Multiplication complexe et discriminants

Gaëtan BISSON

LORIA, Nancy, France

TU/e, Eindhoven, Pays-Bas

Première partie

Multiplication complexe

Variétés abéliennes

Une *variété abélienne* est un groupe algébrique complet connexe.

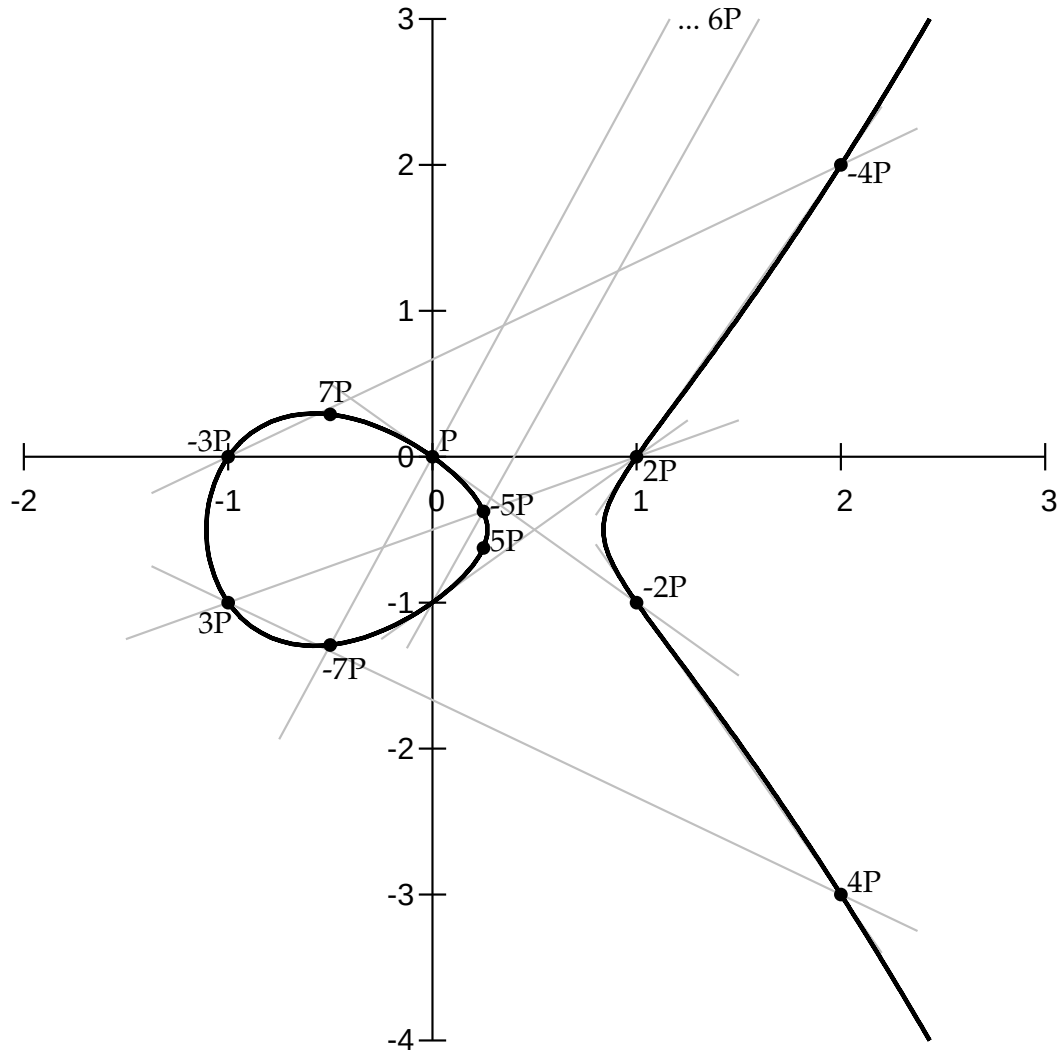
Variétés abéliennes

Une *variété abélienne* est un groupe algébrique complet connexe.

Pour le cryptographe, c'est une famille de groupes :

- où l'on sait calculer très efficacement ;

Variétés abéliennes



Variétés abéliennes

Une *variété abélienne* est un groupe algébrique complet connexe.

Pour le cryptographe, c'est une famille de groupes :

- où l'on sait calculer très efficacement ;
- résistants au problème du logarithme discret.

On voudrait donc **construire des variétés abéliennes**
avec des paramètres fixés, e.g. l'ordre du groupe.

Anneaux d'endomorphismes

Une variété abélienne A a des endomorphismes :

- les *multiplications scalaires*, $P \mapsto mP = \underbrace{P + \cdots + P}_{m \text{ fois}}$;

Anneaux d'endomorphismes

Une variété abélienne A a des endomorphismes :

- les *multiplications scalaires*, $P \mapsto mP = \underbrace{P + \cdots + P}_{m \text{ fois}}$;
- sur les corps finis, l'endomorphisme de Frobenius.

Cela nous donne une partie de son anneau d'endomorphismes :

$$\mathbb{Z}\left[\text{Frob}\right] \subseteq \text{End}(A).$$

Anneaux d'endomorphismes

Une variété abélienne A a des endomorphismes :

- les *multiplications scalaires*, $P \mapsto mP = \underbrace{P + \cdots + P}_{m \text{ fois}}$;
- sur les corps finis, l'endomorphisme de Frobenius.

Cela nous donne une partie de son anneau d'endomorphismes :

$$\mathbb{Z}\left[\mathrm{Frob}\right] \subseteq \mathrm{End}(A).$$

Notant g la dimension de A, on dira, lorsque $\mathrm{End}(A) \otimes \mathbb{Q}$ contient un corps (commutatif) k de degré $2g$, que A a *multiplication complexe* par l'ordre $\mathfrak{o} = k \cap \mathrm{End}(A)$.

Anneaux d'endomorphismes

Si A est simple, k est une extension quadratique imaginaire d'un corps de nombre totalement réel (de degré g), un *corps CM*.

Sinon, A est isogène à une puissance B^s d'une variété abélienne simple et l'on a ainsi $\mathrm{End}(A) \otimes \mathbb{Q} \simeq \mathrm{Mat}_s\left(\mathrm{End}(B) \otimes \mathbb{Q}\right)$.

Anneaux d'endomorphismes

Si A est simple, k est une extension quadratique imaginaire d'un corps de nombre totalement réel (de degré g), un *corps CM*.

Sinon, A est isogène à une puissance B^s d'une variété abélienne simple et l'on a ainsi $\mathrm{End}(A) \otimes \mathbb{Q} \simeq \mathrm{Mat}_s\left(\mathrm{End}(B) \otimes \mathbb{Q}\right)$.

Par exemple, pour une variété simple et ordinaire sur $\mathbb{F}_q$ on a

$$\mathbb{Z}\left[\mathrm{Frob}\right] \subseteq \mathrm{End}(A) = \mathfrak{o} \subseteq \mathscr{O}_k \quad \text{où} \quad k = \mathbb{Q}\left(\mathrm{Frob}\right),$$

et ces variétés ont toutes multiplication complexe.

Propriétés de réduction

Si A a bonne réduction en $\mathfrak{p}$, on a une injection

$$\mathrm{End}(A) \to \mathrm{End}\left(A_{\mathfrak{p}}\right) ;$$

ainsi, si A a multiplication complexe par un certain corps k, il en va de même pour $A_{\mathfrak{p}}$.

Toutefois, l'ordre peut ne pas être préservé.

La méthode CM

La *méthode CM* permet de **construire des variétés abéliennes de polynôme de Frobenius χ donné**. Elle exploite pour cela les propriétés de réduction en s'appuyant sur l'ordre CM.
(L'ordre $\mathfrak{o}$ doit contenir un élément de polynôme caractéristique χ.)

On peut ainsi contrôler tous les paramètres de notre variété, e.g.

$$\#A = \chi(1), \quad q^g = \chi(0).$$

La méthode CM

La *méthode CM* permet de **construire des variétés abéliennes de polynôme de Frobenius χ donné**. Elle exploite pour cela les propriétés de réduction en s'appuyant sur l'ordre CM.
(L'ordre $\mathfrak{o}$ doit contenir un élément de polynôme caractéristique χ.)

On peut ainsi contrôler tous les paramètres de notre variété, e.g.

$$\#A = \chi(1), \quad q^g = \chi(0).$$

À l'heure actuelle, elle est en œuvre pour :

- $g = 1$ et $h(\mathfrak{o}) \leqslant 10^6$;
- $g = 2$ et $h(\mathfrak{o}) \leqslant 10^3$;
- $g \geqslant 3$ dans de rares cas.

Deuxième partie

Courbes elliptiques, i.e. $g = 1$

Concrètement :

Sur $\mathbb{F}_q$, une courbe elliptique a une équation explicite :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Concrètement :

Sur $\mathbb{F}_q$, une courbe elliptique a une équation explicite :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

On a $k = \mathbb{Q}\left(\sqrt{d}\right)$ pour un certain discriminant fondamental $d < 0$, d'où

$$\text{Frob} = \frac{1}{2}\left(t + y\sqrt{d}\right) \quad \text{avec} \quad 4q = t^2 - dy^2.$$

Concrètement :

Sur $\mathbb{F}_q$, une courbe elliptique a une équation explicite :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

On a $k = \mathbb{Q}\left(\sqrt{d}\right)$ pour un certain discriminant fondamental $d < 0$, d'où

$$\text{Frob} = \frac{1}{2}\left(t + y\sqrt{d}\right) \quad \text{avec} \quad 4q = t^2 - dy^2.$$

Et chaque ordre est uniquement déterminé par son conducteur :

$$\underbrace{\mathbb{Z}\left[\text{Frob}\right]}_{\mathbb{Z}+y\mathcal{O}_k} \subseteq \underbrace{\text{End} = \mathfrak{o}}_{\mathbb{Z}+n\mathcal{O}_k} \subseteq \mathcal{O}_k.$$

Une ambigüité

L'équation $4q = t^2 - dy^2$ ne permet pas de déterminer End exactement : **son conducteur n peut être n'importe quel diviseur de y.**

Une ambigüité

L'équation $4q = t^2 - dy^2$ ne permet pas de déterminer End exactement : **son conducteur n peut être n'importe quel diviseur de y.**

AVANTAGE (B.-SATOH [1]) : Pour des paramètres (q, t) donnés, on peut construire autant de courbes que $4q - t^2$ a de diviseurs carrés inférieurs à 10^{12}.

Une ambigüité

L'équation $4q = t^2 - dy^2$ ne permet pas de déterminer End exactement : **son conducteur n peut être n'importe quel diviseur de y.**

AVANTAGE (B.-SATOH [1]) : Pour des paramètres (q, t) donnés, on peut construire autant de courbes que $4q - t^2$ a de diviseurs carrés inférieurs à 10^{12}.

INCONVÉNIENT : Étant donné une courbe elliptique $\mathscr{E}$, comment déterminer le conducteur de son anneau d'endomorphismes ?

Troisième partie

Calcul du conducteur

Quelques isomorphismes

formes quadratiques binaires primitives définies positives avec discriminant n^2d à équivalence près	idéaux fractionnaires de $\mathfrak{o}_{n^2d}$ modulo idéaux principaux	courbes elliptiques avec CM par $\mathfrak{o}_{n^2d}$ à isomorphisme près
$ax^2+bxy+cy^2$	$\left\langle a, \frac{1}{2}\left(-b+n\sqrt{d}\right)\right\rangle$	$\mathbb{C}^2/\left\langle a, \frac{1}{2}\left(-b+n\sqrt{d}\right)\right\rangle$

Quelques isomorphismes

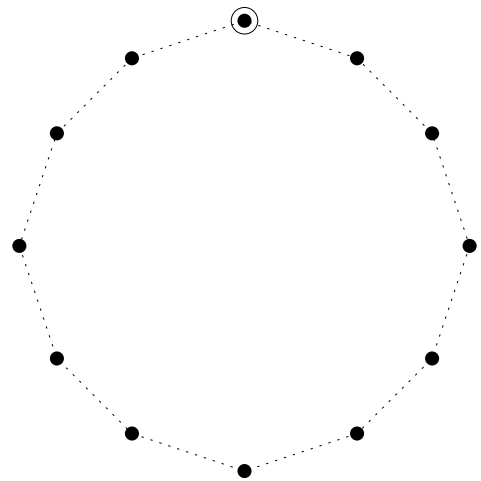
formes quadratiques binaires primitives définies positives avec discriminant n^2d à équivalence près	idéaux fractionnaires de $\mathfrak{o}_{n^2d}$ modulo idéaux principaux	courbes elliptiques avec CM par $\mathfrak{o}_{n^2d}$ à isomorphisme près
$ax^2+bxy+cy^2$	$\left\langle a, \frac{1}{2}\left(-b+n\sqrt{d}\right)\right\rangle$	$\mathbb{C}^2/\left\langle a, \frac{1}{2}\left(-b+n\sqrt{d}\right)\right\rangle$

---

composition par la forme première de norme m	multiplication par les idéaux de norme m	m-isogénies

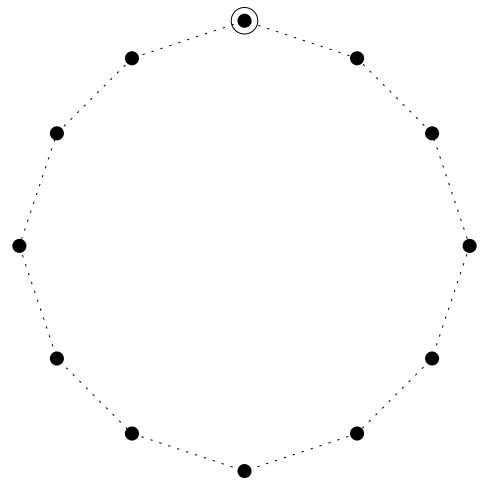
Isogénies

Si m premier ne divise pas $\left[\mathcal{O}_k : \mathbb{Z}\left[\mathrm{Frob}\right]\right]$ et que $\left(\frac{d}{m}\right) = 1$,
il y a deux m-isogénies partant de $\mathscr{E}$; elles mènent toutes deux à des courbes de même anneau d'endomorphismes.
On a ainsi un cycle, et sa longueur divise le nombre de classes.



Isogénies

Si m premier ne divise pas $\left[\mathcal{O}_k : \mathbb{Z}\left[\mathrm{Frob}\right]\right]$ et que $\left(\frac{d}{m}\right) = 1$,
il y a deux m-isogénies partant de $\mathscr{E}$; elles mènent toutes deux
à des courbes de même anneau d'endomorphismes.
On a ainsi un cycle, et sa longueur divise le nombre de classes.



Algorithmiquement, pour m petit, on peut parcourir ce cycle
rapidement en utilisant le *polynôme modulaire* $\Phi_m(x, y)$.

Algorithme

ALGORITHME (SUTHERLAND [2]) :

1. Trouver un premier m convenable :
   - petit, non diviseur de $\left[\mathcal{O}_k : \mathbb{Z}\left[\mathrm{Frob}\right]\right]$ et tel que $\left(\frac{d}{m}\right) = 1$.
   - Calculer les ordres des formes premières de norme m et discriminants $n^2 d$ (pour $n \mid y$) et s'assurer qu'ils sont distincts.

Algorithme

ALGORITHME (SUTHERLAND [2]) :

1. Trouver un premier m convenable :
   - petit, non diviseur de $\left[\mathcal{O}_k : \mathbb{Z}\left[\text{Frob}\right]\right]$ et tel que $\left(\frac{d}{m}\right) = 1$.
   - Calculer les ordres des formes premières de norme m et discriminants $n^2 d$ (pour $n \mid y$) et s'assurer qu'ils sont distincts.
2. Calculer la longueur du cycle contenant $\mathscr{E}$:
   - Calculer le polynôme modulaire et le réduire dans $\mathbb{F}_q[x, y]$.
   - L'évaluer autant de fois que nécessaire pour revenir à $\mathscr{E}$.

Algorithme

ALGORITHME (SUTHERLAND [2]) :

1. Trouver un premier m convenable :
   - petit, non diviseur de $\left[\mathcal{O}_k : \mathbb{Z}\left[\mathrm{Frob}\right]\right]$ et tel que $\left(\frac{d}{m}\right) = 1$.
   - Calculer les ordres des formes premières de norme m et discriminants $n^2 d$ (pour $n \mid y$) et s'assurer qu'ils sont distincts.
2. Calculer la longueur du cycle contenant $\mathscr{E}$:
   - Calculer le polynôme modulaire et le réduire dans $\mathbb{F}_q[x, y]$.
   - L'évaluer autant de fois que nécessaire pour revenir à $\mathscr{E}$.
3. Le conducteur n est celui dont la forme première a pour ordre la longueur du cycle.

C'EST TOUT !

Merci pour votre attention.

[1] G. B. et T. Satoh
"More Discriminants with the Brezing-Weng Method"
À paraître dans *Indocrypt'08*.

[2] A. Sutherland
Communication privée