AGM, theta constantes et applications

Séminaire Algo, 7 novembre 2005

Régis Dupont

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

Plan

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

Plan

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

Moyenne arithmético-géométrique

sur les réels positifs : $a_0 \geqslant b_0 \geqslant 0$

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

- convergence quadratique si $b_0 \neq 0$ (suites adjacentes)
- historiquement : Lagrange, Legendre, Gauss

calcul d'intégrales elliptiques :

$$\int_{e_0}^{e_1} \frac{dx}{\sqrt{(x-e_0)(x-e_1)(x-e_2)}}$$

$$\int_0^{2\pi} \frac{dt}{\sqrt{a^2 \sin^2 t + b^2 \cos^2 t}} = \frac{2\pi}{\mathrm{AGM}(a,b)}$$

Moyenne arithmético-géométrique

et sur $\mathbb{C}$?

$$b_{n+1} = \pm\sqrt{a_n b_n} \quad \rightarrow \quad \text{2 choix de racines possibles}$$

$\Rightarrow$ converge tout le temps

Définition (bon choix de racine) :

$$|b_{n+1} - a_{n+1}| \leqslant |b_{n+1} + a_{n+1}| \quad \left(\text{et } \operatorname{Im}\left(\frac{b_{n+1}}{a_{n+1}}\right) > 0 \text{ si égalité}\right)$$

Proposition :

la limite est non nulle ssi le nombre de mauvais choix est fini

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) ?

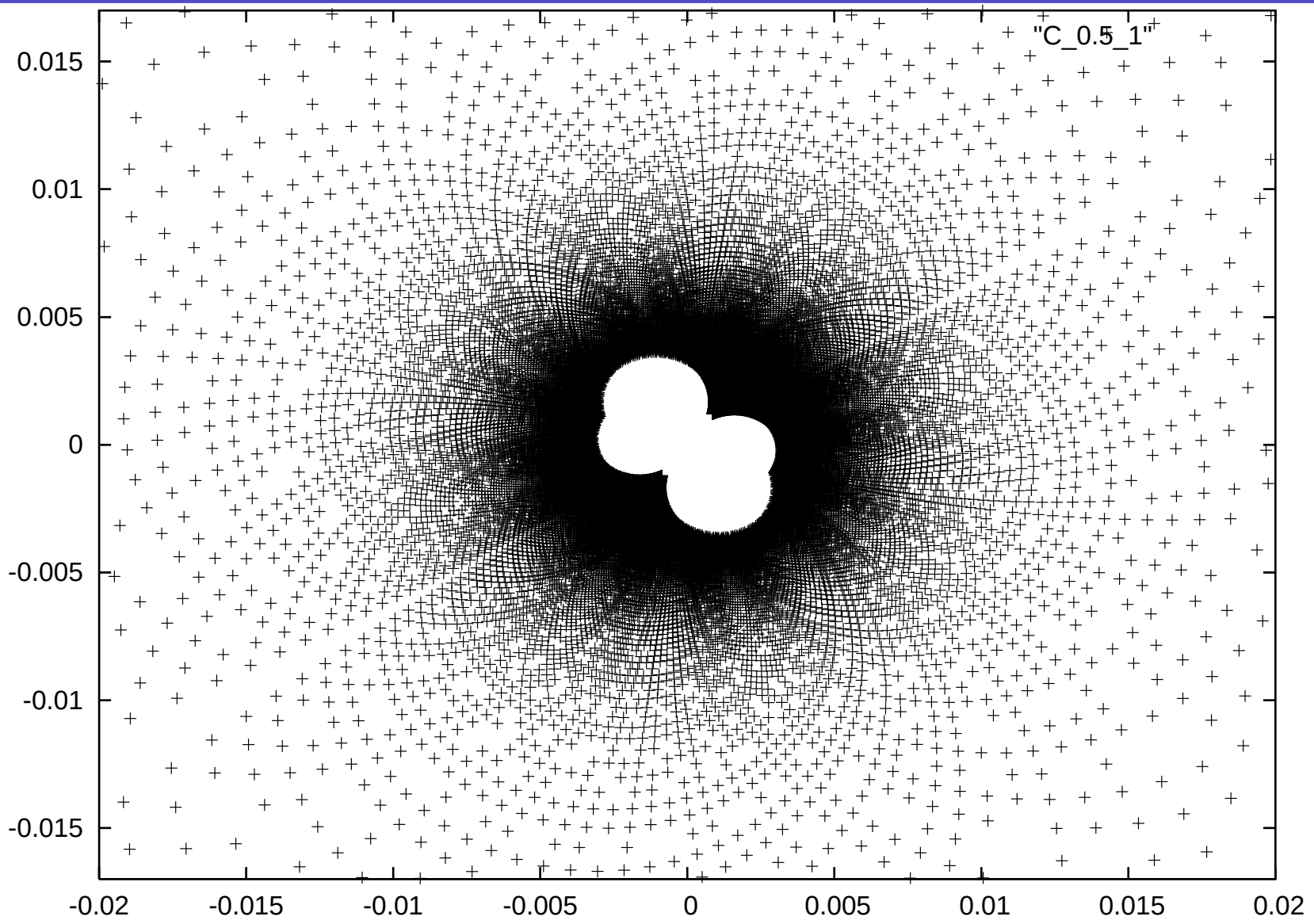
On note cet ensemble

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

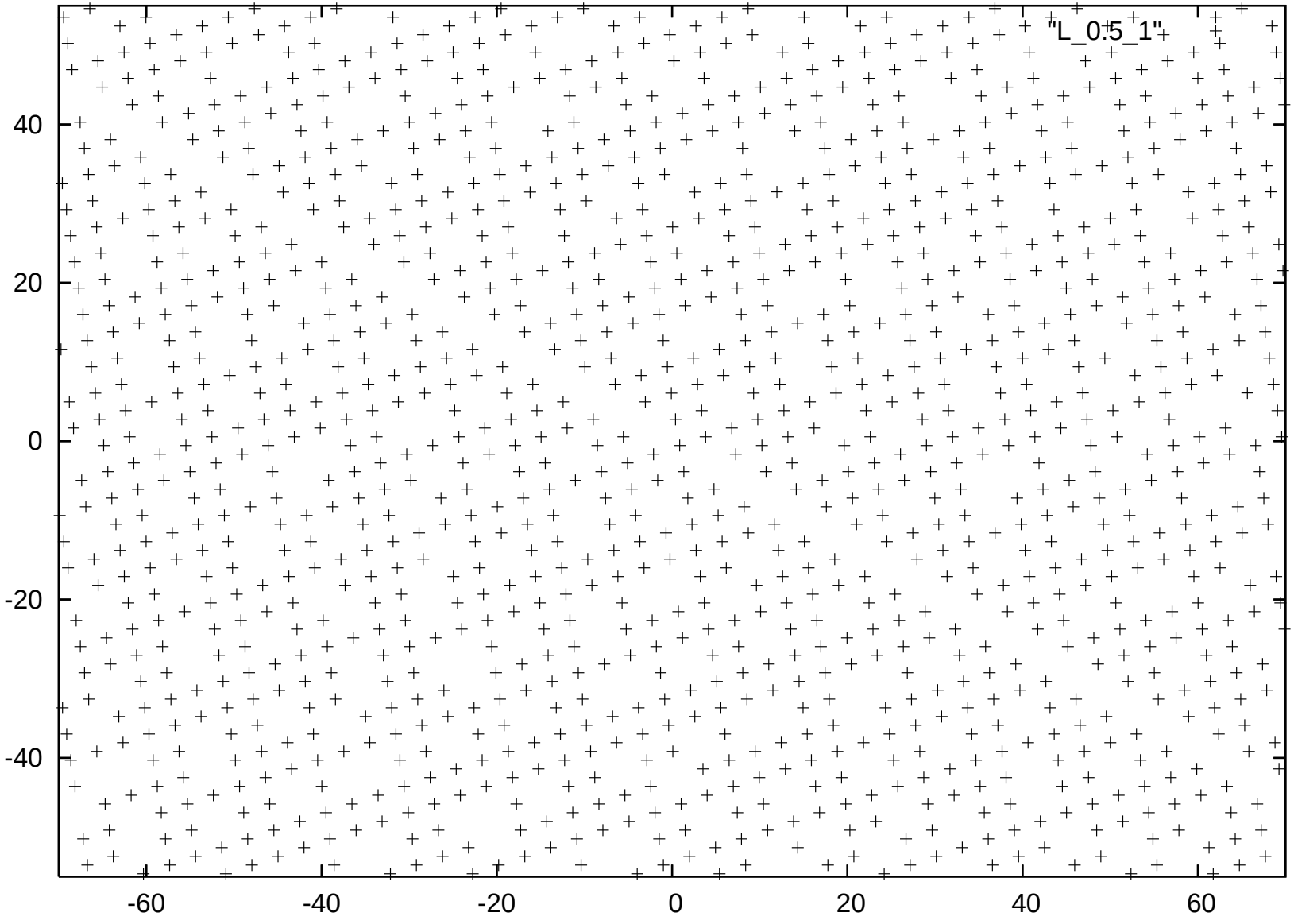
Propriétés :

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

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



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



Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- Limites des suites AGM
- 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 :

$$\mathrm{SL}_2(\mathbb{Z}) \quad \text{(matrice entières de déterminant 1)}$$

action de groupe : $\mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} \to \mathcal{H}$

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\tau = \frac{a\tau + b}{c\tau + d}$$

(en fait, c'est une action de $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\langle -I \rangle$)

Le groupe Γ

$\mathrm{SL}_2(\mathbb{Z})$ est engendré par $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

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

décomposition sur $\langle S, T \rangle$ = algorithme d'Euclide

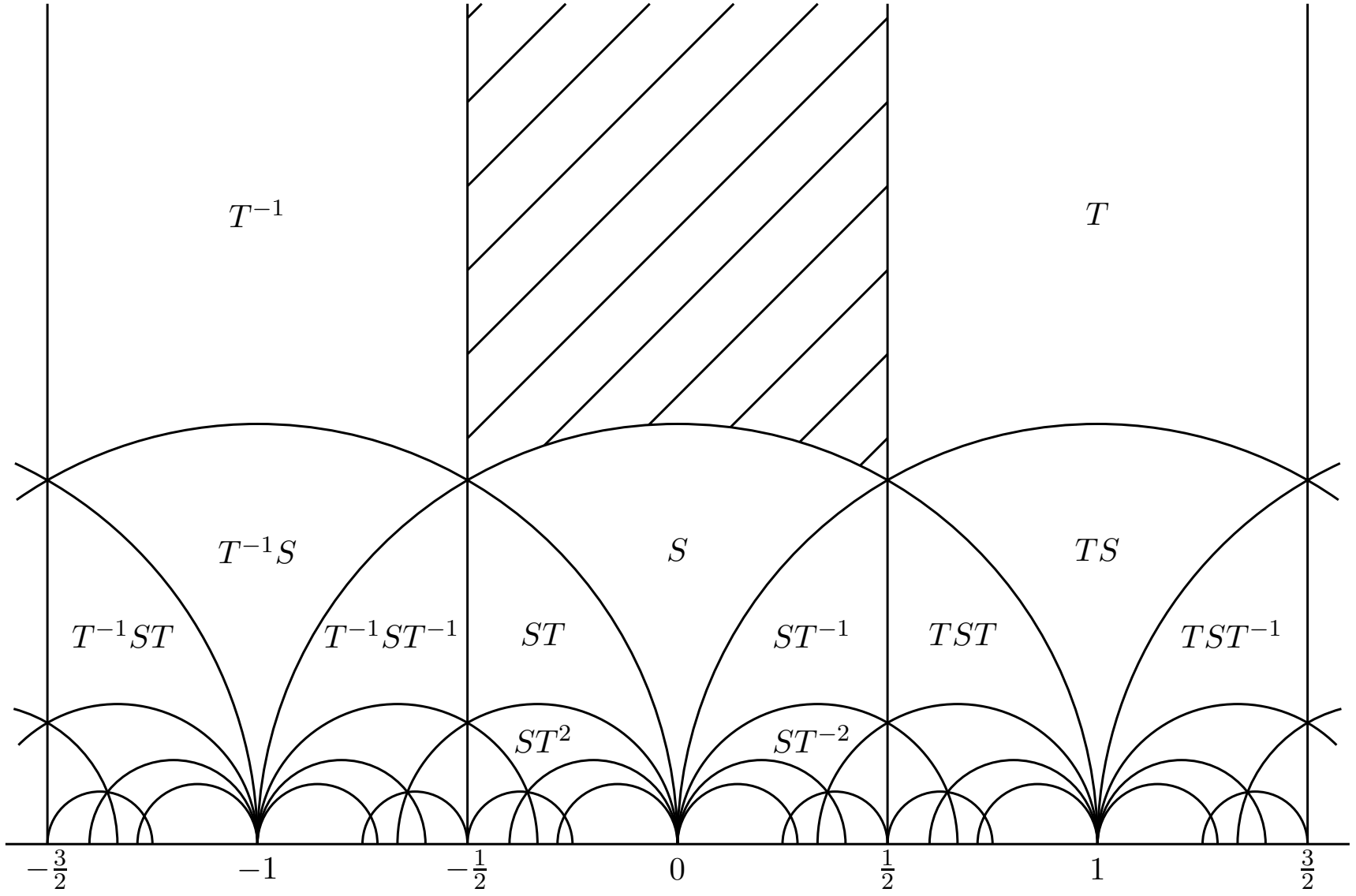
domaine fondamental $\mathcal{F}$:

ensemble de représentants des classes de $\Gamma \backslash \mathcal{H}$

$\Rightarrow$ pour tout $\tau \in \mathcal{H}$, il existe $\gamma \in \Gamma$ tel que

$$\gamma\tau \in \mathcal{F}$$

Le domaine fondamental $\mathcal{F}$



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...)

une fonction modulaire a toujours une période entière

(donc une série de Fourier)

Theta constantes

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

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

Propriétés des theta constantes

- si $\mathrm{Im}\,(\tau_n) \to +\infty$, alors

$$\lim_{n\to+\infty} \theta_0(\tau_n) = \lim_{n\to+\infty} \theta_1(\tau_n) = 1$$

et

$$\lim_{n\to+\infty} \theta_2(\tau_n) = 0$$

- elles sont non nulles sur $\mathcal{H}$

Propriétés des theta constantes

Formules de duplication :

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

$$\theta_1^2(2\tau) = \theta_0(\tau)\cdot\theta_1(\tau)$$

$$\theta_2^2(2\tau) = \frac{\theta_0^2(\tau)-\theta_1^2(\tau)}{2}$$

Égalité de Jacobi :

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

AGM et theta constantes

on en déduit que, pour tout $\tau \in \mathcal{H}$,

$$\left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right)_{n\in\mathbb{N}}$$

est une suite AGM qui converge vers 1.

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

$$\theta_j^2\left(\frac{a\tau+b}{c\tau+d}\right) = \omega_1(\gamma)\omega_2(j,\gamma)(c\tau+d)\theta^2_{\sigma(\gamma,j)}(\tau)$$

$\Rightarrow$ 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 :

$$\begin{aligned} k'(T\tau) &= \frac{1}{k'(\tau)} & k'(S\tau) &= k(\tau) \\ k(T\tau) &= i\frac{k(\tau)}{k'(\tau)} & k(S\tau) &= k'(\tau) \end{aligned}$$

Modularité de k'

k' est une fonction modulaire pour le groupe

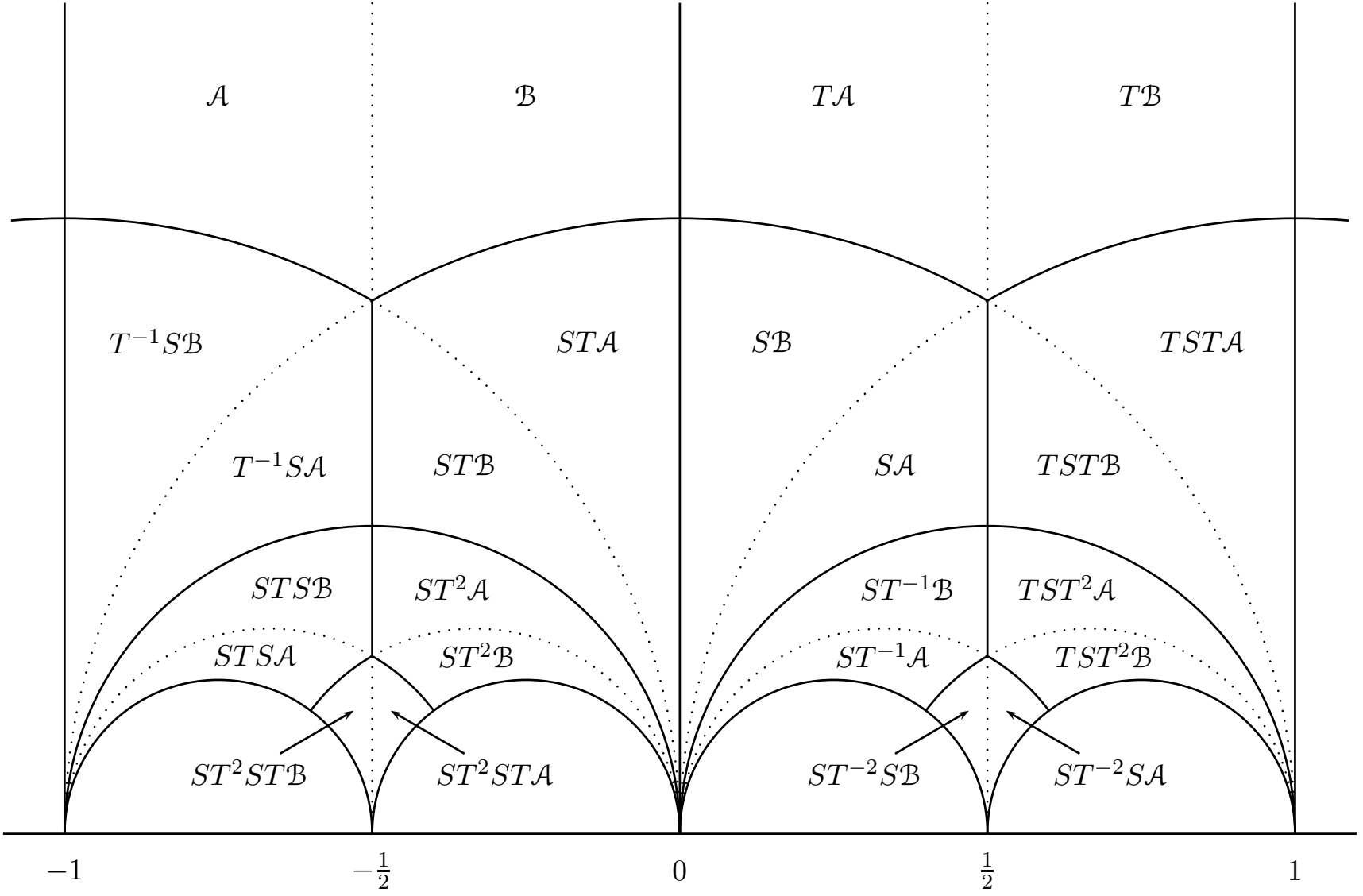
$$\Gamma_{k'} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : b \equiv 0 \bmod 2, c \equiv 0 \bmod 4 \right\},$$

engendré par

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

$k' : \Gamma_{k'} \backslash \mathcal{H} \to \mathbb{C} \setminus \{-1, 0, +1\}$ est bijective

$\mathcal{F}_{k'}$, domaine fondamental pour $\Gamma_{k'}$



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

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

(pôle d'ordre 1 en ∞)

Théorème :

toute fonction modulaire pour Γ est une fraction rationnelle en j

Équations modulaires

Théorème :

deux fonctions modulaires quelconques sont toujours liées algébriquement (équation modulaire)

démonstration :

- f fonction modulaire pour $\Gamma' \subseteq \Gamma$
- $\{\gamma_j\}_{j \in J}$ représentants des classes de $\Gamma' \backslash \Gamma$

$$\prod_{j \in J} (X - f(\gamma_j \tau))$$

$\Rightarrow$ les coefficients sont des fonctions modulaires pour $\Gamma \ldots$

Plan

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

Paramétrisation par k', résultat

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

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

Le “sens facile”

$$\mathcal{L}(a,b) = a\mathcal{L}\left(1, k'(\tau)\right) = \frac{a}{\theta_0^2(\tau)}\mathcal{L}\left(\theta_0^2(\tau), \theta_1^2(\tau)\right)$$

or

- $1 \in \mathcal{L}\left(\theta_0^2(\tau), \theta_1^2(\tau)\right)$,
- k' est invariante sous l’action de $\Gamma_{k'}$

$\Rightarrow$

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

Inclusion réciproque : plus dur!

Limites des suites AGM

soit $(a_n, b_n)_{n\in\mathbb{N}}$ une suite AGM de limite $\neq 0$

$$\left\{ \begin{array}{c} k'\left(\frac{\tau}{2}\right) \\ k'\left(\frac{\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)\tau}{2}\right) \end{array} \right\} \ni \frac{b_{n-1}}{a_{n-1}} \to \frac{b_n}{a_n} = k'(\tau) \to \frac{b_{n+1}}{a_{n+1}} \in \left\{ \begin{array}{c} k'(2\tau) \\ k'\left(2\left(\begin{smallmatrix}1 & 0\\ 4 & 1\end{smallmatrix}\right)\tau\right) \end{array} \right\}$$

$\Rightarrow$ si $\frac{b_0}{a_0} = k'(\tau)$, alors pour tout n, il existe $\tau_n \in \mathcal{F}_{k'}$ tel que

$$\frac{b_n}{a_n} = k'(\tau_n)$$

Limites des suites AGM

$$\lim_{n\to+\infty} k'(\tau_n) = \lim_{n\to+\infty} \frac{b_n}{a_n} = 1 \quad \Rightarrow \quad \lim_{n\to+\infty} \mathrm{Im}\,(\tau_n) = +\infty$$

on en déduit qu'il existe un indice N tel que

$$(a_{N+n}, b_{N+n}) = A\left(\theta_0^2(2^n\tau_N), \theta_1^2(2^n\tau_N)\right)$$

et finalement il existe τ_0' tel que

$$(a_0, b_0) = A\left(\theta_0^2(\tau_0'), \theta_1^2(\tau_0')\right),$$

ce qui permet de conclure...

Plan

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

Objectif

évaluer rapidement certaines fonctions modulaires à grande précision

Applications (A. Enge) :

- calcul de polynômes de classe
  (construction de courbes elliptiques par multiplication complexe)
- calcul de polynômes modulaires
  (comptage de points sur courbes elliptiques par SEA)

Un premier type d'algorithmes

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

La fonction $\mathrm{M}(z)$

pour $z \in \mathbb{C} \setminus \{-1, 0\}$, on pose

- $a_0 = 1$, $b_0 = z$,
- $a_{n+1} = \frac{a_n + b_n}{2}$,
- $b_{n+1} = \sqrt{a_n b_n}$ (bon choix !)

$$\mathrm{M}(z) = \lim_{n \to +\infty} a_n = \lim_{n \to +\infty} b_n$$

évaluation avec une précision de N bits :

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

$O\left(\mathcal{M}(N) \log N\right) = O\left(N^{1+\varepsilon}\right)$ si z dans un compact ne contenant pas 0

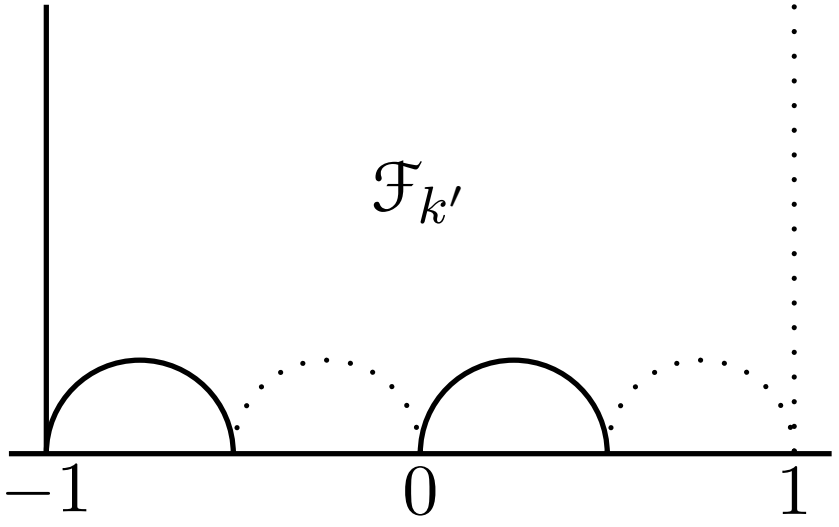
AGM : propriétés

Théorème [Gauss] :

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

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

de plus, M est analytique



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

$\Rightarrow$ 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, et

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

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

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

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

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

$\Rightarrow (z_n)$ 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

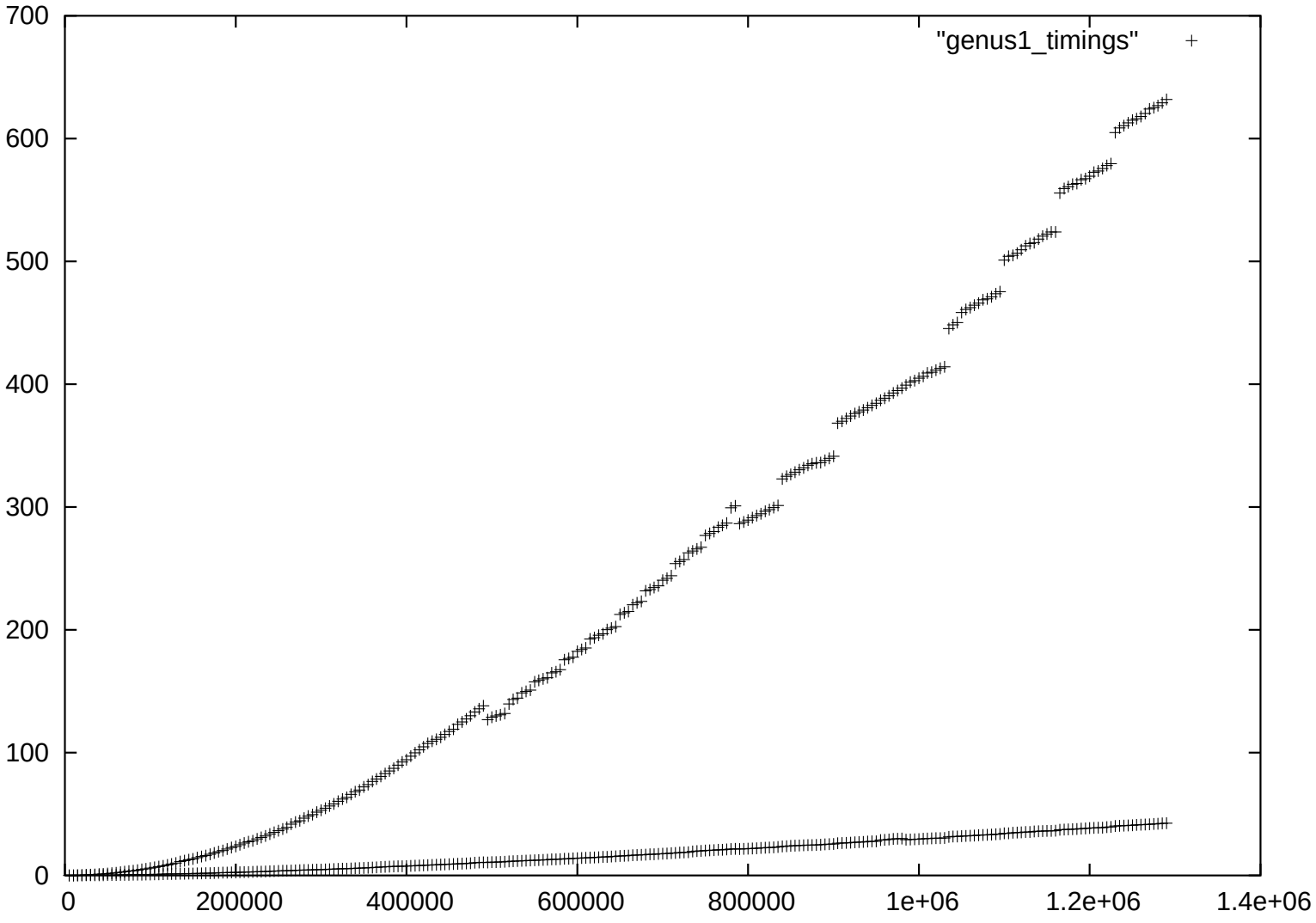
- évaluation de $k'(\tau)$:

$$O\left(\mathcal{M}(N)\log N\right) = O\left(N^{1+\varepsilon}\right)$$

- autres fonctions :

même complexité si un polynôme modulaire est connu

. . . 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

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

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

Propriété : soit $z \in \mathbb{C}$ tel que

- $|z| \leqslant 2^{-12}$
- $|\mathrm{Arg}(z)| \leqslant \frac{\pi}{4}$

alors

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

Évaluation du logarithme

Complexité :

pour calculer $\log z$ avec N bits de précision :

$$z' = \frac{z}{2^n} \text{ tel que } |z'| \simeq \frac{1}{2^N}$$

$\Rightarrow$

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

Plan

- Moyenne arithmético-géométrique (AGM)
- Fonctions modulaires, theta constantes
- Limites des suites AGM
- 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 : $\Gamma_g \times \mathcal{H}_g \to \mathcal{H}_g$

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

Theta constantes

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

Définition générale :

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

si $a = 0$, on a 2^g fonctions de la forme

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

(pour $g = 1$, correspond à θ_0 et θ_1)

Le cas $g = 2$

Formules de duplication :

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

. . . et des formules similaires pour les autres theta constantes

$\Rightarrow$ équations modulaires (toutes les theta constantes sont liées algébriquement aux 4 premières)

Formules de transformation

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

$$\theta_j^2(\gamma\tau) = \omega_1(\gamma)\omega_2(\gamma, j)\mathrm{Det}(C\tau + D)\theta^2_{\sigma(\gamma,j)}(\tau)$$

$\Rightarrow$ on considère les quotients des theta constantes

$\Rightarrow$ notion de fonctions modulaires de Siegel

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)

$\Rightarrow$ il y a toujours convergence quadratique

Résultats en genre 2

- détermination des limites des suites de Borchardt

$$\left\{ \frac{\varepsilon(\gamma)a}{\theta_0^2(\tau)\mathrm{Det}(C\tau+D)} : \gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_b \right\} \cup \{0\}$$

- algorithmes :

$$\text{fonctions modulaires (ou courbes)} \mapsto \tau$$

$$\tau \mapsto \theta_j(\tau), \text{ fonctions modulaires}$$

...en temps $O\left(N^{1+\varepsilon}\right)$

En genre supérieur

- détermination de τ à partir des $\frac{\theta_j^2(\tau)}{\theta_0^2(\tau)}$ en temps

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

- le reste n'est pas possible (raisons théoriques)

Conclusion et perspectives

- amélioration de la complexité :
  $O\left(\mathcal{M}(N)\sqrt{N}\right) \rightarrow O(\mathcal{M}(N)\log N)$
- rapide en pratique
- se généralise au genre 2
  $O(N^{2+\varepsilon}) \rightarrow O(N^{1+\varepsilon})$
  - 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)