AGM et évaluation rapide de fonctions modulaires

Séminaire(s) ACC-CF, Limoges, 16 mai 2006

Régis Dupont

http://www.lix.polytechnique.fr/Labo/Regis.Dupont

Introduction

Objectif : évaluation numérique rapide de fonctions modulaires

Motivations en cryptologie des courbes (hyper)elliptiques :

- multiplication complexe effective

  $\Rightarrow$ calcul de polynômes de classes

- comptage de points sur des corps premiers (algorithme SEA)

  $\Rightarrow$ calcul de polynômes modulaires

utilisation de méthodes d'évaluation/interpolation (A. Enge)

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- AGM et évaluation de fonctions modulaires
- Généralisation (Borchardt)

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- AGM et évaluation de fonctions modulaires
- Généralisation (Borchardt)

Moyenne arithmético-géométrique

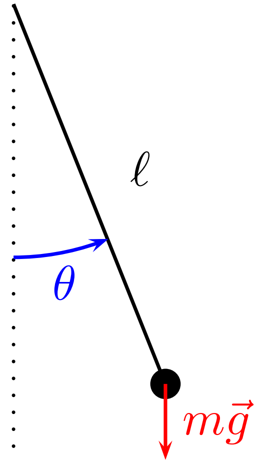

Legendre


Lagrange


Gauss

Intégrales elliptiques (calculs liés à la mécanique) :

$$I(a_0, b_0) = \int_0^{\frac{\pi}{2}} \frac{dt}{\sqrt{a_0^2 \sin^2 t + b_0^2 \cos^2 t}}$$



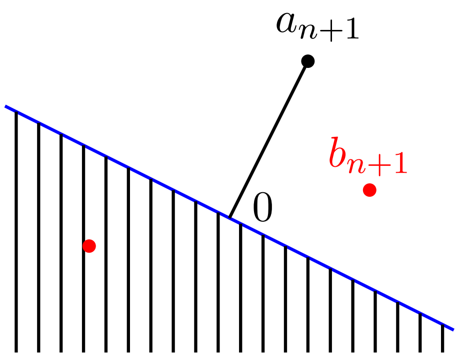
$$\left.\begin{aligned} a_{n+1} &= \frac{a_n + b_n}{2} \\ b_{n+1} &= \sqrt{a_n b_n} \end{aligned}\right\} \to \mathrm{AGM}(a_0, b_0) = \frac{\pi}{2\, I(a_0, b_0)}$$

AGM sur $\mathbb{C}$

$a_0, b_0 \in \mathbb{C}$ [Gauss] : problème de choix de racine pour $b_{n+1} = \sqrt{a_n b_n}$

Définition : b_{n+1} est le bon choix si

$$|a_{n+1} - b_{n+1}| < |a_{n+1} + b_{n+1}|$$



Propriétés :

- (a_n) et (b_n) ont toujours une limite commune
- limite nulle ssi nombre infini de mauvais choix
- convergence *quadratique* si la limite est non nulle

AGM : un exemple

$$
\begin{array}{lcllcl}
a_0 & = & 1.000000000000000000000000000 & b_0 & = & 2.000000000000000000000000000 \\
a_1 & = & 1.500000000000000000000000000 & b_1 & = & 1.414213562373095048801688724 \\
a_2 & = & 1.457106781186547524400844362 & b_2 & = & 1.456475315121970260851161882 \\
a_3 & = & 1.456791048154258892626003122 & b_3 & = & 1.456791013939554946194175396 \\
a_4 & = & 1.456791031046906919410089259 & b_4 & = & 1.456791031046906818962775506 \\
a_5 & = & 1.456791031046906869186432383 & b_5 & = & 1.456791031046906869186432383
\end{array}
$$

Moyenne arithmético-géométrique

Question : on fixe $a, b \in \mathbb{C}$, quel est l'ensemble des limites des suites AGM associées à (a, b) (pour tous les choix possibles de racines) ?

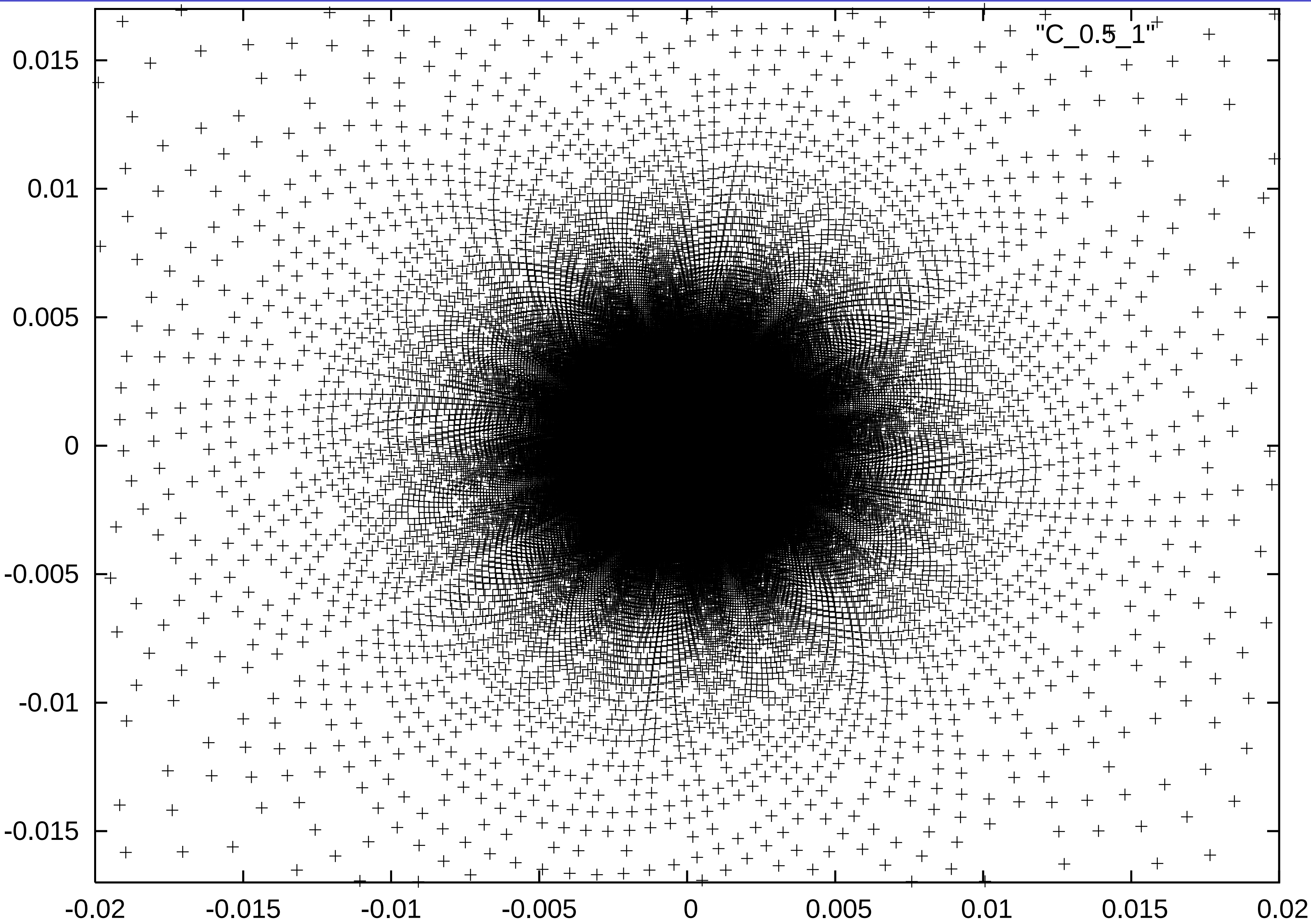
On note cet ensemble

$$\mathfrak{L}(a, b)$$

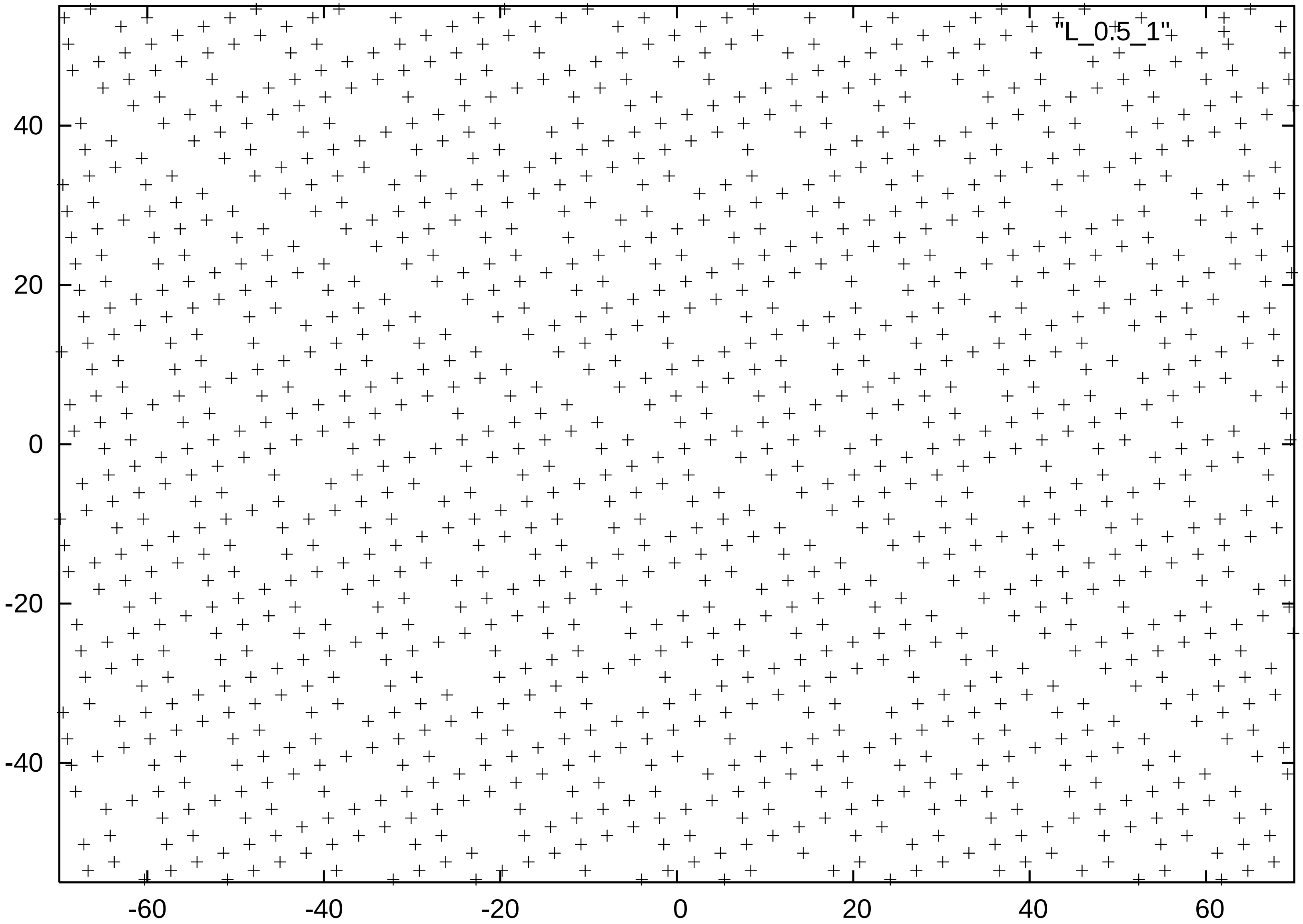
Propriétés :

- $0 \in \mathfrak{L}(a, b)$
- $\mathfrak{L}(a, b) = \mathfrak{L}(b, a)$
- $\mathfrak{L}(\lambda a, \lambda b) = \lambda \mathfrak{L}(a, b)$

Valeurs de $\mathrm{AGM}\left(1, \frac{1}{2} + i\right)$



Valeurs de $1/\mathrm{AGM}\left(1, \frac{1}{2} + i\right)$



Une question riche en développements !

- la réponse nécessite l'introduction des formes et fonctions modulaires
- historiquement, c'est par l'AGM que Gauss les a introduites (publié tardivement. . .)

Une fonction AGM

Propriété (homogénéité) : pour tout $\lambda \in \mathbb{C}$,

$$(a_n, b_n)_{n\in\mathbb{N}} \text{ suite AGM } \Rightarrow (\lambda a_n, \lambda b_n)_{n\in\mathbb{N}} \text{ suite AGM}$$

Définition : pour $z \in \mathbb{C}$, on pose $a_0 = 1$, $b_0 = z$,

$(a_n, b_n)_{n\in\mathbb{Z}}$ la suite AGM n'ayant que des bons choix de racines

$\longrightarrow$ $\mathrm{M}(z)$ est alors la limite de cette suite

Complexité de l'évaluation :

$$O\left(\mathcal{M}(N)\left(\log N + \log\left|\log|z|\right|\right)\right)$$

$O\left(\mathcal{M}(N)\log N\right)$ si z est dans un compact ne contenant pas 0

Intérêt algorithmique

XVIII et XIX$^{\text{èmes}}$ siècles :

- Calculs à la main (intégrales elliptiques)
- Quelques dizaines de bits

Depuis les années 1970 :

- Utilisation d'ordinateurs, regain d'intérêt
- [Salamin, Borwein & Borwein] : calcul de π et du logarithme
- Dizaines de milliards de bits
  (la seule limite est la mémoire des machines utilisées !)

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- AGM et évaluation de fonctions modulaires
- Généralisation (Borchardt)

$\mathcal{H}$ et le groupe modulaire Γ

Demi-plan de Poincaré : $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\,(\tau) > 0\}$

Groupe modulaire elliptique : $\Gamma = \mathrm{SL}_2(\mathbb{Z})$

engendré par $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

Action de groupe : $\Gamma \times \mathcal{H} \to \mathcal{H}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

$$S\tau = \frac{-1}{\tau} \qquad T\tau = \tau + 1$$

Fonctions modulaires

$\Gamma' \subset \Gamma$ (d'indice fini)

Définition : $f : \mathcal{H} \to \mathbb{C}$ est une fonction modulaire pour Γ' si

- f est méromorphe sur $\mathcal{H}$
- pour tous $\gamma \in \Gamma'$ et $\tau \in \mathcal{H}$,

$$f(\gamma\tau) = f(\tau)$$

- f est méromorphe aux pointes

Proposition :

une fonction modulaire a toujours une période entière

(donc une série de Fourier)

Theta constantes

Définition :

$\tau \in \mathcal{H}$, $q = e^{\pi i \tau}$,

$$\begin{aligned}
\theta_0(\tau) &:= \sum_{n\in\mathbb{Z}} q^{n^2} && = 1 + 2\sum_{n\geqslant 1} q^{n^2}, \\
\theta_1(\tau) &:= \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2} && = 1 + 2\sum_{n\geqslant 1} (-1)^n q^{n^2}, \\
\theta_2(\tau) &:= \sum_{n\in\mathbb{Z}} q^{\left(n+\frac{1}{2}\right)^2} && = 2q^{\frac{1}{4}}\left(1 + \sum_{n\geqslant 1} q^{n^2+n}\right)
\end{aligned}$$

Propriétés des theta constantes

Formules de duplication :

$$\left.\begin{aligned} \theta_0^2(2\tau) &= \frac{\theta_0^2(\tau)+\theta_1^2(\tau)}{2} \\ \theta_1^2(2\tau) &= \theta_0(\tau)\cdot\theta_1(\tau) \\ \theta_2^2(2\tau) &= \frac{\theta_0^2(\tau)-\theta_1^2(\tau)}{2} \end{aligned}\right\} \Rightarrow \begin{array}{c} \text{pour tout } \tau \in \mathcal{H}, \\ \left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right)_{n\in\mathbb{N}} \\ \text{est une suite AGM de limite 1} \end{array}$$

Égalité de Jacobi :

$$\theta_0^4 = \theta_1^4 + \theta_2^4$$

Propriétés des theta constantes

Formules de transformation :

$$\begin{aligned} \theta_0^2(T\tau) &= \theta_1^2(\tau) & \qquad \theta_0^2(S\tau) &= -i\tau\theta_0^2(\tau) \\ \theta_1^2(T\tau) &= \theta_0^2(\tau) & \qquad \theta_1^2(S\tau) &= -i\tau\theta_2^2(\tau) \\ \theta_2^2(T\tau) &= i\theta_2^2(\tau) & \qquad \theta_2^2(S\tau) &= -i\tau\theta_1^2(\tau) \end{aligned}$$

plus généralement, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$:

$$\theta_s^2\left(\frac{a\tau + b}{c\tau + d}\right) = \omega(\gamma, s)(c\tau + d)\theta_{\sigma(\gamma,s)}^2(\tau)$$

$\Rightarrow$ passer aux quotients !

Fonctions k et k'

Définition :

$$k'(\tau) = \frac{\theta_1^2}{\theta_0^2}(\tau) \qquad k(\tau) = \frac{\theta_2^2}{\theta_0^2}(\tau)$$

Égalité de Jacobi :

$$k'^2 + k^2 = 1$$

Formules de transformation :

$$k'(T\tau) = \frac{1}{k'(\tau)}, \quad k'(S\tau) = k(\tau), \quad k(T\tau) = i\frac{k(\tau)}{k'(\tau)}, \quad k(S\tau) = k'(\tau)$$

k' est une fonction modulaire pour

$$\Gamma_{k'} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : b \equiv 0 \bmod 2, c \equiv 0 \bmod 4 \right\}$$

La fonction j

Définition :

$$j(\tau) = 256 \frac{\left(1 - k'^2(\tau) + k'^4(\tau)\right)^3}{k'^4(\tau)\left(1 - k'^2(\tau)\right)^2}$$

$\Rightarrow j$ est une fonction modulaire pour Γ

$$j(\tau) = \frac{1}{q^2} + 744 + 196884q^2 + 21493760q^4 + \dots$$

Théorème :

deux fonctions modulaires sont liées algébriquement
(polynôme modulaire)

Exemple : $k^2 + k'^2 = 1$, k' et j,...

Retour sur l'AGM

$a, b \in \mathbb{C} \setminus \{0\}$ et $a \neq \pm b$

$\Rightarrow$ il existe $\tau \in \mathcal{H}$ tel que

$$\frac{b}{a} = k'(\tau)$$

Théorème :

$$\mathcal{L}(a,b) = \left\{ \frac{a}{\theta_0^2(\gamma\tau)} : \gamma \in \Gamma_{k'} \right\} \cup \{0\}$$

et le réseau sous-jacent ?

si $\gamma = \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) \in \Gamma_{k'}$ avec $d \equiv 1 \bmod 4$, alors

$$\frac{a}{\theta_0^2(\gamma\tau)} = \frac{a}{\theta_0^2(\tau)(c\tau + d)}$$

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- AGM et évaluation de fonctions modulaires
- Généralisation (Borchardt)

Évaluation de fonctions modulaires

Objectif : étant donné $\tau \in \mathcal{H}$, évaluer $k', j, \ldots$ en τ

On peut se restreindre à k'

Utilisation de polynômes modulaires connus :

$$f(\tau) \text{ est racine de } \Phi_{f,k'}\left(X, k'(\tau)\right)$$

$\longrightarrow$ itérations de Newton sur ce polynôme !

Un premier type d'algorithmes

Utilisation des séries en q : $k' = \left(\frac{\theta_1}{\theta_0}\right)^2$

$$\theta_0(\tau) = 1 + 2\sum_{n\geqslant 1} q^{n^2} \qquad \theta_1(\tau) = 1 + 2\sum_{n\geqslant 1} (-1)^n q^{n^2}$$

Intérêt :

- ces séries sont creuses
- les coefficients valent ± 1
- $q \mapsto \{q, q^4, \ldots, q^{n^2}\}$: $2n-1$ multiplications
  $(q^{(n+1)^2} = q^{n^2} q^{2n+1})$
- partage des calculs

Complexité : $O(\mathcal{M}(N)\sqrt{N})$ pour une précision de N bits

INRIA FUTURS LIX

Utilisation des suites AGM

- pour tout $\tau \in \mathcal{H}$, on a la suite AGM

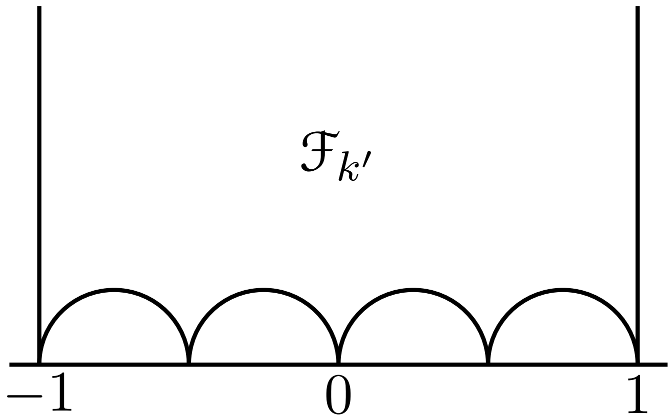
$$\left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right) \to 1$$

- donc il existe une suite AGM partant de $(1, k'(\tau))$ et convergeant vers $\frac{1}{\theta_0^2(\tau)}$

Problème : quels sont les choix de racines correspondant à ces suites ?

Théorème [Gauss] : pour tout $\tau \in \mathcal{F}_{k'}$,
M est analytique en τ et

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)}$$



AGM : calcul de τ à partir de $k'(\tau)$

si τ et $S\tau \in \mathfrak{F}_{k'}$,

$$M\left(k(\tau)\right) = M\left(k'(S\tau)\right) = \frac{1}{\theta_0^2(S\tau)} = \frac{i}{\tau\theta_0^2(\tau)}$$

de plus

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)}$$

on a donc

$$\tau = \frac{iM\left(k'(\tau)\right)}{M\left(k(\tau)\right)} = \frac{iM\left(k'(\tau)\right)}{M\left(\sqrt{1-k'^2(\tau)}\right)}$$

car $k^2(\tau) + k'^2(\tau) = 1$

Évaluation de k' : le principe

$\Rightarrow$ on pose

$$f_\tau(z) = iM(z) - \tau M\left(\sqrt{1-z^2}\right)$$

pour tout $\tau \in \mathfrak{F}_{k'}$ et $S\tau \in \mathfrak{F}_{k'}$,

- $f_\tau\left(k'(\tau)\right) = 0$
- f_τ est analytique
- $$\frac{df_\tau}{dz}\left(k'(\tau)\right) = \frac{-2}{\pi\tau\theta_1^2(\tau)\theta_2^4(\tau)} \neq 0$$

$\Rightarrow$ k' peut être évaluée par des itérations de Newton sur f_τ

Une suite convergeant vers $k'(\tau)$

z_0 approximation “assez précise” de $k'(\tau)$ (séries en q)

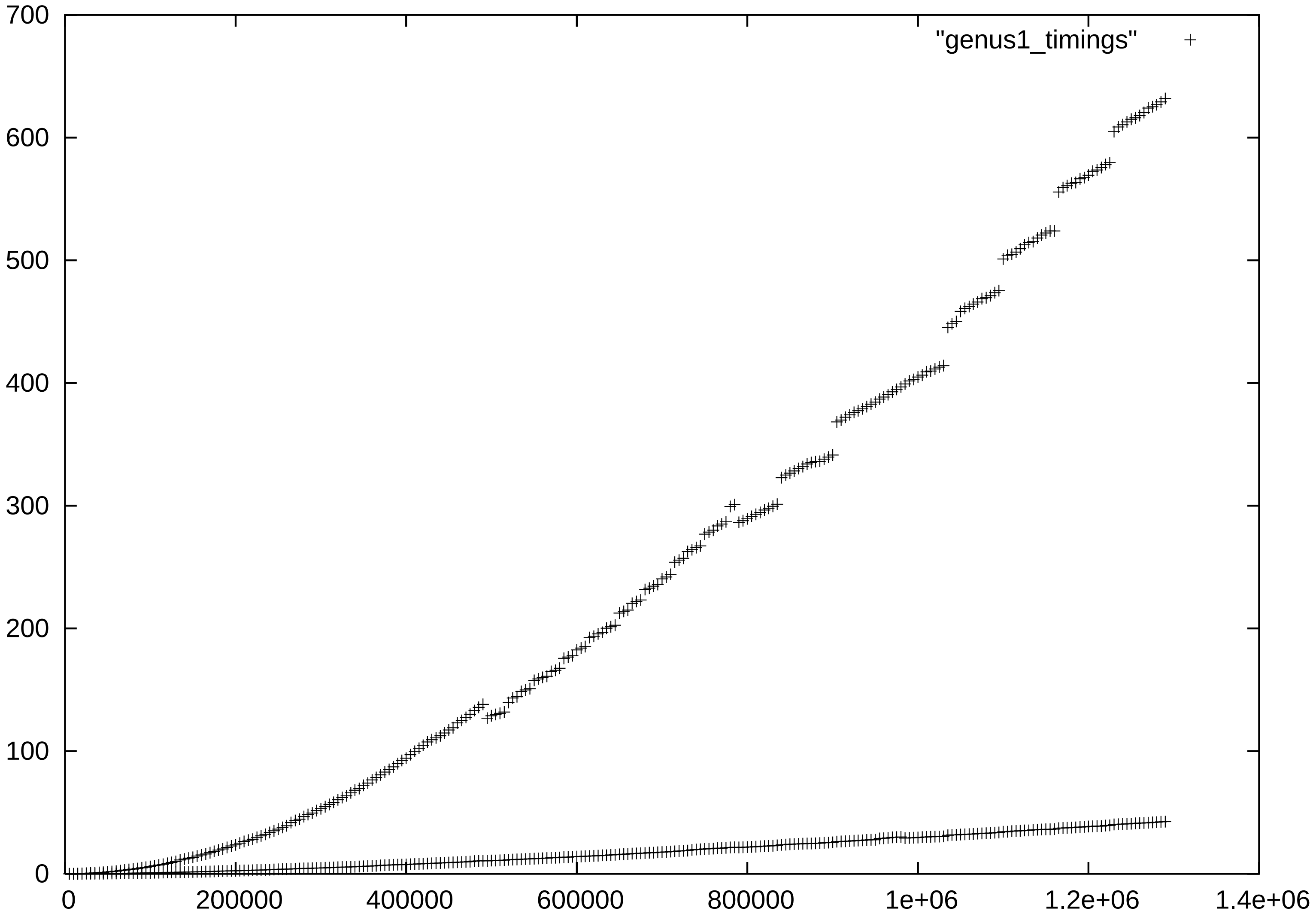
$$z_{n+1} = z_n + \frac{\pi\tau z_n(1 - z_n^2)\left(iM(z_n) - \tau M\left(\sqrt{1 - z_n^2}\right)\right)}{2M(z_n)^3}$$

$\Rightarrow (z_n)$ converge *quadratiquement* vers $k'(\tau)$

Complexité de l’évaluation de k' (Dupont):

$$O\left(\mathcal{M}(N)\log N\right)$$

. . . et ça marche !



"genus1_timings"
700
600
500
400
300
200
100
0
0
200000
400000
600000
800000
1e+06
1.2e+06
1.4e+06

Évaluation du logarithme

Cas réel : Salamin, Borwein & Borwein

Idée : lorsque $\mathrm{Im}\,(\tau) \gg 0$,

$$\log k(\tau) \simeq \log 4q^{\frac{1}{2}} = 2\log 2 + \frac{i\pi\tau}{2} \qquad \mathrm{M}\,(k(\tau)) = \frac{i}{\tau\theta_0^2(\tau)} \simeq \frac{i}{\tau}$$

Proposition (Dupont) :

soit $z \in \mathbb{C}^\times$ tel que $|z| \leqslant 2^{-12}$ et $|\mathrm{Arg}(z)| \leqslant \frac{\pi}{4}$, alors

$$\left|\log z + \frac{\pi}{2\mathrm{M}(4z)}\right| \leqslant 4.16\,|z|^2\,(1 + |\log z|)$$

Complexité (évaluation du log) :

$$O\left(\mathcal{M}(N)\log N\right)$$

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- AGM et évaluation de fonctions modulaires
- Généralisation (Borchardt)

Généralisation

$$\mathcal{H} \to \mathcal{H}_g \quad (\text{matrices } g \times g \text{ symétriques, } \mathrm{Im}\,(\tau) > 0)$$

$$\Gamma \to \Gamma_g \quad (\text{certaines matrices entières } 2g \times 2g)$$

Action de groupe : $\Gamma_g \times \mathcal{H}_g \to \mathcal{H}_g$

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \tau = (A\tau + B)(C\tau + D)^{-1}$$

Lien avec les courbes de genre g (par ex. : $y^2 = x^{2g+1} + \ldots$)

Theta constantes

$\vec{a}, \vec{b} \in \{0,1\}^g$

Définition générale :

$$\theta_{\vec{a},\vec{b}}(\tau) = \sum_{\vec{n}\in\mathbb{Z}^g} \exp\left(\pi i \, {}^t\!\left(\vec{n} + \frac{\vec{a}}{2}\right) \tau \left(\vec{n} + \frac{\vec{a}}{2}\right) + {}^t\!\left(\vec{n} + \frac{\vec{a}}{2}\right) \vec{b}\right)$$

si $\vec{a} = \vec{0}$, on a 2^g fonctions de la forme

$$\theta_{\vec{0},\vec{b}}(\tau) = \sum_{\vec{n}\in\mathbb{Z}^g} (-1)^{{}^t\vec{n}\vec{b}} \exp\left(\pi i {}^t\vec{n}\tau\vec{n}\right)$$

Évaluation par sommation :

$$O\left(\mathcal{M}(N) N^{\frac{g}{2}}\right)$$

INRIA FUTURS LIX

Résumé de l'épisode précédent

Ingrédients :

- formules de duplication
- formules de transformation (action de Γ)
- lien avec l'AGM
- algorithme $k'(\tau) \longrightarrow \tau$
- itérations de Newton : $\tau \longrightarrow k'(\tau)$

Formules de duplication

Dans le cas $g = 2$:

$$\begin{aligned}
\theta_0^2(2\tau) &= \frac{\theta_0^2(\tau)+\theta_1^2(\tau)+\theta_2^2(\tau)+\theta_3^2(\tau)}{4} \\
\theta_1^2(2\tau) &= \frac{\theta_0(\tau)\theta_1(\tau)+\theta_2(\tau)\theta_3(\tau)}{2} \\
\theta_2^2(2\tau) &= \frac{\theta_0(\tau)\theta_2(\tau)+\theta_1(\tau)\theta_3(\tau)}{2} \\
\theta_3^2(2\tau) &= \frac{\theta_0(\tau)\theta_3(\tau)+\theta_1(\tau)\theta_2(\tau)}{2}
\end{aligned}$$

…et des formules similaires pour les autres theta constantes

$\Rightarrow$ toutes les theta constantes sont liées algébriquement aux 2^g premières, par ex. :

$$\theta_4^8 - (\theta_0^4 - \theta_1^4 + \theta_2^4 - \theta_3^4)\theta_4^4 + (\theta_0^2\theta_2^2 - \theta_1^2\theta_3^2)^2 = 0$$

Formules de transformation

si $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$,

$$\theta_s^2(\gamma\tau) = \omega(\gamma, s)\mathrm{Det}(C\tau + D)\theta^2_{\sigma(\gamma,s)}(\tau)$$

$\Rightarrow$ notion de fonctions modulaires de Siegel

$$T_{a,b}(\tau) := \frac{\theta^2_{a,b}(\tau)}{\theta^2_{0,0}(\tau)} \text{ est une telle fonction (généralise } k \text{ et } k'\text{)}$$

Moyenne de Borchardt

$$\begin{aligned} a_{n+1} &= \frac{a_n+b_n+c_n+d_n}{4} \\ b_{n+1} &= \frac{\sqrt{a_n}\sqrt{b_n}+\sqrt{c_n}\sqrt{d_n}}{2} \\ c_{n+1} &= \frac{\sqrt{a_n}\sqrt{c_n}+\sqrt{b_n}\sqrt{d_n}}{2} \\ d_{n+1} &= \frac{\sqrt{a_n}\sqrt{d_n}+\sqrt{b_n}\sqrt{c_n}}{2} \end{aligned}$$

(formules similaires pour 2^g éléments)

Théorème (Dupont) :

- il y a toujours une limite unique
- notion de bon/mauvais choix ($\sqrt{b_n}$, $\sqrt{c_n}$, $\sqrt{d_n}$ “proches” de $\sqrt{a_n}$)
- caractérisation des suites ayant une limite nulle
- convergence quadratique si la limite est non nulle

Remarque sur les suites de Borchardt

- pour tout $\tau \in \mathcal{H}_g$, on a une suite de Borchardt

$$\left(\theta_{0,b}^2(2^n\tau)\right)_{b\in\{0,1\}^g, n\in\mathbb{N}} \longrightarrow 1$$

- donc il existe une suite de Borchardt partant de

$$(T_{0,b}(\tau))_{b\in\{0,1\}^g, n\in\mathbb{N}}$$

convergeant vers $\frac{1}{\theta_{0,0}^2(\tau)}$

(Gros) problème : quels sont les choix de racines correspondants ?

Conjectures, méthodes numériques mais pas de résultat satisfaisant !

Conjecture ($g = 2$)

Conjecture : pour tous $\tau \in \mathcal{F}_2$ et

$$\gamma \in \left\{ I, \begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \right\},$$

la suite $\left(\theta_{0,b}^2(2^n \gamma \tau)\right)_{n \in \mathbb{N}}$ ne contient que des bons choix de racines

La brique de base

Objectif : étant donnés les $T_{0,b}(\tau)$, déterminer τ

Algorithme :

- déterminer les $T_{a,b}(\tau)$ (équations modulaires)
- pour certaines matrices $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$ bien choisies
  - déterminer les $T_{0,b}(\gamma\tau)$ (formules de transformation)
  - déterminer les $\theta^2_{0,0}(\gamma\tau)$ (moyennes de Borchardt)
    $\longrightarrow$ choix de racines ?
  - en déduire $\mathrm{Det}(C\tau + D)$, *via*

$$\theta^2_{0,0}(\gamma\tau) = \omega(\gamma)\mathrm{Det}(C\tau + D)\theta^2_{\sigma(\gamma)}(\tau)$$

- en déduire τ

INRIA FUTURS LIX

En pratique...

Complexité :

$$O\left(g^2 2^g \mathcal{M}(N) \log N\right)$$

Dans le cas du genre 2 :

- on se ramène au cas où $\tau \in \mathcal{F}_2$
- utilisation de la conjecture pour le choix des racines
- variante prouvée : plus difficile à implanter

En genre $g \geqslant 3$:

- domaines fondamentaux moins bien connus
- pas de conjectures pour les choix de racines
- possible en théorie mais sans doute très lent

Utilisations

Tel quel : détermination de matrices de Riemann

- courbe hyperelliptique $\longrightarrow \tau$ sous-jacent
  (utilisation des formules de Thomae)
- implanté en genre 2
- complexité : $O\left(g^2 2^g \mathcal{M}(N) \log N\right)$

Évaluation rapide des theta constantes en genre 2

- $\tau \in \mathcal{F}_2 \longrightarrow \theta_{a,b}(\tau)$
  inversion de l'algorithme *via* des itérations de Newton trivariées
- méthode heuristique (pas de preuve de convergence)
- complexité (heuristique) : $O\left(\mathcal{M}(N) \log N\right)$

Applications

L'évaluation rapide des theta constantes en genre 2 permet

- le calcul de polynômes de classe en genre 2 (multiplication complexe, travail en cours avec T. Houtmann)
- le calcul de polynômes modulaires en genre 2
  - méthode d'évaluation/interpolation
  - utilise aussi l'évaluation rapide de matrices de Riemann
  - encore très expérimental

Polynômes modulaires ($g = 2$)

$\Phi_{p,1}, \Phi_{p,2}, \Phi_{p,3}$ 3 polynômes de $\mathbb{Z}(j_1, j_2, j_3)[X]$

Calcul :

évaluation/interpolation

$p = 2$:

30 Mo compressé

Dénominateur =

$$236196 j_1^5 - 972 j_1^4 j_2^2 + 5832 j_1^4 j_2 j_3 + 19245600 j_1^4 j_2 - 8748 j_1^4 j_3^2 - 104976000 j_1^4 j_3 + 125971200000 j_1^4 + j_1^3 j_2^4$$
$$-12 j_1^3 j_2^3 j_3 - 77436 j_1^3 j_2^3 + 54 j_1^3 j_2^2 j_3^2 + 870912 j_1^3 j_2^2 j_3 - 507384000 j_1^3 j_2^2 - 108 j_1^3 j_2 j_3^3 - 3090960 j_1^3 j_2 j_3^2$$
$$+2099520000 j_1^3 j_2 j_3 + 81 j_1^3 j_3^4 + 3499200 j_1^3 j_3^3 + 78 j_1^2 j_2^5 - 1332 j_1^2 j_2^4 j_3 + 592272 j_1^2 j_2^4 + 8910 j_1^2 j_2^3 j_3^2$$
$$-4743360 j_1^2 j_2^3 j_3 - 29376 j_1^2 j_2^2 j_3^3 + 9331200 j_1^2 j_2^2 j_3^2 + 47952 j_1^2 j_2 j_3^4 - 31104 j_1^2 j_3^5 - 159 j_1 j_2^6 + 1728 j_1 j_2^5 j_3$$
$$-41472 j_1 j_2^5 - 6048 j_1 j_2^4 j_3^2 + 6912 j_1 j_2^3 j_3^3 + 80 j_2^7 - 384 j_2^6 j_3$$

INRIA FUTURS

Dénominateur de Φ_3

$$2^{4} \times 3^{31} \times 5^{5} \times 19^{10} \times 29^{5} j_1^{12} - 2^{4} \times 3^{32} \times 19^{5} \times 47 \times 17064586291\, j_1^{13} + 2^{6} \times 3^{31} \times 5^{3} \times 13 \times 19^{7} \times 29^{2} \times 131 \times 1949\, j_1^{12} j_3 - 2^{4} \times 3^{30} \times 5^{2} \times 7 \times 19^{6} \times 29 \times 4701082031\, j_1^{12} j_2 + 2^{11} \times 3^{28} \times 5^{4} \times 19^{8} \times 29^{3} \times 5557\, j_1^{11} j_2 j_3$$
$$-2^{9} \times 3^{27} \times 5^{3} \times 19^{9} \times 23 \times 29^{2} \times 37 \times 149\, j_1^{11} j_2^{2} - 2^{2} \times 3^{30} \times 11^{12} j_1^{14} + 2^{12} \times 3^{29} \times 5 \times 11^{5} \times 19^{2} \times 41 \times 1399\, j_1^{13} j_3 - 2^{5} \times 3^{27} \times 19^{4} \times 59 \times 109 \times 6570848059\, j_1^{12} j_3^{2} + 2^{9} \times 3^{24} \times 5^{2} \times 19^{6} \times 29 \times 449 \times 160827643\, j_1^{11} j_3^{3}$$
$$-2^{3} \times 3^{28} \times 7 \times 11^{5} \times 19 \times 305677787\, j_1^{13} j_2 + 2^{8} \times 3^{26} \times 11 \times 19^{3} \times 12997844123599\, j_1^{12} j_2 j_3 - 2^{5} \times 3^{24} \times 5 \times 11 \times 19^{5} \times 3517 \times 53807008819\, j_1^{11} j_2 j_3^{2} - 2^{2} \times 3^{25} \times 19^{2} \times 163 \times 368477994090277\, j_1^{12} j_2^{2}$$
$$+2^{7} \times 3^{23} \times 19^{4} \times 64634951 \times 486375839\, j_1^{11} j_2^{2} j_3 + 2^{9} \times 3^{24} \times 5^{2} \times 7 \times 11 \times 19^{6} \times 29 \times 61 \times 241 \times 59051\, j_1^{10} j_2 j_3^{2} - 2^{3} \times 3^{21} \times 19^{3} \times 225900161 \times 27135844457\, j_1^{11} j_2^{3} - 2^{9} \times 3^{23} \times 5 \times 11 \times 19^{5} \times 23413242718669\, j_1^{10} j_2^{3} j_3$$
$$+2^{5} \times 3^{22} \times 19^{4} \times 83 \times 349813 \times 4414606477\, j_1^{10} j_2^{4} - 2^{9} \times 3^{24} \times 13 \times 19^{5} \times 41 \times 7849496341\, j_1^{9} j_2^{5} - 2^{4} \times 3^{28} \times 11^{10} j_1^{13} j_2^{2} + 2^{7} \times 3^{26} \times 5^{2} \times 11^{3} \times 19 \times 239 \times 592133\, j_1^{12} j_2^{3} - 2^{6} \times 3^{24} \times 13 \times 19^{3} \times 53 \times 953 \times 289296559\, j_1^{11} j_2^{4}$$
$$-2^{12} \times 3^{27} \times 19^{5} \times 7943431\, j_1^{10} j_3^{5} + 2^{5} \times 3^{27} \times 11^{10} j_1^{13} j_2 j_3 - 2^{6} \times 3^{26} \times 11^{3} \times 30977 \times 3469639\, j_1^{12} j_2 j_3^{2} + 2^{9} \times 3^{23} \times 13 \times 19^{2} \times 557 \times 62927 \times 2729633\, j_1^{11} j_2 j_3^{3} + 2^{11} \times 3^{23} \times 19^{4} \times 36533154133859\, j_1^{10} j_2 j_3^{4} - 2^{4} \times 3^{26} \times 11^{10} j_1^{13} j_3^{2}$$
$$+2^{4} \times 3^{25} \times 11^{3} \times 149 \times 263 \times 277 \times 32099\, j_1^{12} j_2^{2} j_3 - 2^{4} \times 3^{23} \times 19 \times 251 \times 433 \times 2039 \times 1155491891\, j_1^{11} j_2^{2} j_3^{2} - 2^{10} \times 3^{22} \times 19^{3} \times 73 \times 518831 \times 107124221\, j_1^{10} j_2^{2} j_3^{3} - 2^{2} \times 3^{23} \times 5 \times 11^{3} \times 23 \times 59 \times 71 \times 2390879\, j_1^{12} j_3^{3}$$
$$+2^{8} \times 3^{21} \times 5 \times 7 \times 19 \times 607819187655293\, j_1^{11} j_3^{3} j_3 + 2^{7} \times 3^{23} \times 11 \times 19^{2} \times 2909 \times 2301281960303\, j_1^{10} j_3^{3} j_3^{2} + 2^{13} \times 3^{23} \times 19^{4} \times 858883 \times 6258697\, j_1^{9} j_2^{3} j_3^{3} - 2^{2} \times 3^{20} \times 11 \times 29221 \times 13097683362521\, j_1^{11} j_2^{4}$$
$$-2^{12} \times 3^{20} \times 13 \times 19 \times 853 \times 49417 \times 334911601\, j_1^{10} j_2^{4} j_3 - 2^{12} \times 3^{21} \times 19^{3} \times 1136567 \times 1232464019\, j_1^{9} j_2^{4} j_3^{2} + 2^{4} \times 3^{19} \times 5 \times 7^{2} \times 17 \times 103 \times 353583879893971\, j_1^{10} j_2^{5} + 2^{10} \times 3^{20} \times 5^{3} \times 19^{2} \times 2879 \times 10457 \times 21317083\, j_1^{9} j_2^{5} j_3$$
$$-2^{6} \times 3^{19} \times 19 \times 29 \times 449 \times 51131 \times 9269294087\, j_1^{9} j_2^{6} - 2^{12} \times 3^{21} \times 19^{3} \times 157 \times 193077561767\, j_1^{8} j_2^{6} j_3 + 2^{11} \times 3^{21} \times 5 \times 7 \times 13 \times 19^{2} \times 47 \times 9019003787\, j_1^{8} j_2^{7} - 2^{4} \times 3^{25} \times 5 \times 11^{8} j_1^{12} j_3^{4} - 2^{8} \times 3^{24} \times 11 \times 23 \times 359 \times 5363887\, j_1^{11} j_3^{5}$$
$$+2^{7} \times 3^{21} \times 5 \times 7 \times 19^{2} \times 5241332618339\, j_1^{10} j_3^{6} + 2^{6} \times 3^{24} \times 5 \times 11^{8} j_1^{12} j_2 j_3^{3} + 2^{6} \times 3^{23} \times 11 \times 13^{2} \times 4084495637\, j_1^{11} j_2 j_3^{4} - 2^{14} \times 3^{21} \times 19 \times 46021575357193\, j_1^{10} j_2 j_3^{5} - 2^{11} \times 3^{26} \times 5 \times 19^{3} \times 2251 \times 22807\, j_1^{9} j_2 j_3^{6} - 2^{5} \times 3^{24} \times 5 \times 11^{8} j_1^{12} j_2^{2} j_3^{2}$$
$$-2^{6} \times 3^{22} \times 7 \times 11 \times 145580724439\, j_1^{11} j_2^{2} j_3^{3} + 2^{4} \times 3^{20} \times 7 \times 233 \times 81899 \times 13955891671\, j_1^{10} j_2^{2} j_3^{4} + 2^{13} \times 3^{20} \times 7 \times 19^{2} \times 51787 \times 163788913\, j_1^{9} j_2^{2} j_3^{5} + 2^{6} \times 3^{22} \times 5 \times 11^{8} j_1^{12} j_2^{3} j_3 + 2^{3} \times 3^{21} \times 11 \times 23 \times 59 \times 24749 \times 164011\, j_1^{11} j_2^{3} j_3^{2}$$
$$-2^{6} \times 3^{18} \times 1527894629629140391\, j_1^{10} j_2^{3} j_3^{3} - 2^{7} \times 3^{19} \times 19 \times 289629349486378333\, j_1^{9} j_2^{3} j_3^{4} - 2^{4} \times 3^{21} \times 5 \times 11^{8} j_1^{12} j_2^{4} - 2^{4} \times 3^{20} \times 5^{2} \times 7 \times 11 \times 24509 \times 182029\, j_1^{11} j_2^{4} j_3 + 2^{3} \times 3^{18} \times 110246267 \times 22315765057\, j_1^{10} j_2^{4} j_3^{2}$$
$$+2^{11} \times 3^{19} \times 367 \times 501746471342317\, j_1^{9} j_2^{4} j_3^{3} + 2^{11} \times 3^{20} \times 19^{2} \times 331691 \times 332432941\, j_1^{8} j_2^{4} j_3^{4} + 2^{3} \times 3^{19} \times 5^{2} \times 7 \times 11 \times 13^{2} \times 317 \times 10753\, j_1^{11} j_2^{5} - 2^{9} \times 3^{17} \times 104067191 \times 116556229\, j_1^{10} j_2^{5} j_3 - 2^{5} \times 3^{17} \times 281 \times 701 \times 143110201279489\, j_1^{9} j_2^{5} j_3^{2}$$
$$-2^{18} \times 3^{18} \times 19^{2} \times 71 \times 1373 \times 87398407\, j_1^{8} j_2^{5} j_3^{3} + 3^{15} \times 13 \times 104543 \times 1759532749063\, j_1^{10} j_2^{6} + 2^{6} \times 3^{16} \times 3785393 \times 1469365755259\, j_1^{9} j_2^{6} j_3 + 2^{7} \times 3^{17} \times 11 \times 1279 \times 530730870516383\, j_1^{8} j_2^{6} j_3^{2} - 2^{3} \times 3^{16} \times 67 \times 251 \times 541 \times 254161305991\, j_1^{9} j_2^{7}$$
$$-2^{11} \times 3^{16} \times 5^{2} \times 17 \times 109 \times 28909 \times 176172169\, j_1^{8} j_2^{7} j_3 - 2^{11} \times 3^{18} \times 5^{2} \times 19 \times 179 \times 4003 \times 14631839\, j_1^{7} j_2^{7} j_3^{2} + 2^{4} \times 3^{16} \times 1829155862631992107\, j_1^{8} j_2^{8} + 2^{13} \times 3^{16} \times 11 \times 127 \times 47387 \times 24532093\, j_1^{7} j_2^{8} j_3$$
$$+2^{7} \times 3^{15} \times 7 \times 127 \times 683 \times 17981 \times 1014557\, j_1^{7} j_2^{9} + 2^{11} \times 3^{16} \times 5 \times 15121 \times 24071 \times 39419\, j_1^{6} j_2^{10} - 2^{7} \times 3^{21} \times 5 \times 11^{6} j_1^{11} j_3^{6} + 2^{9} \times 3^{20} \times 139 \times 9439 \times 23357\, j_1^{10} j_3^{7} - 2^{15} \times 3^{20} \times 5 \times 7 \times 19 \times 739425329\, j_1^{9} j_3^{8} + 2^{8} \times 3^{21} \times 5 \times 11^{6} j_1^{11} j_2 j_3^{5}$$
$$-2^{8} \times 3^{19} \times 5 \times 31 \times 2837900633\, j_1^{10} j_2 j_3^{6} + 2^{12} \times 3^{21} \times 11549 \times 309353347\, j_1^{9} j_2 j_3^{7} - 2^{7} \times 3^{20} \times 5^{2} \times 11^{6} j_1^{11} j_2^{2} j_3^{4} + 2^{6} \times 3^{19} \times 5 \times 29501 \times 12118591\, j_1^{10} j_2^{2} j_3^{5} - 2^{10} \times 3^{18} \times 23 \times 2549 \times 3359 \times 2306753\, j_1^{9} j_2^{2} j_3^{6} - 2^{16} \times 3^{20} \times 7 \times 19 \times 955597939\, j_1^{8} j_2^{2} j_3^{7}$$
$$+2^{9} \times 3^{18} \times 5^{2} \times 11^{6} j_1^{11} j_2^{3} j_3^{3} - 2^{4} \times 3^{17} \times 5^{2} \times 17 \times 23563 \times 3595639\, j_1^{10} j_2^{3} j_3^{4} + 2^{9} \times 3^{17} \times 7 \times 11 \times 13 \times 80077 \times 22613431\, j_1^{9} j_2^{3} j_3^{5} + 2^{14} \times 3^{20} \times 19 \times 128219302819\, j_1^{8} j_2^{3} j_3^{6} - 2^{7} \times 3^{18} \times 5^{2} \times 11^{6} j_1^{11} j_2^{4} j_3^{2} + 2^{6} \times 3^{16} \times 5 \times 19 \times 94637239717\, j_1^{10} j_2^{4} j_3^{3}$$
$$-2^{8} \times 3^{17} \times 1051 \times 2099 \times 675639527\, j_1^{9} j_2^{4} j_3^{4} - 2^{12} \times 3^{18} \times 7 \times 17892676054037\, j_1^{8} j_2^{4} j_3^{5} + 2^{8} \times 3^{17} \times 5 \times 11^{6} j_1^{11} j_2^{5} j_3 - 2^{5} \times 3^{16} \times 17 \times 1553 \times 7177 \times 18797\, j_1^{10} j_2^{5} j_3^{2} + 2^{7} \times 3^{15} \times 7 \times 229 \times 25919 \times 168130307\, j_1^{9} j_2^{5} j_3^{3}$$
$$+2^{10} \times 3^{19} \times 23^{2} \times 217454967241\, j_1^{8} j_2^{5} j_3^{4} + 2^{16} \times 3^{19} \times 7 \times 65032448497\, j_1^{7} j_2^{5} j_3^{5} - 2^{7} \times 3^{15} \times 5 \times 11^{6} j_1^{11} j_2^{6} + 2^{7} \times 3^{14} \times 5 \times 29 \times 47 \times 2777 \times 46199\, j_1^{10} j_2^{6} j_3 - 2^{5} \times 3^{14} \times 613 \times 217319 \times 101345213\, j_1^{9} j_2^{6} j_3^{2} - 2^{9} \times 3^{16} \times 2372756188260637\, j_1^{8} j_2^{6} j_3^{3}$$
$$-2^{14} \times 3^{17} \times 6311 \times 5256671467\, j_1^{7} j_2^{6} j_3^{4} - 2^{4} \times 3^{13} \times 5 \times 47 \times 61091 \times 67733\, j_1^{10} j_2^{7} + 2^{6} \times 3^{14} \times 19 \times 877 \times 36902721601\, j_1^{9} j_2^{7} j_3 + 2^{8} \times 3^{15} \times 29 \times 457 \times 174799 \times 1336561\, j_1^{8} j_2^{7} j_3^{2} + 2^{12} \times 3^{16} \times 17 \times 41 \times 409599151231\, j_1^{7} j_2^{7} j_3^{3}$$
$$-2^{5} \times 3^{12} \times 507349 \times 860517659\, j_1^{9} j_2^{8} - 2^{6} \times 3^{14} \times 11 \times 19 \times 31 \times 379 \times 1758651787\, j_1^{8} j_2^{8} j_3 - 2^{10} \times 3^{16} \times 19 \times 181 \times 12923 \times 8578123\, j_1^{7} j_2^{8} j_3^{2} - 2^{16} \times 3^{17} \times 130729 \times 7167367\, j_1^{6} j_2^{8} j_3^{3} + 2^{4} \times 3^{13} \times 2502264181899431\, j_1^{8} j_2^{9}$$
$$+2^{9} \times 3^{14} \times 499 \times 2185411087481\, j_1^{7} j_2^{9} j_3 + 2^{14} \times 3^{14} \times 13 \times 171233 \times 29973487\, j_1^{6} j_2^{9} j_3^{2} - 2^{8} \times 3^{14} \times 5^{2} \times 7 \times 23593 \times 32337101\, j_1^{7} j_2^{10} - 2^{12} \times 3^{14} \times 7 \times 29 \times 43 \times 6319982881\, j_1^{6} j_2^{10} j_3 + 2^{10} \times 3^{12} \times 373 \times 4789 \times 69109921\, j_1^{6} j_2^{11}$$
$$-2^{16} \times 3^{14} \times 4969 \times 300359489\, j_1^{5} j_2^{11} j_3 + 2^{14} \times 3^{13} \times 5 \times 73 \times 139 \times 163 \times 520963\, j_1^{5} j_2^{12} - 2^{6} \times 3^{19} \times 5 \times 11^{4} j_1^{10} j_3^{8} + 2^{10} \times 3^{17} \times 63092123\, j_1^{9} j_3^{9} + 2^{17} \times 3^{20} \times 5\, j_1^{8} j_3^{10} + 2^{9} \times 3^{18} \times 5 \times 11^{4} j_1^{10} j_2 j_3^{7} - 2^{7} \times 3^{18} \times 7 \times 17 \times 71 \times 97 \times 509\, j_1^{9} j_2 j_3^{8}$$
$$-2^{14} \times 3^{17} \times 5 \times 269 \times 2061691\, j_1^{8} j_2 j_3^{9} - 2^{8} \times 3^{17} \times 5 \times 7 \times 11^{4} j_1^{10} j_2^{2} j_3^{6} + 2^{9} \times 3^{18} \times 108716203\, j_1^{9} j_2^{2} j_3^{7} + 2^{15} \times 3^{16} \times 9767 \times 1276579\, j_1^{8} j_2^{2} j_3^{8} + 2^{9} \times 3^{16} \times 5 \times 7 \times 11^{4} j_1^{10} j_2^{3} j_3^{5} - 2^{5} \times 3^{15} \times 5 \times 43 \times 79 \times 1528937\, j_1^{9} j_2^{3} j_3^{6}$$
$$-2^{12} \times 3^{15} \times 71 \times 691 \times 8114567\, j_1^{8} j_2^{3} j_3^{7} - 2^{15} \times 3^{17} \times 697542973\, j_1^{7} j_2^{3} j_3^{8} - 2^{7} \times 3^{15} \times 5^{2} \times 7 \times 11^{4} j_1^{10} j_2^{4} j_3^{4} + 2^{6} \times 3^{15} \times 5 \times 2083 \times 361447\, j_1^{9} j_2^{4} j_3^{5} + 2^{10} \times 3^{15} \times 449 \times 2748159773\, j_1^{8} j_2^{4} j_3^{6} + 2^{16} \times 3^{15} \times 5^{2} \times 11 \times 50130251\, j_1^{7} j_2^{4} j_3^{7}$$
$$+2^{9} \times 3^{14} \times 5 \times 7 \times 11^{4} j_1^{10} j_2^{5} j_3^{3} - 2^{5} \times 3^{15} \times 23 \times 27616361\, j_1^{9} j_2^{5} j_3^{4} - 2^{9} \times 3^{13} \times 13 \times 4091 \times 207679247\, j_1^{8} j_2^{5} j_3^{5} - 2^{13} \times 3^{14} \times 1181 \times 445809677\, j_1^{7} j_2^{5} j_3^{6} - 2^{8} \times 3^{13} \times 5 \times 7 \times 11^{4} j_1^{10} j_2^{6} j_3^{2} - 2^{7} \times 3^{12} \times 13 \times 73 \times 1319 \times 1549\, j_1^{9} j_2^{6} j_3^{3}$$
$$+2^{5} \times 3^{12} \times 1439 \times 1531 \times 79631081\, j_1^{8} j_2^{6} j_3^{4} + 2^{11} \times 3^{14} \times 449 \times 3900368627\, j_1^{7} j_2^{6} j_3^{5} + 2^{21} \times 3^{15} \times 5 \times 16351469\, j_1^{6} j_2^{6} j_3^{6} + 2^{9} \times 3^{12} \times 5 \times 11^{4} j_1^{10} j_2^{7} j_3 + 2^{5} \times 3^{12} \times 11 \times 254892401\, j_1^{9} j_2^{7} j_3^{2} - 2^{7} \times 3^{13} \times 11 \times 359 \times 19603 \times 41579\, j_1^{8} j_2^{7} j_3^{3}$$
$$-2^{8} \times 3^{12} \times 47 \times 307 \times 317 \times 13596893\, j_1^{7} j_2^{7} j_3^{4} - 2^{15} \times 3^{14} \times 7 \times 6661 \times 763381\, j_1^{6} j_2^{7} j_3^{5} - 2^{6} \times 3^{11} \times 5 \times 11^{4} j_1^{10} j_2^{8} - 2^{6} \times 3^{13} \times 5^{2} \times 139 \times 18149\, j_1^{9} j_2^{8} j_3 + 2^{6} \times 3^{10} \times 5 \times 53 \times 1901 \times 48725627\, j_1^{8} j_2^{8} j_3^{2} + 2^{9} \times 3^{11} \times 31 \times 1297 \times 707636873\, j_1^{7} j_2^{8} j_3^{3}$$
$$+2^{13} \times 3^{14} \times 37 \times 43 \times 59 \times 1413271\, j_1^{6} j_2^{8} j_3^{4} + 2^{5} \times 3^{8} \times 5 \times 47^{2} \times 142981\, j_1^{9} j_2^{9} - 2^{7} \times 3^{9} \times 11 \times 17 \times 79 \times 2683 \times 76343\, j_1^{8} j_2^{9} j_3 - 2^{5} \times 3^{12} \times 7^{3} \times 61 \times 24373 \times 55351\, j_1^{7} j_2^{9} j_3^{2} - 2^{12} \times 3^{11} \times 11 \times 53 \times 1069 \times 5642513\, j_1^{6} j_2^{9} j_3^{3}$$
$$-2^{16} \times 3^{14} \times 37 \times 59 \times 525313\, j_1^{5} j_2^{9} j_3^{4} + 2^{5} \times 3^{8} \times 5^{2} \times 31 \times 149 \times 11455231\, j_1^{8} j_2^{10} + 2^{6} \times 3^{9} \times 113 \times 351911687537\, j_1^{7} j_2^{10} j_3 + 2^{14} \times 3^{11} \times 13 \times 31 \times 373 \times 1597147\, j_1^{6} j_2^{10} j_3^{2} + 2^{16} \times 3^{11} \times 50925030661\, j_1^{5} j_2^{10} j_3^{3}$$
$$-2^{5} \times 3^{8} \times 7 \times 13 \times 1181 \times 99900863\, j_1^{7} j_2^{11} - 2^{9} \times 3^{10} \times 53 \times 373 \times 9857 \times 17053\, j_1^{6} j_2^{11} j_3 - 2^{13} \times 3^{10} \times 139 \times 5132331041\, j_1^{5} j_2^{11} j_3^{2} + 2^{5} \times 3^{8} \times 28476287051677\, j_1^{6} j_2^{12} + 2^{10} \times 3^{9} \times 1319 \times 3245505437\, j_1^{5} j_2^{12} j_3 + 2^{17} \times 3^{11} \times 13 \times 853 \times 180007\, j_1^{4} j_2^{12} j_3^{2}$$
$$-2^{7} \times 3^{8} \times 53 \times 109 \times 28493 \times 56957\, j_1^{5} j_2^{13} - 2^{14} \times 3^{9} \times 5 \times 18371 \times 1132141\, j_1^{4} j_2^{13} j_3 + 2^{13} \times 3^{8} \times 47 \times 61 \times 38025503\, j_1^{4} j_2^{14} - 2^{15} \times 3^{9} \times 7 \times 314130631\, j_1^{3} j_2^{15} - 2^{8} \times 3^{16} \times 11^{2} j_1^{9} j_3^{10} + 2^{14} \times 3^{17} \times 967\, j_1^{8} j_3^{11}$$
$$+2^{9} \times 3^{15} \times 5 \times 11^{2} j_1^{9} j_2 j_3^{9} - 2^{12} \times 3^{15} \times 5 \times 23 \times 1091\, j_1^{8} j_2 j_3^{10} + 2^{18} \times 3^{17} j_1^{7} j_2 j_3^{11} - 2^{8} \times 3^{16} \times 5 \times 11^{2} j_1^{9} j_2^{2} j_3^{8} + 2^{12} \times 3^{14} \times 211 \times 2939\, j_1^{8} j_2^{2} j_3^{9} - 2^{18} \times 3^{15} \times 149 \times 197\, j_1^{7} j_2^{2} j_3^{10} + 2^{11} \times 3^{14} \times 5 \times 11^{2} j_1^{9} j_2^{3} j_3^{7}$$
$$-2^{8} \times 3^{14} \times 7 \times 53 \times 26597\, j_1^{8} j_2^{3} j_3^{8} + 2^{14} \times 3^{14} \times 257 \times 18047\, j_1^{7} j_2^{3} j_3^{9} - 2^{9} \times 3^{13} \times 5 \times 7 \times 11^{2} j_1^{9} j_2^{4} j_3^{6} + 2^{11} \times 3^{13} \times 7 \times 113 \times 3121\, j_1^{8} j_2^{4} j_3^{7} - 2^{12} \times 3^{13} \times 11 \times 191 \times 39239\, j_1^{7} j_2^{4} j_3^{8} - 2^{18} \times 3^{15} \times 19^{2} \times 41\, j_1^{6} j_2^{4} j_3^{9}$$
$$+2^{10} \times 3^{13} \times 7 \times 11^{2} j_1^{9} j_2^{5} j_3^{5} - 2^{10} \times 3^{13} \times 7 \times 17 \times 19501\, j_1^{8} j_2^{5} j_3^{6} + 2^{14} \times 3^{12} \times 5 \times 41 \times 264643\, j_1^{7} j_2^{5} j_3^{7} + 2^{19} \times 3^{13} \times 5 \times 45197\, j_1^{6} j_2^{5} j_3^{8} - 2^{9} \times 3^{11} \times 5 \times 7 \times 11^{2} j_1^{9} j_2^{6} j_3^{4} + 2^{11} \times 3^{11} \times 7 \times 61 \times 8263\, j_1^{8} j_2^{6} j_3^{5}$$
$$-2^{9} \times 3^{11} \times 39791 \times 75329\, j_1^{7} j_2^{6} j_3^{6} - 2^{15} \times 3^{12} \times 7^{2} \times 328919\, j_1^{6} j_2^{6} j_3^{7} + 2^{11} \times 3^{10} \times 5 \times 11^{2} j_1^{9} j_2^{7} j_3^{3} - 2^{9} \times 3^{11} \times 29 \times 73 \times 1619\, j_1^{8} j_2^{7} j_3^{4} + 2^{10} \times 3^{10} \times 11 \times 19 \times 2237 \times 3793\, j_1^{7} j_2^{7} j_3^{5} + 2^{13} \times 3^{12} \times 11 \times 709 \times 7079\, j_1^{6} j_2^{7} j_3^{6}$$
$$+2^{19} \times 3^{13} \times 109 \times 113\, j_1^{5} j_2^{7} j_3^{7} - 2^{8} \times 3^{10} \times 5 \times 11^{2} j_1^{9} j_2^{8} j_3^{2} + 2^{11} \times 3^{9} \times 11 \times 13 \times 23 \times 401\, j_1^{8} j_2^{8} j_3^{3} - 2^{9} \times 3^{9} \times 13 \times 224037301\, j_1^{7} j_2^{8} j_3^{4} - 2^{13} \times 3^{10} \times 270832781\, j_1^{6} j_2^{8} j_3^{5} - 2^{19} \times 3^{11} \times 73 \times 3407\, j_1^{5} j_2^{8} j_3^{6}$$
$$+2^{9} \times 3^{7} \times 5 \times 11^{2} j_1^{9} j_2^{9} j_3 - 2^{10} \times 3^{8} \times 907397\, j_1^{8} j_2^{9} j_3^{2} + 2^{11} \times 3^{8} \times 19 \times 21563777\, j_1^{7} j_2^{9} j_3^{3} + 2^{9} \times 3^{9} \times 401 \times 599 \times 19501\, j_1^{6} j_2^{9} j_3^{4} + 2^{15} \times 3^{11} \times 107 \times 35983\, j_1^{5} j_2^{9} j_3^{5} - 2^{8} \times 3^{6} \times 11^{2} j_1^{9} j_2^{10} + 2^{11} \times 3^{6} \times 5 \times 7 \times 8069\, j_1^{8} j_2^{10} j_3$$

Dénominateur de Φ_3 (suite)

$$-2^9 \times 3^7 \times 5 \times 23 \times 83 \times 63353\, j_1^7 j_2^{10} j_3^2 - 2^{11} \times 3^9 \times 7 \times 39893383\, j_1^6 j_2^{10} j_3^3 - 2^{13} \times 3^9 \times 11 \times 101 \times 67493\, j_1^5 j_2^{10} j_3^4 + 2^{19} \times 3^{11} \times 11 \times 677\, j_1^4 j_2^{10} j_3^5 - 2^8 \times 3^5 \times 7 \times 73 \times 419\, j_1^8 j_2^{11} + 2^{10} \times 3^6 \times 331 \times 199559\, j_1^7 j_2^{11} j_3$$
$$+2^{10} \times 3^7 \times 765685001\, j_1^6 j_2^{11} j_3^2 + 2^{14} \times 3^9 \times 3319 \times 3691\, j_1^5 j_2^{11} j_3^3 - 2^{21} \times 3^9 \times 37993\, j_1^4 j_2^{11} j_3^4 - 2^9 \times 3^6 \times 7 \times 43 \times 14369\, j_1^7 j_2^{12} - 2^{11} \times 3^6 \times 5 \times 11 \times 67 \times 27539\, j_1^6 j_2^{12} j_3 - 2^8 \times 3^8 \times 47 \times 53 \times 157 \times 1187\, j_1^5 j_2^{12} j_3^2 + 2^{14} \times 3^8 \times 17 \times 593 \times 1193\, j_1^4 j_2^{12} j_3^3$$
$$+2^9 \times 3^6 \times 15860233\, j_1^6 j_2^{13} + 2^9 \times 3^6 \times 230601383\, j_1^5 j_2^{13} j_3 - 2^{12} \times 3^7 \times 56208829\, j_1^4 j_2^{13} j_3^2 - 2^{18} \times 3^9 \times 44491\, j_1^3 j_2^{13} j_3^3 - 2^8 \times 3^5 \times 5 \times 13179643\, j_1^5 j_2^{14} + 2^{12} \times 3^6 \times 5 \times 7 \times 902987\, j_1^4 j_2^{14} j_3 + 2^{18} \times 3^7 \times 127 \times 3457\, j_1^3 j_2^{14} j_3^2$$
$$-2^8 \times 3^6 \times 5 \times 47 \times 233 \times 673\, j_1^4 j_2^{15} - 2^{14} \times 3^6 \times 11 \times 421 \times 1627\, j_1^3 j_2^{15} j_3 + 2^{12} \times 3^6 \times 1423 \times 2477\, j_1^3 j_2^{16} + 2^{18} \times 3^7 \times 19763\, j_1^2 j_2^{16} j_3 - 2^{19} \times 3^5 \times 5 \times 6029\, j_1^2 j_2^{17} - 2^8 \times 3^{12} j_1^8 j_3^{12} + 2^{17} \times 3^{13} j_1^7 j_3^{13} + 2^{10} \times 3^{12} j_1^8 j_2 j_3^{11}$$
$$-2^{13} \times 3^{12} \times 5 \times 41\, j_1^7 j_2 j_3^{12} - 2^9 \times 3^{11} \times 11\, j_1^8 j_2^2 j_3^{10} + 2^{15} \times 3^{12} \times 101\, j_1^7 j_2^2 j_3^{11} + 2^{16} \times 3^{13} j_1^6 j_2^2 j_3^{12} + 2^{10} \times 3^9 \times 5 \times 11\, j_1^8 j_2^3 j_3^9 - 2^9 \times 3^{10} \times 5 \times 14009\, j_1^7 j_2^3 j_3^{10} - 2^{20} \times 3^{12} j_1^6 j_2^3 j_3^{11} - 2^8 \times 3^{10} \times 5 \times 11\, j_1^8 j_2^4 j_3^8$$
$$+2^{10} \times 3^9 \times 5^2 \times 3449\, j_1^7 j_2^4 j_3^9 + 2^{14} \times 3^{11} \times 19 \times 23\, j_1^6 j_2^4 j_3^{10} + 2^{11} \times 3^9 \times 11\, j_1^8 j_2^5 j_3^7 - 2^9 \times 3^{10} \times 19 \times 1787\, j_1^7 j_2^5 j_3^8 - 2^{15} \times 3^{10} \times 5 \times 173\, j_1^6 j_2^5 j_3^9 - 2^{17} \times 3^{12} j_1^5 j_2^5 j_3^{10} - 2^{10} \times 3^7 \times 7 \times 11\, j_1^8 j_2^6 j_3^6 + 2^{12} \times 3^8 \times 5 \times 13 \times 257\, j_1^7 j_2^6 j_3^7$$
$$+2^8 \times 3^9 \times 5 \times 7 \times 59 \times 139\, j_1^6 j_2^6 j_3^8 + 2^{17} \times 3^{10} \times 5 \times 7\, j_1^5 j_2^6 j_3^9 + 2^{11} \times 3^7 \times 11\, j_1^8 j_2^7 j_3^5 - 2^{10} \times 3^7 \times 65719\, j_1^7 j_2^7 j_3^6 - 2^{11} \times 3^8 \times 23 \times 29 \times 97\, j_1^6 j_2^7 j_3^7 - 2^{13} \times 3^{10} \times 5 \times 191\, j_1^5 j_2^7 j_3^8 - 2^8 \times 3^6 \times 5 \times 11\, j_1^8 j_2^8 j_3^4$$
$$+2^{11} \times 3^7 \times 5^2 \times 17 \times 19\, j_1^7 j_2^8 j_3^5 + 2^{10} \times 3^7 \times 7 \times 23899\, j_1^6 j_2^8 j_3^6 + 2^{16} \times 3^9 \times 5 \times 71\, j_1^5 j_2^8 j_3^7 + 2^{16} \times 3^{10} \times 5\, j_1^4 j_2^8 j_3^8 + 2^{10} \times 3^3 \times 5 \times 11\, j_1^8 j_2^9 j_3^3 - 2^{10} \times 3^4 \times 5^2 \times 19 \times 167\, j_1^7 j_2^9 j_3^4 - 2^{11} \times 3^6 \times 11 \times 7127\, j_1^6 j_2^9 j_3^5$$
$$-2^{10} \times 3^6 \times 5 \times 78623\, j_1^5 j_2^9 j_3^6 - 2^{20} \times 3^7 \times 5^2 j_1^4 j_2^9 j_3^7 - 2^9 \times 3^3 \times 11\, j_1^8 j_2^{10} j_3^2 + 2^{12} \times 3^3 \times 13 \times 599\, j_1^7 j_2^{10} j_3^3 + 2^9 \times 3^5 \times 5 \times 42397\, j_1^6 j_2^{10} j_3^4 + 2^{11} \times 3^6 \times 61 \times 1399\, j_1^5 j_2^{10} j_3^5 + 2^{15} \times 3^6 \times 5 \times 613\, j_1^4 j_2^{10} j_3^6 + 2^{10} \times 3^2 j_1^8 j_2^{11} j_3$$
$$-2^9 \times 3^3 \times 5 \times 11 \times 101\, j_1^7 j_2^{11} j_3^2 - 2^{11} \times 3^7 \times 5 \times 11 \times 17\, j_1^6 j_2^{11} j_3^3 - 2^{10} \times 3^5 \times 5 \times 19 \times 1609\, j_1^5 j_2^{11} j_3^4 - 2^{16} \times 3^6 \times 5 \times 13 \times 17\, j_1^4 j_2^{11} j_3^5 - 2^{18} \times 3^7 \times 5\, j_1^3 j_2^{11} j_3^6 - 2^8 j_1^8 j_2^{12} + 2^{10} \times 3 \times 1361\, j_1^7 j_2^{12} j_3 + 2^{10} \times 3^3 \times 89 \times 181\, j_1^6 j_2^{12} j_3^2$$
$$+2^{12} \times 3^3 \times 5 \times 13963\, j_1^5 j_2^{12} j_3^3 + 2^8 \times 3^4 \times 5 \times 67 \times 3391\, j_1^4 j_2^{12} j_3^4 + 2^{17} \times 3^6 \times 5 \times 13\, j_1^3 j_2^{12} j_3^5 - 2^9 \times 5 \times 41\, j_1^7 j_2^{13} - 2^{11} \times 3^2 \times 7 \times 13 \times 17\, j_1^6 j_2^{13} j_3 - 2^{10} \times 3^3 \times 5 \times 83 \times 89\, j_1^5 j_2^{13} j_3^2 - 2^{10} \times 3^3 \times 5 \times 73 \times 661\, j_1^4 j_2^{13} j_3^3$$
$$-2^{13} \times 3^5 \times 5 \times 557\, j_1^3 j_2^{13} j_3^4 + 2^8 \times 3^2 \times 19^2\, j_1^6 j_2^{14} + 2^{11} \times 3^2 \times 5 \times 863\, j_1^5 j_2^{14} j_3 + 2^9 \times 3^3 \times 5 \times 31 \times 547\, j_1^4 j_2^{14} j_3^2 + 2^{15} \times 3^4 \times 5 \times 197\, j_1^3 j_2^{14} j_3^3 + 2^{16} \times 3^6 \times 5\, j_1^2 j_2^{14} j_3^4 - 2^{10} \times 2707\, j_1^5 j_2^{15} - 2^{10} \times 3 \times 5 \times 23 \times 331\, j_1^4 j_2^{15} j_3$$
$$-2^9 \times 3^3 \times 17 \times 2927\, j_1^3 j_2^{15} j_3^2 - 2^{22} \times 3^4 j_1^2 j_2^{15} j_3^3 + 2^8 \times 5^2 \times 13 \times 61\, j_1^4 j_2^{16} + 2^{10} \times 3^2 \times 10399\, j_1^3 j_2^{16} j_3 + 2^{14} \times 3^7 \times 5\, j_1^2 j_2^{16} j_3^2 - 2^9 \times 3 \times 59 \times 61\, j_1^3 j_2^{17} - 2^{15} \times 3^3 \times 47\, j_1^2 j_2^{17} j_3 - 2^{17} \times 3^4 j_1 j_2^{17} j_3^2 + 2^8 \times 5 \times 2803\, j_1^2 j_2^{18}$$
$$+2^{17} \times 3 \times 19\, j_1 j_2^{18} j_3 - 2^{13} \times 157\, j_1 j_2^{19} + 2^{16} \times 3\, j_2^{20}.$$

Conclusion et perspectives

- amélioration de la complexité :
  $O\left(\mathcal{M}(N)\sqrt{N}\right) \to O(\mathcal{M}(N)\log N)$
- rapide en pratique
- se généralise au genre 2
  $O(N^{2+\varepsilon}) \to O(N^{1+\varepsilon})$
  - pour l'évaluation de formes modulaires de Siegel
  - pour le calcul de la jacobienne analytique
- l'algorithme utilisé en genre 2 n'est pas prouvé !
  (mais il existe une version prouvée plus technique à implanter)