Calcul de coefficients de formes modulaires

Peter Bruin
Séminaire d'arithmétique et de géométrie algébrique
25 janvier 2011

1. Introduction

Soient k et n des entiers positifs. Pour tout corps K dont la caractéristique ne divise pas n, on note $\mathrm{M}_k(\Gamma_1(n), K)$ l'espace des formes modulaires de poids k pour le groupe

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$$

à coefficients dans K. Alors $\mathrm{M}_k(\Gamma_1(n))$ est l'espace des sections globales d'un certain fibré en droites $\omega^{\otimes k}$ sur la courbe modulaire $\mathrm{X}_1(n)$ sur K (le champ modulaire si $n \leq 4$).

On a une application K-linéaire

$$\begin{aligned} \mathrm{M}_k(\Gamma_1(n), K) &\to K[[q]] \\ f &\mapsto \sum_{m=0}^{\infty} a_m(f) q^m \end{aligned}$$

qui à chaque forme associe son q-développement. L'interprétation de $\mathrm{M}_k(\Gamma_1(n), K)$ comme l'espace des sections globales de $\omega^{\otimes k}$ implique qu'une forme $f \in \mathrm{M}_k(\Gamma_1(n), K)$ est déterminée par les coefficients $a_i(f)$ avec

$$0 \leq i \leq \frac{k}{12}[\mathrm{SL}_2(\mathbf{Z}) : \{\pm 1\}\Gamma_1(n)]. \tag{1.1}$$

Question. Étant donnés des entiers $n, k > 0$, un corps de nombres K, les $a_i(f) \in K$ d'une forme $f \in \mathrm{M}_k(\Gamma_1(n), K)$, pour i comme dans (1.1), et un entier $m > 0$, peut-on calculer $a_m(f) \in K$ en temps polynomial par rapport à la taille de l'entrée ?

Théorème 1.1 (Couveignes, Edixhoven, de Jong et Merkl [3] pour $n = 1$; B. [1], [2] pour $n \geq 1$).
(a) Soit f une forme modulaire de poids k pour $\Gamma_1(n)$ à coefficients dans un corps de nombres K. Il existe un algorithme qui prend pour entrée un entier $m > 0$ avec sa factorisation et qui calcule $a_m(f)$ en temps polynomial en $\log m$.
(b) Soit n_0 un entier positif. Il existe un algorithme qui prend en entrée

- *un entier $k > 0$,*
- *un entier $n_1 > 0$ sans facteurs carrés et premier à n_0,*
- *un corps de nombres K (donné soit par un polynôme irréductible sur $\mathbf{Q}$ soit par une table de multiplication sur $\mathbf{Q}$),*
- *une forme modulaire f de poids k pour $\Gamma_1(n)$ sur K, où $n = n_0 n_1$, donnée par ses coefficients $a_i(f) \in K$ comme dans (1.1),*
- *un entier $m > 0$ avec sa factorisation,*

et qui calcule $a_m(f)$ en temps polynomial par rapport à la taille de l'entrée (c'est-à-dire n, k, $\log m$ et la taille des données décrivant K) sous l'hypothèse de Riemann pour les fonctions zêta des corps de nombres.

Remarques. (1) La méthode des symboles modulaires, réalisée dans Magma et Sage, permet de calculer $a_m(f)$ en temps polynomial en m. Cependant, vu le fait que la taille de l'entrée et de la sortie est polynomiale en $\log m$, on peut espérer de trouver un algorithme plus efficace.

(2) Le théorème est facile à démontrer pour les séries d'Eisenstein, grâce aux formules explicites pour leurs coefficients.

(3) La condition que m soit donné avec sa factorisation est "raisonnable". En effet, il existe des formes f (comme la série d'Eisenstein E_4) telles que si l'on savait calculer $a_m(f)$ en temps polynomial en $\log m$, disons pour m produit de deux nombres premiers distincts, alors on pourrait trouver la factorisation de m en temps polynomial en $\log m$.

(4) L'algorithme dans [3] est déterministe ; celui dans [1] est probabiliste. On attend à ce qu'il existe un algorithme déterministe dans tous les cas ; c'est une question ouverte.

2. Esquisse de preuve

Les *représentations galoisiennes* associées aux formes propres forment l'outil central de notre approche. Soient K un corps de nombres. Pour toute place finie λ de K, on note K_λ le complété de K par rapport à λ et $k(\lambda)$ son corps résiduel. Soit $f \in \mathrm{M}_k(\Gamma_1(n), K)$ une forme propre pour l'algèbre de Hecke. Des constructions d'Eichler, Shimura, Igusa, Deligne et Serre associent à une telle f une famille de représentations continues semi-simples

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(K_\lambda)$$

λ parcourant les places finies de K, avec les propriétés suivantes : soit l la caractéristique résiduelle de λ, alors ρ_f est non ramifiée hors de nl et pour tout nombre premier $p \nmid nl$, le polynôme caractéristique de $\rho_f(\sigma_p)$ ($\sigma_p =$ Frobenius) est égal à $t^2 - a_p(f)t + \epsilon(p)p^{k-1}$.

L'idée de l'algorithme est de calculer les représentations galoisiennes *réduites*

$$\rho_{f \bmod \lambda} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(k(\lambda))$$

pour λ parcourant un ensemble suffisamment grand de petits nombres premiers. Une telle $\rho_{f \bmod \lambda}$ est représentée par les données suivantes :

- une extension finie galoisienne $L_{f,\lambda}$ de $\mathbf{Q}$;
- un plongement $\mathrm{Gal}(L_{f,\lambda}/\mathbf{Q}) \rightarrowtail \mathrm{GL}_2(k(\lambda))$.

À partir de ces données, on peut calculer

$$\operatorname{tr} \rho_{f \bmod \lambda}(\sigma_p) = a_p(f) \bmod \lambda \in k(\lambda)$$

pour λ dans notre ensemble fini choisi. Ensuite, on applique la majoration de Deligne pour reconstruire $a_p(f) \in K$ à partir de ces réductions.

On se restreint dans la suite aux $\rho_{f \bmod \lambda}$ qui sont absolument irréductibles ; les autres sont plus faciles à calculer. Alors on peut réduire le problème de calculer ρ_f au problème de calculer des représentations galoisiennes de la forme suivante. Soit n un entier ≥ 5. On note $\mathrm{J}_1(n)$ la jacobienne de $\mathrm{X}_1(n)$ sur $\mathbf{Z}[1/n]$ et

$$\mathbf{T}_1(n) = \mathbf{Z}[\{a_p \mid p \text{ premier}\}, \{\langle d \rangle \mid d \in (\mathbf{Z}/n\mathbf{Z})^\times\}] \subseteq \operatorname{End} \mathrm{J}_1(n)$$

l'algèbre de Hecke agissant sur $\mathrm{J}_1(n)$; c'est une $\mathbf{Z}$-algèbre commutative qui est libre de rang fini en tant que $\mathbf{Z}$-module. On considère un corps fini $\mathbf{F}$ et un homomorphisme surjectif

$$e : \mathbf{T}_1(n) \to \mathbf{F}.$$

On note $\mathfrak{m} = \ker(e)$ et

$$\mathrm{J}_1(n)[\mathfrak{m}] = \bigcap_{h \in \mathfrak{m}} \ker(h) \subset \mathrm{J}_1(n) \ ;$$

c'est un schéma en $\mathbf{F}$-espaces vectoriels fini sur $\mathbf{Q}$. L'ensemble $\mathrm{J}_1(n)[\mathfrak{m}](\overline{\mathbf{Q}})$ nous donne une représentation $\mathbf{F}$-linéaire continue de dimension finie de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Remarques. (1) Le fait que les représentations galoisiennes modulaires sont réalisées dans les jacobiennes des courbes modulaires est expliqué par la *relation d'Eichler–Shimura* : pour $p \nmid n$ premier, on a

$$T_p = \mathrm{Frob}_p + \langle p \rangle p/\mathrm{Frob}_p \quad \text{dans } \operatorname{End} \mathrm{J}_1(n)_{\mathbf{F}_p}.$$

En fait, le polynôme caractéristique de Frob_p sur le module de Tate l-adique de $\mathrm{J}_1(n)_{\mathbf{F}_p}$, pour $l \neq p$ premier, est égal à $t^2 - T_p t + \langle p \rangle p$.

(2) Pour démontrer le théorème 1.1, on peut se restreindre aux places λ de K de caractéristique résiduelle $l > k$. Les schéma en $\mathbf{F}$-espaces vectoriels $\mathrm{J}_1(n)[\mathfrak{m}]$ qu'on obtient ainsi sont irréductibles et de $\mathbf{F}$-dimension égale a 2, et réalisent les $\rho_{f,\lambda}$.

La stratégie pour calculer les représentations $\mathrm{J}_1(n)[\mathfrak{m}]$ est de choisir une immersion fermée

$$\iota : \mathrm{J}_1(n)[\mathfrak{m}] \rightarrowtail \mathbf{A}^1_{\mathbf{Q}}$$

de $\mathbf{Q}$-schémas ; l'image a une structure de schéma en $\mathbf{F}$-espaces vectoriels par transport de structure. Cette structure est donnée par un polynôme $F \in \mathbf{Q}[t]$ et des morphismes "addition"

$$\alpha : \mathbf{Q}[t]/(F) \to \mathbf{Q}[u,v]/(F(u), F(v))$$

et "multiplication par c"

$$\mu_c : \mathbf{Q}[t]/(F) \to \mathbf{Q}[t]/(F) \quad (c \in \mathbf{F}).$$

On peut calculer la représentation galoisienne à partir de F, α et les μ_c.

Soit g le genre de $\mathrm{X}_1(n)$. On obtient un plongement ι convenable via le diagramme suivant de $\mathbf{Q}$-schémas :

$$\begin{array}{ccccccc} D_{\mathfrak{m}} & \rightarrowtail & \mathrm{Sym}^g \mathrm{X}_1(n) & \twoheadrightarrow & \mathrm{J}_1(n) & \hookleftarrow & \mathrm{J}_1(n)[\mathfrak{m}] \\ & & \psi_* \downarrow & & & & \\ & & \mathrm{Sym}^g \mathbf{P}^1_{\mathbf{Q}} & \xrightarrow{\sim} & \mathbf{P}^g_{\mathbf{Q}} & \dashrightarrow & \mathbf{A}^1_{\mathbf{Q}}. \end{array}$$

Les notations sont comme suit :

- ψ est une fonction rationnelle non constante sur $\mathrm{X}_1(n)$;
- $D_{\mathfrak{m}}$ est un sous-schéma fermé de $\mathrm{Sym}^g \mathrm{X}_1(n)$ tel que le morphisme $D_{\mathfrak{m}} \to \mathrm{J}_1(n)$ soit une immersion fermée d'image $\mathrm{J}_1(n)[\mathfrak{m}]$;
- β est une fonction rationnelle qui est quotient de deux formes linéaires.

On choisit ψ et β de telle façon que la composition

$$\mathrm{J}_1(n)[\mathfrak{m}] \xrightarrow{\sim} D_{\mathfrak{m}} \to \mathrm{Sym}^g \mathbf{P}^1_{\mathbf{Q}} \xrightarrow{\sim} \mathbf{P}^g_{\mathbf{Q}} \dashrightarrow \mathbf{A}^1_{\mathbf{Q}}$$

donne une immersion fermée ; c'est là le morphisme ι.

La stratégie pour évaluer ι est en calculant avec ce diagramme soit sur $\mathbf{C}$ en utilisant de l'analyse numérique, soit modulo beaucoup de petits nombres premiers. Pour réconstruire $\mathrm{im}(\iota)$ à partir d'une approximation, il faut une majoration de l'hauteur des données rationnelles que l'on veut approcher. Dans [3] et [1], une telle majoration est trouvée en appliquant la théorie d'intersection arithmétique d'Arakelov à des modèles réguliers et semi-stables de courbes modulaires sur des anneaux d'entiers de corps de nombres. Par example, on utilise de façon essentielle le théorème de Riemann–Roch arithmétique dû a Faltings, ainsi que la formule de Faltings–Hriljac reliant nombres d'intersection et hauteurs de Néron–Tate.

Remarque. Faire le "détour" d'une approximation semble nécessaire parce que une approche exacte mènerait à des systèmes d'un grand nombre d'équations, dont la solution nécessite des méthodes comme les bases de Gröbner.

3. Applications

Théorème 3.1. *Il existe un algorithme qui prend en entrée un entier $k > 0$, un entier $n > 0$ sans facteurs carrés, et un entier $m > 0$ avec sa factorisation, et qui calcule la matrice de l'opérateur de Hecke T_m dans l'algèbre de Hecke agissant sur $\mathrm{M}_k(\Gamma_1(n))$ (par rapport à une $\mathbf{Z}$-base fixée de cette algèbre) en temps polynomial en n, k et $\log m$ sous l'hypothèse de Riemann généralisée.*

Corollaire 3.2. *Il existe un algorithme qui prend en entrée un entier $n > 0$ sans facteurs carrés et un nombre premier p, et qui calcule la fonction zêta de la courbe modulaire $\mathrm{X}_1(n)_{\mathbf{F}_p}$ en temps polynomial en n et $\log p$ sous l'hypothèse de Riemann généralisée.*

Voici enfin une autre application du théorème 1.1. Soit $\theta = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$ la fonction thêta de Jacobi. Les puissances de θ vérifient l'identité

$$\theta^k = \sum_{x \in \mathbf{Z}^k} q^{\|x\|^2} = \sum_{m=0}^{\infty} r_k(m) q^m,$$

où $r_k(m)$ est le nombre de manières dont m peut s'écrire comme somme de k carrés. Si k est pair, alors θ^k est une forme modulaire de poids $k/2$ pour $\Gamma_1(4)$. On en déduit le résultat suivant.

Corollaire 3.3. *Il existe un algorithme qui prend en entrée un entier pair $k > 0$ et un entier $m > 0$, et qui calcule le nombre de manières dont m peut s'écrire comme somme de k carrés en temps polynomial en k et $\log m$ sous l'hypothèse de Riemann généralisée.*

Bibliographie

[1] P. J. Bruin, *Modular curves, Arakelov theory, algorithmic applications*. Thèse, Universiteit Leiden, 2010. Disponible sur la toile : `http://hdl.handle.net/1887/15915`.

[2] P. J. Bruin, Computing coefficients of modular forms. À paraître dans les *Publications mathématiques de Besançon* (actes de la conférence *Théorie des nombres et applications*, CIRM, Marseille, 30 novembre–4 décembre 2009).
Prépublication : `http://www.math.u-psud.fr/~bruin/coefficients.pdf`.

[3] J.-M. Couveignes and S. J. Edixhoven (with J. G. Bosman, R. S. de Jong and F. Merkl), *Computational aspects of modular forms and Galois representations*. À paraître dans les *Annals of Mathematics Studies*, Princeton University Press. Prépublication disponible sur arXiv : `math/0605244`.