

Algorithms for modular correspondences between abelian varieties with level structure

Antoine Dequay¹, David Lubicz^{1,2}

SQLparty 2025

¹Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes

²DGA Maîtrise de l'information, BP 7419, F-35174 Bruz

Context

Definition

An abelian variety is a complete connected group variety over a base field k .

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + algebraic group law.
- An abelian variety is projective, smooth, irreducible and its group law is abelian.

Definition

An abelian variety is a complete connected group variety over a base field k .

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + algebraic group law.
- An abelian variety is projective, smooth, irreducible and its group law is abelian.

Examples

- Elliptic curves = Abelian varieties of dimension 1,
- Jacobians of genus g (smooth) curves are abelian varieties of dimension g ,
- The inclusion is strict for $g \geq 4$.

Definition

An isogeny is a finite surjective morphisme between abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies \iff Finite subgroups :

$$(f : A \rightarrow B) \mapsto \text{Ker} f$$

$$(A \rightarrow A/H) \leftarrow H$$

Definition

An isogeny is a finite surjective morphism between abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies \iff Finite subgroups :

$$(f : A \rightarrow B) \mapsto \text{Ker } f$$

$$(A \rightarrow A/H) \leftarrow H$$

Example

Multiplication by ℓ ($\mapsto A[\ell]$, the ℓ -torsion of A).

Complex abelian varieties

Property

A complex abelian variety is of the form $\mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, with $\Omega \in \mathcal{H}_g$, the Siegel upper-half space.

Complex abelian varieties

Property

A complex abelian variety is of the form $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, with $\Omega \in \mathcal{H}_g$, the Siegel upper-half space.

A projective embedding of $A = \mathbb{C}^g/\Lambda$ can be given by quasi-periodic functions with respect to Λ .

Definition

The space \mathcal{L}_m of Λ -quasi-periodic function of level m is the space of analytic function satisfying, for $z \in \mathbb{C}^g$ and $\lambda \in \mathbb{Z}^g$:

$$f(z + \lambda) = f(z) \quad f(z + \Omega\lambda) = \exp(-m \cdot \pi i {}^t \lambda \Omega \lambda - m \cdot 2\pi i {}^t z \lambda) f(z).$$

Theta functions

Definition

A theta function with rational characteristics $a, b \in \mathbb{Q}^g$ is given by :

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left(i\pi^t (n + a) \Omega (n + a) + 2i\pi^t (n + a)(z + b) \right) .$$

Theta functions

Definition

A theta function with rational characteristics $a, b \in \mathbb{Q}^g$ is given by :

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left(\imath \pi^t (n + a) \Omega (n + a) + 2 \imath \pi^t (n + a) (z + b) \right) .$$

For $m \geq 2$, let $Z(m) = \mathbb{Z}^g / m\mathbb{Z}^g$. A basis of \mathcal{L}_m is given by :

$$\left\{ \theta_i := \theta \begin{bmatrix} \mathbf{o} \\ i/m \end{bmatrix} (\cdot, \Omega/m) \right\}_{i \in Z(m)} .$$

Theta functions

Definition

A theta function with rational characteristics $a, b \in \mathbb{Q}^g$ is given by :

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left(i\pi^t (n + a) \Omega (n + a) + 2i\pi^t (n + a)(z + b) \right).$$

For $m \geq 2$, let $Z(m) = \mathbb{Z}^g / m\mathbb{Z}^g$. A basis of \mathcal{L}_m is given by :

$$\left\{ \theta_i := \theta \begin{bmatrix} 0 \\ i/m \end{bmatrix} (\cdot, \Omega/m) \right\}_{i \in Z(m)}.$$

If $m \geq 3$, it gives us an embedding :

$$\varphi_{m, \Omega} : \begin{pmatrix} A & \longrightarrow & \mathbb{P}^{Z(m)} \\ z & \longmapsto & (\theta_i(z))_{i \in Z(m)} \end{pmatrix}.$$

Theta functions

Definition

A theta function with rational characteristics $a, b \in \mathbb{Q}^g$ is given by :

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left(i\pi^t (n + a) \Omega (n + a) + 2i\pi^t (n + a)(z + b) \right).$$

For $m \geq 2$, let $Z(m) = \mathbb{Z}^g / m\mathbb{Z}^g$. A basis of \mathcal{L}_m is given by :

$$\left\{ \theta_i := \theta \begin{bmatrix} 0 \\ i/m \end{bmatrix} (\cdot, \Omega/m) \right\}_{i \in Z(m)}.$$

If $m \geq 3$, it gives us an embedding :

$$\varphi_{m,\Omega} : \begin{pmatrix} A & \longrightarrow & \mathbb{P}^{Z(m)} \\ z & \longmapsto & (\theta_i(z))_{i \in Z(m)} \end{pmatrix}.$$

The point $\varphi_{m,\Omega}(0_A)$ is called the theta null point of $\varphi_{m,\Omega}$.

Theorem (Mumford)

The level m theta null point $(a_i)_{i \in Z(m)}$ satisfy the Riemann equations of level m :

$$L(x, y)L(u, v) = L(x + z, y - z)L(u - z, v - z),$$

with $L(x, y)$ of the form $\sum_{t \in Z(2)} \chi(t) a_{x+t} a_{y+t}$.

Theorem (Mumford)

The level m theta null point $(a_i)_{i \in Z(m)}$ satisfy the Riemann equations of level m :

$$L(x, y)L(u, v) = L(x + z, y - z)L(u - z, v - z),$$

with $L(x, y)$ of the form $\sum_{t \in Z(2)} \chi(t) a_{x+t} a_{y+t}$, and the symmetry relations of level m :

$$a_x = a_{-x}.$$

Theorem (Mumford)

The level m theta null point $(a_i)_{i \in Z(m)}$ satisfy the Riemann equations of level m :

$$L(x, y)L(u, v) = L(x + z, y - z)L(u - z, v - z),$$

with $L(x, y)$ of the form $\sum_{t \in Z(2)} \chi(t) a_{x+t} a_{y+t}$, and the symmetry relations of level m :

$$a_x = a_{-x}.$$

This system is complete !

Relations

Theorem (Mumford)

The level m theta null point $(a_i)_{i \in Z(m)}$ satisfy the Riemann equations of level m :

$$L(x, y)L(u, v) = L(x + z, y - z)L(u - z, v - z),$$

with $L(x, y)$ of the form $\sum_{t \in Z(2)} \chi(t) a_{x+t} a_{y+t}$, and the symmetry relations of level m :

$$a_x = a_{-x}.$$

This system is complete !

Definition

There is an action by translation of $Z(m) \times Z(m)$ on the theta basis :

$$(i, j) \cdot \theta_k = \theta_k(\cdot - i/m - \Omega j/m) = e_{\mathcal{L}_m}(i + k, j) \theta_{i+k},$$

where $e_{\mathcal{L}_m}$ is the commutator paring.

The isogeny theorem

Theorem

- Let $\psi : Z(m) \rightarrow Z(dm)$ be the canonical embedding. Let $K = (\{0\} \times Z(m)) \cdot 0_A \subset A[m] \subset A[dm]$,

The isogeny theorem

Theorem

- Let $\psi : Z(m) \rightarrow Z(dm)$ be the canonical embedding. Let $K = (\{0\} \times Z(m)) \cdot 0_A \subset A[m] \subset A[dm]$,
- Let $(\theta_i^A)_{i \in Z(md)}$ be the theta functions of level md on $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$,

The isogeny theorem

Theorem

- Let $\psi : Z(m) \rightarrow Z(dm)$ be the canonical embedding. Let $K = (\{0\} \times Z(m)) \cdot 0_A \subset A[m] \subset A[dm]$,
- Let $(\theta_i^A)_{i \in Z(md)}$ be the theta functions of level md on $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$,
- Let $(\theta_i^B)_{i \in Z(m)}$ be the theta functions of level m on $B = A/K = \mathbb{C}^g / (\mathbb{Z}^g + (\Omega/m) \mathbb{Z}^g)$,

The isogeny theorem

Theorem

- Let $\psi : Z(m) \rightarrow Z(dm)$ be the canonical embedding. Let $K = (\{0\} \times Z(m)) \cdot 0_A \subset A[m] \subset A[dm]$,
- Let $(\theta_i^A)_{i \in Z(md)}$ be the theta functions of level md on $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$,
- Let $(\theta_i^B)_{i \in Z(m)}$ be the theta functions of level m on $B = A/K = \mathbb{C}^g / (\mathbb{Z}^g + (\Omega/m) \mathbb{Z}^g)$,
- We have :

$$(\theta_i^B)_{i \in Z(m)} = (\theta_{\psi(i)}^A)_{i \in Z(m)}.$$

The isogeny theorem

Theorem

- Let $\psi : Z(m) \rightarrow Z(dm)$ be the canonical embedding. Let $K = (\{0\} \times Z(m)) \cdot 0_A \subset A[m] \subset A[dm]$,
- Let $(\theta_i^A)_{i \in Z(md)}$ be the theta functions of level md on $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$,
- Let $(\theta_i^B)_{i \in Z(m)}$ be the theta functions of level m on $B = A/K = \mathbb{C}^g / (\mathbb{Z}^g + (\Omega/m) \mathbb{Z}^g)$,
- We have :

$$(\theta_i^B)_{i \in Z(m)} = (\theta_{\psi(i)}^A)_{i \in Z(m)}.$$

Proof.

$$\theta \begin{bmatrix} \circ \\ i/m \end{bmatrix} (\cdot, (\Omega/m)/d) = \theta \begin{bmatrix} \circ \\ di/dm \end{bmatrix} (\cdot, \Omega/dm).$$



Goal

Change of level algorithms and isogeny computation

Definition : Changing level

A change of level algorithm takes the theta null point of level m of A , and $K = A[dm]$, and computes the theta null point of level dm of A (going up) or the other way around (going down).

Change of level algorithms and isogeny computation

Definition : Changing level

A change of level algorithm takes the theta null point of level m of A , and $K = A[dm]$, and computes the theta null point of level dm of A (going up) or the other way around (going down).

Definition : Computing isogeny

An isogeny computation algorithm takes the theta null point of a A of level m , and $K \subset A[dm]$ a subgroup isomorphic to $Z(d)$, and computes the theta null point of an abelian variety B of level m , where $B = A/K$, and the isogeny $f : A \rightarrow B$.

Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :

$$(a_i)_{i \in Z(m)}$$

Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :

$$\begin{array}{c} (X_i)_{i \in Z(md)} \\ \uparrow \\ (a_i)_{i \in Z(m)} \end{array}$$

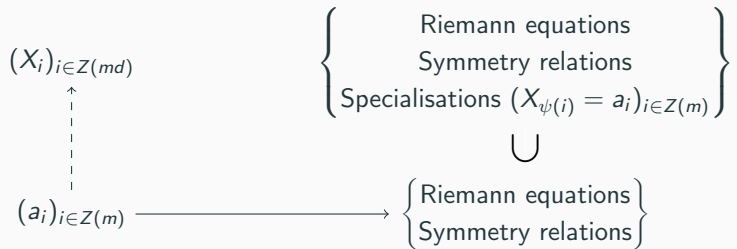
Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :



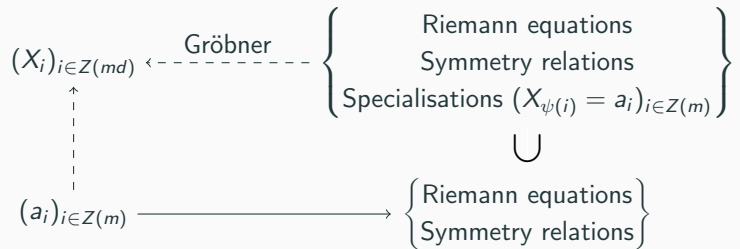
Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :



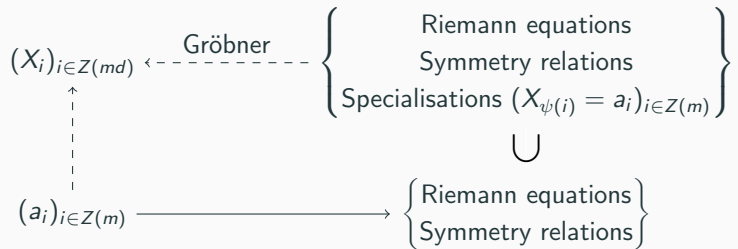
Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :



Just solve a polynomial system !

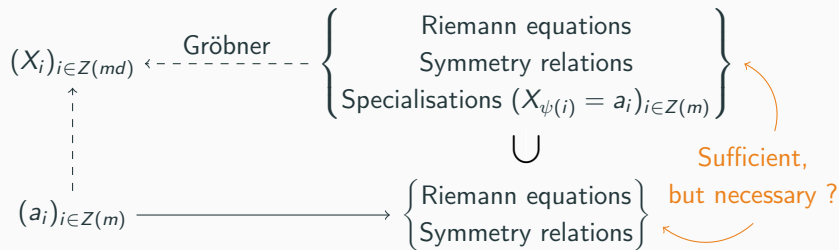
Basic idea : to find a theta null point of level md from a theta null point of level m :



Can we do better ?

Just solve a polynomial system !

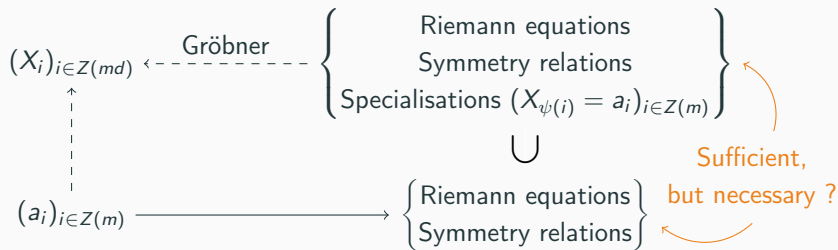
Basic idea : to find a theta null point of level md from a theta null point of level m :



Can we do better ?

Just solve a polynomial system !

Basic idea : to find a theta null point of level md from a theta null point of level m :



Can we do better ?

Previous results :

- Duplication formula : going up from level m to level $2m$;
- Koizumi formula : going down from level dm to level m ;
- [LR22] : change of level alg. & isogeny comp. for $2 \nmid d$ or $d \wedge m = 1$.

Results

Compatibility and first difference

Definition

Two theta null points of level m_1 and m_2 , say $\varphi_{m_1, \Omega_1}(0)$ and $\varphi_{m_2, \Omega_2}(0)$, are said to be compatible if there exists d such that $m_1 = dm_2$, and if there exists $\Omega \in \mathcal{H}_g$ such that $\Omega/m_i \simeq \Omega_i \pmod{\Gamma(m_i, 2m_i)}$ for $i = 1, 2$, where $\Gamma(m, 2m)$ is a congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ (Igusa level m subgroups).

Compatibility and first difference

Definition

Two theta null points of level m_1 and m_2 , say $\varphi_{m_1, \Omega_1}(0)$ and $\varphi_{m_2, \Omega_2}(0)$, are said to be compatible if there exists d such that $m_1 = dm_2$, and if there exists $\Omega \in \mathcal{H}_g$ such that $\Omega/m_i \simeq \Omega_i \pmod{\Gamma(m_i, 2m_i)}$ for $i = 1, 2$, where $\Gamma(m, 2m)$ is a congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ (Igusa level m subgroups).

From A an abelian variety of level m , and $\varphi_{m, \Omega}(0_A)$ its theta null point :

Case 2 $\nmid d$ or $d \wedge m = 1$

Any abelian variety of the form A/K , where $K \subset A[dm]$ is isomorphic to $Z(d)$, can be equipped with a theta null point compatible with $\varphi_{m, \Omega}(0_A)$.

Compatibility and first difference

Definition

Two theta null points of level m_1 and m_2 , say $\varphi_{m_1, \Omega_1}(0)$ and $\varphi_{m_2, \Omega_2}(0)$, are said to be compatible if there exists d such that $m_1 = dm_2$, and if there exists $\Omega \in \mathcal{H}_g$ such that $\Omega/m_i \simeq \Omega_i \pmod{\Gamma(m_i, 2m_i)}$ for $i = 1, 2$, where $\Gamma(m, 2m)$ is a congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ (Igusa level m subgroups).

From A an abelian variety of level m , and $\varphi_{m, \Omega}(0_A)$ its theta null point :

Case $2 \nmid d$ or $d \wedge m = 1$

Any abelian variety of the form A/K , where $K \subset A[dm]$ is isomorphic to $Z(d)$, can be equipped with a theta null point compatible with $\varphi_{m, \Omega}(0_A)$.

Case $2|d|m$

There is a unique $K_0 \subset A[dm]$, isomorphic to $Z(d)$, such that A/K_0 can be equipped with a theta null point compatible with $\varphi_{m, \Omega}(0_A)$:

$$K_0 = \left(\frac{m}{d} Z(d) \times \{0\} \right) \cdot 0_A.$$

What method for our algorithms?

Case 2 $\nmid d$ or $d \wedge m = 1$: Excellent lift

- Compute an affine lift of K (and other groups), consistent with relations on A ;
- Use formulas for theta null point/image by the isogeny.

What method for our algorithms?

Case 2 $\nmid d$ or $d \wedge m = 1$: Excellent lift

- Compute an affine lift of K (and other groups), consistent with relations on A ;
- Use formulas for theta null point/image by the isogeny.

Tools :

- Differential addition : $\widetilde{x + y} = \text{DiffAdd}(\tilde{x}, \tilde{y}, \widetilde{x - y})$;
- Action of $Z(m) \times Z(m)$;
- Inv : $\tilde{x} = (\tilde{x}_i)_{i \in Z(m)} \mapsto \widetilde{-x} = (\tilde{x}_{-i})_{i \in Z(m)}$.

What method for our algorithms?

Case 2 $\nmid d$ or $d \wedge m = 1$: Excellent lift

- Compute an affine lift of K (and other groups), consistent with relations on A ;
- Use formulas for theta null point/image by the isogeny.

Tools :

- Differential addition : $\widetilde{x + y} = \text{DiffAdd}(\tilde{x}, \tilde{y}, \widetilde{x - y})$;
- Action of $Z(m) \times Z(m)$;
- $\text{Inv} : \tilde{x} = (\tilde{x}_i)_{i \in Z(m)} \mapsto \widetilde{-x} = (\tilde{x}_{-i})_{i \in Z(m)}$.

Definition

Let (e_1, \dots, e_g) be a basis of $Z(md)/Z(m)$. We say that $(e_i, e_i + e_j)_{i,j=1,\dots,g}$ is a chain basis of $Z(d)$.

Example

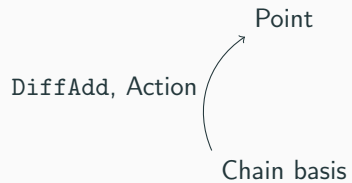
For $g = 2$, a chain basis of $Z(d)$ is $((1, 0), (0, 1), (1, 1))$.

Chain basis

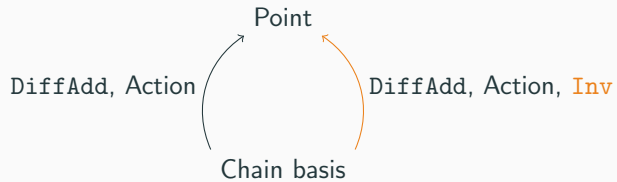
Point

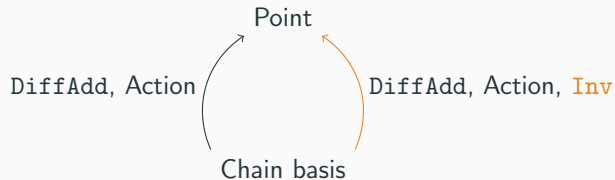
Chain basis

Relations



Relations





Definition

We set :

$$S_{\text{Inv}} = \{t \in Z(dm), t = -t \bmod Z(m)\}.$$

Definition

We set :

$$S_{\text{Inv}} = \{t \in Z(dm), t = -t \bmod Z(m)\}.$$

Case 2 $2 \nmid d$ or $d \wedge m = 1$

If $2 \nmid d$ or $d \wedge m = 1$, then $S_{\text{Inv}} = \{0\}$.

In other words, Inv acts freely on the set of points we can compute thanks to DiffAdd and the action of $Z(m) \times Z(m)$.

Definition

We set :

$$S_{\text{Inv}} = \{t \in Z(dm), t = -t \bmod Z(m)\}.$$

Case $2 \nmid d$ or $d \wedge m = 1$

If $2 \nmid d$ or $d \wedge m = 1$, then $S_{\text{Inv}} = \{0\}$.

In other words, Inv acts freely on the set of points we can compute thanks to DiffAdd and the action of $Z(m) \times Z(m)$.

Case $2 \mid d \mid m$: new relations

Let $\phi : Z(dm) \rightarrow A[dm]$ be a numbering of $A[dm]$. For $t \in S_{\text{Inv}}$, we have :

$$\phi(t) = (2dt, 0) \cdot \text{Inv}(\phi(t)),$$

where $dt \in Z(m)$.

Remedying the obstruction : symmetric compatibility

Proposition

If there exists $t \in S_{inv}$ such that $\phi(t) \neq (2dt, 0) \cdot \text{Inv}(\phi(t))$, then $-\phi(t) = (2dt, 0) \cdot \text{Inv}(\phi(t))$. This property is $Z(m)$ -linear in t !

Remedying the obstruction : symmetric compatibility

Proposition

If there exists $t \in S_{inv}$ such that $\phi(t) \neq (2dt, 0) \cdot \text{Inv}(\phi(t))$, then $-\phi(t) = (2dt, 0) \cdot \text{Inv}(\phi(t))$. This property is $Z(m)$ -linear in t !

Proposition : Changing the theta null point to make it sym. compatible

For $(e_i)_{i=1,\dots,g}$ a basis of $Z(md)$, if $\phi(e_i) \neq (2de_i, 0) \cdot \text{Inv}(\phi(e_i))$, then by replacing θ_k by $-\theta_k$ for $k \in \langle e_i \rangle$, we get the equality.

Example

For $g = 1$, $m = d = 2$ and a theta null point $(a_0 : a_1 : a_2 : a_3)$, either $(a_0 : a_1 : a_2 : a_3)$ or $(a_0 : -a_1 : a_2 : -a_3)$ is symmetric compatible with K .

Remedying the obstruction : symmetric compatibility

Proposition

If there exists $t \in S_{inv}$ such that $\phi(t) \neq (2dt, 0) \cdot \text{Inv}(\phi(t))$, then $-\phi(t) = (2dt, 0) \cdot \text{Inv}(\phi(t))$. This property is $Z(m)$ -linear in t !

Proposition : Changing the theta null point to make it sym. compatible

For $(e_i)_{i=1,\dots,g}$ a basis of $Z(md)$, if $\phi(e_i) \neq (2de_i, 0) \cdot \text{Inv}(\phi(e_i))$, then by replacing θ_k by $-\theta_k$ for $k \in \langle e_i \rangle$, we get the equality.

Example

For $g = 1$, $m = d = 2$ and a theta null point $(a_0 : a_1 : a_2 : a_3)$, either $(a_0 : a_1 : a_2 : a_3)$ or $(a_0 : -a_1 : a_2 : -a_3)$ is symmetric compatible with K .

Proposition : Changing K to make it symmetric compatible

For $(e_i)_{i=1,\dots,g}$ a basis of $Z(md)$, if $\phi(e_i) \neq (2de_i, 0) \cdot \text{Inv}(\phi(e_i))$, then :
 $\phi(e_i) + (0, \frac{md}{2}e_i) \cdot \phi(0) = (2de_i, 0) \cdot \text{Inv}(\phi(e_i))$.

Theorem : Changing level (going up)

- *Input* : A basis of $K = A[dm]$ and $\varphi_{m,\Omega}(0_A)$ the theta null point of level m of A ;
- We make K symmetric compatible with $\varphi_{m,\Omega}(0_A)$ (equivalent to a change of numbering or basis);
- We compute an affine lift of K (and other groups), consistent with relations on A ;
- We use formulas for the theta null point of level dm of A .

Theorem : Changing level (going up)

- *Input* : A basis of $K = A[dm]$ and $\varphi_{m,\Omega}(0_A)$ the theta null point of level m of A ;
- We make K symmetric compatible with $\varphi_{m,\Omega}(0_A)$ (equivalent to a change of numbering or basis);
- We compute an affine lift of K (and other groups), consistent with relations on A ;
- We use formulas for the theta null point of level dm of A .

Theorem : Computing isogeny

- *Input* : A basis of $K \subset A[dm]$ a subgroup isomorphic to $Z(d)$ and $\varphi_{m,\Omega}(0_A)$ the theta null point of level m of A ;
- We make $\varphi_{m,\Omega}(0_A)$ symmetric compatible with it K ;
- We compute an affine lift of K (and other groups), consistent with relations on A ;
- We use formulas for the image by the isogeny $A \rightarrow A/K$.

Theorem : Changing level (going up)

- We make K symmetric compatible with $\varphi_{m,\Omega}(0_A)$ (equivalent to a change of numbering or basis);
- We compute an affine lift of K (and other groups), consistent with relations on A ;
- We use formulas for the theta null point of level dm of A .

Theorem : Computing isogeny

- We make $\varphi_{m,\Omega}(0_A)$ symmetric compatible with it K ;
- We compute an affine lift of K (and other groups), consistent with relations on A ;
- We use formulas for the image by the isogeny $A \rightarrow A/K$.

Thank you for your attention !