La fonction τ de Ramanujan.

François Brunault.

Exposé au séminaire des doctorants de théorie
des nombres de Chevaleret, le 18 mars 2003.

Nous supposerons connues les bases de la théorie des formes modulaires (définition d'une forme modulaire de poids $k \geq 4$ pair et de niveau 1). Le lecteur pourra se référer à [Z] qui est une très bonne introduction.

1 Définitions.

Pour tout entier $k \geq 4$ pair, on définit la *série d'Eisenstein de poids* k par :

$$G_k(z) = \frac{(k-1)!}{2(2\pi i)^k} \sum_{(m,n)\in\mathbf{Z}^2}{}' \frac{1}{(mz+n)^k}. \tag{1}$$

Le symbole $\sum'$ indique que l'on somme sur les $(m,n) \neq (0,0)$. Cette série converge absolument car l'exposant de $(mz+n)$ est > 2. Elle définit une fonction holomorphe sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbf{C},\ \ \Im(z) > 0\}$. Il n'est pas très difficile de vérifier que G_k est modulaire de poids k, c'est-à-dire

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k G_k(z) \qquad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})\right). \tag{2}$$

La série d'Eisenstein G_k est une *forme modulaire de poids* k. Elle admet le développement de Fourier suivant, que l'on peut obtenir grâce à la formule de sommation de Poisson :

$$G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2i\pi nz}, \tag{3}$$

où B_k désigne le k-ième nombre de Bernoulli [S], et $\sigma_{k-1}(n)$ désigne la somme des puissances $(k-1)$-ièmes des diviseurs positifs de n.

Nous noterons $q = e^{2i\pi z}$, de telle sorte que G_k peut être vue comme une série entière en q, de rayon de convergence égal à 1. Notons également que le membre de droite de (3) a encore un sens pour $k = 2$, ce qui permet de définir G_2. En revanche, G_2 ne vérifie plus la condition de modularité (2). Pour les premières valeurs de k, on calcule facilement les développements suivants :

$$
\begin{array}{lclclclclclclclcl}
G_2 & = & -\frac{1}{24} & + & q & + & 3q^2 & + & 4q^3 & + & 7q^4 & + & 6q^5 & + & 12q^6 & + & \ldots \\
G_4 & = & \frac{1}{240} & + & q & + & 9q^2 & + & 28q^3 & + & 73q^4 & + & 126q^5 & + & 252q^6 & + & \ldots \\
G_6 & = & -\frac{1}{504} & + & q & + & 33q^2 & + & 244q^3 & + & 1057q^4 & + & 3126q^5 & + & 8052q^6 & + & \ldots
\end{array}
$$

Ces développements renferment de nombreuses propriétés arithmétiques. Par exemple, le coefficient de q^6 est toujours égal au produit du coefficient de q^2 par le coefficient de q^3 (c'est une conséquence de la multiplicativité de la fonction σ_{k-1}). D'autres propriétés existent, on peut par exemple chercher la relation entre le coefficient de q^2 et celui de q^4.

Remarque 1. *Le membre de droite de (3) a encore un sens et est non trivial pour k impair. On ne peut en revanche pas l'écrire sous la forme (1) car, pour des raisons de parité, cette dernière série s'annule identiquement pour $k \geq 3$ impair. Il serait donc intéressant d'interpréter autrement le membre de droite de (3) lorsque k est impair.*

Nous allons maintenant définir la fonction τ de Ramanujan.

Définition 2. *Soit Δ la série entière en q suivante*

$$\Delta = 8000 G_4^3 - 147 G_6^2. \tag{4}$$

Pour tout entier $n \geq 1$, on note $\tau(n)$ le coefficient de q^n dans Δ. On a donc par définition

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n. \tag{5}$$

La fonction τ sur $\mathbf{N}^*$ ainsi obtenue est appelée fonction τ de Ramanujan*.*

Le calcul des premiers termes donne

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \ldots. \tag{6}$$

Proposition 3. *La série entière Δ, vue comme fonction holomorphe sur $\mathcal{H}$, est une forme modulaire de poids 12.*

Démonstration. On sait que G_4 est de poids 4, et que G_6 est de poids 6. En conséquence G_4^3 et G_6^2 sont modulaires de poids respectifs $4 \times 3 = 12$ et $6 \times 2 = 12$. Il en résulte que Δ est également une forme modulaire de poids 12. □

Notons que par choix des coefficients devant G_4^3 et G_6^2, le terme constant du développement de Fourier de Δ vaut 0. On dit que Δ est une *forme parabolique* de poids 12. Cela signifie que

$$\lim_{\Im(z) \to +\infty} \Delta(z) = 0.$$

On peut même voir que $\Delta(z)$ décroît exponentiellement vite en $\Im(z)$, lorsque $\Im(z) \to +\infty$.

Avant d'entamer l'étude de la fonction τ, signalons que $\tau(n)$ a été calculé par Ramanujan pour $1 \leq n \leq 30$, puis par Lehmer pour $1 \leq n \leq 300$. Le calcul efficace de la fonction τ est l'objet de recherches actuelles [C].

2 Une congruence de Ramanujan.

Nous commençons par la proposition suivante.

Proposition 4. *La fonction τ est à valeurs entières : pour tout $n \geq 1$, on a $\tau(n) \in \mathbf{Z}$.*

Démonstration. Il est clair a priori que la fonction τ est à valeurs rationnelles. La difficulté vient du fait que les termes constants de G_4 et G_6 ne sont pas entiers.

Posons

$$G_4 = \frac{1}{240} + H_4 \qquad \text{et} \qquad G_6 = -\frac{1}{504} + H_6.$$

On a alors

$$\begin{aligned} \Delta &= 8000G_4^3 - 147G_6^2 \\ &= 8000\left(\frac{1}{240} + H_4\right)^3 - 147\left(-\frac{1}{504} + H_6\right)^2 \\ &= 8000H_4^3 - 147H_6^2 + 100H_4^2 + \frac{5H_4 + 7H_6}{12}. \end{aligned}$$

Il suffit donc de montrer que $\frac{5H_4+7H_6}{12}$ est à coefficients entiers. Or, par définition de G_4 et G_6, le n-ième coefficient de cette série entière vaut $\frac{5\sigma_3(n)+7\sigma_5(n)}{12}$.

Il s'agit donc de montrer que 12 divise $5\sigma_3(n) + 7\sigma_5(n)$, pour tout $n \geq 1$. Or

$$\begin{aligned} 5\sigma_3(n) + 7\sigma_5(n) &= \sum_{d|n} 5d^3 + 7d^5 \\ &\equiv \sum_{d|n} 7d^5 - 7d^3 \pmod{12} \\ &\equiv 7\sum_{d|n} d^3(d+1)(d-1) \pmod{12} \\ &\equiv 0 \pmod{12} \end{aligned}$$

car $d^3(d+1)(d-1)$ est divisible par 12 pour tout $d \in \mathbf{Z}$ (en effet il l'est par 4, et par 3). □

Proposition 5. *On a la congruence (dite de Ramanujan)*

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \qquad (n \geq 1). \tag{7}$$

Démonstration. Nous admettrons que l'espace M_{12} des formes modulaires de poids 12 est un espace vectoriel complexe de dimension 2 (voir [Z] pour une démonstration). En conséquence le sous-espace S_{12} des formes paraboliques est de dimension 1, et il est engendré par Δ. On a

$$G_{12} = \frac{691}{65520} + \underbrace{\dots}_{\in \mathbf{Z}[[q]]} \in M_{12},$$

$$G_6^2 = \frac{1}{504^2} + \underbrace{\dots}_{\in \frac{1}{504}\mathbf{Z}[[q]]} \in M_{12}.$$

Nous en déduisons

$$\underbrace{65520 G_{12}}_{\in \mathbf{Z}[[q]]} - 691 \times \underbrace{504^2 G_6^2}_{\in \mathbf{Z}[[q]]} \in S_{12} \cap \mathbf{Z}[[q]].$$

Il existe donc α complexe tel que $65520 G_{12} - 691 \times 504^2 G_6^2 = \alpha\Delta \in S_{12} \cap \mathbf{Z}[[q]]$. Puisque $\tau(1) = 1$, on a nécessairement $\alpha \in \mathbf{Z}$. En identifiant les n-ièmes coefficients des séries entières on obtient

$$65520\sigma_{11}(n) \equiv \alpha\tau(n) \pmod{691} \qquad (n \geq 1).$$

En faisant $n = 1$ on obtient $\alpha \equiv 65520 \equiv 566 \pmod{691}$, en particulier α est inversible modulo 691 (qui est premier). En simplifiant l'équation ci-dessus par α, on obtient $\sigma_{11}(n) \equiv \tau(n) \pmod{691}$, ce qui est la congruence recherchée. $\square$

Il existe beaucoup d'autres congruences vérifiées par les nombres $\tau(n)$. Voici quelques exemples

$$\tau(n) \equiv n\sigma_3(n) \pmod{7} \qquad (n \geq 1) \tag{8}$$

$$\tau(n) \equiv n^2\sigma_7(n) \pmod{27} \qquad (n \geq 1) \tag{9}$$

Pour plus de détails sur les congruences vérifiées par la fonction τ, ainsi que le lien avec les représentations l-adiques, on pourra se reporter à l'exposé de Serre [S2], qui est par ailleurs un très bon exposé (c'est un pléonasme) sur la fonction τ de Ramanujan.

3 Une interprétation elliptique de Δ.

Théorème 6. *(Jacobi) On a l'identité de séries formelles suivante*

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^2 4. \tag{10}$$

La démonstration de ce résultat peut être trouvée dans [Z] ou dans [S]. Un corollaire de ce théorème est que Δ ne s'annule pas sur $\mathcal{H}$.

La forme modulaire Δ est intimement liée aux courbes elliptiques. En effet, pour $z \in \mathcal{H}$, notons E_z la surface de Riemann compacte définie par

$$E_z = \frac{\mathbf{C}}{\mathbf{Z} + z\mathbf{Z}}.$$

On sait que E_z est isomorphe à la courbe elliptique sur $\mathbf{C}$ définie par l'équation

$$E_z : y^2 = 4x^3 - g_2(z)x - g_3(z)$$

où l'on a posé $g_2(z) = 20 \cdot (2\pi)^4 G_4(z)$ et $g_3(z) = -\frac{7}{3}(2\pi)^6 G_6(z)$ (attention au changement d'indice, nous avons adopté ici les notations standard).

Proposition 7. *La valeur de la forme modulaire Δ en z est égale, à un facteur près, au discriminant de la courbe elliptique E_z :*

$$\Delta(E_z) := g_2(z)^3 - 27g_3(z)^2 = (2\pi)^{12}\Delta(z) \qquad (z \in \mathcal{H}).$$

Le discriminant d'une courbe elliptique sur un corps K n'est défini qu'à un élément de $(K^*)^{12}$ près. Ici $K = \mathbf{C}$, donc $(K^*)^{12} = \mathbf{C}^*$. Cela explique le terme 'à un facteur près' dans la proposition précédente.

4 Propriétés arithmétiques de la fonction Δ.

Le développement de Fourier (6) de Δ, que nous récrivons ici :

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \dots$$

a des propriétés arithmétiques très intéressantes. En guise d'exercice (et sans lire la suite !), on peut chercher la relation entre les coefficients de q^2, q^3 et q^6, ou encore celle entre les coefficients de q^2 et q^4.

Ramanujan a le premier observé, et conjecturé en 1916, que les coefficients $\tau(n)$ sont multiplicatifs, i.e. satisfont

$$\tau(mn) = \tau(m)\tau(n) \qquad (m \text{ et } n \geq 1 \text{ premiers entre eux}). \tag{11}$$

On le vérifie ici pour $m = 2$ et $n = 3$. Cette conjecture a été démontrée un an plus tard par Mordell. Pour donner une idée de la démonstration de Mordell, nous sommes amenés à introduire les formes modulaires de Hecke.

Définition 8. *Soit $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ une forme modulaire de poids $k \geq 4$ pair. On dit que f est une* forme de Hecke *lorsque $f \neq 0$ et*

$$a_{mn} = a_m a_n \qquad (m \text{ et } n \geq 1 \text{ premiers entre eux}). \tag{12}$$

Sous cette hypothèse on a toujours $a_1 = 1$. On dit que les formes de Hecke sont *normalisées.* Les séries d'Eisenstein G_k ($k \geq 4$ pair) sont des exemples de formes de Hecke. Un théorème célèbrede Hecke affirme que les formes de Hecke de M_k (resp. S_k) forment une base de M_k (resp. S_k). La conjecture de Ramanujan découle immédiatement de ce théorème : l'espace S_{12} auquel appartient Δ est de dimension 1, et l'on a $\tau(1) = 1$, par conséquent Δ est une forme de

Hecke. En réalité, il n'est pas nécessaire d'utiliser le théorème de Hecke dans toute sa force pour démontrer la conjecture de Ramanujan. On peut se débrouiller en introduisant les opérateurs de Hecke (ce qu'a fait Mordell). On montre alors également la relation de récurrence suivante

$$\tau(p^{n+2}) = \tau(p)\tau(p^{n+1}) - p^{11}\tau(p^n) \qquad (p \text{ premier}, n \geq 0). \tag{13}$$

Cette relation permet de ramener le calcul des $\tau(n)$ ($n \geq 1$) à celui des $\tau(p)$, p premier.

5 Ordre de grandeur de la fonction τ.

Intéressons-nous maintenant à l'ordre de grandeur de $\tau(n)$. Commençons par l'ordre de grandeur des coefficients de Fourier des séries d'Eisenstein.

Proposition 9. *Soit k un entier pair ≥ 2. On a l'estimation suivante pour le n-ième coefficient de Fourier de G_k, lorsque n tend vers l'infini :*

$$a_n(G_k) = \sigma_{k-1}(n) = \begin{cases} O(n^{k-1}) & si\ k \geq 4, \\ O(n^{1+\epsilon}) & si\ k = 2 \qquad (\epsilon > 0). \end{cases} \tag{14}$$

Il n'est pas difficile de voir que ces estimations sont les meilleures possibles, du point de vue de l'exposant de n. À l'aide de la définition (4) de Δ et de cette proposition, on peut montrer à la main que

$$\tau(n) = O(n^{11}).$$

Il existe en fait un résultat plus général.

Théorème 10. *Soient k un entier pair ≥ 4 et $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ une forme modulaire de poids k. Alors on a l'estimation, lorsque n tend vers l'infini :*

$$a_n = O(n^{k-1}) \tag{15}$$

et

$$a_n = O(n^{\frac{k}{2}}) \qquad si\ f \in S_k. \tag{16}$$

En particulier, $\tau(n) = O(n^6)$.

On pourra trouver une démonstration dans [Z].

On peut encore améliorer l'exposant lorsque $f \in S_k$, mais cela demande beaucoup plus de travail !

Théorème 11. *(Deligne). Soit $f = \sum_{n=1}^{\infty} a_n q^n \in S_k$ une forme de Hecke de poids k pair ≥ 4. Alors*

$$|a_p| \leq 2p^{\frac{k-1}{2}} \qquad (p\ premier) \tag{17}$$

ou de façon équivalente

$$|a_n| \le \sigma_0(n) n^{\frac{k-1}{2}} \qquad (n \ge 1). \tag{18}$$

Ici, $\sigma_0(n)$ est le nombre de diviseurs > 0 de n. En particulier, lorsque n tend vers l'infini :

$$\tau(n) = O(n^{\frac{11}{2}+\epsilon}) \qquad (\epsilon > 0). \tag{19}$$

Ce résultat a été conjecturé par Ramanujan dans le cas de Δ, et par Petersson dans le cas général. En 1969, Deligne a montré que ce résultat était une conséquence des conjectures de Weil portant sur les variétés algébriques sur les corps finis. Il a ensuite démontré les conjectures de Weil, en 1974.

Signalons une autre conséquence du théorème de Deligne : soit $f = \sum_{n=1}^{\infty} a_n q^n \in S_k$ une forme parabolique quelconque. Définissons la fonction L de f par

$$L(f, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad (s \in \mathbf{C}). \tag{20}$$

Alors $L(f, s)$ converge pour $\Re(s) > \frac{k+1}{2}$. On peut démontrer de manière élémentaire que la fonction $L(f, s)$ se prolonge en une fonction entière sur $\mathbf{C}$ (ceci n'utilise pas le théorème de Deligne).

Notons que le problème de l'estimation des coefficients de Fourier des formes modulaires (ou plus généralement des formes automorphes) est un des problèmes majeurs de la théorie des nombres.

6 Une conjecture pour finir.

Terminons ce petit tour d'horizon de la fonction τ par la conjecture de Lehmer.

Conjecture 12. *(Lehmer) Pour tout entier $n \ge 1$, on a $\tau(n) \ne 0$.*

Par la propriété de multiplicativité (12), on se ramène au cas où n est une puissance d'un nombre premier. En utilisant la relation de récurrence (13), il me semble (mais je ne l'ai pas rédigé) que l'on peut se ramener au cas où n est un nombre premier p.

Conjecture 13. *Pour tout nombre premier p, on a $\tau(p) \ne 0$.*

À l'heure actuelle, la conjecture de Lehmer est connue pour $n \le 22689242781695999$ [JK]. Un problème lié à la conjecture de Lehmer est le suivant :

Problème ouvert 1. *Pour quels nombres premiers p a-t-on $\tau(p) \equiv 0 \pmod{p}$?*

À l'aide d'un ordinateur, on trouve que les premières valeurs de p satisfaisant $\tau(p) \equiv 0 \pmod{p}$ sont $p = 2$, 3, 5, 7 et 2411.

La condition $\tau(p) \equiv 0 \pmod{p}$ se traduit conjecturalement en terme de la représentation l-adique associée à τ (voir [S2]). Plus généralement, il est intéressant d'étudier les propriétés de τ d'un point de vue géométrique, c'est-à-dire en étudiant les propriétés du *motif* associé.

Pour de plus amples renseignements sur la fonction τ de Ramanujan, on pourra se reporter à la page web [Sl], qui contient de nombreuses références. Attention cependant, car j'ai trouvé un lien vers une page qui démontre tout bonnement la conjecture de Lehmer !

Références

[C] Charles, C. D., Computing the Ramanujan Tau Function. http ://www.cs.wisc.edu/~cdx/CompTau.pdf

[JK] Jordan, B., Kelly, B., The vanishing of the Ramanujan Tau function, Preprint, 1999.

[S] Serre, J.-P., Cours d'arithmétique. Presses Universitaires de France (1970).

[S2] Serre, J.-P., Une interprétation des congruences relatives à la fonction τ de Ramanujan, Séminaire Delange-Pisot-Poitou 9 (1967/68), Théorie des Nombres, exposé 14 (1969). Traduction anglaise http ://public.csusm.edu/public/FranzL/publ/serre.pdf

[Sl] Sloane, N. J. A. Suite A000594. In *The On-Line Encyclopedia of Integer Sequences.* http ://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi ?Anum=000594

[Z] Zagier, D. Introduction to Modular Forms. In *From Number Theory To Physics*, Waldschmidt, Moussa, Luck, Itzykson. Springer (1992), pp. 238-291.