Soutenance de thèse:

Équations modulaires en dimension supérieure, applications au calcul d'isogénies et au comptage de points

---

Jean Kieffer

Directeur de thèse: Damien Robert
Co-encadrant: Aurel Page
Équipe LFANT, Institut de Mathématiques de Bordeaux

Mardi 13 juillet 2021

1. Introduction : courbes elliptiques et cryptographie

2. Comptage de points en dimension supérieure

3. Définition des équations modulaires, exemples

4. Bornes de degré et de hauteur

5. Calcul d'isogénies pour les surfaces abéliennes

6. Algorithmes d'évaluation des équations modulaires

Introduction : courbes elliptiques et cryptographie

Courbes elliptiques

Soit k un corps[1]. Une courbe elliptique E sur k est donnée par une équation de la forme :

$$E : y^2 = x^3 + ax + b$$

où $a, b \in k$ et $4a^3 + 27b^2 \neq 0$. Un point supplémentaire "à l'infini" : E est une courbe projective lisse.

1. car $k \notin \{2, 3\}$.

Courbes elliptiques

Soit k un corps[1]. Une courbe elliptique E sur k est donnée par une équation de la forme :

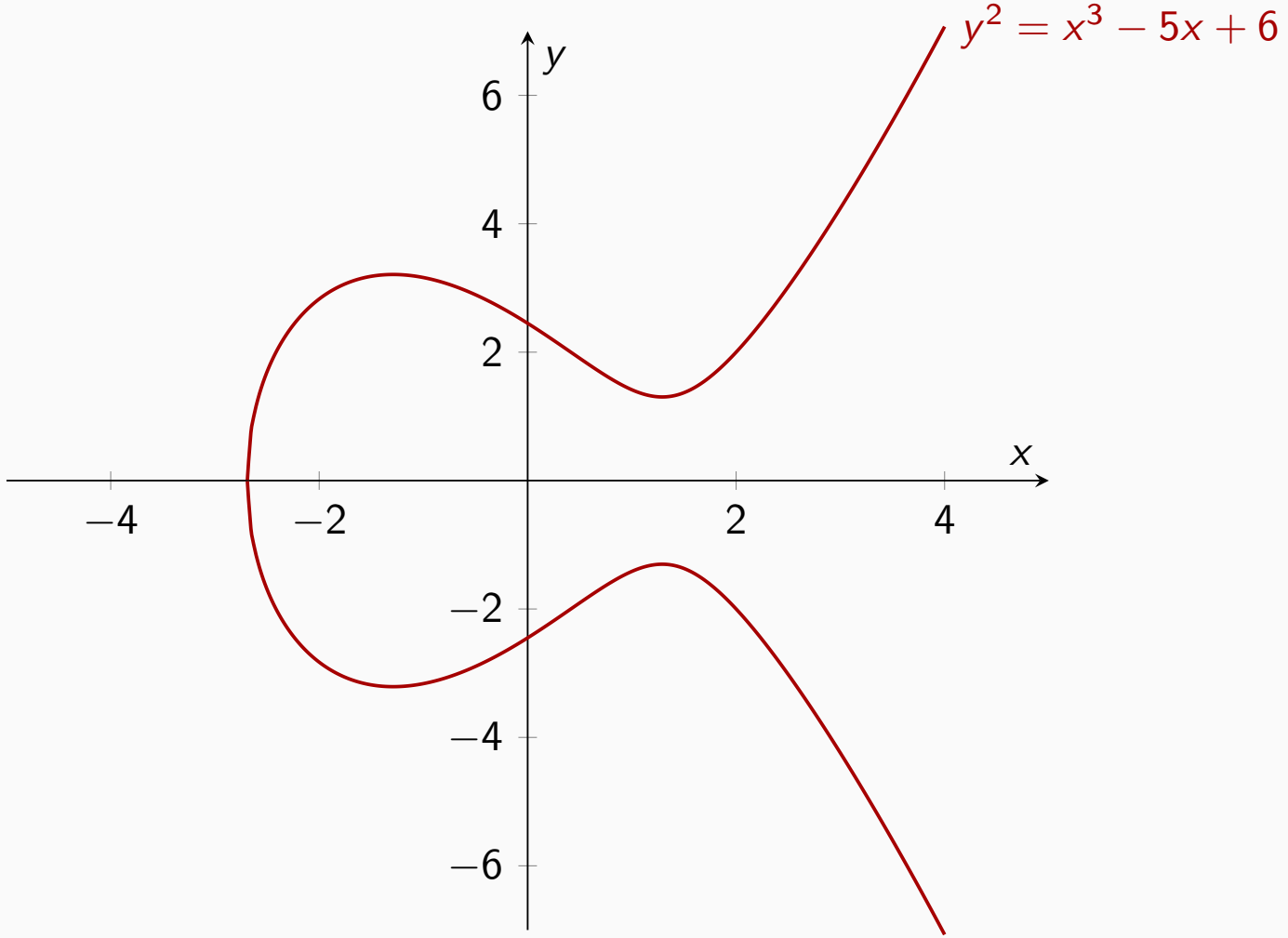
$$E : y^2 = x^3 + ax + b$$

où $a, b \in k$ et $4a^3 + 27b^2 \neq 0$. Un point supplémentaire "à l'infini" : E est une courbe projective lisse.

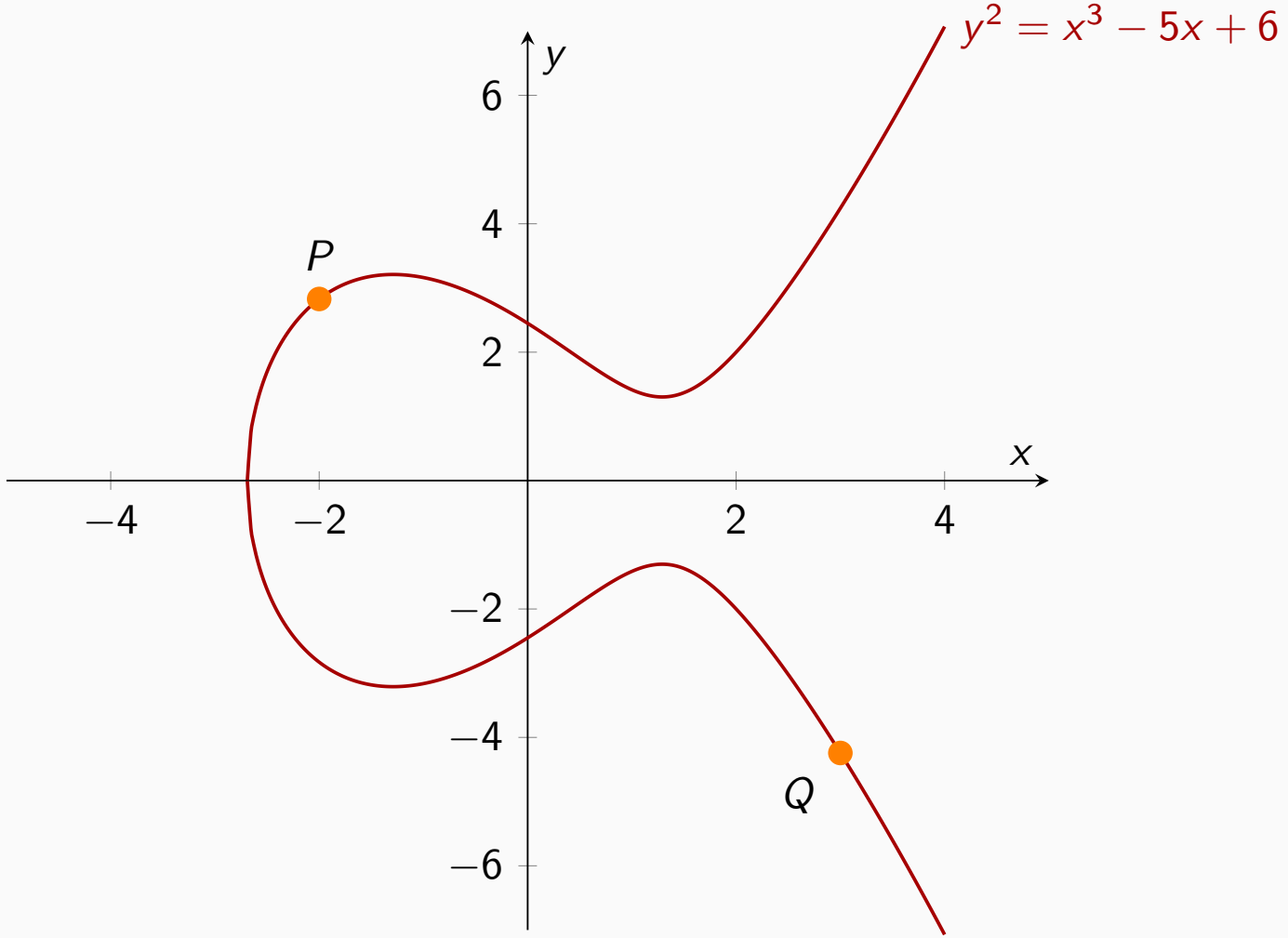
On dessine souvent avec $k = \mathbb{R}$. Mais $k = \mathbb{C}$, ou $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sont également possibles.

1. car $k \notin \{2, 3\}$.

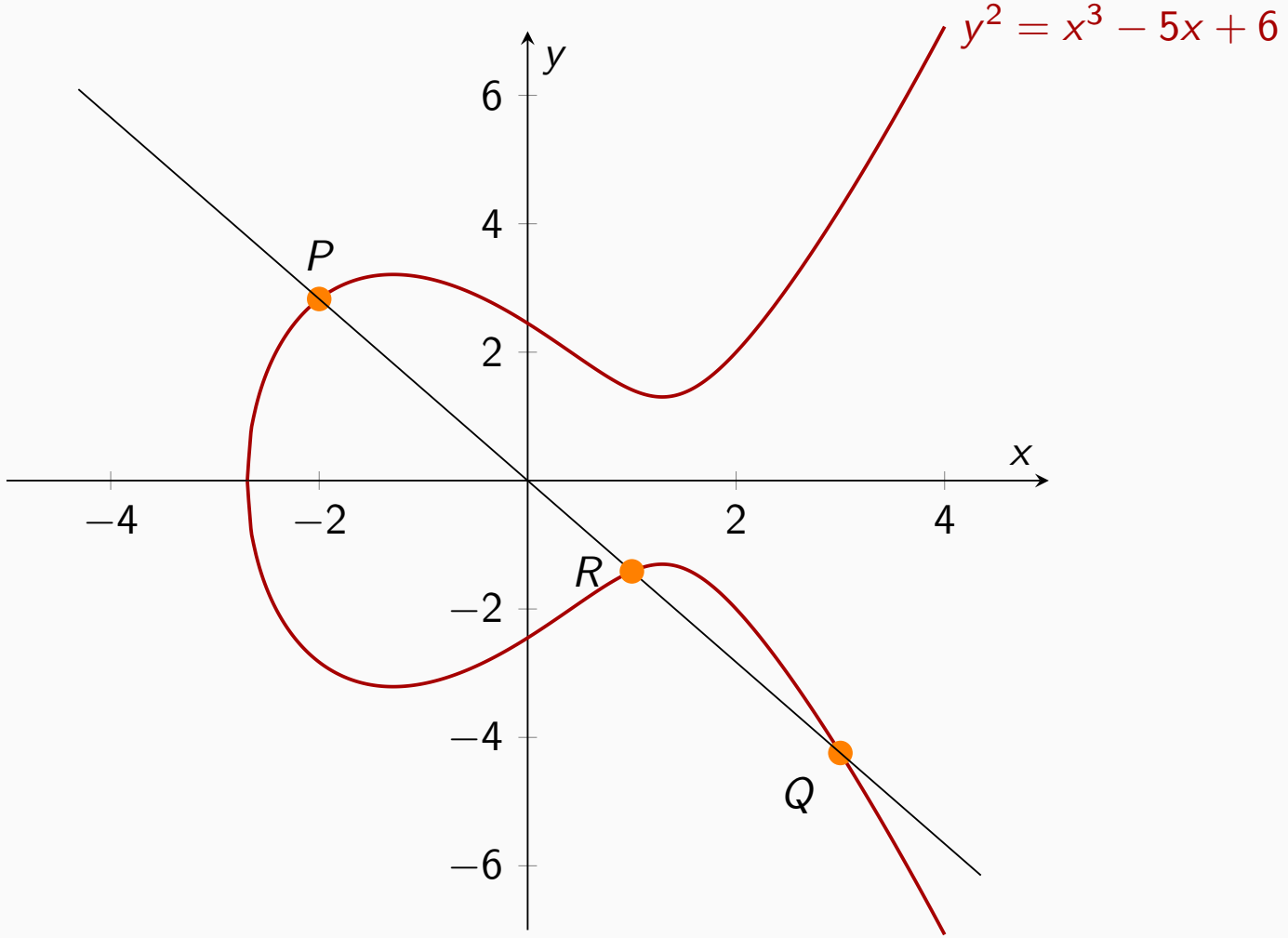
Loi de groupe



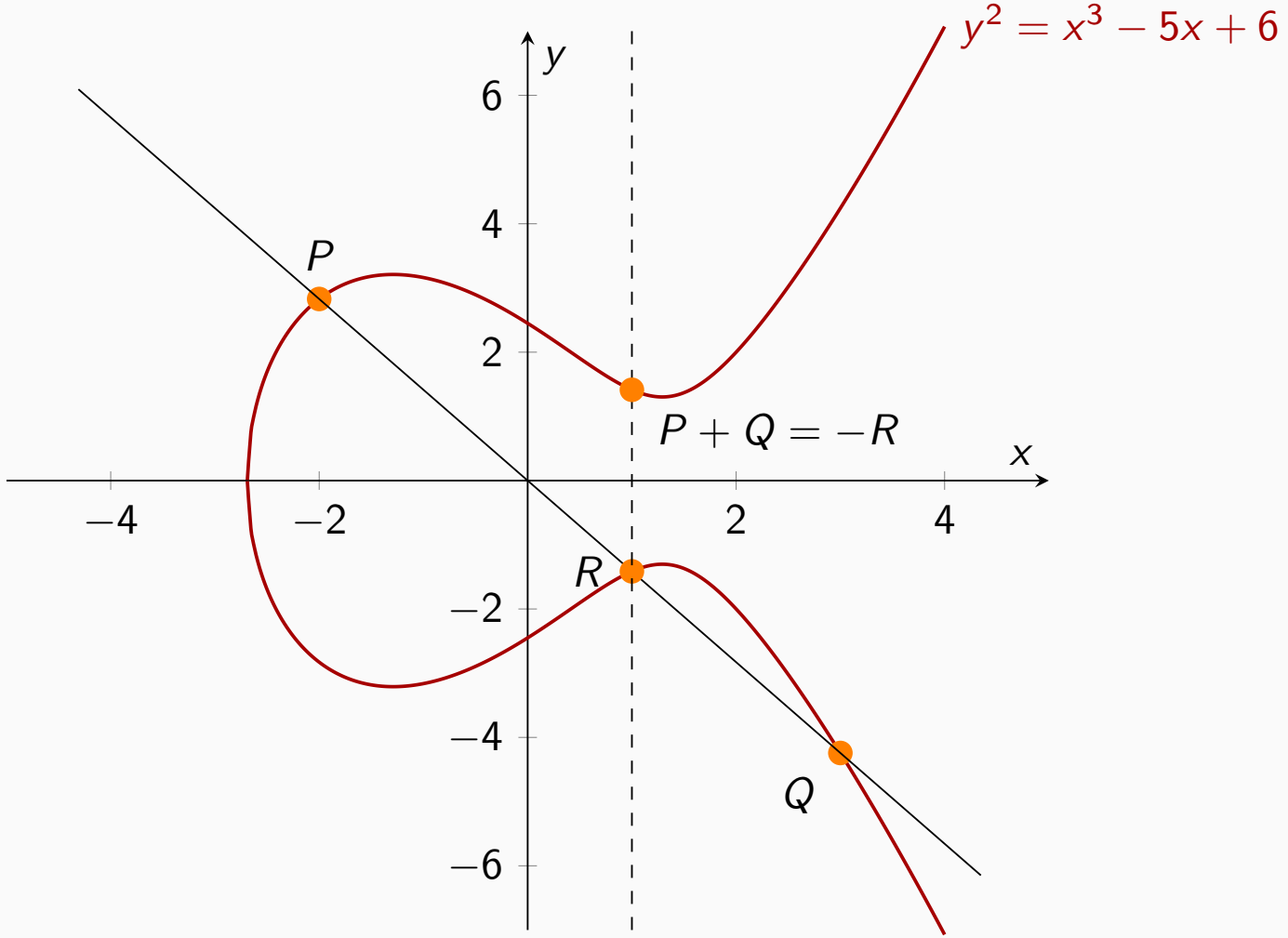
Loi de groupe



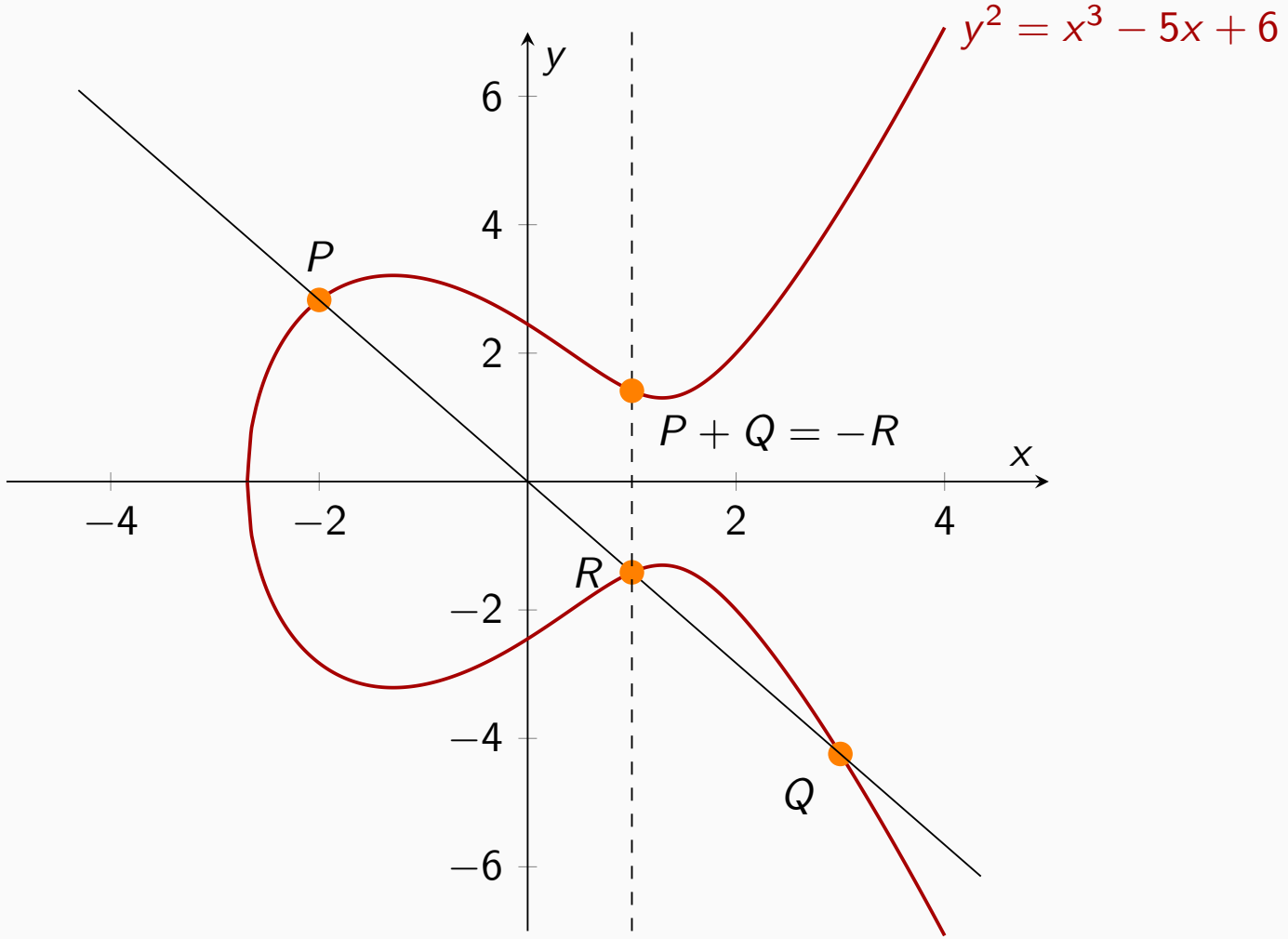
Loi de groupe



Loi de groupe



Loi de groupe



L'existence d'une loi de groupe caractérise les courbes elliptiques.

Lorsque k est un corps fini, $E(k)$ est un groupe abélien fini.

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice **Bob**

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice	**Bob**
$a \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$	$b \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice	**Bob**
$a \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$	$b \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$
Calcule g^a	Calcule g^b

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice		**Bob**
$a \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$	$\xrightarrow{g^a}$	$b \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$
Calcule g^a	$\xleftarrow{g^b}$	Calcule g^b

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice		**Bob**
$a \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$	$\xrightarrow{g^a}$	$b \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$
Calcule g^a	$\xleftarrow{g^b}$	Calcule g^b
$g^{ab} = (g^b)^a$		$g^{ab} = (g^a)^b$.

Le protocole de Diffie–Hellman (1976)

Alice et Bob établissent un secret commun malgré un canal de communication non sécurisé.

Soient $(G, \cdot)$ un groupe cyclique d'ordre n, et $g \in G$ un générateur.

Alice		**Bob**
$a \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$	$\xrightarrow{g^a}$	$b \leftarrow \text{Random}(\mathbb{Z}/n\mathbb{Z})$
Calcule g^a	$\xleftarrow{g^b}$	Calcule g^b
$g^{ab} = (g^b)^a$		$g^{ab} = (g^a)^b$.

Un attaquant voit g, g^a et g^b, mais calculer g^{ab} n'est pas évident. Une méthode consiste à résoudre le

Problème du logarithme discret dans G :

Étant donné g et g^a, calculer a.

Utilisation des courbes elliptiques

Rappel : $n = \#G$.

- Meilleure attaque générique : coûte $\sqrt{p} \cdot \text{poly}(\log n)$ où p est le plus grand facteur premier de n. Si n est premier, temps exponentiel en $\log n$. Exemple : $G = E(\mathbb{F}_p)$ pour E convenable.

Utilisation des courbes elliptiques

Rappel : $n = \#G$.

- Meilleure attaque générique : coûte $\sqrt{p} \cdot \mathrm{poly}(\log n)$ où p est le plus grand facteur premier de n. Si n est premier, temps exponentiel en $\log n$. Exemple : $G = E(\mathbb{F}_p)$ pour E convenable.
- Attaques spécifiques : $G = \mathbb{Z}/n\mathbb{Z}$ (temps polynomial, inutilisable en cryptographie) ; $G = \mathbb{F}_p^\times$ (temps sous-exponentiel).

Utilisation des courbes elliptiques

Rappel : $n = \#G$.

- Meilleure attaque générique : coûte $\sqrt{p} \cdot \mathrm{poly}(\log n)$ où p est le plus grand facteur premier de n. Si n est premier, temps exponentiel en $\log n$. Exemple : $G = E(\mathbb{F}_p)$ pour E convenable.
- Attaques spécifiques : $G = \mathbb{Z}/n\mathbb{Z}$ (temps polynomial, inutilisable en cryptographie) ; $G = \mathbb{F}_p^\times$ (temps sous-exponentiel).

À un niveau de sécurité donné, choisir $G = E(\mathbb{F}_p)$ réduit la taille des paramètres par rapport à $G = \mathbb{F}_p^\times$.
Dans la vie réelle : ECDSA, connexion à Internet ; $p \simeq 2^{256}$.

Le problème du comptage

Une façon de trouver E consiste à tirer des courbes candidates au hasard jusqu'à ce que $\#E(\mathbb{F}_p)$ soit premier.

Problème du comptage de points :

Étant donné une courbe elliptique E sur $\mathbb{F}_p$,
calculer son nombre de points $\#E(\mathbb{F}_p)$.

Le problème du comptage

Une façon de trouver E consiste à tirer des courbes candidates au hasard jusqu'à ce que $\#E(\mathbb{F}_p)$ soit premier.

Problème du comptage de points :

Étant donné une courbe elliptique E sur $\mathbb{F}_p$,
calculer son nombre de points $\#E(\mathbb{F}_p)$.

- Algorithme de Schoof (1985) : temps polynomial $\widetilde{O}(\log^5 p)$.
  [Dans tout l'exposé : $\widetilde{O}(N) = O(N \log^C N)$ pour un certain C.]

Le problème du comptage

Une façon de trouver E consiste à tirer des courbes candidates au hasard jusqu'à ce que $\#E(\mathbb{F}_p)$ soit premier.

Problème du comptage de points :

Étant donné une courbe elliptique E sur $\mathbb{F}_p$,
calculer son nombre de points $\#E(\mathbb{F}_p)$.

- Algorithme de Schoof (1985) : temps polynomial $\widetilde{O}(\log^5 p)$.
  [Dans tout l'exposé : $\widetilde{O}(N) = O(N \log^C N)$ pour un certain C.]
- La méthode d'Elkies (90's) améliore cet algorithme et le rend utilisable en pratique : on atteint $\widetilde{O}(\log^4 p)$ en moyenne.

Principe de la méthode de Schoof

Soit ℓ un premier auxiliaire ($\ell \ll p$). Sous-groupe de ℓ-torsion de E :

$$E[\ell] = \left\{ P \in E(\overline{\mathbb{F}}_p) : \underbrace{P + \cdots + P}_{\ell \text{ fois}} = 0_E \right\} \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

muni d'une action du Frobenius : $(x, y) \mapsto (x^p, y^p)$.

Théorème (Hasse 30's)

- $\#E(\mathbb{F}_p) = p + 1 - t_E$, *où* $t_E \in \mathbb{Z}$ *est la trace du Frobenius.*
- $|t_E| \leq 2\sqrt{p}$.
- t_E *mod* ℓ *est la trace du Frobenius sur* $E[\ell]$.

On détermine $\#E(\mathbb{F}_p)$ mod ℓ en calculant l'action du Frobenius sur $E[\ell]$, pour plusieurs ℓ. On conclut à l'aide du théorème des restes chinois.

Principe de la méthode d'Elkies

Remplacer $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ par un sous-groupe $K \simeq \mathbb{Z}/\ell\mathbb{Z}$ stable par le Frobenius. K est le noyau d'une ℓ-isogénie définie sur $\mathbb{F}_p$:

$$\phi\colon E \to E' \simeq E/K.$$

Degré des polynômes manipulés : $O(\ell^2) \rightsquigarrow O(\ell)$.

Calcul de K

- Détection et calcul de ϕ en utilisant le polynôme modulaire elliptique $\Phi_\ell \in \mathbb{Z}[X, Y]$.

$$E, E' \ \ell\text{-isogènes} \iff \Phi_\ell(j(E), j(E')) = 0.$$

- Complexité : bornes de degré et de hauteur pour Φ_ℓ,

$$\deg_X(\Phi_\ell) = \ell + 1, \quad \deg_Y(\Phi_\ell) = \ell + 1, \quad h(\Phi_\ell) \sim 6\ell \log \ell,$$

combinées avec des algorithmes de calcul de Φ_ℓ quasi-linéaires (approximations complexes ou restes chinois).

But de la thèse

Ma thèse généralise la méthode d'Elkies lorsque l'on remplace E par une surface abélienne, i.e. une variété abélienne de dimension 2.

Comptage de points en dimension supérieure : état de l'art et contributions

Variétés abéliennes

Définitions

- Une variété abélienne A sur k est une variété projective qui admet une loi de groupe.
- Une polarisation sur A est une certaine isogénie $A \to A^\vee$. La polarisation est dite principale si c'est un isomorphisme.
- L'espace de modules (grossier) des variétés abéliennes principalement polarisées (p.p.) de dimension g est noté $\mathcal{A}_g$.

Exemples

- Courbe elliptique = variété abélienne de dimension 1. Il existe une polarisation principale naturelle.
- La Jacobienne d'une courbe lisse de genre g est une variété abélienne p.p. de dimension g.

Le polynôme caractéristique du Frobenius

Soit A une variété abélienne sur $\mathbb{F}_p$ de dimension g.
Si $\ell \neq p$: module de Tate $T_\ell(A) = \varprojlim_{n \to +\infty} A[\ell^n]$, isomorphe à $\mathbb{Z}_\ell^{2g}$.

Théorème (Weil 1948)

Il existe un polynôme $P_A \in \mathbb{Z}[X]$ tel que P_A est le polynôme caractéristique du Frobenius sur chaque $T_\ell(A)$ pour $\ell \neq p$. Les racines complexes de P_A sont de module $\sqrt{p}$. De plus $\#A(\mathbb{F}_p) = P_A(1)$.

Le problème du comptage

Déterminer $P_A \in \mathbb{Z}[X]$. Cas d'intérêt :

- Surface abélienne p.p. ($g = 2$)
- Surface abélienne p.p. à multiplication réelle par $\mathbb{Z}_F$, où F est un corps quadratique réel fixé.

État de l'art en dimension supérieure

- Méthode de Schoof : considérer l'action du Frobenius sur les sous-groupes de ℓ-torsion ou (si multiplication réelle) de β-torsion lorsque $\beta \in \mathbb{Z}_F$. Restes chinois.
- Les polynômes modulaires se généralisent pour les surfaces abéliennes p.p. :
  - équations modulaires de Siegel décrivant les ℓ-isogénies (de degré ℓ^2),
  - Si multiplication réelle par $\mathbb{Z}_F$: équations modulaires de Hilbert décrivant certaines isogénies cycliques de degré ℓ.

  Calculs d'exemples en petit niveau.

Contributions

- Cadre unifié pour l'étude des équations modulaires en dimension supérieure, utilisant les variétés de Shimura PEL.
- Bornes de degré et de hauteur pour les équations modulaires en fonction de leur niveau dans ce cadre général.

Contributions

- Cadre unifié pour l'étude des équations modulaires en dimension supérieure, utilisant les variétés de Shimura PEL.
- Bornes de degré et de hauteur pour les équations modulaires en fonction de leur niveau dans ce cadre général.

Cas des équations modulaires pour les surfaces abéliennes p.p. :

- Algorithme de calcul d'isogénies généralisant l'algorithme d'Elkies pour les courbes elliptiques.
- Étude d'un algorithme efficace d'évaluation à la volée à l'aide approximations complexes.

Contributions

- Cadre unifié pour l'étude des équations modulaires en dimension supérieure, utilisant les variétés de Shimura PEL.
- Bornes de degré et de hauteur pour les équations modulaires en fonction de leur niveau dans ce cadre général.

Cas des équations modulaires pour les surfaces abéliennes p.p. :

- Algorithme de calcul d'isogénies généralisant l'algorithme d'Elkies pour les courbes elliptiques.
- Étude d'un algorithme efficace d'évaluation à la volée à l'aide approximations complexes.

Par conséquent :

- La méthode d'Elkies est généralisée aux surfaces abéliennes p.p.
- D'autres applications algorithmiques des polynômes Φ_ℓ (marches dans les graphes d'isogénies,...) peuvent être généralisées en dimension deux, avec une complexité connue.

Améliorations de complexité

Coût, sous heuristiques, du comptage de points sur $\mathbb{F}_p$:

	Schoof	**Elkies**
Courbes elliptiques	$\widetilde{O}(\log^5 p)$	$\widetilde{O}(\log^4 p)$
Surfaces abéliennes p.p.	$\widetilde{O}(\log^8 p)$	$\widetilde{O}(\log^8 p)$
... de "petite hauteur" †	$\widetilde{O}(\log^8 p)$	$\widetilde{O}(\log^7 p)$
... avec multiplication réelle par $\mathbb{Z}_F$	$\widetilde{O}_F(\log^5 p)$	$\widetilde{O}_F(\log^4 p)$

† Les invariants peuvent être relevés sur un corps de nombre fixé avec hauteur $O(1)$.

Les heuristiques concernent :

- Le calcul rapide de thêta-constantes dans l'algorithme d'évaluation des équations modulaires.
- La distribution des premiers d'Elkies.

Définition des équations modulaires, exemples

Variétés de Shimura PEL

Espace de modules sur $\mathbb{C}$ pour les variétés abéliennes de dimension fixée g munies d'une structure PEL : polarisation, endomorphismes, niveau.

- $G =$ groupe d'automorphismes d'un $\mathbb{Q}$-espace vectoriel V muni d'une polarisation et d'endomorphismes.
- $K \subset G(\mathbb{A}_f)$ sous-groupe compact ouvert, où $\mathbb{A}_f$ désigne l'anneau des adèles finis de $\mathbb{Q}$. Encode la structure de niveau.
- Données à la place archimédienne : $G(\mathbb{R})_+ \subset G(\mathbb{R})$ défini par des conditions de connexité, et $G(\mathbb{Q})_+ = G(\mathbb{Q}) \cap G(\mathbb{R})_+$; enfin $K_\infty \subset G(\mathbb{R})_+$ compact maximal modulo le centre.

Variété de Shimura PEL :

$$\mathrm{Sh}_K = G(\mathbb{Q})_+ \backslash \big(G(\mathbb{R})_+ \times G(\mathbb{A}_f) \big) / (K_\infty \times K).$$

Composantes connexes : quotients d'espaces hermitiens symétriques.

Correspondances de Hecke

Soit $\delta \in G(\mathbb{A}_f)$. La correspondance de Hecke H_δ est définie par :

$$\begin{array}{ccc} \mathrm{Sh}_{K\cap\delta K\delta^{-1}} & \xrightarrow{[x,g]\mapsto[x,g\delta]} & \mathrm{Sh}_{\delta^{-1}K\delta\cap K} \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle p_2} \\ \mathrm{Sh}_K & & \mathrm{Sh}_K\,. \end{array}$$

Son image dans $\mathrm{Sh}_K \times \mathrm{Sh}_K$ est le lieu des variétés abéliennes avec structure PEL liées par une isogénie de type fixé par δ.

Quantités attachées :

- degré $d(\delta)$ ($\deg p_1 =$ nombre d'isogénies),
- degré d'isogénie $i(\delta)$.

Correspondances de Hecke

Soit $\delta \in G(\mathbb{A}_f)$. La correspondance de Hecke H_δ est définie par :

$$\begin{array}{ccc} \mathrm{Sh}_{K\cap\delta K\delta^{-1}} & \xrightarrow{[x,g]\mapsto[x,g\delta]} & \mathrm{Sh}_{\delta^{-1}K\delta\cap K} \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle p_2} \\ \mathrm{Sh}_K & & \mathrm{Sh}_K\,. \end{array}$$

Son image dans $\mathrm{Sh}_K \times \mathrm{Sh}_K$ est le lieu des variétés abéliennes avec structure PEL liées par une isogénie de type fixé par δ.

Quantités attachées :

- degré $d(\delta)$ ($\deg p_1$ = nombre d'isogénies),
- degré d'isogénie $i(\delta)$.

Fixons :

- deux composantes $\mathcal{S}, \mathcal{T}$ de Sh_K, définies sur un corps de nombres L.
- coordonnées = fonctions modulaires : $j_1, \ldots, j_n$ définies sur L.

Les équations modulaires décrivent $H_\delta \subset \mathcal{S} \times \mathcal{T}$ lorsque δ varie.

Formules analytiques

Rappel :

$$\mathrm{Sh}_K = G(\mathbb{Q})_+ \backslash \big(G(\mathbb{R})_+ \times G(\mathbb{A}_f) \big) / (K_\infty \times K).$$

Les coefficients de

$$[x, g] \mapsto \prod_{\gamma \in K/(K \cap \delta K \delta^{-1})} \Big(Y - j_1([x, g\gamma\delta)]) \Big)$$

sont des fonctions modulaires : fractions rationnelles en $j_1, \ldots, j_n$.

Formules analytiques

Rappel :

$$\mathrm{Sh}_K = G(\mathbb{Q})_+ \backslash \big(G(\mathbb{R})_+ \times G(\mathbb{A}_f) \big) / (K_\infty \times K).$$

Les coefficients de

$$[x, g] \mapsto \prod_{\gamma \in K/(K \cap \delta K \delta^{-1})} \Big(Y - j_1([x, g\gamma\delta)]) \Big)$$

sont des fonctions modulaires : fractions rationnelles en $j_1, \ldots, j_n$.

Équations modulaires de niveau δ

$$\Psi_{\delta,m} \in L(J_1, \ldots, J_n)[Y] \quad \text{pour } 1 \leq m \leq n.$$

Si A est une variété abélienne avec structure PEL, alors les racines de

$$\Psi_{\delta,1}\big(j_1(A), \ldots, j_n(A), Y\big) = 0$$

sont les coordonnées j_1 des variétés abéliennes isogènes. Puis $\Psi_{\delta,2}$ donne j_2, etc. Base de Gröbner lexicographique de H_δ.

Exemple 1 : polynômes modulaires elliptiques

La variété de Shimura PEL est $\mathcal{A}_1 = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}_1$, où

$$\mathbb{H}_1 = \big\{\tau \in \mathbb{C} \colon \mathrm{Im}(\tau) > 0\big\}.$$

Groupe sous-jacent : $G = \mathrm{GL}_2$. Le j-invariant est un isomorphisme $\mathcal{A}_1 \to \mathbb{A}^1$ défini sur $\mathbb{Q}$.

Équation modulaire de niveau $\delta = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$:

$$\Phi_\ell(j(\tau), Y) = \Psi_{\delta,1}(j(\tau), Y) = \prod_{\gamma \in \Gamma^{\mathbf{0}}(\ell)\backslash\, \mathrm{SL}_{\mathbf{2}}(\mathbb{Z})} \Big(Y - j(\tfrac{1}{\ell}\gamma\tau)\Big).$$

Exemple 2 : équations modulaires de Siegel

La variété de Shimura PEL est $\mathcal{A}_2 = \mathrm{Sp}_4(\mathbb{Z})\backslash\mathbb{H}_2$, où

$$\mathbb{H}_2 = \big\{\tau \in \mathrm{Mat}_{2\times 2}(\mathbb{C})\colon \tau^t = \tau,\ \mathrm{Im}(\tau) > 0\big\}.$$

Groupe sous-jacent : $G = \mathrm{GSp}_4$. Les invariants d'Igusa j_1, j_2, j_3 forment une application birationnelle $\mathcal{A}_2 \to \mathbb{P}^3$, définie sur $\mathbb{Q}$.

Équations modulaires de niveau $\delta = \begin{pmatrix} \ell I_2 & 0 \\ 0 & I_2 \end{pmatrix}$: trois fractions

$$\Psi_{\ell,m} \in \mathbb{Q}(J_1, J_2, J_3)[Y]$$

pour $1 \le m \le 3$.

$$\Psi_{\ell,1}\big(j_1(\tau), j_2(\tau), j_3(\tau), Y\big) = \prod_{\gamma \in \Gamma^{\mathbf{0}}(\ell)\backslash\, \mathrm{Sp}_{\mathbf{4}}(\mathbb{Z})} \Big(Y - j_1\big(\tfrac{1}{\ell}\gamma\tau\big)\Big).$$

Bornes de degré et de hauteur

Résultat principal

Comme précedemment : H_δ correspondance de Hecke de niveau $\delta \in G(\mathbb{A}_f)$, de degré $d(\delta)$ et de degré d'isogénie $i(\delta)$.

Théorème (K.)

1. *Le degré des équations modulaires est* $O(d(\delta))$.
2. *La hauteur des équations modulaires est* $O(d(\delta) \log i(\delta))$.

Remarques

- Les constantes dépendent du choix d'invariants, notamment de leur relation aux générateurs de l'algèbre des formes modulaires.
- Constantes explicites dans le cas des équations modulaires de Siegel, et de Hilbert pour $F = \mathbb{Q}(\sqrt{5})$.
- Les constantes correspondent à la réalité dans l'estimation de degré, pas dans l'estimation de hauteur.

Exemples

	Degré	Hauteur	# variables	Taille totale
Φ_ℓ	$O(\ell)$	$O(\ell \log \ell)$	2	$O(\ell^3 \log \ell)$
Siegel	$O(\ell^3)$	$O(\ell^3 \log \ell)$	4	$O(\ell^{15} \log \ell)$
Hilbert	$O_F(\ell)$	$O_F(\ell \log \ell)$	3	$O_F(\ell^4 \log \ell)$

- Dans le cas de Φ_ℓ, on retrouve les bornes connues à constantes près.
- En dimension 2, les équations modulaires écrites en entier sont trop volumineuses pour obtenir des gains de complexité via la méthode d'Elkies. Il faut évaluer à la volée pour réduire le nombre de variables.

Idée de preuve : bornes de degré

On identifie un dénominateur explicite des équations modulaires.

Exemple : polynôme modulaire elliptique Φ_ℓ

- Le dénominateur du j-invariant est Δ. Les coefficients de $\Phi_\ell(j(\tau), Y)$ pour $\tau \in \mathbb{H}_1$ sont de la forme f/g_ℓ où

$$g_\ell(\tau) = \prod_{\gamma \in \Gamma^0(\ell) \backslash \mathrm{SL}_2(\mathbb{Z})} (\gamma^* \tau)^{-12} \Delta(\tfrac{1}{\ell}\gamma\tau).$$

- g_ℓ est de poids $\mathrm{wt}(g_\ell) = d(\delta)\,\mathrm{wt}(\Delta) = 12(\ell+1)$.
- Écrivons $\dfrac{f}{g_\ell} = \dfrac{P(E_4, E_6)}{Q(E_4, E_6)}$; alors $\deg(P), \deg(Q) \in O(\ell)$.
- On remplace $E_6^2 \to E_4^3(1 + 1/j)$ et l'on simplifie. On obtient une fraction rationnelle en j de degré $O(\ell)$.

Constante explicite si des générateurs des formes modulaires sont connus.

Idée de preuve : bornes de hauteur

Stratégie d'évaluation-interpolation

Inspirée de travaux de Pazuki (2019) dans le cas de Φ_ℓ.

1. On montre que les évaluations des équations modulaires en des points de "petite hauteur" sont de hauteur $O(d(\delta)\log i(\delta))$.
2. On prouve une borne générale sur la hauteur d'une fraction rationnelle en fonction de la hauteur de ses évaluations.

Bornes de hauteur pour les évaluations

Notions de hauteur attachées à une variété abélienne A :

- Hauteur de Faltings $h_F(A)$.
- Hauteur des thêta constantes $h_{\Theta,r}(A)$ d'un certain niveau pair r ; dépend d'une polarisation principale.
- Hauteur $h_j(A)$ des invariants choisis $j_1, \ldots, j_n$: dépend d'un choix de structure PEL, définie seulement génériquement.

Idée de preuve

1. $\Psi_{\delta,1}(j_1(A), \ldots, j_n(A), Y)$ est donné par un produit de $d(\delta)$ facteurs de la forme $Y - j_1(B)$, où B est une variété abélienne de hauteur de Faltings $h_F(A) + O(\log i(\delta))$.
2. $h_{\Theta,r}(A)$ est relié à $h_F(A)$ (Pazuki 2012).
3. $h_j(A)$ est relié à $h_{\Theta,r}(A)$: relations entre fonctions modulaires.

Conclusion : $h(\Psi_{\delta,1}(j_1(A), \ldots, j_n(A), Y)) = O\Big(d(\delta)(h_j(A) + \log i(\delta))\Big)$.

Hauteur de fractions rationnelles

Soit L un corps de nombres de degré d_L, et $F \in L(X)$ de degré $d \geq 1$.

Théorème (K.)

Soit $S \subset [\![-M, M]\!]$, et soit $H \geq \log(2M)$. Supposons :

- *$h(F(x)) \leq H$ pour tout $x \in S$.*
- *S contient au moins M points.*
- *$M \geq \max\{100, 4d^3H, 16dd_L\}$.*

Alors

$$h(F) \leq H + C_L d \log(2dH) + d \log(2M) + \log(d+1),$$

où C_L dépend uniquement de L. On peut prendre $C_{\mathbb{Q}} = 1920$.

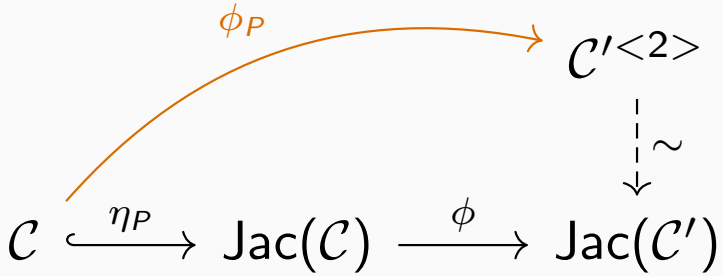
Ce résultat s'applique à la première étape de l'algorithme d'interpolation multivariée.

Calcul d'isogénies pour les surfaces abéliennes

Calcul d'isogénies

Soient $\mathcal{C}$ et $\mathcal{C}'$ des courbes hyperelliptiques lisses de genre 2 sur un corps k, telles que leurs Jacobiennes sont ℓ-isogènes.

Représentation explicite



Principe de l'algorithme

Les équations de $\mathcal{C}$ et $\mathcal{C}'$ définissent des bases de formes différentielles ω et ω' sur leurs Jacobiennes.

1. Calculer l'action de ϕ sur ces formes différentielles.
2. Résoudre un système différentiel : itérations de Newton sur des séries formelles, puis reconstruction rationnelle.

Calcul de l'action sur les formes différentielles

Soit A une variété abélienne p.p. de dimension g avec automorphismes $\{\pm 1\}$. L'isomorphisme de Kodaira–Spencer donne :

$$\mathrm{Sym}^2 T_0(A) \simeq T_A(\mathcal{A}_g).$$

Ainsi

- Les dérivées des coordonnées sur $\mathcal{A}_g$ sont des fonctions modulaires vectorielles de poids Sym^2. Elles peuvent être évaluées en (A, ω).
- Les déformations de ϕ, calculées à l'aide des dérivées des équations modulaires, sont liées à l'action de ϕ sur les formes différentielles.

Expression des dérivées des invariants d'Igusa

Isomorphisme de Kodaira–Spencer explicite pour l'espace de modules $\mathcal{A}_2$ des surfaces abéliennes p.p. (le cas des surfaces abéliennes p.p. avec multiplication réelle s'en déduit) :

$$D(j_1)(Jac(\mathcal{C}), \omega) = \{\text{Expression explicite en termes des coefficients de } \mathcal{C}\}.$$

Méthode de preuve

- Les coefficients de $\mathcal{C}$ forment une fonction modulaire vectorielle de q-développement connu (Cléry, Faber, Van der Geer 2017).
- $D(j_1)(\mathrm{Jac}(\mathcal{C}), \omega)$ est un covariant ; un système générateur de ces covariants est connu (Clebsch 1872).
- Algèbre linéaire sur les q-développements.

Résultat

Théorème (K., Page, Robert)

Soit k un corps de caractéristique 0 ou $> 8\ell + 7$. Supposons que $\mathcal{C}$ et $\mathcal{C}'$ sont "génériques", et que $\mathrm{Jac}(\mathcal{C})$ *et* $\mathrm{Jac}(\mathcal{C}')$ *sont ℓ-isogènes. Alors, étant donné la valeur des dérivées des équations modulaires de Siegel de niveau ℓ au point $(\mathcal{C}, \mathcal{C}')$, on peut calculer la représentation explicite d'une telle isogénie ϕ en utilisant $\widetilde{O}(\ell)$ opérations dans k.*

La manipulation des équations modulaires domine. Résultat analogue pour les surfaces abéliennes p.p. à multiplication réelle.

Algorithmes d'évaluation des équations modulaires

Évaluation des équations modulaires

Problème de l'évaluation

Étant donnés $(j_1, j_2, j_3) \in \mathbb{Q}^3$ de hauteur au plus H, calculer

$$\Psi_{\ell,m}(j_1, j_2, j_3, Y) \in \mathbb{Q}[Y]$$

pour $1 \leq m \leq 3$. Généralisation aux corps de nombres. Les corps finis s'y ramènent par relèvement.

Résumé de l'algorithme

1. Calculer $\tau \in \mathbb{H}_2$ donnant ces invariants d'Igusa.
2. Énumérer les matrices $\frac{1}{\ell}\gamma\tau$ et calculer leurs invariants d'Igusa via les thêta-constantes.
3. Calculer $\Psi_{\ell,m}(j_1, j_2, j_3, Y) \in \mathbb{C}[Y]$ à l'aide de la formule analytique, puis reconnaître des coefficients rationnels.

Calculs sur $\mathbb{C}$

Calcul de $\tau \in \mathbb{H}_2$ et des invariants d'Igusa : algorithmes heuristiques, en temps quasi-linéaire en la précision pour une entrée fixée (Dupont 2006), fondés sur la moyenne arithmético-géométrique (AGM).

Contributions

- Calcul de τ : on lève l'heuristique (choix de signes dans l'AGM), et on exprime la complexité en fonction de H.
- Calcul des invariants d'Igusa : on exprime la complexité en fonction de l'entrée. Heuristiquement l'algorithme de Dupont converge uniformément sur un compact, on s'y ramène par réduction au domaine fondamental et formules de duplication.
- Reconstruction rationnelle : calculer séparément le dénominateur des $\Psi_{\ell,m}$ permet de reconnaître des entiers. Analyser les pertes de précision dans tout l'algorithme permet d'obtenir un résultat prouvé.

Complexité

Théorème (K., sous heuristique)

On peut évaluer les équations modulaires de Siegel de niveau ℓ et leurs dérivées en un point $(j_1, j_2, j_3) \in \mathbb{Q}^3$ de hauteur au plus H en temps $\widetilde{O}(\ell^3 H^2 + \ell^6 H)$.

Résultat analogue pour les équations modulaires de Hilbert. On en déduit les estimations de complexité dans la méthode d'Elkies.

Corollaire

Si $\ell = O(\log p)$, on peut évaluer les équations modulaires de Siegel de niveau ℓ et leur dérivées en un point $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ en temps $\widetilde{O}(\log^7 p)$.

Perspectives

- Terminer l'implémentation.
- Lever les heuristiques ? Convergence de l'algorithme de Dupont ; distribution des premiers d'Elkies.
- Dans l'algorithme d'évaluation, reformuler la réduction au domaine fondamental en termes de réduction de réseaux symplectiques. Temps quasi-linéaire ?
- Extension de l'algorithme d'isogénie au cas des Jacobiennes de quartiques planes (genre 3).
- Construction de familles de surfaces abéliennes p.p. avec multiplication réelle explicite.
- Explorer les équations modulaires en termes d'autres invariants : comprendre les réductions de hauteur ; calcul d'autres anneaux de formes modulaires de Hilbert ou Siegel sur $\mathbb{Z}$.