of the projective embedding of A of level ℓ.
- The symplectic basis $\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g$ induce a decomposition into isotropic subgroups for the commutator pairing :

$$\begin{aligned} A[\ell] &= A[\ell]_1 \oplus A[\ell]_2 \\ &= \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \oplus \frac{1}{\ell}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g \end{aligned}$$

  This decomposition can be recovered by $(a_i)_{i \in \mathcal{Z}_\ell}$.
- The action by translation is given by

$$\vartheta_k\left(z - \frac{i}{\ell} - \Omega\frac{j}{\ell}\right) = e_{\mathcal{L}_\ell}(i+k, j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}_\ell}(x,y) = e^{2\pi i/\ell \cdot x' y}$ is the commutator pairing.

The action of the Theta group

- The point $(a_i)_{i\in\mathcal{Z}_\ell} := (\vartheta_i(0))_{i\in\mathcal{Z}_\ell}$ is called the theta null point of level ℓ of the Abelian Variety $A := \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- $(a_i)_{i\in\mathcal{Z}_\ell}$ determines the equations of the projective embedding of A of level ℓ.
- The symplectic basis $\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g$ induce a decomposition into isotropic subgroups for the commutator pairing :

$$\begin{aligned} A[\ell] &= A[\ell]_1 \oplus A[\ell]_2 \\ &= \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \oplus \frac{1}{\ell}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g \end{aligned}$$

  This decomposition can be recovered by $(a_i)_{i\in\mathcal{Z}_\ell}$.
- The action by translation is given by

$$\vartheta_k\left(z - \frac{i}{\ell} - \Omega\frac{j}{\ell}\right) = e_{\mathcal{L}_\ell}(i+k, j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}_\ell}(x,y) = e^{2\pi i/\ell \cdot x' y}$ is the commutator pairing.

The isogeny theorem

Théorème

- *Let* $\ell = n.m$, *and* $\varphi : \mathcal{Z}_n \to \mathcal{Z}_\ell, x \mapsto m.x$ *be the canonical embedding. Let* $K = A[m]_2 \subset A[\ell]_2$.
- *Let* $(\vartheta_i^A)_{i \in \mathcal{Z}_\ell}$ *be the theta functions of level* ℓ *on* $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- *Let* $(\vartheta_i^B)_{i \in \mathcal{Z}_n}$ *be the theta functions of level* n *of* $B = A/K = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{m}\mathbb{Z}^g)$.
- *We have :*

$$(\vartheta_i^B(x))_{i \in \mathcal{Z}_n} = (\vartheta_{\varphi(i)}^A(x))_{i \in \mathcal{Z}_n}$$

Démonstration.

$$\vartheta_i^B(z) = \vartheta\begin{bmatrix} 0 \\ i/n \end{bmatrix}\left(z, \frac{\Omega}{m}/n\right) = \vartheta\begin{bmatrix} 0 \\ mi/\ell \end{bmatrix}(z, \Omega/\ell) = \vartheta_{m \cdot i}^A(z)$$

□

The isogeny theorem

Théorème

- Let $\ell = n.m$, and $\varphi : \mathcal{Z}_n \to \mathcal{Z}_\ell, x \mapsto m.x$ be the canonical embedding.
  Let $K = A[m]_2 \subset A[\ell]_2$.
- Let $(\vartheta_i^A)_{i \in \mathcal{Z}_\ell}$ be the theta functions of level ℓ on $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- Let $(\vartheta_i^B)_{i \in \mathcal{Z}_n}$ be the theta functions of level n of $B = A/K = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{m}\mathbb{Z}^g)$.
- We have :

$$(\vartheta_i^B(x))_{i \in \mathcal{Z}_n} = (\vartheta_{\varphi(i)}^A(x))_{i \in \mathcal{Z}_n}$$

Démonstration.

$$\vartheta_i^B(z) = \vartheta \begin{bmatrix} 0 \\ i/n \end{bmatrix} \left(z, \frac{\Omega}{m}/n \right) = \vartheta \begin{bmatrix} 0 \\ mi/\ell \end{bmatrix} (z, \Omega/\ell) = \vartheta_{m \cdot i}^A(z)$$

□

The isogeny theorem

Théorème

- *Let* $\ell = n.m$, *and* $\varphi : \mathcal{Z}_n \to \mathcal{Z}_\ell, x \mapsto m.x$ *be the canonical embedding.* *Let* $\mathrm{K} = \mathrm{A}[m]_2 \subset \mathrm{A}[\ell]_2$.
- *Let* $(\vartheta_i^{\mathrm{A}})_{i \in \mathcal{Z}_\ell}$ *be the theta functions of level* ℓ *on* $\mathrm{A} = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- *Let* $(\vartheta_i^{\mathrm{B}})_{i \in \mathcal{Z}_n}$ *be the theta functions of level* n *of* $\mathrm{B} = \mathrm{A}/\mathrm{K} = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{m}\mathbb{Z}^g)$.
- *We have :*

$$(\vartheta_i^{\mathrm{B}}(x))_{i \in \mathcal{Z}_n} = (\vartheta_{\varphi(i)}^{\mathrm{A}}(x))_{i \in \mathcal{Z}_n}$$

Démonstration.

$$\vartheta_i^{\mathrm{B}}(z) = \vartheta\begin{bmatrix} 0 \\ i/n \end{bmatrix}\left(z, \frac{\Omega}{m}/n\right) = \vartheta\begin{bmatrix} 0 \\ mi/\ell \end{bmatrix}(z, \Omega/\ell) = \vartheta_{m \cdot i}^{\mathrm{A}}(z)$$

□

The isogeny theorem

Théorème

- *Let* $\ell = n.m$, *and* $\varphi : \mathcal{Z}_n \to \mathcal{Z}_\ell, x \mapsto m.x$ *be the canonical embedding.* *Let* $\mathrm{K} = \mathrm{A}[m]_2 \subset \mathrm{A}[\ell]_2$.
- *Let* $(\vartheta_i^{\mathrm{A}})_{i \in \mathcal{Z}_\ell}$ *be the theta functions of level* ℓ *on* $\mathrm{A} = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- *Let* $(\vartheta_i^{\mathrm{B}})_{i \in \mathcal{Z}_n}$ *be the theta functions of level* n *of* $\mathrm{B} = \mathrm{A}/\mathrm{K} = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{m}\mathbb{Z}^g)$.
- *We have :*

$$(\vartheta_i^{\mathrm{B}}(x))_{i \in \mathcal{Z}_n} = (\vartheta_{\varphi(i)}^{\mathrm{A}}(x))_{i \in \mathcal{Z}_n}$$

Démonstration.

$$\vartheta_i^{\mathrm{B}}(z) = \vartheta \begin{bmatrix} 0 \\ i/n \end{bmatrix} \left(z, \frac{\Omega}{m}/n \right) = \vartheta \begin{bmatrix} 0 \\ mi/\ell \end{bmatrix} (z, \Omega/\ell) = \vartheta_{m \cdot i}^{\mathrm{A}}(z)$$

$\square$

Mumford : On equations defining Abelian varieties

Théorème (car $k \nmid \ell$)

- *The theta null point of level ℓ $(a_i)_{i \in Z_\ell}$ satisfy the Riemann Relations :*

$$\sum_{t \in Z_2} a_{x+t} a_{y+t} \sum_{t \in Z_2} a_{u+t} a_{v+t} = \sum_{t \in Z_2} a_{z-u+t} a_{z-y+t} \sum_{t \in Z_2} a_{z-x+t} a_{z-v+t} \quad (1)$$

  We note $\mathcal{M}_\ell$ the moduli space given by these relations together with the relations of symmetry :

$$a_x = a_{-x}$$

- *$\mathcal{M}_\ell(k)$ is the modular space of k-Abelian variety with a theta structure of level ℓ. The locus of theta null points of level ℓ is an open subset $\mathcal{M}_\ell^0(k)$ of $\mathcal{M}_\ell(k)$.*

Remark

- *Analytic action :* $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts on $\mathcal{H}_g$ (and preserve the isomorphic classes).
- *Algebraic action :* $\mathrm{Sp}_{2g}(Z_\ell)$ acts on $\mathcal{M}_\ell$.

Mumford : On equations defining Abelian varieties

Théorème (car $k \nmid \ell$)

- *The theta null point of level* ℓ $(a_i)_{i \in \mathcal{Z}_\ell}$ *satisfy the Riemann Relations :*

$$\sum_{t \in \mathcal{Z}_2} a_{x+t} a_{y+t} \sum_{t \in \mathcal{Z}_2} a_{u+t} a_{v+t} = \sum_{t \in \mathcal{Z}_2} a_{z-u+t} a_{z-y+t} \sum_{t \in \mathcal{Z}_2} a_{z-x+t} a_{z-v+t} \qquad (1)$$

We note $\mathcal{M}_\ell$ *the moduli space given by these relations together with the relations of symmetry :*

$$a_x = a_{-x}$$

- $\mathcal{M}_\ell(k)$ *is the modular space of k-Abelian variety with a theta structure of level* ℓ*. The locus of theta null points of level* ℓ *is an open subset* $\mathcal{M}_\ell^0(k)$ *of* $\mathcal{M}_\ell(k)$*.*

Remark

- *Analytic action :* $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts on $\mathcal{H}_g$ (and preserve the isomorphic classes).
- *Algebraic action :* $\mathrm{Sp}_{2g}(\mathcal{Z}_\ell)$ acts on $\mathcal{M}_\ell$.

Mumford : On equations defining Abelian varieties

Théorème (car $k \nmid \ell$)

- *The theta null point of level ℓ $(a_i)_{i \in Z_\ell}$ satisfy the Riemann Relations :*

$$\sum_{t \in \mathcal{Z}_2} a_{x+t} a_{y+t} \sum_{t \in \mathcal{Z}_2} a_{u+t} a_{v+t} = \sum_{t \in \mathcal{Z}_2} a_{z-u+t} a_{z-y+t} \sum_{t \in \mathcal{Z}_2} a_{z-x+t} a_{z-v+t} \tag{1}$$

We note $\mathcal{M}_\ell$ the moduli space given by these relations together with the relations of symmetry :

$$a_x = a_{-x}$$

- *$\mathcal{M}_\ell(k)$ is the modular space of k-Abelian variety with a theta structure of level ℓ. The locus of theta null points of level ℓ is an open subset $\mathcal{M}_\ell^0(k)$ of $\mathcal{M}_\ell(k)$.*

Remark

- *Analytic action :* $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts on $\mathcal{H}_g$ (and preserve the isomorphic classes).
- *Algebraic action :* $\mathrm{Sp}_{2g}(\mathcal{Z}_\ell)$ acts on $\mathcal{M}_\ell$.

Summary

$$\begin{tikzcd} A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d] \\ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[ll, dotted] \end{tikzcd}$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$\begin{tikzcd}[column sep=huge, row sep=huge]
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[l, dotted, "\text{determines}"'] \arrow[d] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[l, dotted]
\end{tikzcd}$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$
\begin{tikzcd}
A_k,\ A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d] \\
B_k,\ B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[ll, dotted]
\end{tikzcd}
$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$
\begin{tikzcd}
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[l, dotted, "\text{determines}"'] \arrow[d] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[l, dotted]
\end{tikzcd}
$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$
\begin{tikzcd}
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[l, dotted, "\text{determines}"'] \arrow[d] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[l, dotted]
\end{tikzcd}
$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$\begin{tikzcd}
A_k,\, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d] \\
B_k,\, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[ll, dotted]
\end{tikzcd}$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

Summary

$$
\begin{tikzcd}
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \arrow[d, shift left, "\pi"] & (a_i)_{i \in \mathcal{Z}_\ell} \in \mathcal{M}_\ell(k) \arrow[l, dotted, "\text{determines}"'] \arrow[d] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\hat{\pi}"] & (b_i)_{i \in \mathcal{Z}_n} \in \mathcal{M}_n(k) \arrow[l, dotted]
\end{tikzcd}
$$

- The kernel of π is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
- Every isogeny comes from a modular solution.

The addition law

Théorème

$$\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big)=$$

$$\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

$$where \quad A=\frac{1}{2}\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}$$

$$\chi\in\hat{\mathcal{Z}}_2,\, i,j,k,l\in\mathcal{Z}_n$$

$$(i',j',k',l')=A(i,j,k,l)$$

Addition and isogenies

- Let $x \in A$. $x = (\vartheta_i(x))_{i \in \mathcal{Z}_{\ell n}}$. Let $\tilde{\pi}$ be the affine cone of π.

$$\tilde{\pi}(x) = (\vartheta_{\ell j}(x))_{j \in \mathcal{Z}_n}$$

- We have an isomorphism $\mathcal{Z}_n \times \mathcal{Z}_\ell \to \mathcal{Z}_{\ell n}, (j, i) \mapsto \ell j + n i$. If $i \in \mathcal{Z}_\ell$ we define :

$$\tilde{\pi}_i(x) = \tilde{\pi}((1, i, 0)\dot{x}) = (\vartheta_{\ell j + n i}(x))_{j \in \mathcal{Z}_n}$$

- We remark that x is entirely determined by $\{\tilde{\pi}_i(x)\}_{i \in \mathcal{Z}_\ell}$

Proposition

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

Addition and isogenies

- Let $x \in A$. $x = (\vartheta_i(x))_{i \in Z_{\ell n}}$. Let $\tilde{\pi}$ be the affine cone of π.

$$\tilde{\pi}(x) = (\vartheta_{\ell j}(x))_{j \in Z_n}$$

- We have an isomorphism $Z_n \times Z_\ell \to Z_{\ell n}, (j, i) \mapsto \ell j + ni$. If $i \in Z_\ell$ we define :

$$\tilde{\pi}_i(x) = \tilde{\pi}((1, i, 0)\,\dot{x}) = (\vartheta_{\ell j + ni}(x))_{j \in Z_n}$$

- We remark that x is entirely determined by $\{\tilde{\pi}_i(x)\}_{i \in Z_\ell}$

Proposition

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

Addition and isogenies

- Let $x \in A$. $x = (\vartheta_i(x))_{i \in Z_{\ell n}}$. Let $\tilde{\pi}$ be the affine cone of π.

$$\tilde{\pi}(x) = (\vartheta_{\ell j}(x))_{j \in Z_n}$$

- We have an isomorphism $Z_n \times Z_\ell \to Z_{\ell n}, (j,i) \mapsto \ell j + ni$. If $i \in Z_\ell$ we define :

$$\tilde{\pi}_i(x) = \tilde{\pi}((1,i,0)\dot{x}) = (\vartheta_{\ell j+ni}(x))_{j \in Z_n}$$

- We remark that x is entirely determined by $\{\tilde{\pi}_i(x)\}_{i \in Z_\ell}$

Proposition

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

Addition and isogenies

- Let $x \in A$. $x = (\vartheta_i(x))_{i \in Z_{\ell n}}$. Let $\tilde{\pi}$ be the affine cone of π.

$$\tilde{\pi}(x) = (\vartheta_{\ell j}(x))_{j \in Z_n}$$

- We have an isomorphism $Z_n \times Z_\ell \to Z_{\ell n}, (j, i) \mapsto \ell j + n i$. If $i \in Z_\ell$ we define :

$$\tilde{\pi}_i(x) = \tilde{\pi}((1, i, 0)\, \dot{x}) = (\vartheta_{\ell j + n i}(x))_{j \in Z_n}$$

- We remark that x is entirely determined by $\{\tilde{\pi}_i(x)\}_{i \in Z_\ell}$

Proposition

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

Point compression

- Let $e_1, \cdots, e_g$ be a basis of $\mathcal{Z}_\ell$. We note

$$R_i = \tilde{\pi}_i(0_A)$$

- We have

$$\tilde{\pi}_{i+j}(x) = \texttt{chaine\_add}(\tilde{\pi}_i(x), R_j, \tilde{\pi}_{i-j}(x))$$

Corollaire

- *x is entirely determined by*

$$\{\tilde{\pi}_i(x)\}_{i \in \{0, e_1, \cdots, e_g, e_1+e_2, \cdots, e_{g-1}+e_g\}}$$

- *Use $(1+g(g+1)/2)n^g$ coordinates rather than $(\ell n)^g$.*
- *The decompression use $O(\ell^g)$ chain additions.*
- *Can still do chain additions with this representation.*

Point compression

- Let $e_1, \cdots, e_g$ be a basis of $\mathcal{Z}_\ell$. We note

$$R_i = \tilde{\pi}_i(0_A)$$

- We have

$$\tilde{\pi}_{i+j}(x) = \texttt{chaine\_add}(\tilde{\pi}_i(x), R_j, \tilde{\pi}_{i-j}(x))$$

Corollaire

- *x is entirely determined by*

$$\{\tilde{\pi}_i(x)\}_{i \in \{0, e_1, \cdots, e_g, e_1+e_2, \cdots, e_{g-1}+e_g\}}$$

- *Use $(1+g(g+1)/2)n^g$ coordinates rather than $(\ell n)^g$.*
- *The decompression use $O(\ell^g)$ chain additions.*
- *Can still do chain additions with this representation.*

Point compression

- Let $e_1, \cdots, e_g$ be a basis of $\mathcal{Z}_\ell$. We note

$$\mathrm{R}_i = \tilde{\pi}_i(0_{\mathrm{A}})$$

- We have

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

Corollaire

- *x is entirely determined by*

$$\{\tilde{\pi}_i(x)\}_{i \in \{0, e_1, \cdots, e_g, e_1+e_2, \cdots, e_{g-1}+e_g\}}$$

- *Use $(1+g(g+1)/2)n^g$ coordinates rather than $(\ell n)^g$.*
- *The decompression use $\mathrm{O}(\ell^g)$ chain additions.*
- *Can still do chain additions with this representation.*

The dual isogeny

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\hat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell.x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell.x) = \texttt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \texttt{chaine\_mult}(\ell, y, y_i)$$

$$y = \texttt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \texttt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell.x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The dual isogeny

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\hat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in \mathcal{Z}_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell . x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell . x) = \mathtt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \mathtt{chaine\_mult}(\ell, y, y_i)$$

$$y = \mathtt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \mathtt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell . x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The dual isogeny

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\hat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in \mathcal{Z}_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell.x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell.x) = \texttt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \texttt{chaine\_mult}(\ell, y, y_i)$$

$$y = \texttt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^{\ell}\, \texttt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell.x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The dual isogeny

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\hat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in \mathcal{Z}_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell.x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell.x) = \texttt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^\ell \, \texttt{chaine\_mult}(\ell, y, y_i)$$

$$y = \texttt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^\ell \, \texttt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell.x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The dual isogeny

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\hat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in \mathcal{Z}_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell . x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell . x) = \texttt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^\ell \, \texttt{chaine\_mult}(\ell, y, y_i)$$
$$y = \texttt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^\ell \, \texttt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell . x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The dual isogeny

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\hat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in \mathcal{Z}_{\ell n}}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\hat{\pi}(y) = \ell.x$$

- Let $y \in B$. We can compute $y_i = y + R_i$ with a normal addition. We have $y_i = \lambda_i \tilde{\pi}_i(x)$.

$$\tilde{\pi}_i(\ell.x) = \mathtt{chaine\_mult}(\ell, y, \tilde{\pi}_i(x)) = \lambda_i^\ell \,\mathtt{chaine\_mult}(\ell, y, y_i)$$
$$y = \mathtt{chaine\_mult}(\ell, R_i, \tilde{\pi}_i(x)) = \lambda_i^\ell \,\mathtt{chaine\_mult}(\ell, R_i, y_i)$$

Corollaire

We can compute $\tilde{\pi}_i(\ell.x)$ with two fast multiplications of length ℓ. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $(1 + g(g+1))/2 \cdot O(\log(\ell))$ additions.

The action of the automorphisms of the Heisenberg group on the modular space

- Let $K \subset B[\ell]$ be an isotropic subgroup of maximal rank. Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a theta null point corresponding to the isogeny $\pi : B \to B/K$.
- The actions of the symplectic group compatible with the isogeny π are generated by

$$\{R_i\}_{i \in \mathcal{Z}_\ell} \mapsto \{R_{\psi_1(i)}\}_{i \in \mathcal{Z}_\ell} \tag{2}$$

$$\{R_i\}_{i \in \mathcal{Z}_\ell} \mapsto \{e(\psi_2(i), i) R_i\}_{i \in \mathcal{Z}_\ell} \tag{3}$$

where ψ_1 is an automorphism of $\mathcal{Z}_\ell$ and ψ_2 is a symmetric endomorphism of $\mathcal{Z}_\ell$.
- In particular by action ??, if $\{T_{e_i}\}_{i \in [1..g]}$ is a basis of K, we may suppose that $R_{e_i} = \lambda_{e_i} T_{e_i}$.

The action of the automorphisms of the Heisenberg group on the modular space

- Let $K \subset B[\ell]$ be an isotropic subgroup of maximal rank. Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a theta null point corresponding to the isogeny $\pi : B \to B/K$.
- The actions of the symplectic group compatible with the isogeny π are generated by

$$\{R_i\}_{i \in \mathcal{Z}_\ell} \mapsto \{R_{\psi_1(i)}\}_{i \in \mathcal{Z}_\ell} \tag{2}$$

$$\{R_i\}_{i \in \mathcal{Z}_\ell} \mapsto \{e(\psi_2(i), i) R_i\}_{i \in \mathcal{Z}_\ell} \tag{3}$$

  where ψ_1 is an automorphism of $\mathcal{Z}_\ell$ and ψ_2 is a symmetric endomorphism of $\mathcal{Z}_\ell$.
- In particular by action **??**, if $\{T_{e_i}\}_{i \in [1..g]}$ is a basis of K, we may suppose that $R_{e_i} = \lambda_{e_i} T_{e_i}$.

Recovering the projective factors

- Since we are working with symmetric Theta structures, we have $\vartheta_i(-x) = \vartheta_{-i}(x)$.
- In particular if $\ell = 2k+1$

$$\mathrm{R}_{(k+1)i} = \lambda_i^{(k+1)^2} \texttt{chaine\_mult}(k+1, \mathrm{T}_i) = -\mathrm{R}_{ki} = \lambda_i^{k^2} \texttt{chaine\_mult}(k, \mathrm{T}_i)$$

  (We say that R_i is a true point of ℓ-torsion). So we may recover λ_i up to a ℓ-root of unity.
- But we only need to recover R_i for $i \in \{e_1, \cdots, e_{g-1} + e_g\}$ and the action **??** shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollaire

We have Vélu's like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-root of unity and $g(g-1)/2$ additions. The compressed coordinates are sufficient to compute the compressed coordinates of the associated isogeny.

Recovering the projective factors

- Since we are working with symmetric Theta structures, we have $\vartheta_i(-x) = \vartheta_{-i}(x)$.
- In particular if $\ell = 2k + 1$

$$R_{(k+1)i} = \lambda_i^{(k+1)^2} \texttt{chaine\_mult}(k+1, T_i) = -R_{ki} = \lambda_i^{k^2} \texttt{chaine\_mult}(k, T_i)$$

(We say that R_i is a true point of ℓ-torsion). So we may recover λ_i up to a ℓ-root of unity.

- But we only need to recover R_i for $i \in \{e_1, \cdots, e_{g-1} + e_g\}$ and the action **??** shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollaire

We have Vélu's like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-root of unity and $g(g-1)/2$ additions. The compressed coordinates are sufficient to compute the compressed coordinates of the associated isogeny.

Recovering the projective factors

- Since we are working with symmetric Theta structures, we have $\vartheta_i(-x) = \vartheta_{-i}(x)$.
- In particular if $\ell = 2k+1$

$$R_{(k+1)i} = \lambda_i^{(k+1)^2}\, \mathtt{chaine\_mult}(k+1, T_i) = -R_{ki} = \lambda_i^{k^2}\, \mathtt{chaine\_mult}(k, T_i)$$

  (We say that R_i is a true point of ℓ-torsion). So we may recover λ_i up to a ℓ-root of unity.
- But we only need to recover R_i for $i \in \{e_1, \cdots, e_{g-1} + e_g\}$ and the action **??** shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollaire

We have Vélu's like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-root of unity and $g(g-1)/2$ additions. The compressed coordinates are sufficient to compute the compressed coordinates of the associated isogeny.

Computing all modular points

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be the theta null point associated to K. The theta structure of level $n\ell$ induces a decomposition $A[\ell] = A[\ell]_1 \oplus A[\ell]_2$ such that $B = A/A[\ell]_2$. Let $C = A/A[\ell]_1$, the isogeny theorem allows us to compute the modular point of level n associated to C.
- Each choice of the ℓ-roots of unity give a different theta structure on A, hence a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K comes from these choices. Moreover we know the kernel of the dual isogeny $C \to A$, this is helpfull for computing isogeny graphs.
- Let $T_{e_1}, \cdots, T_{e_{2g}}$ be a basis for $B[\ell]$. If x, y and $x - y$ are true points of ℓ-torsion, so is $x + y := \texttt{chaine\_add}(x, y, x - y)$. This means we can compute "true" representatives of $B[\ell]$ with $g(2g + 1)$ ℓ-root of unity, $g(2g - 1)$ additions and ℓ^{2g} chain additions.
- **Warning :** When applying our Vélu's formulas to an isotropic kernel, take care of the action of the commutator pairing.

Computing all modular points

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be the theta null point associated to K. The theta structure of level $n\ell$ induces a decomposition $A[\ell] = A[\ell]_1 \oplus A[\ell]_2$ such that $B = A/A[\ell]_2$. Let $C = A/A[\ell]_1$, the isogeny theorem allows us to compute the modular point of level n associated to C.
- Each choice of the ℓ-roots of unity give a different theta structure on A, hence a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K comes from these choices. Moreover we know the kernel of the dual isogeny $C \to A$, this is helpfull for computing isogeny graphs.
- Let $T_{e_1}, \cdots, T_{e_{2g}}$ be a basis for $B[\ell]$. If x,y and $x-y$ are true points of ℓ-torsion, so is $x+y := \texttt{chaine\_add}(x,y,x-y)$. This means we can compute "true" representatives of $B[\ell]$ with $g(2g+1)$ ℓ-root of unity, $g(2g-1)$ additions and ℓ^{2g} chain additions.
- **Warning :** When applying our Vélu's formulas to an isotropic kernel, take care of the action of the commutator pairing.

Computing all modular points

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be the theta null point associated to K. The theta structure of level $n\ell$ induces a decomposition $A[\ell] = A[\ell]_1 \oplus A[\ell]_2$ such that $B = A/A[\ell]_2$. Let $C = A/A[\ell]_1$, the isogeny theorem allows us to compute the modular point of level n associated to C.
- Each choice of the ℓ-roots of unity give a different theta structure on A, hence a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K comes from these choices. Moreover we know the kernel of the dual isogeny $C \to A$, this is helpfull for computing isogeny graphs.
- Let $T_{e_1}, \cdots, T_{e_{2g}}$ be a basis for $B[\ell]$. If x,y and $x - y$ are true points of ℓ-torsion, so is $x + y :=$ `chaine_add`$(x, y, x - y)$. This means we can compute "true" representatives of $B[\ell]$ with $g(2g + 1)$ ℓ-root of unity, $g(2g - 1)$ additions and ℓ^{2g} chain additions.
- **Warning :** When applying our Vélu's formulas to an isotropic kernel, take care of the action of the commutator pairing.

Computing all modular points

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be the theta null point associated to K. The theta structure of level $n\ell$ induces a decomposition $\mathrm{A}[\ell] = \mathrm{A}[\ell]_1 \oplus \mathrm{A}[\ell]_2$ such that $\mathrm{B} = \mathrm{A}/\mathrm{A}[\ell]_2$. Let $\mathrm{C} = \mathrm{A}/\mathrm{A}[\ell]_1$, the isogeny theorem allows us to compute the modular point of level n associated to C.
- Each choice of the ℓ-roots of unity give a different theta structure on A, hence a different decomposition $\mathrm{A}[\ell] = \mathrm{A}[\ell]_1 \oplus \mathrm{K}$. All the ℓ^2-isogenies $\mathrm{B} \to \mathrm{C}$ containing K comes from these choices. Moreover we know the kernel of the dual isogeny $\mathrm{C} \to \mathrm{A}$, this is helpfull for computing isogeny graphs.
- Let $\mathrm{T}_{e_1}, \cdots, \mathrm{T}_{e_{2g}}$ be a basis for $\mathrm{B}[\ell]$. If x,y and $x-y$ are true points of ℓ-torsion, so is $x+y := \mathtt{chaine\_add}(x, y, x-y)$. This means we can compute "true" representatives of $\mathrm{B}[\ell]$ with $g(2g+1)$ ℓ-root of unity, $g(2g-1)$ additions and ℓ^{2g} chain additions.
- **Warning :** When applying our Vélu's formulas to an isotropic kernel, take care of the action of the commutator pairing.