Calcul rapide de coefficients de formes modulaires et représentations galoisiennes

Résumé. Nous verrons comment calculer rapidement un coefficient d'une forme modulaire en passant par une représentation galoisienne. Le cœur du calcul est la résolution d'un problème inverse d'Abel-Jacobi, ce qui est un exemple naturel de système algébrique en grande dimension. Nous montrerons comment une méthode semi-numérique, semi-algébrique permet de résoudre ce problème en temps polynomial en la dimension.

Formes modulaires et problèmes diophantiens

Les coefficients du q-développement d'une forme modulaire admettent de riches interprétations diophantiennes. Par exemple, si Q est une forme quadratique définie positive à coefficients entiers en r variables, alors la fonction thêta associée

$$\vartheta_Q(q) = \sum_{x \in \mathbb{Z}^r} q^{Q(x)} = \sum_{n=0}^{+\infty} a_n q^n$$

est modulaire, et ses coefficients a_n s'interprètent comme le nombre de solutions dans $\mathbb{Z}^r$ de $Q(x) = n$. On peut également citer le cas des courbes elliptiques, où le théorème de Taniyama-Weil affirme que si $a_p = |E_{\mathbb{F}_p}(\mathbb{F}_p)| - p - 1$ pour E une courbe elliptique sur $\mathbb{Q}$ et p premier de bonne réduction de E, alors les a_p sont les coefficients d'une forme modulaire de poids 2. Par conséquent, il serait intéressant de disposer d'algorithmes permettant de calculer rapidement les coefficients d'une forme modulaire.

Dans le contexte des courbes elliptiques, un célèbre algorithme dû à Schoof donne le nombre $p + 1 - a_p$ de points $\mathbb{F}_p$-rationnels d'une courbe elliptique sur $\mathbb{F}_p$ en temps polynomial en $\log p$. Pour ce faire, une borne $|a_p| < 2\sqrt{p}$ étant connue, pour différents petits nombres premiers ℓ, l'algorithme évalue a_p modulo ℓ en l'interprétant comme la trace d'un morphisme de Frobenius, et il en déduit la valeur de a_p par restes chinois.

La méthode de calcul de coefficients de formes modulaires que nous présenterons suit le même schéma. Elle offre en outre l'intérêt de construire tout-à-fait explicitement des représentations galoisiennes, ce qui est toujours intéressant en vue de mieux comprendre le groupe de Galois absolu de $\mathbb{Q}$, et qui fournit des exemples explicites de solutions au problème de Gross, c'est-à-dire des corps de nombres non résolubles ramifiés en un seul nombre premier. Historiquement, l'idée de cet algorithme fut suggérée par Schoof à Edixhoven.

La représentation galoisienne attachée à une forme modulaire

Considérons une newform (forme parabolique propre nouvelle normalisée)

$$f = q + \sum_{n \geqslant 2} a_n q^n$$

de niveau N et de poids 2. Les coefficients a_n appartiennent à l'anneau des entiers $\mathbb{Z}_{K_f}$ d'un corps de nombres K_f. Choisissons un idéal premier $\mathfrak{l}$ de degré résiduel 1 de K_f au-dessus d'un $\ell \nmid N$. On sait alors qu'il existe une représentation galoisienne

$$\rho_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

non-ramifiée en dehors de ℓN et telle que pour tout premier $p \nmid \ell N$,

$$\operatorname{Tr} \rho_{f,\ell}\left(\left(\frac{\overline{\mathbb{Q}}/\mathbb{Q}}{p}\right)\right) = a_p \bmod \mathfrak{l},$$

où $\left(\frac{\overline{\mathbb{Q}}/\mathbb{Q}}{p}\right)$ désigne (la classe de conjugaison de) l'élément de Frobenius en p. Or on sait borner a_p, donc, en calculant cette représentation pour plusieurs ℓ, on peut calculer a_p par restes chinois.

Nous présenterons une méthode pour calculer cette représentation galoisienne en temps polynomial en ℓN. Nous utilisons le fait que le sous-espace propre

$$V_{f,\mathfrak{l}} = \bigcap_{n \geqslant 2} \operatorname{Ker}\left(T_n - (a_n \bmod \mathfrak{l})\right)\big|_{J_1(N)[\ell]}\Big) \subset J_1(N)[\ell]$$

de la ℓ-torsion $J_1(N)[\ell]$ de la jacobienne $J_1(N)$ de la courbe modulaire $X_1(N)$, où les T_n sont les opérateurs de Hecke, est de dimension exactement 2 sur $\mathbb{F}_\ell$, et que l'action de Galois sur ses points réalise cette représentation galoisienne.

Nous verrons tout d'abord comment calculer efficacement le réseau des périodes de la courbe modulaire $X_1(N)$, puis nous verrons comment on peut se servir de ces périodes pour calculer les points de l'espace $V_{f,\mathfrak{l}}$. Notre méthode est basée sur l'application des algorithmes de Khuri-Makdisi aux courbes modulaires afin d'inverser l'application d'Abel-Jacobi par itération de Newton.

Plus précisément, après avoir calculé un diviseur D sur $X_1(N)$ représentant approximativement un point de $V_{f,\mathfrak{l}}$, nous résolvons l'équation $[\ell]D \sim 0$ en appliquant une méthode de Newton en plusieurs variables sur la variété $J_1(N)$.

Finalement, nous verrons comment les algorithmes de théorie de Galois effective proposés par les frères Dokchitser permettent de calculer l'image dans $\mathrm{GL}_2(\mathbb{F}_\ell)$ de l'élément de Frobenius en p en temps polynomial en $\log p$.