Groupe de travail 2ème année (M1) à l'École Normale Supérieure 2025/2026

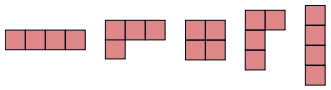
Gaëtan Chenevier, 18/09/2025

La fonction τ de Ramanujan et représentations galoisiennes

Introduction

1. Une motivation : le nombre de partitions d'un entier

Notons $\mathrm{p}(n)$ le nombre de partitions de l'entier n. Par exemple, les partitions de 4 sont $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$, également représentées par leurs *diagrammes de Ferrers*



et on a donc $\mathrm{p}(4) = 5$. Par conventions, on compte l'écriture triviale et on pose $\mathrm{p}(0) = 1$. On a également l'égalité de séries formelles (connue d'Euler)

$$\prod_{n\geqslant 1} \frac{1}{1-q^n} = \sum_{n\geqslant 0} \mathrm{p}(n) q^n, \tag{1}$$

obtenue par développement brutal en remplaçant $\frac{1}{1-q^n}$ par $\sum_{k\geqslant 0} q^{nk}$ et en constatant que $\mathrm{p}(n)$ est le nombre de suites $k_1, k_2, \ldots$ avec $k_i \geqslant 0$ et $\sum_{i\geqslant 1} i\, k_i = n$ (autrement dit, k_i est le nombre de lignes de longueur i dans le diagramme de Ferrers de la partition). Les premières valeurs de $\mathrm{p}(n)$ sont données par la table suivante :

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{p}(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176	231	297	385

La fonction $\mathrm{p}(n)$ s'avère difficile à calculer directement, notamment car ses valeurs croissent très vite : on a $\mathrm{p}(100) = 190\,569\,292$ et

$$\mathrm{p}(1000) \;=\; 24\,061\,467\,864\,032\,622\,473\,692\,149\,727\,991$$

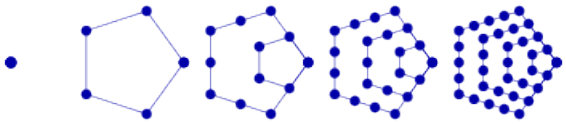
(un nombre à 32 chiffres). Il n'y a pas de formule close simple pour $\mathrm{p}(n)$, mais une formule récursive efficace due à Euler-Ramanujan, que nous allons introduire.

Rappelons que les *nombres pentagonaux généralisés* d'Euler sont les

$$\mathrm{g}_n = \frac{n(3n-1)}{2} \quad \text{avec } n \in \mathbb{Z},$$

soit $0, 1, 2, 5, 7, 12, 15, 22, 26\ldots$ (valeurs $n \geqslant 1$ en bleu). D'après les formules $\frac{n(3n-1)}{2} = n^2 + \frac{n(n-1)}{2}$ et $\frac{n(3n+1)}{2} = \frac{n(3n-1)}{2} + n$, on peut les représenter par les « *manches* »

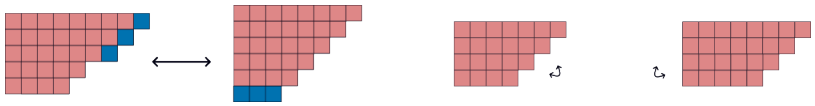
mais la terminologie vient de l'autre représentation suivante pour $n \geqslant 1$:



PROPOSITION 1.1. (Formule des nombres pentagonaux d'Euler) *On a*

$$\prod_{n\geqslant 1}(1-q^n) \;=\; \sum_{n\in\mathbb{Z}}(-1)^n q^{\frac{n(3n-1)}{2}}. \tag{2}$$

DÉMONSTRATION — Le terme de gauche est aussi la série génératrice des $x_n = \mathrm{q}^{pair}(n) - \mathrm{q}^{impair}(n)$, où $\mathrm{q}^{pair/impair}(n)$ désigne *le nombre de partitions de n en un nombre pair/impair d'entiers distincts*. La formule (3) affirme en particulier $x_n \in \{-1, 0, 1\}$ selon la "pentagonalité" de n. Elle résulte d'une involution naturelle sur les partitions en entiers distincts, que l'on peut résumer comme ci-dessous



Précisément, chaque diagramme de Ferrers a une *tête*, définie comme sa diagonale la plus à droite, et une *queue*, qui est sa dernière ligne. Par exemple, le diagramme le plus à gauche (resp. celui d'après) à une tête de taille 3 (resp. 6) et une queue de taille 4 (resp. 3). L'involution consiste, selon que la queue est strictement plus grande que la tête ou non, soit à supprimer la tête pour en faire une nouvelle queue, soit à faire l'inverse (ce qui change dans les deux cas la parité du nombre de lignes). Un peu de réflexion montre que c'est inambigu, sauf si *la tête et la queue se rencontrent et leurs tailles diffèrent d'au plus* 1. Autrement dit, c'est inambigu uniquement si le diagramme est une manche, ce qui n'arrive donc que si le nombre est pentagonal (et au plus une fois car les g_n sont distincts). Ce diagramme contribue au signe $(-1)^n$ où n est son nombre de lignes. Cette belle démonstration est due à Franklin (1881). □

REMARQUE 1.2. *Par l'identité* $\frac{n(3n-1)}{2} = \frac{(6n-1)^2-1}{24}$, *la Formule* (3) *équivaut à*

$$q^{1/24}\prod_{n\geqslant 1}(1-q^n) = \sum_{n\,\in\,6\mathbb{Z}-1} q^{n^2}(-1)^{\frac{n+1}{6}}. \tag{3}$$

Depuis Dedekind, on note η le produit de gauche (fonction η de Dedekind).

COROLLAIRE 1.3. (Formule d'Euler-Ramanujan) *Pour tout $n \geqslant 1$ on a*

$$\mathrm{p}(n) = \sum_{\{m\,\in\,\mathbb{Z}\,|\,0<\mathrm{g}_m\leqslant n\}} (-1)^{m+1}\,\mathrm{p}(n-\mathrm{g}_m) \;= \mathrm{p}(n-1)+\mathrm{p}(n-2)-\mathrm{p}(n-5)-\cdots$$

DÉMONSTRATION — On identifie simplement les coefficients en q^n dans la Formule (3), écrite sous la forme $1 = (\sum_{n\geqslant 0}\mathrm{p}(n)q^n)(\sum_{n\in\mathbb{Z}}(-1)^n q^{\mathrm{g}_n})$ via (1) dans $\mathbb{Z}[[q]]$. □

Il ne faut que 250 `ms` à mon ordinateur pour calculer tous les $\mathrm{p}(n)$ pour $n \leqslant 1000$ à l'aide de cette formule !

REMARQUE 1.4. *L'égalité* (1) *montre que la série génératrice de* $\mathrm{p}(n)$ *converge absolument pour* $|q| < 1$, *et donc* $\mathrm{p}(n) = \mathrm{O}(r^n)$ *pour tout réel* $r > 1$. *Dans un travail célèbre et difficile (1918) introduisant la fameuse méthode du cercle, Hardy et Ramanujan ont démontré l'équivalence* $\mathrm{p}(n) \sim \frac{1}{4\sqrt{3}\,n} \mathrm{e}^{\pi\sqrt{\frac{2n}{3}}}$, $n \longrightarrow +\infty$.

Terminons par une remarque sur la *formule du produit triple* de Jacobi. Pour des complexes q et ζ avec $|q| < 1$ et $\zeta \neq 0$, elle s'écrit

$$\prod_{n\geqslant 1}(1-q^{2n})(1+q^{2n-1}\zeta)(1+q^{2n-1}\zeta^{-1}) \;=\; \sum_{n\in\mathbb{Z}} q^{n^2}\zeta^n, \tag{4}$$

(avec absolue convergence des deux côtés). Elle implique aussi la Formule (3) en posant $q^2 = x^3$ et $\zeta = -qx^{-1}$. En effet, le terme de gauche est alors le produit des $(1-x^{3n})(1-x^{3n-1})(1-x^{3n-2})$ pour $n \geqslant 1$, et celui de droite la somme des $(-1)^n q^{n^2+n} x^{-n} = (-1)^n x^{\frac{n(3n-1)}{2}}$ pour $n \in \mathbb{Z}$. Voir [**HW78**, §19.8] pour une preuve élémentaire de (4).

2. La fonction τ

Dans ses recherches sur la fonction $\mathrm{p}(n)$, Ramanujan considère plusieurs puissances du produit infini $\prod_{n\geqslant 1}(1-q^n)$, et notamment la fonction suivante

$$\Delta \;:=\; \eta^{24} \;=\; q\prod_{n\geqslant 1}(1-q^n)^{24} \;=\; q - 24\,q^2 + 252\,q^3 - 1472\,q^4 + 4830\,q^5 - 6048\,q^6 + \dots$$

(Voir [**RA**, pp 194–197]) Il définit $\tau(n)$ comme étant le coefficient en q^n de Δ, *i.e.*

$$\Delta \;=\; \sum_{n\geqslant 1} \tau(n)\,q^n.$$

Il se trouve que $\tau(n)$, bien que manifestement reliée à $\mathrm{p}(n)$, se comporte très différemment, voire de manière assez magique. Comme pour $\mathrm{p}(n)$, la formule du produit ci-dessus n'est pas commode pour calculer $\tau(n)$. À la place, Ramanujan remarque *loc. cit* que si l'on pose $\sigma(n) = \sum_{d|n} d$, on a la relation de récurrence suivante :

PROPOSITION 2.1. *Pour* $n \geqslant 1$ *on a* $(n-1)\tau(n) \;=\; -24\sum_{1\leqslant k<n} \tau(k)\sigma(n-k)$.

DÉMONSTRATION — Posons $\Delta' = \frac{\partial\Delta}{\partial q}$. On a d'une part $q\Delta' = \sum_{n\geqslant 1} n\tau(n)q^n$, et d'autre part par dérivée logarithmique de la formule du produit (dans $\mathbb{Z}[[q]]$)

$$q\frac{\Delta'}{\Delta} = 1 - 24\sum_{n\geqslant 1}\frac{nq^n}{1-q^n} = 1 - 24\sum_{n,k\geqslant 1} nq^{nk} = 1 - 24\sum_{n\geqslant 1}\sigma(n)q^n.$$

Égalisant les coefficients en q^n dans $q\Delta' = qf\Delta$ on trouve l'égalité $n\tau(n) = \tau(n) - 24\sum_{0\leqslant k<n}\tau(k)\sigma(n-k)$, puis la formule de l'énoncé (on a $\tau(0) = 0$). □

Avec cette formule, il ne faut par exemple que 6 `ms` à mon ordinateur[1] pour calculer tous les $\tau(n)$ avec $n \leqslant 101$, et trouver $\tau(101) = 81\,742\,959\,102$ (11 chiffres, conforme à la borne $|\tau(101)| \leqslant 2\cdot 101^{11/2} \simeq 2\cdot 10^{11}$), et 235 `ms` pour calculer $\tau(1000)$.

1. Dans PARI/GP : `tau(n)={my(s,t); s=vector(n,u,sigma(u)); t=vector(n+1); t[1]=0; t[2]=1; for(i=2,n,t[i+1]=-24*sum(k=0,i-1,t[k+1]*s[i-k])/(i-1)); t[2..(n+1)]; };`

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	-24	252	-1 472	4 830	-6 048	-16 744	84 480	-113 643	-115 920	534 612	-370 944

Examinant alors ses tables, contenant au moins les 30 premières valeurs de τ, Ramanujan avait conjecturé en 1916 [**Ra**, §16] les identités suivantes, dans lesquelles m, n sont des entiers, et p est un nombre premier, arbitraires :

(R1) (*multiplicativité*) $\tau(mn) = \tau(m)\tau(n)$ si m et n sont premiers entre eux,

(R2) (*récurrence*) $\tau(p^{n+2}) = \tau(p)\tau(p^{n+1}) - p^{11}\tau(p^n)$,

(R3) (*borne*) $|\tau(p)| \leqslant 2p^{\frac{11}{2}}$.

Les propriétés (R1) et (R2) ont été rapidement prouvées par Mordell [**Mo**]. Les premières séances du groupe de travail auront pour but de les démontrer. Comme nous le verrons, une propriété clé satisfaite par τ est que la fonction $z \mapsto \Delta(\mathrm{e}^{2i\pi z})$ est une *forme modulaire* pour le groupe $\mathrm{SL}_2(\mathbb{Z})$. Nous commencerons donc par introduire et étudier ces objets, suivant [**Se1**]. La propriété (R3), longtemps désignée comme *la conjecture de Ramanujan*, ne l'a été que beaucoup plus tard par Deligne [**De**], comme conséquence de sa résolution des conjectures de Weil en géométrie algébrique. Sa démonstration est beaucoup plus difficile, et ne sera pas abordée. Donnons enfin deux autres formulations de (R2) et (R3) faisant intervenir le polynôme $t^2 - \tau(p)t + p^{11}$ (ou sa réciproque).

Lemme 2.2. *Les propriétés* (R2) *et* (R3) *sont respectivement équivalentes aux propriétés* (R2') *et* (R3') *ci-dessous :*

(R2') $\frac{1}{1-\tau(p)\,t+p^{11}\,t^2} = \sum_{n\geqslant 0} \tau(p^n)t^n$,

(R3') $t^2 - \tau(p)t + p^{11}$ *a deux racines complexes conjuguées (et de module* $p^{11/2}$*).*

Démonstration — Pour (R2), c'est clair en multipliant par $1 - \tau(p)t + p^{11}t^2$ des deux côtés. Pour (R3), le discriminant de $t^2 - \tau(p)t + p^{11}$ est $\tau(p)^2 - p^{11} \leqslant 0$. □

Remarque 2.3. *Ce n'est pas la fin de l'histoire ! En effet, pour p premier posons $a_p = \tau(p)/2p^{\frac{11}{2}}$. Par* (R3) *c'est un réel dans $[-1, 1]$. La conjecture de Sato-Tate, démontrée assez récemment par Barnet-Lamb, Geraghty, Harris et Taylor* [**BGHT**]*, affirme que les a_p sont équi-distribués dans $[-1, 1]$ pour la mesure $\frac{2}{\pi}\sqrt{1-t^2}\,dt$. Cela signifie que pour toute fonction continue f sur $[-1, 1]$ à valeurs dans $\mathbb{R}$, on a*

$$\sum_{p\leqslant x} f(a_p) \longrightarrow \frac{2}{\pi} \int_{-1}^{1} f(t)\ \sqrt{1-t^2}\,dt,\ \ x \to +\infty.$$

En particulier, la suite des a_p est dense dans $[-1, 1]$.

3. Congruences

Inspectant ses tables, Ramanujan a remarqué et démontré l'existence de congruences surprenantes concernant les $\mathrm{p}(n)$ et $\tau(n)$. Pour $\mathrm{p}(n)$, il a par exemple démontré :

$$\mathrm{p}(5n+4) \equiv 0 \bmod 5,\ \ \mathrm{p}(7n+5) \equiv 0 \bmod 7 \text{ et } \mathrm{p}(11n+6) \equiv 0 \bmod 11.$$

Nous allons surtout nous intéresser aux congruences portant sur $\tau(n)$. Dans l'énoncé ci-dessous, on se bornera à considérer $\tau(p)$ pour p premier, ce qui est raisonnable par (R1) et (R2) (et voir la Proposition 3.3).

THÉORÈME 3.1. (Ramanujan [**RA2, BO**]) *Pour tout premier p, on a :*

$$\tau(p) \equiv 0 \bmod 2, \tag{C1}$$

$$\tau(p) \equiv p + p^2 \bmod 3, \tag{C2}$$

$$\tau(p) \equiv p + p^2 \bmod 5, \tag{C3}$$

$$\tau(p) \equiv p + p^4 \bmod 7, \tag{C4}$$

$$\tau(p) \equiv \begin{cases} 0 \bmod 23, & \text{si } p \text{ non carré modulo } 23, \\ 2 \bmod 23, & \text{si } p \text{ de la forme } u^2 + 23v^2 \text{ et } p \neq 23, \\ 1 \bmod 23, & \text{si } p = 23, \\ -1 \bmod 23, & \text{sinon.} \end{cases} \tag{C5}$$

$$\tau(p) \equiv 1 + p^{11} \bmod 691. \tag{C6}$$

En fait, pour (C5) Ramanujan ne démontre que $\tau(p) \neq 0 \bmod 23 \Rightarrow p$ carré mod 23, le cas général est dû à Wilton [**WI**]. Les preuves de Ramanujan sont basées notamment sur des utilisations astucieuses de la formule du produit triple de Jacobi. Nous renvoyons à l'article [**BO**] pour une exposition particulièrement claire des travaux de Ramanujan (incluant les non publiés), et une discussion des travaux qui ont suivi, notamment sur $\mathrm{p}(n)$. Nous verrons ci-dessous deux exemples représentatifs des méthodes utilisées en démontrant (C1) et (C5). Les autres congruences, dont l'étonnante (C6), seront démontrées plus tard par d'autres méthodes.

EXEMPLE 3.2. *Les congruences ci-dessus déterminent $\tau(p)$ modulo $2 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 691 = 3\,337\,530$. Par exemple, un calcul montre qu'elles donnent $\tau(13) \equiv 2\,759\,792 \bmod 3\,337\,530$. Mais par* (R3) *on sait aussi $|\tau(13)| \leqslant 2 \cdot 13^{11/2} \simeq 2.68 \cdot 10^6$. On en déduit $\tau(13) = -577\,738$.*

Les conguences ci-dessus s'étendent à tous les $\tau(n)$. En effet, pour $k \geqslant 0$ posons

$$\sigma_k(n) = \sum_{d|n} d^k, \quad n \geqslant 1.$$

En particulier, $\sigma_0(n)$ est le nombre de diviseurs de n, et $\sigma_1(n) = \sigma(n)$ la somme des diviseurs de n. On a les propriétés suivantes :

(S1) (multiplicativité) $\sigma_k(mn) = \sigma_k(m)\sigma_k(n)$ si $\gcd(m, n) = 1$,

(S2) $\sigma_k(p^n) = 1 + p^k + p^{2k} + \cdots + p^{nk}$ pour tout p premier et $n \geqslant 1$.

La première vient de ce que, pour $\gcd(m, n) = 1$, tout diviseur de mn est s'écrit de manière unique sous la forme ab avec $a|m$ et $b|n$. La seconde s'écrit aussi

$$\frac{1}{1 - \sigma_k(p)t + p^k t^2} = \frac{1}{(1-t)(1-p^k t)} = \sum_{0 \leqslant k \leqslant n} p^k t^n = \sum_{n \geqslant 0} \sigma_k(p^n) t^n. \tag{5}$$

En particulier, σ_{11} satisfait l'équivalent de (R1) et (R2). [2]

2. Mais pas du tout (R3) car on a $\sigma_{11}(p) = 1 + p^{11}$.

PROPOSITION 3.3. *Soient ℓ un nombre premier et $0 \leqslant a \leqslant b$ des entiers vérifiant $a+b \equiv 11 \bmod \ell-1$ et $a+b \geqslant 1$. On a équivalence entre :*

(i) $\tau(p) \equiv p^a + p^b \bmod \ell$ pour tout premier p,

(ii) $\tau(n) \equiv n^a \sigma_{b-a}(n) \bmod \ell$ pour tout entier $n \geqslant 1$.

DÉMONSTRATION — On a (ii) $\Rightarrow$ (i) car $\sigma_k(p) = 1 + p^k$ pour p premier. Supposons (i). En utilisant la multiplicativité de $\tau(n)$ et $f(n) = n^a\sigma_{b-a}(n)$ (par (R1) et (S1)), on peut supposer que n est une puissance d'un nombre premier p. On a $f(p) \equiv \tau(p) \bmod \ell$ et $p^{a+b} \equiv p^{11} \bmod \ell$ par hypothèses. Appliquant la Formule (5) avec $k = b-a$ et $t = p^a x$, ainsi que (R2), on trouve bien dans $(\mathbb{Z}/\ell\mathbb{Z})[[x]]$

$$\sum_{n\geqslant 0} f(n)x^n \;=\; \frac{1}{1-f(p)x+p^{a+b}x^2} \equiv \frac{1}{1-\tau(p)x+p^{11}x^2} = \sum_{n\geqslant 0}\tau(n)x^n.$$

□

On en déduit que hormis (C5), les congruences du Théorème 3.1 s'étendent à tous les entiers : pour tout entier $n \geqslant 1$ on a

$$\tau(n) \equiv \begin{cases} n\,\sigma_0(n) & \bmod 2, \\ n\,\sigma_1(n) & \bmod 15, \\ n\,\sigma_3(n) & \bmod 7, \\ \sigma_{11}(n) & \bmod 11. \end{cases} \tag{6}$$

Comme $\sigma_0(p^k) = k+1$ est impair si, et seulement si, k est pair. On en déduit le joli :

COROLLAIRE 3.4. (Ramanujan) *$\tau(n)$ est impair si, et seulement si, n est un carré impair. Autrement dit, on a la congruence $\Delta \equiv \sum_{n\geqslant 0} q^{(2n+1)^2} \bmod 2\mathbb{Z}[[q]]$.*

On peut également déduire $\tau(n) \bmod \ell$ pour tout n à partir de (C5), (R1) et (R2). Posons $\mathrm{a}(n) = 1$ ou 0 selon que n pair ou impair, puis $\mathrm{b}(n) = 1, -1$ ou 0 selon que $n \equiv 0, 1$ ou $2 \bmod 3$. On a les identités

$$\frac{1}{1-t^2} = \sum_{n\geqslant 0}\mathrm{a}(n)t^n, \quad \frac{1}{1-2t+t^2} = \sum_{n\geqslant 0}(n+1)t^n \quad \text{et} \quad \frac{1}{1+t+t^2} = \sum_{n\geqslant 0}\mathrm{b}(n)t^n.$$

Le Lemme 2.2 et $n^{11} \equiv \left(\frac{n}{23}\right) \bmod 23$ (symbole de Legendre) entraînent donc :

$$\tau(p^n) \equiv \begin{cases} \mathrm{a}(n) \bmod 23, & \text{si } p \text{ non carré modulo } 23, \\ n+1 \bmod 23, & \text{si } p \text{ de la forme } u^2+23v^2 \text{ et } p \neq 23, \\ 1 \bmod 23, & \text{si } p = 23, \\ \mathrm{b}(n) \bmod 23, & \text{sinon.} \end{cases}$$

REMARQUE 3.5. (au sujet de $\mathrm{p}(n)$) *Des travaux de Ono* [**ON**] *(2000) montrent que pour tout premier $\ell > 3$, il existe une suite arithmétique infinie d'entiers n vérifiant $\mathrm{p}(n) \equiv 0 \bmod \ell$. On sait aussi qu'il n'existe pas de telle suite pour $\ell = 2, 3$. En revanche, on ne sait pas si $\mathrm{p}(n)$ est multiple de 3 pour une infinité de n, ou encore s'il existe un ensemble de densité > 0 d'entiers n avec $\mathrm{p}(n) \equiv 0 \bmod 2$.*

4. Démonstrations des congruences modulo 2 et 23

Démonstration — (Preuve de (C1)) On a $(1-x)^{24} \equiv (1-x^8)^3 \bmod 2\mathbb{Z}[x]$, puis

$$\Delta \equiv q \prod_{n\geqslant 1}(1-q^{8n})^3 \bmod 2\mathbb{Z}[[q]]. \tag{7}$$

La formule du produit triple de Jacobi pour $\zeta = q$ et $q^2 = x$ s'écrit

$$\prod_{n\geqslant 1}(1-x^n)(1+x^n)(1+x^{n-1}) \;=\; \sum_{n\in\mathbb{Z}} x^{\frac{n^2+n}{2}}.$$

Mais $1+x^{n-1}$ vaut 2 pour $n=1$, et $n \mapsto n(n+1)$ est invariant pas $n \mapsto -1-n$, d'où divisant tout par 2 l'identité remarquable

$$\prod_{n\geqslant 1}(1-x^n)(1+x^n)^2 \;=\; \sum_{n\geqslant 0} x^{\frac{n^2+n}{2}}. \tag{8}$$

En remplaçant x par q^8, et en observant $8\cdot\frac{n^2+n}{2} = (2n+1)^2-1$, on en déduit bien

$$\Delta \equiv \sum_{n\geqslant 0} q^{(2n+1)^2} \bmod 2\mathbb{Z}[[q]]. \tag{9}$$

□

Proposons maintenant une seconde preuve de (C1) utilisant la formule pentagonale d'Euler plutôt que l'identité de Jacobi, de sorte que ce texte soit auto-contenu.

Démonstration — (Seconde preuve de (C1), évitant la formule de Jacobi) On part encore de la Formule (7). La formule pentagonale d'Euler modulo 2 s'écrit alors

$$\Delta \equiv q\prod_{n\geqslant 1}(1-q^{8n})^3 \equiv \eta(q^8)^3 \equiv \sum_{a,b,c\,\in\, 6\mathbb{Z}-1} q^{\frac{a^2+b^2+c^2}{3}} \bmod 2\mathbb{Z}[q].$$

On en déduit $\tau(p) \equiv |\{(a,b,c)\in(6\mathbb{Z}-1)^2 \mid 3p = a^2+b^2+c^2\}|$. En utilisant l'involution $(a,b,c)\mapsto(c,a,b)$, de points fixes les (a,b,a), on a alors

$$\tau(p) \equiv |\{(a,b)\in(6\mathbb{Z}-1)^2 \mid 3p = 2a^2+b^2\}| \bmod 2.$$

Supposons $3p = 2a^2+b^2$ et posons $a = u-v$ et $b = u+2v$ (u et v sont entiers si $a\equiv b \bmod 3$). Alors on a $2a^2+b^2 = 3(u^2+2v^2)$, *i.e.* $p = u^2+2v^2$, et les congruences $a\equiv b\equiv -1 \bmod 6$ sont équivalentes à u impair, v pair et $u-v\equiv -1 \bmod 3$. On a donc $\tau(p)\equiv |X(p)| \bmod 2$ avec

$$\mathrm{S}(p) := \{(u,v)\in\mathbb{Z}^2 \mid p = u^2+2v^2,\ (u,v)\equiv(1,0) \bmod 2,\ u-v\equiv -1 \bmod 3\}.$$

Mais si on a $p = u^2+2v^2$ avec $u,v\in\mathbb{Z}$, on sait que les entiers u et v sont uniques au signe près.[3] Pour $p=3$, on a $(u,v) = (\pm 1,\pm 1)$ donc v est impair et $|\mathrm{S}(3)| = 0$. On peut donc supposer $p\neq 3$, ce qui entraîne $u\neq \pm v \bmod 3$, et donc que u ou v est multiple de 3. Mais alors parmi (u,v), $(-u,-v)$, $(-u,v)$ et $(u,-v)$, il y a exactement deux couples (x,y) avec $x+y\equiv -1 \bmod 3$. On a montré que dans tous les cas on a $|\mathrm{S}(p)| = 0$ ou 2, puis $\tau(p)\equiv 0 \bmod 2$. □

3. Voir [**Ch3**, Lemme 1.7 Chap. 3] pour une preuve élémentaire. Cela peut aussi se montrer en raisonnant dans l'anneau $\mathbb{Z}[\sqrt{-2}]$.

Démonstration — (Preuve de (C5)) Par le petit théorème de Fermat on a

$$\Delta \equiv q\prod_{n\geqslant 1}(1-q^n)(1-q^{23n}) \mod 23\mathbb{Z}[[q]].$$

La formule pentagonale d'Euler montre alors $\tau(23)\equiv 1 \bmod 23$, et plus généralement la remarque (1.2) montre que le terme de droite vaut

$$\sum_{r,s\in\mathbb{Z}}(-1)^{r+s}q^{(6r-1)^2+23(6s-1)^2}.$$

On a donc $\tau(p)\equiv\sum_{r,s}(-1)^{r+s} \bmod 23$, la somme portant sur les $(r,s)\in\mathbb{Z}^2$ avec

$$24p=(6r-1)^2+23(6s-1)^2. \tag{10}$$

Si un tel couple existe (et donc si $\tau(p)\not\equiv 0 \bmod 23$), on en déduit bien que p est un carré modulo 23. De plus, 2 et 3 sont des carrés modulo 23, non de la forme u^2+23v^2, et $\tau(2)=-24$ et $\tau(3)=252$ sont bien $\equiv -1 \bmod 23$. On peut donc supposer $p>3$.

Pour terminer la démonstration, nous allons utiliser la théorie des formes binaires (voir par exemple [**Ch1**, §2]). Voir aussi [**Wi**] pour des démonstrations utilisant à la place l'arithmétique de l'anneau $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ (de nombre de classes 3). Rappelons qu'à équivalence près, les deux seules formes primitives de discriminant $-4\cdot 23$ sont a^2+23b^2 et $3a^2+2ab+8b^2$. En particulier, tout nombre premier $p\neq 2,23$ tel que p est un carré modulo 23, ou ce qui revient au même tel que -23 est un carré modulo p par réciprocité quadratique, est représenté par une, et une seule, de ces deux formes.

Supposons qu'un couple (r,s) avec $r+s$ pair vérifie (10), disons $r=s+2t$. Un petit calcul montre $p=(6s-1)^2+t(6s-1)+6t^2$, et donc $t=2u$ est pair, puis

$$p=a^2+23b^2$$

avec $a=6s-1+u$ et $b=-u$, et donc $a+b\equiv -1 \bmod 6$. Réciproquement, supposons $p=a^2+23b^2$. On sait que l'écriture $p=a^2+23b^2$ est unique aux signes près de a et b [**Ch3**, Lemme 1.7 Ch. 3]. On a $a+b\equiv 1 \bmod 2$ et $\pm a\pm b\not\equiv 0 \bmod 3$ car $p\neq 3$. Ainsi, on constate que a ou b est multiple de 3, et exactement 2 couples (A,B) parmi les 4 $(\pm a,\pm b)$ vérifient $p=A^2+23B^2$ et $A+B\equiv -1 \bmod 6$. Ces deux couples sont distincts sauf pour $p=23$, *i.e.* $A=0$ et $B=-1$. Ainsi, il existe exactement deux couples (r,s) avec $r+s\equiv 0 \bmod 2$ vérifiant (10), sauf si $p=23$ auquel cas il n'y en a qu'un seul.

Supposons enfin qu'un couple (r,s) avec $r+s$ impair vérifie (10). Il sera commode de définir a et c par $a+c=r-s$ et $a-c=6s-1$ (des entiers car $r+s$ est impair). Un petit calcul montre que (10) se réécrit alors $p=3a^2+ac+2c^2$ avec $a-c\equiv -1 \bmod 6$. Comme $p>2$, on a nécessairement c pair, puis posant $c=2b$,

$$p=3a^2+2ab+8b^2 \text{ avec } a+b\equiv -1 \bmod 6.$$

On sait qu'une telle écriture de p est unique modulo $(a,b)\mapsto(-a,-b)$. Enfin, si $p=3a^2+2ab+8b^2$ avec $p>3$ on a $a+b\not\equiv 0 \bmod 3$, et donc un et un seul couple (A,B) parmi (a,b) et $(-a,-b)$ vérifie $A+B\equiv -1 \bmod 6$. □

5. Représentations galoisiennes modulaires

L'un des buts de ce groupe de travail sera d'une part d'avoir un autre point de vue sur les congruences de la Section 3 portant sur les $\tau(n)$, et d'autre part de comprendre pourquoi, en un certain sens que nous préciserons, *ce sont les seules congruences modulo un premier portant sur les* $\tau(n)$. Les deux outils que nous utiliserons seront la théorie des formes modulaires modulo p développée dans [**SD**], de la théorie algébrique des nombres et des représentations galoisiennes. Un résultat clé sera alors le suivant, démontré par Deligne [**De**] en même temps que (R3) :

Théorème 5.1. (Deligne) *Pour tout nombre premier ℓ, il existe :*

(i) un corps de nombres K_ℓ galoisien sur $\mathbb{Q}$ et non ramifié hors de ℓ,
(ii) une représentation fidèle et semisimple $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

vérifiant, pour tout nombre premier $p \neq \ell$,

$$\mathrm{trace}\,\rho_\ell(\mathrm{Frob}_p) \equiv \tau(p) \bmod \ell \quad \text{et} \quad \det \rho_\ell(\mathrm{Frob}_p) \equiv p^{11} \bmod \ell.$$

Il s'agira d'abord de comprendre ce que signifie cet énoncé ! Il établit un lien surprenant entre la décomposition des nombres premiers p dans le corps K_ℓ et les $\tau(p) \bmod \ell$, donnant un tout autre point de vue sur les congruences mod ℓ. Plusieurs exposés seront consacrés à des notions de théorie algébrique des nombres, suivant par exemple les chapitres 12 et 13 de [**IR**], en vue de comprendre ces assertions. Nous ne démontrerons pas le Théorème 5.1, car la démonstration est très difficile. En revanche, nous verrons comment l'appliquer pour étudier $\tau(n) \bmod \ell$, suivant des idées de Serre [**Se2**] et Swinnerton-Dyer [**SD**], et cela devrait prendre tout le temps imparti. L'étude des images possibles de ρ_ℓ, et en particulier des sous-groupes de $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, jouera un rôle.

Remarque 5.2. *Une conséquence du théorème de Cebotarev et du théorème de Brauer-Nesbitt est que si (K_ℓ, ρ_ℓ) existe, alors K_ℓ est uniquement déterminé à l'intérieur de $\mathbb{C}$, et ρ_ℓ est également unique à conjugaison près par $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Par exemple, nous verrons que la congruence* (C1) *est équivalente à $K_2 = \mathbb{Q}$ et $\rho_\ell = 1$.*

Bibliographie

[BGHT] T. Barnet-Lamb, D. Geraghty, M. Harris & R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, P.R.I.M.S. 47 (2011).

[BO] B. C. Berndt & K. Ono, *Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary*, Séminaire Lotharingien de Combinatoire (1999).

[Ch1] G. Chenevier, *Théorie algébrique des nombres*, cours à l'École Polytechnique 2010-2019.

[Ch2] G. Chenevier, *Introduction aux formes modulaires*, mini-cours à l'ÉNS (2015).

[Ch3] G. Chenevier, *Algèbre 1*, cours à l'ENS (2021-2024).

[De] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, séminaire Bourbaki (1968).

[HW78] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford University Press (1975).

[IR] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84 (1990).

[Wi] R. Wilton, *Congruence properties of Ramanujan's function $\tau(n)$*, Proc. London Math. Soc. (2) 31 (1930).

[Mo] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Camb. Philos. Soc. 19 (1917).

[On] K. Ono, *Distribution of the Partition Function Modulo m*, Annals of Mathematics 151 (2000).

[Ra] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. 22 (1916).

[Ra2] S. Ramanujan, *Congruence properties of partitions*, non publié, archives Trinity College Cambridge.

[Se1] J. P. Serre, *Cours d'arithmétique*, P. U. F. (1970).

[Se2] J. P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou 9 (1967-1968).

[SD] H. P. F. Swinnerton Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, International Summer School on Modular Functions, Antwerp (1972).