Computing isogenies of small degrees on Abelian Varieties

D. Lubicz[1] **D. Robert** [2]

[1]Célar, Délégation Générale de l'Armement, Rennes, France

[2]Loria, Nancy, France

4 November 2008, Tsukuba University

Outline

Outline

Outline

1. Abelian Varieties
2. Isogenies, a fundamental tool
3. Computing isogenies

Outline

1. Abelian Varieties
2. Isogenies, a fundamental tool
3. Computing isogenies

Abelian Varieties

Définition

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

- An Abelian variety is just a set of points on a projective space, satisfying some homogeneous polynomials, together with an algebraic group law between them.
- An Abelian Variety is projective, smooth and irreducible. The group law is Abelian.
- Abelian Varieties of dimension 1 are called elliptic curves.

Abelian Varieties

Définition

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

- An Abelian variety is just a set of points on a projective space, satisfying some homogeneous polynomials, together with an algebraic group law between them.
- An Abelian Variety is projective, smooth and irreducible. The group law is Abelian.
- Abelian Varieties of dimension 1 are called elliptic curves.

Abelian Varieties

Définition

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

- An Abelian variety is just a set of points on a projective space, satisfying some homogeneous polynomials, together with an algebraic group law between them.
- An Abelian Variety is projective, smooth and irreducible. The group law is Abelian.
- Abelian Varieties of dimension 1 are called elliptic curves.

Abelian Varieties

Définition

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

- An Abelian variety is just a set of points on a projective space, satisfying some homogeneous polynomials, together with an algebraic group law between them.
- An Abelian Variety is projective, smooth and irreducible. The group law is Abelian.
- Abelian Varieties of dimension 1 are called elliptic curves.

Examples

- If C is a curve of genus g, we can consider the space consisting of sets of g points of C (with multiplicity). One can find addition laws such that this space is an Abelian Variety, this is called the Jacobian of C. $\mathrm{Jac}(C)$ is of dimension g.
- The Jacobian of a curve C of genus 1 is isomorphic to C.

Abelian Varieties over $\mathbb{C}$

If the base field is $\mathbb{C}$, an Abelian Variety A of dimension n is isomorphic to a torus V/Λ where $V = \mathbb{C}^n$ and Λ is a lattice of rank $2n$.

Examples

- If C is a curve of genus g, we can consider the space consisting of sets of g points of C (with multiplicity). One can find addition laws such that this space is an Abelian Variety, this is called the Jacobian of C. $\mathrm{Jac}(C)$ is of dimension g.
- The Jacobian of a curve C of genus 1 is isomorphic to C.

Abelian Varieties over $\mathbb{C}$

If the base field is $\mathbb{C}$, an Abelian Variety A of dimension n is isomorphic to a torus V/Λ where $V = \mathbb{C}^n$ and Λ is a lattice of rank $2n$.

Abelian Varieties and cryptography

- The Discrete Logarithm Problem is conjectured to be hard on Abelian Varieties (at last if the dimension is small). So Abelian Varieties provide the classic asymmetric cryptographic architecture : public/private keys, zero knowledge, signatures.
- An Abelian Variety is provided with pairings, that is a non degenerate bilinear map from a subset of the Abelian Variety to an extension of the base field. This provide new cryptographic protocols : identity based encryption, short signatures, tripartite Diffie-Helmann.

Abelian Varieties and cryptography

- The Discrete Logarithm Problem is conjectured to be hard on Abelian Varieties (at last if the dimension is small). So Abelian Varieties provide the classic asymmetric cryptographic architecture : public/private keys, zero knowledge, signatures.
- An Abelian Variety is provided with pairings, that is a non degenerate bilinear map from a subset of the Abelian Variety to an extension of the base field. This provide new cryptographic protocols : identity based encryption, short signatures, tripartite Diffie-Helmann.

Working with Abelian Varieties

- One usually work with Jacobian of curves defined over finite fields. One can use Mumford representation to represent points of the Jacobian ($2g$ coordinates), and use Cantor's algorithm for the addition.
- However there is no such representation for general Abelian Varieties. And Mumford representation does not give an embedding from the Jacobian to a projective space.
- One can use theta functions to embed the Jacobian to the projective space. However, if the genus of the curve is g, one has to use 4^g coordinates. For example in Cassels and Flynn, they describe the Jacobian of a curve of genus 2 by using 16 coordinates, and the Jacobian is defined by 72 equations in $\mathbb{P}^{15}$.
- Solution : we will consider Abelian Varieties over $\mathbb{C}$.

Working with Abelian Varieties

- One usually work with Jacobian of curves defined over finite fields. One can use Mumford representation to represent points of the Jacobian ($2g$ coordinates), and use Cantor's algorithm for the addition.
- However there is no such representation for general Abelian Varieties. And Mumford representation does not give an embedding from the Jacobian to a projective space.
- One can use theta functions to embed the Jacobian to the projective space. However, if the genus of the curve is g, one has to use 4^g coordinates. For example in Cassels and Flynn, they describe the Jacobian of a curve of genus 2 by using 16 coordinates, and the Jacobian is defined by 72 equations in $\mathbb{P}^{15}$.
- Solution : we will consider Abelian Varieties over $\mathbb{C}$.

Working with Abelian Varieties

- One usually work with Jacobian of curves defined over finite fields. One can use Mumford representation to represent points of the Jacobian ($2g$ coordinates), and use Cantor's algorithm for the addition.
- However there is no such representation for general Abelian Varieties. And Mumford representation does not give an embedding from the Jacobian to a projective space.
- One can use theta functions to embed the Jacobian to the projective space. However, if the genus of the curve is g, one has to use 4^g coordinates. For example in Cassels and Flynn, they describe the Jacobian of a curve of genus 2 by using 16 coordinates, and the Jacobian is defined by 72 equations in $\mathbb{P}^{15}$.
- Solution : we will consider Abelian Varieties over $\mathbb{C}$.

Working with Abelian Varieties

- One usually work with Jacobian of curves defined over finite fields. One can use Mumford representation to represent points of the Jacobian ($2g$ coordinates), and use Cantor's algorithm for the addition.
- However there is no such representation for general Abelian Varieties. And Mumford representation does not give an embedding from the Jacobian to a projective space.
- One can use theta functions to embed the Jacobian to the projective space. However, if the genus of the curve is g, one has to use 4^g coordinates. For example in Cassels and Flynn, they describe the Jacobian of a curve of genus 2 by using 16 coordinates, and the Jacobian is defined by 72 equations in $\mathbb{P}^{15}$.
- Solution : we will consider Abelian Varieties over $\mathbb{C}$.

Abelian Varieties over $\mathbb{C}$

- An abelian variety of dimension n over $\mathbb{C}$ is a torus $A = V/\Lambda$. We can assume $\Lambda = \mathbb{Z}^n + \Omega\mathbb{Z}^n$ where $\Omega \in \mathrm{GL}_n(\mathbb{Z})$.
- For a torus $V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$ to be an Abelian Variety, Ω needs to be in Siegel upper half space : Ω is symmetric and $\mathrm{Im}(\Omega)$ is definite positive.
- To get an embedding to the projective space, we need analytic functions on V that are quasi periodic with respect to the lattice Λ.
- For every Ω in Siegel upper half space, we can associate a theta function

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

Then for every $n \in \mathbb{Z}^n$ we have :

$$\theta(z+n,\Omega) = \theta(z,\Omega) \quad (1)$$

$$\theta(z+n\Omega,\Omega) = \exp(-\pi i n'\Omega n - 2\pi i n' z)\theta(z,\Omega) \quad (2)$$

Abelian Varieties over $\mathbb{C}$

- An abelian variety of dimension n over $\mathbb{C}$ is a torus $A = V/\Lambda$. We can assume $\Lambda = \mathbb{Z}^n + \Omega\mathbb{Z}^n$ where $\Omega \in \mathrm{GL}_n(\mathbb{Z})$.
- For a torus $V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$ to be an Abelian Variety, Ω needs to be in Siegel upper half space : Ω is symmetric and $\mathrm{Im}(\Omega)$ is definite positive.
- To get an embedding to the projective space, we need analytic functions on V that are quasi periodic with respect to the lattice Λ.
- For every Ω in Siegel upper half space, we can associate a theta function

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

Then for every $n \in \mathbb{Z}^n$ we have :

$$\theta(z+n,\Omega) = \theta(z,\Omega) \quad (1)$$

$$\theta(z+n\Omega,\Omega) = \exp(-\pi i n'\Omega n - 2\pi i n' z)\theta(z,\Omega) \quad (2)$$

Abelian Varieties over $\mathbb{C}$

- An abelian variety of dimension n over $\mathbb{C}$ is a torus $A = V/\Lambda$. We can assume $\Lambda = \mathbb{Z}^n + \Omega\mathbb{Z}^n$ where $\Omega \in \mathrm{GL}_n(\mathbb{Z})$.
- For a torus $V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$ to be an Abelian Variety, Ω needs to be in Siegel upper half space : Ω is symmetric and $\mathrm{Im}(\Omega)$ is definite positive.
- To get an embedding to the projective space, we need analytic functions on V that are quasi periodic with respect to the lattice Λ.
- For every Ω in Siegel upper half space, we can associate a theta function

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

Then for every $n \in \mathbb{Z}^n$ we have :

$$\theta(z + n, \Omega) = \theta(z, \Omega) \tag{1}$$

$$\theta(z + n\Omega, \Omega) = \exp(-\pi i n' \Omega n - 2\pi i n' z)\theta(z, \Omega) \tag{2}$$

Theta functions

- We can find more functions by translating (and twisting) θ : if $a, b \in \mathbb{Q}^n$ we define

$$\theta[a,b](z,\Omega) = \exp(\pi i a' \Omega a + 2\pi i a'(z+b))\theta(z+\Omega a + b, \Omega)$$

Then for every $n \in \mathbb{Z}^n$ we have :

$$\theta[a,b](z+n,\Omega) = \exp(2\pi i a' n)\theta[a,b](z,\Omega)$$
$$\theta[a,b](z+n\Omega,\Omega) = \exp(-2\pi i b' n)\exp(-\pi i n'\Omega n - 2\pi i n' z)\theta[a,b](z,\Omega)$$

- If we can find theta functions θ_i satisfying the same factor of automorphy, then if $x \in A$, $(\theta_1(\tilde{x}) : \theta_2(\tilde{x}) : \ldots) \in \mathbb{P}_{\mathbb{C}}$ does not depend on the representative $\tilde{x}$ of x in V.

Theta functions

- We can find more functions by translating (and twisting) θ : if $a, b \in \mathbb{Q}^n$ we define

$$\theta[a,b](z,\Omega) = \exp(\pi i a' \Omega a + 2\pi i a'(z+b))\theta(z + \Omega a + b, \Omega)$$

Then for every $n \in \mathbb{Z}^n$ we have :

$$\theta[a,b](z+n,\Omega) = \exp(2\pi i a' n)\theta[a,b](z,\Omega)$$
$$\theta[a,b](z+n\Omega,\Omega) = \exp(-2\pi i b' n)\exp(-\pi i n'\Omega n - 2\pi i n' z)\theta[a,b](z,\Omega)$$

- If we can find theta functions θ_i satisfying the same factor of automorphy, then if $x \in A$, $(\theta_1(\tilde{x}) : \theta_2(\tilde{x}) : \ldots) \in \mathbb{P}_{\mathbb{C}}$ does not depend on the representative $\tilde{x}$ of x in V.

Projective embeddings given by theta functions

Définition

Let $\mathcal{L}_l$ be the vector space of analytic functions f satisfying the factor of automorphy

$$f(z+n) = f(z)$$
$$f(z+n\Omega) = \exp(-l \times \pi i n'\Omega n - l \times 2\pi i n' z) f(z)$$

This is called the space of theta functions of level l.

Théorème

- *$\theta[0, b/l](z, \Omega/l)_{b \in [0,l-1]^n}$ forms a basis of theta functions of level l. For $i \in \mathbb{Z}_l := \mathbb{Z}^n/l\mathbb{Z}^n$, we denote $\theta_i := \theta[0, i/l](z, \Omega/l)$.*
- *If $l \geq 3$ then $x \mapsto (\theta_i(x))_{i \in \mathbb{Z}^n/l\mathbb{Z}^n}$ is a projective embedding $A \to \mathbb{P}_{\mathbb{C}}^{l^g - 1}$.*

Projective embeddings given by theta functions

Définition

Let $\mathcal{L}_l$ be the vector space of analytic functions f satisfying the factor of automorphy

$$f(z+n) = f(z)$$
$$f(z+n\Omega) = \exp(-l \times \pi i n'\Omega n - l \times 2\pi i n' z) f(z)$$

This is called the space of theta functions of level l.

Théorème

- $\theta[0, b/l](z, \Omega/l)_{b \in [0,l-1]^n}$ *forms a basis of theta functions of level* l. *For* $i \in \mathbb{Z}_l := \mathbb{Z}^n / l\mathbb{Z}^n$, *we denote* $\theta_i := \theta[0, i/l](z, \Omega/l)$.
- *If* $l \geq 3$ *then* $x \mapsto (\theta_i(x))_{i \in \mathbb{Z}^n / l\mathbb{Z}^n}$ *is a projective embedding* $A \to \mathbb{P}_{\mathbb{C}}^{l^g - 1}$.

Symplectic basis and pairings

- Recall that $\theta[a,b](z+c+d\Omega)$ is easy to compute if we know $\theta[a,b](z+c+d\Omega)$. As $\theta_i = \theta[0,i/l](z,\Omega/l)$, this mean that adding a point of l-torsion $P \in \frac{1}{l}\mathbb{Z}^n + \frac{1}{l}\Omega\mathbb{Z}^n$ is easy.
- This give an action from $A[l]$ to the space of theta functions of level l.
- The commutator of this action give a pairing $A[l] \times A[l] \to k^\star$. This pairing is the exponential of the factor of automorphy

$$E = \begin{pmatrix} O & l \\ -l & 0 \end{pmatrix}$$

- For a factor of automorphy of level l, this give the Weil pairing :

$$e(x_1/l\mathbb{Z}^n + x_2/l\Omega\mathbb{Z}^n, y_1/l\mathbb{Z}^n + y_2/l\Omega\mathbb{Z}^n) = \frac{\exp(-\pi i l (x_1|y_2))}{\exp(-\pi i l (x_2|y_1))}$$

Symplectic basis and pairings

- Recall that $\theta[a,b](z+c+d\Omega)$ is easy to compute if we know $\theta[a,b](z+c+d\Omega)$. As $\theta_i = \theta[0,i/l](z,\Omega/l)$, this mean that adding a point of l-torsion $P \in \frac{1}{l}\mathbb{Z}^n + \frac{1}{l}\Omega\mathbb{Z}^n$ is easy.
- This give an action from $A[l]$ to the space of theta functions of level l.
- The commutator of this action give a pairing $A[l] \times A[l] \to k^\star$. This pairing is the exponential of the factor of automorphy

$$E = \begin{pmatrix} O & l \\ -l & 0 \end{pmatrix}$$

- For a factor of automorphy of level l, this give the Weil pairing :

$$e(x_1/l\mathbb{Z}^n + x_2/l\Omega\mathbb{Z}^n, y_1/l\mathbb{Z}^n + y_2/l\Omega\mathbb{Z}^n) = \frac{\exp(-\pi i l(x_1|y_2))}{\exp(-\pi i l(x_2|y_1))}$$

Symplectic basis and pairings

- Recall that $\theta[a,b](z+c+d\Omega)$ is easy to compute if we know $\theta[a,b](z+c+d\Omega)$. As $\theta_i = \theta[0,i/l](z,\Omega/l)$, this mean that adding a point of l-torsion $P \in \frac{1}{l}\mathbb{Z}^n + \frac{1}{l}\Omega\mathbb{Z}^n$ is easy.
- This give an action from $A[l]$ to the space of theta functions of level l.
- The commutator of this action give a pairing $A[l] \times A[l] \to k^\star$. This pairing is the exponential of the factor of automorphy

$$E = \begin{pmatrix} O & l \\ -l & 0 \end{pmatrix}$$

- For a factor of automorphy of level l, this give the Weil pairing :

$$e(x_1/l\mathbb{Z}^n + x_2/l\Omega\mathbb{Z}^n, y_1/l\mathbb{Z}^n + y_2/l\Omega\mathbb{Z}^n) = \frac{\exp(-\pi i l (x_1|y_2))}{\exp(-\pi i l (x_2|y_1))}$$

Addition formulas

Cf Mumford, TATA Lectures on Theta[1]. They give the fastest addition for Jacobians of curves of genus 2 ! [Gaudry]

22

III. Addition Formulae

$$(A_1):\ \vartheta_{00}(x+u)\,\vartheta_{00}(x-u)\,\vartheta_{00}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)+\vartheta_{11}^2(x)\vartheta_{11}^2(u) = \vartheta_{01}^2(x)\vartheta_{01}^2(u)+\vartheta_{10}^2(x)\vartheta_{10}^2(u)$$

$$\vartheta_{01}(x+u)\,\vartheta_{01}(x-u)\,\vartheta_{01}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)-\vartheta_{10}^2(x)\vartheta_{10}(u) = \vartheta_{01}^2(x)\vartheta_{01}^2(u)-\vartheta_{11}^2(x)\vartheta_{11}^2(u)$$

$$\vartheta_{10}(x+u)\,\vartheta_{10}(x-u)\,\vartheta_{10}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)-\vartheta_{01}^2(x)\vartheta_{01}^2(u) = \vartheta_{10}^2(x)\vartheta_{10}^2(u)-\vartheta_{11}^2(x)\vartheta_{11}^2(u)$$

$$\vartheta_{00}(x+u)\vartheta_{01}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{01}(u) - \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$$

$$\vartheta_{01}(x+u)\vartheta_{00}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{01}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$$

$$\vartheta_{00}(x+u)\vartheta_{10}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{00}(u)\vartheta_{10}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$$

$$\vartheta_{10}(x+u)\vartheta_{00}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{00}(u)\vartheta_{10}(u) - \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$$

$$\vartheta_{01}(x+u)\vartheta_{10}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$$

$$\vartheta_{10}(x+u)\vartheta_{01}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = -\vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$$

$$(A_{10}):\ \vartheta_{11}(x+u)\vartheta_{11}(x-u)\vartheta_{00}^2(0) = \vartheta_{11}^2(x)\vartheta_{00}^2(u) - \vartheta_{00}^2(x)\vartheta_{11}^2(u) = \vartheta_{01}^2(x)\vartheta_{10}^2(u)-\vartheta_{10}^2(x)\vartheta_{01}^2(u)$$

$$\vartheta_{11}(x+u)\vartheta_{00}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) + \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{11}(u)$$

$$\vartheta_{00}(x+u)\vartheta_{u}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) - \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{11}(u)$$

$$\vartheta_{11}(x+u)\vartheta_{01}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{10}(u)$$

$$\vartheta_{01}(x+u)\vartheta_{11}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = -\vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{10}(u)$$

$$\vartheta_{11}(x+u)\vartheta_{10}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u)+\vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{01}(u)$$

$$\vartheta_{10}(x+u)\vartheta_{11}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = -\vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u)+\vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{01}(u)$$

Outline

Morphisms and isogenies

- Let A and B be two abelian varieties. A morphism $A \to B$ is an algebraic map $f : A \to B$ respecting the group law : $f(x + y) = f(x) + f(y)$. The kernel of f is the set of (geometric) points on A sent to 0_B by f (in fact we only need to check that $f(0_A) = 0_B$).
- We will work on morphisms between abelian varieties of the same dimension (think about Jacobians). We also want the Kernel to be finite. A morphism between two abelians varieties of dimension n and of finite kernel is called an isogeny.
- An isogeny is flat, finite and surjective.
- The multiplication by m map $[m]$ is an isogeny $A \to A$. It's kernel is $A[m]$, the set of m-torsions points.
- There is a bijection between finite subgroups of the variety and isogenies, so one can see an isogeny as a way to define a subgroup.

Morphisms and isogenies

- Let A and B be two abelian varieties. A morphism $A \to B$ is an algebraic map $f : A \to B$ respecting the group law : $f(x+y) = f(x) + f(y)$. The kernel of f is the set of (geometric) points on A sent to 0_B by f (in fact we only need to check that $f(0_A) = 0_B$).
- We will work on morphisms between abelian varieties of the same dimension (think about Jacobians). We also want the Kernel to be finite. A morphism between two abelians varieties of dimension n and of finite kernel is called an isogeny.
- An isogeny is flat, finite and surjective.
- The multiplication by m map $[m]$ is an isogeny $A \to A$. It's kernel is $A[m]$, the set of m-torsions points.
- There is a bijection between finite subgroups of the variety and isogenies, so one can see an isogeny as a way to define a subgroup.

Morphisms and isogenies

- Let A and B be two abelian varieties. A morphism $A \to B$ is an algebraic map $f : A \to B$ respecting the group law : $f(x+y) = f(x) + f(y)$. The kernel of f is the set of (geometric) points on A sent to 0_B by f (in fact we only need to check that $f(0_A) = 0_B$).
- We will work on morphisms between abelian varieties of the same dimension (think about Jacobians). We also want the Kernel to be finite. A morphism between two abelians varieties of dimension n and of finite kernel is called an isogeny.
- An isogeny is flat, finite and surjective.
- The multiplication by m map $[m]$ is an isogeny $A \to A$. It's kernel is $A[m]$, the set of m-torsions points.
- There is a bijection between finite subgroups of the variety and isogenies, so one can see an isogeny as a way to define a subgroup.

Morphisms and isogenies

- Let A and B be two abelian varieties. A morphism $A \to B$ is an algebraic map $f : A \to B$ respecting the group law : $f(x+y) = f(x) + f(y)$. The kernel of f is the set of (geometric) points on A sent to 0_B by f (in fact we only need to check that $f(0_A) = 0_B$).
- We will work on morphisms between abelian varieties of the same dimension (think about Jacobians). We also want the Kernel to be finite. A morphism between two abelians varieties of dimension n and of finite kernel is called an isogeny.
- An isogeny is flat, finite and surjective.
- The multiplication by m map $[m]$ is an isogeny $A \to A$. It's kernel is $A[m]$, the set of m-torsions points.
- There is a bijection between finite subgroups of the variety and isogenies, so one can see an isogeny as a way to define a subgroup.

Isogenies over $\mathbb{C}$

- If $A = V_1/\Lambda_1$ and $B = V_2/\Lambda_2$, a morphism $f : A \to B$ is a linear map $f : A \to B$ such that $f(\Lambda_1) \subset \Lambda_2$.
- If $f : V_1 \to V_2$ is bijective, then f is an isogeny of kernel $f^{-1}(\Lambda_2)/\Lambda_1$.
- If f is an isogeny, we can always assume that $V_1 = V_2$ and that $f = \mathrm{id}_V$. The kernel is Λ_2/Λ_1.
- The multiplication by m map has kernel isomorphic to $m\Lambda/\Lambda$, we find there are m^{2n} points of m-torsion.
- There is a bijection between isogenies and lattices containing Λ.

Constructive use

- Before we use an abelian variety for the DLP, we have to compute the number of points and see if it is a multiple of a big prime. In genus 1 one can use isogenies to considerably speedup Schoof algorithm (SEA).
- Isogenies help in CM-Methods.
- Every isogeny give a non degenerate pairing. The Weil pairing comes from the multiplication by m map.

Constructive use

- Before we use an abelian variety for the DLP, we have to compute the number of points and see if it is a multiple of a big prime. In genus 1 one can use isogenies to considerably speedup Schoof algorithm (SEA).
- Isogenies help in CM-Methods.
- Every isogeny give a non degenerate pairing. The Weil pairing comes from the multiplication by m map.

Destructive use

- One can use isogenies to transfer the DLP problem from an abelian variety A to an abelian variety B where it is easier.
- Every abelian variety of dimension 3 is the Jacobian of a curve of genus 3, but not every curve of genus 3 is hyperelliptic. Solving the DLP over a Jacobian of a non-hyperelliptic curve is easier, and one can try to use isogenies to go from an hyperelliptic curve to a non-hyperelliptic one.
- In dimension $n > 3$, there are abelian variety that are not Jacobians of curve. Again the DLP is easier on such abelian varieties, and one can try to find isogenies to go from a Jacobian to a non-Jacobian.

Destructive use

- One can use isogenies to transfer the DLP problem from an abelian variety A to an abelian variety B where it is easier.
- Every abelian variety of dimension 3 is the Jacobian of a curve of genus 3, but not every curve of genus 3 is hyperelliptic. Solving the DLP over a Jacobian of a non-hyperelliptic curve is easier, and one can try to use isogenies to go from an hyperelliptic curve to a non-hyperelliptic one.
- In dimension $n > 3$, there are abelian variety that are not Jacobians of curve. Again the DLP is easier on such abelian varieties, and one can try to find isogenies to go from a Jacobian to a non-Jacobian.

Destructive use

- One can use isogenies to transfer the DLP problem from an abelian variety A to an abelian variety B where it is easier.
- Every abelian variety of dimension 3 is the Jacobian of a curve of genus 3, but not every curve of genus 3 is hyperelliptic. Solving the DLP over a Jacobian of a non-hyperelliptic curve is easier, and one can try to use isogenies to go from an hyperelliptic curve to a non-hyperelliptic one.
- In dimension $n > 3$, there are abelian variety that are not Jacobians of curve. Again the DLP is easier on such abelian varieties, and one can try to find isogenies to go from a Jacobian to a non-Jacobian.

The isogeny theorem 1

- Let A be an abelian variety, given by an embedding of theta functions with respect to a factor of automorphy. We want to compute the isogeny of a finite subgroup, isotropic with respect to the commutator pairing induced by this factor of automorphy. (The pairing induced by this isogeny will be induced by this commutator pairing).
- To simplify the exposition, we will restrict ourselves to a subgroup of l torsion isotropic under the Weil pairing, that is we will use coordinates given by a factor of automorphy of level a multiple of l.
- We have seen that there are l^{2n} points of l-torsion, we want half the l torsion as kernel.
- Write $A = V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$, there are two canonical isotropic subgroups : $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$. We will choose the last one as our Kernel.

The isogeny theorem 1

- Let A be an abelian variety, given by an embedding of theta functions with respect to a factor of automorphy. We want to compute the isogeny of a finite subgroup, isotropic with respect to the commutator pairing induced by this factor of automorphy. (The pairing induced by this isogeny will be induced by this commutator pairing).
- To simplify the exposition, we will restrict ourselves to a subgroup of l torsion isotropic under the Weil pairing, that is we will use coordinates given by a factor of automorphy of level a multiple of l.
- We have seen that there are l^{2n} points of l-torsion, we want half the l torsion as kernel.
- Write $A = V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$, there are two canonical isotropic subgroups : $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$. We will choose the last one as our Kernel.

The isogeny theorem 1

- Let A be an abelian variety, given by an embedding of theta functions with respect to a factor of automorphy. We want to compute the isogeny of a finite subgroup, isotropic with respect to the commutator pairing induced by this factor of automorphy. (The pairing induced by this isogeny will be induced by this commutator pairing).
- To simplify the exposition, we will restrict ourselves to a subgroup of l torsion isotropic under the Weil pairing, that is we will use coordinates given by a factor of automorphy of level a multiple of l.
- We have seen that there are l^{2n} points of l-torsion, we want half the l torsion as kernel.
- Write $A = V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$, there are two canonical isotropic subgroups : $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$. We will choose the last one as our Kernel.

The isogeny theorem 2

Théorème

Let $A = V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$ be a variety, and $(\theta_i^A)_{i \in \mathbb{Z}^n/kl\mathbb{Z}^n}$ the theta functions of A of level kl. Let $\phi : \mathbb{Z}^n/k\mathbb{Z}^n \to \mathbb{Z}^n/kl\mathbb{Z}^n$ be the canonical inclusion $x \mapsto lx$. Let $B = A/\frac{1}{l}\Omega\mathbb{Z}^n = V/(\mathbb{Z}^n + \frac{\Omega}{l}\mathbb{Z}^n)$ and $(\theta_i^B)_{i \in \mathbb{Z}^n/k\mathbb{Z}^n}$ be the theta functions of B of level k. Then :

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

Démonstration.

$$\theta_i^B = \theta[0, i/k](z, \Omega/lk) = \theta[0, li/lk](z, \Omega/lk)$$

□

The isogeny theorem 2

Théorème

Let $A = V/(\mathbb{Z}^n + \Omega\mathbb{Z}^n)$ be a variety, and $(\theta_i^A)_{i\in\mathbb{Z}^n/kl\mathbb{Z}^n}$ the theta functions of A of level kl. Let $\phi : \mathbb{Z}^n/k\mathbb{Z}^n \to \mathbb{Z}^n/kl\mathbb{Z}^n$ be the canonical inclusion $x \mapsto lx$. Let $B = A/\frac{1}{l}\Omega\mathbb{Z}^n = V/(\mathbb{Z}^n + \frac{\Omega}{l}\mathbb{Z}^n)$ and $(\theta_i^B)_{i\in\mathbb{Z}^n/k\mathbb{Z}^n}$ be the theta functions of B of level k. Then :

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

Démonstration.

$$\theta_i^B = \theta[0, i/k](z, \Omega/lk) = \theta[0, li/lk](z, \Omega/lk)$$

□

Outline

State of the art

- In genus 1, if one choose the kernel K of the isogeny of an elliptic curve $E : y^2 = f(x)$, Velu's formulas give the isogeny of kernel K :

$$X(P) = \sum_{Q \in K} x(P+Q) - \sum_{Q \in K^\star} x(Q)$$

$$Y(P) = \sum_{Q \in K} y(P+Q) - \sum_{Q \in K^\star} y(Q)$$

and formulas for the equation of the curve E/K.

- One can then use these formulas together with the l-modular polynomial to compute isogenies of degree l.
- In genus 2, Richelot formulas (a generalisation of AGM) give isogenies of degree $(2,2)$.
- Smith generalized this to compute $(2,2,2)$-isogenies on genus 3.

State of the art

- In genus 1, if one choose the kernel K of the isogeny of an elliptic curve $E : y^2 = f(x)$, Velu's formulas give the isogeny of kernel K :

$$X(P) = \sum_{Q \in K} x(P+Q) - \sum_{Q \in K^\star} x(Q)$$

$$Y(P) = \sum_{Q \in K} y(P+Q) - \sum_{Q \in K^\star} y(Q)$$

  and formulas for the equation of the curve E/K.
- One can then use these formulas together with the l-modular polynomial to compute isogenies of degree l.
- In genus 2, Richelot formulas (a generalisation of AGM) give isogenies of degree $(2, 2)$.
- Smith generalized this to compute $(2, 2, 2)$-isogenies on genus 3.

The moduli space 1

- We will use the isogeny theorem to compute isogenies. We have stated it over $\mathbb{C}$, but it works over $\mathbb{F}_q$ too : every algebraic relations between thetas functions is valid over $\mathbb{F}_q$.
- To use the isogeny theorem, we still need to find an "algebraic" definition of Ω. In "On equations defining abelian varieties", Mumford show that the moduli space to consider is $(A, \mathcal{L}, G_\Theta)$, the set of abelian varieties marked with a theta-structure.
- Remember our theta function $\theta(z, \Omega)$. We can vary z and get the coordinate of the corresponding point of the torus, but we can also vary Ω and get a coordinate corresponding to the variety. So to get a coordinate on the set of abelian varieties, we need to find a way to associate a canonical point z_A to each variety A, and then evaluate $\theta(z_A, \Omega_A)$. Of course we will take $z_A = 0_A$.

The moduli space 1

- We will use the isogeny theorem to compute isogenies. We have stated it over $\mathbb{C}$, but it works over $\mathbb{F}_q$ too : every algebraic relations between thetas functions is valid over $\mathbb{F}_q$.
- To use the isogeny theorem, we still need to find an "algebraic" definition of Ω. In "On equations defining abelian varieties", Mumford show that the moduli space to consider is $(A, \mathcal{L}, G_\Theta)$, the set of abelian varieties marked with a theta-structure.
- Remember our theta function $\theta(z, \Omega)$. We can vary z and get the coordinate of the corresponding point of the torus, but we can also vary Ω and get a coordinate corresponding to the variety. So to get a coordinate on the set of abelian varieties, we need to find a way to associate a canonical point z_A to each variety A, and then evaluate $\theta(z_A, \Omega_A)$. Of course we will take $z_A = 0_A$.

The moduli space 1

- We will use the isogeny theorem to compute isogenies. We have stated it over $\mathbb{C}$, but it works over $\mathbb{F}_q$ too : every algebraic relations between thetas functions is valid over $\mathbb{F}_q$.
- To use the isogeny theorem, we still need to find an "algebraic" definition of Ω. In "On equations defining abelian varieties", Mumford show that the moduli space to consider is $(A, \mathcal{L}, G_\Theta)$, the set of abelian varieties marked with a theta-structure.
- Remember our theta function $\theta(z, \Omega)$. We can vary z and get the coordinate of the corresponding point of the torus, but we can also vary Ω and get a coordinate corresponding to the variety. So to get a coordinate on the set of abelian varieties, we need to find a way to associate a canonical point z_A to each variety A, and then evaluate $\theta(z_A, \Omega_A)$. Of course we will take $z_A = 0_A$.

The moduli space 2

Définition

Les A be an abelian variety, and θ_i be the theta functions of level l. The point $(\theta_0(0) : \theta_1(0) : \ldots : \theta_{l-1}(0)) \in \mathbb{P}^{l^g-1}$ is called the theta constant of level l of A.

Théorème

Mumford : If $8|l$ then the theta constants of level l form an open dense subset of the variety

$$\sum_{t\in\mathbb{Z}_2} q(x+t)q(y+t) \sum_{t\in\mathbb{Z}_2} q(u+t)q(v+t) = \sum_{t\in\mathbb{Z}_2} q(x+z+t)q(y+z+t) \sum_{t\in\mathbb{Z}_2} q(u+z+t)q(v+z+t)$$

$$q(x) = q(-x)$$

where $\mathbb{Z}_2 \subset \mathbb{Z}_l$ are the points of 2-torsion, and $x, y, u, v \in \mathbb{Z}_l, x + y + u + v = -2z$.

The moduli space 2

Définition

Les A be an abelian variety, and θ_i be the theta functions of level l. The point $(\theta_0(0) : \theta_1(0) : \ldots : \theta_{l-1}(0)) \in \mathbb{P}^{l^g-1}$ is called the theta constant of level l of A.

Théorème

Mumford : If $8|l$ then the theta constants of level l form an open dense subset of the variety

$$\sum_{t\in\mathbb{Z}_2} q(x+t)q(y+t) \sum_{t\in\mathbb{Z}_2} q(u+t)q(v+t) = \sum_{t\in\mathbb{Z}_2} q(x+z+t)q(y+z+t) \sum_{t\in\mathbb{Z}_2} q(u+z+t)q(v+z+t)$$

$$q(x) = q(-x)$$

where $\mathbb{Z}_2 \subset \mathbb{Z}_l$ are the points of 2-torsion, and $x, y, u, v \in \mathbb{Z}_l, x+y+u+v = -2z$.

The moduli space 3

Suppose we start with a theta constant $(q(i))_{i\in\mathbb{Z}_l}$, Mumford theorem tells us that if $8|l$ the matrix Ω is uniquely determined. Let θ_i be the corresponding theta functions of level l, we have to find an algebraic characterisations of θ_i. If we use the embedding to the projective space they provide, we can see them as coordinate on the projective space together with every algebraic relations between the (θ_i). A basis of these relations is given by Riemann theta relations :

Théorème

Riemann Relations : if $4|l$ and $(q(0):\ldots,q(l-1))$ is a theta constant of level l, then the corresponding abelian variety has equations :

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

Computing isogenies, first try

- To compute an isogeny, we can try to find points of the modular space, this will give theta constants of level l : $(q(0) : q(1) : \ldots : q(l-1))$, and then we apply the isogeny theorem to get an isogeny of degree l. In fact, to get the equation of the isogenous variety, we have to go from level $4l$ to level 4.
- But we want to find theta constants corresponding to our abelian variety.
- If we start with the Jacobian J of an hyperelliptic curve $C : y^2 = f(x)$, then Thomae's formulas relate the theta constants of level 4 of J with the roots of f.

Computing isogenies, first try

- To compute an isogeny, we can try to find points of the modular space, this will give theta constants of level $l : (q(0) : q(1) : \ldots : q(l-1))$, and then we apply the isogeny theorem to get an isogeny of degree l. In fact, to get the equation of the isogenous variety, we have to go from level $4l$ to level 4.
- But we want to find theta constants corresponding to our abelian variety.
- If we start with the Jacobian J of an hyperelliptic curve $C : y^2 = f(x)$, then Thomae's formulas relate the theta constants of level 4 of J with the roots of f.

Computing isogenies, first try

- To compute an isogeny, we can try to find points of the modular space, this will give theta constants of level $l : (q(0) : q(1) : \ldots : q(l-1))$, and then we apply the isogeny theorem to get an isogeny of degree l. In fact, to get the equation of the isogenous variety, we have to go from level $4l$ to level 4.
- But we want to find theta constants corresponding to our abelian variety.
- If we start with the Jacobian J of an hyperelliptic curve $C : y^2 = f(x)$, then Thomae's formulas relate the theta constants of level 4 of J with the roots of f.

Computing isogenies, second try

- We proceed backwards. We start with our theta constants of level 4 corresponding to our variety $B : (b(0) : b(1) : b(2) : b(3))$. We try to find an abelian variety A and an isogeny $f : A \to B$ of degree l. We only need to find the theta constants of A of degree $4l : (a(0) : \ldots : a(4l-1))$.
- The isogeny theorem says that $a(l * i) = b(i)$ for every $i \in \mathbb{Z}_4$. We plug these equations in the moduli space of abelian varieties of level $4l$, we obtain a zero dimensional variety and use Gröbner Basis to find the solutions.
- We obtain some degenerate solutions, but they are easy to detect.

Computing isogenies, second try

- We proceed backwards. We start with our theta constants of level 4 corresponding to our variety $B : (b(0) : b(1) : b(2) : b(3))$. We try to find an abelian variety A and an isogeny $f : A \rightarrow B$ of degree l. We only need to find the theta constants of A of degree $4l : (a(0) : \ldots : a(4l-1))$.
- The isogeny theorem says that $a(l * i) = b(i)$ for every $i \in \mathbb{Z}_4$. We plug these equations in the moduli space of abelian varieties of level $4l$, we obtain a zero dimensional variety and use Gröbner Basis to find the solutions.
- We obtain some degenerate solutions, but they are easy to detect.

Computing isogenies, second try

- We proceed backwards. We start with our theta constants of level 4 corresponding to our variety $B : (b(0) : b(1) : b(2) : b(3))$. We try to find an abelian variety A and an isogeny $f : A \to B$ of degree l. We only need to find the theta constants of A of degree $4l : (a(0) : \ldots : a(4l-1))$.
- The isogeny theorem says that $a(l * i) = b(i)$ for every $i \in \mathbb{Z}_4$. We plug these equations in the moduli space of abelian varieties of level $4l$, we obtain a zero dimensional variety and use Gröbner Basis to find the solutions.
- We obtain some degenerate solutions, but they are easy to detect.

Remarks

- We have an isogeny $f : A \to B$. If we just want to compute the equation of a subgroup of order l^g of B, then we can take the image of the points of l-torsions of A.
- If we need to find an isogeny $g : B \to A$, we can take the dual of f. To compute g, if $b \in B$, we take any antecedent $a \in f^{-1}(b)$ (there are l^g such antecedents), and multiply by l. If we take b to be the generic point, this give the equations of g. In practice this is very fast.
- This isogeny $B \to A$ goes from a level 4 variety to a level $4l$ variety. If we want the codomain to be of level 4 (to reduce the number of variables), one can proceed like this : in the isogeny theorem, we had to choose between $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$ as our kernel. If we take $l\mathbb{Z}^n$, we obtain a new isogeny theorem, and an isogeny : $h : A \to C$. The composition hg give an l^2 isogeny between two varieties of level 4.

Remarks

- We have an isogeny $f : A \to B$. If we just want to compute the equation of a subgroup of order l^g of B, then we can take the image of the points of l-torsions of A.
- If we need to find an isogeny $g : B \to A$, we can take the dual of f. To compute g, if $b \in B$, we take any antecedent $a \in f^{-1}(b)$ (there are l^g such antecedents), and multiply by l. If we take b to be the generic point, this give the equations of g. In practice this is very fast.
- This isogeny $B \to A$ goes from a level 4 variety to a level $4l$ variety. If we want the codomain to be of level 4 (to reduce the number of variables), one can proceed like this : in the isogeny theorem, we had to choose between $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$ as our kernel. If we take $l\mathbb{Z}^n$, we obtain a new isogeny theorem, and an isogeny : $h : A \to C$. The composition hg give an l^2 isogeny between two varieties of level 4.

Remarks

- We have an isogeny $f : A \to B$. If we just want to compute the equation of a subgroup of order l^g of B, then we can take the image of the points of l-torsions of A.
- If we need to find an isogeny $g : B \to A$, we can take the dual of f. To compute g, if $b \in B$, we take any antecedent $a \in f^{-1}(b)$ (there are l^g such antecedents), and multiply by l. If we take b to be the generic point, this give the equations of g. In practice this is very fast.
- This isogeny $B \to A$ goes from a level 4 variety to a level $4l$ variety. If we want the codomain to be of level 4 (to reduce the number of variables), one can proceed like this : in the isogeny theorem, we had to choose between $1/l\mathbb{Z}^n$ and $1/l\Omega\mathbb{Z}^n$ as our kernel. If we take $l\mathbb{Z}^n$, we obtain a new isogeny theorem, and an isogeny : $h : A \to C$. The composition hg give an l^2 isogeny between two varieties of level 4.

Perspective

- The blocking point of the algorithm is to compute the theta constants of A of level $4l$ when we plug the theta constants of B of level 4.
- Can we use the commutator pairing and the action of the points of $4l$-torsion to speedup the Gröbner Basis ? We have a big polynomial system, and each class of isogeny give many solutions according to the action of the points of $4l$-torsions. It is easy to explicit the action and get every such solutions in one isogeny class. This mean we have to solve a polynomial system highly symmetrical, but how can we use the symmetry ?
- Can we compute the commutator pairing of level l with theta functions of lower level ?

Perspective

- The blocking point of the algorithm is to compute the theta constants of A of level $4l$ when we plug the theta constants of B of level 4.
- Can we use the commutator pairing and the action of the points of $4l$-torsion to speedup the Gröbner Basis ? We have a big polynomial system, and each class of isogeny give many solutions according to the action of the points of $4l$-torsions. It is easy to explicit the action and get every such solutions in one isogeny class. This mean we have to solve a polynomial system highly symmetrical, but how can we use the symmetry ?
- Can we compute the commutator pairing of level l with theta functions of lower level ?

Perspective

- The blocking point of the algorithm is to compute the theta constants of A of level $4l$ when we plug the theta constants of B of level 4.
- Can we use the commutator pairing and the action of the points of $4l$-torsion to speedup the Gröbner Basis ? We have a big polynomial system, and each class of isogeny give many solutions according to the action of the points of $4l$-torsions. It is easy to explicit the action and get every such solutions in one isogeny class. This mean we have to solve a polynomial system highly symmetrical, but how can we use the symmetry ?
- Can we compute the commutator pairing of level l with theta functions of lower level ?