Évaluation rapide de fonctions modulaires *via* l'AGM

Aussois, 4 février 2005

Régis Dupont

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

Plan

- introduction, motivations
- theta constantes *and co.*
- premier algorithme “naïf”
- moyenne arithmético-géométrique (AGM)
- algorithme et complexité

Introduction

Objectif : évaluer rapidement certaines fonctions modulaires, typiquement

$$j(\tau) = \frac{1}{q^2} + 744 + 196884q^2 + \ldots, \quad q = e^{i\pi\tau}$$

(évaluation "naïve" : $O(\mathcal{M}(N)N)$)

Lien avec les courbes elliptiques sur $\mathbb{C}$

$$\tau \in \mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(\tau) > 0\} \mapsto E_\tau : y^2 = f(x, j(\tau))$$

τ : période $\qquad$ $j(\tau)$: invariant

de plus :

pour toute courbe elliptique E sur $\mathbb{C}$, il existe $\tau \in \mathcal{H}$ t.q.

$$E \cong E_\tau \cong \mathbb{C}/(\mathbb{Z}.1 \oplus \mathbb{Z}.\tau)$$

Motivations : applications

- calcul de polynômes de classes
  $\Rightarrow$ construction de courbes elliptiques ayant des propriétés particulières (couplages calculables,...) par multiplication complexe
- calcul de polynômes modulaires
  $\Rightarrow$ comptage de points sur courbes elliptiques (algorithme SEA)

Notations

- $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\langle -I \rangle$,
- action de Γ sur $\mathcal{H}$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$,
- Γ est engendré par $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

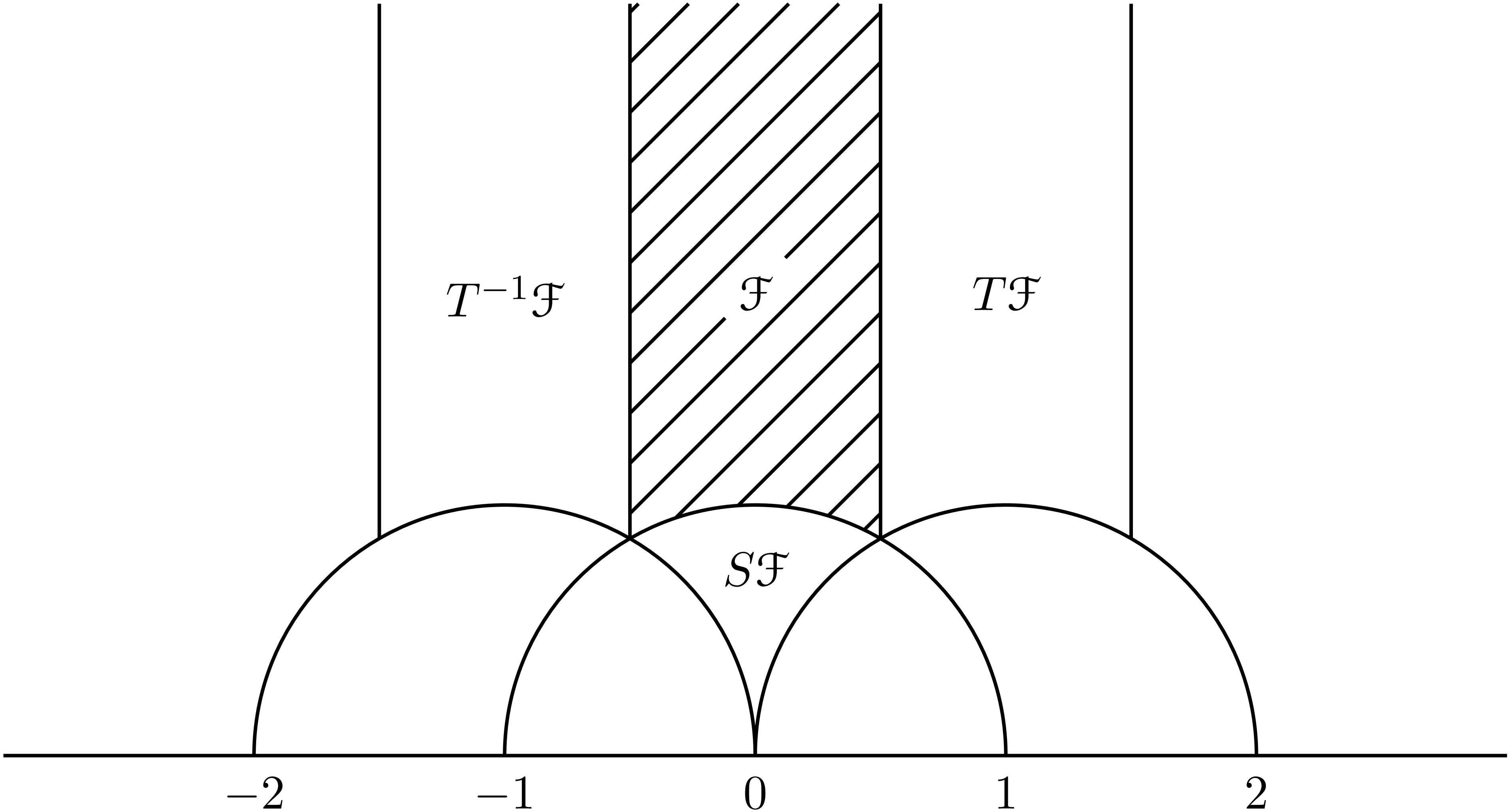
$$S\tau = \frac{-1}{\tau}, \quad T\tau = \tau + 1.$$

- si $\mathcal{F} = \left\{\tau \in \mathbb{C} : |\mathrm{Re}(\tau)| \leqslant \frac{1}{2}, |\tau| \geqslant 1\right\}$, alors

$$\mathcal{F} \setminus (\partial\mathcal{F} \cap \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) > 0\})$$

est un domaine fondamental pour l'action de Γ sur $\mathcal{H}$

Domaine fondamental $\mathcal{F}$



Fonctions modulaires

Γ' sous-groupe d'indice fini de Γ

Définition : f est une fonction modulaire pour Γ' si :

- f est méromorphe sur $\mathcal{H}$,
- f est invariante sous l'action de Γ' :

$$\forall \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right), \tau \right) \in \Gamma' \times \mathcal{H}, \quad f\left(\frac{a\tau + b}{c\tau + c} \right) = f(\tau)$$

- f est méromorphe aux pointes

Exemple :

j est modulaire pour le groupe Γ

Theta constantes : définition

$$q = q(\tau) = e^{i\pi\tau},$$

$$\begin{array}{rclcl}
\theta_{00}(\tau) & = & \sum_{n\in\mathbb{Z}} q^{n^2} & = & 1 + 2q + 2q^4 + 2q^9 + \dots \\
\theta_{01}(\tau) & = & \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2} & = & 1 - 2q + 2q^4 - 2q^9 + \dots \\
\theta_{10}(\tau) & = & \sum_{n\in\mathbb{Z}} q^{\left(n+\frac{1}{2}\right)^2} & = & 2q^{\frac{1}{4}} + 2q^{\frac{9}{4}} + 2q^{\frac{25}{4}} + \dots
\end{array}$$

$\Longrightarrow$ fonctions analytiques et non nulles sur $\mathcal{H}$

Theta constantes : propriétés

pour tout $\tau \in \mathcal{H}$,

$$\theta_{00}^2(S\tau) = -i\tau\theta_{00}^2(\tau)$$

$$\theta_{01}^2(S\tau) = -i\tau\theta_{10}^2(\tau)$$

$$\theta_{10}^2(S\tau) = -i\tau\theta_{01}^2(\tau)$$

et

$$\theta_{00}^4(\tau) = \theta_{01}^4(\tau) + \theta_{10}^4(\tau)$$

de plus :

$$\lim_{\mathrm{Im}(\tau)\to+\infty} \theta_{00}(\tau) = \lim_{\mathrm{Im}(\tau)\to+\infty} \theta_{01}(\tau) = 1$$

$$\lim_{\mathrm{Im}(\tau)\to+\infty} \theta_{10}(\tau) = 0$$

Theta constantes : propriétés

Formules de duplication :

pour tout $\tau \in \mathcal{H}$,

$$\theta_{00}^2(2\tau) = \frac{\theta_{00}^2(\tau) + \theta_{01}^2(\tau)}{2}$$

et

$$\theta_{01}^2(2\tau) = \theta_{00}(\tau)\theta_{01}(\tau)$$

Les fonctions k et k'

Définition :

$$k(\tau) = \left(\frac{\theta_{10}(\tau)}{\theta_{00}(\tau)}\right)^2 \quad \text{et} \quad k'(\tau) = \left(\frac{\theta_{01}(\tau)}{\theta_{00}(\tau)}\right)^2$$

$\Rightarrow$ fonctions modulaires

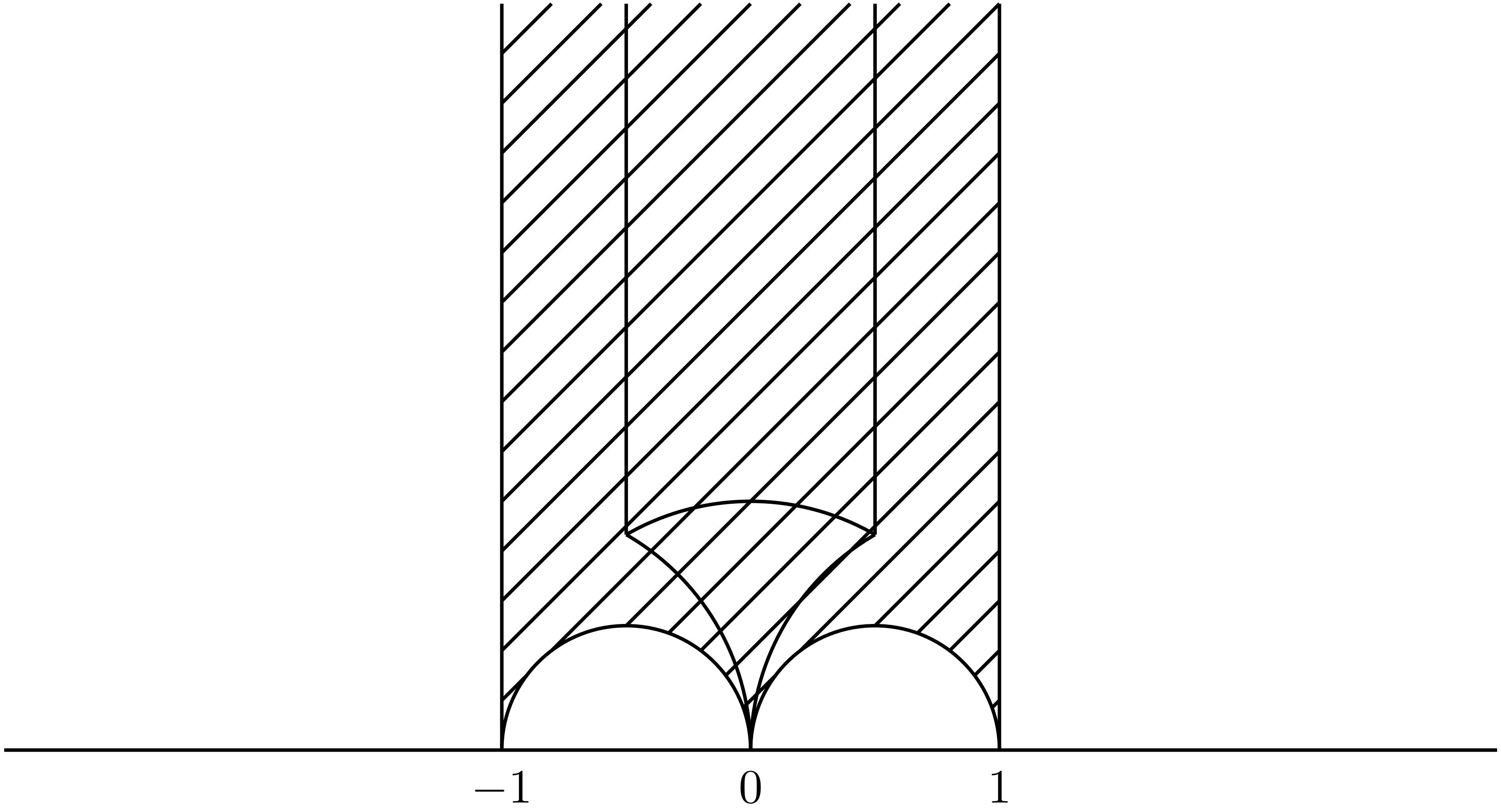
vérifient $k^2 + k'^2 = 1$, $k'(S\tau) = k(\tau)$ et

$$k(\mathcal{F}') = k'(\mathcal{F}') = \{z \in \mathbb{C} \setminus \{0,1\} : \mathrm{Re}(z) \geqslant 0\}$$

avec

$$\mathcal{F}' = \left\{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \leqslant 1, \left|\tau \pm \frac{1}{2}\right| \geqslant \frac{1}{2}\right\}$$

Région $\mathcal{F}'$



Relation avec la fonction j

Propriété :

soit j la fonction modulaire elliptique (modulaire pour Γ) :

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

on a :

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

$\Rightarrow$ on se ramène donc à l'évaluation de k'

Un premier algorithme

Utilisation des séries en q :

$$\theta_{00}(\tau) = \sum_{n\geq 0} q^{n^2} \qquad \theta_{01}(\tau) = \sum_{n\geq 0} (-1)^n q^{n^2}$$

Intérêt :

- ces séries sont creuses
- les coefficients valent ± 1
- $q \mapsto \{q, q^4, \ldots, q^{n^2}\}$: $2n - 1$ multiplications

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

AGM : définition

si $a, b \in \mathbb{C}$, on définit :

- $a_0 = a$, $b_0 = b$,
- $a_{n+1} = \frac{a_n + b_n}{2}$,
- $b_{n+1} = \sqrt{a_n b_n}$ (problème de choix !)

$$\mathrm{AGM}(a, b) = \lim_{n \to +\infty} a_n = \lim_{n \to +\infty} b_n$$

$\Longrightarrow$ la convergence est quadratique

Remarque : $AGM(a, b) = aAGM(1, \frac{b}{a})$

AGM : propriétés

$\mathcal{R} = \{z \in \mathbb{C} \setminus \{0\} : \mathrm{Re}(z) > 0\}$

on considère

$$\begin{array}{rccc} M: & \mathcal{R} & \longrightarrow & \mathcal{R} \\ & z & \longmapsto & \mathrm{AGM}(1, z) \end{array}$$

Théorème :

pour tout $\tau \in \mathcal{F}'$,

$$M\left(k'(\tau)\right) = \frac{1}{\theta_{00}^2(\tau)}$$

de plus, M est analytique sur $\mathcal{R}$

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

pour tout $\tau \in \mathcal{F}'$,

$$\begin{aligned} M\left(k(\tau)\right) &= M\left(k'(S\tau)\right) \\ &= \frac{1}{\theta_{00}^2(S\tau)} \\ &= \frac{i}{\tau\theta_{00}^2(\tau)} \end{aligned}$$

de plus

$$M\left(k'(\tau)\right) = \frac{1}{\theta_{00}^2(\tau)}$$

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

$\Longrightarrow$ on pose

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

pour tout $\tau \in \mathcal{F}$,

$$f_\tau\left(k'(\tau)\right) = 0$$

or f_τ est analytique sur $\mathcal{R}$, et de plus

$$\frac{df_\tau}{dz}\left(k'(\tau)\right) = \frac{-2}{\pi\tau\theta_{01}^2(\tau)\theta_{10}^4(\tau)} \neq 0$$

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

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

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

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

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

il existe une constante B t.q. $\forall\tau \in \mathcal{F}$, $|\tau| \leqslant 2$,

$$\left|z_0 - k'(\tau)\right| \leqslant \frac{1}{2^B} \Rightarrow \forall n \geqslant 0, \left|z_n - k'(\tau)\right| \leqslant \frac{1}{2^{2^n}}$$

Remarque : B ne dépend pas de τ

Complexité de quelques opérations

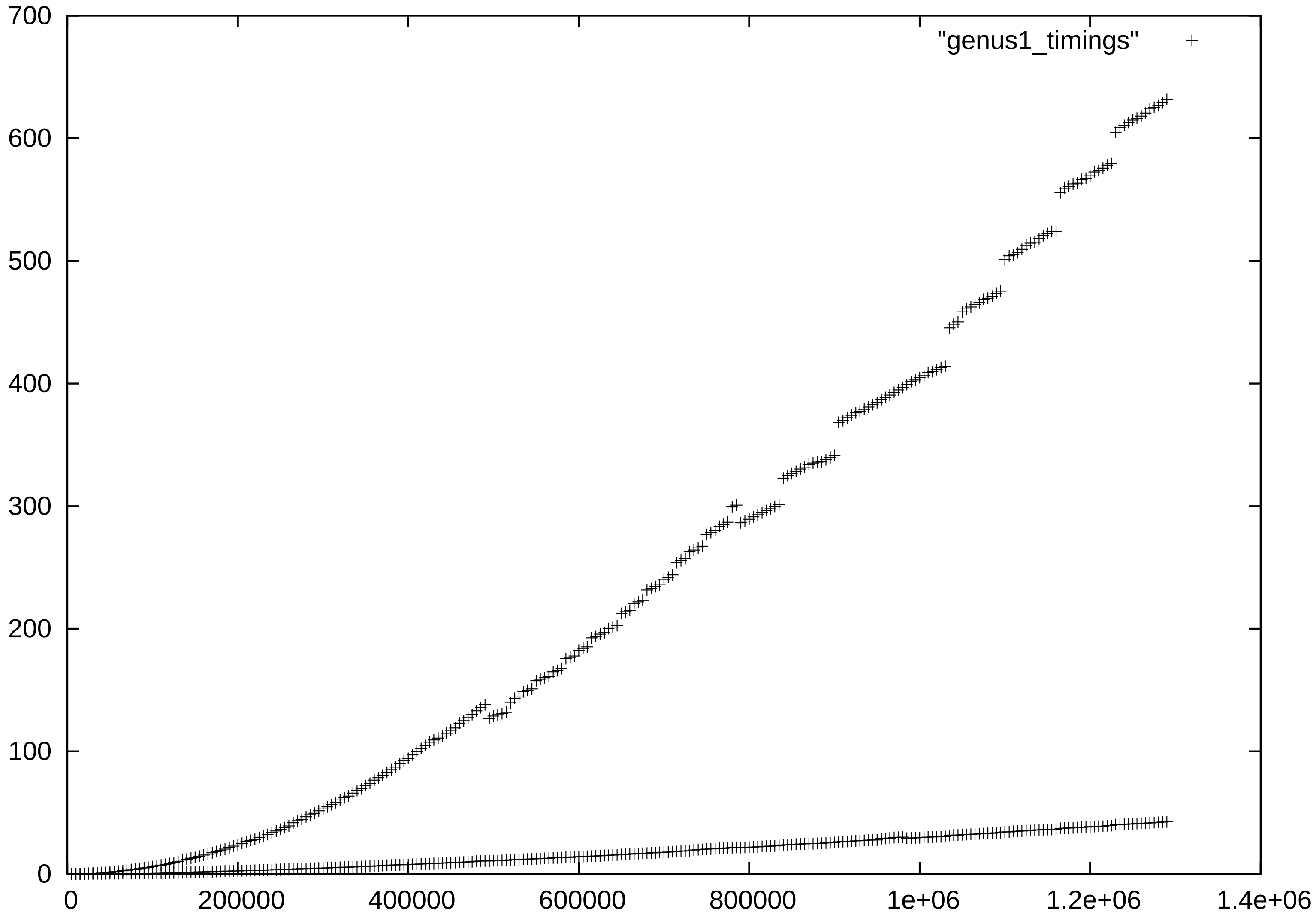
- utilisation de l'AGM
  - log : $O(\mathcal{M}(N)\log N)$
- itérations de Newton
  - racines carrées, cubiques, ... : $O(\mathcal{M}(N))$
  - exp, sin, cos : $O(\mathcal{M}(N)\log N)$
- évaluation de $M(z)$:

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

mais $O\left(\mathcal{M}(N)\log N\right)$ si z est dans un compact de $\mathcal{R}$

$\Rightarrow k'$ s'évalue en $O(\mathcal{M}(N)\log N) = O(N^{1+\varepsilon})$

. . . et ça marche !



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

Conclusion et perspectives

- amélioration de la complexité :
  $O\left(\mathcal{M}(N)\sqrt{N}\right) \longrightarrow O(\mathcal{M}(N)\log N)$
- rapide en pratique
- permet d'évaluer d'autres formes/fonctions modulaires
- se généralise au genre 2
  $O(N^{2+\varepsilon}) \longrightarrow O(N^{1+\varepsilon})$
  - pour l'évaluation de formes modulaires de Siegel
  - pour le calcul de la jacobienne analytique

  (utilisation de la moyenne de Borchardt)
- genre $\geqslant 3$: possible en théorie…

Principe général

theta constantes : $\mathcal{H}_g (\subset \mathcal{M}_{g\times g}(\mathbb{C})) \to \mathbb{C}$
$\mathrm{Sp}_{2g}(\mathbb{Z}) \subset \mathcal{M}_{2g\times 2g}(\mathbb{Z})$ agit sur $\mathcal{H}_g$

1. formules de duplication pour les (carrés des) theta constantes
2. formules de transformation des theta constantes
3. algorithme permettant de calculer la période à partir des theta constantes
4. itérations de Newton

Formules de duplication ($g = 2$)

$$\begin{aligned}
\vartheta_0^2(2\tau) &= \frac{\vartheta_0^2(\tau)+\vartheta_1^2(\tau)+\vartheta_2^2(\tau)+\vartheta_3^2(\tau)}{4}\\
\vartheta_1^2(2\tau) &= \frac{\vartheta_0(\tau)\vartheta_1(\tau)+\vartheta_2(\tau)\vartheta_3(\tau)}{2}\\
\vartheta_2^2(2\tau) &= \frac{\vartheta_0(\tau)\vartheta_2(\tau)+\vartheta_1(\tau)\vartheta_3(\tau)}{2}\\
\vartheta_3^2(2\tau) &= \frac{\vartheta_0(\tau)\vartheta_3(\tau)+\vartheta_1(\tau)\vartheta_2(\tau)}{2}
\end{aligned}$$

de plus

$$\lim_{n\to+\infty} \vartheta_i(2^n\tau) = 1$$