A Vélu-like formula for computing isogenies on Abelian Varieties

Algorithmique et Arithmétique, avec applications à la cryptographie

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

[1]Caramel team, Nancy Université, CNRS, Inria Nancy Grand Est

[2]CÉLAR

[3]IRMAR, Université de Rennes 1

18-05-2010, Moscow

Outline

Outline

1. Abelian varieties and isogenies
2. Theta functions
3. Computing isogenies

Outline

Outline

Abelian varieties

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) + an algebraic group law.
- Abelian varieties are projective, smooth, irreducible with an Abelian group law.
- *Example:* Elliptic curves, Jacobians of genus g curves...

Abelian varieties

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) + an algebraic group law.
- Abelian varieties are projective, smooth, irreducible with an Abelian group law.
- *Example:* Elliptic curves, Jacobians of genus g curves...

Abelian varieties

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) + an algebraic group law.
- Abelian varieties are projective, smooth, irreducible with an Abelian group law.
- *Example:* Elliptic curves, Jacobians of genus g curves...

Abelian varieties

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) + an algebraic group law.
- Abelian varieties are projective, smooth, irreducible with an Abelian group law.
- *Example:* Elliptic curves, Jacobians of genus g curves...

Usage of Abelian varieties in cryptography

- Public key cryptography with the Discrete Logarithm Problem.

$\Rightarrow$ Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

- Pairing based cryptography.

$\Rightarrow$ Abelian varieties of dimension $g \leqslant 4$.

Usage of Abelian varieties in cryptography

- Public key cryptography with the Discrete Logarithm Problem.

⇒ Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

- Pairing based cryptography.

⇒ Abelian varieties of dimension $g \leqslant 4$.

Usage of Abelian varieties in cryptography

- Public key cryptography with the Discrete Logarithm Problem.

$\Rightarrow$ Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

- Pairing based cryptography.

$\Rightarrow$ Abelian varieties of dimension $g \leqslant 4$.

Usage of Abelian varieties in cryptography

- Public key cryptography with the Discrete Logarithm Problem.

$\Rightarrow$ Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

- Pairing based cryptography.

$\Rightarrow$ Abelian varieties of dimension $g \leqslant 4$.

Working with Jacobian of hyperelliptic curves

Let $C : y^2 = f(x)$ be a smooth irreducible hyperelliptic curve of genus g, with a rational point at infinity ($\deg f = 2g - 1$).

- Every divisor D on C has a unique representative ($k \leqslant g$)

$$D = \sum_{i=1}^{k} P_i - P_\infty .$$

- Mumford coordinates: $D = (u, v)$ where $u = \prod(x - x_i)$ and $v(x_i) = y_i$ ($\deg v < \deg u$).
- Cantor algorithm: Given a divisor D compute the Mumford representation $D = (u, v) \Rightarrow$ addition law.

Remark

- *For elliptic curves: more efficient coordinates (Edwards...).*
- *Pairing computation: use Miller algorithm.*

Working with Jacobian of hyperelliptic curves

Let $C : y^2 = f(x)$ be a smooth irreducible hyperelliptic curve of genus g, with a rational point at infinity ($\deg f = 2g - 1$).

- Every divisor D on C has a unique representative ($k \leqslant g$)

$$D = \sum_{i=1}^{k} P_i - P_\infty .$$

- Mumford coordinates: $D = (u, v)$ where $u = \prod(x - x_i)$ and $v(x_i) = y_i$ ($\deg v < \deg u$).
- Cantor algorithm: Given a divisor D compute the Mumford representation $D = (u, v) \Rightarrow$ addition law.

Remark

- *For elliptic curves: more efficient coordinates (Edwards...).*
- *Pairing computation: use Miller algorithm.*

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- *Example:* Multiplication by ℓ ($\Rightarrow$ ℓ-torsion), Frobenius (non separable).

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- *Example:* Multiplication by ℓ ($\Rightarrow$ ℓ-torsion), Frobenius (non separable).

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies ⇔ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- *Example:* Multiplication by ℓ ($\Rightarrow \ell$-torsion), Frobenius (non separable).

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- *Example*: Multiplication by ℓ ($\Rightarrow$ ℓ-torsion), Frobenius (non separable).

Cryptographic usage of isogenies

- Transfert the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic).
- Compute the class field polynomials (CM-method).
- Compute the modular polynomials.
- Determine $\mathrm{End}(A)$.

Cryptographic usage of isogenies

- Transfert the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic).
- Compute the class field polynomials (CM-method).
- Compute the modular polynomials.
- Determine $\mathrm{End}(A)$.

Cryptographic usage of isogenies

- Transfert the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic).
- Compute the class field polynomials (CM-method).
- Compute the modular polynomials.
- Determine $\mathrm{End}(A)$.

Cryptographic usage of isogenies

- Transfert the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic).
- Compute the class field polynomials (CM-method).
- Compute the modular polynomials.
- Determine $\mathrm{End}(A)$.

Cryptographic usage of isogenies

- Transfert the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic).
- Compute the class field polynomials (CM-method).
- Compute the modular polynomials.
- Determine $\mathrm{End}(A)$.

Vélu's formula

Theorem

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

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

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

Vélu's formula

Theorem

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

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

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

The modular polynomial

Definition

- The modular polynomial is a polynomial $\phi_n(x, y) \in \mathbb{Z}[x, y]$ such that $\phi_n(x, y) = 0$ 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 $\phi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes: the compressed coefficients of ϕ_2 take 26.8 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

Definition

- The modular polynomial is a polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$ such that $\phi_n(x,y) = 0$ 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 $\phi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes: the compressed coefficients of ϕ_2 take 26.8 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

Definition

- The modular polynomial is a polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$ such that $\phi_n(x,y)=0$ 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 $\phi_n(j(E),.) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes: the compressed coefficients of ϕ_2 take 26.8 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

Definition

- The modular polynomial is a polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$ such that $\phi_n(x,y)=0$ 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 $\phi_n(j(E),.) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes: the compressed coefficients of ϕ_2 take 26.8 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

Definition

- The modular polynomial is a polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$ such that $\phi_n(x,y)=0$ 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 $\phi_n(j(E),.) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes: the compressed coefficients of ϕ_2 take 26.8 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.

Outline

The theta group

Definition

Let $(A, \mathcal{L})$ be a (separably) polarized abelian variety over an algebraically closed field k. The polarisation $\mathcal{L}$ induces an isogeny

$$\begin{array}{rcl} \phi_{\mathcal{L}} \colon A & \longrightarrow & \widehat{A}_k \\ x & \longmapsto & t_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \end{array}.$$

We note $K(\mathcal{L}) = \operatorname{Ker} \phi_{\mathcal{L}}$, the theta group is $G(\mathcal{L}) = \{(x, \psi) \mid \psi : t_x^* \mathcal{L} \xrightarrow{\sim} \mathcal{L}\}$. $G(\mathcal{L})$ is a central extension of $K(\mathcal{L})$:

$$0 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0.$$

- Group law: $(x, \phi).(y, \psi) = (x + y, t_x^* \psi \circ \phi)$:

$$\mathcal{L} \xrightarrow{\phi} t_x^* \mathcal{L} \xrightarrow{t_x^* \psi} t_x^* (t_y^* \mathcal{L}) = t_{x+y}^* \mathcal{L}.$$

- Descent theory: If $K \subset K(\mathcal{L})$ is isotropic, sections $s : K \to G(\mathcal{L}) \Leftrightarrow$ descent data $\pi : (X, \mathcal{L}) \to (X/K, \mathcal{M})$.

The theta group

Definition

Let $(A, \mathcal{L})$ be a (separably) polarized abelian variety over an algebraically closed field k. The polarisation $\mathcal{L}$ induces an isogeny

$$\begin{array}{rccl} \phi_{\mathcal{L}}\colon A & \longrightarrow & \widehat{A}_k \\ x & \longmapsto & t_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \end{array}.$$

We note $K(\mathcal{L}) = \operatorname{Ker} \phi_{\mathcal{L}}$, the theta group is $G(\mathcal{L}) = \{(x, \psi) \mid \psi : t_x^* \mathcal{L} \xrightarrow{\sim} \mathcal{L}\}$. $G(\mathcal{L})$ is a central extension of $K(\mathcal{L})$:

$$0 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0.$$

- Group law: $(x, \phi).(y, \psi) = (x + y, t_x^* \psi \circ \phi)$:

$$\mathcal{L} \xrightarrow{\phi} t_x^* \mathcal{L} \xrightarrow{t_x^* \psi} t_x^*(t_y^* \mathcal{L}) = t_{x+y}^* \mathcal{L}.$$

- Descent theory: If $K \subset K(\mathcal{L})$ is isotropic, sections $s : K \to G(\mathcal{L}) \Leftrightarrow$ descent data $\pi : (X, \mathcal{L}) \to (X/K, \mathcal{M})$.

The theta group

Definition

Let $(A, \mathcal{L})$ be a (separably) polarized abelian variety over an algebraically closed field k. The polarisation $\mathcal{L}$ induces an isogeny

$$\begin{array}{rcl} \phi_{\mathcal{L}} \colon A & \longrightarrow & \widehat{A}_k \\ x & \longmapsto & t_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \end{array}.$$

We note $K(\mathcal{L}) = \operatorname{Ker} \phi_{\mathcal{L}}$, the theta group is $G(\mathcal{L}) = \{(x, \psi) \mid \psi : t_x^* \mathcal{L} \xrightarrow{\sim} \mathcal{L}\}$. $G(\mathcal{L})$ is a central extension of $K(\mathcal{L})$:

$$0 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0.$$

- Group law: $(x, \phi).(y, \psi) = (x + y, t_x^* \psi \circ \phi)$:

$$\mathcal{L} \xrightarrow{\phi} t_x^* \mathcal{L} \xrightarrow{t_x^* \psi} t_x^*(t_y^* \mathcal{L}) = t_{x+y}^* \mathcal{L}.$$

- Descent theory: If $K \subset K(\mathcal{L})$ is isotropic, sections $s : K \to G(\mathcal{L}) \Leftrightarrow$ descent data $\pi : (X, \mathcal{L}) \to (X/K, \mathcal{M})$.

Heisenberg group

Definition

The Heisenberg group of level n is $H(n) = k^* \times Z(n) \times \hat{Z}(n)$ where $Z(n) := \mathbb{Z}^g/n\mathbb{Z}^g$ and $\hat{Z}(n)$ is the dual of $Z(n)$. The group law is given by

$$(\alpha, x_1, x_2)(\beta, y_1, y_2) = (\langle x_1, y_2\rangle \alpha\beta, x_1 + y_1, x_2 + y_2),$$

where $\langle x_1, y_2\rangle = y_2(x_1)$ is the canonical pairing.

- A polarised abelian variety $(A, \mathcal{L})$ is of level n if $K(\mathcal{L}) \simeq Z(n)$.
- A theta structure on $(A, \mathcal{L})$ is an isomorphism $\Theta_{\mathcal{L}} : H(n) \to G(\mathcal{L})$.
- The theta structure $\Theta_{\mathcal{L}}$ induces a symplectic isomorphism (for the commutator pairing) $\overline{\Theta}_{\mathcal{L}} : K(n) := Z(n) \oplus \hat{Z}(n) \xrightarrow{\sim} K(\mathcal{L})$.
- The symplectic decomposition $K(n) = Z(n) \oplus \hat{Z}(n)$ induces a decomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.

Heisenberg group

Definition

The Heisenberg group of level n is $H(n) = k^* \times Z(n) \times \hat{Z}(n)$ where $Z(n) := \mathbb{Z}^g/n\mathbb{Z}^g$ and $\hat{Z}(n)$ is the dual of $Z(n)$. The group law is given by

$$(\alpha, x_1, x_2)(\beta, y_1, y_2) = (\langle x_1, y_2 \rangle \alpha\beta, x_1 + y_1, x_2 + y_2),$$

where $\langle x_1, y_2 \rangle = y_2(x_1)$ is the canonical pairing.

- A polarised abelian variety $(A, \mathcal{L})$ is of level n if $K(\mathcal{L}) \simeq Z(n)$.
- A theta structure on $(A, \mathcal{L})$ is an isomorphism $\Theta_{\mathcal{L}} : H(n) \to G(\mathcal{L})$.
- The theta structure $\Theta_{\mathcal{L}}$ induces a symplectic isomorphism (for the commutator pairing) $\overline{\Theta}_{\mathcal{L}} : K(n) := Z(n) \oplus \hat{Z}(n) \xrightarrow{\sim} K(\mathcal{L})$.
- The symplectic decomposition $K(n) = Z(n) \oplus \hat{Z}(n)$ induces a decomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.

Heisenberg group

Definition

The Heisenberg group of level n is $H(n) = k^* \times Z(n) \times \hat{Z}(n)$ where $Z(n) := \mathbb{Z}^g / n\mathbb{Z}^g$ and $\hat{Z}(n)$ is the dual of $Z(n)$. The group law is given by

$$(\alpha, x_1, x_2)(\beta, y_1, y_2) = (\langle x_1, y_2 \rangle \alpha\beta, x_1 + y_1, x_2 + y_2),$$

where $\langle x_1, y_2 \rangle = y_2(x_1)$ is the canonical pairing.

- A polarised abelian variety $(A, \mathcal{L})$ is of level n if $K(\mathcal{L}) \simeq Z(n)$.
- A theta structure on $(A, \mathcal{L})$ is an isomorphism $\Theta_{\mathcal{L}} : H(n) \to G(\mathcal{L})$.
- The theta structure $\Theta_{\mathcal{L}}$ induces a symplectic isomorphism (for the commutator pairing) $\overline{\Theta}_{\mathcal{L}} : K(n) := Z(n) \oplus \hat{Z}(n) \xrightarrow{\sim} K(\mathcal{L})$.
- The symplectic decomposition $K(n) = Z(n) \oplus \hat{Z}(n)$ induces a decomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.

Heisenberg group

Definition

The Heisenberg group of level n is $H(n) = k^* \times Z(n) \times \hat{Z}(n)$ where $Z(n) := \mathbb{Z}^g/n\mathbb{Z}^g$ and $\hat{Z}(n)$ is the dual of $Z(n)$. The group law is given by

$$(\alpha, x_1, x_2)(\beta, y_1, y_2) = (\langle x_1, y_2\rangle \alpha\beta, x_1 + y_1, x_2 + y_2),$$

where $\langle x_1, y_2\rangle = y_2(x_1)$ is the canonical pairing.

- A polarised abelian variety $(A, \mathcal{L})$ is of level n if $K(\mathcal{L}) \simeq Z(n)$.
- A theta structure on $(A, \mathcal{L})$ is an isomorphism $\Theta_{\mathcal{L}} : H(n) \to G(\mathcal{L})$.
- The theta structure $\Theta_{\mathcal{L}}$ induces a symplectic isomorphism (for the commutator pairing) $\overline{\Theta}_{\mathcal{L}} : K(n) := Z(n) \oplus \hat{Z}(n) \xrightarrow{\sim} K(\mathcal{L})$.
- The symplectic decomposition $K(n) = Z(n) \oplus \hat{Z}(n)$ induces a decomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.

Heisenberg group

Definition

The Heisenberg group of level n is $H(n) = k^* \times Z(n) \times \hat{Z}(n)$ where $Z(n) := \mathbb{Z}^g/n\mathbb{Z}^g$ and $\hat{Z}(n)$ is the dual of $Z(n)$. The group law is given by

$$(\alpha, x_1, x_2)(\beta, y_1, y_2) = (\langle x_1, y_2 \rangle \alpha\beta, x_1 + y_1, x_2 + y_2),$$

where $\langle x_1, y_2 \rangle = y_2(x_1)$ is the canonical pairing.

- A polarised abelian variety $(A, \mathcal{L})$ is of level n if $K(\mathcal{L}) \simeq Z(n)$.
- A theta structure on $(A, \mathcal{L})$ is an isomorphism $\Theta_{\mathcal{L}} : H(n) \to G(\mathcal{L})$.
- The theta structure $\Theta_{\mathcal{L}}$ induces a symplectic isomorphism (for the commutator pairing) $\overline{\Theta}_{\mathcal{L}} : K(n) := Z(n) \oplus \hat{Z}(n) \xrightarrow{\sim} K(\mathcal{L})$.
- The symplectic decomposition $K(n) = Z(n) \oplus \hat{Z}(n)$ induces a decomposition $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$.

Theta functions

- The Heisenberg group $H(n)$ admits a unique irreducible representation:

$$(\alpha, i, j).\delta_k = \langle i+k, -j\rangle \delta_{i+k}.$$

- The action of $G(\mathcal{L})$ on $\Gamma(\mathcal{L})$ given by

$$(x, \psi).\vartheta \mapsto \psi(t_x^* \vartheta)$$

  is irreducible.
- The basis of theta functions (induced by $\Theta_{\mathcal{L}}$) is the unique basis (up to a constant) such that

$$(\alpha, i, j).\vartheta_k = e_{\mathcal{L}}(i+k, -j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}}$ is the commutator pairing.
- If $l \geqslant 3$ then

$$z \mapsto (\vartheta_i(z))_{i \in Z(\overline{n})}$$

  is a projective embedding $A \to \mathbb{P}_k^{n^g - 1}$.

Theta functions

- The Heisenberg group $H(n)$ admits a unique irreducible representation:

$$(\alpha, i, j).\delta_k = \langle i+k, -j \rangle \delta_{i+k}.$$

- The action of $G(\mathcal{L})$ on $\Gamma(\mathcal{L})$ given by

$$(x, \psi).\vartheta \mapsto \psi(t_x^* \vartheta)$$

  is irreducible.
- The basis of theta functions (induced by $\Theta_{\mathcal{L}}$) is the unique basis (up to a constant) such that

$$(\alpha, i, j).\vartheta_k = e_{\mathcal{L}}(i+k, -j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}}$ is the commutator pairing.
- If $l \geqslant 3$ then

$$z \mapsto (\vartheta_i(z))_{i \in Z(\overline{n})}$$

  is a projective embedding $A \to \mathbb{P}_k^{n^g - 1}$.

Theta functions

- The Heisenberg group $H(n)$ admits a unique irreducible representation:

$$(\alpha, i, j).\delta_k = \langle i+k, -j\rangle \delta_{i+k}.$$

- The action of $G(\mathcal{L})$ on $\Gamma(\mathcal{L})$ given by

$$(x, \psi).\vartheta \mapsto \psi(t_x^* \vartheta)$$

  is irreducible.
- The basis of theta functions (induced by $\Theta_{\mathcal{L}}$) is the unique basis (up to a constant) such that

$$(\alpha, i, j).\vartheta_k = e_{\mathcal{L}}(i+k, -j)\vartheta_{i+k}$$

  where $e_{\mathcal{L}}$ is the commutator pairing.
- If $l \geqslant 3$ then

$$z \mapsto (\vartheta_i(z))_{i \in Z(\overline{n})}$$

  is a projective embedding $A \to \mathbb{P}_k^{n^g - 1}$.

Theta functions

- The Heisenberg group $H(n)$ admits a unique irreducible representation:
$$(\alpha, i, j).\delta_k = \langle i+k, -j\rangle \delta_{i+k}.$$
- The action of $G(\mathcal{L})$ on $\Gamma(\mathcal{L})$ given by
$$(x, \psi).\vartheta \mapsto \psi(t_x^* \vartheta)$$
is irreducible.
- The basis of theta functions (induced by $\Theta_{\mathcal{L}}$) is the unique basis (up to a constant) such that
$$(\alpha, i, j).\vartheta_k = e_{\mathcal{L}}(i+k, -j)\vartheta_{i+k}$$
where $e_{\mathcal{L}}$ is the commutator pairing.
- If $l \geqslant 3$ then
$$z \mapsto (\vartheta_i(z))_{i \in Z(\overline{n})}$$
is a projective embedding $A \to \mathbb{P}_k^{n^g - 1}$.

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 $\mathbb{C}^g$.

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

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = e^{\pi i\, {}^t a\Omega a + 2\pi i\, {}^t a(z+b)}\vartheta(z+\Omega a+b,\Omega) \quad a,b\in\mathbb{Q}^g$$

- The quasi-periodicity is given by

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+m+\Omega n,\Omega) = e^{2\pi i({}^t a m - {}^t b n) - \pi i\, {}^t n\Omega n - 2\pi i\, {}^t n z}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)$$

- Ω induces a theta structure of level ∞. The corresponding theta basis of level n is given by

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

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 $\mathbb{C}^g$.

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

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = e^{\pi i \, {}^t a \Omega a + 2\pi i \, {}^t a (z+b)} \vartheta(z + \Omega a + b, \Omega) \quad a, b \in \mathbb{Q}^g$$

- The quasi-periodicity is given by

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + m + \Omega n, \Omega) = e^{2\pi i ({}^t a m - {}^t b n) - \pi i \, {}^t n \Omega n - 2\pi i \, {}^t n z} \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)$$

- Ω induces a theta structure of level ∞. The corresponding theta basis of level n is given by

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

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 $\mathbb{C}^g$.

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

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = e^{\pi i \, {}^t a \Omega a + 2\pi i \, {}^t a (z+b)} \vartheta(z + \Omega a + b, \Omega) \quad a, b \in \mathbb{Q}^g$$

- The quasi-periodicity is given by

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + m + \Omega n, \Omega) = e^{2\pi i ({}^t a m - {}^t b n) - \pi i \, {}^t n \Omega n - 2\pi i \, {}^t n z} \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)$$

- Ω induces a theta structure of level ∞. The corresponding theta basis of level n is given by

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

The isogeny theorem

Theorem

Let $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ be a marked abelian variety of level ℓn. The canonical section $\hat{Z}(\ell n) \to H(\ell n), j \mapsto (1, 0, j)$ induce via $\Theta_{\mathcal{L}}$ a section $K = K_2(\mathcal{L})[\ell] \to G(\mathcal{L})$. The theta structure $\Theta_{\mathcal{L}}$ descend to a theta structure $(B, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ such that $B = A/K$ and if $\pi : A \to B$ is the corresponding isogeny:

$$\pi^* \vartheta_i^{\mathcal{L}_0} = \lambda \vartheta_i^{\mathcal{L}}.$$

Here $Z(n) \hookrightarrow Z(\ell n)$ is the canonical embedding $x \mapsto \ell x$.

Proof with $k = \mathbb{C}$.

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

$\square$

The isogeny theorem

Theorem

Let $(A, \mathcal{L}, \Theta_\mathcal{L})$ be a marked abelian variety of level ℓn. The canonical section $\hat{Z}(\ell n) \to H(\ell n)$, $j \mapsto (1, 0, j)$ induce via $\Theta_\mathcal{L}$ a section $K = K_2(\mathcal{L})[\ell] \to G(\mathcal{L})$. The theta structure $\Theta_\mathcal{L}$ descend to a theta structure $(B, \mathcal{L}_0, \Theta_{\mathcal{L}_0})$ such that $B = A/K$ and if $\pi : A \to B$ is the corresponding isogeny:

$$\pi^* \vartheta_i^{\mathcal{L}_0} = \lambda \vartheta_i^{\mathcal{L}}.$$

Here $Z(n) \hookrightarrow Z(\ell n)$ is the canonical embedding $x \mapsto \ell x$.

Proof with $k = \mathbb{C}$.

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

$\square$

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid n$)

- *The theta null point of level n $(a_i)_{i \in Z(\overline{n})} := (\vartheta_i(0))_{i \in Z(n)}$ satisfy the Riemann Relations:*

$$\sum_{t \in Z(\overline{2})} a_{x+t} a_{y+t} \sum_{t \in Z(\overline{2})} a_{u+t} a_{v+t} = \sum_{t \in Z(\overline{2})} a_{x'+t} a_{y'+t} \sum_{t \in Z(\overline{2})} a_{u'+t} a_{v'+t} \tag{1}$$

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

$$a_x = a_{-x}$$

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

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid n$)

- *The theta null point of level n $(a_i)_{i \in Z(\overline{n})} := (\vartheta_i(0))_{i \in Z(n)}$ satisfy the Riemann Relations:*

$$\sum_{t \in Z(\overline{2})} a_{x+t} a_{y+t} \sum_{t \in Z(\overline{2})} a_{u+t} a_{v+t} = \sum_{t \in Z(\overline{2})} a_{x'+t} a_{y'+t} \sum_{t \in Z(\overline{2})} a_{u'+t} a_{v'+t} \tag{1}$$

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

$$a_x = a_{-x}$$

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

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid n$)

- *The theta null point of level n $(a_i)_{i \in Z(\overline{n})} := (\vartheta_i(0))_{i \in Z(n)}$ satisfy the Riemann Relations:*

$$\sum_{t \in Z(\overline{2})} a_{x+t} a_{y+t} \sum_{t \in Z(\overline{2})} a_{u+t} a_{v+t} = \sum_{t \in Z(\overline{2})} a_{x'+t} a_{y'+t} \sum_{t \in Z(\overline{2})} a_{u'+t} a_{v'+t} \qquad (1)$$

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

$$a_x = a_{-x}$$

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

Remark

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

Summary

$$
\begin{array}{ccc}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 & \overset{\text{determines}}{\longleftarrow\cdots\cdots} & (a_i)_{i \in Z(\overline{\ell})} \in \mathcal{M}_{\overline{\ell n}}(k) \\
\hat{\pi} \uparrow \downarrow \pi & & \downarrow \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 & \longleftarrow\cdots\cdots & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k)
\end{array}
$$

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

Summary

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

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

Summary

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

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

Summary

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

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

Summary

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

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

Summary

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

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

Outline

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a_i')_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a_i')_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a'_i)_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a'_i)_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a'_i)_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

An Example with $n \wedge \ell = 1$

We will show an example with $g = 1$, $n = 4$ and $\ell n = 12$ ($\ell = 3$).

- Let B be the elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$. The corresponding theta null point (b_0, b_1, b_2, b_3) of level 4 is $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- We note $V_B(k)$ the subvariety of $\mathcal{M}_{12}(k)$ defined by

$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

$$\pi(\vartheta_i^A(x)_{i \in Z(12)}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x))$$

- Program:
  - Compute $\widehat{\pi}$ from a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$ from the kernel K of $\widehat{\pi}$.
  - Compute a theta null point $(a'_i)_{i \in Z(\overline{n})}$ of level n corresponding to $A = B/K$.

Program

The kernel of $\widehat{\pi}$

- Let $(a_i)_{i \in Z(\overline{\ell n})}$ be a valid theta null point solution. Let ζ be a primitive ℓ root of unity.
  The kernel of π is

$$\{(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}),$$
$$(a_0, \zeta a_1, \zeta^2 a_2, a_3, \zeta a_4, \zeta^2 a_5, a_6, \zeta a_7, \zeta^2 a_8, a_9, \zeta a_{10}, \zeta^2 a_{11}),$$
$$(a_0, \zeta^2 a_1, \zeta a_2, a_3, \zeta^2 a_4, \zeta a_5, a_6, \zeta^2 a_7, \zeta a_8, a_9, \zeta^2 a_{10}, \zeta a_{11})\}$$

- If $i \in Z(\overline{\ell})$ we define
$$\pi_i(x) = (x_{ni+\ell j})_{j \in Z(\overline{n})}$$
  Let $R_0 := \pi_0(0_A) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(0_A) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(0_A) = (a_8, a_{11}, a_2, a_5)$.
- The kernel K of $\widehat{\pi}$ is
$$K = \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\}$$

The kernel of $\widehat{\pi}$

- Let $(a_i)_{i \in Z(\overline{\ell n})}$ be a valid theta null point solution. Let ζ be a primitive ℓ root of unity.
  The kernel of π is

$$\{(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}),$$
$$(a_0, \zeta a_1, \zeta^2 a_2, a_3, \zeta a_4, \zeta^2 a_5, a_6, \zeta a_7, \zeta^2 a_8, a_9, \zeta a_{10}, \zeta^2 a_{11}),$$
$$(a_0, \zeta^2 a_1, \zeta a_2, a_3, \zeta^2 a_4, \zeta a_5, a_6, \zeta^2 a_7, \zeta a_8, a_9, \zeta^2 a_{10}, \zeta a_{11})\}$$

- If $i \in Z(\overline{\ell})$ we define
$$\pi_i(x) = (x_{ni+\ell j})_{j \in Z(\overline{n})}$$
  Let $R_0 := \pi_0(0_A) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(0_A) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(0_A) = (a_8, a_{11}, a_2, a_5)$.
- The kernel K of $\widehat{\pi}$ is

$$K = \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\}$$

The kernel of $\widehat{\pi}$

- Let $(a_i)_{i \in Z(\overline{\ell n})}$ be a valid theta null point solution. Let ζ be a primitive ℓ root of unity.
  The kernel of π is

$$\{(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}),$$
$$(a_0, \zeta a_1, \zeta^2 a_2, a_3, \zeta a_4, \zeta^2 a_5, a_6, \zeta a_7, \zeta^2 a_8, a_9, \zeta a_{10}, \zeta^2 a_{11}),$$
$$(a_0, \zeta^2 a_1, \zeta a_2, a_3, \zeta^2 a_4, \zeta a_5, a_6, \zeta^2 a_7, \zeta a_8, a_9, \zeta^2 a_{10}, \zeta a_{11})\}$$

- If $i \in Z(\overline{\ell})$ we define

$$\pi_i(x) = (x_{ni+\ell j})_{j \in Z(\overline{n})}$$

  Let $R_0 := \pi_0(0_A) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(0_A) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(0_A) = (a_8, a_{11}, a_2, a_5)$.
- The kernel K of $\widehat{\pi}$ is

$$K = \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\}$$

The pseudo addition law ($k = \mathbb{C}$)

Theorem

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) = \Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

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

$$\chi \in \hat{Z}(\overline{2}), i, j, k, l \in Z(\overline{n})$$

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

Addition and isogenies

Proposition

$\pi_i(x) = \pi_0(x) + R_i$ so we have:

$$\pi_{i+j}(x+y) = \pi_i(x) + \pi_j(y)$$
$$\pi_{i-j}(x-y) = \pi_i(x) - \pi_j(y)$$

- $x \in A$ is entirely determined by $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \pi_1(x) + R_1$, $\pi_1(x) - R_1 = \pi_0(x) = y$.

Corollary

- *x is entirely determined by*

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

- *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.*

Addition and isogenies

Proposition

$\pi_i(x) = \pi_0(x) + R_i$ so we have:

$$\pi_{i+j}(x+y) = \pi_i(x) + \pi_j(y)$$
$$\pi_{i-j}(x-y) = \pi_i(x) - \pi_j(y)$$

- $x \in A$ is entirely determined by $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \pi_1(x) + R_1$, $\pi_1(x) - R_1 = \pi_0(x) = y$.

Corollary

- *x is entirely determined by*

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

- *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.*

Addition and isogenies

Proposition

$\pi_i(x) = \pi_0(x) + R_i$ so we have:

$$\pi_{i+j}(x+y) = \pi_i(x) + \pi_j(y)$$
$$\pi_{i-j}(x-y) = \pi_i(x) - \pi_j(y)$$

- $x \in A$ is entirely determined by $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \pi_1(x) + R_1$, $\pi_1(x) - R_1 = \pi_0(x) = y$.

Corollary

- *x is entirely determined by*

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

- *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.*

Addition and isogenies

Proposition

$\pi_i(x) = \pi_0(x) + R_i$ so we have:

$$\pi_{i+j}(x+y) = \pi_i(x) + \pi_j(y)$$
$$\pi_{i-j}(x-y) = \pi_i(x) - \pi_j(y)$$

- $x \in A$ is entirely determined by $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \pi_1(x) + R_1$, $\pi_1(x) - R_1 = \pi_0(x) = y$.

Corollary

- *x is entirely determined by*

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

- *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.*

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

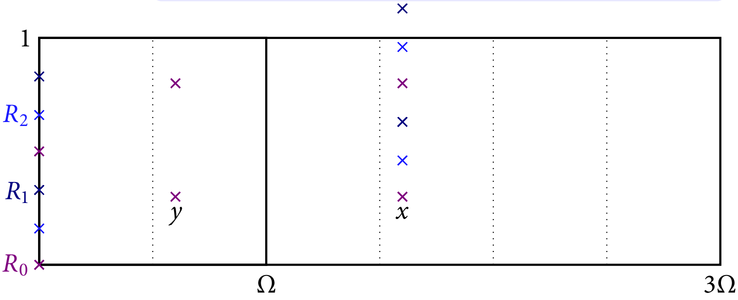
$$\widehat{\pi}(y) = \ell.x$$

The contragredient isogeny

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

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

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



The contragredient isogeny

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

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

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

Let $y \in B$. We can compute $y_i = y \oplus R_i$ with a normal addition. We have $y_i = \lambda_i \pi_i(x)$.

$$y = [\pi_i(x) + (\ell - 1).R_i] = \lambda_i^\ell [y_i + (\ell) R_i]$$

$$\pi_i(\ell.x) = [\pi_i(x) + (\ell).y] = \lambda_i^\ell [y_i + (\ell).y]$$

Corollary

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

The contragredient isogeny

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

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

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

Let $y \in B$. We can compute $y_i = y \oplus R_i$ with a normal addition. We have $y_i = \lambda_i \pi_i(x)$.

$$y = [\pi_i(x) + (\ell - 1).R_i] = \lambda_i^\ell [y_i + (\ell) R_i]$$
$$\pi_i(\ell.x) = [\pi_i(x) + (\ell).y] = \lambda_i^\ell [y_i + (\ell).y]$$

Corollary

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

Example

Let $K = \{(3:1:18:1), (22:15:4:1), (18:29:23:1)\}$, a point solution corresponding to this kernel is given by $(3, \eta^{14233}, \eta^{2317}, 1, \eta^{1324}, \eta^{5296}, 18, \eta^{5296}, \eta^{1324}, 1, \eta^{2317}, \eta^{14233})$ where $\eta^3 + \eta + 28 = 0$.
Let $y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$. We want to determine $\pi_1(x)$, we have to compute:

$$
\begin{array}{ccccc}
 & y & & & \\
R_1 & y + R_1 & y + 2R_1 & y + 3R_1 = y \\
 & 2y + R_1 & & & \\
 & 3y + R_1 & & &
\end{array}
$$

Example

Let $K = \{(3:1:18:1), (22:15:4:1), (18:29:23:1)\}$, a point solution corresponding to this kernel is given by $(3, \eta^{14233}, \eta^{2317}, 1, \eta^{1324}, \eta^{5296}, 18, \eta^{5296}, \eta^{1324}, 1, \eta^{2317}, \eta^{14233})$ where $\eta^3 + \eta + 28 = 0$.

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y + R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$

$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032}$$

$$2y + R_1 = \lambda_1^2(\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$

$$3y + R_1 = \lambda_1^3(\eta^{7096}, \eta^{11068}, \eta^{8089}, \eta^{20005}) = \eta^{5772} R_1$$

We have $\lambda_1^3 = \eta^{28758}$ and

$$\widehat{\pi}(y) = (3, \eta^{21037}, \eta^{15925}, 1, \eta^{8128}, \eta^{18904}, 18, \eta^{12100}, \eta^{14932}, 1, \eta^{9121}, \eta^{27841})$$

Program

The action of the symplectic group on the modular space

- Let $K \subset B[\ell]$ be an isotropic subgroup of maximal rank. Let $(a_i)_{i \in Z(\overline{\ell n})}$ 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

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

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

  where ψ_1 is an automorphism of $Z(\overline{\ell})$ and ψ_2 is a symmetric endomorphism of $Z(\overline{\ell n})$.

- In particular by action (2), 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 symplectic group on the modular space

- Let $K \subset B[\ell]$ be an isotropic subgroup of maximal rank. Let $(a_i)_{i \in Z(\overline{\ell n})}$ be a theta null point corresponding to the isogeny $\pi : B \to B/K$.

Example

These points corresponds to the same isogeny:

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$$

$$(a_0, \zeta a_1, \zeta^{2^2} a_2, a_3, \zeta a_4, \zeta^{2^2} a_5, a_6, \zeta a_7, \zeta^{2^2} a_8, a_9, \zeta a_{10}, \zeta^{2^2} a_{11})$$

$$(a_0, \zeta^2 a_1, \zeta^2 a_2, a_3, \zeta^2 a_4, \zeta^2 a_5, a_6, \zeta^2 a_7, \zeta^2 a_8, a_9, \zeta^2 a_{10}, \zeta^2 a_{11})$$

$$(a_0, a_5, a_{10}, a_3, a_8, a_1, a_6, a_{11}, a_4, a_9, a_2, a_7)$$

$$(a_0, \zeta a_5, \zeta a_{10}, a_3, \zeta a_8, \zeta a_1, a_6, \zeta a_{11}, \zeta a_4, a_9, \zeta a_2, \zeta a_7)$$

$$(a_0, \zeta^2 a_5, \zeta^2 a_{10}, a_3, \zeta^2 a_8, \zeta^2 a_1, a_6, \zeta^2 a_{11}, \zeta^2 a_4, a_9, \zeta^2 a_2, \zeta^2 a_7)$$

Recovering the projective factors

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

$$(\ell' + 1).R_i = -\ell'.R_i$$
$$\lambda_i^{(\ell'+1)^2}(\ell' + 1).T_i = \lambda_i^{\ell'^2}\ell'.T_i$$

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 (3) shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollary

We have Vélu-like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-roots and $g(g+1)/2 \cdot O(\log(\ell))$ 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 $\ell = 2\ell' + 1$

$$(\ell' + 1).R_i = -\ell'.R_i$$
$$\lambda_i^{(\ell'+1)^2}(\ell' + 1).T_i = \lambda_i^{\ell'^2}\ell'.T_i$$

  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 (3) shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollary

We have Vélu-like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-roots and $g(g+1)/2 \cdot O(\log(\ell))$ 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 $\ell = 2\ell' + 1$

$$(\ell' + 1).R_i = -\ell'.R_i$$
$$\lambda_i^{(\ell'+1)^2}(\ell' + 1).T_i = \lambda_i^{\ell'^2}\ell'.T_i$$

  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 (3) shows that each choice of a ℓ-root of unity corresponds to a valid theta null point.

Corollary

We have Vélu-like formulas to recover the compressed modular point solution, by computing $g(g+1)/2$ ℓ-roots and $g(g+1)/2 \cdot O(\log(\ell))$ additions. The compressed coordinates are sufficient to compute the compressed coordinates of the associated isogeny.

Program

Changing level by taking an isogeny

$$
\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}
$$

- $\pi_2 \circ \widehat{\pi}$ is an ℓ^2 isogeny between two varieties of level n.
- Each choice of the ℓ-roots of unity in the Vélu's-like formulas give a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K come from these choices.
- We know the kernel of the contragredient isogeny $C \to A$, this is helpful for computing isogeny graphs.

Changing level by taking an isogeny

$$
\begin{tikzcd}
B \arrow[dr, "\widehat{\pi}"] \arrow[dd, "{[\ell]}"'] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}
$$

- $\pi_2 \circ \widehat{\pi}$ is an ℓ^2 isogeny between two varieties of level n.
- Each choice of the ℓ-roots of unity in the Vélu's-like formulas give a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K come from these choices.
- We know the kernel of the contragredient isogeny $C \to A$, this is helpful for computing isogeny graphs.

Changing level by taking an isogeny

$$
\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}
$$

- $\pi_2 \circ \widehat{\pi}$ is an ℓ^2 isogeny between two varieties of level n.
- Each choice of the ℓ-roots of unity in the Vélu's-like formulas give a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K come from these choices.
- We know the kernel of the contragredient isogeny $C \to A$, this is helpful for computing isogeny graphs.

Changing level by taking an isogeny

$$\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}$$

- $\pi_2 \circ \widehat{\pi}$ is an ℓ^2 isogeny between two varieties of level n.
- Each choice of the ℓ-roots of unity in the Vélu's-like formulas give a different decomposition $A[\ell] = A[\ell]_1 \oplus K$. All the ℓ^2-isogenies $B \to C$ containing K come from these choices.
- We know the kernel of the contragredient isogeny $C \to A$, this is helpful for computing isogeny graphs.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny. There existe a line bundle $\mathcal{L}'$ on A such that $\mathcal{L} = \mathcal{L}'^{\ell}$ and a theta structure on $\mathcal{L}'$ such that the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r)\in K_1(\mathcal{L}')\times\ldots\times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r)=(i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ give the Riemann relations. (For general ℓ use the matrix from the quaternions.)
- Can be combined with the preceding method to compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ pseudo-additions in $B \Rightarrow$ full generalisation of Vélu's formulas.
- The formulas are rational if the kernel K is rational.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell\,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny. There existe a line bundle $\mathcal{L}'$ on A such that $\mathcal{L} = \mathcal{L}'^{\ell}$ and a theta structure on $\mathcal{L}'$ such that the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r)\in K_1(\mathcal{L}')\times\ldots\times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r)=(i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ give the Riemann relations. (For general ℓ use the matrix from the quaternions.)
- Can be combined with the preceding method to compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ pseudo-additions in $B \Rightarrow$ full generalisation of Vélu's formulas.
- The formulas are rational if the kernel K is rational.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny. There existe a line bundle $\mathcal{L}'$ on A such that $\mathcal{L} = \mathcal{L}'^{\ell}$ and a theta structure on $\mathcal{L}'$ such that the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r)\in K_1(\mathcal{L}')\times\ldots\times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r)=(i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ give the Riemann relations. (For general ℓ use the matrix from the quaternions.)
- Can be combined with the preceding method to compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ pseudo-additions in $B \Rightarrow$ full generalisation of Vélu's formulas.
- The formulas are rational if the kernel K is rational.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny. There existe a line bundle $\mathcal{L}'$ on A such that $\mathcal{L} = \mathcal{L}'^{\ell}$ and a theta structure on $\mathcal{L}'$ such that the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r)\in K_1(\mathcal{L}')\times\ldots\times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r)=(i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ give the Riemann relations. (For general ℓ use the matrix from the quaternions.)
- Can be combined with the preceding method to compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ pseudo-additions in $B \Rightarrow$ full generalisation of Vélu's formulas.
- The formulas are rational if the kernel K is rational.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny. There existe a line bundle $\mathcal{L}'$ on A such that $\mathcal{L} = {\mathcal{L}'}^{\ell}$ and a theta structure on $\mathcal{L}'$ such that the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r)\in K_1(\mathcal{L}')\times\ldots\times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r)=(i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ give the Riemann relations. (For general ℓ use the matrix from the quaternions.)
- Can be combined with the preceding method to compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ pseudo-additions in $B \Rightarrow$ full generalisation of Vélu's formulas.
- The formulas are rational if the kernel K is rational.

Perspectives

- We need to know the kernel ⇒ find equations for the quotient of the modular space by the action of the symplectic group.
- Theta functions are not rational ⇒ go back and forth between theta functions and Mumford coordinates (Romain Cosset).
- Fast computation of the commutator pairing with theta functions ⇒ ANTS IX, Nancy!

Perspectives

- We need to know the kernel ⇒ find equations for the quotient of the modular space by the action of the symplectic group.
- Theta functions are not rational ⇒ go back and forth between theta functions and Mumford coordinates (Romain Cosset).
- Fast computation of the commutator pairing with theta functions ⇒ ANTS IX, Nancy!

Perspectives

- We need to know the kernel $\Rightarrow$ find equations for the quotient of the modular space by the action of the symplectic group.
- Theta functions are not rational $\Rightarrow$ go back and forth between theta functions and Mumford coordinates (Romain Cosset).
- Fast computation of the commutator pairing with theta functions $\Rightarrow$ ANTS IX, Nancy!