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

26 Novembre 2009, Marseille

Outline

Outline

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

Outline

Outline

Discrete logarithm

Definition (DLP)

Let G be a commutative finite group, $g \in G$ and $x \in \mathbb{N}$. Let $h = x \cdot g$. The discrete logarithm $\log_g(h)$ is x.

- The DLP is hard (in a generic group) if the order of g is divisible by a large prime.
  - $\Rightarrow$ Usual tools of public key cryptography (and more!)
  - $\Rightarrow$ Find suitable abelian groups.

Discrete logarithm

Definition (DLP)

Let G be a commutative finite group, $g \in G$ and $x \in \mathbb{N}$. Let $h = x \cdot g$. The discrete logarithm $\log_g(h)$ is x.

- The DLP is hard (in a generic group) if the order of g is divisible by a large prime.
  - $\Rightarrow$ Usual tools of public key cryptography (and more!)
  - $\Rightarrow$ Find suitable abelian groups.

Discrete logarithm

Definition (DLP)

Let G be a commutative finite group, $g \in G$ and $x \in \mathbb{N}$. Let $h = x \cdot g$. The discrete logarithm $\log_g(h)$ is x.

- The DLP is hard (in a generic group) if the order of g is divisible by a large prime.
  - $\Rightarrow$ Usual tools of public key cryptography (and more!)
  - $\Rightarrow$ Find suitable abelian groups.

Discrete logarithm

Definition (DLP)

Let G be a commutative finite group, $g \in G$ and $x \in \mathbb{N}$. Let $h = x \cdot g$. The discrete logarithm $\log_g(h)$ is x.

- The DLP is hard (in a generic group) if the order of g is divisible by a large prime.
  - $\Rightarrow$ Usual tools of public key cryptography (and more!)
  - $\Rightarrow$ Find suitable abelian groups.

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...

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.

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

- *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).

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 ($\Rightarrow \ell$-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.
- 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.
- 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.
- 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.
- 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.
- 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

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

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

Vélu's formula

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

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

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

The modular polynomial

Definition

- 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

Definition

- 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

Definition

- 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

Definition

- 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

Definition

- 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.

Outline

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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

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

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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

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

Projective embeddings given by theta functions

Theorem

- *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

Theorem

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

The isogeny theorem

Theorem

- 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:

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

Proof.

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

□

The isogeny theorem

Theorem

- 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:

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

Proof.

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

□

The isogeny theorem

Theorem

- *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:*

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

Proof.

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

□

The isogeny theorem

Theorem

- *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:*

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

Proof.

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

$\square$

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

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

$$\sum_{t \in \mathcal{Z}_2} a_{x+t} a_{y+t} \sum_{t \in \mathcal{Z}_2} a_{u+t} a_{v+t} = \sum_{t \in \mathcal{Z}_2} a_{x'+t} a_{y'+t} \sum_{t \in \mathcal{Z}_2} a_{u'+t} a_{v'+t} \quad (1)$$

  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 preserves the isomorphic classes).
- *Algebraic action:* $\mathrm{Sp}_{2g}(\mathcal{Z}_\ell)$ acts on $\mathcal{M}_\ell$.

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

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

$$\sum_{t \in Z_2} a_{x+t} a_{y+t} \sum_{t \in Z_2} a_{u+t} a_{v+t} = \sum_{t \in Z_2} a_{x'+t} a_{y'+t} \sum_{t \in Z_2} a_{u'+t} a_{v'+t} \qquad (1)$$

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 preserves the isomorphic classes).
- *Algebraic action:* $\mathrm{Sp}_{2g}(Z_\ell)$ acts on $\mathcal{M}_\ell$.

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

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

$$\sum_{t \in \mathcal{Z}_2} a_{x+t} a_{y+t} \sum_{t \in \mathcal{Z}_2} a_{u+t} a_{v+t} = \sum_{t \in \mathcal{Z}_2} a_{x'+t} a_{y'+t} \sum_{t \in \mathcal{Z}_2} a_{u'+t} a_{v'+t} \tag{1}$$

  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 preserves the isomorphic classes).
- *Algebraic action:* $\mathrm{Sp}_{2g}(\mathcal{Z}_\ell)$ acts on $\mathcal{M}_\ell$.

Summary

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

- 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

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

- 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

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

- 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.

Outline

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

An Example with $n \wedge m = 1$

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

- 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 $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \to B$:

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

- Program:
  - Compute $\hat{\pi}$ from a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}} \in V_B^0(k)$.
  - Compute a valid theta null point $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ from the kernel K of $\hat{\pi}$.
  - Compute all valid theta null points $V_B^0(k)$ from $B[\ell]$.

Program

3. Computing isogenies
   - Computing the contragredient isogeny
   - Vélu-like formula in dimension g

The kernel of $\hat{\pi}$

- Let $(a_i)_{i \in \mathcal{Z}_\ell}$ be a valid theta null point solution. Let ζ be a primitive m 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 $i \in \mathcal{Z}_m$ we define

$$\pi_i(x) = (x_{ni+mj})_{j \in \mathcal{Z}_n}$$

Let $R_0 := \pi_0(\widetilde{0}_{A_k}) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(\widetilde{0}_{A_k}) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(\widetilde{0}_{A_k}) = (a_8, a_{11}, a_2, a_5)$.

- The kernel K of $\hat{\pi}$ 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 $\hat{\pi}$

- Let $(a_i)_{i \in \mathcal{Z}_\ell}$ be a valid theta null point solution. Let ζ be a primitive m 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 $i \in \mathcal{Z}_m$ we define

$$\pi_i(x) = (x_{ni+mj})_{j \in \mathcal{Z}_n}$$

  Let $R_0 := \pi_0(\widetilde{0}_{A_k}) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(\widetilde{0}_{A_k}) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(\widetilde{0}_{A_k}) = (a_8, a_{11}, a_2, a_5)$.

- The kernel K of $\hat{\pi}$ 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 $\hat{\pi}$

- Let $(a_i)_{i \in \mathcal{Z}_\ell}$ be a valid theta null point solution. Let ζ be a primitive m 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 $i \in \mathcal{Z}_m$ we define

$$\pi_i(x) = (x_{ni+mj})_{j \in \mathcal{Z}_n}$$

  Let $R_0 := \pi_0(\widetilde{0}_{A_k}) = (a_0, a_3, a_6, a_9)$, $R_1 := \pi_1(\widetilde{0}_{A_k}) = (a_4, a_7, a_{10}, a_1)$, $R_2 := \pi_2(\widetilde{0}_{A_k}) = (a_8, a_{11}, a_2, a_5)$.

- The kernel K of $\hat{\pi}$ 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 addition law

Theorem

$$\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) =$$
$$\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

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

$$\chi \in \hat{\mathcal{Z}}_2, i, j, k, l \in \mathcal{Z}_n$$
$$(i', j', k', l') = A(i, j, k, l)$$

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 $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \texttt{chaine\_add}(\pi_1(x), R_1, \pi_0(x))$

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 $O(m^g)$ 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 $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \texttt{chaine\_add}(\pi_1(x), R_1, \pi_0(x))$

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 $O(m^g)$ 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 $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \texttt{chaine\_add}(\pi_1(x), R_1, \pi_0(x))$

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 $O(m^g)$ 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 $\pi_0(x), \pi_1(x), \pi_2(x)$.
- $\pi_2(x) = \texttt{chaine\_add}(\pi_1(x), R_1, \pi_0(x))$

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 $O(m^g)$ chain additions.*
- *Can still do chain additions with this representation.*

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

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

The contragredient isogeny

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

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

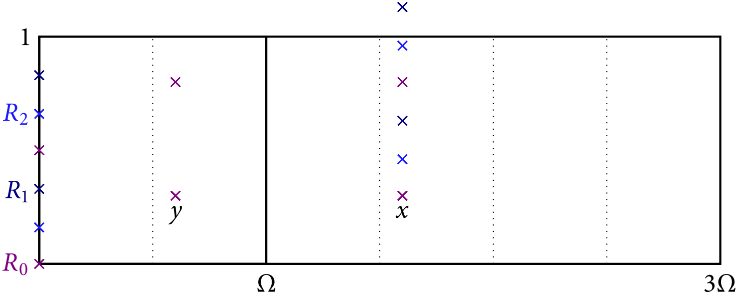
$$\hat{\pi}(y) = m.x$$

The contragredient isogeny

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

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

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



The contragredient isogeny

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

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

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

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

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

Corollary

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

The contragredient isogeny

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

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

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

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

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

Corollary

We can compute $\pi_i(m.x)$ with two fast multiplications of length m. To recover the compressed coordinates of $\hat{\pi}(y)$, we need $g(g+1)/2 \cdot O(\log(m))$ 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 $\eta^3 + \eta + 28 = 0$. We have to compute:

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

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 $\eta^3+\eta+28=0$. We have to compute:

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

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

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

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

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

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

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

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

Program

3. Computing isogenies
   - Computing the contragredient isogeny
   - Vélu-like formula in dimension g

The action of the symplectic group on the modular space

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

The action of the symplectic group on the modular space

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

- These points corresponds to the same isogeny:

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

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

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

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

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

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

The action of the symplectic group on the modular space

- Let $K \subset B[\ell]$ be an isotropic subgroup of maximal rank. Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ 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 (2), if $\{T_{e_i}\}_{i \in [1..g]}$ is a basis of K, we may suppose that $R_{e_i} = \lambda_{e_i} T_{e_i}$.

Recovering the projective factors

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

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

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 m-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 $g(g+1)/2$ m-roots and $g(g+1)/2 \cdot O(\log(m))$ 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 $m = 2m' + 1$

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

  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 m-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 $g(g+1)/2$ m-roots and $g(g+1)/2 \cdot O(\log(m))$ 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 $m = 2m' + 1$

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

  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 m-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 $g(g+1)/2$ m-roots and $g(g+1)/2 \cdot O(\log(m))$ additions. The compressed coordinates are sufficient to compute the compressed coordinates of the associated isogeny.

Isogeny graphs

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

- $\pi_2 \circ \hat{\pi}$ is an m^2 isogeny between two varieties of level n.
- Each choice of the m-roots of unity in the Vélu's-like formulas give a different decomposition $A[m] = A[m]_1 \oplus K$. All the m^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.

Isogeny graphs

$$\begin{tikzcd}
B \arrow[d, "{[m]}"'] \arrow[dr, "\hat{\pi}"] & & \\
{B= A/A[m]_2} & {A, A[m] = A[m]_1 \oplus A[m]_2} \arrow[l, "\pi"'] \arrow[d, "\pi_2"] & \\
& {C= A/A[m]_1} &
\end{tikzcd}$$

- $\pi_2 \circ \hat{\pi}$ is an m^2 isogeny between two varieties of level n.
- Each choice of the m-roots of unity in the Vélu's-like formulas give a different decomposition $A[m] = A[m]_1 \oplus K$. All the m^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.

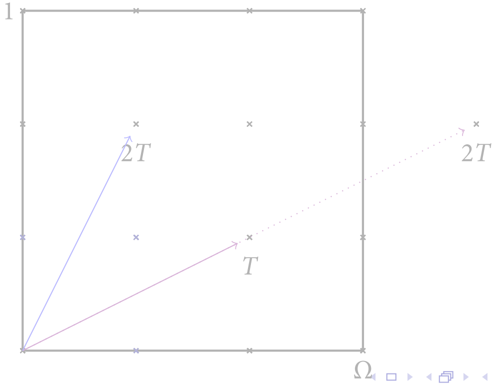
Isogeny graphs

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

- $\pi_2 \circ \hat{\pi}$ is an m^2 isogeny between two varieties of level n.
- Each choice of the m-roots of unity in the Vélu's-like formulas give a different decomposition $A[m] = A[m]_1 \oplus K$. All the m^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.

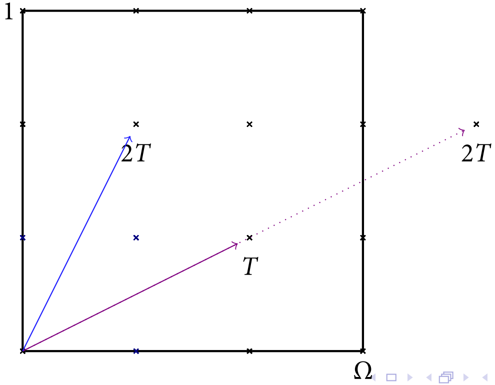
Computing all modular points

- Let $T_{e_1}, \cdots, T_{e_{2g}}$ be a basis for $B[m]$. 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 $B[m]$ with $g(2g+1)$ m-roots of unity, $g(2g-1)$ additions and m^{2g} chain additions.
- **Warning:** When applying our Vélu's formulas to an isotropic kernel, take into account the action of the commutator pairing:



Computing all modular points

- Let $T_{e_1}, \cdots, T_{e_{2g}}$ be a basis for $B[m]$. 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 $B[m]$ with $g(2g+1)$ m-roots of unity, $g(2g-1)$ additions and m^{2g} chain additions.
- **Warning:** When applying our Vélu's formulas to an isotropic kernel, take into account the action of the commutator pairing:



Perspectives

- Find equations for the modular space quotiented by the action of the symplectic group.
- Fast computation of the commutator pairing in level 2?

Perspectives

- Find equations for the modular space quotiented by the action of the symplectic group.
- Fast computation of the commutator pairing in level 2?