Méthode AGM pour les courbes de genre 3 non hyperelliptiques

Christophe Ritzenthaler

IEM, Essen (Allemagne)

GTEM

Plan de l'exposé

- Motivations cryptographiques.

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.
- Géneralisation de la méthode : duplication, produit des π_i.

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.
- Géneralisation de la méthode : duplication, produit des π_i.
- Cas du genre 3 :

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.
- Géneralisation de la méthode : duplication, produit des π_i.
- Cas du genre 3 :

1. calcul des thêta constantes.

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.
- Géneralisation de la méthode : duplication, produit des π_i.
- Cas du genre 3 :

1. calcul des thêta constantes.
2. bon relèvement du modèle.

Plan de l'exposé

- Motivations cryptographiques.
- Définition des méthodes de la Moyenne Arithmético-Géométrique, dites A.G.M. dans le cadre 2-adique (Mestre).
- Rappels sur le genre 1.
- Géneralisation de la méthode : duplication, produit des π_i.
- Cas du genre 3 :

1. calcul des thêta constantes.
2. bon relèvement du modèle.
3. Exemple et utilisation de LLL.

Diffie-Hellman

G un groupe ($\simeq \mathbb{Z}/p\mathbb{Z}$) et $g \in G$ un générateur (publics).

Protocole :

1. Alice choisit $a \in \mathbb{Z}$ et envoie g^a à Bob.
2. Bob choisit $b \in \mathbb{Z}$ et envoie g^b à Alice.
3. Clé commune secrète : $g^{ab} = (g^a)^b = (g^b)^a$.

Le secret de g^{ab} est basé sur la difficulté à calculer $a = \log_g g^a$.

Pourquoi des jacobiennes de courbes ?

- Nombre maximal d'opérations réalisables : $2^{50} - 2^{60}$.
- Sûr basé sur le DL pour un groupe quelconque : > 160 bits.
  1. Pour $\mathbb{F}_q^*$: $L_q(1/3) \Rightarrow$ 1024 bits (comme la factorisation).
  2. Pour le groupe des classes : sous-exponentiel.
  3. Pour les jacobiennes de courbes : pas de meilleure attaque en général (genre < 4).

$\rightsquigarrow$ Trouver rapidement une bonne courbe (i.e $|\mathrm{Jac}(C)(k)|$ presque premier) : théorie CM ou en tester beaucoup !

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).
3. Calcul de 2^g «thêta constantes» initiales : $(\vartheta_i^{(0)})_{i=1,\ldots 2^g}$.

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).
3. Calcul de 2^g «thêta constantes» initiales : $(\vartheta_i^{(0)})_{i=1,\ldots 2^g}$.
4. Duplication de ces constantes : $(\vartheta_i^{(n)}) \rightsquigarrow$ isogénies de degré 2.

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).
3. Calcul de 2^g «thêta constantes» initiales : $(\vartheta_i^{(0)})_{i=1,\dots 2^g}$.
4. Duplication de ces constantes : $(\vartheta_i^{(n)}) \rightsquigarrow$ isogénies de degré 2.
5. $\left(\vartheta_i^{(Nn)}/\vartheta_i^{(N(n+1))}\right)$ converge vers $\alpha = \pm\pi_1 \dots \pi_g$.

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).
3. Calcul de 2^g «thêta constantes» initiales : $(\vartheta_i^{(0)})_{i=1,\dots 2^g}$.
4. Duplication de ces constantes : $(\vartheta_i^{(n)}) \rightsquigarrow$ isogénies de degré 2.
5. $\left(\vartheta_i^{(Nn)}/\vartheta_i^{(N(n+1))}\right)$ converge vers $\alpha = \pm\pi_1 \dots \pi_g$.
6. Calcul du polynôme minimal P_{sym} de $\alpha + 2^{gN}/\alpha$.

Comment fonctionnent les méthodes AGM ?

1. Entrée : courbe C de genre g ordinaire sur $\mathbb{F}_{2^N}$.
2. Relèvement sur l'extension 2-adique de degré N non ramifiée (Satoh).
3. Calcul de 2^g «thêta constantes» initiales : $(\vartheta_i^{(0)})_{i=1,\dots 2^g}$.
4. Duplication de ces constantes : $(\vartheta_i^{(n)}) \rightsquigarrow$ isogénies de degré 2.
5. $\left(\vartheta_i^{(Nn)}/\vartheta_i^{(N(n+1))}\right)$ converge vers $\alpha = \pm\pi_1 \dots \pi_g$.
6. Calcul du polynôme minimal P_{sym} de $\alpha + 2^{gN}/\alpha$.
7. Sortie : le polynôme caractéristique du Frobenius χ_C.

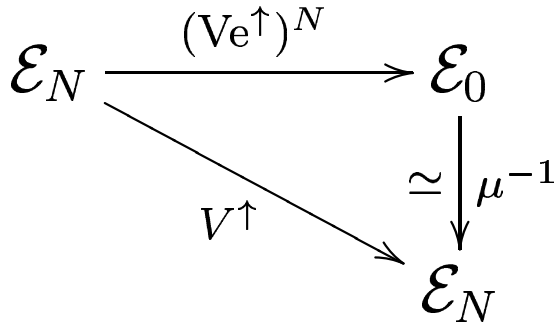
Rappel rapide du genre 1

Problème initial : $\tilde{E} : y^2 + xy = x^3 + a_2\, x^2 + a_4\, x$ **sur** $\mathbb{F}_{2^N}$.
Relèvement canonique :
$\tilde{E}^{\uparrow} : y^2 = x(x - (\vartheta_1^{(0)})^2)(x - (\vartheta_2^{(0)})^2)$.

Duplication : $(\vartheta_1^{(i+1)}, \vartheta_2^{(i+1)}) = \left(\frac{\vartheta_1^{(i)} + \vartheta_2^{(i)}}{2}, \vartheta_1^{(i)} \sqrt{\frac{\vartheta_2^{(i)}}{\vartheta_1^{(i)}}} \right)$.

$$\begin{array}{ccccccc}
\mathcal{E}_N & \longrightarrow & \cdots & \longrightarrow & \mathcal{E}_1 & \xrightarrow{\mathrm{Ve}^{\uparrow}} & \mathcal{E}_0 = \tilde{E}^{\uparrow} \\
\downarrow & & & & \downarrow & & \downarrow \\
\tilde{E}^{(N)} & \longrightarrow & \cdots & \longrightarrow & \tilde{E}^{(1)} & \xrightarrow{\mathrm{Ve}} & \tilde{E} \\
\downarrow \simeq & & & & & & \downarrow = \\
\tilde{E} & & & \xleftarrow{\phi = \mathrm{Fr}^N} & & & \tilde{E}
\end{array}$$

Fin du rappel



avec $\mu(x_N, y_N) = (u^2 x_N, u^3 y_N)$ et $u^2 = \frac{(\vartheta_1^{(0)})^2 + (\vartheta_2^{(0)})^2}{(\vartheta_1^{(N)})^2 + (\vartheta_2^{(N)})^2}$.

$$V^{\uparrow *}(\omega_N) = (\mu^{-1} \circ ((\mathrm{Ve}^{\uparrow})^N)^*(\omega_N) = ((\mathrm{Ve}^{\uparrow})^N)^*(u\omega) = u\omega_N.$$

$$\mathrm{Tr}(\mathrm{V}^{\uparrow}) = \mathrm{Tr}(\phi^{\uparrow}) = \mathrm{Tr}(\phi) = \mathrm{u} + \frac{2^{\mathrm{N}}}{\mathrm{u}}.$$

Duplication : convergence vers le relèvement canonique.

Une implémentation simple

Entrée : $a_6 \in \mathbb{F}_{2^N}^*$.
Sortie : $\pm$ la trace pour $y^2 + xy = x^3 + a_6$.

1. $\lambda := 1 + 8a_6 \pmod{16}$;
2. Pour k égal à 4 à $\lceil N/2 \rceil + 3$:
3. relève arbitrairement $\lambda \pmod{2^{k+2}}$.
4. $\lambda := \frac{1+\lambda}{2\sqrt{\lambda}} \pmod{2^{k+1}}$; // ou action du Frobenius (MSST)
5. Renvoie Norm $\left(\frac{2}{1+\lambda}\right) \pmod{2^{\lceil N/2 \rceil + 2}}$.

MSST ?

$\lambda := \frac{1+\lambda}{2\sqrt{\lambda}} \rightsquigarrow E(X,Y) = 4Y^2X - (1+X)^2$ (équation modulaire).

$X \leftarrow 1 + 8X$ et $Y \leftarrow 1 + 8Y$
$\tilde{E} = (X + 2Y + 8XY)^2 + Y + 4XY = 0$ (Kohel : $X_0(8)$)

$$\begin{aligned} 0 &= \tilde{E}(\lambda, {}^{\sigma}\lambda) = \tilde{E}(\Lambda + 2^k e, {}^{\sigma}\Lambda + 2^k\ {}^{\sigma}e) \\ &= \tilde{E}(\Lambda, {}^{\sigma}\Lambda) + 2^k\, e\, \partial_X \tilde{E}(\Lambda, {}^{\sigma}\Lambda) + 2^k\, {}^{\sigma}e\, \partial_Y \tilde{E}(\Lambda, {}^{\sigma}\Lambda) \\ &\quad +2^{2k-1}(reste) \end{aligned}$$

Les problèmes d'une généralisation

- Généraliser la formule de duplication.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.
  $\rightsquigarrow$ géométrie, invariants.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.
  $\rightsquigarrow$ géométrie, invariants.
- Bon modèle de calcul : la duplication s'effectue dans une extension non ramifiée fixe.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.
  $\rightsquigarrow$ géométrie, invariants.
- Bon modèle de calcul : la duplication s'effectue dans une extension non ramifiée fixe.
  $\rightsquigarrow$ arithmétique.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.
  $\rightsquigarrow$ géométrie, invariants.
- Bon modèle de calcul : la duplication s'effectue dans une extension non ramifiée fixe.
  $\rightsquigarrow$ arithmétique.
- Calcul des polyômes minimaux et caractéristiques.

Les problèmes d'une généralisation

- Généraliser la formule de duplication.
  $\rightsquigarrow$ fonctions thêta.
- Généraliser la formule reliant les thêta et le $\prod \pi_i$.
  $\rightsquigarrow$ géométrie arithmétique.
- Exprimer les thêta constantes algébriquement.
  $\rightsquigarrow$ géométrie, invariants.
- Bon modèle de calcul : la duplication s'effectue dans une extension non ramifiée fixe.
  $\rightsquigarrow$ arithmétique.
- Calcul des polyômes minimaux et caractéristiques.
  $\rightsquigarrow$ LLL, calculs sur la jacobienne.

Généralisation de la duplication

Thêta caractéristiques $(q = exp(i\pi))$:

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} q^{(n+\epsilon/2)\ \Omega\ {}^t(n+\epsilon/2)+2(n+\epsilon/2)\ {}^t(z+\epsilon'/2)}$$

Duplication :

$$\vartheta \begin{bmatrix} 0 \\ \varepsilon' \end{bmatrix} (0, 2\Omega)^2 = \frac{1}{2^g} \sum_{d \in (\mathbb{Z}/2\mathbb{Z})^g} \vartheta \begin{bmatrix} 0 \\ \varepsilon' + d \end{bmatrix} (0, \Omega) \cdot \vartheta \begin{bmatrix} 0 \\ d \end{bmatrix} (0, \Omega)$$

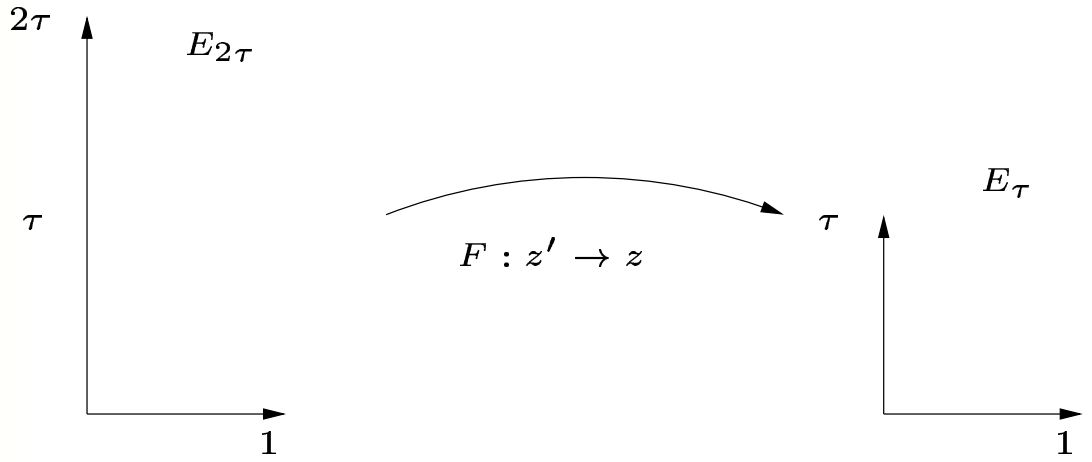
Pourquoi cela décrit-il des 2-isogénies ?

A variété abélienne sur $\mathbb{C} \Rightarrow A(\mathbb{C}) \simeq \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g\Omega)$.

L'application

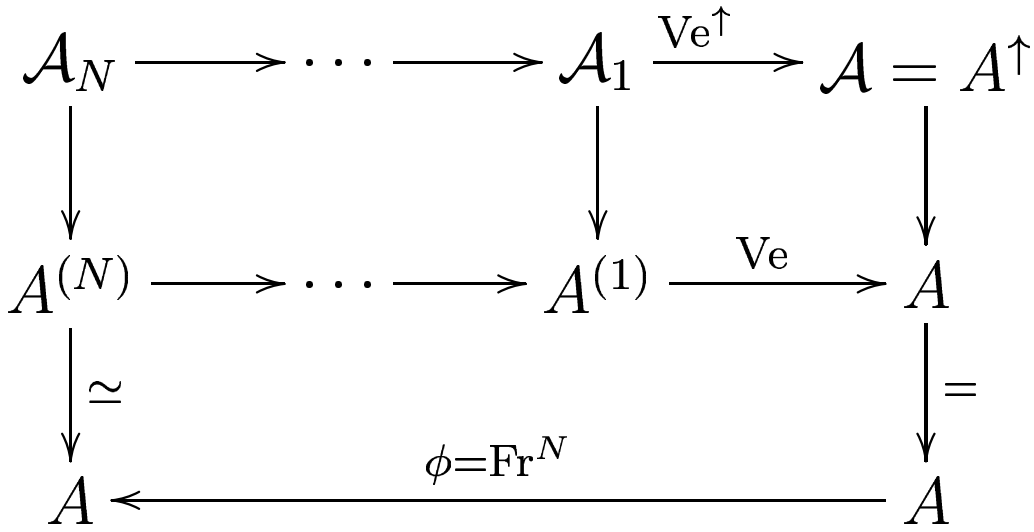
$$\begin{array}{ccc} \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g 2\Omega) & \to & \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g\Omega) \\ z & \mapsto & z \end{array}$$

est une 2-isogénie de noyau $(\mathbb{Z}^g/2\mathbb{Z}^g)\Omega$.



Cas général

A/k ordinaire, principalement polarisée sur k, simple et $|A[2](k)| = 2^g$.



$A^{\uparrow}$ (relèvement canonique) : $\mathrm{End}(A^{\uparrow}) = \mathrm{End}(A)$ (unique à isomorphisme près) $\Rightarrow$ variété CM.

Théorème principal

Lemme : $\ker \mathrm{Ve}^{\uparrow}$ est un $\mathbb{F}_2$-espace vectoriel isotrope maximal pour le couplage de Weil (induit par le relèvement de la polarisation principale).

En complexe : $\mathcal{A}_{\mathbb{C}} = \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g\Omega)$ et $(\mathcal{A}_N)_{\mathbb{C}} = \mathbb{C}^g/(\mathbb{Z}^g + \mathbb{Z}^g 2^N\Omega)$.

Théorème : Soit $\pi_1, \ldots, \pi_g$ les racines de χ_A qui sont des unités 2-adiques. Avec les notations ci-dessus, supposons qu'il existe $[\epsilon]$ tel que $\vartheta[\epsilon](0,\Omega) \neq 0$. Alors $\vartheta[\epsilon](0,2^N\Omega)$ est non nulle et

$$\frac{\vartheta[\epsilon](0,\Omega)^2}{\vartheta[\epsilon](0,2^N\Omega)^2} = \pm(\pi_1 \ldots \pi_g).$$

Arguments de la preuve

- Lemme : Soit $[\epsilon]$ une caractéristique entière alors si $M \in \Gamma_g(2)$ on a

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (0, (A\Omega+B)(C\Omega+D)^{-1})^2 = \pm \det(C\Omega + D) \cdot \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (0, \Omega$$

- L'action de $M \in \Gamma_g(1) : z \mapsto (C\Omega + D)^{-1} z$.

$$\begin{aligned} \Rightarrow M^*(dz_1 \wedge \ldots \wedge dz_g) &= \det(C\Omega + D)^{-1} \cdot (dz_1 \wedge \ldots \wedge dz_g) \\ &= \det(\rho_{\mathbb{C}}(V))^{-1} (dz_1 \wedge \ldots \wedge dz_g) \end{aligned}$$

- Variété abélienne CM : valeurs propres de $\rho_{\mathbb{C}}(V)$:

$\pi_1, \ldots, \pi_g$.

Convergence vers le relèvement canonique

Théorème (Carls) : Soit A une variété abélienne ordinaire sur k, $\mathcal{A}/\mathcal{O}$ un schéma abélien de fibre spéciale A. On définit alors une suite

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

où les noyaux des isogénies sont les composantes $\mathcal{A}_i[2]^{loc}$. On a alors

$$\lim_{n\to\infty} \mathcal{A}_{nN} = A^{\uparrow}$$

i.e. pour tout n, $(\mathcal{A}_{Nn})/\mathcal{O}^{(Nn+1)} = (A^{\uparrow}_{Nn})/\mathcal{O}^{(Nn+1)}$ où l'on note $\mathcal{O}^{(i)} = \mathcal{O}/\mathcal{M}^i$.

Restrictions et genre 3

- En hyperelliptique : formule de Thomae. Pas d'analogue dans le cas général pour g quelconque.
- Croissance exponentielle avec le genre.
- retrouver P_{sym} à partir de $\prod \pi_i$ (Lercier) :

genre	1	2	3	4	5	6
précision	$N/2$	N	$10N$	$62N$	$390N$	$2210N$

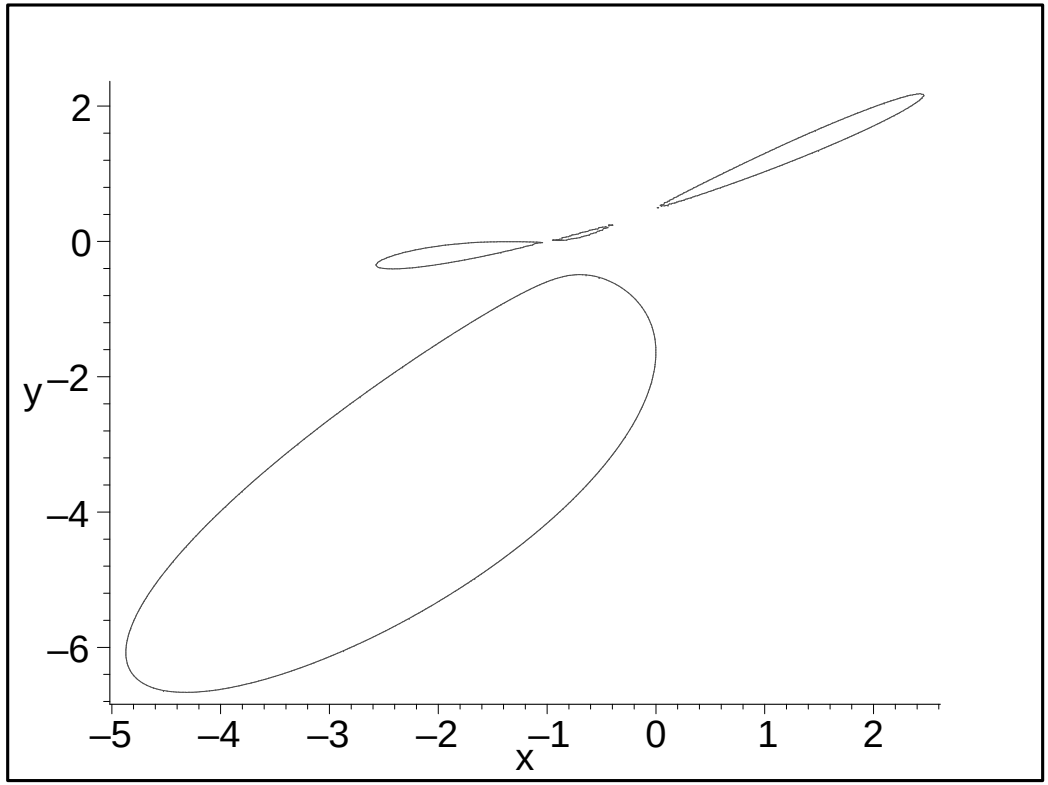
- $g > 3$: cryptographiquement faible.

$\rightsquigarrow$ $g = 3$: taille crypto $3N = 180$ bits (pas de multi-précision).

Plongement canonique

Proposition : C une courbe de genre 3 non hyperelliptique $=$ quartique plane non singulière.

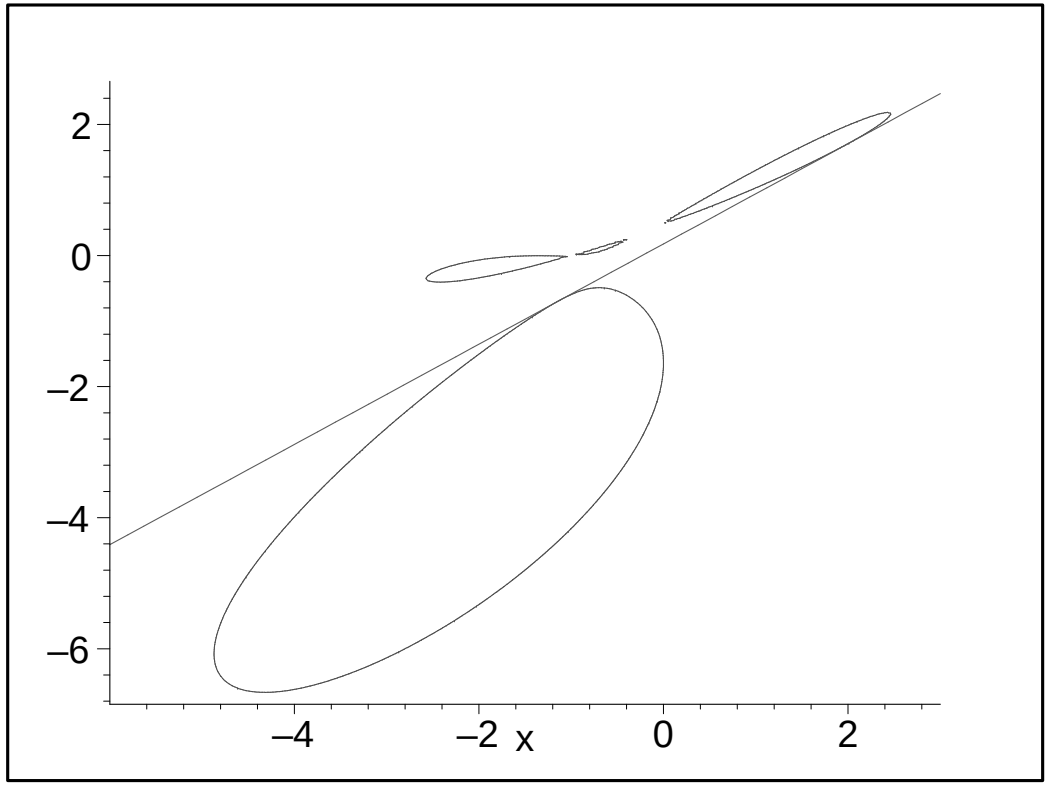
$\rightsquigarrow$ Etude des bitangentes.



Plongement canonique

Proposition : C une courbe de genre 3 non hyperelliptique $=$ quartique plane non singulière.

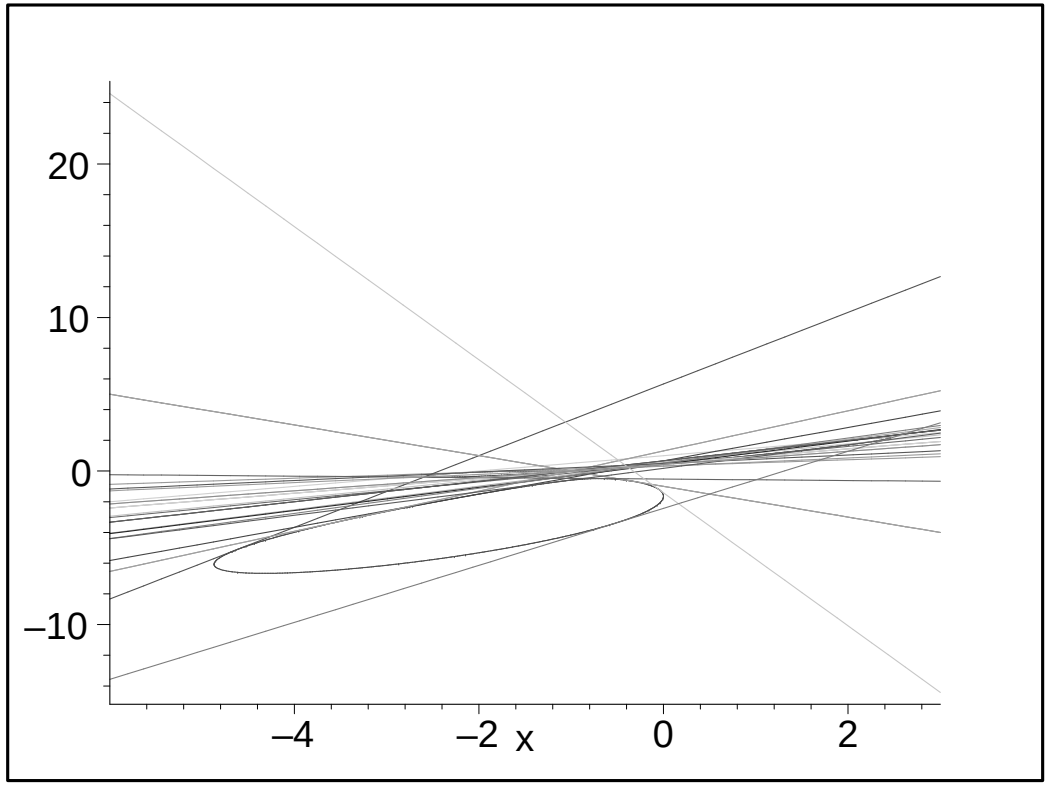
$\rightsquigarrow$ Etude des bitangentes.



Plongement canonique

Proposition : C une courbe de genre 3 non hyperelliptique $=$ quartique plane non singulière.

$\rightsquigarrow$ Etude des bitangentes.



Bitangentes sur $\mathbb{C}$

Proposition : Une quartique plane non singulière possède 28 bitangentes.

Démonstration :
Géométrique : par la courbe duale.
Analytique : relation avec les fonctions thêta.

Corollaire : Il y a une bijection explicite entre les bitangentes et les $[\epsilon]$ impaires.

Modèle de Riemann

Proposition (Riemann) : Toute quartique lisse peut s'écrire sous la forme

$$\sqrt{x_1u_1} + \sqrt{x_2u_2} + \sqrt{x_3u_3} = 0.$$

Démonstration : Etude des sections de $L(D)$ avec $2D \simeq nK$ (fonctions racines de degré n) pour $n = 2$.

$\rightsquigarrow$ détermination des bitangentes, thêta constantes.

Modèle de Riemann

Proposition (Riemann) : Toute quartique lisse peut s'écrire sous la forme

$$(x_1u_1 + x_2u_2 - x_3u_3)^2 - 4x_1u_1x_2u_2 = 0$$

Démonstration : Etude des sections de $L(D)$ avec $2D \simeq nK$ (fonctions racines de degré n) pour $n = 2$.

$\rightsquigarrow$ détermination des bitangentes, thêta constantes.

Modèle de Riemann

Proposition (Riemann) : Toute quartique lisse peut s'écrire sous la forme

$$\sqrt{x_1 u_1} + \sqrt{x_2 u_2} + \sqrt{x_3 u_3} = 0.$$

Démonstration : Etude des sections de $L(D)$ avec $2D \simeq nK$ (fonctions racines de degré n) pour $n = 2$.

$\rightsquigarrow$ détermination des bitangentes, thêta constantes.

Système d'Aronhold

7 bitangentes β_i de caractéristiques $[i]$ telles que

- $[\epsilon]$ impaire s'écrit soit $[i]$, soit $[i]+[j]$.
- $[\epsilon]$ paire s'écrit soit $[i]+[j]+[k]$ soit $[0]$.

$$[1]=\begin{bmatrix}1&0&1\\0&0&1\end{bmatrix}\quad [2]=\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix}\quad [3]=\begin{bmatrix}1&1&1\\0&1&0\end{bmatrix}\quad [4]=\begin{bmatrix}0&1&1\\1&0&1\end{bmatrix}$$

$$[5]=\begin{bmatrix}1&0&0\\1&0&0\end{bmatrix}\quad [6]=\begin{bmatrix}0&0&1\\1&1&1\end{bmatrix}\quad [7]=\begin{bmatrix}0&1&0\\1&1&0\end{bmatrix}$$

Calcul du système d'Aronhold

• Étude de deux familles de sections de $L(D)$ avec $2D \simeq 2K$.

$\rightsquigarrow$ Etude théorique (corps de définition).

• Géométriquement : $U_1 = (u_2 \cap u_3)^*$, $U_2 = (u_3 \cap u_1)^*$ et $U_3 = (u_1 \cap u_2)^*$.

$(\beta_i)^*_{i=4\ldots7}$ sont les points d'intersection des coniques $x_1U_1 - x_2U_2$, $x_2U_2 - x_3U_3$, $x_3U_3 - x_1U_1$.

Calcul des bitangentes

- Système d'Aronhold (obtenu à partir d'une équation de degré 4)

$$\begin{cases} \beta_1 : x_1 = 0 \\ \beta_2 : x_2 = 0 \\ \beta_3 : x_3 = 0 \\ \beta_4 : x_1 + x_2 + x_3 = 0 \end{cases} \qquad \begin{aligned} \beta_5 &= a_1 x_1 + a_2 x_2 + a_3 x_3 \\ \beta_6 &= a'_1 x_1 + a'_2 x_2 + a'_3 x_3 \\ \beta_7 &= a''_1 x_1 + a''_2 x_2 + a''_3 x_3 \end{aligned}$$

- Calcul linéaire de constantes de normalisation k, k', k''.

Expressions des bitangentes (Riemann)

$$\beta_1 : x_1 = 0 \quad \beta_2 : x_2 = 0 \quad \beta_3 : x_3 = 0$$
$$\beta_{23} : u_1 = 0 \quad \beta_{13} : u_2 = 0 \quad \beta_{12} : u_3 = 0$$

$$\beta_4 : x_1 + x_2 + x_3 = 0 \qquad \beta_5 : a_1 x_1 + a_2 x_2 + a_3 x_3 = 0$$
$$\beta_6 : a'_1 x_1 + a'_2 x_2 + a'_3 x_3 = 0 \quad \beta_7 : a''_1 x_1 + a''_2 x_2 + a''_3 x_3 = 0$$

$$\beta_{14} : u_1 + x_2 + x_3 = 0 \qquad \beta_{15} : \frac{u_1}{a_1} + k a_2 x_2 + k a_3 x_3 = 0$$
$$\beta_{16} : \frac{u_1}{a'_1} + k' a'_2 x_2 + k' a'_3 x_3 = 0 \quad \beta_{17} : \frac{u_1}{a''_1} + k'' a''_2 x_2 + k'' a''_3 x_3 = 0$$

$$\beta_{24} : x_1 + u_2 + x_3 = 0 \qquad \beta_{25} : k a_1 x_1 + \frac{u_2}{a_2} + k a_3 x_3 = 0$$
$$\beta_{26} : k' a'_1 x_1 + \frac{u_2}{a'_2} + k' a'_3 x_3 = 0 \quad \beta_{27} : k'' a''_1 x_1 + \frac{u_2}{a''_2} + k'' a''_3 x_3 = 0$$

Expressions des bitangentes (suite)

$$\beta_{34} : x_1 + x_2 + u_3 = 0 \qquad \beta_{35} : ka_1x_1 + ka_2x_2 + \frac{u_3}{a_3} = 0$$
$$\beta_{36} : k'a'_1x_1 + k'a'_2x_2 + \frac{u_3}{a'_3} = 0 \qquad \beta_{37} : k''a''_1x_1 + k''a''_2x_2 + \frac{u_3}{a''_3} = 0$$

$$\beta_{67} : \frac{u_1}{1-ka_2a_3} + \frac{u_2}{1-ka_3a_1} + \frac{u_3}{1-ka_1a_2} = 0$$
$$\beta_{57} : \frac{u_1}{1-k'a'_2a'_3} + \frac{u_2}{1-k'a'_3a'_1} + \frac{u_3}{1-k'a'_1a'_2} = 0$$
$$\beta_{56} : \frac{u_1}{1-k''a''_2a''_3} + \frac{u_2}{1-k''a''_3a''_1} + \frac{u_3}{1-k''a''_1a''_2} = 0$$

$$\beta_{45} : \frac{u_1}{a_1(1-ka_2a_3)} + \frac{u_2}{a_2(1-ka_3a_1)} + \frac{u_3}{a_3(1-ka_1a_2)} = 0$$
$$\beta_{46} : \frac{u_1}{a'_1(1-k'a'_2a'_3)} + \frac{u_2}{a'_2(1-k'a'_3a'_1)} + \frac{u_3}{a'_3(1-k'a'_1a'_2)} = 0$$
$$\beta_{47} : \frac{u_1}{a''_1(1-ka''_2a''_3)} + \frac{u_2}{a''_2(1-k''a''_3a''_1)} + \frac{u_3}{a''_3(1-k''a''_1a''_2)} = 0$$

Détermination des thêta constantes

Théorème (Weber) : Soit $[\epsilon] = [i] + [j] + [k]$ paire. On note $[\beta_{l_1}, \beta_{l_2}, \beta_{l_3}] = \det(\beta_{l_1}, \beta_{l_2}, \beta_{l_3})$ alors

$$\left(\frac{\vartheta[\epsilon](0)}{\vartheta[0](0)}\right)^4 = \frac{[\beta_i, \beta_j, \beta_{ij}][\beta_{ik}, \beta_{jk}, \beta_{ij}][\beta_j, \beta_{jk}, \beta_k][\beta_i, \beta_{ik}, \beta_k]}{[\beta_j, \beta_{jk}, \beta_{ij}][\beta_i, \beta_{ik}, \beta_{ij}][\beta_i, \beta_j, \beta_k][\beta_{ik}, \beta_{jk}, \beta_k]}$$

Preuve : Utilisation des fonctions racines de degré 3.

Modèles et relèvements : cas hyperelliptiques

Courbes hyperelliptiques ordinaires sur $\mathbb{F}_{2^N}$:
$y^2 + yh(x) = u(x)$ où u, h sont de degré $g+1$ et h est scindé à racines simples.

$y \leftarrow y + v$ on peut se ramener à $y^2 + yh = hu$.

Relèvement :
$Y^2 = (2y+h)^2 = h(h+4u) = \prod (x - \alpha_i)(x - (\alpha_i + 4e_i))$.

$\rightsquigarrow$ Détermination des thêta initiales : formules de Thomae.

Importance d'un bon modèle : les calculs se font dans un corps fixe.

Quartiques ordinaires en caractéristique 2

Proposition : C est ordinaire si et seulement si elle a exactement 7 bitangentes.

Proposition : Elles sont isomorphes à $(*)$

$$(ax^2 + by^2 + cz^2 + dxy + exz + fyz)^2 = xyz(x + y + z)$$

avec la condition suivante

$$abc(a+b+d)(a+c+e)(b+c+f)(a+b+c+d+e+f+1) \neq 0.$$

Inversement toutes les courbes qui vérifient ces conditions sont des courbes de genre 3 ordinaires, non hyperelliptiques.

Transformation du modèle et relèvement

«Modèle d'Artin-Schreier».

$$\begin{cases} Y_1^2 = x_1 u_1 \\ Y_2^2 = x_2 u_2 \\ Y_3^2 = x_3 u_3 \\ Y_1 + Y_2 + Y_3 = 0 \end{cases}$$

Courbe de genre 5, revêtement de degré 2 non ramifié de C.

Transformation du modèle et relèvement

«Modèle d'Artin-Schreier».

$$\begin{cases} Y_1^2 = x_1 u_1 \\ Y_2^2 = x_2 u_2 \\ Y_3^2 = x_3 u_3 \\ Y_1 + Y_2 + Y_3 = 0 \end{cases} \overset{k}{\rightsquigarrow} \begin{cases} Y_1^2 + l_1 Y_1 = l_1 v_1 \\ Y_2^2 + l_2 Y_2 = l_2 v_2 \\ Y_3^2 + l_3 Y_3 = l_3 v_3 \\ l_1 + l_2 + l_3 = 0 \\ Y_1 + Y_2 + Y_3 = l \end{cases}$$

Courbe de genre 5, revêtement de degré 2 non ramifié de C.

Transformation du modèle et relèvement

«Modèle d'Artin-Schreier».

$$\begin{cases} Y_1^2 = x_1u_1 \\ Y_2^2 = x_2u_2 \\ Y_3^2 = x_3u_3 \\ Y_1+Y_2+Y_3 = 0 \end{cases} \overset{k}{\rightsquigarrow} \begin{cases} Y_1^2 + l_1Y_1 = l_1v_1 \\ Y_2^2 + l_2Y_2 = l_2v_2 \\ Y_3^2 + l_3Y_3 = l_3v_3 \\ l_1+l_2+l_3 = 0 \\ Y_1+Y_2+Y_3 = l \end{cases} \overset{K}{\rightsquigarrow} \begin{cases} (2Y_1+l_1)^2 = l_1(4v_1+l_1) \\ (2Y_2+l_2)^2 = l_2(4v_2+l_2) \\ (2Y_3+l_3)^2 = l_3(4v_3+l_3) \\ l_1+l_2+l_3 = -2l \\ (2Y_1+l_1)+(2Y_2+l_2)+ \\ (2Y_3+l_3) = 0 \end{cases}$$

Courbe de genre 5, revêtement de degré 2 non ramifié de C.

Modèle pour le relèvement

Proposition : C donnée par le modèle $(*)$ est isomorphe sur k à la courbe quotient du modèle ci-dessus par le morphisme $(Y_1 : Y_2 : Y_3 : x' : y' : z') \mapsto (x' : y' : z')$ avec

$$\begin{cases} l_1 = x', l_2 = y', l_3 = x' + y' \\ l = z' \\ v_1 = bcy' + (c+f)z' \\ v_2 = acx' + dcy' + (c+e)z' \\ v_3 = acx' + (d+b)cy' + (1+c+e+f)z' \end{cases}$$

Proposition : Le modèle ainsi défini a toutes ses bitangentes sur K.

Algorithme (du calcul de $\prod \pi_i$)

Entrée : C sous la forme $(*)$.
Sortie : $\pm \prod \pi_i \pmod{2^{10N}}$.

1. Relève C sur K par les équations précédentes.
2. Calcul du système d'Aronhold (1 racine quatrième).
3. Expression de l'ensemble des bitangentes.
4. Calcul des huit $(\vartheta_i^{(0)})^2 = (\vartheta[\epsilon](0)/\vartheta[0](0))^4$ qui sont des unités 2-adiques (précision 7).
5. Duplication ($+1$ de précision à chaque itération, 8 racines carrées).
6. Renvoie $\alpha = \vartheta_0^{(11N)}/\vartheta_0^{(10N)} \pmod{2^{10N}}$.

Exemple

Soit $\tilde{C}$ sur $\mathbb{F}_{2^{100}}$ (ω racine de $(X^{101}-1)/(X-1)$) définie par

$$(\omega x^2+(\omega^3+1)y^2+\omega^4xy+(\omega^3+\omega^2)x+\omega^6y+\omega^2)^2-xy(x+y+1)=0.$$

Relèvement sur l'extension non ramifiée de degré 100 de $\mathbb{Q}_2$:

$$\begin{cases} v_1 = & (w^5+w^2)y+(w^2+w^6)z \\ v_2 = & w^3x+w^6y+(w^3+2w^2)z \\ v_3 = & w^3+(w^6+w^5+w^2)y+(w^6+w^3+2w+1)z \end{cases}$$

Exemple (suite)

Les 8 constantes initiales (de valuation 0) (temps < 1mn) :

$$\begin{cases} 1 + O(p^4) \\ 1 + (w^{17} + w^{14} + w^{13} + w^9)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{19} + w^{18} + w^{17} + w^{14} + w^{12} + w^{11} + w^{10} + w^5 + w^4 + w)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{19} + w^{18} + w^{13} + w^{12} + w^{11} + w^{10} + w^9 + w^5 + w^4 + w)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{14} + w^{13} + w^{10} + w^9 + w^7 + w^6 + w^4 + w^2)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{17} + w^{10} + w^7 + w^6 + w^4 + w^2)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{19} + w^{18} + w^{17} + w^{13} + w^{12} + w^{11} + w^9 + w^7 + w^6 + w^5 + w^2 + w)p^3 + \mathrm{O}(p^4) \\ 1 + (w^{19} + w^{18} + w^{14} + w^{12} + w^{11} + w^7 + w^6 + w^5 + w^2 + w)p^3 + \mathrm{O}(p^4) \end{cases}$$

Exemple (suite)

$$\alpha = \frac{\vartheta_1^{(1000)}}{\vartheta_1^{(1100)}} + \mathrm{O}(2^{1000}) = \left\{ \begin{array}{l} 1 + 2^5 + 2^9 + 2^{12} + 2^{13} + 2^{18} + 2^{20} + 2^{22} + 2^{24} \\ +2^{25} + 2^{27} + 2^{29} + 2^{31} + 2^{32} + 2^{34} + 2^{38} + 2^{40} \\ +2^{45} + 2^{47} + 2^{49} + 2^{51} + 2^{53} + 2^{55} + 2^{60} + 2^{61} \\ +2^{62} + 2^{63} + 2^{65} + 2^{67} + 2^{68} + 2^{69} + 2^{71} + 2^{72} \\ +2^{73} + \ldots + 2^{991} + 2^{993} + 2^{995} + 2^{996} + \\ 2^{997} + 2^{999} + \mathrm{O}(2^{1000}) \end{array} \right.$$

Temps de calcul : version peu optimisée (11mn) ; version Lercier-Lubicz (1mn).

Fin de l'algorithme

Calcul du polynôme minimal de $\beta = \alpha + 2^{3N}/\alpha$ (connu à la précision $\delta \approx 10N$) : utilisation de LLL.

β vérifie : $X^4 + r_3X^3 + r_2qX^2 + r_1q^2X + q^3r_0$.

Relation linéaire à coefficients dans $\mathbb{Z}$:

$$(\beta_{-1}, \beta_4, \beta_3, \beta_2, \beta_1, \beta_0) = (2^\delta, \beta^4 \pmod{2^\delta}, \beta^3 \pmod{2^\delta}, q\beta^2 \pmod{2^\delta}, q^2\beta \pmod{2^\delta}, q^3 \pmod{2^\delta}).$$

Forme quadratique sur le réseau :

$$\begin{aligned} Q((s_{-1}, s_4, s_3, s_2, s_1, s_0)) &= 2^{\lfloor \delta/2+N \rfloor} s_4^2 + 2^{3N} s_3^2 + 2^{2N} s_2^2 + 2^N s_1^2 + s_0^2 \\ &+ 2^\delta (s_{-1}\beta_{-1} + s_4\beta_4 + s_3\beta_3 + s_2\beta_2 + s_1\beta_1 + s_0\beta_0)^2. \end{aligned}$$

Fin de l'exemple

Polynôme minimal de β (temps < 2s) :

$$P_{\mathrm{sym}} = X^4 - 267153656730945219545193916024670843780592 97 \cdot X^3$$
$$-19824284288430790577592347107087136233792411585403536847077 41 \cdot 2^{100} \cdot X^2 +$$
$$24855084236941449872175958669174440469589327790633558658772827397072671346 9 \cdot$$
$$X + 17505802925734816911329803763098347224059055501 4//$$
$$//95607628540728368503770181273637994266016 1 \cdot 2^{300}$$

Polynôme caractéristique au signe près :

$$\begin{aligned}\chi_{\tilde{C}} \quad = \quad & X^6 + 377276036264709 \cdot X^5 + 345535106116904583889422793740 3 \cdot X^4 + \\ & 92979302197227669130776666646461687227769187 1 \cdot X^3 \\ & +345535106116904583889422793740 3 \cdot 2^{100} \cdot X^2 \\ & +377276036264709 \cdot 2^{200} \cdot X + 2^{300}\end{aligned}$$

Détermination du signe : $\chi_{\tilde{C}}(1) \cdot D \overset{?}{\sim} 0$ (temps 4s).