Computing isogenies of small degrees on Abelian Varieties

Jean-Charles Faugère¹, David Lubicz²,³, Damien Robert⁴

¹INRIA, Centre Paris-Rocquencourt, SALSA Project
²CÉLAR
³IRMAR, Université de Rennes 1
⁴Nancy Université, CNRS, Inria Nancy Grand Est

7 July 2009, Journées Arithmétiques
**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 $\Rightarrow$ can be used for public key cryptography (Discrete Logarithm Problem).
- *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 $\Rightarrow$ can be used for public key cryptography (Discrete Logarithm Problem).
- *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** ⇒ can be used for public key cryptography (Discrete Logarithm Problem).

*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 $\Rightarrow$ can be used for public key cryptography (Discrete Logarithm Problem).
- *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 ⇔ Finite subgroups.

\[(f : A \to B) \mapsto \text{Ker } f\]
\[(A \to A/H) \leftrightarrow H\]

Example: Multiplication by \(\ell\) (\(\Rightarrow \ell\)-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** ⇔ Finite subgroups.

\[(f : A \to B) \mapsto \text{Ker } f\]
\[(A \to A/H) \leftrightarrow H\]

- *Example*: Multiplication by \(\ell\) (⇒ \(\ell\)-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 ↔ Finite subgroups.

\[(f : A \to B) \mapsto \text{Ker } f\]
\[(A \to A/H) \leftrightarrow H\]

*Example:* Multiplication by \(\ell\) (\(\Rightarrow \ell\)-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 ↔ Finite subgroups.

\[(f : A \to B) \mapsto \text{Ker } f\]
\[(A \to A/H) \leftrightarrow H\]

- Example: Multiplication by $\ell$ (⇒ $\ell$-torsion), Frobenius (non separable).
Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-addic or $p$-addic).
- Compute the class field polynomials.
- Compute the modular polynomials.
- Determine $\text{End}(A)$. 
Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-addic or $p$-addic).
- Compute the class field polynomials.
- Compute the modular polynomials.
- Determine $\text{End}(A)$. 
Cryptography usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-addic or $p$-addic).
- Compute the class field polynomials.
- Compute the modular polynomials.
- Determine $\text{End}(A)$. 
Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-adic or $p$-adic).
- Compute the class field polynomials.
- Compute the modular polynomials.
- Determine $\text{End}(A)$. 
Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-adic or $p$-adic).
- Compute the class field polynomials.
- Compute the modular polynomials.
- Determine $\text{End}(A)$.
**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

  $$
  v_0_E(x) = -3 \quad v_P(x) \geq 0 \quad \text{if } P \neq 0_E
  $$

  $$
  v_0_E(y) = -2 \quad v_P(y) \geq 0 \quad \text{if } P \neq 0_E
  $$

  $$
  y^2 / x^3(O_E) = 1
  $$

- 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

  $$\nu_{0_E}(x) = -3 \quad \nu_P(x) \geq 0 \quad \text{if} \ P \neq 0_E$$

  $$\nu_{0_E}(y) = -2 \quad \nu_P(y) \geq 0 \quad \text{if} \ P \neq 0_E$$

  $$y^2/x^3(O_E) = 1$$

- 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

  \[
  \nu_0(x) = -3 \quad \nu_P(x) \geq 0 \quad \text{if } P \neq 0_E
  \]
  \[
  \nu_0(y) = -2 \quad \nu_P(y) \geq 0 \quad \text{if } P \neq 0_E
  \]
  \[
  y^2/x^3(O_E) = 1
  \]

- 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: $\varphi_2 = 50MB$.

⇒ Use the moduli space given by theta functions.
⇒ 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: \( \varphi_2 = 50MB \).

⇒ Use the moduli space given by theta functions.
⇒ 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: \( \varphi_2 = 50MB \).

⇒ Use the moduli space given by theta functions.
⇒ 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 \( \varphi_n(j(E), .) \) \( \iff \) elliptic curves \( n \)-isogeneous to \( E \).
- In genus 2, modular polynomials use **Igusa invariants**. The height explodes: \( \varphi_2 = 50MB \).

⇒ Use the moduli space given by theta functions.
⇒ 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 $\varphi_n(j(E), .)$ $\iff$ elliptic curves $n$-isogeneous to $E$.

- In genus 2, modular polynomials use Igusa invariants. The height explodes: $\varphi_2 = 50MB$.

⇒ Use the moduli space given by **theta functions**.

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

⇒ Use the moduli space given by theta functions.
⇒ Fix the form of the isogeny and look for coordinates compatible with the isogeny.
Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.

- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on $\mathbb{C}^g$.

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

\[
\vartheta\left[\begin{array}{c} a \\ b \end{array}\right](z, \Omega) = e^{\pi ia'\Omega a + 2\pi ia'(z+b)} \vartheta(z + \Omega a + b, \Omega) \quad a, b \in \mathbb{Q}^g
\]

- The quasi-periodicity is given by

\[
\vartheta\left[\begin{array}{c} a \\ b \end{array}\right](z + m + \Omega n, \Omega) = e^{2\pi i(a'm - b'n) - \pi in' \Omega n - 2\pi in'z} \vartheta\left[\begin{array}{c} a \\ b \end{array}\right](z, \Omega)
\]
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 $\mathbb{C}^g$.

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

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

- The quasi-periodicity is given by

$$\theta \left[ \begin{array}{c} a \\ b \end{array} \right] (z + m + \Omega n, \Omega) = e^{2\pi i (a' m - b' n) - \pi i \Omega n - 2\pi i n' z} \theta \left[ \begin{array}{c} a \\ b \end{array} \right] (z, \Omega)$$
Complex abelian varieties

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

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

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

- The **quasi-periodicity** is given by

\[
\vartheta\left[\begin{array}{c} a \\ b \end{array}\right](z + m + \Omega n, \Omega) = e^{2\pi i (a'm - b'n) - \pi i \Omega n - 2\pi i n' z} \vartheta\left[\begin{array}{c} a \\ b \end{array}\right](z, \Omega)
\]
Theorem

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

\begin{align*}
  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{align*}

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

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

Let $\mathcal{Z}_\ell = \mathbb{Z}^g / \ell \mathbb{Z}^g$. If $i \in \mathcal{Z}_\ell$ we define $\vartheta_i = \vartheta \left[ \begin{array}{c} 0 \\ i/\ell \end{array} \right](., \Omega/\ell)$. If $l \geq 3$ then

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

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

Projective embeddings given by theta functions
Projective embeddings given by theta functions

Theorem

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

\[
\begin{align*}
    f(z + n) &= f(z) \\
    f(z + n\Omega) &= \exp(-\ell \cdot \pi i n' \Omega n - \ell \cdot 2\pi i n' z) f(z)
\end{align*}
\]

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

\[
\left\{ \Theta \begin{bmatrix} 0 \\ b \end{bmatrix}(z, \Omega/\ell) \right\}_{b \in \frac{1}{\ell} \mathbb{Z}_g / \mathbb{Z}_g}
\]

- 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 $A \to \mathbb{P}^{\ell g - 1}_C$. 
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

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

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

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

  is a projective embedding $A \to \mathbb{P}_{\mathbb{C}}^{|\mathbb{Z}_\ell| - 1}$. 
The action of the Theta group

- The point \((a_i)_{i \in \mathbb{Z}_\ell} := (\vartheta_i(0))_{i \in \mathbb{Z}_\ell}\) is called the theta null point of level \(\ell\) of the Abelian Variety \(A := \mathbb{C}^g/(\mathbb{Z}^g + \Omega \mathbb{Z}^g)\).

- \((a_i)_{i \in \mathbb{Z}_\ell}\) determines the equations of the projective embedding of \(A\) of level \(\ell\).

- The symplectic basis \(\mathbb{Z}^g \oplus \Omega \mathbb{Z}^g\) induce a decomposition into isotropic subgroups for the commutator pairing:

\[
A[\ell] = A[\ell]_1 \oplus A[\ell]_2 = \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g \oplus \frac{1}{\ell} \Omega \mathbb{Z}^g / \Omega \mathbb{Z}^g
\]

This decomposition can be recovered by \((a_i)_{i \in \mathbb{Z}_\ell}\).

- The action by translation is given by

\[
\vartheta_k \left( z - \frac{i}{\ell} - \Omega \frac{j}{\ell} \right) = e_{L_\ell}(i + k, j) \vartheta_{i+k}
\]

where \(e_{L_\ell}(x, y) = e^{2\pi i / \ell \cdot x' y}\) is the commutator pairing.
The action of the Theta group

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

\[
A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \\
= \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g \oplus \frac{1}{\ell} \Omega\mathbb{Z}^g / \Omega\mathbb{Z}^g
\]

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

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

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

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

\[
A[\ell] = A[\ell]_1 \oplus A[\ell]_2 = \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g \oplus \frac{1}{\ell} \Omega \mathbb{Z}^g / \Omega \mathbb{Z}^g
\]

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

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

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

The point \((a_i)_{i \in \mathbb{Z}_\ell} := (\vartheta_i(0))_{i \in \mathbb{Z}_\ell}\) is called the \textbf{theta null point} of level \(\ell\) of the Abelian Variety \(A := \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)\).

\((a_i)_{i \in \mathbb{Z}_\ell}\) determines the equations of the projective embedding of \(A\) of level \(\ell\).

The symplectic basis \(\mathbb{Z}^g \oplus \Omega \mathbb{Z}^g\) induce a decomposition into isotropic subgroups for the commutator pairing:

\[
A[\ell] = A[\ell]_1 \oplus A[\ell]_2
= \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g \oplus \frac{1}{\ell} \Omega \mathbb{Z}^g / \Omega \mathbb{Z}^g
\]

This decomposition can be recovered by \((a_i)_{i \in \mathbb{Z}_\ell}\).

The \textbf{action by translation} is given by

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

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

**Theorem**

- Let $\ell = n.m$, and $\varphi : \mathbb{Z}_n \to \mathbb{Z}_\ell, x \mapsto m.x$ be the canonical embedding.
  
  Let $K = A[m]_2 \subset A[\ell]_2$.

- Let $(\theta_i^A)_{i \in \mathbb{Z}_\ell}$ be the theta functions of level $\ell$ on $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega \mathbb{Z}^g)$.

- Let $(\theta_i^B)_{i \in \mathbb{Z}_n}$ be the theta functions of level $n$ of $B = A/K = \mathbb{C}^g/(\mathbb{Z}^g + \Omega m \mathbb{Z}^g)$.

- We have:
  
  $$ (\theta_i^B(x))_{i \in \mathbb{Z}_n} = (\theta_{\varphi(i)}^A(x))_{i \in \mathbb{Z}_n} $$

**Proof.**

$$ \theta_i^B(z) = \theta \left[ \begin{array}{c} 0 \\ i/n \end{array} \right] \left( z, \frac{\Omega}{m}/n \right) = \theta \left[ \begin{array}{c} 0 \\ mi/\ell \end{array} \right] \left( z, \Omega/\ell \right) = \theta_{m \cdot i}^A(z) $$
The isogeny theorem

**Theorem**

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

\[
\left( \vartheta_i^B(x) \right)_{i \in \mathbb{Z}_n} = \left( \vartheta_{\varphi(i)}^A(x) \right)_{i \in \mathbb{Z}_n}
\]

**Proof.**

\[
\vartheta_i^B(z) = \vartheta \left[ \begin{array}{c} 0 \\ i/n \end{array} \right] (z, \frac{\Omega}{m/n}) = \vartheta \left[ \begin{array}{c} 0 \\ mi/\ell \end{array} \right] (z, \Omega/\ell) = \vartheta_{m \cdot i}^A(z)
\]
The isogeny theorem

**Theorem**

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

$$ (\vartheta^B_i(x))_{i \in \mathbb{Z}_n} = (\vartheta^A_{\varphi(i)}(x))_{i \in \mathbb{Z}_n} $$

**Proof.**

$$ \vartheta^B_i(z) = \vartheta \left[ \begin{array}{c} 0 \\ i/n \end{array} \right] (z, \frac{\Omega}{m}/n) = \vartheta \left[ \begin{array}{c} 0 \\ \frac{mi}{\ell} \end{array} \right] (z, \frac{\Omega}{\ell}) = \vartheta^A_{m \cdot i}(z) $$
The isogeny theorem

Theorem

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

$$ (\vartheta^B_i(x))_{i \in \mathbb{Z}_n} = (\vartheta^{\varphi(i)}_A(x))_{i \in \mathbb{Z}_n} $$

Proof.

$$ \vartheta^B_i(z) = \vartheta \begin{bmatrix} 0 \\ i/n \end{bmatrix} \left( z, \frac{\Omega}{m/n} \right) = \vartheta \begin{bmatrix} 0 \\ mi/\ell \end{bmatrix} \left( z, \frac{\Omega}{\ell} \right) = \vartheta^A_{m \cdot i}(z) $$
The isogeny theorem

Theorem

- Let \( \ell = n \cdot m \), and \( \varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_\ell \), \( x \mapsto m \cdot x \) be the canonical embedding.
  - Let \( K = A[m]_2 \subset A[\ell]_2 \).
- Let \( (\vartheta^A_i)_{i \in \mathbb{Z}_\ell} \) be the theta functions of level \( \ell \) on \( A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g) \).
- Let \( (\vartheta^B_i)_{i \in \mathbb{Z}_n} \) 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:
  \[
  (\vartheta^B_i(x))_{i \in \mathbb{Z}_n} = (\vartheta^A_{\varphi(i)}(x))_{i \in \mathbb{Z}_n}
  \]

Proof.

\[
\vartheta^B_i(z) = \vartheta \begin{bmatrix} 0 \\ i/n \end{bmatrix} \left( z, \frac{\Omega}{m/n} \right) = \vartheta \begin{bmatrix} 0 \\ mi/\ell \end{bmatrix} \left( z, \frac{\Omega}{\ell} \right) = \vartheta^A_{m \cdot i}(z)
\]
Mumford: On equations defining Abelian varieties

**Theorem (car \( k \perp \ell \))**

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

\[
\sum_{t \in \mathbb{Z}_2} a_{x+t}a_{y+t} = \sum_{t \in \mathbb{Z}_2} a_{z-u+t}a_{z-y+t} = \sum_{t \in \mathbb{Z}_2} a_{z-x+t}a_{z-v+t}
\] (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 \( \ell \). The locus of theta null points of level \( \ell \) is an open subset \( \mathcal{M}_\ell^0(k) \) of \( \mathcal{M}_\ell(k) \).

**Remark**

- Analytic action: \( \text{Sp}_{2g}(\mathbb{Z}) \) acts on \( \mathcal{H}_g \) (and preserve the isomorphic classes).
- Algebraic action: \( \text{Sp}_{2g}(\mathbb{Z}_\ell) \) acts on \( \mathcal{M}_\ell \).
The theta null point of level $\ell (a_i)_{i \in \mathbb{Z}_\ell}$ satisfy the Riemann Relations:

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

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

$$a_{x} = a_{-x}$$

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

**Remark**

- **Analytic action**: $\text{Sp}_{2g}(\mathbb{Z})$ acts on $\mathcal{H}_g$ (and preserve the isomorphic classes).
- **Algebraic action**: $\text{Sp}_{2g}(\mathbb{Z}_\ell)$ acts on $\mathcal{M}_\ell$. 
Mumford: On equations defining Abelian varieties

**Theorem (car \( k + \ell \))**

The theta null point of level \( \ell \) \((a_i)_{i \in \mathbb{Z}_\ell}\) satisfy the Riemann Relations:

\[
\sum_{t \in \mathbb{Z}_2} a_{x+t} a_{y+t} \sum_{t \in \mathbb{Z}_2} a_{u+t} a_{v+t} = \sum_{t \in \mathbb{Z}_2} a_{z-u+t} a_{z-v+t} \sum_{t \in \mathbb{Z}_2} a_{z-x+t} a_{z-v+t}
\]

(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 \( \ell \). The locus of theta null points of level \( \ell \) is an open subset \( \mathcal{M}_\ell^0(k) \) of \( \mathcal{M}_\ell(k) \).

**Remark**

- **Analytic action**: \( \text{Sp}_{2g}(\mathbb{Z}) \) acts on \( \mathcal{H}_g \) (and preserve the isomorphic classes).
- **Algebraic action**: \( \text{Sp}_{2g}(\mathbb{Z}_\ell) \) acts on \( \mathcal{M}_\ell \).
Mumford: On equations defining Abelian varieties

Theorem (car $k + \ell$)

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

\[
\sum_{t \in \mathbb{Z}_2} a_{x+t}a_{y+t} \sum_{t \in \mathbb{Z}_2} a_{u+t}a_{v+t} = \sum_{t \in \mathbb{Z}_2} a_{z-u+t}a_{z-y+t} \sum_{t \in \mathbb{Z}_2} a_{z-x+t}a_{z-v+t} \tag{1}
\]

We note $M_\ell$ the moduli space given by these relations together with the relations of symmetry:

\[a_x = a_{-x}\]

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

Remark

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

\[ A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \ \text{determines} \ \ (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k) \]

\[ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \ \text{determines} \ \ (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k) \]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
Summary

\[ A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k) \]

\[ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k) \]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
Summary

\[ A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k) \]

\[ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k) \]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
\[ A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in M_\ell(k) \]

\[ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in M_n(k) \]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
Summary

\[ A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k) \]

\[ B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k) \]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
The kernel of $\pi$ is $A_k[m]_2 \subset A_k[\ell]_2$.

The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$. 

\[
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k)
\]

\[
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k)
\]
Summary

\[
A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2 \quad \text{determines} \quad (a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k)
\]

\[
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \quad \text{determines} \quad (b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k)
\]

- The kernel of \( \pi \) is \( A_k[m]_2 \subset A_k[\ell]_2 \).
- The kernel of \( \hat{\pi} \) is \( \pi(A_k[m]_1) \).
Summary

- $A_k, A_k[\ell] = A_k[\ell]_1 \oplus A_k[\ell]_2$ determines $(a_i)_{i \in \mathbb{Z}_\ell} \in \mathcal{M}_\ell(k)$.
- $B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2$ determines $(b_i)_{i \in \mathbb{Z}_n} \in \mathcal{M}_n(k)$.

- The kernel of $\pi$ is $A_k[m]_2 \subset A_k[\ell]_2$.
- The kernel of $\hat{\pi}$ is $\pi(A_k[m]_1)$.
An Example with \( n \land m = 1 \)

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

- Let \( B \) be the elliptic curve \( y^2 = x^3 + 11x + 47 \) over \( k = \mathbb{F}_{79} \). The corresponding theta null point \((b_0, b_1, b_2, b_3)\) of level 4 is \((1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79})\).

- We note \( V_B(k) \) the subvariety of \( \mathcal{M}_{12}(k) \) defined by

\[
\begin{align*}
a_0 &= b_0, \\
a_3 &= b_1, \\
a_6 &= b_2, \\
a_9 &= b_3
\end{align*}
\]

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

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

- Program:
  - Compute the solutions.
  - Identify the valid theta null points.
  - Compute the dual isogeny.
An Example with $n \wedge m = 1$

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

- Let $B$ be the elliptic curve $y^2 = x^3 + 11x + 47$ over $k = \mathbb{F}_{79}$. The corresponding theta null point $(b_0, b_1, b_2, b_3)$ of level 4 is $(1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79})$.

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

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

Program:

- Compute the solutions.
- Identify the valid theta null points.
- Compute the dual isogeny.
An Example with $n \wedge m = 1$

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

- Let $B$ be the elliptic curve $y^2 = x^3 + 11x + 47$ over $k = \mathbb{F}_{79}$. The corresponding theta null point $(b_0, b_1, b_2, b_3)$ of level 4 is $(1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79})$.
- 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 $(a_i)_{i \in \mathbb{Z}_{\ell n}} \in V_B^0(k)$ corresponds a 3-isogeny $\pi : A \rightarrow B$:
  \[ \pi(\vartheta_i^A(x)_{i \in \mathbb{Z}_{12}}) = (\vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x)) \]

**Program:**
- Compute the solutions.
- Identify the valid theta null points.
- Compute the dual isogeny.
An Example with \( n \wedge m = 1 \)

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

1. Let \( B \) be the elliptic curve \( y^2 = x^3 + 11x + 47 \) over \( k = \mathbb{F}_{79} \). The corresponding theta null point \( (b_0, b_1, b_2, b_3) = (1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79}) \).

2. We note \( V_B(k) \) the subvariety of \( \mathcal{M}_{12}(k) \) defined by

\[
\begin{align*}
 a_0 &= b_0, \\
 a_3 &= b_1, \\
 a_6 &= b_2, \\
 a_9 &= b_3
\end{align*}
\]

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

\[
\pi\left( \vartheta_i^A(x)_{i \in \mathbb{Z}_{12}} \right) = \left( \vartheta_0^A(x), \vartheta_3^A(x), \vartheta_6^A(x), \vartheta_9^A(x) \right)
\]

Program:

- Compute the solutions.
- Identify the valid theta null points.
- Compute the dual isogeny.
An Example with $n \wedge m = 1$

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

- Let $B$ be the elliptic curve $y^2 = x^3 + 11x + 47$ over $k = \mathbb{F}_{79}$. The corresponding theta null point $(b_0, b_1, b_2, b_3)$ of level 4 is $(1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79})$.

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

  $$\pi(\vartheta^A_i(x)_{i \in \mathbb{Z}_{12}}) = (\vartheta^A_0(x), \vartheta^A_3(x), \vartheta^A_6(x), \vartheta^A_9(x))$$

Program:

- Compute the solutions.
- Identify the valid theta null points.
- Compute the dual isogeny.
An Example with $n \wedge m = 1$

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

- Let $B$ be the elliptic curve $y^2 = x^3 + 11x + 47$ over $k = \mathbb{F}_{79}$. The corresponding theta null point $(b_0, b_1, b_2, b_3)$ of level 4 is $(1 : 1 : 12 : 1) \in \mathcal{M}_4(\mathbb{F}_{79})$.

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

$$\pi(\vartheta^A_i(x)_{i \in \mathbb{Z}_{12}}) = (\vartheta^A_0(x), \vartheta^A_3(x), \vartheta^A_6(x), \vartheta^A_9(x))$$

Program:

- Compute the solutions.
- Identify the valid theta null points.
- Compute the dual isogeny.
The kernel of the dual isogeny

Let \((a_i)_{i \in \mathbb{Z}_\ell}\) be a valid theta null point solution. Let \(\zeta\) be a primitive 3-th root of unity.

The kernel \(K\) of \(\pi\) is

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

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

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

Theorem

Let \((a_i)_{i \in \mathbb{Z}_{12}}\) be any solution. Then \((a_i)_{i \in \mathbb{Z}_{12}}\) is valid if and only if

\[
\# \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\} = 3
\]
The kernel of the dual isogeny

- Let \((a_i)_{i \in \mathbb{Z}_\ell}\) be a valid theta null point solution. Let \(\zeta\) be a primitive 3-th root of unity.
  The kernel \(K\) of \(\pi\) is

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

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

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

Theorem

Let \((a_i)_{i \in \mathbb{Z}_{12}}\) be any solution. Then \((a_i)_{i \in \mathbb{Z}_{12}}\) is valid if and only if

\[
\# \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\} = 3
\]
The kernel of the dual isogeny

- Let \((a_i)_{i \in \mathbb{Z}_\ell}\) be a valid theta null point solution. Let \(\zeta\) be a primitive 3-th root of unity.
  
  The kernel \(K\) of \(\pi\) 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})\}
  
- 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)\}
  
**Theorem**

Let \((a_i)_{i \in \mathbb{Z}_{12}}\) be any solution. Then \((a_i)_{i \in \mathbb{Z}_{12}}\) is valid if and only if

\[\# \{(a_0, a_3, a_6, a_9), (a_4, a_7, a_{10}, a_1), (a_8, a_{11}, a_2, a_5)\} = 3\]
The automorphisms of the theta group

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

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

In general, for each \(m\)-isogeny, there will be \(\approx m^{g^2 + g(g+1)/2}\) solutions.
The automorphisms of the theta group

- 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

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

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

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

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

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

- In general, for each \(m\)-isogeny, there will be \(\approx m^{g^2 + g(g+1)/2}\) solutions.
The solutions

Solutions of the system

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


  \[(v^{465647} : 1 : 3 : v^{465647} : 40 : 16 : v^{29498} : 16 : 40 : v^{465647} : 3 : 1)\]


- And the following degenerate solutions:

  \[(1 : 1 : 12 : 1 : 1 : 12 : 1 : 1 : 12 : 1)\]

  \[(1 : 0 : 0 : 1 : 0 : 12 : 0 : 0 : 1 : 0 : 0)\]
The solutions

Solutions of the system

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

  $$(\nu^{490931} : 1 : 46 : \nu^{490931} : 37 : 54 : \nu^{54782} : 54 : 37 : \nu^{490931} : 46 : 1)$$

  $$(\nu^{476182} : 1 : 68 : \nu^{476182} : 67 : 10 : \nu^{40033} : 10 : 67 : \nu^{476182} : 68 : 1)$$

  $$(\nu^{465647} : 1 : 3 : \nu^{465647} : 40 : 16 : \nu^{29498} : 16 : 40 : \nu^{465647} : 3 : 1)$$

  $$(\nu^{450898} : 1 : 33 : \nu^{450898} : 69 : 24 : \nu^{14749} : 24 : 69 : \nu^{450898} : 33 : 1)$$

- And the following degenerate solutions:


  $$(1 : 0 : 0 : 1 : 0 : 0 : 12 : 0 : 0 : 1 : 0 : 0)$$
The dual isogeny

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

$$\tilde{\pi}(y) = 3x$$

Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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 $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$. 

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

$$\tilde{\pi}(y) = 3x$$

Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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 $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$. 

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

$$\tilde{\pi}(y) = 3x$$

Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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 $\lambda_0, \lambda_{P_1}, \lambda_{2P_1}$. 

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

$$\tilde{\pi}(y) = 3x$$

Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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

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

\[
\tilde{\pi}(y) = 3x
\]

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

\[
\begin{align*}
y &= (x_0, x_3, x_6, x_9) \\
y + P_1 &= (x_4, x_7, x_{10}, x_1) \\
y + 2P_1 &= (x_8, x_{11}, x_2, x_5)
\end{align*}
\]

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

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

$$\tilde{\pi}(y) = 3x$$

- Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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**

Let $\pi : A \rightarrow B$ 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 $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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

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

Let $P_1 = (a_4, a_7, a_{10}, a_1) \in \tilde{K}$, $P_1$ 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)**

\[
2^g \vartheta \left[ a' \right] (x + y) \vartheta \left[ b' \right] (x - y) \vartheta \left[ c' \right] (0) \vartheta \left[ d' \right] (0) = \\
\sum_{\alpha, \beta \in \frac{1}{2} \mathbb{Z}^g / \mathbb{Z}^g} e^{2\pi i \beta' (a + b + c + d)} \vartheta \left[ a + \alpha \right] (x) \vartheta \left[ b + \alpha \right] (x) \vartheta \left[ c + \alpha \right] (y) \vartheta \left[ d + \alpha \right] (y)
\]

where \( A = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \)

\( a, b, c, d, e, f, g, h \in \frac{1}{2} \mathbb{Z}^g / \mathbb{Z}^g \)

\( (a', b', c', d') = A(a, b, c, d), (e', f', g', h') = A(e, f, g, h) \)
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 $\lambda_{P_1}^3, \lambda_{2P_1}^3$, so we don’t need to extract roots.
- Vélu’s like formulas: If we know the kernel $\tilde{\mathcal{K}}$ 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 $\lambda_{ij}$. 
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 $\tilde{\mathcal{K}}$ 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 $\lambda_{ij}$. 
Computing isogenies

Computing the projective factors

- Using the addition formulas, we have $\lambda_{2P_1} = \lambda_{P_1}^2$.
- Since $\gamma + 3P_1 = \gamma$, 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 $\tilde{\mathcal{K}}$ 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 $\lambda_{i,j}$.
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.
- \( \text{Vélu’s like formulas} \): If we know the kernel \( \tilde{\mathcal{K}} \) 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 \( \lambda_{i,j} \).
Perspective

- The bottleneck of the algorithm is the computation of the modular solutions. Use the action on the solutions to speed-up this part. [In progress]
- By using a method similar to the computation of the dual isogeny, one can compute the commutator pairing. Is this computation competitive?
Perspective

- The bottleneck of the algorithm is the computation of the modular solutions. Use the action on the solutions to speed-up this part. [In progress]
- By using a method similar to the computation of the dual isogeny, one can compute the commutator pairing. Is this computation competitive?