FORMES MODULAIRES DANS PARI/GP

KARIM BELABAS ET HENRI COHEN

Bill Allombert est récipiendaire en 2020 de la médaille de cristal du CNRS pour sa contribution exceptionnelle au système de calcul Pari/GP (`http://pari.math.u-bordeaux/`). À cette occasion, et à l'occasion de la publication de la version 2.13 de ce système de calcul, Karim Belabas et Henri Cohen, tous deux professeurs de l'université de Bordeaux et membres de l'Institut mathématique de Bordeaux (IMB, UMR5251, Bordeaux INP, CNRS et Université de Bordeaux) présentent le module «Formes modulaires» récemment inclus dans le système.

1. Formes modulaires classiques

Les formes modulaires ont leur origine dans la respectable théorie des fonctions elliptiques due à Jacobi, Weierstraß, et Eisenstein. On les retrouve partout : en analyse complexe, en théorie des nombres, en combinatoire, en topologie algébrique, en physique théorique ; voir le livre «Modular forms are everywhere» [4]. Sous leur forme la plus simple, ce sont des fonctions holomorphes sur le demi-plan supérieur $\operatorname{Im} z > 0$, périodiques de période 1 (donc admettant un dévelopement de Fourier, série en $q = e^{2\pi i z}$) et vérifiant une symétrie $f(-1/z) = z^k f(z)$ pour un certain entier $k \geq 0$. Plus généralement, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est dans un sous-groupe de transformations $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ du demi-plan, on demande $f \mid_k \gamma = f$, où $(f \mid_k \gamma)(z) = (cz+d)^{-k} f((az+b)/(cz+d))$. Pour un sous-groupe Γ d'indice fini et un poids k fixés, ces fonctions forment un $\mathbb{C}$-espace vectoriel de dimension *finie*. Les formes qui apparaissent en théorie des nombres, sont la plupart du temps associées à des groupes Γ définissables par des congruences, en particulier le sous-groupe $\Gamma_1(N)$ des matrices $\gamma \equiv \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \pmod N$ pour un entier $N \geq 1$. On parle de formes de *niveau* N.

Il est naturel de se donner f comme $f(z) = \sum_{n \geq 0} a_n q^n$, par exemple les séries d'Enseistein

$$E_k = 1 - \frac{2}{\zeta(1-k)} \sum_{n \geq 1} \sigma_{k-1}(n) q^n,$$

où $\sigma_j(n) = \sum_{d \mid n} d^j$ et ζ est la fonction zeta de Riemann. Beaucoup de formes modulaires, tel le discriminant modulaire

$$\Delta = (E_4^3 - E_3^4)/1728 = q \prod_{n \geq 1} (1-q^n)^{24}$$

de Ramanujan, ont d'autres représentations, ici comme produit établissant un lien avec la théorie des partitions à travers la série génératrice $\sum_n p(n)q^n = \prod_n (1-q^n)^{-1}$. D'autre part la série de Dirichlet $L(f,s) = \sum_{n\geq 1} a_n n^{-s}$ peut admettre un *produit eulérien*

$$L(f,s) = \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}, \quad \Re(s) \gg 1.$$

La théorie des opérateurs de Hecke (généralisée par Atkin-Lehner) permet de découper les espaces de formes modulaires de niveau N en espaces de formes «anciennes», provenant de niveaux divisant strictement N, et formes «nouvelles» ; l'espace des formes nouvelles admet une base canonique dont les éléments admettent tous un tel produit eulérien.

L'ubiquité des formes modulaires et la finitude de la dimension des espaces correspondant implique d'innombrables relations arithmétiques ou combinatoires. L'exemple le plus célèbre est probablement $E_4^2 = E_8$ qui donne l'identité élémentaire mais hautement non triviale

$$\sigma_7(N) = \sigma_3(N) + 120 \sum_{1\leq n\leq N} \sigma_3(n)\sigma_3(N-n) \ .$$

En développant θ^j où $\theta(q) = \sum_{n\in\mathbb{Z}} q^{n^2}$ on obtient aussi des identités pour le nombre $r_j(N)$ de décomposition de N en somme de j carrés : par exemple si N est sans facteur carré, alors

$$\begin{cases} r_3(N) = 24L(0,\chi_{-N}), & \text{si } N \equiv 3 \pmod 8 \quad \text{(Gauß)}, \\ r_5(N) = -280L(-1,\chi_N), & \text{si } N \equiv 5 \pmod 8 \quad \text{(Smith-Minkowski)}. \end{cases}$$

Dans ces formules, $L(\chi,s) = \sum_{n\geq 1} \chi(n)n^{-s}$ est la fonction L associée au caractère de Dirichlet χ. Le caractère χ_D en question est le symbole de Kronecker tel que, pour tout premier p impair ne divisant pas D, on a $\chi_D(p) = 1$ ou -1 suivant que D est ou non un carré modulo p. Les fonctions θ^j sont de poids $k = j/2$, qui n'est pas entier quand j est impair ; cette généralisation introduit quelques complications ; par exemple l'équation fonctionnelle de θ est $\theta \mid_{1/2} \gamma = \nu(\gamma)\cdot\theta$ pour tout $\gamma \in \Gamma_\theta$, le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ et $T^2 = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$. Dans cette formule $\nu(\gamma)$ est une racine 8-ème de l'unité explicite, par exemple $\nu(S) = e^{-i\Pi/4}$ et bien sûr $\nu(T^2) = 1$.

Le discriminant Δ de Ramanujan, que nous avons défini par

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24} \ ,$$

est une forme nouvelle et c'est l'une des plus célèbres formes modulaires. Si on écrit son développement de Fourier

$$\Delta(z) = \sum_{n\geq 1} \tau(n)q^n = q - 24q^2 + 252q^3 + \cdots \ ,$$

la fonction $\tau(n) \in \mathbb{Z}$ a des propriétés remarquables dont les plus simples se résument en la formule

$$L(\Delta,s) = \sum_{n\geq 1} \tau(n)n^{-s} = \prod_{p \text{ premier}} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}} \ .$$

L'inégalité $\tau(p)^2 < 4p^{11}$, démontrée en 1969 par Deligne, est bien plus profonde. Le calcul d'une valeur de $\tau(p)$ est difficile quand p est grand. Malgré un résultat théorique remarquable de Edixhoven, Couveignes, et al. [3] qui donnent un algorithme en temps polynomial en $\log p$ (en calculant $\tau(p)$ modulo suffisamment de premiers pour que sa valeur soit déterminée grâce à la borne de Deligne), des formules en $O(\sqrt{p})$ seront plus rapide pour calculer une valeur isolée pour p modérément grand, par exemple

$$\tau(p) = 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 - \sum_{1 \le s < 2\sqrt{p}} s^{10} H(4p - s^2) \ ,$$

où $H(N)$ est le nombre de classes de Hurwitz, lié au nombre de classes de formes quadratiques binaires de discriminant $-N$.

Comme dans l'exemple des sommes de carrés, il est fréquent de constater qu'un problème arithmétique s'encode dans les coefficients a_n d'une forme modulaire $f(q) = \sum_n a_n q^n$. Dans les cas simples, on obtient une formule explicite pour a_n et des identités comme $E_4^2 = E_8$. Mais, même dans les cas compliqués, la dimension finie des espaces permet d'écrire f comme combinaison linéaire de séries d'Eisenstein, très bien comprises, et de formes nouvelles, dont les coefficients sont plus mystérieux mais contrôlés par la borne de Deligne. À défaut de formules, on obtient ainsi des résultats asymptotiques pour les a_n : le terme principal est donné par des séries d'Eisenstein (typiquement de taille n^{k-1} en poids k), et les formes nouvelles introduisent un terme d'erreur (en $n^{(k-1)/2}$).

Mentionnons finalement l'utilisation des formes modulaires dans la démonstration par Wiles *et al.* du grand théorème de Fermat, ainsi qu'ultérieurement dans l'étude de nombreuses équations diophantiennes analogues.

2. Formes modulaires dans Pari/GP

Trois logiciels importants permettent de manipuler facilement les espaces de formes modulaires classiques : Magma et les logiciels libres SageMath et Pari/GP. Les deux premiers s'appuient sur la théorie des symboles modulaires, qui sont des objets algébriques calculables associés à N et un entier $k \ge 2$ permettant d'obtenir une base de l'espace des formes modulaires de poids k pour $\Gamma_1(N)$. Nous présentons une implantation alternative dans le troisième, reposant sur la formule des traces d'Eichler-Selberg, qui permet d'obtenir les q-développements d'une base du même espace. Plus précisément, l'espace ambient étant de dimension finie, une forme $f(q) = \sum a_n q^n$ est déterminée par les $\{a_n \colon n \le B(N,k)\}$ pour une borne B effective et la formule de traces calcule ces coefficients dans le corps cyclotomique $\mathbb{Q}(\zeta_N)$. Un peu d'algèbre linéaire permet ensuite de manipuler facilement formes et opérateurs linéaires (opérateurs de Hecke, involution d'Atkin-Lehner) à partir de ces données. Tous les algorithmes s'exécutent en temps polynomial en la dimension de l'espace, qui est elle-même en $O(Nk)$.

En fait, cette formule de traces donne directement l'espace des formes nouvelles de niveau N. On en extrait la base canonique des *newforms*, admettant un produit eulérien, qui sont les plus intéressantes pour l'arithmétique. Toujours dans l'optique de représenter les formes comme combinaison linéaires de formes très bien comprises, nous utilisons aussi un théorème de Borissov et Gunnells qui indique qu'à des exceptions facilement contrôlables

près[1] en poids $k = 2$, les produits de deux séries d'Eisenstein engendrent tout l'espace. On obtient ainsi de nouvelles bases, plus du tout canoniques mais très explicites, qui permettent d'autres application comme le calcul de périodes, de produits de Petersson ou le calcul des coefficients de $f \mid_k \gamma$ pour $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (développement aux pointes). Un défaut de cette méthode est que, même si on s'intéresse uniquement à des formes à coefficients rationnels, travailler dans $\mathbb{Q}(\zeta_N)$ n'est plus suffisant : on a besoin de racines de l'unité d'ordre $\mathrm{ppcm}(N, \phi(N))$, à cause des caractères modulo N intervenant dans les séries d'Eisenstein.

Le même type de techniques permet de construire les espaces de formes de poids $k = 1$ ou demi-entier, dans $\frac{1}{2}\mathbb{Z}$: on multiplie les formes de l'espace à construire par une forme de référence f_0 bien connue (une série d'Eisenstein ou une fonction θ), ce qui augmente le poids de manière à travailler dans un des espaces qu'on savait déjà construire. (Dans certains cas, on ne peut pas éviter d'augmenter aussi le niveau, ce qui ralentit les calculs.) On peut maintenant calculer dans cet espace, et la seule difficulté est de décider quand la forme f_0 en divise une autre, pour pouvoir revenir dans l'espace d'origine.

Sans rentrer dans le détail, ces méthodes permettent aussi de calculer les espaces de Kohnen et la correspondance de Shimura pour les espaces de formes de poids demi-entier.

3. Exemples

Nous donnons maintenant quelques applications des outils disponibles dans le module décrit au §2. Commençons par calculer les dimensions et des bases en niveau 1 et poids 12 :

```
? mfdim([1,12])   \\ l'espace total est de dimension 2
%1 = 2
? mfdim([1,12], 3)   \\ dim(séries d'Eisenstein) = 1
%2 = 1
? M = mfinit([1,12]); [f, g] = mfbasis(M);
? mfcoefs(f, 6)
%3 = [691/65520, 1, 2049, 177148, 4196353, 48828126, 362976252]
? mfcoefs(g, 8)
%4 = [0, 1, -24, 252, -1472, 4830, -6048, -16744, 84480]
```

La forme g n'est rien d'autre que Δ, quand à f c'est essentiellement la série d'Eisenstein E_{12} :

```
? mftobasis(M, mfDelta())
%5 = [0, 1]~
? mftobasis(M, mfEk(12))
%6 = [65520/691, 0]~   \\ (2 / zeta(-11)) E12
```

Notons au passage qu'en niveau et poids 2, l'espace des formes nouvelles est trivial :

```
? mfdim([2,2], 0)  \\ 0 sous espace "new"
%7 = 0
```

1. qui se produisent exactement quand il existe une *newform* f dans l'espace telle que $L(f, 1) = 0$, par exemple les formes attachées à des courbes elliptiques rationnelles de rang ≥ 1.

Modulo quelques lemmes dont ni l'énoncé, ni la démonstration, ne tiennent dans la marge de cette page, cette assertion démontre le grand théorème de Fermat (voir [1, §15] ; [2]).

Un exemple de calcul de la base des formes nouvelles en niveau 57 et poids 2 :

```
? F = mfeigenbasis(mfinit([57,2])); #F
%8 = 3    \\ il y a 3 newforms
? foreach(F, f, print(mfcoefs(f,10)))
[0, 1, 1, 1, -1, -2, 1, 0, -3, 1, -2]
[0, 1, -2, 1, 2, 1, -2, 3, 0, 1, -2]
[0, 1, -2, -1, 2, -3, 2, -5, 0, 1, 6]
```

Donnons maintenant quelques exemples de recherches de formes, connaissant quelques coefficients, en bornant niveau et poids. En niveau ≤ 200 et poids 4, on cherche une *newform* rationnelle telle que $a_2 = -3$, $a_3 = -3$, $a_5 = -18$:

```
? v = mfeigensearch ([[1..200], 4],  [[2,-3], [3,-3], [5,-18]]);
? #v
%11 = 1 \\ il n'y en a qu'une
? mfcoefs(v[1], 10)
%12 = [0, 1, -3, -3, 1, -18, 9, 7, 21, 9, 54]
```

Puis en niveau ≤ 100 et poids 3, une forme rationnelle telle que $a_i = i$ pour $i \leq 42$:

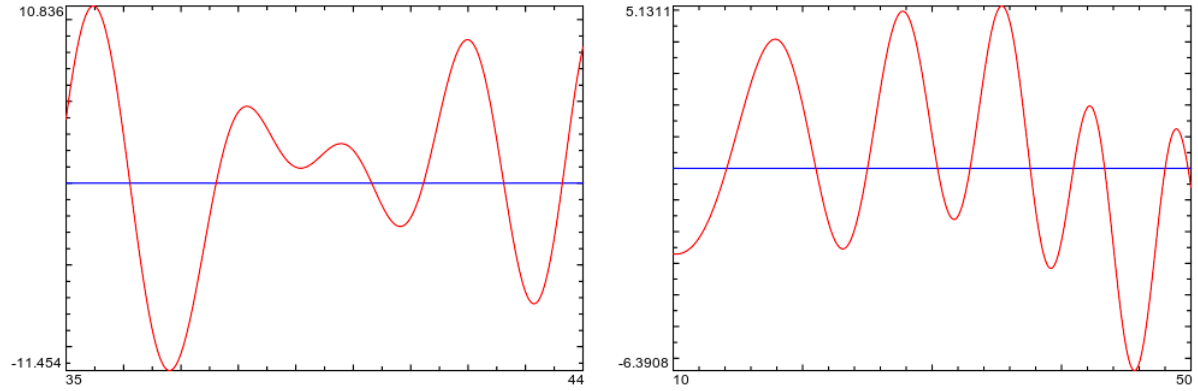
```
? F = mfsearch([[1..100], 3], [0..42]); #F
%13 = 1   \\ de nouveau une seule newform
```

Quelques applications plus avancées pour finir. Dans PARI/GP, on appelle «symbole» une structure permettant le calcul de polynômes de périodes et des produits de Petersson, y compris quand il n'y a pas de notion de symbole modulaire comme en poids 1 ou demi-entier. Ici, on calcule le carré de Petersson de la fonction θ :

```
? t = mfsymbol(mfTheta()); bestappr(mfpetersson(t) / Pi)
%14 = 1/3  \\ <theta,theta> ~ Pi/3
```

La commande suivante construit la forme f associée à la forme quadratique définie positive $4x^2 + 2xy + 6y^2$ ainsi que l'espace ambient (en niveau 23 et poids 1), puis la fonction L et la fonction de Hardy associée (une fonction de $\mathbb{R} \to \mathbb{R}$ qui a les mêmes zéros que la fonction $L(1/2 + it)$), et compare son graphe avec celui obtenu pour la fonction ζ :

```
? [mf,f] = mffromqf([4,1; 1,6]); L = lfuninit(lfunmf(mf,f), [50]);
  ploth(t=35,44,lfunhardy(L,t)); ploth(t=10,50,lfunhardy(1,t))
```



Dans le graphe de droite, chaque franchissement de l'axe (le premier pour $t \approx 14.1$) correspond à un zéro de ζ sur la droite critique. Dans le graphe de gauche, le minimum local au dessus de l'axe des abscisses indique que cette fonction L ne vérifie pas l'hypothèse de Riemann.

Références

[1] H. Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007.

[2] G. Cornell, J. H. Silverman, & G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1997, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[3] B. Edixhoven & J.-M. Couveignes (eds.), *Computational aspects of modular forms and Galois representations*, Annals of Mathematics Studies, vol. 176, Princeton University Press, Princeton, NJ, 2011, How one can compute in polynomial time the value of Ramanujan's tau at a prime.

[4] K. Ono, Modular forms are everywhere : celebration of Don Zagier's 65th birthday, *Res. Math. Sci.* **6** (2019), no. 1.

[5] The PARI Group, Bordeaux, PARI/GP, version `2.13.0`, 2020, `http://pari.math.u-bordeaux.fr/`.