Computing isogenies of small degrees on Abelian Varieties

Jean-Charles Faugère[1], David Lubicz[2,3], **Damien Robert**[4]

[1]INRIA, Centre Paris-Rocquencourt, SALSA Project

[2]CÉLAR

[3]IRMAR, Université de Rennes 1

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

17 Avril 2009, Rennes

Outline

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

Outline

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 ($\Rightarrow \ell$-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).

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-addic or p-addic).
- 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-addic or p-addic).
- 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-addic or p-addic).
- 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-addic or p-addic).
- 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-addic or p-addic).
- 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

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

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

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

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

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

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

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

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

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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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: $\phi_2 = 50MB$.

$\Rightarrow$ Use the modulai 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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

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

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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

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

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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

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

Theta functions

- Every projective embedding comes from a polarization $\mathcal{L}$. A polarization $\mathcal{L}$ =
  - a factor of automorphy $e_L(x, y) = e^{2\pi i E_{\mathcal{L}}(x,y)}$ (where $E_{\mathcal{L}}$ is a symplectic form on $\mathbb{Z}^{2g}$)
  - a maximal isotropic decomposition of the kernel of the polarisation:

$$\begin{aligned} K(\mathcal{L}) &:= \left\{ z \in \mathbb{Q}^g + \Omega\mathbb{Q}^g | E_{\mathcal{L}}(z, \mathbb{Z}^g + \Omega\mathbb{Z}^g) \subset \mathbb{Z} \right\} \\ &= K(\mathcal{L})_1 \oplus K(\mathcal{L})_2 \end{aligned}$$

- The polarization $\mathcal{L}_\ell$ of level ℓ is given by analytic functions f satisfying:

$$\begin{aligned} f(z+n) &= f(z) \\ f(z+n\Omega) &= \exp(-\ell \cdot \pi i n' \Omega n - \ell \cdot 2\pi i n' z) f(z) \end{aligned}$$

Theta functions

- Every projective embedding comes from a polarization $\mathcal{L}$. A polarization $\mathcal{L}$ =
  - a factor of automorphy $e_L(x,y) = e^{2\pi i E_{\mathcal{L}}(x,y)}$ (where $E_{\mathcal{L}}$ is a symplectic form on $\mathbb{Z}^{2g}$)
  - a maximal isotropic decomposition of the kernel of the polarisation:

$$\begin{aligned} K(\mathcal{L}) &:= \left\{ z \in \mathbb{Q}^g + \Omega\mathbb{Q}^g | E_{\mathcal{L}}(z, \mathbb{Z}^g + \Omega\mathbb{Z}^g) \subset \mathbb{Z} \right\} \\ &= K(\mathcal{L})_1 \oplus K(\mathcal{L})_2 \end{aligned}$$

- The polarization $\mathcal{L}_\ell$ of level ℓ is given by analytic functions f satisfying:

$$\begin{aligned} f(z+n) &= f(z) \\ f(z+n\Omega) &= \exp(-\ell \cdot \pi i n'\Omega n - \ell \cdot 2\pi i n' z) f(z) \end{aligned}$$

Theta functions

- Every projective embedding comes from a polarization $\mathcal{L}$. A polarization $\mathcal{L}$ =
  - a factor of automorphy $e_L(x, y) = e^{2\pi i E_{\mathcal{L}}(x,y)}$ (where $E_{\mathcal{L}}$ is a symplectic form on $\mathbb{Z}^{2g}$)
  - a maximal isotropic decomposition of the kernel of the polarisation:

$$\begin{aligned} K(\mathcal{L}) &:= \left\{ z \in \mathbb{Q}^g + \Omega\mathbb{Q}^g | E_{\mathcal{L}}(z, \mathbb{Z}^g + \Omega\mathbb{Z}^g) \subset \mathbb{Z} \right\} \\ &= K(\mathcal{L})_1 \oplus K(\mathcal{L})_2 \end{aligned}$$

- The polarization $\mathcal{L}_\ell$ of level ℓ is given by analytic functions f satisfying:

$$\begin{aligned} f(z+n) &= f(z) \\ f(z+n\Omega) &= \exp(-\ell \cdot \pi i n' \Omega n - \ell \cdot 2\pi i n' z) f(z) \end{aligned}$$

Theta functions

- Every projective embedding comes from a polarization $\mathcal{L}$. A polarization $\mathcal{L}$ =
  - a factor of automorphy $e_L(x, y) = e^{2\pi i E_{\mathcal{L}}(x,y)}$ (where $E_{\mathcal{L}}$ is a symplectic form on $\mathbb{Z}^{2g}$)
  - a maximal isotropic decomposition of the kernel of the polarisation:

$$\begin{aligned} K(\mathcal{L}) &:= \left\{ z \in \mathbb{Q}^g + \Omega\mathbb{Q}^g | E_{\mathcal{L}}(z, \mathbb{Z}^g + \Omega\mathbb{Z}^g) \subset \mathbb{Z} \right\} \\ &= K(\mathcal{L})_1 \oplus K(\mathcal{L})_2 \end{aligned}$$

- The polarization $\mathcal{L}_\ell$ of level ℓ is given by analytic functions f satisfying:

$$\begin{aligned} f(z+n) &= f(z) \\ f(z+n\Omega) &= \exp(-\ell \cdot \pi i n'\Omega n - \ell \cdot 2\pi i n' z) f(z) \end{aligned}$$

Projective embeddings given by theta functions

Theorem

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

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

$$\left\{\theta\begin{bmatrix}a\\0\end{bmatrix}(\ell z,\ell\Omega)\right\}_{a\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g} \tag{2}$$

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

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

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

- *The point $(\theta_i(0))_{i\in\mathcal{Z}_\ell}$ is called the theta null point of the Theta structure Ω.*

Projective embeddings given by theta functions

Theorem

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

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

$$\left\{ \theta \begin{bmatrix} a \\ 0 \end{bmatrix} (\ell z, \ell\Omega) \right\}_{a \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g} \tag{2}$$

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

$$z \mapsto (\theta_i(z))_{i \in Z_\ell}$$

is a projective embedding $A \to \mathbb{P}_{\mathbb{C}}^{\ell^g - 1}$.
- *The point* $(\theta_i(0))_{i \in Z_\ell}$ *is called the theta null point of the Theta structure* Ω.

Projective embeddings given by theta functions

Theorem

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

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

$$\left\{\theta\begin{bmatrix}a\\0\end{bmatrix}(\ell z,\ell\Omega)\right\}_{a\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g} \tag{2}$$

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

$$z \mapsto (\theta_i(z))_{i\in Z_\ell}$$

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

- *The point $(\theta_i(0))_{i\in Z_\ell}$ is called the theta null point of the Theta structure Ω.*

The action of the Theta group

- $K(\mathcal{L}_\ell)$ is the subgroup of ℓ-torsion

$$A[\ell] = \left\{ \frac{i}{\ell} + \Omega \frac{j}{\ell} \right\} \; i, j \in \mathbb{Z}^g$$

- The action by translation is given by

$$(i,j).\theta_k(z) := \theta_k \left(z - \frac{i}{\ell} - \Omega \frac{j}{\ell} \right) \tag{3}$$
$$= e_{\mathcal{L}_\ell}(i+k, j) \theta_{i+k} \tag{4}$$

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

The action of the Theta group

- $K(\mathcal{L}_\ell)$ is the subgroup of ℓ-torsion

$$A[\ell] = \left\{ \frac{i}{\ell} + \Omega \frac{j}{\ell} \right\} \; i, j \in \mathbb{Z}^g$$

- The action by translation is given by

$$(i, j).\theta_k(z) := \theta_k \left(z - \frac{i}{\ell} - \Omega \frac{j}{\ell} \right) \tag{3}$$

$$= e_{\mathcal{L}_\ell}(i + k, j) \theta_{i+k} \tag{4}$$

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

Equations of the Abelian varieties

Theorem (Riemann Relations)

Let $(q_i)_{i \in \mathcal{Z}_\ell}$ be the theta null point. Then if $4 | \ell$, the homogeneous ideal of the Abelian variety is given by the Riemann Relations:

$$\sum_{t \in \mathcal{Z}_2} X_{x+t} X_{y+t} \sum_{t \in \mathcal{Z}_2} q_{u+t} q_{v+t} = \sum_{t \in \mathcal{Z}_2} X_{z-u+t} X_{z-v+t} \sum_{t \in \mathcal{Z}_2} q_{z-x+t} q_{z-y+t} \tag{5}$$

for every $x, y, u, v \in \mathcal{Z}_\ell$ such that $\exists z, x+y+u+v = -2z$.

Corollary

$$\sum_{t \in \mathcal{Z}_2} q_{x+t} q_{y+t} \sum_{t \in \mathcal{Z}_2} q_{u+t} q_{v+t} = \sum_{t \in \mathcal{Z}_2} q_{z-u+t} q_{z-y+t} \sum_{t \in \mathcal{Z}_2} q_{z-x+t} q_{z-v+t} \tag{6}$$

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

$$q_x = q_{-x}$$

Equations of the Abelian varieties

Theorem (Riemann Relations)

Let $(q_i)_{i \in Z_\ell}$ be the theta null point. Then if $4|\ell$, the homogeneous ideal of the Abelian variety is given by the Riemann Relations:

$$\sum_{t \in Z_2} X_{x+t} X_{y+t} \sum_{t \in Z_2} q_{u+t} q_{v+t} = \sum_{t \in Z_2} X_{z-u+t} X_{z-v+t} \sum_{t \in Z_2} q_{z-x+t} q_{z-y+t} \tag{5}$$

for every $x, y, u, v \in Z_\ell$ such that $\exists z, x + y + u + v = -2z$.

Corollary

$$\sum_{t \in Z_2} q_{x+t} q_{y+t} \sum_{t \in Z_2} q_{u+t} q_{v+t} = \sum_{t \in Z_2} q_{z-u+t} q_{z-y+t} \sum_{t \in Z_2} q_{z-x+t} q_{z-v+t} \tag{6}$$

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

$$q_x = q_{-x}$$

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

- *Let k be a field. Then every projective embedding is given by the Riemann Relations.*
  - *More precisely, for every projective embedding $\phi_{\mathcal{L}} : A_k \to \mathbb{P}_k^N$ of level ℓ, there is a unique basis of $\mathbb{P}_k^N$ such that the theta group acts as in (4).*
- *The locus of theta null points giving an Abelian Variety is an open subset $\mathcal{M}_\ell^0$ of $\mathcal{M}_\ell$.*

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

- *Let k be a field. Then every projective embedding is given by the Riemann Relations.*
  - *More precisely, for every projective embedding $\phi_{\mathcal{L}} : A_k \to \mathbb{P}^N_k$ of level ℓ, there is a unique basis of $\mathbb{P}^N_k$ such that the theta group acts as in (4).*
- *The locus of theta null points giving an Abelian Variety is an open subset $\mathcal{M}^0_\ell$ of $\mathcal{M}_\ell$.*

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

- *Let k be a field. Then every projective embedding is given by the Riemann Relations.*
  - *More precisely, for every projective embedding $\phi_{\mathcal{L}} : A_k \to \mathbb{P}^N_k$ of level ℓ, there is a unique basis of $\mathbb{P}^N_k$ such that the theta group acts as in (4).*
- *The locus of theta null points giving an Abelian Variety is an open subset $\mathcal{M}^0_\ell$ of $\mathcal{M}_\ell$.*

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

- *Let k be a field. Then every projective embedding is given by the Riemann Relations.*
  - *More precisely, for every projective embedding $\phi_{\mathcal{L}} : A_k \to \mathbb{P}_k^N$ of level ℓ, there is a unique basis of $\mathbb{P}_k^N$ such that the theta group acts as in (4).*
- *The locus of theta null points giving an Abelian Variety is an open subset $\mathcal{M}_\ell^0$ of $\mathcal{M}_\ell$.*

Remark

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

Mumford: On equations defining Abelian varieties

Theorem (car $k \nmid \ell$)

- *Let k be a field. Then every projective embedding is given by the Riemann Relations.*
  - *More precisely, for every projective embedding $\phi_{\mathcal{L}} : A_k \to \mathbb{P}_k^N$ of level ℓ, there is a unique basis of $\mathbb{P}_k^N$ such that the theta group acts as in (4).*
- *The locus of theta null points giving an Abelian Variety is an open subset $\mathcal{M}_\ell^0$ of $\mathcal{M}_\ell$.*

Remark

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

The isogeny theorem

Theorem

Let $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ be an Abelian variety with a theta structure of level ℓ. Suppose that $\ell = kn$ and let $K = \frac{1}{k}\Omega\mathbb{Z}^g$, and $\pi : A \to B = A/K$ the corresponding isogeny.
There is an induced theta structure of level n on B such that

$$\theta_i^B = \theta_{\phi(i)}^A \tag{7}$$

where $\phi : \mathcal{Z}_n \to \mathcal{Z}_\ell$ is the canonical inclusion $x \mapsto k \cdot x$.

Proof.

$$\theta_i^B(z) = \theta\begin{bmatrix} 0 \\ i/n \end{bmatrix}\left(z, \frac{\Omega}{k}/n\right) = \theta\begin{bmatrix} 0 \\ ki/\ell \end{bmatrix}(z, \Omega/\ell) = \theta_{k\cdot i}^A(z)$$

□

The isogeny theorem

Theorem

Let $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ be an Abelian variety with a theta structure of level ℓ. Suppose that $\ell = kn$ and let $K = \frac{1}{k}\Omega\mathbb{Z}^g$, and $\pi : A \to B = A/K$ the corresponding isogeny.
There is an induced theta structure of level n on B such that

$$\theta_i^B = \theta_{\phi(i)}^A \tag{7}$$

where $\phi : \mathcal{Z}_n \to \mathcal{Z}_\ell$ is the canonical inclusion $x \mapsto k \cdot x$.

Proof.

$$\theta_i^B(z) = \theta\begin{bmatrix} 0 \\ i/n \end{bmatrix}\left(z, \frac{\Omega}{k}/n\right) = \theta\begin{bmatrix} 0 \\ ki/\ell \end{bmatrix}(z, \Omega/\ell) = \theta_{k\cdot i}^A(z)$$

□

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Summary

Given a valid theta null point $(a_i)_{i \in \mathcal{Z}_\ell}$, we have

- The equations of the Abelian variety A.
- A symplectic basis $A[\ell] \simeq \mathcal{Z}_\ell \times \hat{\mathcal{Z}}_\ell$.
- The action of points of ℓ-torsion.
- An isogeny $A \to B = A/K_2$ (where K_2 is the subgroup $\hat{\mathcal{Z}}_k \subset \hat{\mathcal{Z}}_\ell$).

Remark

- The level ℓ of an Abelian variety A with a polarization is fixed. ($\ell = 4$ if A is the Jacobian of an hyperelliptic curve).
- The only way to change the level is given by the isogeny theorem.

Outline

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in Z_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- By the isogeny theorem, to every valid theta null point $(a_i)_{i \in Z_{\ell n}} \in V_B^0(k)$ corresponds a ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in \mathcal{Z}_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- 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 ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in Z_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by

$$\{q_{\phi(i)} = b_i\}$$

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

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in \mathcal{Z}_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- 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 ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in \mathcal{Z}_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- 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 ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i \in \mathcal{Z}_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- 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 ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

Definition

- Let B be an Abelian variety with a theta structure of level n, and $(b_i)_{i\in \mathcal{Z}_n}$ the corresponding theta null point. We note V_B the subvariety of $\mathcal{M}_{\ell n}$ defined by
$$\{q_{\phi(i)} = b_i\}$$
- 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 ℓ-isogeny $\pi : A \to B$.

- The algorithm is as follows:
  - Compute the solutions $V_B(k)$.
  - Identify the valid theta null points.
  - Compute the dual isogeny $\tilde{\pi} : B \to A$.
- For the examples, we will use $g = 1$, $n = 4$ and $\ell = 3$.

Program

3. Computing isogenies
   - The structure of the system
   - Computing the solutions
   - Computing the dual isogeny

The kernel of the dual isogeny

- Let $(a_0, \cdots, a_{11})$ be a valid solution corresponding to an isogeny $\pi : A \to B$. We have

$$\pi(\theta_i^A(x)_{i \in \mathcal{Z}_{12}}) = (\theta_0^A(x), \theta_3^A(x), \theta_6^A(x), \theta_9^A(x))$$
$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- The kernel K of π is

$$\{(\zeta^{ki} a_i)_{i \in \mathcal{Z}_{12}}\}_{k \in \mathcal{Z}_3} \qquad \zeta^3 = 1$$

- The kernel $\tilde{K}$ of the dual isogeny is given by the projection of the dual of K:

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

The kernel of the dual isogeny

- Let $(a_0, \cdots, a_{11})$ be a valid solution corresponding to an isogeny $\pi : A \to B$. We have

$$\pi(\theta_i^A(x)_{i\in\mathcal{Z}_{12}}) = (\theta_0^A(x), \theta_3^A(x), \theta_6^A(x), \theta_9^A(x))$$
$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- The kernel K of π is

$$\{(\zeta^{ki} a_i)_{i\in\mathcal{Z}_{12}}\}_{k\in\mathcal{Z}_3} \qquad \zeta^3 = 1$$

- The kernel $\tilde{K}$ of the dual isogeny is given by the projection of the dual of K:

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

The kernel of the dual isogeny

- Let $(a_0, \cdots, a_{11})$ be a valid solution corresponding to an isogeny $\pi : A \to B$. We have

$$\pi(\theta_i^A(x)_{i\in\mathcal{Z}_{12}}) = (\theta_0^A(x), \theta_3^A(x), \theta_6^A(x), \theta_9^A(x))$$
$$a_0 = b_0, a_3 = b_1, a_6 = b_2, a_9 = b_3$$

- The kernel K of π is

$$\{(\zeta^{ki} a_i)_{i\in\mathcal{Z}_{12}}\}_{k\in\mathcal{Z}_3} \qquad \zeta^3 = 1$$

- The kernel $\tilde{K}$ of the dual isogeny is given by the projection of the dual of K:
$$\tilde{K} = \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\}$$

The valid solutions

Lemma

Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a solution. Let $\phi : \mathcal{Z}_\ell \times \mathcal{Z}_n \to \mathcal{Z}_{\ell n}, (i, j) \mapsto in + j\ell$. If $i \in \mathcal{Z}_\ell$, we define

$$P_i = (a_{\phi(i,j)})_{j \in \mathcal{Z}_n}$$

Then the points $\{P_i\}_{i \in \mathcal{Z}_\ell}$ that are well defined form a subgroup of the points of ℓ-torsion in B.

Theorem ($n \wedge \ell = 1$)

Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a solution, and $\tilde{K} = \{P_i\}_{i \in \mathcal{Z}_\ell}$ the associated subgroup of ℓ-torsion. Then $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ is a valid solution if and only if $\tilde{K}$ is a maximal subgroup of rank g.

The valid solutions

Lemma

Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a solution. Let $\phi : \mathcal{Z}_\ell \times \mathcal{Z}_n \to \mathcal{Z}_{\ell n}, (i,j) \mapsto in + j\ell$. If $i \in \mathcal{Z}_\ell$, we define

$$P_i = (a_{\phi(i,j)})_{j \in \mathcal{Z}_n}$$

Then the points $\{P_i\}_{i \in \mathcal{Z}_\ell}$ that are well defined form a subgroup of the points of ℓ-torsion in B.

Theorem ($n \wedge \ell = 1$)

Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a solution, and $\tilde{K} = \{P_i\}_{i \in \mathcal{Z}_\ell}$ the associated subgroup of ℓ-torsion. Then $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ is a valid solution if and only if $\tilde{K}$ is a maximal subgroup of rank g.

The automorphisms of the theta group

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a valid solution. The actions of the automorphisms of the theta group compatible with the theta structure of B are generated by

$$(a_u)_{u \in \mathcal{Z}_{\ell n}} \mapsto (a_{\psi_1(u)})_{u \in \mathcal{Z}_{\ell n}} \tag{8}$$

$$(a_u)_{u \in \mathcal{Z}_{\ell n}} \mapsto (e(\psi_2(u), u).a_u)_{u \in \mathcal{Z}_{\ell n}} \tag{9}$$

Where ψ_1 is an automorphism of $\mathcal{Z}_{\ell n}$ fixing $\mathcal{Z}_n$ and ψ_2 is a morphism $\mathcal{Z}_{\ell n} \to \mathcal{Z}_\ell \subset \mathcal{Z}_{\ell n}$.

Example

If $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$ is a valid solution corresponding to an Abelian variety A, the solutions isomorphic to A are given by

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

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

The automorphisms of the theta group

- Let $(a_i)_{i\in \mathcal{Z}_{\ell n}}$ be a valid solution. The actions of the automorphisms of the theta group compatible with the theta structure of B are generated by

$$(a_u)_{u\in \mathcal{Z}_{\ell n}} \mapsto (a_{\psi_1(u)})_{u\in \mathcal{Z}_{\ell n}} \tag{8}$$

$$(a_u)_{u\in \mathcal{Z}_{\ell n}} \mapsto (e(\psi_2(u),u).a_u)_{u\in \mathcal{Z}_{\ell n}} \tag{9}$$

Where ψ_1 is an automorphism of $\mathcal{Z}_{\ell n}$ fixing $\mathcal{Z}_n$ and ψ_2 is a morphism $\mathcal{Z}_{\ell n} \to \mathcal{Z}_\ell \subset \mathcal{Z}_{\ell n}$.

Example

If $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$ is a valid solution corresponding to an Abelian variety A, the solutions isomorphic to A are given by

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

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

The automorphisms of the theta group

- Let $(a_i)_{i \in \mathcal{Z}_{\ell n}}$ be a valid solution. The actions of the automorphisms of the theta group compatible with the theta structure of B are generated by

$$(a_u)_{u \in \mathcal{Z}_{\ell n}} \mapsto (a_{\psi_1(u)})_{u \in \mathcal{Z}_{\ell n}} \tag{8}$$

$$(a_u)_{u \in \mathcal{Z}_{\ell n}} \mapsto (e(\psi_2(u), u).a_u)_{u \in \mathcal{Z}_{\ell n}} \tag{9}$$

Where ψ_1 is an automorphism of $\mathcal{Z}_{\ell n}$ fixing $\mathcal{Z}_n$ and ψ_2 is a morphism $\mathcal{Z}_{\ell n} \to \mathcal{Z}_{\ell} \subset \mathcal{Z}_{\ell n}$.

Example

If $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$ is a valid solution corresponding to an Abelian variety A, the solutions isomorphic to A are given by

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

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

Proof of the theorem (Outline)

Proof.

- Every solutions giving the same set of associated points $\{P_i\}_{i \in \mathcal{Z}_\ell}$ differ by an action of type (8) or (9)
- Let $\tilde{K} = \{P_i\}_{i \in \mathcal{Z}_\ell}$ be the associated subgroup of rank g in B. Let $A = B/\tilde{K}$, and $\pi : A \to B$ be the dual isogeny. We construct a theta structure on A such that π is the associated isogeny.

□

Corollary

$$\#V_B^0(\overline{k}) \simeq \ell^g \text{ (number of isogenies)} \times \ell^{2g} \text{ (cardinal of each orbit)}$$

Proof of the theorem (Outline)

Proof.

- Every solutions giving the same set of associated points $\{P_i\}_{i \in \mathcal{Z}_\ell}$ differ by an action of type (8) or (9).
- Let $\tilde{K} = \{P_i\}_{i \in \mathcal{Z}_\ell}$ be the associated subgroup of rank g in B. Let $A = B/\tilde{K}$, and $\pi : A \to B$ be the dual isogeny. We construct a theta structure on A such that π is the associated isogeny.

$\square$

Corollary

$$\#V_B^0(\overline{k}) \simeq \ell^g \text{ (number of isogenies)} \times \ell^{2g} \text{ (cardinal of each orbit)}$$

Proof of the theorem (Outline)

Proof.

- Every solutions giving the same set of associated points $\{P_i\}_{i \in Z_\ell}$ differ by an action of type (8) or (9)
- Let $\tilde{K} = \{P_i\}_{i \in Z_\ell}$ be the associated subgroup of rank g in B. Let $A = B/\tilde{K}$, and $\pi : A \to B$ be the dual isogeny. We construct a theta structure on A such that π is the associated isogeny.

□

Corollary

$$\# V_B^0(\overline{k}) \simeq \ell^g \text{ (number of isogenies)} \times \ell^{2g} \text{ (cardinal of each orbit)}$$

An example

Example

The theta null point $(1:1:12:1) \in \mathcal{M}_4(\mathbb{F}_{79})$ corresponds to the elliptic curve $E: y^2 = x^3 + 11.x + 47$.

- We have the following valid solutions (v is a primitive root of degree 3):

$$(v^{490931}:1:46:v^{490931}:37:54:v^{54782}:54:37:v^{490931}:46:1)$$
$$(v^{476182}:1:68:v^{476182}:67:10:v^{40033}:10:67:v^{476182}:68:1)$$
$$(v^{465647}:1:3:v^{465647}:40:16:v^{29498}:16:40:v^{465647}:3:1)$$
$$(v^{450898}:1:33:v^{450898}:69:24:v^{14749}:24:69:v^{450898}:33:1)$$

- And the following degenerate solutions:

$$(1:1:12:1:1:1:12:1:1:1:12:1)$$
$$(1:0:0:1:0:0:12:0:0:1:0:0)$$

An example

Example

The theta null point $(1:1:12:1) \in \mathcal{M}_4(\mathbb{F}_{79})$ corresponds to the elliptic curve $E: y^2 = x^3 + 11.x + 47$.

- We have the following valid solutions (v is a primitive root of degree 3):

$$(v^{490931}:1:46:v^{490931}:37:54:v^{54782}:54:37:v^{490931}:46:1)$$
$$(v^{476182}:1:68:v^{476182}:67:10:v^{40033}:10:67:v^{476182}:68:1)$$
$$(v^{465647}:1:3:v^{465647}:40:16:v^{29498}:16:40:v^{465647}:3:1)$$
$$(v^{450898}:1:33:v^{450898}:69:24:v^{14749}:24:69:v^{450898}:33:1)$$

- And the following degenerate solutions:

$$(1:1:12:1:1:1:12:1:1:1:12:1)$$
$$(1:0:0:1:0:0:12:0:0:1:0:0)$$

An example

Example

The theta null point $(1:1:12:1) \in \mathcal{M}_4(\mathbb{F}_{79})$ corresponds to the elliptic curve $E: y^2 = x^3 + 11.x + 47$.

- We have the following valid solutions (v is a primitive root of degree 3):

$$(v^{490931} : 1 : 46 : v^{490931} : 37 : 54 : v^{54782} : 54 : 37 : v^{490931} : 46 : 1)$$
$$(v^{476182} : 1 : 68 : v^{476182} : 67 : 10 : v^{40033} : 10 : 67 : v^{476182} : 68 : 1)$$
$$(v^{465647} : 1 : 3 : v^{465647} : 40 : 16 : v^{29498} : 16 : 40 : v^{465647} : 3 : 1)$$
$$(v^{450898} : 1 : 33 : v^{450898} : 69 : 24 : v^{14749} : 24 : 69 : v^{450898} : 33 : 1)$$

- And the following degenerate solutions:

$$(1:1:12:1:1:1:12:1:1:1:12:1)$$
$$(1:0:0:1:0:0:12:0:0:1:0:0)$$

Program

3. Computing isogenies
   - The structure of the system
   - Computing the solutions
   - Computing the dual isogeny

A specialized Groebner algorithm

We use the fact that $J = I \bigcap k[a_4, a_7, a_{10}, a_1]$ contains polynomial of low degree as follow:

Step 1 Compute a truncated Groebner basis (for an elimination order) to obtain a zero dimensional ideal J_1 contained in J.

Step 2 Compute the coordinates a_4, a_7, a_{10}, a_1:

$$\mathrm{Var}(J_1)(\overline{k}) \supset \left\{(a_4, a_7, a_{10}, a_1) : a \in V_B(\overline{k})\right\}$$

Step 3 Compute (recursively) the other coordinates (a_8, a_{11}, a_2, a_5).

A specialized Groebner algorithm

We use the fact that $J = I \bigcap k[a_4, a_7, a_{10}, a_1]$ contains polynomial of low degree as follow:

Step 1 Compute a truncated Groebner basis (for an elimination order) to obtain a zero dimensional ideal J_1 contained in J.

Step 2 Compute the coordinates a_4, a_7, a_{10}, a_1:

$$\mathrm{Var}(J_1)(\overline{k}) \supset \left\{ (a_4, a_7, a_{10}, a_1) : a \in V_B(\overline{k}) \right\}$$

Step 3 Compute (recursively) the other coordinates (a_8, a_{11}, a_2, a_5).

A specialized Groebner algorithm

We use the fact that $J = I \bigcap k[a_4, a_7, a_{10}, a_1]$ contains polynomial of low degree as follow:

Step 1 Compute a truncated Groebner basis (for an elimination order) to obtain a zero dimensional ideal J_1 contained in J.

Step 2 Compute the coordinates a_4, a_7, a_{10}, a_1:

$$\mathrm{Var}(J_1)(\overline{k}) \supset \left\{(a_4, a_7, a_{10}, a_1) : a \in V_B(\overline{k})\right\}$$

Step 3 Compute (recursively) the other coordinates (a_8, a_{11}, a_2, a_5).

A specialized Groebner algorithm

We use the fact that $J = I \bigcap k[a_4, a_7, a_{10}, a_1]$ contains polynomial of low degree as follow:

Step 1 Compute a truncated Groebner basis (for an elimination order) to obtain a zero dimensional ideal J_1 contained in J.

Step 2 Compute the coordinates a_4, a_7, a_{10}, a_1:

$$\mathrm{Var}(J_1)(\overline{k}) \supset \left\{(a_4, a_7, a_{10}, a_1) : a \in V_B(\overline{k})\right\}$$

Step 3 Compute (recursively) the other coordinates (a_8, a_{11}, a_2, a_5).

Program

3. Computing isogenies
   - The structure of the system
   - Computing the solutions
   - Computing the dual isogeny

The dual isogeny

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

  Let $\pi : A \to B$ be the isogeny associated to $(a_0, \cdots, a_{11})$. Let $y = (y_0, y_1, y_2, y_3) \in B$. Let $x = (x_0, \cdots, x_{11})$ be one of the 3 antecedents. Then
  $$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1)$, P_1 is a point of 3-torsion in B. We have:
  $$y = (x_0, x_3, x_6, x_9)$$
  $$y + P_1 = (x_4, x_7, x_{10}, x_1)$$
  $$y + 2P_1 = (x_8, x_{11}, x_2, x_5)$$
  So x can be recovered from y, $y + P_1$, $y + 2P_1$ up to three projective factors $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$.

The dual isogeny

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

  Let $\pi : A \to B$ be the isogeny associated to $(a_0, \cdots, a_{11})$. Let $y = (y_0, y_1, y_2, y_3) \in B$. Let $x = (x_0, \cdots, x_{11})$ be one of the 3 antecedents. Then
  $$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1)$, P_1 is a point of 3-torsion in B. We have:

$$y = (x_0, x_3, x_6, x_9)$$
$$y + P_1 = (x_4, x_7, x_{10}, x_1)$$
$$y + 2P_1 = (x_8, x_{11}, x_2, x_5)$$

So x can be recovered from y, $y + P_1$, $y + 2P_1$ up to three projective factors $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$.

The dual isogeny

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

  Let $\pi : A \to B$ be the isogeny associated to $(a_0, \cdots, a_{11})$. Let $y = (y_0, y_1, y_2, y_3) \in B$. Let $x = (x_0, \cdots, x_{11})$ be one of the 3 antecedents. Then
  $$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1)$, P_1 is a point of 3-torsion in B. We have:

$$y = (x_0, x_3, x_6, x_9)$$
$$y + P_1 = (x_4, x_7, x_{10}, x_1)$$
$$y + 2P_1 = (x_8, x_{11}, x_2, x_5)$$

So x can be recovered from y, $y + P_1$, $y + 2P_1$ up to three projective factors $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$.

The dual isogeny

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

  Let $\pi : A \to B$ be the isogeny associated to $(a_0, \cdots, a_{11})$. Let $y = (y_0, y_1, y_2, y_3) \in B$. Let $x = (x_0, \cdots, x_{11})$ be one of the 3 antecedents. Then
  $$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1)$, P_1 is a point of 3-torsion in B. We have:
  $$y = (x_0, x_3, x_6, x_9)$$
  $$y + P_1 = (x_4, x_7, x_{10}, x_1)$$
  $$y + 2P_1 = (x_8, x_{11}, x_2, x_5)$$
  So x can be recovered from y, $y + P_1$, $y + 2P_1$ up to three projective factors $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$.

The dual isogeny

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

  Let $\pi : A \to B$ be the isogeny associated to $(a_0, \cdots, a_{11})$. Let $y = (y_0, y_1, y_2, y_3) \in B$. Let $x = (x_0, \cdots, x_{11})$ be one of the 3 antecedents. Then
  $$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1)$, P_1 is a point of 3-torsion in B. We have:
  $$y = (x_0, x_3, x_6, x_9)$$
  $$y + P_1 = (x_4, x_7, x_{10}, x_1)$$
  $$y + 2P_1 = (x_8, x_{11}, x_2, x_5)$$

  So x can be recovered from y, $y + P_1$, $y + 2P_1$ up to three projective factors $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$.

The addition formula

Theorem (Addition formula)

$$2^g \theta \begin{bmatrix} a' \\ e' \end{bmatrix} (x+y) \theta \begin{bmatrix} b' \\ f' \end{bmatrix} (x-y) \theta \begin{bmatrix} c' \\ g' \end{bmatrix} (0) \theta \begin{bmatrix} d' \\ h' \end{bmatrix} (0) =$$

$$\sum_{\alpha,\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{2\pi i \beta'(a+b+c+d)} \theta \begin{bmatrix} a+\alpha \\ e+\beta \end{bmatrix} (x) \theta \begin{bmatrix} b+\alpha \\ f+\beta \end{bmatrix} (x) \theta \begin{bmatrix} c+\alpha \\ g+\beta \end{bmatrix} (y) \theta \begin{bmatrix} d+\alpha \\ h+\beta \end{bmatrix} (y)$$

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

$$a,b,c,d,e,f,g,h \in \tfrac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$$

$$(a',b',c',d') = A(a,b,c,d), (e',f',g',h') = A(e,f,g,h)$$

Computing the projective factors

- Using the addition formulas, we have $\lambda_{2P_1} = \lambda_{P_1}^2$.
- Since $y + 3P_1 = y$, we obtain a formula

$$\lambda_{P_1}^3 = \alpha$$

hence we can find the three antecedents.
- In fact when computing $3 \cdot x$, the projective factors become $\lambda_0^3, \lambda_{P_1}^3, \lambda_{2P_1}^3$ so we don't need to extract roots.
- *Vélu's like formulas:* If we know the kernel $\tilde{K}$ of the isogeny, we can use the same methods to compute the valid theta null points in $\mathcal{M}_{\ell n}(k)$, by determining the $g(g+1)/2$ indeterminates λ_{ij}.

Computing the projective factors

- Using the addition formulas, we have $\lambda_{2P_1} = \lambda_{P_1}^2$.
- Since $y + 3P_1 = y$, we obtain a formula

$$\lambda_{P_1}^3 = \alpha$$

  hence we can find the three antecedents.
- In fact when computing $3 \cdot x$, the projective factors become $\lambda_0^3, \lambda_{P_1}^3, \lambda_{2P_1}^3$ so we don't need to extract roots.
- *Vélu's like formulas:* If we know the kernel $\tilde{K}$ of the isogeny, we can use the same methods to compute the valid theta null points in $\mathcal{M}_{\ell n}(k)$, by determining the $g(g+1)/2$ indeterminates λ_{ij}.

Computing the projective factors

- Using the addition formulas, we have $\lambda_{2P_1} = \lambda_{P_1}^2$.
- Since $y + 3P_1 = y$, we obtain a formula

$$\lambda_{P_1}^3 = \alpha$$

  hence we can find the three antecedents.
- In fact when computing $3 \cdot x$, the projective factors become $\lambda_0^3, \lambda_{P_1}^3, \lambda_{2P_1}^3$ so we don't need to extract roots.
- *Vélu's like formulas:* If we know the kernel $\tilde{K}$ of the isogeny, we can use the same methods to compute the valid theta null points in $\mathcal{M}_{\ell n}(k)$, by determining the $g(g+1)/2$ indeterminates λ_{ij}.

Computing the projective factors

- Using the addition formulas, we have $\lambda_{2P_1} = \lambda_{P_1}^2$.
- Since $y + 3P_1 = y$, we obtain a formula

$$\lambda_{P_1}^3 = \alpha$$

hence we can find the three antecedents.
- In fact when computing $3 \cdot x$, the projective factors become $\lambda_0^3, \lambda_{P_1}^3, \lambda_{2P_1}^3$ so we don't need to extract roots.
- *Vélu's like formulas:* If we know the kernel $\tilde{K}$ of the isogeny, we can use the same methods to compute the valid theta null points in $\mathcal{M}_{\ell n}(k)$, by determining the $g(g+1)/2$ indeterminates λ_{ij}.

Perspective

- We have an algorithm to compute isogenies! In practice, only for small degrees and low genus.
- The blocking point of the algorithm is the lifting of the theta null point (even with the improved Groebner basis algorithm).
- We have seen that we have a nice action on the solutions, and we are only interested in equivalence classes. Can we use this action to speed up the lifting part?
- Can we use Theta functions to compute pairings?

Perspective

- We have an algorithm to compute isogenies! In practice, only for small degrees and low genus.
- The blocking point of the algorithm is the lifting of the theta null point (even with the improved Groebner basis algorithm).
- We have seen that we have a nice action on the solutions, and we are only interested in equivalence classes. Can we use this action to speed up the lifting part?
- Can we use Theta functions to compute pairings?

Perspective

- We have an algorithm to compute isogenies! In practice, only for small degrees and low genus.
- The blocking point of the algorithm is the lifting of the theta null point (even with the improved Groebner basis algorithm).
- We have seen that we have a nice action on the solutions, and we are only interested in equivalence classes. Can we use this action to speed up the lifting part?
- Can we use Theta functions to compute pairings?

Perspective

- We have an algorithm to compute isogenies! In practice, only for small degrees and low genus.
- The blocking point of the algorithm is the lifting of the theta null point (even with the improved Groebner basis algorithm).
- We have seen that we have a nice action on the solutions, and we are only interested in equivalence classes. Can we use this action to speed up the lifting part?
- Can we use Theta functions to compute pairings?