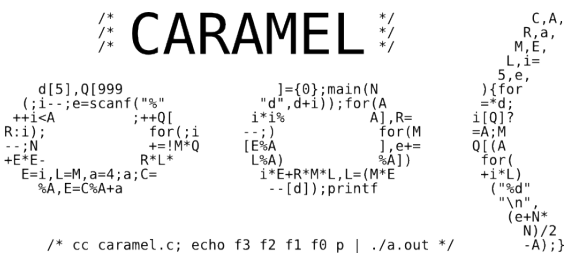
Calcul de la fonction thêta de Jacobi en temps quasi-optimal

Hugo Labrande

RAIM 2015, Rennes, 8 avril 2015



Fonction thêta de Jacobi

Définition

La fonction thêta de Jacobi est définie par :

$$\begin{aligned} \theta : \mathbb{C} \times \{Im(\tau) > 0\} &\rightarrow \mathbb{C} \\ (z, \tau) &\rightarrow \sum_{n \in \mathbb{Z}} e^{2i\pi nz} e^{i\pi n^2 \tau} \end{aligned}$$

Problème : calcul multiprécision de $\theta(z, \tau)$, à une précision P.

Série converge rapidement : besoin de considérer $\sqrt{P}$ termes à précision P.

D'où : algorithme naïf en $O(\mathcal{M}(P)\sqrt{P})$.

Contribution : nouvel algorithme en $O(\mathcal{M}(P) \log P)$ (*quasi-optimal*).

Fonction thêta de Jacobi

$$\boldsymbol{\theta_0(z,\tau)} = \theta(z,\tau) \qquad \theta_2(z,\tau) = \theta\left(z+\frac{\tau}{2},\tau\right)e^{\pi i\tau/4+\pi iz}$$

$$\theta_1(z,\tau) = \theta(z+\tfrac{1}{2},\tau) \qquad \theta_3(z,\tau) = \theta\left(z+\frac{1+\tau}{2},\tau\right)e^{\pi i(\tau/4+z+1/2)}$$

Applications :

En crypto (courbes elliptiques) :

$$\begin{aligned} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) &\to \mathbb{P}^3(\mathbb{C}) \\ z &\to (\boldsymbol{\theta_0(z,\tau)} : \theta_1(z,\tau) : \theta_2(z,\tau) : \theta_3(z,\tau)) \end{aligned}$$

Formes modulaires, équations différentielles (équation de la chaleur)...

Thêta-constantes

Définition

On appelle « thêta-constantes » les valeurs $\boldsymbol{\theta_0(0, \tau)}$, $\theta_1(0, \tau)$, $\theta_2(0, \tau)$ *et* $\theta_3(0, \tau)$.

Dupont (2005) :

> Trouver une fonction F telle que :
>
> > F est rapide à calculer ;
> > $F(\boldsymbol{\theta_0(0, \tau)}, \theta_1(0, \tau)) = \tau$.
>
> Calculer les thêta-constantes à précision P, en appliquant la méthode de Newton à F.

Application (Enge) : calcul record du polynôme de classe d'un corps de nombres (génération de courbes elliptiques sûres par la méthode CM).

Thêta-constantes et AGM

$$\begin{aligned} \theta_0(0, 2\tau)^2 &= \frac{\theta_0(0, \tau)^2 + \theta_1(0, \tau)^2}{2} \\ \theta_1(0, 2\tau)^2 &= \theta_0(0, \tau)\theta_1(0, \tau) \end{aligned}$$

Ressemble à la moyenne arithmético-géométrique :

Définition (AGM)

Pour $a, b \in \mathbb{R}^+$ (ou $\mathbb{C}$), poser $a_0 = a, b_0 = b$, puis :

$$a_{n+1} = \frac{a_n + b_n}{2}, b_{n+1} = \sqrt{a_n b_n}.$$

Alors $AGM(a, b) = \lim_{n\to\infty} a_n$ (ou b_n).

Thêta-constantes et AGM

Proposition

$$AGM(\boldsymbol{\theta_0(0,\tau)}^2, \theta_1(0,\tau)^2) = \lim_{n\to\infty} \theta_0(0,2^n\tau)^2 = 1.$$

Proposition

$$\theta_1\left(0,\frac{-1}{\tau}\right) = \theta_2(0,\tau)\sqrt{-i\tau} \quad ; \quad \boldsymbol{\theta_0}\left(\mathbf{0},\frac{\mathbf{-1}}{\boldsymbol{\tau}}\right) = \boldsymbol{\theta_0(0,\tau)}\sqrt{-i\tau}$$

d'où $AGM(\boldsymbol{\theta_0(0,\tau)}^2, \theta_2(0,\tau)^2) = \frac{1}{-i\tau}$.

$$F : \boldsymbol{\theta_0(0,\tau)}, \theta_1(0,\tau) \quad \to \quad \theta_2(0,\tau) \text{ (formule de Jacobi)}$$
$$\to \quad i/\tau \text{ (AGM)}$$

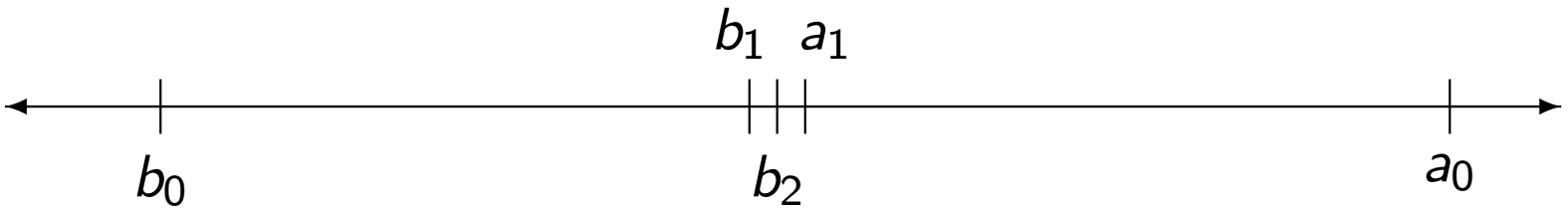
Convergence de l'AGM

Propriété

Une suite AGM converge quadratiquement – le nombre de chiffres qui coïncident avec la limite double à chaque itération.

$AGM(a, b)$ à précision P : besoin de $\sim \log P$ itérations.

$\rightarrow$ $O(\mathcal{M}(P) \log P)$ bit ops (*quasi-optimal*).



$$
\begin{aligned}
a_0 &= \sqrt{2} = 1.41421356237\ldots & b_0 &= 1.00000000000\ldots \\
a_1 &= 1.18920711500\ldots & b_1 &= 1.20710678118\ldots \\
a_2 &= 1.19812352149\ldots & b_2 &= 1.19815694809\ldots \\
a_3 &= 1.19814023467\ldots & b_3 &= 1.19814023479\ldots \\
a_4 &= 1.19814023473\ldots & b_4 &= 1.19814023473\ldots
\end{aligned}
$$

Méthode de Newton

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Théorème

Newton converge quadratiquement vers un zéro de f.

- Calculer x_0, approx à P_0 chiffres près ;
- Calculer $\frac{f(x_0)}{f'(x_0)}$ à précision $2P_0$, puis x_1 à cette même précision ;
- Calculer $\frac{f(x_1)}{f'(x_1)}$ à précision $4P_0$, puis x_2 à cette même précision ;
- ...

Sous les bonnes hypothèses :

x_i est une approximation à $\sim 2^i$ chiffres près ;

Le coût asymptotique est **égal au coût de la dernière étape**.

$\rightarrow$ calcul des thêta-constantes à précision P en $O(\mathcal{M}(P) \log P)$.

Calculer $\theta(z, \tau)$

On peut donc calculer $\theta_i(0, \tau)$ avec P chiffres exacts en $O(\mathcal{M}(P) \log P)$.

On veut pouvoir calculer $\theta_i(z, \tau)$, pour tout z, $O(\mathcal{M}(P) \log P)$.

Essayons de généraliser cette approche :

Il faut trouver une fonction F telle que

$$F(\boldsymbol{\theta_0(z, \tau)}, \theta_1(z, \tau)) = (z, \tau).$$

F doit être facile à calculer (**s'appuyer sur l'AGM ou une autre suite quadratiquement convergente ?**).
On appliquera ensuite la méthode de Newton.

AGM modifiée

Proposition

$$\theta_0(z,2\tau)^2 = \frac{\theta_0(z,\tau)\theta_0(0,\tau) + \theta_1(z,\tau)\theta_1(0,\tau)}{2}$$
$$\theta_1(z,2\tau)^2 = \frac{\theta_0(z,\tau)\theta_1(0,\tau) + \theta_1(z,\tau)\theta_0(0,\tau)}{2}$$

Si on prend $z = 0$ on retombe sur l'AGM ! ($\frac{\theta_0^2+\theta_1^2}{2}$ et $\theta_0\theta_1$)

Définition

$$M(x,y,z,t) = \left(\sqrt{\frac{xz+yt}{2}}, \sqrt{\frac{xt+yz}{2}}, \sqrt{\frac{z^2+t^2}{2}}, \sqrt{zt}\right)$$

AGM modifiée

La situation est la même qu'avec les thêta-constantes :

Proposition

- *La suite* $(M^n(x, y, z, t))_{n \in \mathbb{N}}$ *converge quadratiquement.*
- *Posons* $F(x, y, z, t)$ *comme étant la limite de cette suite : F peut se calculer en* $O(\mathcal{M}(P) \log P)$ *ops.*
- *Posons* $S_{z,\tau} = (\boldsymbol{\theta_0(z, \tau)}, \theta_1(z, \tau), \boldsymbol{\theta_0(0, \tau)}, \theta_1(0, \tau))$. *Alors :*

  $M(S_{z,\tau}) = S_{z,2\tau}$;

  $\forall z, \tau$, *on a* $F(S_{z,\tau}) = (1, 1, 1, 1)$.

Extraire z et τ

Proposition

$$\begin{aligned}\theta_1\left(\frac{z}{\tau},\frac{-1}{\tau}\right) &= \theta_2(z,\tau)e^{i\pi z^2/\tau}\sqrt{-i\tau}\\ \boldsymbol{\theta_0}\left(\frac{\boldsymbol{z}}{\boldsymbol{\tau}},\frac{\boldsymbol{-1}}{\boldsymbol{\tau}}\right) &= \boldsymbol{\theta_0(z,\tau)}e^{i\pi z^2/\tau}\sqrt{-i\tau}\end{aligned}$$

Donc

$$\begin{aligned}&F(\boldsymbol{\theta_0(z,\tau)},\theta_2(z,\tau),\boldsymbol{\theta_0(0,\tau)},\theta_2(0,\tau))\\ =\ &F\left(\lambda\boldsymbol{\theta_0}\left(\frac{\boldsymbol{z}}{\boldsymbol{\tau}},\frac{\boldsymbol{-1}}{\boldsymbol{\tau}}\right),\lambda\theta_1\left(\frac{z}{\tau},\frac{-1}{\tau}\right),\mu\boldsymbol{\theta_0}\left(\boldsymbol{0},\frac{\boldsymbol{-1}}{\boldsymbol{\tau}}\right),\mu\theta_1\left(0,\frac{-1}{\tau}\right)\right)\end{aligned}$$

avec $\lambda = e^{i\pi z^2/\tau}\sqrt{-i\tau}$, $\mu = \sqrt{-i\tau}$.

Extraire z et τ

Proposition

$F(\lambda x, \lambda y, \mu z, \mu t) = \mu F(x, y, z, t)$.

$\rightarrow$ Ne dépend pas de λ !

$\rightarrow$ Donc F ne dépend pas de z : on ne peut pas appliquer directement Newton pour inverser F.

Proposition

$$\lim_{n\to\infty} \left(\frac{M^n(\lambda x,\lambda y,\mu z,\mu t)_x}{M^n(\lambda x,\lambda y,\mu z,\mu t)_z} \right)^{2^n} = \frac{\lambda}{\mu} \frac{F(x,y,z,t)_x}{F(x,y,z,t)_z}.$$

M^n converge quadratiquement, donc on peut s'arrêter au rang $n = O(\log P)$.

Donc λ est calculable à préc. P en $O(\mathcal{M}(P) \log P)$.

Algorithme final

$$\boldsymbol{\theta_0(z,\tau)}, \theta_1(z,\tau), \boldsymbol{\theta_0(0,\tau)}, \theta_1(0,\tau) \quad \to \quad \theta_2(z,\tau), \theta_2(0,\tau)$$

(formule de Jacobi + formules de Riemann)

$$\to \quad e^{-i\pi z^2/\tau}, \frac{1}{\sqrt{-i\tau}}$$

(AGM modifiée + trouver λ)

$$\to \quad z, \tau$$

On calcule des approximations initiales avec l'algorithme naïf ;

On applique Newton (ou diff finies) à cette fonction.

On calcule $\theta_{0,1,2}([z,0],\tau)$ à précision P en $O(\mathcal{M}(P)\log P)$!

Implantation

Implantation de l'algorithme en C (MPC).

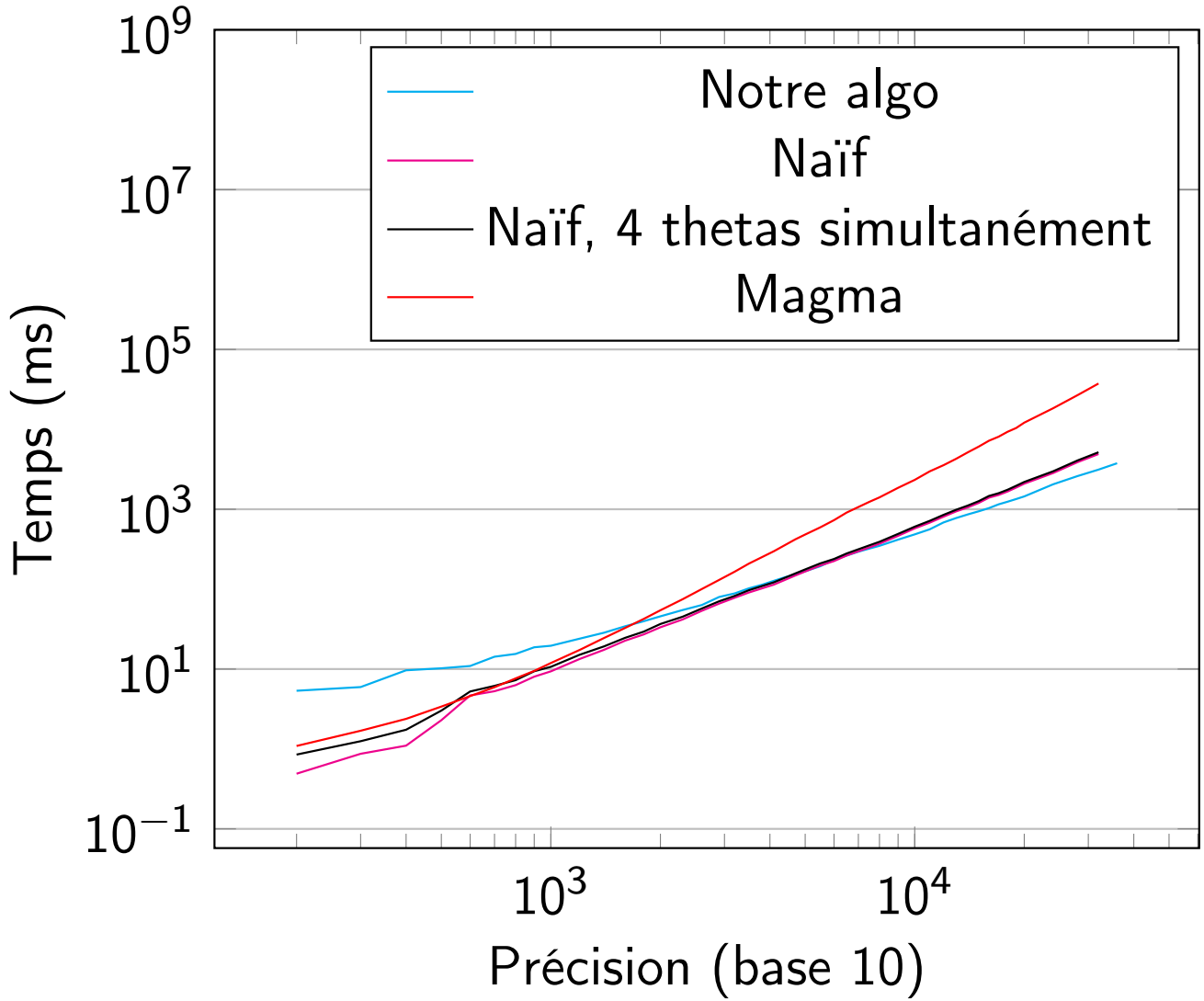
On compare à

- notre implantation de l'algorithme naïf pour $\theta_0(z, \tau)$ en C (MPC) ;
- notre implantation de la méthode naïve pour calculer $\theta_{0,1}([z, 0], \tau)$ en C (MPC) ;
- la fonction `Theta` de Magma.

Résultat :

Magma est battu à partir de 1600 chiffres décimaux.
La méthode naïve est battue à partir de 5000 chiffres décimaux.

Implantation



That's all folks !

Merci de votre attention !