Les formes modulaires, la « cinquième opération de l'arithmétique »

Cécile Armana, Institut de Mathématiques de Jussieu

Séminaire lambda, Institut de Mathématiques de Bordeaux, 16 mai 2007

Selon une citation attribuée à M. Eichler, il y aurait cinq opérations fondamentales en arithmétique : l'addition, la soustraction, la multiplication, la division et les formes modulaires. Cet exposé est une introduction, d'un point de vue élémentaire, aux formes modulaires, ces fonctions si exceptionnellement symétriques que leur existence paraît « miraculeuse ». Nous verrons quelques exemples d'identités arithmétiques non triviales qu'elles permettent d'obtenir. Malheureusement, le temps ne permettra pas d'aborder un point de vue plus profond (surfaces de Riemann, fonction-L associée, lien avec les courbes elliptiques et les courbes modulaires) qui permet d'aborder des problèmes arithmétiques plus ardus (par exemple, le théorème de Fermat et le problème des nombres congruents).

Soit $n \geq 1$ un entier. Le théorème de Lagrange (1770) affirme que n peut s'exprimer comme somme de quatre carrés, éventuellement nuls. On s'intéresse au nombre de façons d'écrire n comme somme de quatre carrés, c'est-à-dire à

$$A(n) = \#\{(a,b,c,d) \in \mathbb{Z}^4 \mid n = a^2+b^2+c^2+d^2\}.$$

Par exemple, pour $n = 1$, il y a 8 écritures possibles :

$$\begin{array}{cccc} 1^2+0+0+0 & 0+1^2+0+0 & 0+0+1^2+0 & 0+0+0+1^2 \\ (-1)^2+0+0+0 & 0+(-1)^2+0+0 & 0+0+(-1)^2+0 & 0+0+0+(-1)^2 \end{array}$$

Pour $n = 2$, les écritures possibles se déduisent de 1^2+1^2+0+0 et il y en a 24. Le but de l'exposé est de démontrer la formule générale suivante grâce à la théorie des formes modulaires.

Théorème (Jacobi, 1829)**.** *Le nombre de façons d'écrire un entier $n > 0$ comme la somme de quatre carrés est :*

- 8 *fois la somme de ses diviseurs si n est impair ;*
- 24 *fois la somme de ses diviseurs* impairs *si n est pair.*

Pour cela, nous allons utiliser une fonction thêta, dont les premières apparitions semblent remonter à Jacques Bernoulli (1713), Euler (1748) et Jacobi (1829).

1 Formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$

Il va de soit que le langage moderne que nous utiliserons ici n'était pas celui employé par Jacobi...

1.1 Définitions

On « rappelle » que $\mathrm{SL}_2(\mathbb{Z}) = \{g \in M_2(\mathbb{Z}) \mid \det(g) = 1\}$.

Définition. Le *demi-plan de Poincaré* est $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

Soit $k \in \mathbb{Z}$.

Définition. Une *forme modulaire de poids k pour* $\mathrm{SL}_2(\mathbb{Z})$ est une fonction holomorphe $f : \mathcal{H} \to \mathbb{C}$ vérifiant

1) $f\left(\dfrac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ pour toute $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. En particulier, $f(z+1) = f(z)$ et f admet un développement en série de Fourier : $f(z) = \sum_{n\in\mathbb{Z}} c_n q^n$ où $q = \mathrm{e}^{2i\pi z}$.
2) $f(z) = \sum_{n\geq 0} c_n q^n$ (on dit que f est holomorphe en $i\infty$).

Remarque. Généralement, on demande qu'une forme modulaire soit seulement méromorphe sur $\mathcal{H}$. Nous n'en ferons pas usage ici.

Les formes modulaires de poids k forment un $\mathbb{C}$-espace vectoriel M_k. La condition 1 (appelée parfois condition de modularité) correspond à des équations fonctionnelles relativement au groupe de matrices $\mathrm{SL}_2(\mathbb{Z})$. Notons que ce groupe est engendré par les matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Définition. Avec les notations précédentes, une forme modulaire f vérifiant $c_0 = 0$ (c'est-à-dire f s'annule en $i\infty$) est dite *parabolique* (*cuspidal* en anglais).

Les formes paraboliques forment un sous-espace vectoriel de M_k noté S_k. De plus, on a une application linéaire

$$\begin{array}{ccc} M_k & \to & \mathbb{C} \\ f & \mapsto & c_0 \end{array}$$

de noyau S_k. Donc M_k/S_k est de dimension au plus 1.

Remarque. 1) En considérant la matrice $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on obtient $f(z) = (-1)^k f(z)$. Donc pour k impair, $M_k = S_k = \{0\}$.

2) Si f est de poids k et g de poids k' alors fg est de poids $k+k'$. L'espace des formes modulaires de tout poids est donc une algèbre graduée par le poids.

1.2 Ça existe !

Séries d'Eisenstein. Soit $k \geq 4$ un entier pair.

Définition. Pour $z \in \mathcal{H}$, on pose $G_k(z) = \dfrac{(k-1)!}{2(2\pi\mathrm{i})^k} \sum\limits_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \dfrac{1}{(mz+n)^k}$.

Cette série converge absolument pour $k > 2$. Elle est nulle pour k impair, les termes en (m,n) et $(-m,-n)$ se compensant. C'est une sorte de fonction zêta de Riemann en dimension 2. On vérifie sans trop de difficulté la propriété de transformation pour les matrices de $\mathrm{SL}_2(\mathbb{Z})$ (cela correspond à faire un changement d'indice dans la somme).

En utilisant la formule classique donnant un développement en série de la fonction cotangente, on obtient le développement de Fourier

$$G_k(z) = \frac{(-1)^{k/2}(k-1)!}{(2\pi)^k}\zeta(k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

ce qui montre que $G_k \in M_k$. On a posé

$$\sigma_h(n) = \sum_{\substack{d>0 \\ d|n}} d^h$$

et $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ est la fonction zêta de Riemann. Ce développement justifie la normalisation adoptée dans la définition de G_k. Notons que G_k n'est pas parabolique car son terme constant n'est pas nul (c'est la valeur de ζ en des entiers pairs !). Enfin, ce terme constant peut être remplacé par

$$-\frac{B_k}{2k}$$

où $B_k \in \mathbb{Q}$ désigne le $k$ème nombre de Bernoulli, que l'on peut définir comme le coefficient de $\frac{x^k}{k!}$ dans le développement en série de $\frac{x}{\exp(x)-1}$.

Voici les premiers termes de ces développements.
$G_4(z) = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6 + \cdots$
$G_6(z) = \frac{-1}{504} + q + 33q^2 + 244q^3 + 1057q^4 + \cdots$
$G_8(z) = \frac{1}{480} + q + 129q^2 + 2188q^3 + \cdots$
$G_{10}(z) = \frac{-1}{264} + q + 513q^2 + \cdots$
$G_{12}(z) = \frac{691}{65520} + q + 2049q^3 + \cdots$

Comme on peut le voir sur la formule générale, tous les coefficients sont des entiers naturels sauf le coefficient constant qui est rationnel. Le coefficient en q est $\sigma_{k-1}(1) = 1$.

La fonction Δ.

Définition. $\Delta = 8000G_4^3 - 147G_6^2 \in M_{12}$

Jacobi a obtenu le développement en produit infini suivant :

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

On obtient que le développement de Δ commence ainsi :

$$\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

En particulier, Δ est parabolique (les coefficients 8000 et 147 ont bien entendu été choisis pour cela).

2 La cinquième opération

2.1 Calculs de dimensions

Nous allons étudier plus en détail les espaces M_k et montrer notamment qu'ils sont de dimension finie.

Proposition. *Pour $k \geq 4$ pair, $M_k = \langle G_k \rangle \oplus S_k$.*

En effet, G_k a un terme constant non nul et si $f \in M_k$, on peut se débrouiller pour faire disparaître son terme constant en lui ajoutant un bon multiple de G_k...

Proposition. $S_k \simeq M_{k-12}$

L'isomorphisme est donné par l'application linéaire $f \mapsto \dfrac{f}{\Delta}$. Ce quotient est holomorphe sur $\mathcal{H}$ (car Δ ne s'annule pas sur $\mathcal{H}$ comme le montre son expression comme produit infini) et holomorphe en $i\infty$ (car f et Δ n'ont pas de terme constant).

Théorème. *Soit f une forme modulaire de poids k, $f \neq 0$. Alors*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{P \in \mathcal{H}/G}{}' \, v_P(f) = \frac{k}{12}.$$

Dans cette formule, i désigne le nombre complexe du même nom, $\rho = e^{i\pi/3}$. Le groupe $G = \mathrm{SL}_2(\mathbb{Z})/\{+I, -I\}$ agit sur $\mathcal{H}$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$ et $\mathcal{H}/G$ désigne un système de représentants des orbites ; $v_P(f)$ désigne l'ordre d'annulation de f en P comme fonction holomorphe ; il ne dépend que de l'orbite de P. La somme $'$ porte sur les P différents de i et ρ et on montre que c'est une somme finie. Enfin, $v_\infty(f)$ désigne l'ordre d'annulation en $q = 0$ du développement en série de Fourier de f. En fait, i et ρ subissent un traitement particulier car ce sont les seuls points du domaine fondamental à avoir un stabilisateur non trivial (d'ordre resp. 2 et 3).

La démonstration s'obtient par un calcul de résidus (plus précisément, en intégrant f'/f le long du « bord » d'un domaine fondamental de $\mathcal{H}/G$).

Examinons des conséquences de ces résultats.

1) Pour $k < 0$ et $k = 2$, on a $M_k = S_k = 0$.

En effet, si $f \neq 0$, on a une relation de la forme $n + \frac{1}{2}n' + \frac{1}{3}n'' + m = \frac{k}{12}$. De plus, n, n', n'', m sont des entiers ≥ 0 car f holomorphe sur $\mathcal{H}$ et en $i\infty$. Pour $k < 0$ et $k = 2$, on constate qu'une telle équation est impossible.

2) Si M_k est de dimension d, alors M_{k+12} est de dimension $d + 1$.

Cela vient des deux propositions précédentes.

Résumons ceci dans un tableau.

k	< 0	1	2	4	6	8	10	12	$\cdots$	k	$\cdots$	$k+12$	$\cdots$
$\dim M_k$	0	?	0	?	?	?	?	?	$\cdots$	d	$\cdots$	$d+1$	$\cdots$

Si on arrive à déterminer les points d'interrogation, on aura montré par récurrence que M_k, et donc S_k, sont de dimension finie.

Pour $k = 0$, on a $S_0 \simeq M_{-12} = 0$. Donc $\dim M_0 \leq 1$. On connaît une forme modulaire non nulle de poids 0, la fonction constante égale à 1 ! Donc $\dim M_0 = 1$.

Pour $k = 4, 6, 8, 10$, on a $S_k \simeq M_{k-12} = 0$ car $k - 12 < 0$. Donc $\dim M_k \leq 1$. Là encore, on connaît une forme modulaire non nulle de poids k, la série d'Eisenstein G_k. Donc $\dim M_k = 1$.

Pour $k = 12$, on a $M_{12} =< G_{12} > \oplus S_{12}$ avec $S_{12} \simeq M_0$ qui est de dimension 1 (et même engendré par la forme parabolique Δ de poids 12). Donc $\dim M_{12} = 2$.

On obtient le tableau suivant.

k	< 0	0	2	4	6	8	10	12	$\cdots$	k	$\cdots$	$k+12$	$\cdots$
$\dim M_k$	0	1	0	1	1	1	1	2	$\cdots$	d	$\cdots$	$d+1$	$\cdots$

Quel est l'intérêt de ces résultats ? D'une part, une philosophie générale dit que les coefficients des formes modulaires portent une information arithmétique (par exemple, G_k et les sommes de puissances de diviseurs de $k - 1$). D'autre part, si on fabrique plus de $d = \dim M_k$ formes de poids k, elles sont nécessairemment liées. En identifiant les coefficients de leur développements de Fourier, on obtient ainsi « gratuitement » des identités arithmétiques non triviales.

2.2 Quelques identités

Les formes G_4^2 et G_8 sont évidemment de poids 8. Comme M_8 est de dimension 1, elles sont proportionnelles. En examinant leurs coefficients constants, on constate que

$$G_8 = 120 G_4^2.$$

Par unicité du développement en série de Fourier, on obtient l'identité suivante pour tout $n \geq 1$

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

Dans le cas où n est un premier p, on obtient

$$p^7 \equiv p^3 \mod 120.$$

(cela vient du fait que $\sigma_h(p) = p^h + 1$)

De même, en comparant G_{10} et $G_4 G_6$, on obtient

$$G_{10} = \frac{5040}{11} G_4 G_6$$

puis

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m).$$

Pour tout p premier, on obtient la congruence

$$11p^9 \equiv 21p^5 - 10p^3 \mod 5040.$$

2.3 Une congruence de Ramanujan

Définition. La fonction τ *de Ramanujan* est définie par l'égalité suivante : $\Delta(z) = \sum_{n=1}^{+\infty} \tau(n) q^n$.

Les premiers termes du dévelopement de Δ donnent :

$$\begin{aligned}
\tau(1) &= 1 \\
\tau(2) &= -24 \\
\tau(3) &= 252 \\
\tau(4) &= -1472 \\
\tau(5) &= 4830 \\
\tau(6) &= -6048
\end{aligned}$$

Proposition. *Pour tout $n \geq 1$, $\tau(n) \in \mathbb{Z}$.*

Elle se démontre en utilisant la définition de Δ à partir des séries d'Eisenstein.

Remarque. Une conjecture, attribuée à Lehmer, affirme que pour tout $n \geq 1$, $\tau(n) \neq 0$. Elle n'est toujours pas démontrée à l'heure actuelle mais a été vérifiée pour tout $n \leq 22689242781695999$.

Proposition. $\tau(n) \equiv \sigma_{11}(n) \mod 691$

Démonstration. Les formes modulaires G_{12} et G_6^2 sont dans M_{12} qui est de dimension 2. De plus, $G_{12} = \frac{691}{65520} + \cdots$ et $G_6 = \frac{1}{504} + \cdots$. Donc $65520G_{12} - 691(504)^2 G_6^2$ n'a plus de coefficient constant et tombe dans S_{12}. Comme S_{12} est de dimension 1 et engendré par Δ, il existe $\alpha \in \mathbb{C}$ tel que

$$65520G_{12} - 691(504)^2 G_6^2 = \alpha\Delta.$$

En regardant les coefficients en q des développements et en utilisant le fait que $\tau(1) = 1$, on voit que $\alpha \in \mathbb{Z}$. On identifie les coefficients des développements puis les réduit modulo 691.

$$65520\sigma_{11}(n) \equiv \alpha\tau(n) \mod 691$$

Comme $\tau(1) = 1$, $\alpha \equiv 65520 \equiv 566 \mod 691$ donc α est inversible modulo 691 qui est premier. En simplifiant des deux côtés par 691, on obtient

$$\sigma_{11}(n) \equiv \tau(n) \mod 691.$$

□

La démonstration explique comment apparaît le nombre 691 dans la congruence annoncée : c'est le numérateur du 12ème nombre de Bernoulli B_{12}.

3 Les sommes de quatres carrés

3.1 Fonction thêta

On rappelle que $A(n)$ désigne le nombre de façons d'écrire n comme somme de quatre carrés. L'idée de Jacobi est de construire une série génératrice. Formellement, considérons

$$\sum_{n\in\mathbb{N}} A(n)X^n.$$

qu'on peut réécrire ainsi

$$\sum_{n_1,n_2,n_3,n_4\in\mathbb{Z}} X^{n_1^2+n_2^2+n_3^2+n_4^2} = (\sum_{n\in\mathbb{Z}} X^{n^2})^4.$$

Il est alors naturel d'introduire la fonction suivante.

Définition. La fonction thêta est

$$\begin{array}{rccll} \theta: & \mathcal{H} & \to & \mathbb{C} & \\ & z & \mapsto & \sum_{n\in\mathbb{Z}} q^{n^2} & \text{où } q = \mathrm{e}^{2i\pi z}. \end{array}$$

Cette série converge absolument sur $\mathcal{H}$.

La fonction θ^4 serait-elle une forme modulaire ? Il est facile de voir qu'elle vérifie $\theta(z+1) = \theta(z)$. La formule de sommation de Poisson permet de montrer que

$$\sqrt{\frac{z}{2i}}\theta\left(\frac{z}{2}\right) = \theta\left(\frac{-1}{2z}\right).$$

En combinant ces deux relations, on obtient

$$\begin{aligned} &\theta^4(z+1) = \theta^4(z) \\ &\theta^4(\tfrac{z}{4z+1}) = (4z+1)^2\theta^4(z) \end{aligned}$$

Il semble alors naturel de donner une définition plus générale adaptée à cette situation. Pour un entier $N \geq 1$, on pose $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N\}$.

Définition. Une *forme modulaire de poids k pour* $\Gamma_0(N)$ est une fonction holomorphe $f : \mathcal{H} \to \mathbb{C}$ vérifiant

1) $f\left(\dfrac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

2) Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, la fonction $(cz+d)^{-k} f\left(\dfrac{az+b}{cz+d}\right)$ admet un développement de Fourier $f(z) = \sum_{n \geq 0} c_n q_N^n$ où $q_N = e^{2i\pi z/N}$.

Remarque. Par la condition 1, la fonction $(cz+d)^{-k} f\left(\dfrac{az+b}{cz+d}\right)$ est invariante par translation $z \mapsto z+N$ donc admet toujours un développement de Fourier $f(z) = \sum_{n \in \mathbb{Z}} c_n q_N^n$.

On note $M_k(\Gamma_0(N))$ le $\mathbb{C}$-espace vectoriel des formes modulaires de poids k pour $\Gamma_0(N)$. Si de plus tous les coefficients constants c_0 sont nuls, alors f est dite *parabolique*. On note $S_k(\Gamma_0(N))$ le sous-espace vectoriel des formes paraboliques. On montre que ces espaces sont de dimension finie (on dispose de formules pour leurs dimensions en fonction de k et de N).

Bien entendu, le cas $N = 1$ correspond aux formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$. Enfin, si f est modulaire pour $\mathrm{SL}_2(\mathbb{Z})$, on voit que $z \mapsto f(Nz)$ est modulaire de même poids pour $\Gamma_0(N)$.

Pour en revenir à notre problème, la fonction θ^4 est dans $M_2(\Gamma_0(4))$.

Remarque. On a $\dim S_2(\Gamma_0(N)) = 0$ pour $N = 1, 2$. C'est un élément-clé de la démonstration du théorème de Fermat.

3.2 Fausse série d'Eisenstein de poids 2

La série de fonctions définissant la série d'Eisenstein de poids k ne converge pas pour $k = 2$. On peut contourner le problème de la manière suivante.

Définition.

$$G_2^*(z) = \lim_{s \to 0} \frac{1}{2(2\mathrm{i}\pi)^2} \sum_{\substack{(m,n) \in \mathbb{Z} \times \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k} \frac{y^s}{|cz+d|^{2s}}$$

Ici, y désigne la partie imaginaire de z. Cette limite existe. La fonction ainsi obtenue vérifie la loi de transformation pour $\mathrm{SL}_2(\mathbb{Z})$. Malheureusement, elle n'est pas holomorphe à l'infini (mais elle n'est pas loin de l'être) :

$$G_2^*(z) = -\frac{1}{8\pi y} - \frac{\zeta(2)}{(2\pi)^2} + \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Remarquons que les deux termes de droite correspondent au développement en série de Fourier de G_k dans lequel on aurait fait $k = 2$. Si on considère la fonction $z \mapsto 4G_2^*(4z) - G_2^*(z)$, elle vérifie la loi de transformation pour $\Gamma_0(4)$; de plus, elle est holomorphe car les termes en $\frac{-1}{8\pi y}$ s'éliminent. Elle est donc dans $M_2(\Gamma_0(4))$.

3.3 Conclusion

Finalement $z \mapsto 4G_2^*(4z) - G_2^*(z)$ et θ^4 sont dans $M_2(\Gamma_0(4))$ qui est un espace de dimension 2. Cependant, le sous-espace $S_2(\Gamma_0(4))$ est de dimension 0. Comme

$$\theta^4(z) = (1 + \cdots)^4 = 1 + \cdots$$

et

$$4G_2^*(4z) - G_2^*(z) = -\frac{3\zeta(2)}{(2\pi)^2} + \cdots$$

on a

$$4G_2^*(4z) - G_2^*(z) + \frac{3\zeta(2)}{(2\pi)^2}\theta^4(z) = q + \cdots$$

donc

$$4G_2^*(4z) - G_2^*(z) = -\frac{3\zeta(2)}{(2\pi)^2}\theta^4(z)$$

Il ne reste plus qu'à identifier les développements de Fourier des deux membres pour obtenir

$$1 + 8\sum_{n=1}^{\infty}(\sum_{\substack{d|n \\ 4\nmid d}} d)q^n) = (\sum_{n\in\mathbb{Z}} q^{n^2})^4 = \sum_{n\in\mathbb{N}} A(n)q^n.$$

Pour tout $n > 0$, on obtient enfin

$$A(n) = 8\sum_{\substack{d|n \\ 4\nmid d}} d.$$

d'où le théorème de Jacobi.

Remarque. Des techniques similaires quoique plus délicates permettent de traiter les sommes de deux, six et huit carrés.

Bibliographie

– Serre, *Cours d'arithmétique*, PUF.
– Zagier, *Introduction to modular forms* dans *From Number Theory to Physics*, Springer.
– Hellegouarch, *Invitation aux mathématiques de Fermat-Wiles*, Dunod.

armana@math.jussieu.fr